FORUM Wirtschaftsrecht - Band 14

Institut für Wirtschaftsrecht

Mark Bedner

Cloud Computing

Technik, Sicherheit und rechtliche Gestaltung

kassel university press

FORUM Wirtschaftsrecht

Band 14

Herausgegeben vom
Institut für Wirtschaftsrecht an der Universität Kassel

Cloud Computing

Technik, Sicherheit und rechtliche Gestaltung

Mark Bedner

kassel
university
press

Die vorliegende Arbeit wurde vom Fachbereich Wirtschaftswissenschaften der Universität Kassel als Dissertation zur Erlangung des akademischen Grades eines Doktors der Rechtswissenschaften (Dr. jur.) angenommen.

Erster Gutachter: Prof. Dr. Alexander Roßnagel
Zweiter Gutachter: Prof. Dr. Dr. Walter Blocher

Tag der mündlichen Prüfung 29. November 2012

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar

Zugl.: Kassel, Univ., Diss. 2012
ISBN print: 978-3-86219-080-5
ISBN online: 978-3-86219-081-2
URN: http://nbn-resolving.de/urn:nbn:de:0002-30816

© 2013 kassel university press GmbH, Kassel
www.uni-kassel.de/upress

Druck und Verarbeitung: Unidruckerei der Universität Kassel
Umschlaggestaltung: Heike Arend, Unidruckerei der Universität Kassel
Printed in Germany

Vorwort

Cloud Computing verspricht völlig neue Möglichkeiten, Datenverarbeitungsprozesse zu organisieren und zu finanzieren. Indem Hardware und Software nicht mehr als Eigentum von jedem Nutzer erworben werden müssen, sondern als Dienstleistung nur für die jeweilige Nutzungszeit und im jeweiligen Nutzungsumfang quasi „aus der Steckdose“ abgerufen werden können, erhalten Unternehmen und Verwaltungen im Umgang mit Informationstechnik bisher ungeahnte Freiheitsspielräume. Um diese Dienstleistungen über das Internet bei jeder Nachfrage zuverlässig erbringen zu können, nutzen die – meist großen, weltweit operierenden – Anbieter auch die jeweils verfügbare Hard- und Software von vielen Unterauftragnehmern, die unter Umständen weltweit verteilt sind. Da die Dienstleistungen über automatisierte Prozesse abgerufen und erbracht werden, kann oft niemand genau angeben, wo in der „Cloud“ die Software heruntergeladen oder Daten gespeichert oder verarbeitet werden.

Diese neue Freiheit ist für die Cloud-Nutzer aber auch mit neuen Risiken für die Sicherheit der Prozesse, die Vertraulichkeit der Daten und die Unabhängigkeit der Nutzer verbunden. Für bestimmte Nutzergruppen stellt sich daher die Frage, ob sie Cloud Computing für bestimmte Verfahren und für bestimmte Daten nutzen können, ohne gegen die ihnen anvertrauten Interessen Dritter zu verstoßen, wenn sie solche Risiken eingehen. Daher ist für Cloud Computing generell die Frage zu beantworten, ob und wo für die Nutzung dieser neuen Dienstleistung rechtliche Grenzen bestehen.

Für die rechtlichen Fragen, die Cloud Computing aufwirft, gibt es jedoch keine gesetzliche Regelung. Vielmehr muss zur Lösung von Problemen, die durch Cloud Computing verursacht werden, auf allgemeine Regelungen zurückgegriffen werden. Diese sind in ihrer Konzeption nicht auf die Spezifika des Cloud Computing ausgerichtet. Um sie auf Cloud Computing anwenden zu können, müssen sie durch entsprechende Interpretation und Konkretisierung an dessen Eigenheiten angepasst werden. Dies ist deshalb besonders schwierig, weil die charakteristischen Eigenschaften des Cloud Computing sich diametral von den konzeptionellen Grundprinzipien von Rechtsregeln unterscheiden. Cloud Computing ist eine dynamische Dienstleistung, die flexibel angeboten und bedarfsorientiert abgerufen wird, die nicht von Personen, sondern durch automatische Prozesse erbracht wird und die vom Ort der Leistungserbringung unabhängig ist und daher von jedem Ort weltweit angeboten und erbracht werden kann. Dagegen sind Rechtsregeln jeweils genau durch das Gegenteil ausgezeichnet. Sie enthalten (meist) eine feste, statische normative Vorgabe, die prinzipielle Geltung beansprucht, ausreichend bestimmt sein muss, personenbezogen und bezogen auf ein bestimmtes Gebiet zur Anwendung kommt und nur national gilt. Daher stellt sich die erste sehr schwierig zu beantwortende Frage, wie das geltende Recht zu konkretisieren ist, um den Fragestellungen, die das Cloud Computing aufwirft, gerecht werden zu können.

Zugleich stellt sich aber eine weitere wichtige Frage. Die derzeit allein anwendbaren allgemeinen Regelungen schützen bestimmte Interessen, die nicht einfach zur Durchsetzung neuer Technikkonzepte aufgegeben werden können. Daher darf Recht sich nicht nur den neuen Anforderungen des Cloud Computing anpassen, sondern muss auch versuchen, Cloud Computing nach rechtlichen Vorgaben so zu gestalten, dass die rechtlich zu schützenden Interessen gewahrt werden. Hierfür muss Recht Anforderungen an Funktionen dieser Technik stellen oder diese beschränken. Cloud Computing wirft daher eine zweite Frage auf, ob und wie aus den bestehenden Rechtsregelungen technisch-organisatorische Anforderungen und Gestaltungsvorschläge abgeleitet werden können oder ob neue Rechtsregeln erlassen werden müssen, die Technikmerkmale und Anwendungsbedingungen des Cloud Computing berücksichtigen, aber die rechtlich gebotenen Zielsetzungen ohne Funktions- und Niveauverlust erreichen.

Für beide Fragen bietet die Arbeit von Herrn Bedner Antworten an. Sie verfolgt das Ziel, auf der Grundlage eines technischen Verständnisses von Cloud Computing Untersuchungen durchzuführen, um „die passenden rechtlichen Vorschriften direkt oder analog anwenden zu können und effektive technische Gestaltungsvorschläge unterbreiten zu können“. Sie legt dabei zurecht einen Schwerpunkt auf die Gewährleistung einer ausreichenden Sicherheit des Cloud Computing für die zu schützenden Interessen, das wohl größte rechtliche Problem dieses neuen Paradigmas der Techniknutzung. Beide Zielsetzungen sind methodisch und fachlich eine große Herausforderung, die in der Arbeit aber souverän bewältigt wird. Mit ihr füllt Herr Bedner zwei wesentliche Lücken im Recht des elektronischen Rechtsverkehrs. Indem er die für die Sicherheit des Cloud Computing geltenden Regelungen zusammenträgt und hinsichtlich ihrer Anforderungen überprüft, bietet er sowohl wertvolle Hinweise für das notwendige Rechtsverständnis gegenüber modernster Informationstechnologie und damit grundlegende Hilfestellungen für die Praxis. Indem er zeigt, wie technische Gestaltungsziele und -vorschläge aus verfassungs- und einfachrechtlichen Vorgaben abgeleitet werden können, trägt er zur Bewältigung schwieriger grundlegender methodischer Fragen der rechtswissenschaftlichen Technikgestaltung bei und bietet viele innovative Hinweise zur rechtskonformen Fortentwicklung des Cloud Computing.

Die Arbeit entstand zu großen Teilen im Rahmen der Mitarbeit im Center for Advanced Security Research Darmstadt (CASED), das im Rahmen der Landes-Offensive zur Entwicklung wissenschaftlich-ökonomischer Exzellenz (LOEWE) des Landes Hessen gefördert wird. Die dort entstehenden Rechtsfragen werden von der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Forschungszentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel erforscht. Im Arbeitsbereich „Sichere Dienste“ konnte Herr Bedner von 2009 bis 2011 die Frage des Cloud Computing in enger interdisziplinärer Zusammenarbeit zusammen mit Informatikern und Ökonomen untersuchen.

Es ist der Arbeit zu wünschen, dass sie von denjenigen ebenso zur Kenntnis genommen wird, die für die Entwicklung und Gestaltung von Cloud Computing verantwortlich sind, wie auch von denjenigen, die für die Fortentwicklung des Datenschutzrechts Verantwortung tragen.

Kassel, Dezember 2012 *Prof. Dr. Alexander Roßnagel*

Vorwort des Autors

Diese Dissertation ist während meiner Zeit als wissenschaftlicher Mitarbeiter in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) und als Stipendiat des interdisziplinären Centers for Advanced Security Research Darmstadt (CASED) entstanden. Ausgangspunkt für die Entstehung der Dissertation war die Kooperation zwischen provet und dem CASED-Arbeitsbereich „Sichere Dienste“.

Die Dissertation wurde im Wintersemester 2012/2013 von der Universität Kassel angenommen. Grundlage der Veröffentlichung ist der Literatur- und Gesetzesstand vom Dezember 2011.

Zum Gelingen dieser Arbeit haben viele Menschen beigetragen, deren namentliche Aufzählung allerdings den Rahmen sprengen würde.

Mein ganz besonderer Dank gilt meinem Doktorvater Prof. Dr. Alexander Roßnagel. Sein Vertrauen in meine Fähigkeiten und seine stets positiven Anregungen haben mir die Erstellung der Dissertation erst möglich gemacht. Die Mischung aus wissenschaftlichen Freiräumen, konstruktiver Kritik und sein immerzu freundlicher und respektvoller Umgang waren vorbildlich. Ebenso möchte ich ihm für die Begutachtung der Arbeit und seine Unterstützung bei der Veröffentlichung danken.

Herrn Prof. Dr. Dr. Walter Blocher danke ich für die zügige Erstellung des Zweitgutachtens.

Meinen ehemaligen Kollegen von provet danke ich ganz herzlich für die drei besonders schönen und erkenntnisreichen Jahre der Zusammenarbeit. Sie standen mir allzeit mit freundschaftlichem und kollegialem Rat zur Seite. Ich bedanke mich zudem für die Unterstützungen, Aufmunterungen und Ablenkungen während der gemeinsamen Zeit.

Die freie, freundschaftliche und lehrreiche Arbeitsatmosphäre in Kassel war für die erfolgreiche Fertigstellung der Dissertation von großer Bedeutung. Bessere Forschungs- und Arbeitsbedingungen konnte man sich nicht wünschen.

Meinem Projektpartner Dr. Tobias Ackermann danke ich ganz herzlich für die kollegiale und konstruktive Zusammenarbeit im Rahmen des CASED.

Dank gebührt auch meinem privaten Umfeld und Freundeskreis für die Motivation, den Beistand und die notwendigen Abwechslungen und Zeitvertreibe.

Der größte Dank gilt meinen Eltern, die mir durch ihre andauernde Unterstützung meine berufliche und persönliche Entwicklung überhaupt erst ermöglicht und deren Zuversicht und Vertrauen in meine Fähigkeiten mir stets den notwendigen Rückhalt gegeben haben. Ihnen widme ich diese Arbeit.

Zweibrücken, Dezember 2012 *Mark Bedner*

Inhalt

Abkürzungsverzeichnis……XXV
Abbildungsverzeichnis……..XXXIV

1 Einleitung 1
1.1 Cloud Computing als Dienstleistung 6
1.2 Konsequenzen des Cloud Computing für sonstige Dienstleistungen im Internet .. 7
1.3 Bedeutung der Sicherheit 8
1.3.1 IT-Sicherheit 8
1.3.2 Rechtssicherheit 9
1.4 Vorlaufende Technikgestaltung anhand der KORA-Methode 10
1.5 Rolle des Rechts im Verhältnis zur Technik 10
1.5.1 Einordnung der KORA-Methode in den Gesamtzusammenhang 10
1.5.2 Technikrecht als historisch gewachsenes Beispiel für das Verhältnis zwischen Recht und Technik 12
1.6 Forschungsbedingungen und Notwendigkeit einer interdisziplinären Herangehensweise 14
1.7 Gang der Untersuchung 14

2 Untersuchungsgegenstand 16
2.1 Begriff des Cloud Computing 16
2.1.1 Cloud Computing als Hype? 17
2.1.2 Definitionsversuche 22
2.1.3 Vorzugswürdige Definition 24
2.1.4 Informationstechnische Systeme, Cloudsysteme und Cloudumgebungen 24
2.2 Begriffliche Einordnung 25
2.2.1 Technologie und Technik 26
2.2.2 Konzept 26
2.2.3 Paradigma und Inhalt des Paradigmenwechsels 27

2.2.4 Geschäftsmodell 28
2.2.5 Konsequenzen der begrifflichen Einordnung 28
2.3 Detailstruktur des Cloud Computing 28
2.3.1 Architektur und Erscheinungsformen (Schichtenmodell) 29
2.3.1.1 Infrastructure as a Service (IaaS) 29
2.3.1.2 Platform as a Service (PaaS) 30
2.3.1.3 Software as a Service (SaaS) 30
2.3.1.4 Weitere Services (XaaS) 31
2.3.2 Nutzungsmodelle 32
2.3.2.1 Public und External Cloud 32
2.3.2.2 Private Cloud 33
2.3.2.3 Internal Cloud 33
2.3.2.4 Hybrid Cloud 34
2.3.2.5 Virtual Private Cloud 35
2.3.2.6 Community Cloud 36
2.3.3 Beteiligte 37
2.3.3.1 Cloudnutzer und Cloudanbieter 37
2.3.3.2 Ressourcenanbieter (Subunternehmen) 38
2.3.3.3 Telekommunikationsanbieter 38
2.3.4 Technische und infrastrukturelle Voraussetzungen 38
2.3.4.1 Virtualisierung 39
2.3.4.1.1 Vorteile der Virtualisierung 39
2.3.4.1.2 Virtualisierung und Cloud Computing 40
2.3.4.2 Virtualisierungsformen 41
2.3.4.2.1 Hypervisorbasierte Virtualisierung 42
2.3.4.2.2 Netzwerkvirtualisierung mittels VLAN und VPN 42
2.3.4.2.3 Speichervirtualisierung 43
2.3.4.3 Verteilte Systeme, Parallelisierung und Computercluster 43
2.3.4.4 Flächendeckende Durchsetzung von Breitbandinternetzugängen 45
2.3.5 Merkmale und Eigenschaften des Cloud Computing 47
2.3.5.1 Mehrmandantenfähigkeit 47

2.3.5.2 Schnelle Bereitstellung und Self-Service-Modell 47
2.3.5.3 Einfachere Wartung und Aufrüstung 48
2.3.5.4 On-Demand-Nutzung 49
2.3.5.5 Geographische Verteilung der Server 49
2.3.5.6 Zuverlässigkeit, Verfügbarkeit und Robustheit 50
2.3.5.7 Skalierbarkeit 51
2.3.5.8 Homogenität 51
2.3.5.9 Messbarkeit und Überprüfbarkeit 52
2.3.5.10 Lizenzfreiheit und -klarheit 52
2.3.6 Entwicklung des Cloud Computing und Abgrenzung zu seinen Vorläufermodellen 52
2.3.6.1 Internet und verteilte Systeme 54
2.3.6.2 Cluster Computing 55
2.3.6.3 Grid Computing 56
2.3.6.4 Utility Computing 58
2.3.6.5 Klassisches IT-Outsourcing 58
2.3.6.6 Application Service Providing (ASP) 61
2.3.6.7 Verhältnis von Cloud Computing zu serviceorientierten Architekturen (SoA) 63
2.3.7 Anwendungsbereiche, Anwendungsbeispiele und Einsatzszenarien 64
2.3.7.1 Privatbereich 64
2.3.7.1.1 Mailservices 64
2.3.7.1.2 Fotodienste und Webalben 65
2.3.7.1.3 Filehosting und Storage 65
2.3.7.1.4 Spiele (Cloud Gaming) 66
2.3.7.1.5 Weitere Dienste 68
2.3.7.2 Unternehmensbereich 69
2.3.7.2.1 Startupunternehmen 69
2.3.7.2.2 Unternehmen mit bestehender Infrastruktur 69
2.3.7.2.3 Konkrete Anwendungsbereiche in Unternehmen 70
2.3.7.3 Behörden und öffentliche Verwaltung 71

2.3.8 Ausgewählte Cloudprovider ... 72
2.3.8.1 Amazon ... 73
2.3.8.2 Salesforce ... 76
2.3.8.3 Google ... 78
2.3.8.4 Microsoft ... 80
2.3.9 Weitere Cloudprovider ... 82
2.3.10 Provider im öffentlichen Bereich ... 83
2.4 Soziale Folgen des Cloud Computing ... 84
2.4.1 Chancen und Risiken des Cloud Computing ... 85
2.4.1.1 Vorteile und Chancen ... 85
2.4.1.1.1 Kostenersparnis ... 85
2.4.1.1.2 Förderung des Wirtschaftswachstums ... 87
2.4.1.1.3 Hohe Skalierbarkeit ... 88
2.4.1.1.4 Verfügbarkeit ... 89
2.4.1.1.5 Elastizität und Flexibilität ... 90
2.4.1.1.6 Energieeffizienz und Umweltschutz ... 90
2.4.1.1.7 Ortsunabhängigkeit ... 93
2.4.1.1.8 Einfachheit ... 94
2.4.1.1.9 Unabhängigkeit von proprietären Betriebssystemen ... 94
2.4.1.1.10 Sicherheit ... 95
2.4.1.1.11 Verringerung von Datensätzen und Verarbeitungsvorgängen durch Zentralisierung ... 97
2.4.1.1.12 Demokratisierung und Innovationsförderung ... 98
2.4.1.1.13 Zukunftssicherheit ... 99
2.4.1.2 Nachteile und Risiken ... 101
2.4.1.2.1 Unvorhersehbare Fehler ... 101
2.4.1.2.2 Lock-In-Effekte und fehlende Standards ... 102
2.4.1.2.3 Oligopolbildung und marktbeherrschende Stellung ... 103
2.4.1.2.4 Gefahr der Profilbildung und Weitergabe von Daten ... 103
2.4.1.2.5 Bedrohungen ... 104

3 Rechtsrahmen und rechtliche Aspekte des Cloud Computing 105
3.1 Datenschutzrecht 105
3.1.1 Entwicklung des Datenschutzrechts 105
3.1.2 Zwischenstaatliche Regelungen zum Datenschutz 107
3.1.2.1 Internationale Abkommen 107
3.1.2.2 Europarecht und Europäische Abkommen 108
3.1.2.2.1 EU-Ebene 108
3.1.2.2.2 Europaratsebene 109
3.1.3 Nationales Verfassungsrecht 110
3.1.3.1 Recht auf informationelle Selbstbestimmung 110
3.1.3.2 Vertraulichkeit und Integrität informationstechnischer Systeme 112
3.1.3.3 Telekommunikationsgeheimnis 113
3.1.3.4 Wirtschaftsgrundrechte 113
3.1.4 Cloud Computing als Telekommunikation oder Telemedium? 115
3.1.4.1 Cloud Computing als Telekommunikationsdienstleistung? 115
3.1.4.2 Cloud Computing als Telemediendienst? 116
3.1.4.3 Konsequenzen für den Datenschutz und Abgrenzung 116
3.1.5 Anwendungs- und Geltungsbereich des Bundesdatenschutzgesetzes 118
3.1.5.1 Normadressaten 118
3.1.5.2 Sachlicher Anwendungsbereich 118
3.1.5.3 Personenbezogene Daten 119
3.1.5.3.1 Definition gemäß § 3 BDSG und Relativität des Personenbezugs 119
3.1.5.3.2 Einordnung verschlüsselter personenbezogener Daten 120
3.1.5.4 Räumlicher Geltungsbereich 121
3.1.6 Datenschutzprinzipien 123
3.1.6.1 Notwendigkeit eines Erlaubnistatbestands und Gedanke der Selbstbestimmung 123
3.1.6.2 Transparenz 123
3.1.6.3 Grundsatz der Direkterhebung 124
3.1.6.4 Erforderlichkeit 124

3.1.6.5 Datenvermeidung und Datensparsamkeit 125
3.1.6.6 Zweckfestlegung, Zweckbindung, informationelle Gewaltenteilung 127
3.1.7 Cloud Computing und Behörden 128
3.1.7.1 Datenschutzrecht 128
3.1.7.2 Verbot der Mischverwaltung gemäß Art. 83 GG 129
3.1.7.3 IT-Zusammenarbeit gemäß Art. 91c GG 130
3.1.8 Auftragsdatenverarbeitung 130
3.1.8.1 Auftrag 131
3.1.8.2 Beteiligte, Privilegierungsfunktion und Rechtsstellung 132
3.1.8.3 Theorie der Funktionsübertragung 133
3.1.8.4 Cloud Computing als Auftragsdatenverarbeitung? 136
3.1.8.4.1 Infrastructure as a Service 137
3.1.8.4.2 Restliche Services (PaaS, SaaS) 138
3.1.8.5 Detailstruktur der Auftragsdatenverarbeitung 139
3.1.8.5.1 Pflichten des Auftraggebers und wesentliche Merkmale einer Auftragsdatenverarbeitung den Auftraggeber betreffend 139
3.1.8.5.2 Kontrollrechte des Auftraggebers 148
3.1.8.5.3 Pflichten des Auftragnehmers 149
3.1.8.5.4 Wartungs- und Servicearbeiten 151
3.1.8.5.5 Bußgeldtatbestände 151
3.1.8.6 Mögliches Transparenzproblem und Problem der Unterbeauftragung (Auslagerungsketten) 152
3.1.8.7 Spezialregelungen 154
3.1.8.8 Datenschutzrechtlicher Reformbedarf 156
3.1.9 Technisch-organisatorische Maßnahmen zur IT- und Datensicherheit 157
3.1.9.1 IT-Sicherheit und Datensicherheit 157
3.1.9.2 Bedeutung der Sicherheit allgemein und für den weiteren Gang der Untersuchung 158
3.1.9.3 Geltende Rechtslage 160
3.1.9.3.1 Regelungsinhalt des § 9 BDSG und der Anlage zu Satz 1 161
3.1.9.3.2 Maßnahmen gemäß der Anlage 162

3.1.9.3.2.1 Zutrittskontrolle (Nr. 1) ... 163
3.1.9.3.2.2 Zugangskontrolle (Nr. 2) ... 164
3.1.9.3.2.3 Zugriffs- und Speicherkontrolle (Nr. 3) ... 166
3.1.9.3.2.4 Weitergabekontrolle (Nr. 4) ... 167
3.1.9.3.2.5 Eingabekontrolle (Nr. 5) ... 169
3.1.9.3.2.6 Auftragskontrolle (Nr. 6) ... 170
3.1.9.3.2.7 Verfügbarkeitskontrolle (Nr. 7) ... 171
3.1.9.3.2.8 Trennungsgebot (Nr. 8) ... 172
3.1.9.3.3 Spezialvorschrift des § 109 TKG ... 172
3.1.9.3.4 Wertungen des Bundesverfassungsgerichts zur Vorratsdatenspeicherung ... 174
3.1.9.4 Datenschutzrechtlicher Reformbedarf ... 175
3.1.9.5 Schutzziele der IT-Sicherheit ... 176
3.1.9.5.1 Vertraulichkeit ... 176
3.1.9.5.2 Unverkettbarkeit ... 177
3.1.9.5.3 Nicht-Verfolgbarkeit ... 178
3.1.9.5.4 Unbeobachtbarkeit ... 179
3.1.9.5.5 Verdecktheit ... 179
3.1.9.5.6 Anonymität und Pseudonymität ... 180
3.1.9.5.7 Transparenz ... 181
3.1.9.5.8 Zurechenbarkeit ... 182
3.1.9.5.9 Authentizität ... 183
3.1.9.5.10 Revisionsfähigkeit ... 183
3.1.9.5.11 Verfügbarkeit ... 184
3.1.9.5.12 Integrität ... 185
3.1.9.5.13 Verlässlichkeit ... 185
3.1.9.5.14 Beherrschbarkeit ... 186
3.1.9.5.15 Nicht-Vermehrbarkeit ... 186
3.1.9.5.16 Kontingenz und glaubhafte Abstreitbarkeit ... 187
3.1.9.6 Konzept der mehrseitigen Sicherheit ... 188
3.1.9.7 Zentrale Probleme des Cloud Computing ... 190

3.1.9.7.1 Vertraulichkeit 190
3.1.9.7.2 Integrität 191
3.1.9.7.3 Transparenz 192
3.1.9.7.3.1 Technikbedingte Intransparenz 193
3.1.9.7.3.2 Anbieterbedingte Intransparenz 193
3.1.9.7.4 Bedeutung sonstiger Schutzziele 194
3.1.9.8 Bedrohungsanalyse 194
3.1.9.8.1 Begriffsdefinitionen und gegenseitige Abgrenzung 196
3.1.9.8.1.1 Bedrohung, Gefährdung und verwandte Begriffe 196
3.1.9.8.1.2 Bedeutungen des Gefahrbegriffs und Abgrenzung zur Gefährdung 197
3.1.9.8.1.3 Schadensbegriff 199
3.1.9.8.1.4 Risiko und Risikovorsorge 201
3.1.9.8.2 Bedrohungsklassifizierungen 204
3.1.9.8.2.1 Unbeabsichtigte Eingriffe 204
3.1.9.8.2.2 Beabsichtigte Eingriffe 205
3.1.9.8.3 Komplexität und IT-Sicherheit 206
3.1.9.8.4 Angreifertypen 209
3.1.9.8.5 Angriffsarten 210
3.1.9.8.5.1 Passive Angriffe 210
3.1.9.8.5.2 Aktive Angriffe 212
3.1.9.9 Allgemeine Sicherheitsmaßnahmen 213
3.1.9.9.1 Verschlüsselung 214
3.1.9.9.2 Systemtrennung, Abschottung und Kanalisierung von Datenströmen 215
3.1.9.9.3 Datentrennung 216
3.1.9.9.4 Rollentrennung 217
3.1.9.9.5 Protokollierung 217
3.1.9.9.6 Redundanz 218
3.1.9.9.7 Nutzungskompetenz und IT-Sicherheitsbewusstsein 218
3.1.9.9.8 Audits und Zertifizierungen 219

3.1.9.10 Neuartige cloudspezifische Bedrohungen und notwendige Sicherheitsmaßnahmen 221
3.1.9.10.1 Bedrohungen durch unzureichende Trennung und Segmentierung 221
3.1.9.10.1.1 Hypervisorsicherheit 222
3.1.9.10.1.2 Absicherung des Management Interfaces und des Datenverkehrs durch Trennung 224
3.1.9.10.2 Kontrollverlust durch Verteilung 225
3.1.9.10.3 Kontrollverlust durch die Weiterübermittlung von Daten 226
3.1.9.10.4 Abhängigkeit der Nutzer vom Provider in Sicherheitsfragen 226
3.1.9.10.5 SoA-bedingte Bedrohungen 227
3.1.9.10.6 Bedrohungen für Rechtsgüter Dritter durch Clouddienste 227
3.1.9.11 Sicherheitskonzept 228
3.1.10 Datenschutzaudit 229
3.1.11 Verpflichtung der Mitarbeiter auf das Datengeheimnis 231
3.1.12 Datenübermittlung ins außereuropäische Ausland 233
3.1.12.1 Erlaubnisnormen und Zusammenwirken mit §§ 4b und 4c BDSG 234
3.1.12.1.1 Öffentliche und nichtöffentliche Stellen als Übermittler 234
3.1.12.1.2 Erforderlichkeit 235
3.1.12.1.3 Weitere Voraussetzungen 235
3.1.12.1.4 Interesse des Betroffenen an einem Ausschluss der Übermittlung 236
3.1.12.1.5 Einwilligung 237
3.1.12.1.6 Zwischenergebnis 237
3.1.12.2 Besondere Arten personenbezogener Daten 237
3.1.12.3 Bereichsspezifische Vorschriften außerhalb des BDSG 238
3.1.12.4 Angemessenheit des Datenschutzniveaus als Interessensaspekt 239
3.1.12.5 Ausnahmen gemäß § 4c BDSG 239
3.1.12.5.1 EU-Standardvertragsklauseln 241
3.1.12.5.1.1 Inhalt und Bedeutung 241
3.1.12.5.1.2 Möglichkeit der Unterauftragsverarbeitung 242

3.1.12.5.1.3 Anwendbarkeit bei innereuropäischer Unterauftragsdatenverarbeitung? 243
3.1.12.5.2 Binding Corporate Rules und Codes of Conduct 247
3.1.12.5.3 Safe-Harbor-Übereinkommen 248
3.1.12.6 Verhältnis zur Auftragsdatenverarbeitung 253
3.2 Infrastrukturrecht 256
3.2.1 Cloud Computing als kritische Infrastruktur? 257
3.2.2 Staatliche Schutz- und Gewährleistungspflicht für Cloudinfrastruktur? 259
3.3 Deutsches und europäisches Kartellrecht 260
3.4 Internationales Privatrecht 263
3.5 Vertragsrecht 265
3.5.1 Vertragstypologische Einordnung 265
3.5.1.1 Bereitstellung von Speicherplatz 266
3.5.1.2 Bereitstellung von Software und Verarbeitung von Daten 267
3.5.1.3 Bereitstellung von Rechenleistung 268
3.5.2 Back-to-Back-Verträge zwischen Cloudprovidern und Subunternehmen 269
3.5.3 Service Level Agreements (SLAs) 269
3.5.3.1 Funktion und Formen 269
3.5.3.2 Vertragsgestaltung und konkrete Regelungsinhalte 271
3.5.3.2.1 Leistungspflichten und Leistungsbeschreibung 271
3.5.3.2.2 Reaktions- und Mängelbeseitigungsfristen 272
3.5.3.2.3 Verfügbarkeit und Latenzzeiten 272
3.5.3.2.4 Service Level Management 273
3.5.3.2.5 Sanktionen 274
3.5.3.2.6 Vertragsbeendigung und weiterer Umgang mit Daten (Exit Management) 275
3.5.3.2.7 Urheber- und Nutzungsrechte 276
3.5.3.2.8 Datenschutz, Rechtswahl und Gerichtsstand 276
3.5.3.3 Einschränkungen durch AGB-Recht 276
3.5.4 Bedeutung von DIN SPEC 1041 278
3.6 Compliance und Aufbewahrungspflichten 280

3.6.1 Allgemeine Compliancevorschriften, Haftung und Risikomanagement 280
3.6.2 Bereichsspezifische Regelungen (Risikomanagement, territoriale Beschränkungen und nationale Aufbewahrungspflichten) 282
3.7 Urheberrecht 283
3.7.1 Lizenzierung der Software und Wegfall des Lizenzmanagements für die Nutzer 283
3.7.2 Geltende Rechtslage nach dem UrhG 285
3.7.3 Internationales Urheberrecht 287
3.7.3.1 Räumlicher Anwendungsbereich 287
3.7.3.2 Völkerrechtliche Verträge 288
3.7.3.3 Persönlicher Anwendungsbereich 288
3.7.3.4 Kollisionsrecht und Internationales Privatrecht 289
3.7.4 Bedeutung für Cloud Computing 289
3.7.4.1 Verhältnis zwischen Softwarehersteller und Cloudprovider 289
3.7.4.2 Verhältnis zwischen Cloudprovider und Cloudnutzer 290
3.7.4.2.1 Rechtmäßige Nutzungshandlungen 291
3.7.4.2.2 Verletzungshandlungen (Unerlaubte Handlungen) 291
3.8 Strafrecht, Strafprozessrecht, Strafverfolgung und Cloudforensik 292
3.8.1 Probleme bei der Strafverfolgung und neue Ermittlungsansätze 292
3.8.1.1 Telekommunikationsüberwachung gemäß § 100a StPO mittels Deep Packet Inspection 296
3.8.1.1.1 Funktionsweise der Deep Packet Inspection 296
3.8.1.1.2 Deep Packet Inspection und deren Relevanz für die IT-Sicherheit 298
3.8.1.1.3 Rechtliche Bedeutung 299
3.8.1.2 Strafrechtliche Regelungen zum Geheimnisschutz 299
3.9 Bezüge zum Recht der Vereinigten Staaten 302
3.9.1 Electronic Discovery 302
3.9.1.1 Beschreibung und Besonderheiten der e-Discovery 302
3.9.1.2 Probleme im Zusammenhang mit Cloud Computing 303
3.9.1.3 Konflikt zwischen US-Recht und deutschem Datenschutzrecht 305
3.9.2 USA PATRIOT Act 308

3.9.3 Auskunfts- und Aufbewahrungspflichten nach dem Sarbanes-Oxley-Act . 309
3.10 Empfehlungen zur Rechtsgestaltung 310

4 Gestaltung rechtsverträglicher Cloudsysteme 315
4.1 Notwendigkeit und Maßstab der rechtlichen Gestaltung von Technik 315
4.2 Rechtliche Gestaltung anhand der KORA-Methode 315
4.3 Ableitung von rechtlichen Anforderungen aus grundrechtlichen Vorgaben 316
4.4 Rechtliche Kriterien 319
4.4.1 Techniksicherheit (K1) 319
4.4.2 Vertraulichkeit (K2) 319
4.4.3 Transparenz (K3) 320
4.4.4 Entscheidungsfreiheit (K4) 321
4.4.5 Erforderlichkeit (K5) 322
4.4.6 Zweckbindung (K6) 323
4.4.7 Trennbarkeit (K7) 324
4.4.8 Beherrschbarkeit und Steuerungsfähigkeit (K8) 324
4.4.9 Überprüfbarkeit (K9) 325
4.4.10 Beweissicherung (K10) 326
4.4.11 Integrität (K11) 326
4.4.12 Verfügbarkeit (K12) 327
4.5 Technische Gestaltungsziele 327
4.5.1 Verschlüsselung von Daten und Datenträgern (Z1) 327
4.5.2 Etablierung eines umfassenden Management Interfaces (Z2) 328
4.5.3 Sicherung des Interfaces durch Zugriffsschutzverfahren (Z3) 328
4.5.4 Etablierung und technische Umsetzung des Vieraugenprinzips (Z4) 328
4.5.5 Nutzung von Identitäts- und Zugriffsmanagementsystemen (Z5) 329
4.5.6 Sichere Authentisierung (Z6) 329
4.5.7 Trennung des Nutzertraffic vom administrativen Datenverkehr (Z7) 330
4.5.8 Trennung der virtuellen Nutzersysteme durch sichere Hypervisoren (Z8) . 330
4.5.9 Implementierung von Dokumentationsfunktionen (Z9) 330

4.5.10 Keine Weitergabe von administrativen Protokollen (Z10) 331
4.5.11 Kein Zugriff des Providers auf Protokollinhalte der Nutzer (Z11) 331
4.5.12 Sicherung der Protokolldaten durch Zugriffsschutzverfahren (Z12) 331
4.5.13 Sichere Löschung der Protokolldaten (Z13) 331
4.5.14 Sichere Löschung sonstiger Daten (Z14) 331
4.5.15 Bestätigung der Löschung von Daten bei Subunternehmen (Z15) 332
4.5.16 Aufbau von Redundanzen (Z16) 332
4.5.17 Nutzung von Fehlerkorrekturverfahren, Checksummen und Hashwerten (Z17) 332
4.5.18 Technisch unterstützte Auswahl von Subunternehmen (Z18) 334
4.5.19 Regelbasiertes Load Balancing (Z19) 334
4.5.20 Etablierung und Nutzung standardisierter Schnittstellen und APIs (Z20) .. 335
4.5.21 Fortschreitende Abstraktion und Zusammenfassung zu logischen Geräten (Z21) 335
4.6 Technische Gestaltungsvorschläge 337
4.6.1 Verschlüsselung der beim Datentransport übermittelten Daten (G1) 337
4.6.2 Verschlüsselung während der Speicherung (G2) 338
4.6.3 Sichere Schlüssel- und Passwortverwaltung (G3) 338
4.6.4 Trennung von Schlüsseln und Daten (G4) 339
4.6.5 Nutzung von homomorphen Verschlüsselungsalgorithmen (G5) 339
4.6.6 Trennung der verarbeitenden Rechner von der Cloudinfrastruktur während der Verarbeitung (G6) 340
4.6.7 Einsatz von bewährten und gehärteten Hypervisoren (G7) 341
4.6.8 Verteilung und Replizierung der Daten auf unterschiedliche physische Server (G8) 341
4.6.9 Identifizierung und Authentisierung mittels tauglicher Identifikationsverfahren (G9) 343
4.6.10 Nutzung von geeigneten und erprobten Zugriffs- und Identitätsmanagementsystemen (G10) 343
4.6.11 Bereitstellung von Steuerungs- und Monitoringoberflächen und Data Tracking Tools (G11) 344
4.7 KORA-Methode als disziplinenübergreifende Methode im Cloud-Computing-Kontext 345

5 Schlussbetrachtungen 347

5.1 Zusammenfassung der Erkenntnisse und Ergebnisse 347

5.2 Ausblick und künftiger Forschungsbedarf 350

Anlage 353

Literaturverzeichnis 356

Abkürzungsverzeichnis

1-9

3D	dreidimensional
4G	vierte Generation (des Mobilfunks)

A

a. A.	anderer Ansicht/anderer Auffassung
Abl. EG	Amtsblatt der der Europäischen Gemeinschaften
Abl. EU	Amtsblatt der Europäischen Union
Abs.	Absatz
ACM	Association for Computing Machinery
AES	Advanced Encryption Standard
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
a.F.	alte Fassung
AG	Amtsgericht/Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
AktG	Aktiengesetz
Alt.	Alternative
AMT	Amazon Mechanical Turk
AO	Abgabenordnung
AOL	America Online
API	Application Programming Interface
App	Application
Arpanet	Advanced Research Projects Agency Network
ASP	Application Service Providing
AtomG	Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Atomgesetz)
AWS	Amazon Web Services

B

BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BBG	Bundesbeamtengesetz
BDSG	Bundesdatenschutzgesetz
BeamtStG	Beamtenstatusgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen
BGP	Border Gateway Protocol

BImSchG	Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnlichen Vorgängen (Bundes-Immissionsschutzgesetz)
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BMJ	Bundesministerium der Justiz
BR-Drs.	Bundesratsdrucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BvR	Aktenzeichen einer Verfassungsbeschwerde zum Bundesverfassungsgericht

C

ca.	circa
CAD	Computer-Aided Design
CEO	Chief Executive Officer
CIA	Central Intelligence Agency/Abkürzung für Confidentiality, Integrity, Availability
CIO	Chief Information Officer
CO2	Kohlendioxid
CPU	Central Processing Unit
CR	Computer und Recht
CRi	Computer Law Review International
CRM	Customer Relationship Management
c’t	Magazin für Computertechnik

D

D-A-CH	Deutschland-Österreich-Schweiz
DDoS	Distributed Denial of Service
ders.	derselbe
DHS	Department of Homeland Security
DIN	Deutsches Institut für Normung e. V.
DIN SPEC	DIN Spezifikation
DISA	Defense Information Systems Agency
DoD	Department of Defense
Dok.	Dokument

DÖV	Die Öffentliche Verwaltung
DPI	Deep Packet Inspection
DSB	Datenschutz-Berater
DSG	Datenschutzgesetz
DSRL	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtline)
DuD	Datenschutz und Datensicherheit
DVBl.	Deutsches Verwaltungsblatt
DVD	Digital Versatile Disc

E

EC2	Amazon Elastic Compute Cloud
EDGE	Enhanced Data Rates for GSM Evolution
e-Discovery	electronic Discovery
EDV	Elektronische Datenverarbeitung
e.g.	exempli gratia
EG	Europäische Gemeinschaften
EGBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuch
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
EMC	EMC² Corporation
EMRK	Europäische Menschenrechtskonvention
EN	Europäische Norm
ENISA	Europäische Agentur für Netz- und Informationssicherheit
ErfK	Erfurter Kommentar (zum Arbeitsrecht)
ERP	Enterprise Resource Planning
EU	Europäische Union
EuG	Europäisches Gericht erster Instanz
EuGH	Europäischer Gerichtshof
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
e.V.	eingetragener Verein
EWR	Europäischer Wirtschaftsraum

F

FAQ	Frequently Asked Questions
FedRAMP	Federal Risk and Authorization Management Program
FCC	Federal Communications Commission
FISMA	Federal Information Security Management Act
FLOPS	Floating Point Operations Per Second
Fn.	Fußnote

FRCP	Federal Rules of Civil Procedure
FTC	Federal Trade Commission

G

GB	Gigabyte
GCHQ	Government Communications Headquarters
GDD	Gesellschaft für Datenschutz und Datensicherung e.V
gem.	gemäß
GG	Grundgesetz
GMail	Google Mail
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GMX	Global Message eXchange
GNU	GNU's Not Unix
GnuPG	Gnu Privacy Guard
GPRS	General Packet Radio Service
GPU	Graphics Processing Unit
GRC	Grundrechte Charta (eigentlich: Charta der Grundrechte der Europäischen Union)
GSA	United States General Services Administration
GSM	Global System for Mobile Communications

H

HaaS	Hardware as a Service
HD	High Definition
HDSG	Hessisches Datenschutzgesetz
HGB	Handelsgesetzbuch
HMD	Handbuch der maschinellen Datenverarbeitung
HP	Hewlett-Packard Company
HPC	High Performance Computing
HSPA	High Speed Packet Access

I

IaaS	Infrastructure as a Service
IBM	International Business Machines Corporation
ICC	International Chamber of Commerce
ICT	Information and Communication Technologies
IDS	Intrusion-Detection-System
IEC	International Electrotechnical Commission
InvG	Investmentgesetz
IP	Internet Protocol

IPbpR	Internationaler Pakt über bürgerliche und politische Rechte
IPR	Internationales Privatrecht
IPS	Intrusion-Prevention-System
IPSEC	IP Security Protocol Working Group
ISMS	Information Security Management System/Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IT	Informationstechnologie
ITRB	IT-Rechtsberater
it+ti	Informationstechnik und technische Informatik
i.V.m.	in Verbindung mit

K

K&R	Kommunikation und Recht
Kap.	Kapitel
KFZ	Kraftfahrzeug
KMU	Kleine und mittlere (mittelständische) Unternehmen
KOM	Mitteilung der EU-Kommission
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KORA	Konkretisierung rechtlicher Anforderungen
KRITIS (-Strategie)	Nationale Strategie zum Schutz Kritischer Infrastrukturen
KVM	Kernel-based Virtual Machine
KWG	Gesetz über das Kreditwesen

L

LAN	Local Area Network
LG	Landgericht
lit.	litera
LSA	Land Sachsen-Anhalt
LTE	Long Term Evolution
Ltd.	Limited

M

MaRisk	Mindestanforderungen an das Risikomanagement
MBit	Megabit
MByte	Megabyte
MIR	Medien Internet und Recht
MITM	Man in the Middle
MMR	Multimedia und Recht
MP3	MPEG Audio Layer III (Musikformat)

ms	Millisekunden
MS	Microsoft
mwN	mit weiteren Nachweisen

N

NAT	Network Adress Translation
Nds.	Niedersächsische
NIST	National Institute of Standards and Technology
NJOZ	Neue Juristische Online Zeitschrift
NJW	Neue Juristische Wochenschrift
NSA	National Security Agency
NVwZ	Neue Zeitschrift für Verwaltungsrecht

O

OECD	Organisation for Economic Co-operation and Development
OLG	Oberlandesgericht
OS	Operating System
OSI	Open Systems Interconnection
OWiG	Ordnungswidrigkeitengesetz

P

PaaS	Platform as a Service
PC	Personal Computer
PCI DSS	Payment Card Industry Data Security Standard
PDOS	Permanent Denial of Service
PGP	Pretty Good Privacy
PIM	Privileged Identity Management

Q

QoS	Quality of Service

R

RAID	Redundant Array of Independent Disks
RBÜ	Revidierte Berner Übereinkunft
RDV	Recht der Datenverarbeitung
RFC	Request For Comments
RL	Richtlinie

S

S + S	Software-plus-Service
S.	Seite

S3	Amazon Simple Storage Service
SaaS	Software as a Service
SCM	Supply Chain Management
SEC	Securities and Exchange Commission
SGB	Sozialgesetzbuch
SLA	Service Level Agreement
Slg.	Sammlung (der Rechtsprechung des Europäischen Gerichtshofs und des Europäischen Gerichts Erster Instanz)
SoA	Serviceorientierte Architektur
SOG	Sicherheits- und Ordnungsgesetz
SOX	Sarbanes-Oxley-Act
SPI	Shallow Packet Inspection
SSL	Secure Socket Layer
SSLA	Security Service Level Agreements
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
SWIFT	Society for Worldwide Interbank Financial Telecommunication

T

TCP	Transmission Control Protocol
TDDSG	Teledienstedatenschutzgesetz
ThürOBG	Thüringer Gesetz über die Aufgaben und Befugnisse der Ordnungsbehörden
TK	Telekommunikation
TKG	Telekommunikationsgesetz
T-KIBS	Technology-Oriented Knowledge-Intensive Business Services
TLS	Transport Layer Security
TMG	Telemediengesetz
TPM	Trusted Platform Module
TRIPs	Agreement on Trade-Related Aspects of Intellectual Property Rights

U

UMTS	Universal Mobile Telecommunications System
UN	United Nations
UPR	Umwelt und Planungsrecht
US	United States
USA	United States of America

USA PATRIOT (Act)	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
USB	Universal Serial Bus
U.S.C.	United States Code
USV	unterbrechungsfreie Stromversorgung
usw.	und so weiter
UWG	Gesetz gegen den unlauteren Wettbewerb

V

v. Chr.	vor Christus
VAG	Versicherungsaufsichtsgesetz
VIG	Gesetz zur Verbesserung der gesundheitsbezogenen Verbraucherinformation
VLAN	Virtual Local Area Network
VM	Verwaltung und Management/ Virtuelle Maschine
VO	Verordnung/Virtuelle Organisation
VoIP	Voice over IP
VPN	Virtual Private Network
vs.	versus
VwVfG	Verwaltungsverfahrensgesetz
VZ-Netzwerke	Sammelbegriff für die Social Communities StudiVZ, MeinVZ und SchuelerVZ

W

WAN	Wide Area Network
WCT	WIPO Copyright Treaty
WIPO	World Intellectual Property Organisation
WP	Working Paper (Arbeitspapier) der Artikel-29-Datenschutzgruppe
WpHG	Wertpapierhandelsgesetz
WPPT	WIPO Performances and Phonograms Treaty

X

XaaS	Everything as a Service

Z

z. B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZDF	Zweites Deutsches Fernsehen
ZPO	Zivilprozessordnung

ZRP	Zeitschrift für Rechtspolitik
ZSKG	Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes
ZUM	Zeitschrift für Urheber- und Medienrecht

Abbildungsverzeichnis

Abbildung 1: Hype Cycle 2010 mit Cloud Computing auf dem Höhepunkt 21
Abbildung 2: Zusammenhang unterschiedlicher Nutzungsmodelle 37
Abbildung 3: Übersicht der Virtualisierungsvarianten 41
Abbildung 4: Entstehung des Cloud Computing aus den Vorgängermodellen 54
Abbildung 5: Beziehung zwischen Kunden und Anbietern beim IT-Outsourcing 59
Abbildung 6: Beziehung zwischen Kunden und Anbietern bei ASP 61
Abbildung 7: Übersicht über Amazons Web- und Cloudservices 73
Abbildung 8: Beispiel für die Preisgestaltung eines Cloudangebots 74
Abbildung 9: OSI-Schichtenmodell 297

1 Einleitung

Forschungsgegenstände dieser interdisziplinär angelegten Arbeit sind die technischen und ökonomischen Hintergründe, die Sicherheitsaspekte, die rechtliche Bewertung und Einordnung und die sich aus diesen Aspekten ergebenden Konsequenzen für eine rechtsgemäße technische Gestaltung des sogenannten „Cloud Computing“. Ausgangspunkt und Schwerpunkt der Untersuchung ist aber, trotz der interdisziplinären Herangehensweise, das Recht.

Cloud Computing, mit „Rechnen in der Wolke“ übersetzt, liegt die Vision zugrunde, dass Informationstechnologiedienstleistungen, bildlich gesprochen, wie elektrischer Strom „aus der Steckdose“ beim Nutzer ankommen und ebenso nach Verbrauch abgerechnet werden.[1] IT-Dienste und Ressourcen werden damit bedarfsbezogen verfügbar, genauso, wie dies bei Strom, Wasser oder anderen Grundversorgungsleistungen der Fall ist.[2] Die sozialen Folgen sollen, um im Bild zu bleiben, mit der Elektrifizierung Ende des 19. Jahrhunderts und den bis heute andauernden Konsequenzen vergleichbar sein.[3]

Cloud Computing ist aber auch eine Geschäftsidee, nämlich die Idee, dass Software und Daten nicht mehr lokal beim Nutzer bearbeitet oder gespeichert werden, sondern über das Internet als Vermittlungsinstanz bei einem Dritten, der die Software und Daten dynamisch und nach Bedarf bereitstellt.[4] Die Onlinebereitstellung von Hardware, Software und Daten durch Cloud Computing ist folglich eine Dienstleistung.[5]

Mit der Etablierung des Cloud Computing wird das Zeitalter kleinerer dezentraler Rechenzentren oder hochgerüsteter Einzelplatzrechner, die die meiste Zeit ungenutzt leerlaufen und erhebliche Personal-, Energie- und Produktionskosten verursachen, dem Ende entgegen gehen.[6] Rechenleistung, Speicherkapazität (Infrastructure

---

1 *Rodenhäuser*, Damit Sie nicht aus allen Wolken fallen, http://www.manager-magazin.de/unternehmen/it/0,2828,582750,00.html; *Van der Kamp/Burger/Weisenhaus*, Erfolgsfaktoren des Cloud Computing, http://winfwiki.wi-fom.de/index.php/Erfolgsfaktoren_des_Cloud_Computing#Vision; *Reindl*, in: Taeger/Wiebe, Inside the Cloud, 441; *Söbbing*, MMR, 2008, Heft 5, XIII; *Repschläger/Pannicke/Zarnekow* 2010, 6; *Söbbing*, in: Leible/Sosnitza, Onlinerecht 2.0: Alte Fragen – neue Antworten? Cloud Computing – Datenschutz – Urheberrecht – Haftung, 40, 50, der das Prinzip als „Strommodell“ bezeichnet.

2 *Schulz/Rosenkranz*, ITRB 2009, 232.

3 *Carr* 2009, 20 ff.; *ders.*, The Big Switch, http://www.nicholasgcarr.com/bigswitch.

4 *Spies*, MMR 2009, Heft 5, XI; *Pohle/Ammann*, CR 2009, 273.

5 Im Folgenden werden die Begriffe „Dienstleistung“, „Dienst“ und „Service“ synonym gebraucht; siehe dazu auch sogleich 1.1.

6 Nach Angaben des BITKOM sollen Server durchschnittlich nur zu 10-15 % und maximal zu 30 % ausgelastet sein, *Beckereit/Harrer/Koch/Schaupp/Skurk/Stedler/Walther/Wild*e 2009, 7; Google sieht das Ende der Desktop-PCs in Unternehmen spätestens 2013 hereinbrechen; *Marks*, Google: Desktop-PCs werden irrelevant,

as a Service), Softwareentwicklungsplattformen (Platform as a Service) oder Applikationssoftware (Software as a Service) werden von den Nutzern nur noch bei Bedarf „aus der Wolke“ genutzt und bezahlt. Diese bedarfsorientierte Nutzung wird als „Pay per Use“ oder „Pay as You Go“ bezeichnet.[7]

Cloud Computing bietet im Vergleich zur herkömmlichen Bereitstellung von IT eine Reihe von Vorteilen. Das Betriebsrisiko für die Software wird auf Dritte ausgelagert, eine Aktualisierung der Programme auf den einzelnen Rechnern ist nicht erforderlich, sondern erfolgt zentral, die Verfügbarkeit wird erhöht, da oft mehrere, zum Teil weltweit, verteilte Rechenzentren zur Verfügung stehen und somit Komplettausfälle weniger wahrscheinlich werden. Lizenzgebühren für individuelle Nutzerlizenzen entfallen und außerdem sinkt der Wartungs-, und damit der Personalaufwand, für Hard- und Software.[8] Eine kostspielige Neuanschaffung von Hard- und Software ist vielfach nicht mehr nötig. Das Problem der Über- oder Unterlizenzierung von Software wird ebenfalls gemindert.

Betrachtet man das Schadenspotential und nicht nur die Schadenswahrscheinlichkeit, kommt man außerdem zum erfreulichen Ergebnis, dass das Schadenspotential und die Verletzlichkeit durch die Nutzung von Clouddiensten im Vergleich zu herkömmlichen lokalen IT-Lösungen nicht höher liegen. Die betroffenen Geschäftsprozesse und Daten sind nämlich immer noch die gleichen. Das Aufkommen von neuartigen Bedrohungen durch die Nutzung von Clouds wird nur für die Schadenseintrittswahrscheinlichkeit relevant werden. Im Übrigen spricht auch nichts gegen einen parallelen Betrieb von lokaler IT, beispielsweise für wenige besonders wertvolle Daten, und die teilweise Auslagerung von vergleichsweise weniger wertvollen Daten in die Cloud. Daneben ist die Nutzung von Cloudservices zum Überbrücken von Lastspitzen oder projektbezogen denkbar.[9] Auch diese Bereitstellung von zusätzlichen Optionen und Steuerungsmöglichkeiten ist folglich ein Flexibilitätsaspekt, genauso wie die theoretisch unbegrenzte Skalierbarkeit und Elastizität[10] in einer Cloud oder die Möglichkeit, Softwareservices global und zeitnah an geänderte Anforderungen anzupassen. Cloud Computing erfährt deshalb gerade einen Wandel vom Trendbegriff zur populären Unternehmensstrategie.

Im Verbraucherumfeld ist der Begriff allerdings noch nicht verbreitet und laut einer Umfrage im Herbst 2010 kennen lediglich sechs Prozent der Befragten Cloud Com-

---

http://www.computerbase.de/news/hardware/komplettsysteme/2010/maerz/google_desktop-pcs; *Marwan*, Der PC: nur krank oder doch schon tot?, http://www.zdnet.de/it_business_bizz_talk_der_pc_nur_krank_oder_doch_schon_tot_story-39002398-41551811-1.htm.

7 *Schulz/Rosenkranz*, ITRB 2009, 232; *Schulz*, in: Taeger/Wiebe, Inside the Cloud, 404; *Kurz*, Netzwoche 17/2008, 34.

8 *Spies*, MMR 2009, Heft 5, XI.

9 Dies ist in der Übergangsphase für Unternehmen mit eigener IT-Ausstattung das Hauptanwendungsgebiet für Cloudservices; für SaaS so auch *Born*, iX Special 2/2010, 18.

10 Sofortiges Hinzufügen von virtualisierter Hardware bei Bedarf.

puting und dessen Einsatzmöglichkeiten.[11] Ganze 94 Prozent der Befragten wissen nicht, was Cloud Computing bedeutet.[12] Zwar haben laut der Umfrage viele Privatnutzer Berührungspunkte[13] mit Cloud Computing, jedoch dürfte noch einige Zeit vergehen, bis die Mehrheit der Bevölkerung mit dem Thema vertraut sein wird.

Eine Beschäftigung mit dem Thema lohnt sich aber nicht nur für Unternehmensentscheider, sondern auch und gerade für Verbraucher und Privatanwender. Für diese Zielgruppe liegt der wesentliche Vorteil darin, dass sie von jedem Ort an dem ein Zugang zum Internet besteht auf die Daten in der Wolke zugreifen können, ohne diese Daten zwischen mehreren Geräten synchronisieren zu müssen. Durch die Bereitstellung und Berechnung in der Cloud sind außerdem die Performanceanforderungen an die genutzten Geräte gering, so dass auch viele ältere Geräte moderne Anwendungen oder sogar modernste Spiele nutzen können, für deren lokalen Betrieb sie von ihrer Leistungsfähigkeit her eigentlich gar nicht geeignet wären.[14] Insbesondere Smartphones und Tablets geraten verstärkt in den Focus der Forschungsabteilungen. Trotz ihrer relativ leistungsschwachen Hardware werden auch an Mobiltelefone und Tablet-PCs mittlerweile dieselben Ansprüche gestellt wie an gewöhnliche Desktoprechner. Eine technische Lösung zur Überwindung des Performanceunterschieds kommt aus Intels Forschungsabteilung. Bei der sogenannten „Clone Cloud“ wird eine exakte Kopie des Smartphones in der Cloud abgebildet. Alle für das Smartphone zu rechenintensiven Aufgaben werden dann von diesem Klon in der Cloud übernommen.[15] Ähnlich arbeitsteilig funktioniert Amazons Webbrowser „Silk“. Zur schnelleren Darstellung auf Amazons Tablet werden Teile der angeforderten Webseiten in der eigenen Cloud vorberechnet, optimiert und anschließend auf dem Tablet zur Verfügung gestellt.[16] Operas Webbrowser,

---

11 *Kien*, HP-Umfrage: Cloud-Computing für Verbraucher noch ohne Bedeutung, http://www.funkschau.de/telekommunikation/news/article/69108/0/HP-Umfrage_Cloud-Computing_fuer_Verbraucher_noch_ohne_Bedeutung; *Hackmann*, Deutsche kennen Cloud Computing nicht, http://www.computerwoche.de/management/cloud-computing/2354805.

12 *Kien*, HP-Umfrage: Cloud-Computing für Verbraucher noch ohne Bedeutung, http://www.funkschau.de/telekommunikation/news/article/69108/0/HP-Umfrage_Cloud-Computing_fuer_Verbraucher_noch_ohne_Bedeutung.

13 Zu den einzelnen Berührungspunkten, beispielsweise Webmail oder Webalben, siehe die Umfrageergebnisse bei *Hackmann*, Deutsche kennen Cloud Computing nicht, http://www.computerwoche.de/management/cloud-computing/2354805.

14 So können zum Beispiel hochaufgelöste Videos in einer Cloud verkleinert und so heruntergerechnet werden, dass sie auch auf schwächerer Hardware laufen; *Kremp*, Schwarmintelligenz für Alt-Elektronik, http://www.spiegel.de/netzwelt/gadgets/0,1518,671162,00.html.

15 *Chun/Maniatis*, CloneCloud, http://berkeley.intel-research.net/bgchun/clonecloud; *Intel*, Intel's Clone Cloud: Increase the IQ of Your Smart Phone, http://www.intel.com/pressroom/kits/innovation/newsletter/eNewsJune/Q2articles/ article4.html.

16 *Amazon Silk Team*, Introducing Amazon Silk, http://amazonsilk.wordpress.com/2011/09/28/introducing-amazon-silk; bei dieser Art Browser muss man aber bedenken, dass der Cloudbetreiber den Webstream nutzerspezifisch analysieren und Nutzungsprofile erstellen kann.

insbesondere die Mobilbrowser „Mini“ und „Mobile“, funktionieren im Übrigen schon seit fünf Jahren nach dem gleichen Prinzip.[17]

Bestes und ältestes praktisches Beispiel für Software as a Service und damit älteste Vorreiter des Cloud Computing sind die seit Jahren bestehenden kostenlosen Webmaildienste.[18] Weitere Beispiele sind Fotodienste (Flickr), Videodienste (YouTube) und zum Teil auch Social Communities (Facebook, VZ-Netzwerke) oder Musikdienste, wie zum Beispiel itunes[19] oder Last.fm. Sogar grafisch anspruchsvolle und rechenintensive Spiele lassen sich in der Cloud berechnen und werden dem Spieler über das Internet in HD-Auflösung per Stream bereitgestellt.[20] Computerspiele sind dann nur noch Dienste unter vielen anderen. Dass Cloud Gaming mit allen Spielgenres, inklusive den hardware- und netzwerktechnisch anspruchsvollen 3D-Shootern, im praktischen Einsatz tadellos funktioniert, wird vom Cloud-Gaming-Dienst OnLive[21] unter Beweis gestellt.[22] Dessen Produzent versteigt sich sogar zur Prognose, dass Cloud Gaming das Ende der herkömmlichen Spielkonsolen einläuten wird.[23] Auch das Drucken soll zukünftig über die Cloud erfolgen, zum Beispiel über „Google Cloud Print“. Dazu sind jedoch zunächst von den Herstellern neue cloudfähige Druckermodelle zu entwickeln.[24] Die Dienste, Spiele und Anwendungen funktionieren mittels eines Webbrowsers praktisch auf jedem herkömmlichen Computer, Tablet-PC oder Smartphone.[25] Kleinen, schlanken und sparsamen Com-

---

17 *Hachman*, Opera: Amazon's Silk Browser is Flattering, But Five Years Late, http://www.pcmag.com/article2/0,2817,2393786,00.asp.

18 *Fickert*, in: Taeger/Wiebe, Inside the Cloud, 419; *Wunderlich* 2010, 12; *Singer* 2010, 1.

19 *Laube*, Apple plant Speicherbank für Musik, http://www.ftd.de/it-medien/medien-internet/:cloud-computing-apple-plant-speicherbank-fuer-musik/50085662.html.

20 Sogenanntes „Cloud Gaming“; *Austinat/Fechteler/Gieselmann*, c’t 21/2010, 76; *Bonnert*, GDC: Onlive und Gaikai starten Cloud-Spiele in den USA, http://www.heise.de/newsticker/meldung/GDC-Onlive-und-Gaikai-starten-Cloud-Spiele-in-den-USA-952069.html.

21 http://www.onlive.com.

22 Ein Test von On Live mit diversen Spielen findet sich bei *Austinat/Fechteler/Gieselmann*, c’t 21/2010, 76 ff.; OnLive ist mittlerweile auch auf Tablets nutzbar; *Sebayang*, Unreal Tournament auf einem Android-Tablet, http://www.golem.de/1102/81410.html; *Bonnert*, E3: OnLive streamt Spiele aus der Cloud auf Tablets, http://www.heise.de/newsticker/meldung/E3-OnLive-streamt-Spiele-aus-der-Cloud-auf-Tablets-1257877.html.

23 *Senerd*, OnLive-Produzent sagt das Ende der Konsole voraus, http://www.gulli.com/news/onlive-produzent-sagt-das-ende-der-konsole-voraus-2010-09-08; ähnlich *Austinat/Fechteler/Gieselmann*, c’t 21/2010, 76 ff.

24 *Kolokythas*, Google will das Drucken radikal vereinfachen, http://www.pcwelt.de/start/dsl_voip/online/news/2341824/google-will-das-drucken-radikal-vereinfachen; *Ihlenfeld*, Cloud Print - Google will das Drucken neu erfinden, http://www.golem.de/1004/74538.html.

25 Künftig werden Smartphones Desktop-PCs als Informationssuche- und Medienkonsumgerät immer schneller und immer umfassender ablösen; siehe *Diestelberg*, Google: Desktop-PCs sind in drei Jahren irrelevant, http://winfuture.de/news,53950.html.

putern und Smartphones gehört folglich die Zukunft.[26] Das Zeitalter der „Thin Clients“ erlebt in einer modernen praxistauglichen und ressourcenschonenden Fassung eine Renaissance. Wie einst Wasserleitungen den eigenen Brunnen überflüssig machten, wird Cloud Computing die lokalen Rechner und Rechenzentren reduzieren. Der Verkaufserfolg der Netbooks ist ein Vorbote dafür, in welche Richtung sich der Computerhardwaremarkt künftig entwickeln wird. Die Geräte müssen künftig nur noch in der Lage sein, einen Webbrowser adäquat nutzen zu können. Alles andere wird irgendwo im Netz vorgehalten. So sind nicht zuletzt Googles „Chrome OS“[27] oder das cloudbasierte Betriebssystem „Jolicloud“[28] ein Hinweis darauf, dass diese Zukunft nicht mehr allzu fern ist.

Auch die großen Softwarehersteller entwickeln vielfach bereits jetzt schon nur noch Software, die mit Cloud Computing und Cloudservices kompatibel ist. Bei Microsoft arbeiteten beispielsweise im Jahr 2010 70 Prozent der 40 000 Mitarbeiter an Software, die cloudfähig ist. Im Jahr 2011 sollen es sogar 90 Prozent gewesen sein.[29] Die Linuxdistribution „Ubuntu“ soll künftig ebenfalls erweiterte[30] Möglichkeiten bieten, Daten und Dienste in der Cloud vorzuhalten. Insbesondere der Desktop eines Systems soll cloudfähig werden, so dass man von überall mit einem Internetzugang darauf zugreifen kann.[31]

Verteilte Systeme in einer modernen und für die Allgemeinheit nutzbaren Form sind im Entstehen. Vernetzung, Virtualisierung von Systemen, Clustering, Parallelisierung von Rechnern, Rechenzentren und Rechenleistung, Grid Computing, dynamische Lastverteilung und die flächendeckende Verfügbarkeit von breitbandigen Internetzugängen sind Wegbereiter dieses Paradigmenwechsels in der IT-Geschichte. Der Fortschritt ist mittlerweile so weit, dass ein Spotmarkt wie bei Energie- und Rohstoffmärkten entsteht, in dem freie Rechen- und Speicherkapazitäten ersteigerbar sind.[32] „Ubiquitous Computing“ wird dieses Paradigma der mobi-

---

26 Erste Erfahrungen mit der „mobilen Wolke“ finden sich bei *Dannen*, In der mobilen Wolke, http://www.heise.de/tr/artikel/In-der-mobilen-Wolke-1132571.html.

27 http://www.chromium.org/chromium-os.

28 http://www.jolicloud.com; auch als „Joli OS“ bekannt.

29 *Chip Online*, Steve Ballmer: Plädoyer für Wolke und Wandel, http://business.chip.de/news/Steve-Ballmer-Plaedoyer-fuer-Wolke-und-Wandel_41805938.html.

30 Cloudstorage ist bereits seit längerem möglich, *Subramanian*, Canonical Attempts To Integrate Cloud Storage Into Ubuntu Desktop, http://www.cloudave.com/link/canonical-attempts-to-integrate-cloud-storage-into-ubuntu-desktop.

31 *Mühlwitz*, Cloud Computing: Ubuntu Desktop in der Cloud, http://t3n.de/news/cloud-computing-ubuntu-desktop-cloud-268510.

32 *Kirsch*, Amazon versteigert freie Cloud-Kapazitäten, http://www.heise.de/newsticker/meldung/Amazon-versteigert-freie-Cloud-Kapazitaeten-885005.html; *Schwan*, Marktplatz für Cloud-Computing-Dienste, http://www.heise.de/newsticker/meldung/Marktplatz-fuer-Cloud-Computing-Dienste-1192541.html.

len, allseits verfügbaren und vernetzten Computerisierung noch weiter treiben und unumkehrbar in den künftigen Alltag integrieren. Dieser nächste Schritt in der Entwicklung wird jedoch nur dann erfolgreich werden, wenn die massenhaft und in Echtzeit situativ anfallenden Daten der Sensoren, Klein- und Kleinstrechner über das Internet bereitgestellt, in leistungsfähigen Cloudsystemen berechnet, über Webservices kombiniert und vorgefiltert werden und dem Nutzer in einer verständlichen Form präsentiert werden. Hierfür werden die bisher erlangten und künftig zu erlangenden Erfahrungen mit verteilten Systemen und das Vorhandensein von Cloudumgebungen und funktionsfähigen Webservices essentiell werden.

Durch Cloud Computing erfolgt eine Zentralisierung von Kapazitäten, weg von Einzelplatzrechnern oder kleinen dezentralen Rechenzentren (Inhouse-Lösungen). Diese Zentralisierung in großen Rechenzentren und die hardwareunabhängige Virtualisierung führen einerseits zu Flexibilisierung, Kosteneinsparungen, optimaler Ausnutzung von Kapazitäten, dem Schutz der Umwelt,[33] der Reduktion der „Time-to-Market“ und von Markteintrittsbarrieren bei Startups,[34] aber andererseits auch zu neuen Gefahren für die in der metaphorischen Wolke vorgehaltenen Daten und Dienste.

Unabdingbare Voraussetzung und kritischer Erfolgsfaktor dieser „neuen Computerwelt“ ist die Gewährleistung der Sicherheit und des Schutzes der Daten und Systeme.[35] Das anzustrebende Sicherheitsniveau muss dabei mindestens dem bisherigen Stand entsprechen, um die Akzeptanz bei den Nutzern zu gewährleisten. Die Daten in der Wolke müssen mindestens genauso sicher sein, wie auf den bisherigen Privat- oder Unternehmenssystemen. Teile dieser Sicherheitsvoraussetzungen sind rechtlich konkret vorformuliert, überwiegend jedoch abstrakt in Grundrechten und der Rechtsprechung des Bundesverfassungsgerichts als soziale Verhaltens- und Gebotsnormen enthalten. Die Ableitung von konkreten technisch-organisatorischen Sicherheitsanforderungen und technischen Gestaltungsanforderungen erfolgt mit Hilfe der sogenannten KORA-Methode.

1.1 Cloud Computing als Dienstleistung

Wie einleitend schon angedeutet, bedeutet Cloud Computing die Nutzung von Software- und sonstigen Diensten (Storage, Rechenleistung) über das Internet auf physischer und virtueller Hardware des Cloudproviders. Der Provider stellt dem

---

33 *Oertel*, Wie Internetnutzer zum Klimaschutz beitragen können, http://www.heise.de/newsticker/meldung/Wie-Netznutzer-zum-Klimaschutz-beitragen-koennen-914671.html.

34 Weil keine Hardwareinvestitionen und die Hardware betreuendes Personal nötig werden.

35 *Jaster/Collier de Mendoca/Slamka/Radmacher* 2010, 9 sprechen von „Sicherheit als derzeitige Achillesferse des Cloud Computing“; *Tsvihun/Stephanow/Streitberger* 2010, 7 sehen „Sicherheit als Kernkompetenz eines Providers“ an, weil „Sicherheit einen integralen Bestandteil des Geschäftsmodells darstellt“.

Kunden (Cloudnutzer) diese Dienste gegen Bezahlung zur Verfügung, so dass der Kunde seinerseits entweder nahezu komplett auf eigene Hard- und Software verzichten kann oder die Cloudservices ergänzend zu seiner IT-Infrastruktur nutzt. Auch bei einem Verzicht auf Hardware, insbesondere Server oder Rechenzentren, benötigt der Nutzer weniger leistungsfähige Rechner mit einem Webbrowser auf denen die Clouddienste vom Kunden und seinen Mitarbeitern genutzt werden können. Zur ergänzenden Nutzung gehören gewisse Geschäftsprozesse, regelmäßig auftretende Ereignisse, zum Beispiel regelmäßig auftretende Lastspitzen durch Abrechnungen am Quartalsende oder der Kundenansturm auf einen Webshop während der Vorweihnachtszeit, oder Einzelanwendungen wie Maildienste oder Kundendatenmanagementsoftware. Bei einem Komplettersatz müssen alle Berechnungen, die im Rechenzentrum oder auf speziellen Rechnern abliefen, und vor allem die komplette Software auf die das Unternehmen und seine Mitarbeiter angewiesen ist und die bisher auf den lokalen Computern installiert war, zentral durch den Provider bereitgestellt werden.

1.2 Konsequenzen des Cloud Computing für sonstige Dienstleistungen im Internet

Konsequenz einer flächendeckenden Nutzung von Cloudservices ist die Zentralisierung aller anderen Dienste und Informationen auf wenige Cloudanbieter. Während bisher Dienstleistungsanbieter und Webangebote auf eigene dezentrale Hardwareinfrastruktur vertrauten, wird mit der Zeit der komplette Betrieb dieser Unternehmen auf der Hardware einiger weniger Cloudanbieter ablaufen. Neben der oben angeführten Reduzierung von Markteintrittsbarrieren für neue Unternehmen bedeutet dies jedoch eine physische Zentralisierung von vielen, bisher dezentralen, Daten und Geschäftsprozessen bei einem Anbieter mit der scheinbaren Konsequenzen einer erhöhten Anfälligkeit für Schäden, beispielsweise durch Angriffe oder Ausfälle der Clouddienste. Ob dies tatsächlich so ist und ob eine erhöhte Gefahr für die Daten und Dienste besteht, wird zu untersuchen sein.

Eine weitere Konsequenz ist die sich ergebende Flexibilität. Die Anbieter herkömmlicher Dienstleistungen und jetzigen Cloudkunden können flexibler als bisher agieren, haben Einsparungen und können somit schneller billigere Dienstleistungen anbieten, was mittelbar den Endkunden der Dienstleistungsanbieter zugutekommt. Auch die Entwicklung von neuen Dienstleistungen und Diensten wird vorangetrieben, wenn ein potentieller Anbieter nicht erst große Anfangsinvestitionen tätigen muss, sondern sofort seine Angebote vermarkten kann. Bestes Beispiel sind Social Communities oder Onlineshops. Während früher jeder Anbieter einer solchen Community erst einmal in Hardware investieren musste, um den Dienst anbieten zu können, besteht nunmehr die Möglichkeit sofort Dienste eines Cloudproviders in Anspruch zu nehmen. Während der Betreiber einer Community oder eines Shops früher abschätzen musste, wieviele Nutzer im Laufe der Zeit hinzukommen, kann er

nunmehr auf die Skalierbarkeit in der Cloud vertrauen und auch nur so viel Leistung bezahlen, wie er tatsächlich benötigt. Früher bestand das Risiko, entweder den eigenen Serverpark einerseits unterdimensioniert aufzubauen, was Ausfälle oder einen verlangsamten Betrieb zur Folge hatte oder andererseits überdimensioniert, was hohe und unnötige Kosten nach sich zog. Kurz gefasst konnte ein Anbieter einer Dienstleistung entweder am eigenen Erfolg zugrundegehen oder sich mit Investitionen übernehmen und dadurch zahlungsunfähig werden. Die nunmehr bestehende Planungssicherheit hat folglich zuverlässige, im Sinne von existierenden, Dienste zur Folge. Dies kommt nicht zuletzt der Sicherheit der genutzten Daten zugute. Plötzlich von der Bildfläche verschwindende Anbieter, die insolvent sind, haben in der Regel auch keinen großen Anreiz oder die Möglichkeiten mehr, die ihnen anvertrauten Daten zu sichern und zu schützen. Schlimmstenfalls werden diese illegal weiterveräußert, um doch noch irgendwie an finanzielle Mittel zu kommen und den nichtabwendbaren Bankrott zumindest hinauszuzögern.

1.3 Bedeutung der Sicherheit

Wie man bereits an den vorherigen Ausführungen ersehen konnte, soll einer der Schwerpunkte in der Betrachtung der Sicherheit des Cloud Computing liegen. Sicherheit ist allerdings ein sehr allgemeiner Begriff.

1.3.1 IT-Sicherheit

Nach dem hier zugrundeliegenden Verständnis handelt es sich bei der Sicherheit primär um die technisch geprägte Sichtweise, nämlich Sicherheit von Informationstechnik, kurz, IT-Sicherheit. Diese betrifft sowohl Daten als auch die zur Datenverarbeitung und Übermittlung notwendigen IT-Systeme.

Vorab ist festzustellen, dass es *die* IT-Sicherheit an sich nicht gibt. IT-Sicherheit umfasst das Erfüllen einer Vielzahl von sogenannten „IT-Schutzzielen“, die jedoch ihrerseits nicht abschließend sind, weil sie der technischen Entwicklung folgen und jeweils für ein spezifisches Sicherheitsproblem eines Systems stehen. Aus der Bindung an die technische Entwicklung folgt zudem die Erkenntnis, dass es absolute Sicherheit nie geben kann.[36]

Die Schutzziele definieren Zustände oder Umstände, die jeweils eine gewisse Voraussetzung bieten, die es erlaubt, von Daten- oder Systemsicherheit zu sprechen. Zum Beispiel ist das Schutzziel der Datenintegrität gewährleistet, wenn die betrachteten Daten über einen bestimmten Zeitraum vollständig und unverändert vorhanden waren. Nicht selten finden sich allgemeine oder sogar spezielle rechtliche Anknüpfungspunkte, die die Erfüllung eines oder mehrerer IT-Schutzziele ermöglichen. Dies erfolgt nicht ausdrücklich unter Bezugnahme auf die Schutzziele, sondern vom

[36] So bereits *Roßnagel*, UPR 1986, 46.

Ergebnis her. Zum Beispiel fördern Vorschriften zum Geheimnisschutz das Schutzziel der Vertraulichkeit.

Ausgangspunkt mangelnder IT-Sicherheit und einer Verletzung der Schutzziele sind Bedrohungen, die sich aus der jeweils betrachteten Technik ergeben. In der Regel sind die Bedrohungen nicht nur technikinhärent, sondern auch vom Einsatzbereich der Technik und dem jeweiligen Kontext abhängig. Um IT-Sicherheit einschätzen und ermöglichen zu können, ist es notwendig die Bedrohungen zu kennen. Die Bedrohungsfindung erfolgt mit Hilfe einer Bedrohungsanalyse. Die Beseitigung oder Abmilderung der negativen Konsequenzen einer Bedrohung erfolgt durch konkrete Sicherheitsmaßnahmen. Diese sind erfolgreich, wenn die Bedrohung beseitigt wurde und damit ein Schutzziel erfüllt wurde. Für ein strukturiertes Vorgehen bei der Umsetzung der Sicherheitsmaßnahmen ist ein Sicherheitskonzept hilfreich.

Für die Bewertung und Lösung der Sicherheitsaspekte des Cloud Computing sind demnach eine Klassifizierung der IT-Schutzziele, eine Bedrohungsanalyse und notwendige Sicherheitsmaßnahmen sowie ein Sicherheitskonzept notwendig. Die zu findenden Sicherheitsmaßnahmen sind zudem im Rahmen der Anwendung der, sogleich darzustellenden, KORA-Methode auf der Ebene der technischen Gestaltungsziele und Gestaltungsvorschläge unmittelbar zu berücksichtigen.

Die Klassifizierung und Berücksichtigung von IT-Schutzzielen ist daher nicht nur akademischer Natur, sondern erlaubt die Ableitung anerkannter Sicherheitsmaßnahmen, die im spezifischen Kontext einer Technik, (grund)rechtlich abgeleitet, dazu führen, dass die so gestaltete Technologie, zum Beispiel Cloud Computing, technisch sicher und damit rechtsgemäß ist.

1.3.2 Rechtssicherheit

Von der IT- und Datensicherheit und dem damit einhergehenden technischen Schutz der Daten, ist die Rechtssicherheit abzugrenzen. Kunden und Anbieter müssen sich verlassen können, dass mit Eintritt eines unvorhergesehenen Ereignisses oder Fehlverhaltens die rechtliche Abwicklung und Kompensation gewährleistet ist. Neben Beweisbarkeitsfragen in Prozessen gehört dazu auch die Abschreckungswirkung von Rechtsnormen. Dazu gehört nicht nur die strafrechtliche General- und Spezialprävention, sondern auch die „Sicherheit“, dass zivilrechtliche Schäden bei einer Nachweisbarkeit von Fehlverhalten durch einen rechtlichen Anspruch kompensierbar sind. Stichworte sind Verantwortlichkeit und Haftung. Inwieweit dieser rechtliche Schutz durch die Internationalität des Cloud Computing vermindert wird, muss ebenfalls untersucht werden. Rechtssicherheit ist wertlos ohne die Möglichkeit der Rechtsdurchsetzung. Dies gilt ganz besonders für die strukturell unterlegenen Verbraucher.

Um Rechtssicherheit erreichen zu können, ist es aber auch notwendig die geltende Rechtslage mit ihren Rechten und Pflichten zu kennen. Die Darstellung des rechtlichen Rahmens des Cloud Computing ist nicht zuletzt diesem Gedanken geschuldet.

Diese Herangehensweise erfordert eine rechtswissenschaftliche Betrachtung aller in Betracht kommenden Rechtsgebiete. Schwerpunkt dieser rechtswissenschaftlichen Forschungen bildet allerdings das Datenschutzrecht, da die wesentlichen Probleme des Cloud Computing in diesem Rechtsgebiet angesiedelt sind.

1.4 Vorlaufende Technikgestaltung anhand der KORA-Methode

Rechtsnormen regeln das Zusammenleben und sind Ergebnis eines sozialen Konsenses.[37] Sie regeln also nur selten direkt technische Systeme. Dort, wo solche Regeln existieren, sollen diese im Rahmen dieser Arbeit angewendet werden. Wo aber Regeln benötigt werden und keine expliziten Vorschriften bestehen, sollen sie aus übergeordneten Rechtsregeln abgeleitet werden und es sollen aus ihnen mit Hilfe der Methode zur „Konkretisierung rechtlicher Anforderungen“ (KORA) Vorschläge für die Technikgestaltung erarbeitet werden.

Die Methode ist eine Vorgehensweise, um rechtliche Anforderungen bereits bei der Gestaltung von Informationstechnik zu berücksichtigen. Hierdurch wird erreicht, dass das Recht auf neuartige Technik nicht mehr nur nachträglich reagiert, sondern die jeweilige Technik vor oder während ihrer Entwicklung rechtsgemäß mitgestaltet wird.

Mittels KORA werden aus rechtlichen Anforderungen in vier Schritten technische Anforderungen abgeleitet. Die abgeleiteten Anforderungen werden von Schritt zu Schritt technischer und konkreter. Um nicht auf allen Ebenen unterschiedslos von „Anforderungen“ zu sprechen, werden sie in Vorgaben, Anforderungen, Kriterien, Ziele und Vorschläge begrifflich aufgespalten. Die Begriffe entsprechen dabei in etwa den Verwendungszwecken der jeweiligen Anforderungen.[38]

1.5 Rolle des Rechts im Verhältnis zur Technik

1.5.1 Einordnung der KORA-Methode in den Gesamtzusammenhang

Zur juristischen Behandlung des Themas „Cloud Computing“ und dessen Gestaltung mittels der Methode KORA muss die zugrundeliegende Technik erforscht und verstanden werden, um die passenden rechtlichen Vorschriften direkt oder analog anwenden zu können und effektive technische Gestaltungsvorschläge unterbreiten zu können, die ihrerseits mittelbar auf Rechtsregeln, namentlich den Grundrechten, basieren.

---

[37] *Pordesch* 2003, 257.

[38] *Pordesch* 2003, 262.

Bei einer ersten Betrachtung fällt auf, dass üblicherweise auf allgemeine rechtliche Regelungen und Vorgaben, wie eben die Grundrechte, zurückgegriffen werden muss, da spezielle Regelungen meist nicht existieren oder nur unvollständig gewisse Teilaspekte abdecken. Hintergrund ist, neben der schnelleren technischen Entwicklung und dem „Nachlaufen“[39] des Rechts hinter dieser Entwicklung, der bereits erwähnte Umstand, dass Recht nicht dazu dient, Technik und deren konkrete Ausgestaltung, sondern soziale Funktionen und divergierende Interessen zu regeln. Dies erfolgt möglichst abstrakt. Die unterschiedlichen Interessen sind zu einem ausgewogenen Ausgleich zu bringen, um Rechtsfrieden und Rechtssicherheit zu schaffen und damit letztlich das Zusammenleben zu regeln.[40]

Bei der Anwendung der KORA-Methode muss nicht auf die Formulierung von technikspezifischem Recht durch den Gesetzgeber gewartet werden, zumal, wie gerade geschildert, nicht jede neue Technik auch rechtlich als solche eine Einzelregelung erfährt, so dass die eben erwähnte Problematik des „Nachlaufens“ des Rechts hinter der technischen Entwicklung vermieden wird. Im Optimalfall ist durch die praktische Umsetzung der Methode nicht nur eine nachträgliche Anpassung der Technik nicht mehr notwendig, sondern es kann auch von spezifischen Regelungen abgesehen werden, um mit solchen nachträglichen Normen Fehler der Technik und damit einhergehende Risiken für Einzelne oder die Gesellschaft zu minimieren. Vorlaufende verfassungsverträgliche Technikgestaltung ist damit nicht nur ein Beitrag zur Risikominimierung und Risikovorsorge, sondern hat mittelbar auch eine Stärkung und bessere Akzeptanz des Rechts in der Gesellschaft zur Folge, weil technische Missstände gerade nicht durch negativ besetzte rechtliche Verbote gelöst werden müssen.

Manchmal besteht aber die Notwendigkeit oder der politische Wille, eine gewisse risikobehaftete Technik nicht (nachträglich) zu verbieten, da eine gewisse gesellschaftliche Akzeptanz oder das tatsächliche oder vermeintliche Bedürfnis für deren rechtliche Legitimierung besteht. Beispiele hierfür wären die Nutzung von Atomkraft oder die Gentechnik. Bei Cloud Computing geht es im Vergleich dazu um anders geartete und weniger gravierende Risiken für Rechtsgüter der Betroffenen und der Gesellschaft. Es wäre aber nicht undenkbar und von manchen wird dies bereits gefordert, die Auslagerung von Daten in Clouds wegen der damit einhergehenden Intransparenz (daher auch der Begriff der „Wolke“) und den damit verbundenen Nachteilen für die informationelle Selbstbestimmung zu verbieten.[41] Dass eine solche, rein rechtlich vertretbare, Sichtweise von der „normativen Kraft des Fakti-

---

39 *Hornung* 2005, 88 bezeichnet das „Nachlaufen“ des Rechts hinter der technischen Entwicklung als „Reaktivität“.

40 *Pordesch* 2003, 262, 264.

41 Für einen Verzicht der Auslagerung von personenbezogenen Daten in die Cloud tritt beispielsweise *Weichert*, DuD 2010, 679 ein.

schen“ überholt wird, ist offensichtlich. Es besteht nämlich keine normative Selbstbegrenzung der Technik. Manche bezweifeln deswegen auch, dass der eigentlich notwendige Überlegenheits- und Geltungsanspruch des Rechts gegenüber der Technik tatsächlich gegeben ist.[42] Erfahrungen zeigen nämlich, dass alles, was technisch möglich ist, irgendwann früher oder später, sehenden Auges unter Umgehung der rein normativen Vorgaben des Rechts und dessen Geltungsanspruchs, praktisch umgesetzt und genutzt wird.[43]

Deswegen sollte frühzeitig auf die Gestaltung risikobehafteter Technik im Sinne einer Risikoverringerung, rechtlich basiert, eingewirkt werden. Solche begrenzenden Ansätze müssen aber, wegen der fehlenden Selbstbegrenzung der Technik, nicht nur von außen und möglichst frühzeitig, sondern idealerweise noch während der Entwicklungsphase gemeinsam mit den entwickelnden Informatikern erarbeitet werden.[44] Neben der vorlaufenden Technikgestaltung sind auch die zum Teil identischen By-Design-Ansätze, beispielsweise „Privacy by Design“, zu erwähnen. Im Rahmen des Systemdatenschutzes ist auch der Aspekt des Selbstschutzes des Betroffenen durch „Privacy Enhancing Technologies“ eine weitere Möglichkeit auf die zeitliche Verzögerung oder Mängel bei der rechtlichen Regulierung und Durchsetzung zu reagieren.[45]

1.5.2 Technikrecht als historisch gewachsenes Beispiel für das Verhältnis zwischen Recht und Technik

Zwar sollen im Rahmen der Arbeit Rechtsfragen aus allen einschlägigen Blickwinkeln beleuchtet werden, jedoch bietet es sich an dieses besondere Verhältnis zwischen Technik und Recht am Beispiel des Technikrechts historisch zu beleuchten.

Das Technikrecht an sich ist älter als der akademische Begriff des Technikrechts. Letzterer existiert seit Mitte bis Ende des 19. Jahrhunderts und steht in Verbindung mit der Industriellen Revolution. Technikrecht in diesem Sinne ist ein Rechtsgebiet mit eigenen Charakteristika und eine eigene Disziplin, während der weite Begriff an die vorchristliche Existenz von Technik anknüpft und die punktuelle Regelung von solchen frühen Formen von Technik mit umfasst.[46]

Mit der Industriellen Revolution entstand die Notwendigkeit der Regelung und Normierung von technischen und wirtschaftlichen Gegebenheiten, mit denen das herkömmliche und davor geltende Recht nicht zurechtkam.[47] Ziele dieser Normie-

---

42 *Hornung* 2005, 87; *Roßnagel/Wedde/Hammer/Pordesch* 1990, 57 ff.
43 *Roßnagel* 2001, 21 ff.; *Schnabel* 2009, 27; *Hornung* 2005, 87.
44 *Roßnagel* 1993, 28; *Schnabel* 2009, 27.
45 *Roßnagel*, ZRP 1997, 26 ff.; *Hornung* 2005, 88.
46 *Vec*, in: Schulte/Schröder, Handbuch des Technikrechts, 2011, 4, 9.
47 *Vec*, in: Schulte/Schröder, Handbuch des Technikrechts, 2011, 4 f.

rung waren Rationalisierungsgedanken und die Risikovermeidung.[48] Die Parallelen zu Cloud Computing sind nicht zu übersehen. Die einfachgesetzlichen rechtlichen Rahmenbedingungen folgen in beiden Fällen der technischen Entwicklung nach, wobei zudem die gesetzgeberischen Ziele jeweils die gleichen sind.

Technikrecht stellt sich als Querschnittsmaterie dar und hat immer Bezüge zu den vorhandenen rechtlichen Regelungen und Strukturen. Es ist und war eine Anhäufung von Normen, die sich auf die technischen Gegebenheiten beziehen und nie den Schutz eines einzelnen Rechtsgutes oder einer Technik an sich zum Ziel hatten, sondern oft mehrere mit dem Aufkommen einer Technik betroffene und bereits anerkannte Rechtsgüter betreffen oder betrafen. Schwerpunkt bei seiner Entwicklung Ende des 19. Jahrhunderts war demzufolge die Regulierung gesellschaftlicher und individueller Risiken, begründet im Aufkommen neuartiger Techniken, die zudem zu einer neuartigen Wirtschaftsverfassung und bis dahin unbekannten Produktionsmethoden führten.[49]

Im Kontext des Cloud Computings sind diese Merkmale immer noch aktuell. Die rechtlichen Rahmenbedingungen sollen die Risiken für die Rechtsgüter der Betroffenen minimieren, die dadurch entstehen, dass eine neuartige Technik im Entstehen begriffen ist, die weitgehende gesellschaftliche Folgen hat. Bei Cloud Computing sind dies die Art und Weise der Bereitstellung von Informationstechnologie und das Einhergehen eines neuen Paradigmas der Nutzung von IT-Leistungen.

Während bei der Entstehung des Technikrechts die industrielle Produktion und neuartige Produktionsmethoden den Ausschlag für die Regulierungsbedürftigkeit gaben, sind bei Cloud Computing IT-Dienstleistungen und die neuen Formen der Bereitstellung und Nutzung solcher Dienstleistungen ausschlaggebend.

Die Industrielle Revolution und vor allem deren Ende in den 70er Jahren des 20. Jahrhunderts ist damit auch für eine weitere Parallele zu Cloud Computing heranziehbar, nämlich dem Strukturwandel vom Industriestaat zur Dienstleistungsgesellschaft.[50] Eine treibende Kraft dieses Strukturwandels war nicht zuletzt das Outsourcing, so dass Cloud Computing als dessen Nachfolger im Grunde genommen den aktuellen Höhepunkt dieser Entwicklung zu einer Dienstleistungsgesellschaft im IT-Bereich darstellt.

---

48 *Vec*, in: Schulte/Schröder, Handbuch des Technikrechts, 2011, 7.

49 *Vec*, in: Schulte/Schröder, Handbuch des Technikrechts, 2011, 59, 60.

50 Letzteres wird auch als Tertiarisierung bezeichnet; siehe dazu *Pfeuffer*, Dienstleistungsgesellschaft, http://www.socialinfo.ch/cgi-bin/dicopossode/show.cfm?id=135.

1.6 Forschungsbedingungen und Notwendigkeit einer interdisziplinären Herangehensweise

Angesichts der bisherigen Ausführungen wird deutlich, dass bei der wissenschaftlichen Untersuchung und Bewertung des Cloud Computing zwingend unterschiedliche Disziplinen zu beteiligen sind. Für eine effektive und umfassende rechtliche Betrachtung müssen vor allem die technisch-informatischen Hintergründe und Umstände, die hinter Cloud Computing stehen, berücksichtigt und verstanden werden. Entsprechendes gilt für die ökonomischen Aspekte, weil Cloud Computing auch ein Geschäftsmodell darstellt. Die sozialen Chancen und Risiken sind nicht zuletzt für die konkrete Technikgestaltung unter dem Aspekt der sozialen Erwünschtheit maßgeblich.

Die Voraussetzungen für das Verständnis unterschiedlicher Disziplinen ergaben sich durch die dreijährige Mitarbeit im Center for Advanced Security Research Darmstadt (CASED) und der Projektgruppe verfassungsverträgliche Technikgestaltung (provet). Die intensive Zusammenarbeit zwischen Informatikern, Ökonomen und Juristen erleichterte die interdisziplinäre Betrachtung und ermöglichte die ganzheitliche Herangehensweise an das Forschungsthema. Nicht zuletzt die Einbindung in den Arbeitsbereich „Sichere Dienste“ und die juristisch-ökonomische Zusammenarbeit im Teilprojekt des Arbeitsbereichs lieferten hilfreiche neue Blickwinkel, Fragestellungen und vor allem Antworten bei der ganzheitlichen wissenschaftlichen Durchdringung und Erforschung des Forschungsthemas.

1.7 Gang der Untersuchung

Im zweiten Teil sollen sogleich die verwendeten Begriffe, insbesondere Cloud Computing an sich, die technischen, aber auch die sozialen und ökonomischen Folgen und Hintergründe des Cloud Computing in Form von Vor- und Nachteilen und der Zusammenhang zur Methode KORA definiert und erläutert werden. Ebenso wird auf die historischen Vorläufer und die notwendigen Grundvoraussetzungen zur Entwicklung des Cloud Computing einzugehen sein. Abgrenzungsfragen, Unterschiede und Neuerungen im Vergleich zu Vorläufermodellen sind ebenso Teil der Untersuchung.

Im dritten Teil[51] werden die rechtlichen Implikationen und im Hinblick auf die später anzuwendende KORA-Methode auch die grundrechtlichen Vorgaben und rechtlichen Anforderungen im Detail untersucht. Schwerpunkt der Untersuchung bildet, wie bereits angedeutet, das Datenschutzrecht. Insbesondere ist auf die Kernprobleme des Cloud Computing einzugehen, nämlich die Anforderungen zur Sicherung aus § 9 BDSG samt Anlage und die Problematik der Internationalität sowie die Klä-

[51] Siehe Kap. 3.

rung der Frage und der Voraussetzungen einer Privilegierung der Auftragnehmer im Rahmen der sogenannten Auftragsdatenverarbeitung gemäß § 11 BDSG.

Technikgestaltung im Zusammenhang mit Cloud Computing hat auch die Sicherheit der genutzten Systeme und der darin verarbeiteten und gespeicherten Daten als wesentliches Ziel. Aus diesem Grund wird im Rahmen des Datenschutzrechts auch vertieft auf das Thema IT-Sicherheit allgemein und die Schutzziele im Speziellen einzugehen sein.[52] Für die sichere Technikgestaltung und Entwicklung ganzheitlicher Sicherheitskonzepte muss man die aktuellen und künftigen Bedrohungen kennen. Im Rahmen einer Bedrohungsanalyse sollen deshalb allgemeine und für die Cloud spezifische Bedrohungen der Sicherheit erörtert werden. Als Folge dieser Bedrohungsanalyse sollen anschließend allgemeine und cloudspezifische Sicherheitsmaßnahmen untersucht und aufgezeigt werden.

Weitere Rechtsgebiete umfassen das Vertragsrecht und Service Level Agreements, internationales Privatrecht, Urheber- und Kartellrecht, aber auch Strafprozessrecht, insbesondere aus dem Blickwinkel der praktischen Strafverfolgung und möglicher Beweisbarkeitsprobleme innerhalb einer (internationalen) Cloud. Stichwort in diesem Zusammenhang ist die sogenannte Cloudforensik.

Weitere internationalrechtliche Aspekte, die kurz betrachtet werden, namentlich die E-Discovery oder der USA PATRIOT Act, sind dem Umstand geschuldet, dass die meisten Cloudprovider in den Vereinigten Staaten angesiedelt sind und zudem überwiegend auf US-Territorium ihre Rechenzentren stehen haben. Auch auf Konflikte zwischen deutschem und US-Recht soll kurz eingegangen werden.

Der vierte Teil[53] ist der Konkretisierung von Gestaltungsvorschlägen durch die Anwendung der KORA-Methode vorbehalten. Konkrete Gestaltungsvorschläge, die im Rahmen der Anwendung der Methode abgeleitet werden, sollen sich nicht nur an der Rechtsgemäßheit und den rechtlichen Anforderungen und Vorgaben orientieren, sondern auch aus IT-Schutzzielen abgeleitete konkrete technische Maßnahmen zur Erreichung der IT-Sicherheit umfassen. Ein weiteres Augenmerk bei der konkreten Gestaltung ist auf die im ersten Teil ermittelten Chancen und Risiken in Form von Vor- und Nachteilen zu werfen.

---

52 Siehe Kap. 3.1.9.

53 Siehe Kap. 4.

2 Untersuchungsgegenstand

Bevor vertieft auf die sozialen Folgen und die jeweiligen Vor- und Nachteile eingegangen wird, bietet es sich an, die Cloud Computing zugrundeliegende Technik, Verfahren, Eigenschaften, Ursachen und die im weiteren Verlauf verwendeten Begriffe zu definieren und zu beschreiben. Außerdem soll Cloud Computing zu vorhandenen Technologien und Geschäftsmodellen abgegrenzt werden.

2.1 Begriff des Cloud Computing

Der Ursprung des Begriffspaars „Cloud Computing“ wird *Ramnath Chellappa* zugeordnet.[54] Der Hintergrund für diese Bezeichnung liegt in der schematischen Darstellung des Internets in Zeichnungen. Seit jeher wird dafür eine kleine Ansammlung von stilisierten vernetzten Computern verwendet, um die eine Wolke gezeichnet ist, die das Internet symbolisieren soll. Teilweise wird auch nur eine Wolke verwendet. Die Wolke symbolisiert dabei den Umstand, dass der physische und geographische Speicherort von Daten für den Nutzer nicht mehr ersichtlich ist. Früher hieß es Daten sind „im Netz“, mittlerweile liest man immer öfter die Wendung „in der Cloud“. Dabei meint man umgangssprachlich vorwiegend im Internet vorgehaltene Daten. Insbesondere im Werbeumfeld gibt es „schwarze Schafe“, die wegen der Werbewirkung auch über unpassende Dienstleistungen den Begriff des Cloud Computing überstülpen, um diesen einen „modernen Anstrich zu verpassen“. Es ist jedoch absehbar, dass dieses Phänomen im Laufe der Zeit verschwinden wird, wenn sich die Eigenschaften und Hauptmerkmale des Cloud Computing im Bewusstsein der potentiellen Nutzer durchsetzen.

Noch bis Mitte 2011 war die Bedeutung des Begriffs „Cloud Computing“ relativ unscharf und jeder meinte damit etwas anderes, was zu einer Beliebigkeit in der Verwendung führte.[55] Teilweise wurde der Begriff als „Hype“ verschrien und es wurde behauptet, Cloud Computing sei bildlich gesprochen „alter Wein in neuen Schläuchen“. So bezeichnete *Richard Stallmann* das Cloudkonzept als „Dummheit“ und „schlimmer als Dummheit, es ist ein Hype“.[56] Von *Larry Ellison*, dem CEO

---

54 *Fickert*, in: Taeger/Wiebe, Inside the Cloud, 419.

55 *Everett/Marwan*, Cloud Computing: zwischen Wunsch und Wirklichkeit, http://www.zdnet.de/it_business_technik_cloud_computing_zwischen_wunsch_und_wirklichkeit_story-11000009-39202000-1.htm; *Marwan*, Cloud-Computing kommt langsam, aber gewaltig, http://www.zdnet.de/it_business_technik_cloud_computing_kommt_langsam__aber_gewaltig_story-11000009-41005211-1.htm.

56 *Krangel*, Open Source Guru Richard Stallman: Cloud Computing „Worse Than Stupidity“, http://www.businessinsider.com/2008/9/gnu-founder-richard-stallman-cloud-computing-worse-than-stupidity-; *Armbrust/Fox/Griffith/Joseph/Katz/Konwinksi/Lee/Patterson/Rabkin/Stoica/Zaharia* 2009, 3; *Stallmann* warnt im Übrigen auch vor der Nutzung von Chrome OS, da die Nutzer die Kontrolle über die Daten verlieren könnten; siehe dazu *Arthur*, Google's ChromeOS means losing con-

von Oracle ist der Ausspruch überliefert Cloud Computing sei „alles was Oracle schon bisher gemacht hat“ und „nur noch die Werbung für die Produkte umgeschrieben werden müsste“.[57] Im gleichen Zusammenhang bezeichnete er Cloud Computing als „Modetrend“ und brandmarkte dieses mode- und trendgetriebene Verhalten der Computerindustrie als „geisteskrank“ und „Idiotie“.[58] *Andy Isherwood* von Hewlett Packard polemisierte gegen den Begriff, indem er behauptete noch keine zwei Menschen getroffen zu haben, die mit dem Begriff das gleiche gemeint hätten.[59] Diese Zweifel und Unwägbarkeiten sind inzwischen weitestgehend ausgeräumt. Mittlerweile sind die Hauptcharakteristika und Kriterien des Cloud Computing anerkannt, wodurch auch die ursprünglich leicht unterschiedlichen Definitionen inzwischen weitgehend kohärent sind.

2.1.1 Cloud Computing als Hype?

Bevor auf einige ausgesuchte Definitionsversuche eingegangen wird, ist noch auf den bereits erwähnten Vorwurf des „Hypes“ um Cloud Computing einzugehen. Beim Begriff „Hype“ schwingt immer das Übertriebene, Kurzlebige und Aufbauschende mit, wodurch der Begriff im deutschen Sprachraum meist negativ besetzt ist. Dass Cloud Computing jedoch alles andere als kurzlebig und aufgebauscht ist, demonstrieren die fast täglich aufkommenden Initiativen von Staaten, europäischen Behörden oder Agenturen und privatwirtschaftlichen Verbänden oder Einzelunternehmen sowie die immensen Investitionen in die wissenschaftliche Erforschung und die Entwicklung von Cloudservices und deren Rahmenbedingungen. Nicht zuletzt ist die vorliegende Arbeit ebenfalls Teil dieser wissenschaftlichen Forschungen.

So investierte zum Beispiel das Bundesministerium für Wirtschaft und Technologie im Jahr 2011 50 Millionen Euro in einen Forschungswettbewerb namens „Trusted Cloud“.[60] Zudem hat das Ministerium ein „Aktionsprogramm Cloud Computing“ mit vier Handlungsfeldern aufgesetzt, in denen Wirtschaft, Wissenschaft und Politik

---

trol of data, warns GNU founder Richard Stallman, http://www.guardian.co.uk/technology/blog/2010/dec/14/chrome-os-richard-stallman-warning.

57 *Computerwoche*, Zwischen Euphorie und Blödsinn, http://www.computerwoche.de/management/cloud-computing/1907276.

58 *Krangel*, Larry Ellison: Someone Explain To Me This “Cloud Computing” Thing My Company Is Committing To, http://www.businessinsider.com/2008/9/larry-ellison-someone-explain-to-me-this-cloud-computing-thing-my-company-is-committing-to-orcl-; *Armbrust/Fox/Griffith/Joseph/Katz/Konwinksi/Lee/Patterson/Rabkin/Stoica/Zaharia* 2009, 3.

59 *Armbrust/Fox/Griffith/Joseph/Katz/Konwinksi/Lee/Patterson/Rabkin/Stoica/* 2009, 3.

60 *Bundesministerium für Wirtschaft und Technologie*, Sichere Internet-Dienste – Sicheres Cloud Computing für Mittelstand und öffentlichen Sektor (Trusted Cloud), http://www.trusted-cloud.de; *Kleinz*, Bundesregierung investiert in Cloud Computing, http://www.heise.de/newsticker/meldung/Bundesregierung-investiert-in-Cloud-Computing-1098975.html.

künftig gemeinsam tätig werden sollen.[61] Über das erste Handlungsfeld sollen Innovations- und Marktpotentiale erschlossen werden. Im zweiten Handlungsfeld geht es um die Erzeugung von innovationsfreundlichen Rahmenbedingungen, die vorrangig die Aspekte Sicherheit, Vertrauen und den Rechtsrahmen betreffen, während innerhalb des dritten Handlungsfelds internationale Entwicklungen mitgestaltet werden sollen. Letzteres erfolgt insbesondere durch die Etablierung von einheitlichen Standards für die notwendige Interoperabilität.[62] Im vierten Handlungsfeld soll den Anwendern durch Leitfäden und Webportale das erforderliche Wissen über Cloud Computing vermittelt werden.[63] Hauptziele des Aktionsprogramms sind die Erschließung der großen Potentiale von Cloud Computing für die deutsche Wirtschaft und das Angehen der bestehenden Herausforderungen bei der Nutzung von Cloud Computing.[64]

Als Beispiel auf EU-Ebene sind die sogenannte „Digitale Agenda"[65] der EU-Kommission zu erwähnen, die unter anderem die Rahmenbedingungen für Cloud Computing verbessern soll, oder die Forschungen der Europäischen Agentur für Netz- und Informationssicherheit (ENISA), die sich mit dem Thema Cloud Computing und Risikomanagement befasst.[66] Ein konkret von der EU-Kommission mit 7,5 Millionen Euro gefördertes Cloudprojekt ist „TClouds", das die Entwicklung sicherer und datenschutzkonformer Cloudtechnik zum Ziel hat.[67] Das gesamte Projektvolumen der dreizehn beteiligten Partner beträgt etwa 10,5 Millionen Euro.[68]

---

61 *Bundesministerium für Wirtschaft und Technologie*, Aktionsprogramm Cloud Computing, http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Technologie-und-Innovation/aktionsprogramm-cloud-computing,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf; *Franz*, Recht und Standards, http://www.netzwelt.de/news/84260_2-aktionsprogramm-staat-rechnet-cloud.html.

62 *Paulus*, DuD 2011, 317 untersucht, für welche Bereiche interoperable Standards notwendig sind, um Vertrauenswürdigkeit zu schaffen.

63 *Bundesministerium für Wirtschaft und Technologie*, Brüderle startet Aktionsprogramm Cloud Computing, http://www.bmwi.de/BMWi/Navigation/Presse/pressemitteilungen,did=361742.html.

64 *Bundesministerium für Wirtschaft und Technologie*, Brüderle startet Aktionsprogramm Cloud Computing, http://www.bmwi.de/BMWi/Navigation/Presse/pressemitteilungen,did=361742.html

65 *Europäische Kommission*, Digital Agenda for Europe, http://ec.europa.eu/information_society/digital-agenda/index_de.htm; *Europäische Union*, Digitale Agenda: Kommissionsmaßnahmen bringen Europa schnelle und ultraschnelle Breitbandtechnik – was bedeutet das für mich?, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/426&format=HTML&aged=0&language=DE.

66 *Catteddu/Hogben* 2010, 1 ff.

67 Näheres zum Projekt siehe bei *Hansen/Marnau/Schlehahn/Husmann*, <kes> Special - Sicheres Cloud Computing, März 2011, 14 und http://www.tclouds-project.eu.

68 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, TClouds - Projekt für datenschutzkonformes Cloud Computing gestartet, https://www.datenschutzzentrum.de/presse/20101129-tclouds.htm.

Als Stellvertreter für die Privatwirtschaft soll der Branchenverband BITKOM mit seinen diversen Leitfäden[69] und Initiativen[70] genannt werden. Eine Mischung aus staatlicher Schirmherrschaft und der Beteiligung einer Vielzahl von Unternehmen aus dem IT-Bereich stellt das Internetportal „Cloud-Practice.de“ dar.[71] Auf europäischer Ebene gibt es, analog zur „deutschen Cloud“ des BITKOM, das privatwirtschaftliche Netzwerk „Eurocloud“.[72] Neben diesen deutschen und europäischen Initiativen gibt es entsprechende Aktivitäten in vielen anderen Staaten, insbesondere aber den Vereinigten Staaten von Amerika und China. Als Beispiele für US-Initiativen seien die „Cloud Security Alliance“[73] oder die „Open Data Center Alliance“[74] genannt. Chinesische Initiativen bestehen meist aus Kooperationen mit internationalen Unternehmen zum Aufbau von Cloudinfrastruktur. Als Beispiel sei der Bau eines kleinstadtähnlichen IT-Zentrums samt Rechenzentrum für Cloudanwendungen in Zusammenarbeit mit IBM erwähnt. Das Rechenzentrum wird bei seiner Fertigstellung mit 576 000 Quadratmetern mehr als fünf Mal so groß sein, wie das heutige größte Rechenzentrum.[75]

Neben diesen auf die Zukunft ausgerichteten Initiativen, Forschungsvorhaben und Investitionen ist in immer mehr Unternehmen Cloud Computing bereits heute im Alltagseinsatz. Es verstärkt sich der Eindruck, dass Ergebnisse von Umfragen bei CEOs, CIOs oder Administratoren hinsichtlich des geplanten Einsatzes oder zu ersten Erfahrungen im Unternehmenseinsatz beinahe täglich neu erscheinen.[76]

Die Mehrheit der Unternehmensentscheider ist zudem der Ansicht, dass Cloud Computing zukünftig eine hohe bis sehr hohe Bedeutung in ihrem Unternehmen haben wird.[77] Manche sprechen bereits davon, dass aus dem vermeintlichen Cloud-Computing-Hype der Standard für die Nutzung von IT werden wird.[78] Andere be-

---

69 Zum Beispiel der „Leitfaden Cloud Computing – Evolution in der Technik, Revolution im Business” und „Cloud Computing – Was Entscheider wissen müssen“.

70 Zum Beispiel die Initiative einer „deutschen Cloud“; *Krempl*, Nationale Computerindustrie soll „deutsche Cloud“ entwickeln, http://www.heise.de/newsticker/meldung/Nationale-Computerindustrie-soll-deutsche-Cloud-entwickeln-910368.html.

71 http://www.cloud-practice.de/de.

72 http://www.eurocloud.org.

73 http://www.cloudsecurityalliance.org/About.html.

74 http://www.opendatacenteralliance.org.

75 *Thibodeau*, China building a city for cloud computing, http://www.computerworld.com/s/article/9208398/China_building_a_city_for_cloud_computing; siehe zu den größten Rechenzentren auch unten Kap. 2.3.6.2.

76 So ergibt eine Googlesuche nach „Cloud Computing Umfrage“ unzählige Links zu Studienergebnissen; einzelne Studien wurden oder werden noch im Laufe der Darstellung thematisiert.

77 28 Prozent der befragten Unternehmensverantwortlichen gaben an, dass Cloud Computing in ihrem Unternehmen bereits genutzt wird; 58 Prozent sprachen sich für die hohe bis sehr hohe Bedeutung aus; siehe hierzu *Kretschmer/Bolliger/Koob* 2010, 24 ff.

78 *Ziegler*, Studie: Arbeiten in der Cloud wird künftig zum Standard, http://www.heise.de/newsticker/meldung/Studie-Arbeiten-in-der-Cloud-wird-kuenftig-zum-

zeichnen es, weder negativ (Hype) noch positiv (Standard) besetzt, als Trend.[79] Für manche ist bereits „der Wandel da“.[80] Andere propagieren beispielsweise die Slogans „die Cloud ist hier“ und „aus einem Buzzword wird jetzt Business“.[81]

So waren 81 Prozent der befragten Unternehmensentscheider der Ansicht, dass sich Cloud Computing am Markt etablieren wird. Drei Viertel der ICT-Entscheider,[82] in deren Unternehmen Cloud Computing bereits zur Anwendung kommt, gaben an, dass dieses Thema im Unternehmen einen sehr hohen oder hohen Stellenwert habe.[83] Für manche ist Cloud Computing bereits eine etablierte Technologie, wie im Rahmen der Berichterstattung zur CeBIT 2011 zu sehen war.[84]

Welchen Stellenwert Cloud Computing hat und zukünftig haben wird, erkennt man auch an den Reden und Auftritten von Microsofts CEO *Steve Ballmer*. Er verknüpft nicht weniger als die Zukunft von Microsoft mit dem Thema Cloud Computing. So sind folgende Zitate aus einer Rede vom 4.3.2010 zum Thema Cloud Computing überliefert: „for the cloud, we're all in“ und „literally, I will tell you we are betting our company on it“.[85]

In den Vereinigten Staaten von Amerika ist der Begriff des Hype ähnlich negativ besetzt, jedoch im Gegensatz zum deutschen Verständnis mit der Aussicht verbunden, dass sich die Technologie dennoch im Laufe der Zeit durchsetzen wird.

Das Marktforschungsinstitut Gartner präsentiert jedes Jahr den sogenannten „Hype Cycle Report“, der ältere, aktuelle und künftige Technologien bewertet und die Marktreife von 1.800 dieser Technologien und Trends in 75 Technologie- und Themenbereichen und Branchen untersucht. Ausgangspunkt des Zyklus ist ein sogenannter „technologischer Auslöser“ (Technology Trigger). Der Höhepunkt des Zyklus wird mit „Gipfel der überzogenen Erwartungen“ (Peak of Inflated Expectations) umschrieben. Im August 2010 waren unter anderem Cloud Computing allge-

---

Standard-1074638.html unter Bezugnahme auf die „Life 2“-Studie von *Kretschmer/Bolliger/Koob*; ebenso *Niemann/Hennrich*, CR 2010, 690.

79 *Birk/Wegener*, DuD 2010, 641.

80 *Dueck*, Informatik Spektrum 2009, 266.

81 So Microsoft-Deutschlandchef *Ralph Haupter* im Vorfeld zur CeBIT 2011; siehe hierzu *Grimming*, Microsoft will beim Cloud-Computing „Tempomacher“ sein, http://www.heise.de/newsticker/meldung/Microsoft-will-beim-Cloud-Computing-Tempomacher-sein-1195606.html.

82 ICT steht für „Information and Communications Technologies“.

83 *Kretschmer/Bolliger/Koob* 2010, 27.

84 *Digmayer*, IT-Sicherheit 1/2011, 18.

85 *Microsoft*, Steve Ballmer: Cloud Computing, https://www.microsoft.com/presspass/exec/steve/2010/03-04cloud.mspx.

mein und Cloudplattformen an der Spitze des Zyklus angelangt. Private Cloud Computing war zu dem Zeitpunkt kurz davor die Spitze zu erklimmen.[86]

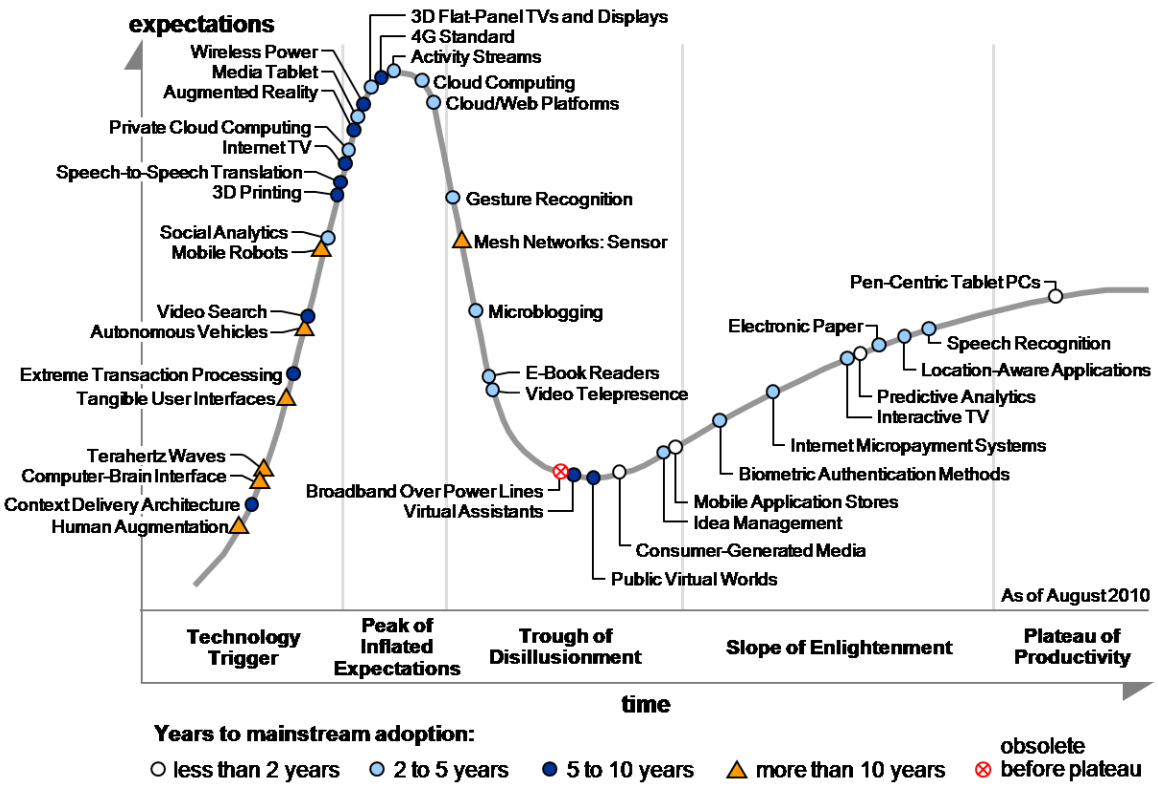

Abbildung 1: Hype Cycle 2010 mit Cloud Computing auf dem Höhepunkt[87]

Dem Höhepunkt folgt das sogenannte „Tal der Ernüchterung“ (Trough of Disillusionment), dem sich der „Weg der Erkenntnis“[88] (Slope of Enlightenment) anschließt. Hat eine Technologie schließlich all diese Höhen und Tiefen durchlaufen, folgt das sogenannte „Plateau der Produktivität“ (Plateau of Productivity).[89]

---

86 *Gartner*, 2010 Emerging Technologies Hype Cycle, http://blogs.gartner.com/hypecyclebook/files/2010/09/2010-EmergingTech-HypeCycle.png; *Baun/Kunze*, iX Special 2/2010, 40.

87 *Gartner*, 2010 Emerging Technologies Hype Cycle, http://blogs.gartner.com/hypecyclebook/files/2010/09/2010-EmergingTech-HypeCycle.png.

88 Auch als „Pfad der Erleuchtung“ übersetzt.

89 *Gartner*, 2010 Emerging Technologies Hype Cycle, http://blogs.gartner.com/hypecyclebook/files/2010/09/2010-EmergingTech-HypeCycle.png; *Hörmannsdorfer*, Gartner Hype-Cycle-Report: Cloud erklimmt Spitze, http://www.speicherguide.de/Magazin/StorageNews/tabid/114/articleType/ArticleView/articleId/13123/Gartner-Hype-Cycle-Report-Cloud-erklimmt-Spitze.aspx.

Gartner geht in seinem Hype Cycle 2010 davon aus, dass die Cloudtechnologien zwei bis fünf Jahre benötigen, um sich am Markt zu etablieren.[90]

2.1.2 Definitionsversuche

Eine der ersten wissenschaftlichen Definitionen aus dem Jahr 2008 beschreibt die Cloud als eine Art paralleles und verteiltes System, das aus einer Ansammlung von vernetzten und virtualisierten Computern besteht, die dynamisch bereitgestellt werden und als einzelne vereinigte Computerressource angezeigt werden, wobei das System auf Service Level Agreements basiert, die zwischen dem Provider und den Nutzer ausgehandelt wurden.[91]

Die weit überwiegenden Definitionsversuche entstammen jedoch nicht der Wissenschaft und Forschung, sondern sind parallel zum praktischen Einsatz und bei der Beobachtung der Entwicklung des Cloud-Computing-Marktes entstanden. So definiert beispielsweise das Analystenhaus Forrester Research Cloud Computing als „einen Pool aus abstrahierender, hochskalierbarer und verwaltbarer IT-Infrastruktur für Kundenanwendungen, dessen Dienste nach Verbrauch abgerechnet werden“.[92]

Das auf IT spezialisierte Marktforschungsunternehmen Gartner spricht wenig konkret vom „Bereitstellen skalierbarer IT-Services über das Internet für eine potenziell große Zahl externer Kunden“.[93]

Saugatuck Technology, ein auf SaaS- und Cloudthemen spezialisiertes Beratungshaus, versteht unter Cloud Computing „eine Kombination aus On-Demand-Infrastruktur (Rechner, Speicher, Netze) und On-Demand-Software (Betriebssysteme, Anwendungen, Middleware, Management- und Entwicklungs-Tools), die jeweils dynamisch an Geschäftsprozesse angepasst werden“.[94] Dazu gehört auch die Fähigkeit, komplette Prozesse zu betreiben und zu managen.[95]

Die Experton Group beschreibt Cloud Computing und Cloudservices als Dienstleistungen, die gewisse Kriterien erfüllen müssen. Die Dienste müssen im Self-Service-Modell bereitgestellt werden, der Zugriff muss über IP-Netze erfolgen und dabei orts- und geräteunabhängig möglich sein, die Dienste müssen skalierbar sein, stan-

---

90 *Gartner*, 2010 Emerging Technologies Hype Cycle, http://blogs.gartner.com/hypecyclebook/files/2010/09/2010-EmergingTech-HypeCycle.png.

91 *Buyya/Yeo/Venugopal* 2008, 3.

92 *Herrmann*, Cloud Computing - was ist damit gemeint?, http://www.pcwelt.de/news/Neuer-Hype-Cloud-Computing-was-ist-damit-gemeint-90005.html.

93 *Herrmann*, Cloud Computing - was ist damit gemeint?, http://www.pcwelt.de/news/Neuer-Hype-Cloud-Computing-was-ist-damit-gemeint-90005.html.

94 *Grohmann*, SaaS, PaaS, IaaS, S+S, Cloud Computing – Durchblick im Begriffswirrwarr, http://www.on-demand-business.de/2009/12/saas-paas-iaas-s-plus-s-cloud-computing-durchblick-im-begriffswirrarr.

95 *Grohmann*, Definition Cloud Computing, http://www.cloud-computing-report.de/definition.

dardisierte, virtualisierte Infrastruktur nutzen und nutzungsabhängig bezahlt werden.[96]

Für manche ist Cloud Computing ein neu entstehendes Computerparadigma, bei dem Daten und Services in großen, skalierbaren Datenzentren aufbewahrt werden und ubiquitär von jeder Internetverbindung aus erreicht werden können.[97]

Andere sehen Cloud Computing als einen neuen Trend, bei dem Daten und Rechnerleistung von PCs in große Datenzentren verlagert wird. Treiber für diesen Trend sind die allgemeine Verfügbarkeit von Breitbandzugängen, fallende Speicherkosten und Verbesserungen bei Internetsoftware.[98]

Dem BITKOM-Leitfaden zufolge ist Cloud Computing eine Form der bedarfsgerechten und flexiblen Nutzung von IT-Leistungen, die in Echtzeit als Service über das Internet bereitgestellt und nach Nutzung abgerechnet werden. Cloud Computing ermöglicht den Nutzern eine Umverteilung von Investitions- zu Betriebsaufwand.[99]

Der deutsche ICT-Anbieter T-Systems versteht unter Cloud Computing „die Miete von Infrastruktur und Software sowie Bandbreiten zu definierten Servicekonditionen. Diese Komponenten sollten täglich an den Kundenbedarf angepasst und mit höchster Verfügbarkeit und Sicherheit angeboten werden können. Ebenfalls Bestandteile von Cloud Computing sind End-to-End Service Level Agreements (SLAs) und verbrauchsabhängige Leistungsabrechnungen.“

Baun, *Kunze*, *Nimis* und *Tai* definieren Cloud Computing in ihrem gleichnamigen Buch wie folgt: „Unter Ausnutzung virtualisierter Rechen- und Speicherressourcen und moderner Webtechnologien stellt Cloud Computing skalierbare, netzwerkzentrierte, abstrahierte IT-Infrastrukturen, Plattformen und Anwendungen als On-Demand-Dienste zur Verfügung. Die Abrechnung dieser Dienste erfolgt nutzungsabhängig.“[100]

Das amerikanische National Institute of Standards and Technology (NIST) hat eine Definition von Cloud Computing formuliert, die auch im Laufe der Zeit immer detaillierter wurde. Die Definition in der finalen Version 16 lautet: „Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage,

---

96 *Hierlmeier*, Märchenstunde Cloud Computing, http://www.heise.de/resale/artikel/Maerchenstunde-Cloud-Computing-981746.html.

97 *Hug*, Will Cloud-based Multi-Enterprise Information Systems Replace Extranets?, http://www.infoq.com/articles/will-meis-replace-extranets; ähnlich *Schuster/Reichl*, CR 2010, 39.

98 *Dikaikos/Pallis/Katsaros/Mehra/Vakali*, IEEE Internet Computing, September/October 2009, 10; *Schuster/Reichl*, CR 2010, 39.

99 *Münzl/Przywara/Reti/Schäfer/Sondermann/Weber/Wilker* 2009, 9; *Schuster/Reichl*, CR 2010, 39.

100 *Baun/Kunze/Nimis/Tai* 2009, 4.

applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.“[101] Zu Deutsch: „Cloud Computing ist ein Ansatz, um den allgegenwärtigen und bequemen On-Demand-Netzwerkzugriff auf einen gemeinsamen Pool konfigurierbarer Rechnerressourcen (zum Beispiel Netzwerke, Server, Speichersysteme, Anwendungen und Dienstleistungen) zu ermöglichen, die mit geringstem Managementaufwand oder Eingriff eines Serviceanbieters schnell bereitgestellt und freigegeben werden können.“[102]

2.1.3 Vorzugswürdige Definition

Man könnte hier noch unzählige weitere Definitionsversuche[103] aufführen, wobei man jedoch bei einer vergleichenden Betrachtung bemerkt, dass sich die für Cloud Computing wesentlichen Merkmale in den Definitionsversuchen überschneiden und mehrfach vorkommen. Am weitesten und am detailliertesten ist die Definition des NIST vorangeschritten. Sie hat alle relevanten Eigenschaften, Merkmale und Kriterien zum Inhalt. Sie wurde mehrfach überarbeitet und angepasst. Außerdem spricht für die Definition die Behördeneigenschaft und Normierungsfunktion des NIST, so dass sie gewissermaßen offiziell wirkt. Entgegen der Definitionen privatwirtschaftlicher Unternehmen hat die NIST die Objektivität auf ihrer Seite, ohne verklausuliert die Tätigkeitsschwerpunkte eines Unternehmens herausstellen zu wollen. Je nach dem, was sich jeder Definierende für sich selbst und sein Unternehmen verspricht, werden jeweils andere Aspekte nach vorne gekehrt und betont.[104] Es ist also kein Zufall, dass sich die NIST-Definition immer weiter durchsetzt und immer mehr Akzeptanz findet.[105]

2.1.4 Informationstechnische Systeme, Cloudsysteme und Cloudumgebungen

Im Verlauf der Untersuchung werden auch die Begriffe „informationstechnische Systeme“, „Cloudsysteme“ und „Cloudumgebungen“ gehäuft vorkommen, so dass es sich anbietet, diese vorab zu erläutern und zueinander in Beziehung zu setzen.

Informationstechnische Systeme, oft nur als „IT-Systeme“ abgekürzt, sind nach dem Urteil des Bundesverfassungsgerichts zur Onlinedurchsuchung, in dem es das neue Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität eigengenutz-

---

101 *Mell/Grance* 2011, 3.

102 Siehe auch *Böhmer*, Warum Cloud Computing und IT-Grundschutz nur schwer vereinbar sind, http://www.searchsecurity.de/index.cfm?pid=8772&pk=248654.

103 Eine Sammlung mit 21 weiteren Definitionsversuchen findet sich bei *Geelan*, Twenty-One Experts Define Cloud Computing, http://cloudcomputing.sys-con.com/node/612375/print%5B2009-05-14.

104 *Herrmann*, Cloud Computing - was ist damit gemeint?, http://www.pcwelt.de/start/computer/pc/praxis/164486/cloud_computing_was_ist_damit_gemeint.

105 *Sotnikov*, Cloud Definitions: NIST, Gartner, Forrester, http://cloudenterprise.info/2009/08/04/cloud-definitions-nist-gartner-forrester; *Metzger/Reitz/Villar* 2011, 13.

ter informationstechnischer Systeme entwickelt hat, auch rechtlich belegt.[106] Zwar vermeidet das Bundesverfassungsgericht den Begriff zu definieren, jedoch wird aus der Aufzählung deutlich was darunter im Sinne des Gerichts unter Berücksichtigung der zugrundeliegenden Verfassungsbeschwerde zu verstehen ist. Nach dem Verfassungsgericht sind dies vom Endanwender eigengenutzte Geräte, wie Personal Computer oder Smartphones.[107] Zwar spricht das Gericht von der Vernetzung solcher Einzelsysteme und der gesteigerten Persönlichkeitsgefährdung und der Bedeutung für die Persönlichkeitsentfaltung, jedoch ist die Einschränkung der Systeme dem Umstand geschuldet, dass sich die Schutzrichtung nur auf die eigengenutzten Systeme der Endanwender beschränkt.[108]

Ebenfalls im Zusammenhang mit Onlinedurchsuchungen hat das Bundesministerium der Justiz im Vergleich zum Urteil ein weitergehendes und allgemeineres Verständnis des IT-Systembegriffs vertreten. Dem Ministerium zufolge ist ein informationstechnisches System „ein System, welches aus Hard- und Software sowie aus Daten besteht, das der Erfassung, Speicherung, Verarbeitung, Übertragung und Anzeige von Informationen und Daten dient“.[109]

Nach dieser vorzugswürdigen Definition zählen auch Großrechner oder ganze Rechenzentren, zum Beispiel für Cloud Computing, zu den IT-Systemen. Analog zu allgemeinen informationstechnischen Systemen wird deswegen im Weiteren auch von „Cloudsystemen“ gesprochen. Synonym dazu wird auch von „Cloudumgebungen“ die Rede sein.

Informationstechnische Systeme und die Einordnung als solche haben auch Bedeutung für die Sicherheit derselben, wie weiter unten zu sehen sein wird. So beziehen sich die IT-Schutzziele auch auf ebensolche informationstechnische Systeme, beispielsweise unter dem Aspekt der Systemsicherheit.

2.2 Begriffliche Einordnung

Cloud Computing wird in unterschiedlichen Zusammenhängen und insbesondere in medialen Erwähnungen, in der Regel ohne nähere Begründung, meist als eine Technologie, sehr oft als ein Geschäftsmodell und nicht selten als ein Konzept oder auch ein Paradigma bezeichnet. Der Verdeutlichung der jeweils dahinterstehenden Intention bei der Begriffswahl und als Konkretisierung des Begriffs sollen die anschließenden Ausführungen beitragen.

---

[106] BVerfGE 120, 274; siehe dazu auch weiter unten Kap. 3.1.3.2.

[107] BVerfGE 120, 302 f.

[108] BVerfGE 120, 304.

[109] *Bundesministerium der Justiz*, Fragenkatalog des Bundesministeriums der Justiz, http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf.

Bevor aber auf die einzelnen, den jeweiligen Begriff definierenden, Eigenschaften und Merkmale einzugehen ist, ist jedoch zu klären was Cloud Computing in einem übergeordneten Sinne darstellt.

Die freie Online-Enzyklopädie Wikipedia umschreibt Cloud Computing als einen Begriff aus der Informationstechnik.[110] Dem ist zwar zuzustimmen, führt aber nicht weiter. Im Folgenden werden in der weiteren Umschreibung des Begriffs in Wikipedia die Formulierungen „Ansatz“ und „Konzept“ verwendet.[111] Unstreitig dürfte sein, dass Cloud Computing keine Software oder Produkt als solches darstellt.[112] Die Einordnung als Technologie ist auch schwierig. Hinzu kommen die Abgrenzungsschwierigkeiten der Begriffe „Technik“ und „Technologie“.

2.2.1 Technologie und Technik

Technologie ist die Lehre von der Gewinnung, Bearbeitung, Herstellung, Produktion oder Distributionspolitik und -logistik von Stoffen und Erzeugnissen oder allgemein Waren sowie Dienstleistungen mithilfe der verfügbaren Techniken.[113] Der Begriff Technik bezeichnet eine Methode, die eingesetzt wird, um ein bestimmtes Ergebnis zu erreichen. Der enge Begriff der Technologie bezeichnet folglich das Wissen um diese Technik.[114] Nach diesem Verständnis ist Cloud Computing eine Technologie, weil mit Hilfe von Technik, beispielsweise der Virtualisierung, eine Anleitung oder Lehre gegeben wird, wie man möglichst schnell, einfach und billig eine neue Dienstleistung, nämlich IT-Services über das Internet „produziert“, sprich anbietet.

Nach einem weitläufigeren Begriffsverständnis ist eine Technologie eine Gesamtheit von Verfahren zur Produktion von Waren und Dienstleistungen.[115] Gerade dieser Aspekt der Gesamtheit und Kombination unterschiedlicher Einzelverfahren ist für Cloud Computing typisch, so dass auch der weite Technologiebegriff für Cloud Computing passend ist.

2.2.2 Konzept

Der Begriff Konzept beschreibt eine erste Fassung eines Textes oder einer Idee.[116] Cloud Computing wird als Konzept bezeichnet, weil es sich noch in einem frühen Anfangsstadium seiner Entwicklung befindet und nur allmählich tatsächlich nutzbare Dienstleistungen verfügbar werden. Für viele ist Cloud Computing immer noch theoretischer Natur und ein eher diffuser Begriff, der auch definitorische Schwie-

---

110 *Wikipedia*, Cloud Computing, http://de.wikipedia.org/wiki/Cloud_Computing.
111 *Wikipedia*, Cloud Computing, http://de.wikipedia.org/wiki/Cloud_Computing.
112 *Kurz*, Netzwoche 17/2008, 34.
113 *Rammert* 1999, 3.
114 *Wikipedia*, Technologie, http://de.wikipedia.org/wiki/Technologie.
115 *Wikipedia*, Technologie, http://de.wikipedia.org/wiki/Technologie.
116 *Wikipedia*, Konzept, http://de.wikipedia.org/wiki/Konzept.

rigkeiten bereitet. Konzepte kann man ändern und erweitern, genauso wie man die Vorstellung was genau Cloud Computing sein soll, kontinuierlich ändern kann.

Mit der Etablierung des Cloud Computing im Alltag und der Durchsetzung einer konsensfähigen Definition, wie der sich abzeichnenden NIST-Definition, wird die Bezeichnung als „Konzept“ im Laufe der Zeit verschwinden. Mittelfristig wird sogar der Begriff des Cloud Computing obsolet werden, weil irgendwann die Bereitstellung von IT als Dienst und die Auslagerung von Daten in verteilte Systeme den Normalzustand darstellen wird, der dann nicht mehr durch einen abgrenzenden Begriff beschrieben werden muss.[117]

2.2.3 Paradigma und Inhalt des Paradigmenwechsels

Das Wort „Paradigma“ kann mit den Synonymen „Beispiel“, „Vorbild“, „Muster“ oder „Abgrenzung“ und in allgemeinerer Form auch „Weltsicht“ oder „Weltanschauung“ umschrieben werden.[118] Im Zusammenhang mit Cloud Computing sind die Bedeutungen des Musters und der Abgrenzung zweckdienlich. „Muster“ meint die dem Technikbegriff inhärente Lehre und Anleitung, während durch den Aspekt der Abgrenzung der Unterschied zu herkömmlicher Informationstechnologie und die Neuheit verdeutlicht werden soll.

Der Paradigmenwechsel ergibt sich durch die „Tertiarisierung“[119] der IT und die Möglichkeit IT-Leistungen als Dienstleistung bereitzustellen und zu nutzen. Cloud Computing stellt zudem eine Verbindung zwischen Rechenleistung und TK-Infrastruktur her. Während sich früher Rechenleistung allenfalls in Grids mit mehreren Beteiligten teilen ließ, kann nunmehr jedermann einfach billig bereitgestellte Rechenleistung über das Internet nutzen. Bisher wurden Rechenleistung und Infrastrukturentwicklung parallel und getrennt als Maßstäbe für die technologische Entwicklung herangezogen (Maße sind zum Beispiel FLOPS[120] und Gbit/s). Insbesondere eine Variation des Mooreschen Gesetzes[121], nämlich die Rechenleistung pro 1000 US-Dollar ist ein anerkanntes Indiz für den technologischen Fort-

---

117 So auch *Metzger/Reitz/Villar* 2011, 182.

118 *Duden Online*, Paradigma, http://www.duden.de/rechtschreibung/Paradigma; *Wikipedia*, Paradigma, http://de.wikipedia.org/wiki/Paradigma.

119 Siehe dazu auch obige Fn. 50.

120 FLOPS steht für Floating Point Operations Per Second und bezeichnet die Gleitkommaoperationen, die ein Prozessor pro Sekunde ausführen kann.

121 *Intel*, Vierzig Jahre Mooresches Gesetz, http://www.intel.com/cd/corporate/techtrends/EMEA/deu/209836.htm.

schritt.[122] Diese hat sich bisher alle 18 bis 24 Monate verdoppelt.[123] Durch Cloud Computing soll sich dieser Zeitraum erheblich verringern.[124]

2.2.4 Geschäftsmodell

Um den ökonomischen Aspekt, also insbesondere die möglichen Einsparungen und das prognostizierte Wachstum und damit die beabsichtigten Gewinne zu verdeutlichen wird gerne vom „Geschäftsmodell Cloud Computing“ gesprochen. Schwerpunkt dieser Betrachtung sind weniger einzelne technische Merkmale und Eigenschaften, sondern die Konsequenzen für den Informationstechnologiemarkt. Cloud Computing hat demzufolge nicht nur einen technologischen Einschlag, sondern auch vor allem wirtschaftliche Bedeutung. Ohne diesen wirtschaftlichen Aspekt wäre Cloud Computing in der heutigen Form nie zustande gekommen.

2.2.5 Konsequenzen der begrifflichen Einordnung

Die jeweiligen Bezeichnungen sind alle in sich berechtigt, soweit sie eine gewisse sekundäre Bedeutung verdeutlichen sollen. Cloud Computing ist primär als ein Überbegriff zu verstehen.[125] Im weiteren Verlauf der Arbeit werden die obigen Begriffe auch weiter verwendet werden, je nachdem, welche Zielrichtung verfolgt wird. Unter technischen Gesichtspunkten wird von „Technologie“ und unter ökonomischen vom „Geschäftsmodell Cloud Computing“ zu sprechen sein. Um eine Abgrenzung zu Vorläufermodellen zu verdeutlichen, bietet sich die Verwendung des Begriffs „Paradigma“ an, während das frühe Entwicklungsstadium von Cloud Computing, wie erwähnt, am besten durch den Begriff „Konzept“ zu kennzeichnen ist. Bedeutsamste Erkenntnis dieser Auflösung begrifflicher Abgrenzungsfragen ist jedoch die, dass Cloud Computing gleichzeitig eine Technologie und ein Geschäftsmodell darstellt.[126]

2.3 Detailstruktur des Cloud Computing

Nach der begrifflichen Einordnung und Eingrenzung sollen im Folgenden die technischen und (infra)strukturellen Details und Voraussetzungen, Merkmale und Eigenschaften, die praktischen Einsatzbereiche, die Beteiligten und einige ausgewählte Anbieter, aber auch die Vorläufermodelle des Cloud Computing dargestellt werden.

---

122 Siehe zum Beispiel *Kurzweil*, The Law of Accelerating Returns, http://www.kurzweilai.net/the-law-of-accelerating-returns.

123 *Wikipedia*, Mooresches Gesetz, http://de.wikipedia.org/wiki/Mooresches_Gesetz.

124 *Martin*, Moore's Law Is Too Slow, http://www.infoq.com/news/2009/01/Moore-Law-Is-Slow; *Oswald*, Cloud-Computing to invalidate Moore’s Law?, http://thecloud2010.blogspot.com/2009/01/cloud-computing-to-invalidate-moores.html.

125 *Kurz*, Netzwoche 17/2008, 34.

126 So auch *Kesdogan*, in: Lepper, Privatsphäre mit System – Datenschutz in einer vernetzten Welt, 2010, 37.

2.3.1 Architektur und Erscheinungsformen (Schichtenmodell)

Eine erste Auffälligkeit ist das, mittlerweile nicht mehr in Frage gestellte, Schichtenmodell des Cloud Computing. Man unterscheidet, wie einleitend schon angesprochen, zwischen Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS).[127] Die Infrastrukturschicht stellt die unterste Schicht dar, gefolgt von der Plattformschicht, auf der wiederum die Anwendungs(software)schicht aufliegt. Je höher also die Schicht, umso eher handelt es sich um Softwaredienste.

2.3.1.1 Infrastructure as a Service (IaaS)

Auf der Infrastrukturebene werden durch die Anbieter grundlegende Dienste wie Rechenleistung (Prozessorleistung), Datenspeicher (Storage und Hosting) und zum Teil auch Kommunikationsverbindungen bereitgestellt. Wegen der Hardwarebezogenheit dieser Dienste ist auch die Bezeichnung Hardware as a Service (HaaS) gebräuchlich.

Mit Hilfe dieser virtualisierten Hardwareservices können die beiden SaaS- und PaaS-Schichten realisiert werden.[128] Dies ist jedoch nicht zwingend. Nutzer können die Basisservices auch für ihre anfallenden Aufgaben benutzen, beispielsweise umfangreiche Rechenoperationen durchführen oder Daten auf die Providerserver auslagern. Bei IaaS-Angeboten hat der Benutzer nämlich vollen Zugriff auf die virtuelle Hardware und kann auch selbst Anwendungen installieren. Im Gegenzug muss er die Server aber auch selbst administrieren und die nötigen Sicherheitspatches[129] für die von ihm eingesetzte Software einspielen.[130] Der Cloudprovider haftet dementsprechend auch nicht für Schäden, die auf die Fehlkonfiguration durch den Kunden zurückgehen.

Bekanntester Infrastrukturdienst ist die von Amazon angebotene Elastic Compute Cloud (EC2). Auch der Speicherdienst Amazon Simple Storage Service (S3) ist der IaaS-Schicht zuzuordnen. Weitere bekannte Cloudhostingdienste sind GoGrid[131] und Linode[132] oder das Angebot von Google namens „Google Storage“[133].

---

127 *Vaquero/Rodero-Merino/Caceres/Lindner*, ACM SIGCOMM Computer Communication Review, 51; *Niemann/Paul*, K&R 2009, 445; *Fickert*, in: Taeger/Wiebe, Inside the Cloud, 419.

128 Zu Einzelheiten zur Virtualisierung und den weiteren IaaS-Formen, wie Storage- oder Netzwerkvirtualisierung siehe unten Kap. 2.3.4.1.

129 Patch bedeutet übersetzt „Flicken”, „Füllstück“ oder auch „Pflaster”, wodurch die Zielrichtung eines Sicherheitspatches erkennbar wird, nämlich ein vorhandenes Sicherheitsloch zu „flicken”.

130 *Wikipedia*, Cloud Computing, http://de.wikipedia.org/wiki/Cloud_Computing#Infrastruktur.

131 http://www.gogrid.com.

132 http://www.linode.com.

133 http://code.google.com/intl/de-DE/apis/storage.

In der Literatur werden noch die unter IaaS liegenden Ebenen „Software Kernel“ und „Firmware/Hardware“ unterschieden.[134] Diese sind aber, wie mittlerweile wohl allgemeine Ansicht, auch problemlos als Teil der Infrastruktur einordenbar. Die über das dreiteilige Schichtenmodell hinausgehende Differenzierung ist auch nicht zielführend, weil die zusätzlichen Schichten nicht eigens als Service zur Verfügung gestellt werden können. Basishardware und Kernelsoftware sind schließlich immer notwendig und unabdingbare Basis aller Serviceangebote. Die Einordnung als Teil der Infrastruktur ist daher sachgerecht.

2.3.1.2 Platform as a Service (PaaS)

Platform as a Service bedeutet zum einen die Bereitstellung von Softwareentwicklungsplattformen durch Cloudprovider (Programming Environment) und zum anderen die Möglichkeit der Ausführung der entwickelten Software auf den Providerrechnern (Execution Environment).[135] PaaS richtet sich demzufolge an selbständige Softwareentwickler, Softwareentwicklungsunternehmen oder IT-Abteilungen von sonstigen Unternehmen.[136]

Der Vorteil der zentralen Bereitstellung in der Cloud liegt darin, dass der Aufwand der Erstellung einer Softwareentwicklungsumgebung für die Entwickler entfällt und nur einmal durch den Provider erbracht werden muss. Außerdem müssen sich Entwickler nicht mehr um die bisher notwendige Serveradministration kümmern, sondern können sich vollständig auf ihre Programmier- und Softwareentwicklungsaufgaben konzentrieren. Im Gegensatz zu IaaS können und sollen die Nutzer also nicht die zugrundeliegenden Server administrieren. Dieser Schritt wird vom Plattformanbieter übernommen.

2.3.1.3 Software as a Service (SaaS)

Für Unternehmen, Behörden und private Endnutzer ist Software as a Service die relevanteste Schicht. Anwendungssoftware wird vom Provider als Dienstleistung online bereitgestellt, wobei die Nutzung durch die Kunden üblicherweise nach der tatsächlichen Nutzungszeit abgerechnet wird. Das Modell stellt demnach eine Form der Softwaremiete dar. Softwareanwendungen werden entweder gar nicht mehr lokal installiert und nur noch ausschließlich über den Webbrowser genutzt oder nur rudimentär und in Teilen lokal installiert, während die Hauptbestandteile über das Netz bezogen werden. Dieses zuletzt erwähnte Modell ist die Integration des SaaS-Gedankens in lokal installierte Software und kann als Übergangsphase zu den vollständig online bereitgehaltenen Anwendungen angesehen werden.

---

[134] *Schuster/Reichl*, CR 2010, 39.
[135] *Baun/Kunze/Nimis/Tai* 2009, 33.
[136] *Heidrich/Wegener*, MMR 2010, 804.

Die Vorteile für SaaS-Nutzer sind vielfältig. Sie müssen die Software nicht lizenzieren, da diese Verpflichtung den Anbieter trifft.[137] Die Nutzer müssen sich nicht um die Pflege und Wartung der Software kümmern und nutzen, soweit der SaaS-Provider dies anbietet, immer die aktuellste Version der Software. Wegen der zentralen Bereitstellung sind die Wartung, die Softwarepflege und das Patchmanagement erheblich einfacher als bei vielen dezentral und lokal verteilten Versionen. Zudem bezahlt der Kunde nur die konkrete Nutzung, so dass insbesondere bei nur kurzzeitigem Nutzungsbedarf erhebliche Einsparungen im Vergleich zu einer herkömmlichen Anschaffung möglich sind. Für die längerfristige Nutzung einer bestimmten Software sind hingegen Pauschaltarife (Flatrates) oder sogar einmalige Zahlungen denkbar.[138] Auf Bedarfssteigerungen bei den Kunden sollte ein Anbieter flexibel und kurzfristig reagieren können.

Nachteilig sind die zeitweise Abhängigkeit vom ausgewählten SaaS-Anbieter und die zwingende Notwendigkeit einer funktionierenden Internetverbindung. Manche SaaS-Anwendungen sind allerdings auch in einem Offlinemodus benutzbar, so dass kurzzeitige Ausfälle des Zugangs zum Internet keine oder nur geringe Auswirkungen auf die Nutzung haben.

SaaS ist vom Vorgängermodell des Application Service Providing (ASP) und zum Teil vom klassischen IT-Sourcing abzugrenzen. Manche betrachten SaaS als Unterfall des Application Service Providing.[139]

2.3.1.4 Weitere Services (XaaS)

Oft wird in diesem Zusammenhang auch von „Everything as a Service“[140] gesprochen, wobei die Abkürzung XaaS verwendet wird und das „X“ als Platzhalter für den möglichen Service steht. Diese Erweiterung ist jedoch mehr marketingtechnisch bedingt, da sich die Services auch unter die drei Schichten subsumieren lassen. Oft werden auch Dienstleistungen, die überhaupt keinen Bezug mehr zum klassischen Cloud Computing haben, hinzugezählt, um auf den Werbehype um Cloud Computing „aufzuspringen“. Erwähnt sei beispielsweise „Humans as a Service“ (HuaaS), auch als „Crowdsourcing“ bekannt. Dabei wird menschliche Arbeits- und Geisteskraft online weltweit für die Lösung kleinerer Aufgaben nutzbar gemacht. Die menschliche Intelligenz wird zum Onlineservice. Für die Lösung werden Kleinstbeträge, meist wenige Cent oder Dollar, bezahlt. Beispiele der zu lösenden Aufgaben sind die Beschreibung eines Bildinhalts oder die Lösung sprachlicher Aufgaben,

---

137 Zu den urheberrechtlichen Einzelheiten siehe unten Kap. 3.7.

138 Amazon bietet bei EC2 sogenannte „Reserved Instances“ an, die für ein oder drei Jahre zum Festpreis gemietet werden können; zu Einzelheiten siehe *Amazon*, EC2 Reserved Instances http://aws.amazon.com/de/ec2/reserved-instances//180-8734204-0030346.

139 *Helwig/Koglin*, in: Taeger/Wiebe, Inside the Cloud, 176; *Dietrich*, ZUM 2010, 567; zu den jeweiligen Abgrenzungen siehe Kap. 2.3.6.

140 Unter anderem bei *Weiner/Renner/Kett* 2010, 74.

mithin für Menschen wenig zeitintensive Kleinstaufgaben, die von Computern entweder überhaupt nicht oder nur schwierig und sehr zeitaufwendig gelöst werden können.

Als bekanntestes Beispiel einer solchen Crowdsourcingumgebung sei der sogenannte „Amazon Mechanical Turk (AMT)“ genannt.[141] Die Bezeichnung nimmt Bezug auf den sogenannten „Schachtürken“ von 1769, ein Gerät, das bei den Zuschauern den Eindruck erweckte, dass dieses selbständig Schach spielte. Tatsächlich war aber im Inneren ein menschlicher Schachspieler versteckt, der es bediente.[142]

Im Gegensatz zu Crowdsourcing, das sich die mediale Aufmerksamkeit um Cloud Computing zunutze macht, hat Communication as a Service (CaaS), die vermeintlich modern angehauchte Bezeichnung für klassische Telekommunikationsdienstleistungen, zumindest einen Zusammenhang mit Cloud Computing, da TK-Dienstleistungen in Form von klassischen Internetzugängen und Internetbackbones die Basis für die Nutzung von Clouddiensten bilden.[143] Solche klassischen TK-Dienste können von einem einzelnen Anbieter auch zusammen mit Cloudservices bereitgestellt werden, so dass zumindest in einer solchen Konstellation die Notwendigkeit bestehen kann „CaaS“ von den eigentlichen Clouddiensten durch einen ähnlich klingenden Begriff abzugrenzen.

2.3.2 Nutzungsmodelle

Neben der Unterscheidung zwischen den drei Schichten ist auch eine Unterscheidung nach der organisatorischen Ausgestaltung der Cloudangebote üblich. Da diese verschiedenen Angebote unterschiedlich genutzt werden, werden sie auch mit dem Oberbegriff der „Nutzungsmodelle“ umschrieben. Die Unterscheidung dieser Nutzungsmodelle erfolgt zwischen jedermann zugänglichen und nutzbaren öffentlichen Clouds (Public und External Clouds) und solchen die nur unternehmens- oder organisationsintern, also nichtöffentlich, genutzt werden (Private und Internal Clouds).[144]

2.3.2.1 Public und External Cloud

Wenn man Cloud Computing sagt, meint man in den allermeisten Fällen das Nutzungsmodell der Public Clouds. Dies wird auch im Folgenden so gehandhabt. Soweit speziell Private oder Internal Clouds Gegenstand der Betrachtung sind, werden diese auch so bezeichnet.

---

141 https://www.mturk.com/mturk/welcome.

142 *Wikipedia*, Schachtürke, http://de.wikipedia.org/wiki/Schacht%C3%BCrke.

143 Zu diesem Modebegriff für TK-Leistungen siehe *Grünwald/Döpkens*, MMR 2011, 287 und *Gaul/Koehler*, Betriebsberater 2011, 2229; zu TK-Leistungen als Basis des Cloud Computing siehe auch unten Kap. 3.1.3.3.

144 *Niemann/Paul*, K&R 2009, 449.

Public Clouds richten sich an eine Vielzahl von potentiellen Kunden und sind für jedermann nutzbar, also an die Öffentlichkeit (Public) gerichtet. Die Leistungen werden dabei von Dritten im Sinne des § 3 Abs. 8 Satz 2 BDSG angeboten. Während Private und Internal Clouds unterscheidbar sind, wie zugleich zu sehen ist, werden die Begriffe Public Cloud und External Cloud synonym gebraucht.[145]

2.3.2.2 Private Cloud

Eine Private Cloud ist nicht für die Öffentlichkeit bestimmt, sondern wird von einer Organisation, zum Beispiel einem Unternehmen oder einer Behörde, intern genutzt. „Private“ bedeutet allerdings nicht zwingend, dass die Server Eigentum des Unternehmens sind, und auch nicht, dass das Unternehmen Betreiber der Cloud ist. Private bedeutet lediglich, dass diese organisatorische Einheit eine Cloudumgebung alleine und exklusiv nutzt und kontrolliert. Die Infrastruktur, insbesondere Rechenzentren und Server, können auch von einem externen Ressourcenanbieter angemietet sein. Datenschutzrechtlich stehen die Server aber immer unter der Verantwortung einer einzigen Daten verarbeitenden Stelle, nämlich der die Ressourcen nutzenden Organisation.[146] Private Clouds zeichnen sich also dadurch aus, dass sie von einer sie nutzenden Organisation kontrolliert werden.[147]

2.3.2.3 Internal Cloud

Anders ist dies bei der Internal Cloud. Die physische Infrastruktur, insbesondere das zwingend notwendige Rechenzentrum, ist im Eigentum und Besitz der Organisation, wodurch diese die unmittelbare physische Herrschaftsgewalt über die Server und Infrastrukturen, wie zum Beispiel Strom- und Datenleitungen, ausübt. Außerdem wird die Cloud von der Organisation selbst betrieben, wodurch diese die alleinige Entscheidungskompetenz hinsichtlich der Nutzungsrichtlinien und der zu nutzenden Software hat.[148] Die Anbieter- und die Benutzerseite sind damit immer identisch. Die alleinige datenschutzrechtliche Verantwortlichkeit ist damit offensichtlich.

Man kann Internal Clouds als Unternehmensintranet in Cloudform bezeichnen. Hauptziel ist die effiziente Nutzung vorhandener unternehmenseigener Ressourcen, wodurch sich auch der Schutz der Daten einfacher gestaltet. Die, auch vor allem physische, Kontrolle über die Daten wird vereinfacht und die Durchsetzung von Unternehmensrichtlinien ist leichter möglich als bei sonstigen Cloudnutzungsmodellen. Nachteilig sind dagegen die vergleichsweise eingeschränkte Flexibilität und

---

145 Anderer Ansicht jedoch *Urquhart*, Clarifying Internal Cloud versus Private Cloud, http://blogs.cisco.com/datacenter/clarifying_internal_cloud_versus_private_cloud.

146 *Weichert*, DuD 2010, 679.

147 Ähnlich *Urquhart*, Clarifying Internal Cloud versus Private Cloud, http://blogs.cisco.com/datacenter/clarifying_internal_cloud_versus_private_cloud.

148 *Curry/Darbyshire/Fisher/Hartman/Herrod/Kumar/Martins/Orrin/Wolf* 2010, 4.

Skalierbarkeit.[149] Je größer jedoch der zur Verfügung stehende Serverpark, desto flexibler ist dieser nutzbar und umso besser ist die Skalierbarkeit.

Eine Internal Cloud ist zwingend eine Private Cloud, aber eine Private Cloud muss keine Internal Cloud sein. Internal Clouds zeichnen sich also durch das Eigentum der Organisation an den Ressourcen aus, während es bei Private Clouds lediglich um die Ausübung der Kontrolle über (auch lediglich angemietete) Ressourcen geht.[150]

Rechtlich ist die Handhabung einer Internal Cloud weniger problematisch, da im Gegensatz zu weltweit angelegten Public Clouds oder angemieteten Ressourcen bei Private Clouds die Lokalisierung der Daten einfacher möglich ist. Zudem sind nur Daten einer Organisation vorhanden, so dass die Abschottung von Systemen und Teilen der Cloud entweder ganz entfallen kann oder weniger restriktiv erfolgen muss. Oft sind solche internen Clouds auch nur über das Hoheitsgebiet eines einzelnen Staates verteilt, so dass auch dadurch weniger rechtliche Probleme entstehen. Nichtsdestotrotz kann eine interne Cloud eines internationalen Großkonzerns die weltweite Ausbreitung und Verteilung einer Public Cloud erreichen. Die großen Cloudanbieter wie Amazon oder Google haben schließlich ihre faktisch vorhandene Internal Cloud, auch wenn diese Ressourcen zum Zeitpunkt des Aufbaus sicherlich nicht als solche bezeichnet wurden, zu einer Public Cloud umfunktioniert.

2.3.2.4 Hybrid Cloud

Hybrid Clouds sind eine Mischform aus Public und Private Clouds. Ein Teil der Daten und Dienste wird von den Nutzern in öffentliche Clouds ausgelagert oder Rechenleistung bezogen, während der andere Teil in der unternehmensinternen Private oder Internal Cloud vorgehalten und verarbeitet wird. Meist werden öffentliche Clouds mit Internal Clouds zu Hybrid Clouds kombiniert, um kurzfristig und kurzzeitig auftretende Lastspitzen abzufedern. Die Public Cloud ist in solchen Konstellationen nur Hilfsmittel, um die begrenzten Kapazitäten einer Private Cloud zu erweitern.

Auch unter Sicherheitsaspekten hat die Nutzung von Hybrid Clouds Vorteile. Dabei werden die schutzbedürftigsten Daten, insbesondere personenbezogene Daten Dritter oder Betriebs- und Geschäftsgeheimnisse, in der Private Cloud vorgehalten, während die weniger oder überhaupt nicht schützenswerten Daten in die Public Cloud ausgelagert werden.[151] Insofern ist diese nach Schutzbedürftigkeitserwägun-

---

149 *Streitberger*, Cloud-Computing-Sicherheit, http://www1.gi-ev.de/fileadmin/gliederungen/fb-sec/Dateien_FG_SECMGT/Workshop_2009-11-20/Streitberger_SIT_MUC_SST_GI_SECMGT_WS_v3.pdf, S. 13.

150 Siehe auch die ähnliche Unterscheidung bei *Urquhart*, Clarifying Internal Cloud versus Private Cloud, http://blogs.cisco.com/datacenter/clarifying_internal_cloud_versus_private_cloud.

151 So auch *Baun/Kunze/Nimis/Tai* 2009, 27 und die Umfrageergebnisse unter ICT-Entscheidern bei *Slamka/Georg*, in: Schartner/Weippl, D-A-CH Security 2010, 23 f.

gen getrennte Nutzung in gewisser Weise ein grober Gestaltungsvorschlag zur sicheren Nutzung von Cloud Computing.

Hybrid Clouds dürften zudem einen bruchfreien und schonenden Übergang zum Cloud Computing-Zeitalter ebnen, da viele Unternehmen bereits vorhandene eigene Hardware und Infrastrukturen in Form von Rechenzentren als Internal Clouds zusammenführen und nur schrittweise in öffentliche Clouds „umsiedeln“ werden. Diese Vorgehensweise hat den Vorteil, die vorhandenen Ressourcen möglichst lange auszunutzen und gleichzeitig für die Zukunft gewappnet zu sein. Sobald das eigene Rechenzentrum nicht mehr ausreicht oder finanziell nicht mehr tragbar ist, kann man vollständig in die, bis dahin nur parallel genutzte, öffentliche Cloud migrieren. Gewonnenes Know-how, Praxiserfahrungen aus dem Parallelbetrieb und praktisch erprobte Standards und Schnittstellen dürften diesen Übergang erleichtern.

2.3.2.5 Virtual Private Cloud

Mitte 2011 hat sich ein weiteres Nutzungsmodell herausgebildet, das – ähnlich wie die Hybrid Cloud – eine Kombination aus einer Public Cloud und einer Private Cloud darstellt. Dieses wird als Virtual Private Cloud bezeichnet. Erstes und bekanntestes Angebot einer solchen neuartigen Cloudform ist Amazons „Virtual Private Cloud“, das im August 2011 öffentlich verfügbar wurde.[152]

Die Neuerung besteht darin, dass ein Cloudanbieter ein virtuelles Rechenzentrum mit allen virtuellen Komponenten, die in einem physischen Rechenzentrum vorkommen, also eine virtuelle Private Cloud, über eine Public Cloud bereitstellt. Anstatt lediglich Speicherplatz oder Rechenleistung in Form von einzelnen virtuellen Rechnern bereitzustellen, wie dies bei herkömmlichen IaaS-Angeboten üblich ist, wird auch die Netzwerkinfrastruktur virtualisiert zur Verfügung gestellt.[153] Zudem können die Nutzer über eigene IP-Adressbereiche verfügen.[154]

Dadurch lassen sich viele Vorteile von Private und Public Clouds kombinieren. Die Beherrschbarkeit einer Private Cloud geht mit der Skalierbarkeit, Verfügbarkeit, Flexibilität und dem Self-Service-Modell einer Public Cloud einher. Außerdem ist eine Verbindung einer Virtual Private Cloud mit einem eigenen physischen Rechenzentrum möglich, so dass ein solches erweitert werden kann, ohne jedoch physische Komponenten kaufen und einbauen zu müssen.[155]

---

[152] http://aws.amazon.com/de/vpc.

[153] Siehe dazu insbesondere Kap. 2.3.4.2.2 und zu den einzelnen Komponenten *Amazon*, Welche Komponenten umfasst Amazon VPC?, http://aws.amazon.com/de/vpc/faqs/#G2.

[154] *Amazon*, VPC Funktionsweise, http://aws.amazon.com/de/vpc/#functionality.

[155] *Büst*, Arten von Cloud Computing (Redux), http://clouduser.org/grundlagen/arten-von-cloud-computing-redux-6048.

2.3.2.6 Community Cloud

Bei Community Clouds wird ursprünglich getrennt vorhandene Infrastruktur von mehreren Organisationen gemeinsam genutzt, wobei gemeinsame Anforderungen, beispielsweise zur Sicherheit oder zum Datenschutz kollektiv vereinbart und festgelegt werden.[156] Community Clouds sind damit Private Clouds mit einer überschaubaren Anzahl unterschiedlicher Organisationen als Nutzern. Mittels Community Clouds sind Einsparungen möglich, da die vorhandenen Ressourcen besser ausgenutzt werden.

Community Clouds sind, ebenso wie Internal Clouds, gerade in der öffentlichen Verwaltung und bei größeren Behörden oder sogar Geheimdiensten denkbar.[157] So planen angeblich die US-Geheimdienste CIA, NSA und die Defense Information Systems Agency (DISA) die Nutzung von Cloud Computing.[158] Für weniger sensitive Bereiche bietet die US-Regierungsbehörde „United States General Services Administration (GSA)“ unter „Apps.gov“ US-Bundesbehörden die Möglichkeit, Cloudressourcen für ihre Zwecke zu nutzen.[159] Die GSA selbst nutzt aber nicht nur eigene Ressourcen, sondern auch die Clouddienste von Microsoft oder Google.[160]

Einen groben Überblick über den Zusammenhang unterschiedlicher Nutzungsmodelle bietet die nachfolgende Grafik.

---

156 *Weichert*, DuD 2010, 680.

157 *Arthur*, Government to set up own cloud computing system, http://www.guardian.co.uk/technology/2010/jan/27/cloud-computing-government-uk.

158 *Melcon*, The CIA, NSA, and Others Precipitate Cloud Computing Reign, http://virtualization.sys-con.com/node/1335970.

159 https://apps.gov/cloud/advantage/main/start_page.do; zu Details siehe auch weiter unten Kap. 2.3.10; die Zahl der regierungseigenen Rechenzentren soll aber halbiert werden; siehe dazu *Sawall*, US-Regierung schließt fast die Hälfte ihrer Rechenzentren http://www.golem.de/1107/85094.html.

160 *Sawall*, US-Regierung schließt fast die Hälfte ihrer Rechenzentren, http://www.golem.de/1107/85094.html; siehe auch obige Fn. 159.

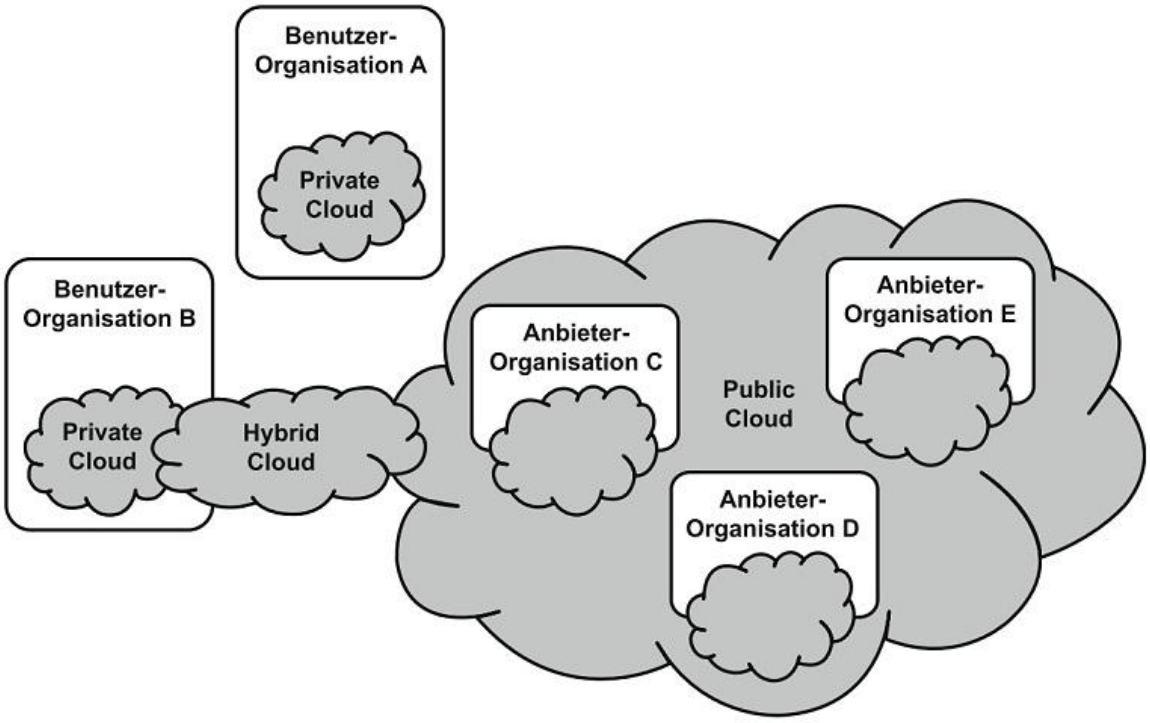

Abbildung 2: Zusammenhang unterschiedlicher Nutzungsmodelle[161]

2.3.3 Beteiligte

Wie an den unterschiedlichen Nutzungsmodellen zu sehen war, gibt es unterschiedliche Beteiligte. Es wird zwischen Cloudnutzern (Cloudkunden), Cloudanbietern (Cloudprovidern) und Ressourcenanbietern unterschieden.[162] Unter gewissen Umständen sind auch noch die Telekommunikationsanbieter zu berücksichtigen.

2.3.3.1 Cloudnutzer und Cloudanbieter

Abhängig vom Nutzungsmodell ist nicht immer zwingend ein Anbieter-Nutzer-Verhältnis vorhanden. Bei Internal und Private Clouds fällt nämlich die Nutzer- und Anbieterseite zusammen. Allerdings ist es bei Private Clouds nicht unüblich, dass das nutzende Unternehmen die notwendigen Infrastrukturen und Rechenzentren von Ressourcenanbietern anmietet, so dass ein weiterer Beteiligter zu beachten ist.[163]

Bei Public Clouds sind immer unterschiedliche Cloudanbieter und Cloudnutzer beteiligt. Cloudprovider vermarkten ihre eigenen Ressourcen und manchmal auch diejenigen von Ressourcenanbietern als Subunternehmen direkt an die Nutzer.

---

161 Aus *Baun/Kunze/Nimis/Tai* 2009, 27.

162 *Weichert*, DuD 2010, 680.

163 *Niemann/Hennrich*, CR 2010, 691; siehe hierzu auch noch einmal die Ausführungen im Rahmen der Nutzungsmodelle in Kap. 2.3.2; Einzelheiten zu den Ressourcenanbietern siehe sogleich in Kap. 2.3.3.2.

Wesentliches Merkmal eines Public-Cloudproviders ist folglich die Vermarktung seiner Dienstleistungen an jedermann als Endkunden, insbesondere auch an Verbraucher.

Bekannteste Cloudanbieter sind Amazon, Google, Microsoft und Salesforce. Diese und weitere Anbieter und deren Angebote und Geschäftsmodelle sollen weiter unten näher dargestellt werden.[164]

2.3.3.2 Ressourcenanbieter (Subunternehmen)

Die Clouddienstleistungen müssen nicht zwangsläufig vom Cloudprovider selbst stammen, sondern können auch durch Dritte, nämlich die Ressourcenanbieter als Unterauftragnehmer, erbracht werden.[165] Dies geschieht oft unter Einschaltung mehrerer, auch oft wechselnder Subunternehmen, die zudem auch noch in Kette zueinander stehen können. Insbesondere kleinere Cloudprovider werden die Ressourcen Dritter benötigen, um die Vollauslastung ihrer Infrastruktur zu verhindern.[166]

2.3.3.3 Telekommunikationsanbieter

Telekommunikationsanbieter sind zwar keine agierenden Stellen und nur mittelbar Teil des Cloudsystems, jedoch sind ihre Dienstleistungen, nämlich die Bereitstellung von Internetzugängen, Voraussetzung der Funktionsfähigkeit und Verfügbarkeit von Clouddienstleistungen. Noch selten, aber denkbar ist, dass ein Cloudanbieter auch noch zusätzlich die Bereitstellung des Internetzugangs realisiert und quasi alle Services aus einer Hand bietet, was auch für die Ausgestaltung der Service Level Agreements und die darin garantierten Verfügbarkeiten erhebliche Relevanz entfaltet.[167]

2.3.4 Technische und infrastrukturelle Voraussetzungen

Bevor Cloud Computing entstehen konnte, mussten einige Technologien in der Unternehmenspraxis heranreifen und sich außerdem das Internet als Vermittlungsinstanz in der Bevölkerung durch billige und performante Internetzugänge durchsetzen. Ohne Virtualisierung und Breitbandinternetzugänge sowie die Weiterentwicklungen im Bereich der verteilten Systeme wäre Cloud Computing nie in der jetzigen Form möglich gewesen. Im Folgenden sollen diese Einzelvoraussetzungen, nicht zuletzt, um das Verständnis für das Funktionieren der Cloudtechnologie zu schärfen, in gebotener Kürze näher erklärt werden.

---

164 Siehe dazu Kap. 2.3.8.

165 *Schulz/Rosenkranz*, ITRB 2009, 233; *Niemann/Hennrich*, CR 2010, 691; *Schulz*, MMR 2010, 78.

166 *Niemann/Hennrich*, CR 2010, 691.

167 Ähnlich ist die Kooperation zwischen Google und Vodafone, bei der Vodafone alle Services aus einer Hand bietet; siehe *Schmitt*, Google und Vodafone: Neue Clouds für Profis, http://business.chip.de/news/Google-und-Vodafone-Neue-Clouds-fuer-Profis_45376145.html.

2.3.4.1 Virtualisierung

Virtualisierung ist Kernelement des Cloud Computing und bedeutet die Abstraktion logischer Systeme von der physischen Implementierung und Infrastruktur.[168] Software und hierbei insbesondere das Betriebssystem und Daten sind von einer spezifischen physischen Hardware entkoppelt, dynamisch zuordenbar und als Dienst nutzbar.[169]

2.3.4.1.1 Vorteile der Virtualisierung

Die Vorteile der Virtualisierung liegen in der dynamischen Rekonfigurierbarkeit, der Unterstützung unterschiedlicher Netzwerkarchitekturen, der Reduktion des Verwaltungsaufwands und der Steigerung der Energieeffizienz.[170]

Dynamische Rekonfigurierbarkeit ist der Hauptvorteil der Virtualisierung. Virtuelle Ressourcen können erzeugt, bewegt, verworfen und sogar dynamisch verändert werden. Ein weiterer Vorteil der mittelbar mit der Rekonfigurierbarkeit zusammenhängt, ist die Steigerung der Funktionstüchtigkeit und damit der Verfügbarkeit von Systemen. Problembereiche eines virtuellen Systems können flexibel und schnell isoliert werden und notfalls durch funktionierende (virtuelle) Teilsysteme ersetzt werden. Virtuelle Systeme können mitunter sogar unterbrechungsfrei von einer physischen Maschine auf eine andere migriert werden.[171] Teilweise werden diese Möglichkeiten als „Erhöhung der Widerstandsfähigkeit eines Systems“ bezeichnet.[172]

Die Unterstützung unterschiedlicher Netzwerkarchitekturen bedeutet, dass mehrere virtuelle Netze mit unterschiedlichen Protokollschichten parallel zueinander auf dem physischen Netzwerk betrieben werden können.[173] Durch vereinheitlichte Schnittstellen und die Nutzung von Software ist zudem der Verwaltungsaufwand im Vergleich zu physischen Ressourcen und Hardware geringer.[174]

Virtualisierung kann auch genutzt werden, um die Energieeffizienz zu steigern. Vorhandene Hardware kann für mehrere Aufgaben gleichzeitig genutzt werden, wodurch die Auslastung steigt und die Hardwareressource im Idealfall optimal ausgenutzt wird. Die Zusammenfassung und Virtualisierung von physisch verteilten Diensten auf einer einzelnen physischen Hardwareinstanz kann sogar dazu führen,

---

168 *Beckereit/Frei/Koch/Meyer/Schaupp/Stedler/Walther 2009,* 4.
169 *Curry/Darbyshire/Fisher/Hartman/Herrod/Kumar/Martins/Orrin/Wolf* 2010, 2.
170 *Berl/Fischer/De Meer*, Informatik Spektrum 2010, 186, 192.
171 *Berl/Fischer/De Meer*, Informatik Spektrum 2010, 192.
172 *Berl/Fischer/De Meer*, Informatik Spektrum 2010, 191.
173 *Berl/Fischer/De Meer*, Informatik Spektrum 2010, 186.
174 *Berl/Fischer/De Meer*, Informatik Spektrum 2010, 186.

dass gewisse Hardware obsolet wird und damit abgeschaltet und ausgemustert werden kann.[175]

Das Ziel der Kapazitätsauslastung durch Virtualisierung ist einerseits vergleichbar mit dem Mainframezeitalter, als die damaligen Großrechner möglichst voll ausgelastet liefen, andererseits ergibt sich eine noch höhere Flexibilität als in der PC-Ära. Virtualisierung bietet das Beste aus beiden Welten.[176]

Im Ergebnis führt Virtualisierung zu einer neuen Anpassungsfähigkeit, wie man sie im Rahmen der Nutzung lediglich physischer Hardware nicht kennt und wie sie dort auch nicht möglich ist. Virtualisierung verbirgt einerseits die strukturelle Komplexität der physischen Systeme, erhöht jedoch andererseits die technische Komplexität eines solchen Gesamtsystems durch die zusätzliche Abstraktionsschicht.

2.3.4.1.2 Virtualisierung und Cloud Computing

Ohne Virtualisierung ist Cloud Computing nur eingeschränkt oder möglicherweise überhaupt nicht denkbar. Die meisten Vorteile des Cloud Computing ergeben sich erst aus der Nutzung von Virtualisierung. Die Vorteile der Virtualisierung äußern sich unmittelbar im Konzept „Cloud Computing“. Die Virtualisierung ist eine bereits seit längerem erprobte Technologie, so dass die Umsetzung durch einen Cloudprovider kaum Schwierigkeiten bereiten dürfte.[177] Auch ohne die Umsetzung durch das Cloudkonzept erlaubt die Virtualisierung für Unternehmen erhebliche Einsparungen. Hierbei ist auch noch viel Spielraum, weil lediglich ein Fünftel aller kleineren und mittleren Unternehmen (KMU) Virtualisierung einsetzt.[178] Außerdem ist ein kompletter oder nur schrittweiser Umstieg auf Cloud Computing einfacher, wenn vorher Virtualisierung genutzt wurde.[179]

Genauer betrachtet handelt es sich in Cloudumgebungen um sogenannte „Servervirtualisierung“. Bei der Nutzung unterscheidet man mehrere Klassen, Formen und Ebenen der Virtualisierung, je nachdem wie diese technisch und konzeptionell umgesetzt ist. Generell lassen sich drei Klassen der Virtualisierung ableiten, nämlich die Aufteilung einzelner physischer Systeme in mehrere logische Systeme (Partitio-

---

175 *Berl/Fischer/De Meer*, Informatik Spektrum 2010, 193.

176 *Carr* 2009, 94 f.

177 Insbesondere für die Umstellung vorhandener physischer Systeme auf virtuelle Systeme gibt es eine Vielzahl von Software, Tipps und Hinweisen, so zum Beispiel bei *Jung*, Server-Virtualisierung: Aller Anfang ist schwer, http://www.zdnet.de/it_business_technik_server_virtualisierung_aller_anfang_ist_schwer_story-11000009-41528094-1.htm; *Rath*, in: Schartner/Weippl, D-A-CH Security 2010, 191.

178 *Jung*, Server-Virtualisierung: Aller Anfang ist schwer, http://www.zdnet.de/it_business_technik_server_virtualisierung_aller_anfang_ist_schwer_story-11000009-41528094-1.htm.

179 So bezeichnet *Carr* in einem Interview der Computerwoche den Umstieg aus vorhandener Virtualisierung zu Cloud Computing als bloßes „Add-on“; siehe dazu *Cloer*, Nicholas Carr über den „Big Switch“, http://www.computerwoche.de/management/cloud-computing/1879045/index4.html.

nierung), die Verbindung mehrerer physischer Systeme zu größeren logischen Systemen (Aggregation) oder die Abbildung unterschiedlicher Systemarchitekturen aufeinander (Emulation).[180] Für Cloud Computing sind nur die beiden ersten Klassen maßgeblich. Emulation kommt eher im Privatbereich[181] oder zur Nutzung von älteren Systemen zum Einsatz.

2.3.4.2 Virtualisierungsformen

Virtualisierung ist auf verschiedenste Weise möglich. Üblicherweise wird zwischen physischer Partitionierung, der hypervisorbasierten Virtualisierung, Virtualisierung in einem Trägerbetriebssystem, der Betriebssystemvirtualisierung und der Anwendungsvirtualisierung unterschieden.[182] Daneben bestehen Sonderformen, wie die Konsolidierung und Aggregation von Ressourcen oder die Speicher- und Netzwerkvirtualisierung, die auf die Virtualisierung von Peripherie abzielen.

Einen Überblick über die verschiedenen Virtualisierungsformen soll das folgende Schaubild ermöglichen.

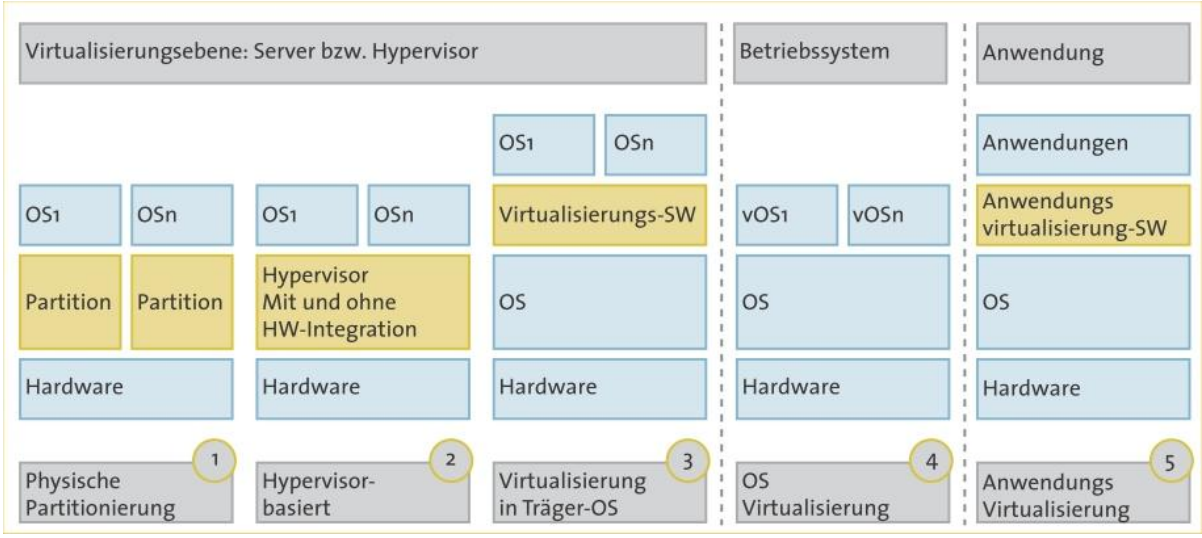

Abbildung 3: Übersicht der Virtualisierungsvarianten[183]

Für die weiteren Betrachtungen sind nur die hypervisorbasierte Virtualisierung und die Virtualisierung der Peripherie bedeutsam, so dass diese jeweils kurz erläutert werden sollen.

---

[180] *Beckereit/Frei/Koch/Meyer/Schaupp/Stedler/Walther 2009*, 4.

[181] Für weitere Einsatzmöglichkeiten im privaten Bereich siehe *Behrens*, Virtueller PC in zehn Minuten, http://www.pcwelt.de/start/software_os/systemtools/praxis/199097/virtueller_pc_in_zehn_minuten.

[182] *Beckereit/Frei/Koch/Meyer/Schaupp/Stedler/Walther 2009*, 5.

[183] *Beckereit/Frei/Koch/Meyer/Schaupp/Stedler/Walther 2009*, 7.

2.3.4.2.1 Hypervisorbasierte Virtualisierung

Bei dieser Virtualisierungsform wird eine hardwarenahe Virtualisierungsschicht implementiert, auf der Gastbetriebssysteme laufen können. Je nach eingesetztem Produkt ist hierfür teilweise eine Modifikation des Gastbetriebssystems notwendig (Paravirtualisierung). Ein Hypervisor ist dabei ein Softwaremechanismus für die Bereitstellung dieser zusätzlichen Virtualisierungsschicht. Diese beinhaltet die virtualisierte Hardware, also virtuelle Maschinen (VM) und die darauf laufenden virtuellen Gastbetriebssysteme.[184] Die Hypervisoren werden auch als Virtual Machine Monitor bezeichnet, was ihre Funktion etwas deutlicher beschreibt. Für die Datensicherheit ist es essentiell, dass eine Überführung von Daten zwischen unterschiedlichen virtuellen Maschinen oder Gastbetriebssystemen unmöglich ist. Moderne Prozessoren und Serverhardware unterstützen diese Form der Virtualisierung auch in Hardware, so dass in der Praxis kaum Leistungseinbußen durch die Nutzung von Virtualisierung auftreten. Die hypervisorbasierte Virtualisierung ist die für Cloudsysteme einfachste und am meisten eingesetzte Virtualisierungsform.

2.3.4.2.2 Netzwerkvirtualisierung mittels VLAN und VPN

Die Virtualisierung von Netzwerken mittels sogenannter Virtual Local Area Networks (VLANs) und Virtual Private Networks (VPN) hat für Cloud Computing ebenfalls Bedeutung, was nicht zuletzt an den neuartigen Virtual Private Clouds zu sehen ist.[185] VLANs erlauben die flexible organisationsinterne Auf- und Verteilung von virtuellen Netzen unter Nutzung eines zugrundeliegenden physischen Netzwerks. Die erneute physische Verkabelung, der Hinzukauf von zusätzlichen Routern und Switches und deren Konfiguration entfällt oder wird durch die Nutzung von VLANs erleichtert. Hinzu kommt die Flexibilität bei der Zuordnung von Endgeräten zu Netzwerksegmenten unabhängig vom Standort der Station.[186] Neben einer effizienten Nutzung eines physischen LANs[187] erlauben VLANs auch eine bessere Absicherung von Teilnetzen als geswitchte Teilnetze, so dass auch die Sicherheit durch deren Nutzung gesteigert wird. Schließlich lässt sich die Performance steigern, indem gewisse VLANs priorisiert werden.[188] Nachteilig ist jedoch, dass durch VLANs ein erhöhter Aufwand bei der Netzwerkadministration und bei der Programmierung der aktiven Netzkomponenten entsteht.[189]

---

184 *Slamka/Georg*, in: Schartner/Weippl, D-A-CH Security 2010, 27.

185 Siehe dazu oben Kap. 2.3.2.5.

186 *Wikipedia*, Virtual Local Area Network, http://de.wikipedia.org/wiki/Virtual_Local_Area_Network.

187 LAN steht für „Local Area Network", also ein lokales Netzwerk im Gegensatz zu einem WAN, das für „Wide Area Network" steht und ein Weitverkehrsnetzwerk bedeutet.

188 *Wikipedia*, Virtual Local Area Network, http://de.wikipedia.org/wiki/Virtual_Local_Area_Network.

189 *Baun/Kunze/Nimis/Tai* 2009, 15.

VPNs erlauben durch die Nutzung verschlüsselter Tunnel die sichere Verbindung von mehreren Rechnern oder Netzwerken über das öffentliche Internet und damit den sicheren Zugriff auf organisationsinterne Netze von außen.[190] Typischer Anwendungsfall ist der Zugriff von extern tätigen Mitarbeitern auf das organisationsinterne Intranet oder sogar den Zugriff auf einzelne ganz bestimmte Rechner, beispielsweise der Zugriff mittels Smartphone oder Laptop auf den eigenen Bürorechner.

2.3.4.2.3 Speichervirtualisierung

Speichervirtualisierung, oft auch als Storagevirtualisierung bezeichnet, ermöglicht eine effizientere Nutzung von vorhandenen Datenspeichern, zum Beispiel Serverfestplatten. Die Grundidee bei der Speichervirtualisierung liegt darin, den Datenspeicher von den klassischen Fileservern zu trennen und die physischen Speicher in Pools zusammenzufassen.[191] Durch Speichervirtualisierung erscheint Nutzern Speicherplatz virtuell. Der Speicherplatz kann durchaus in Speichersysteme oder Festplatten eingeteilt sein, allerdings müssen diese Medien nicht physisch vorhanden sein. Eine Software stellt dabei sicher, dass die virtuelle Speichereinteilung auf den physisch vorhandenen Speicherplatz passt. Nutzer profitieren von Speichervirtualisierung, indem sie nicht an physische Grenzen gebunden sind. Für Systembetreuer besteht der Vorteil darin, dass das vorhandene physische Speicherangebot effektiver auf die vorhandenen Nutzer aufgeteilt werden kann, wodurch sich der Auslastungsgrad verbessert.[192]

2.3.4.3 Verteilte Systeme, Parallelisierung und Computercluster

Cloudumgebungen, insbesondere Public Clouds, bestehen aus vielen, zum Teil weltweit, verteilten Rechnern und Rechenzentren. Sie bilden, nicht zuletzt wegen der Aggregation, ein verteiltes System. Dem Nutzer erscheint „die Cloud“ als ein einzelnes System. Vorteile einer solchen Anordnung sind die Steigerung der Rechenleistung, die Erhöhung der Ausfallsicherheit und Verfügbarkeit und die Möglichkeit Load Balancing einzusetzen und damit die Last optimal auf die verschiedenen Rechner und Rechenzentren zu verteilen. Durch die Parallelisierung der Rechenzentren werden die verteilten Ressourcen eines Anbieters optimal zusammengefasst und viel effizienter ausgelastet verglichen mit einer dezentralen und unkombinierten Nutzung.

Die Ausgestaltung als Computercluster führt zudem dazu, dass bei den Kunden die Illusion erweckt wird, die Ressourcen seien unendlich vorhanden und unendlich erweiterbar. Die Skalierbarkeit und schnelle Bereitstellung der Dienste verstärken diesen Anschein.

---

190 *Berl/Fischer/De Meer*, Informatik Spektrum 2010, 189.

191 *Baun/Kunze/Nimis/Tai* 2009, 13 f.

192 *Wikipedia*, Speichervirtualisierung, http://de.wikipedia.org/wiki/Speichervirtualisierung.

In diesem Zusammenhang ist die Tatsache interessant, dass sich Cloud Computing vorwiegend aus dem Umstand entwickelt hat, dass große Internetunternehmen, nicht zuletzt wegen des sogenannten „Dotcom-Booms“ zur Jahrtausendwende, überdimensionierte und nur teilweise ausgelastete und damit Kosten verursachende Rechenzentren besaßen. Dies brachte die Unternehmensverantwortlichen auf die Geschäftsidee, die brachliegenden Ressourcen zu vermarkten. Die Ursprünge des Geschäftsmodells „Cloud Computing“ sind somit eine Art Notlösung und wurden nicht klassisch geplant.

So hat der Onlinehändler Amazon mit seinen „Simple Storage Services (S3)“ und der sogenannten „Elastic Compute Cloud (EC2)“ im Jahr 2006 erstmals Cloud Computing für die Allgemeinheit zur Nutzung bereitgestellt. Die Testversion von EC2 startete am 24.8.2006 und wird von manchen als Geburtsstunde des öffentlich nutzbaren Cloud Computing angesehen.[193] Bei Amazon ergab sich davor das Problem, dass die IT-Infrastruktur auf das Weihnachtsgeschäft ausgelegt war, bei dem die Zahl der Anfragen und Einkäufe weit über der sonstigen Verkaufssaison liegen. Um den elektronischen Ansturm vor den Weihnachtsfeiertagen bewältigen zu können, sind große Rechenleistungen und Speicherkapazitäten erforderlich, die in diesem Umfang im restlichen Jahr nicht benötigt werden.[194] Dem Beispiel Amazons folgten Google, Microsoft, T-Systems und viele andere Internetunternehmen mit großen und unausgelasteten Rechenzentren.[195]

Besonders anspruchsvoll ist die Verteilung und Berechnung von großen Datenmengen, die angesichts des stetig ansteigenden Datenaufkommens immer größere, kaum vorstellbare, Dimensionen annehmen. Hierzu sind neuartige Ansätze und Technologien, insbesondere spezielle Datenbanksysteme, notwendig.

Apache Hadoop MapReduce ist ein auf Googles „BigTable“[196] basierender Open-Source-Java-Framework und erlaubt es, Rechenprozesse mit extrem großen Datenmengen im Petabytebereich (10^{15} Byte) durchzuführen.[197] So gehört die von Facebook verwendete Hadoop-Datenbank mit etwa 30 Petabyte (Stand: März 2011) zu den größten der Welt.[198] Auch der britische Nachrichtendienst „Government Communications Headquarters (GCHQ)“ soll die Technologie zur Auswertung der

---

193 *Reti/Pauly* 2009, 4.

194 *Kesdogan*, in: Lepper, Privatsphäre mit System – Datenschutz in einer vernetzten Welt, 2010, 38.

195 Die historische Entwicklung sowie die derzeit wichtigsten Cloudanbieter werden in Kap. 2.3.8 genauer beschrieben.

196 *Chang/Dean/Ghemawat/Hsieh/Wallach/Burrows/Chandra/Fikes/Gruber*, Bigtable: A Distributed Storage System for Structured Data, http://labs.google.com/papers/bigtable.html; *Sokolov* 2009, 60 f.

197 http://hadoop.apache.org/mapreduce; *Baun/Kunze*, iX Special 2/2010, 43.

198 *Yang*, Moving an Elephant: Large Scale Hadoop Data Migration at Facebook, https://www.facebook.com/notes/paul-yang/moving-an-elephant-large-scale-hadoop-data-migration-at-facebook/10150246275318920.

überwachten Kommunikation nutzen.[199] Hadoop wurde im Jahr 2011 vom britischen Guardian als „Innovator of the Year“ ausgezeichnet und als „Schweizer Taschenmesser des 21. Jahrhunderts“ sowie als „Beginn einer neuen Datenrevolution“ bezeichnet.[200]

Der Kurznachrichtendienst Twitter nutzt intern eine Bittorrenttechnologie namens „Murder“[201], um die Daten zwischen seinen Servern möglichst effizient zu verteilen. Analog zum P2P-Filesharing verteilen „Seederserver“ die Daten auf kleinere „Peerserver“. Die Echtzeitupdates der Daten auf allen Servern mithilfe von Bittorrenttechnologie soll Ressourcen schonen und damit den Dienst kosteneffizienter und letztlich auch zuverlässiger machen.[202] Von diesen Erkenntnissen und Entwicklungen wird auch das unternehmensrelevante[203] Cloud Computing profitieren.

2.3.4.4 Flächendeckende Durchsetzung von Breitbandinternetzugängen

Der Informatiker und heutige Google-Manager, *Eric Schmidt*, prophezeite bereits im Jahr 1993, dass in dem Moment, in dem die Bandbreite kein Nadelöhr mehr darstellen würde, „der Computer ausgehöhlt wird und sich über das Netzwerk verteilt“.[204]

Mit dem Aufkommen schneller Internetzugänge wurde es möglich, immer größere Datenmengen ins Internet zu verschieben und herunterzuladen. Die flächendeckende Durchsetzung schneller und breitbandiger DSL- und Kabelanschlüsse war Wegbereiter der effizient nutzbaren Vernetzung der Gesamtbevölkerung und ermöglichte damit erst die effiziente Nutzung von Cloudservices.[205] Jedes Jahr steigt die Anzahl der Internetnutzer, so dass mittlerweile knapp drei Viertel der

---

199 *Kremer*, Google-Software soll dem GCHQ beim Data-Mining helfen, http://www.gulli.com/news/google-software-soll-dem-gchq-beim-data-mining-helfen-2010-11-08.

200 *Guardian*, Megas 2011: Guardian Digital Innovation awards - Winners 2011, http://www.guardian.co.uk/megas/winners-2011; *Diedrich*, Apache Hadoop ist “Innovator Of The Year”, http://www.heise.de/newsticker/meldung/Apache-Hadoop-ist-Innovator-Of-The-Year-1215111.html.

201 http://github.com/lg/murder; „Murder“ steht dabei für den englischen Begriff eines Krähenschwarms.

202 *Ernesto*, Twitter Uses BitTorrent For Server Deployment, http://torrentfreak.com/twitter-uses-bittorrent-for-server-deployment-100210; *Vatter*, Kampf gegen den Fail-Whale: Twitter setzt auf BitTorrent, http://www.basicthinking.de/blog/2010/02/10/kampf-gegen-den-fail-whale-twitter-setzt-auf-bittorrent.

203 Facebook und Twitter sind zwar auch als Cloud Computing anzusehen, allerdings haben diese Privatanwender als Zielgruppe.

204 *Rodenhäuser*, Damit Sie nicht aus allen Wolken fallen, http://www.manager-magazin.de/unternehmen/it/0,2828,582750-2,00.html.

205 *Mansmann*, c’t 25/2010, 93; *International Telecommunication Union*, Measuring the Information Society 2010, http://www.itu.int/newsroom/press_releases/2010/pdf/PR08_ExecSum.pdf.

deutschen Bevölkerung online sind.[206] Mit der einhergehenden schnellen Vernetzung im Privatsektor und der allgemeinen Bereitstellung schnellerer Internetzugänge durch die Telekommunikationsanbieter wurden auch die Unternehmen in die Lage versetzt günstig breitbandige Zugänge zu nutzen.

Weil die meisten Internetzugänge asymmetrische Up- und Downloadgeschwindigkeiten aufweisen, ist das Senden von Daten durch einen Cloudkunden in Richtung Cloudanbieter oft noch mit längeren Wartezeiten verbunden, wenn größere Datenmengen hochgeladen werden sollen.[207] Insbesondere das erstmalige Aufsetzen des Kundensystems erfordert einen erhöhten Transferaufwand. Um dieses Problem zu entschärfen bieten Cloudprovider den Kunden die Option, Festplatten oder sonstige Datenträger mit den Daten per Post zuzuschicken, um sie dann vor Ort in die Cloudsysteme einzuspielen.[208] Auch der umgekehrte Weg ist denkbar, wenn auch weniger wahrscheinlich und nur bei sehr großen Datenmengen (Terabytebereich) angebracht.[209] Dieses umgekehrte Szenario greift meist dann, wenn der Kunde die Gesamtdaten auf lokale Ressourcen zurückportieren möchte.

Neben leitungsgebundenen Zugängen werden auch die im Mobilbereich bereits erreichten (HSPA) und mit der Vierten Generation (4G) geplanten Geschwindigkeiten (LTE) zu einer weiteren Durchsetzung von Cloudservices führen.

Als Beispiel für mobiles Internet und als spezifisch für den Mobilbereich ältester Cloudservice sei die Onlinenavigation erwähnt. Hierbei werden die Karten beim Anbieter vorgehalten und auch die Routen in dessen Systemen berechnet und nur noch die Navigationsanweisungen über das Mobilfunknetz an das Smartphone des Nutzers übermittelt. Da sich dadurch auch die Komplexität der im Handy benötigten Software in Grenzen hält, sind solche Navigationsservices auch auf älteren wenig leistungsfähigen Geräten nutzbar. Mittlerweile werden solche Dienste kostenlos angeboten. Der Vorteil der Onlinenavigation ist die Bereitstellung aktueller Karten durch den Anbieter und die Möglichkeit der Kunden, online Änderungen an der Verkehrsinfrastruktur und vor allem der aktuellen Verkehrssituation (automatisiert) melden zu können. Mittlerweile gibt es schon Systeme die anhand der im Mobilnetz eingebuchten Navigationsgeräte und den anonym übermittelten Positionsdaten den Verkehrsfluss und mögliche Staus in Echtzeit anzeigen können.[210] Auch hierfür werden Cloudservices genutzt, indem alle Berechnungen beim Onlinenavigations-

---

206 *Initiative D21*, (N)ONLINER Atlas 2011, http://www.nonliner-atlas.de.

207 *Mansmann*, c't 25/2010, 93.

208 *Tanenbaum*, AWS Import/Export: Ship Us That Disk!, http://aws.typepad.com/aws/2009/05/send-us-that-data.html; *Hagn*, Strato HiDrive macht Datenhaltung mobil, http://www.computerwoche.de/netzwerke/web/1928281/index2.html.

209 *Benz*, Download per Festplatte und Post, http://www.heise.de/newsticker/meldung/Download-per-Festplatte-und-Post-751501.html.

210 http://www.tomtom.com/livetraffic.

anbieter durchgeführt werden. Ähnliche Dienste werden in Zukunft, insbesondere mit der Durchsetzung des Ubiquitous Computing, vermehrt entwickelt werden.

2.3.5 Merkmale und Eigenschaften des Cloud Computing

Cloud Computing als Technologie und Geschäftsmodell sind gewisse spezifische Merkmale inhärent. Diese münden in vorteilhaften Eigenschaften, haben allerdings auch spezifische Charakteristika, die sich in Nachteilen äußern können. Bevor jedoch auf die Vor- und Nachteile im Einzelnen eingegangen wird, sind diese cloudspezifischen Merkmale und Eigenschaften zu untersuchen und darzustellen.

2.3.5.1 Mehrmandantenfähigkeit

Ein großer Vorteil der Virtualisierung liegt in der effizienteren Ausnutzung und Auslastung der physischen Hardware, indem auf einem physischen System virtualisiert mehrere Systeme laufen können. Dies führt dazu, dass mehrere Kunden (Mandanten) gleichzeitig das physische System nutzen können (Multitenancy).[211]

Ein Hypervisor sorgt dafür, dass die einzelnen virtuellen Systeme voneinander abgeschottet sind und nur der jeweils berechtigte Nutzer auf die eigenen Daten und Einstellungen zugreifen kann. Auch das laufende virtuelle System ist im Optimalfall durch den Hypervisor komplett abgeschottet, so dass keine Daten im Arbeitsspeicher abgreifbar sind.[212] Programmierfehler oder durch Malware hervorgerufene Fehler im Hypervisor, die diese Abschottung nicht mehr gewährleisten oder Zugriffe auf flüchtigen oder festen Speicher und die darin enthaltenen Daten anderer Kunden zulassen, sind zwar selten, jedoch nicht ganz auszuschließen. Daher ist es essentiell, dass die verwendete Virtualisierungssoftware höchsten Qualitäts- und Sicherheitsansprüchen gerecht wird. Mit der Sicherheit und der durchgehenden Funktionsfähigkeit des Hypervisors steht und fällt das Geschäftsmodell eines Anbieters. Bereits das einmalige „Überspringen“ der virtuell eingerichteten Grenzen kann das Vertrauen der Kunden erschüttern.

2.3.5.2 Schnelle Bereitstellung und Self-Service-Modell

Ein weiteres Merkmal, das mit der Virtualisierung einhergeht ist die schnelle Bereitstellung von Ressourcen, wie zum Beispiel Speicherplatz, Rechenleistung oder Software zur Nutzung durch den Kunden. Die Bereitstellung erfolgt durch Einrichtung einer virtuellen Maschine, die auf Knopfdruck erzeugt, abgeschaltet oder umkonfiguriert werden kann. Je tiefer die Cloudschicht, umso eher kann der Nutzer Einfluss darauf nehmen. Bei IaaS kann er sich die Ressourcen weitestgehend selbst

---

[211] Siehe zum Begriff und Konzept auch *Metzger/Reitz/Villar* 2011, 16.

[212] Zur Sicherheit von Hypervisoren und dem Trennungserfordernis siehe auch die Ausführungen im Rahmen der cloudspezifischen Bedrohungen in Kap. 3.1.9.10.1.1.

aussuchen, während bei SaaS lediglich die Software und fest zugewiesene Ressourcen, insbesondere Speicherplatz, bereitgestellt werden.[213]

Die jeweilige Bereitstellung erfolgt ohne das Zutun von Cloudmitarbeitern, so dass der Nutzer selbständig und ohne mühsame Überwindung von technisch oder organisatorisch bedingten Hindernissen seitens des Providers unkompliziert und schnell die Leistungen nutzen kann (sogenanntes „Self-Service-Modell“).[214]

Viele Softwareanwendungen in Form von Diensten sind zudem kostenlos verfügbar, so dass die Nutzer noch weniger Aufwand, wie zum Beispiel die Hinterlegung von Zahlungsdaten, vor der eigentlichen Nutzung haben.

2.3.5.3 Einfachere Wartung und Aufrüstung

Es ist offensichtlich, dass die zentrale Wartung und das Patchmanagement durch hochqualifizierte Mitarbeiter eines großen Cloudanbieters effektiver sind als in vielen kleinen dezentralen Rechenzentren oder bei unzähligen Privatrechnern. Herkömmlicherweise muss die Software auf jedem lokalen Computer aktualisiert und gewartet werden. Nicht selten obliegt es dem einzelnen Nutzer sich um die regelmäßig notwendig gewordenen Updates und Patches zu kümmern. Dass dies nur bedingt funktioniert, sieht man an den unzähligen Botnetzen und den von ihnen gekaperten Computern. Neben Kenntnissen, was genau aktualisiert werden muss (Betriebssystem, Anwendungssoftware, Browserplugins oder andere Software), fehlt es den meisten Internetnutzern an der Bereitschaft, sich regelmäßig um diese Pflichtaufgabe zur Wahrung der IT-Sicherheit zu kümmern.[215] Angesichts dieser Umstände dürfte die zentrale und einfachere Aktualisierung durch einen Cloudprovider zu einer erheblichen Steigerung der Sicherheit im gesamten Internet führen.

Die Einfachheit ergibt sich insbesondere aus dem Umstand, dass virtuelle Maschinen genutzt werden. Im Idealfall muss ein aktualisiertes System nur noch mehrfach geklont werden oder sogar nur einmal an zentraler Stelle aktualisiert werden, um den Kunden die aktuellste Software als Service anbieten zu können. Diese Aktualisierung von homogenen virtuellen Systemen auf Knopfdruck ist einfacher möglich als an unzähligen lokalen und unterschiedlich konfigurierten Computern, bei denen es nicht selten zu Updateschwierigkeiten kommt.

---

[213] Bei Amazons Cloudangeboten wird dem Nutzer hierfür die sogenannte „AWS Management Console“ zur Verfügung gestellt.

[214] Siehe dazu auch *Metzger/Reitz/Villar* 2011, 13.

[215] *BSI*, BSI-Bürgerumfrage zur Internetsicherheit, https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2011/BSI-Buergerumfrage-Internetsicherheit_11022011.html; so wissen die Mehrzahl der Internetnutzer um die potentiellen Bedrohungen und taugliche Gegenmaßnahmen, wie zum Beispiel zeitnahe Softwareupdates, jedoch handeln viele nicht nach diesem Wissen und unterlassen notwendige Sicherheitsmaßnahmen.

Virtuelle Systeme verringern auch den Aufwand der Hardwarewartung. Physische Wartungs- und Aufrüstarbeiten beziehen sich nur noch auf die Server in den Rechenzentren. Wegen der Virtualisierung sind Wartungs-, Update- und Aufrüstaufgaben nahezu unterbrechungsfrei und für den Kunden ohne Störungen oder Arbeitszeitverlust möglich.

Nicht unerwähnt soll jedoch bleiben, dass die lokalen Clients ebenso gewartet und mit Updates versehen werden müssen, was sich jedoch auch automatisiert lösen lässt, indem diese automatisch über die Cloud mit den neuesten Patches und Updates versorgt werden. Angesichts von schlanken und möglichst homogenen cloudspezifischen Betriebssystemen mit wenigen installierten Anwendungen ist auch die Komplexität der Updateprozedur erheblich geringer und weniger herausfordernd verglichen zu einem herkömmlichen Computer mit einem komplexen Betriebssystem mit einer Vielzahl installierter Anwendungen. Patchmanagement auf herkömmlichen Systemen ist praktisch nicht mehr machbar, solange man nicht Restriktionen einführt und nur noch die Installation von vorgegebener und geteseter Software zulässt, was jedoch praktisch allenfalls auf Unternehmensrechnern machbar ist.

2.3.5.4 On-Demand-Nutzung

On-Demand-Nutzung meint die, meist nur kurzzeitige, Nutzung bei Bedarf. Bezahlt wird nur die genutzte Rechenzeit oder das übertragene Datenvolumen oder eine Kombination aus beidem. Damit einhergehend sind auch einfache Bezahlmodelle wie Prepaid- und Postpaidverfahren. Teilweise kann man als Kunde auch Abonnements abschließen, insbesondere wenn man die Leistungen häufiger und regelmäßig nutzt. Die Modelle sind so vielfältig wie die Zahl der Anbieter. Allen gemein ist jedoch die Möglichkeit einer kurzen Vertragslaufzeit und die möglichst lose Bindung an einen Anbieter. Die Vielzahl der Anbieter und die oft nur befristete Bindung erleichtert zudem die – auch gleichzeitige – Nutzung mehrerer spezialisierter Cloudanbieter.

2.3.5.5 Geographische Verteilung der Server

Oft stehen die Server und Rechenzentren an vielen verschiedenen physischen Standorten. Je größer und internationaler eine Cloud, desto höher ist die Anzahl der Server und umso weiter verteilt sind diese. Neben der Ausfallsicherheit spielt auch die Verfügbarkeit in Form von Paketlaufzeiten eine Rolle. So sind wegen der begrenzten Lichtgeschwindigkeit und dem erhöhten Routingaufwand Paketlaufzeiten über längere Strecken zwischen dem Rechenzentrum und dem Endnutzer bereits so hoch, dass gewisse Anwendungen unter Umständen nicht mehr reibungslos funktionieren. Zu denken ist an Internettelefonie (VoIP) oder Onlinecomputerspiele, die eine sehr geringe Latenz benötigen.

Anbieter wie Google oder Amazon haben, angesichts ihrer weltweiten Aktivitäten, zahlreiche international verteilte Rechenzentren aufgebaut. Nicht zuletzt aus Gründen des Wettbewerbs und der Datensicherheit werden deren Standorte und genaue Anzahl geheim gehalten.[216] Ob sich dieses Vorgehen ändern wird, um beispielsweise Audits zu ermöglichen, muss die Zukunft zeigen.[217]

2.3.5.6 Zuverlässigkeit, Verfügbarkeit und Robustheit

Durch die Konzipierung als verteiltes System haben Clouds eine hohe Verfügbarkeit und Zuverlässigkeit. Es ist meist sehr unwahrscheinlich, dass sämtliche verteilten Rechenzentren gleichzeitig ausfallen. Nichtsdestotrotz können durch Fehlkonfigurationen oder sonstige Softwareprobleme auch solche Komplettausfälle vorkommen.[218] Indes ist die Wahrscheinlichkeit auf jeden Fall geringer als im Vergleich zu einem einzelnen kleinen dezentralen Unternehmensrechenzentrum, da ein solches selten über vergleichbare Redundanzen verfügt und das Know-how der Beschäftigten auch nicht unbedingt demjenigen von Beschäftigten in Großrechenzentren entspricht.

Große Rechenzentren, wegen der Größe auch als Serverfarmen, Serverparks oder Datacenter bezeichnet, werden auch von ihrer physischen Aufstellung schon anders konzipiert als ein Rechenzentrum oder Serverraum eines kleinen Unternehmens. Standorte für solche Serverfarmen müssen Erdbeben standhalten können oder werden direkt in erdbebenarmen Gebieten errichtet. Außerdem ist die Aufstellung in kälteren Regionen oder in der Nähe von Flüssen zwecks Nutzung als Kühlwasser ein wichtiger Standortfaktor. Weitere Aspekte spielen ebenfalls eine Rolle, wie zum Beispiel die Nähe zu Stromerzeugern, der Zugang zum Zentrum selbst, die Anbindung an Glasfasernetze und Internetbackbones oder die Qualifikation des Personals.

In diesem Zusammenhang ist die im Verantwortungsbereich der Telekommunikationsanbieter liegende Verfügbarkeit zu erwähnen. So muss nicht nur auf die Verfüg-

---

216 *Miller*, Google Data Center FAQ, http://www.datacenterknowledge.com/archives/2008/03/27/google-data-center-faq; eine Ausnahme ist das Rechenzentrum „Moncks Corner“ im US-Bundesstaat South Carolina; siehe *Wilkens*, Google gibt Einblicke in Rechenzentrum, http://www.heise.de/newsticker/meldung/Google-gibt-Einblicke-in-Rechenzentrum-1234222.html.

217 Erste Ansätze einer Öffnung sind durch die Präsentation des oben erwähnten Rechenzentrums erkennbar.

218 So war Salesforce.com beispielsweise im Januar 2009 für 38 Minuten nicht verfügbar; siehe dazu *Marwan*, Ausfall bei Salesforce.com: na und?, http://www.zdnet.de/magazin/39340246/ausfall-bei-salesforce-com-na-und.htm; Google und seine Dienste, insbesondere Google Mail fielen schon mehrfach aus; siehe dazu *McCarthy/Beiersmann*, Erneuter Ausfall von Google Mail, http://www.zdnet.de/news/wirtschaft_telekommunikation_erneuter_ausfall_von_google_mail_story-39001023-41003838-1.htm; ein Rechenzentrum von Amazon war sogar mehrere Tage nicht richtig nutzbar; siehe *Bleich*, US-Cloud von Amazon gestört, http://www.heise.de/newsticker/meldung/US-Cloud-von-Amazon-gestoert-1231873.html.

barkeit des Cloudproviders geachtet werden, sondern gerade auch auf diejenige des TK-Anbieters. Nicht selten wird es eher am stabilen Zugang zum Internet mangeln als an einem Ausfall auf Seiten des Cloudproviders. Deshalb ist es angebracht bereits bei der Planung des Internetzugangs über redundante Zugangsmöglichkeiten und Backupinternetprovider über alternative Infrastrukturen nachzudenken.

2.3.5.7 Skalierbarkeit

Skalierbarkeit ist die Fähigkeit, Ressourcen so zu erweitern, dass im Idealfall die Dienstkapazitäten linear zunehmen. Das wesentliche Merkmal einer skalierbaren Anwendung ist der Umstand, dass bei steigender Auslastung lediglich zusätzliche Ressourcen und keine umfangreichen Veränderungen der Anwendung selbst erforderlich sind.[219] Ein Produkt ist „gut skalierbar“, wenn es beispielsweise bei der zehnfachen Leistung mit etwa den zehnfachen Ressourcen auskommt, wohingegen ein „schlecht skalierbares“ Produkt zum Beispiel bei nur doppelter Last die zehnfachen Ressourcen benötigen und bei zehnfacher Last komplett ausfallen würde.[220]

Die Nutzung von effizienter Virtualisierungssoftware, die jahrelang in kleineren und größeren lokalen Rechenzentren praktisch eingesetzt und von den Herstellern im Laufe der Zeit immer weiter optimiert wurde, gewährleistet auch in Cloudumgebungen Skalierbarkeit auf einem hohen Niveau. Einer der großen Vorteile von Cloudumgebungen ist, dass sie aufgrund ihrer hohen Skalierbarkeit für alle Unternehmensgrößen einsetzbar sind. Sie erlauben eine flexible Skalierbarkeit „nach oben“ aber auch „nach unten.“ Je nach Unternehmensgröße, erhöhtem Kundenansturm oder Abflauen der Kundenzahlen können die Ressourcen einfach, schnell und flexibel zugeteilt und entzogen werden, wobei die Leistung entsprechend der Zuteilung oder Entziehung der Ressourcen skaliert.[221]

2.3.5.8 Homogenität

Wie bei der einfacheren Wartung und Aufrüstung erwähnt wurde, sind Cloudsysteme homogene Systeme.[222] Die Cloudkunden nutzen als Basis gleichartige Software oder Infrastrukturen. Bei SaaS und PaaS ist die Homogenität am höchsten, während IaaS die größten Spielräume zur individuellen Gestaltung der Systeme lässt, da hierbei nur die Infrastruktur, zum Beispiel Rechenleistung in Form von CPU-Instanzen oder Speicherplatz, und Steuerungssoftware vom Anbieter vorgegeben ist. Die zur Ausnutzung der Infrastruktur nötige Anwendungssoftware wird entweder vom Kunden auf den Cloudservice aufgespielt oder auch nur lokal ausgeführt,

---

[219] *Microsoft*, Skalierbarkeit, http://msdn.microsoft.com/de-de/library/aa292172%28VS.71%29.aspx.

[220] *Wikipedia*, Skalierbarkeit, http://de.wikipedia.org/wiki/Skalierbarkeit.

[221] Zu weiteren Aspekten der Skalierbarkeit siehe auch die Ausführungen zu den Vorteilen von Cloudsystemen weiter unten in Kap. 2.4.1.1.3.

[222] Siehe dazu Kap. 2.3.5.3.

wobei dann nur noch zu verarbeitende und verarbeitete Nutzdaten zwischen dem Infrastrukturprovider und dem Nutzer zirkulieren. SaaS- und PaaS-Angebote und deren Anwendungs- und Entwicklungssoftware sind hingegen vom Provider vorgegeben und werden bei diesem ausgeführt.

2.3.5.9 Messbarkeit und Überprüfbarkeit

Die Einhaltung von Vorgaben und der Leistungsbeschreibung aus SLAs, insbesondere die Verfügbarkeit und Servicequalität (QoS), muss messbar und nachvollziehbar sein. Protokollierung (Logging) und Monitoring sind essentielle Voraussetzung zur Überprüfbarkeit der Leistungserbringung sowie zur Vergleichbarkeit zwischen unterschiedlichen Cloudanbietern. Nur anhand von bestimmten nachprüfbaren Kriterien kann ein potentieller Kunde seinen Wunschanbieter heraussuchen. Dass Monitoring und die Protokollierung nicht nur Vorteile mit sich bringen, wird weiter unten zu thematisieren sein.[223]

2.3.5.10 Lizenzfreiheit und -klarheit

Im Gegensatz zu herkömmlichen Lizenzmodellen muss die Software nur einmal vom Cloudprovider angeschafft werden. Angesichts der cloudtypischen Nutzung durch die Kunden muss jedoch gewährleistet sein, dass die Lizenzen so ausgestaltet sind, dass der Cloudprovider die Software den Kunden anbieten darf. Ob die schwankenden Nutzerzahlen im Lizenzierungsmodell mitberücksichtigt werden oder ein Festpreis vereinbart wird, ist Sache des Softwareherstellers und des Cloudproviders. Im Ergebnis dürfte die, insbesondere nur sporadische, Nutzung für den Kunden eine Ersparnis im Vergleich zu eigenlizenzierten lokalen Softwarelösungen bedeuten. Wie oben angedeutet hat der Cloudkunde auch kein Problem mehr mit Über- oder Unterlizenzierung, da er die Cloudanwendungen nur noch nach Bedarf nutzt und bezahlt.

2.3.6 Entwicklung des Cloud Computing und Abgrenzung zu seinen Vorläufermodellen

Die Darstellung der Entwicklung des Cloud Computing und vor allem der Vergleich zu den Vorläufermodellen hat auch Bedeutung für die späteren rechtlichen Betrachtungen. Insbesondere die rechtliche Bewertung der Vorläufermodelle kann auch für Cloud Computing vergleichbare Lösungsansätze aufzeigen. Um diese rechtliche Bewertung möglichst treffend durchführen zu können und Analogien bilden zu können, ist es jedoch unabdingbar die Details der Vorläufermodelle und die Unterschiede zu Cloud Computing zu kennen.

Cloud Computing ist nicht „über Nacht“ entstanden, sondern resultiert aus verschiedenen längerfristigen technologischen Trends und Vorläufermodellen sowie

[223] Siehe dazu auch die Aspekte der Protokollierung als Sicherheitsmaßnahme, aber auch als Sicherheits- und Datenschutzrisiko in Kap. 3.1.9.9.5.

den wechselnden Bedürfnissen von Privatanwendern und Unternehmen.[224] Die Grundidee ist auch keineswegs neu. Bereits vor 20 Jahren prägte *John Gage* von Sun Microsystems den Slogan „the network is the computer“.[225]

Mit der Vorstellung von Amazons EC2 kann man den 24.8.2006 als den Geburtstag des nutzbaren Cloud Computing ansehen. Der Begriff an sich wurde schon viel früher geprägt.[226] Populär wurde er aber erst 2007, was auch der erste Eintrag in der englischen Wikipedia vom 3.3.2007 beweist. Dieser enthielt bezeichnenderweise einen Verweis auf Utility Computing. Etwa zu diesem Zeitpunkt versuchte Dell, sich die Wortmarke schützen zu lassen. Das gelang zwar im Juli des gleichen Jahres, aber bereits wenige Tage später wurde die Marke wieder gelöscht.[227]

Größere Popularität gewann die Idee Cloud Computing im Jahr 2008. Damals fanden sich bei Google über 10,3 Millionen Treffer zum Suchbegriff „Cloud Computing“. Der Geltungsbereich von Cloud Computing wuchs von einfachen Infrastrukturdiensten wie Speicher und Rechenressourcen hin zu Applikationen. Das bedeutete jedoch auch, dass zum Teil Vorläufer wie Application Service Providing (ASP) als Cloud Computing bezeichnet wurden.[228] Im Laufe der letzten Jahre ist Cloud Computing zum Trendthema der Informationstechnologie avanciert. Mitte März 2010 waren 33,4 Millionen Treffer in Googles Suchmaschine zu finden, während im Oktober 2011 über 176 Millionen angezeigt wurden. Allein im Newsdienst „Google News“ kommen innerhalb von wenigen Minuten immer wieder neue Nachrichten- oder Fachartikel hinzu, die das Begriffspaar enthalten.

Trotz der überbordenden Euphorie ist noch einmal darauf hinzuweisen, dass durch die Idee brachliegende Ressourcen zu vermarkten, Cloud Computing „aus der Not geboren“ ist und deshalb eine nur beschränkt durchdachte und stringent konzeptionierte Technologie darstellt.[229] Nicht zuletzt deswegen war auch die Definitionslage so unübersichtlich. Cloud Computing entwickelte sich folglich im Laufe der Zeit stetig weiter, man kann sogar sagen, dass sich sein Kerngehalt erst im Laufe der anfänglichen Entwicklung herauskristallisierte.

Cloud Computing besteht zwar aus einer Neukombination vorhandener Technologien und früherer Geschäfts- und Bereitstellungsmodelle, jedoch ist es durch weitergehende und unterschiedliche Merkmale davon abgrenzbar.

Angesichts der Vorläufertechnologien und Geschäftsmodelle sowie deren Abwandlung und Kombination ist es sicherlich berechtigt zu sagen, dass Cloud Computing

---

224 *Kurz*, Netzwoche 17/2008, 34; siehe dazu auch Kap. 1.
225 *Schuster/Reichl*, CR 2010, 39.
226 Siehe auch oben Kap. 2.1 und Fn. 54.
227 *Reti/Pauly* 2009, 4.
228 *Reti/Pauly* 2009, 4.
229 Siehe zur Geschichte des Cloud Computing auch die einleitenden Ausführungen in Kap. 2.1.

keine Revolution, sondern eine Evolution darstellt. Sowohl die Entwicklung der Infrastruktur (Utility Computing, Grid Computing) als auch die verschiedenen Vorläufermodelle zur Bereitstellung von Software (ASP, SaaS) haben im Ergebnis zu Cloud Computing geführt.[230] In der gegenwärtigen Diskussion um Cloud Computing wird allerdings häufig ausgeklammert, dass leistungsfähige Netze eine unverzichtbare Basis darstellen. Konsequenterweise müsste man also den Startpunkt des Cloud Computing mit der Entwicklung des Internet in Zusammenhang bringen.[231]

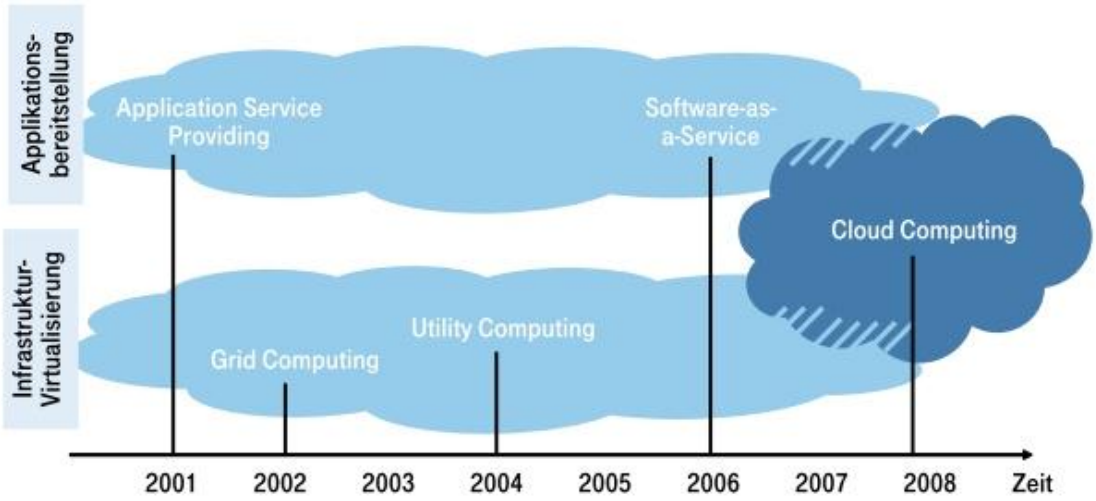

Abbildung 4: Entstehung des Cloud Computing aus den Vorgängermodellen[232]

2.3.6.1 Internet und verteilte Systeme

Auf die Darstellung der historischen Entwicklung des Internets wird hier verzichtet.

Cloud Computing stellt eine Form verteilter Systeme dar. Ein verteiltes System ist nach der Definition von *Andrew Tanenbaum* ein Zusammenschluss unabhängiger Computer, der sich für den Benutzer als ein einzelnes System präsentiert.[233] Dies gilt auch für Cloud Computing. Die unterschiedlichen Server oder Serverfarmen erscheinen dem Nutzer als ein zusammenhängendes Einzelsystem. Auch die Buchung von spezifischer Rechenleistung oder Speicherplatz ändert daran nichts. Dem Nutzer erscheint der gebuchte virtualisierte „Cloudrechner“ oder der Cloudspeicherplatz als Teil eines einzigen, scheinbar unlimitierten Systems, das vermeintlich unendlich erweiter- und skalierbar ist.

---

230 So zum Beispiel bei *Reti/Pauly* 2009, 4 nachzulesen; siehe dazu auch die folgende Grafik.

231 *Reti/Pauly* 2009, 5.

232 *Reti/Pauly* 2009, 4.

233 *Tanenbaum/van Steen* 2007, 1 ff.; *Wikipedia*, Verteiltes System, http://de.wikipedia.org/wiki/Verteiltes_System.

2.3.6.2 Cluster Computing

Ein Computercluster ist ein verteiltes System und die Vernetzung von mehreren Rechnern, nicht selten Hochleistungsrechnern, über ein lokales Netzwerk (LAN). „Cluster“ bedeutet „Schwarm“, „Gruppe“ oder „Haufen“ und beschreibt bildhaft das zugrundeliegende Modell. Die in einem Rechenzentrum miteinander verbundenen Server bilden ein solches Cluster. Wie bereits erwähnt kann man diese auch als Serverfarmen oder Serverparks bezeichnen.[234] Ziel des Clusterings ist die Erhöhung der Rechenleistung und der Verfügbarkeit.

Eine Statistik aus dem Jahr 2010 über Internetunternehmen mit der größten Serveranzahl wird mit weitem Abstand von Google (über 1 Million Server oder ca. zwei Prozent aller Server weltweit) angeführt, gefolgt von Intel (um die 100 000), der deutschen 1&1 Internet AG (70 000), dem französischen Hostinganbieter OVH (65 000), dem Webbeschleuniger Akamai Technologies (61 000) und dem Cloudanbieter Rackspace (56 671).[235] Facebook verfügt hingegen lediglich über ca. 30 000 Server und rangiert damit im Mittelfeld.[236] Beachtlich ist zudem, dass Unternehmen wie Amazon, Microsoft oder Hewlett-Packard keine Angaben zu ihren Servern machen wollten. Schätzungen belaufen sich auf jeweils mehr als 50 000 Server.[237] Über die tatsächlich verfügbare Rechenleistung oder Speicherkapazität sagt die Statistik jedoch nichts aus.

Eine andere Statistik weist die größten Rechenzentren anhand der von den Servern genutzten Fläche aus. Demzufolge ist das „Lakeside Technology Center“ in Chicago im April 2010 mit 1,1 Millionen Quadratfuß (ca. 102 000 Quadratmeter) das größte Rechenzentrum der Welt, gefolgt vom „Metro Technology Center“ in Atlanta mit 990 000 Quadratfuß und dem „NAP of the Americas“ in Miami mit 750 000 Quadratfuß.[238] China plant 2016 ein Rechenzentrum mit 576 000 Quadratmetern fertigzustellen.[239]

Computercluster stellen nur die Vernetzung von vorhandenen Ressourcen dar, ohne dass etwas über die konkrete Art der Bereitstellung oder Nutzungsmöglichkeit von

---

234 Siehe dazu Kap. 2.3.5.6.

235 *Intac*, Who owns the most servers?, http://www.intac.net/wp-content/uploads/2010/04/most-dedicated-servers.png; *Kremp*, Wer die meisten Server hat, http://www.spiegel.de/netzwelt/gadgets/0,1518,689123,00.html.

236 *Intac*, Who owns the most servers?, http://www.intac.net/wp-content/uploads/2010/04/most-dedicated-servers.png.

237 *Kremp*, Wer die meisten Server hat, http://www.spiegel.de/netzwelt/gadgets/0,1518,689123,00.html.

238 *Miller*, Special Report: The World’s Largest Data Centers, http://www.datacenterknowledge.com/special-report-the-worlds-largest-data-centers.

239 *Thibodeau*, China building a city for cloud computing, http://www.computerworld.com/s/article/9208398/China_building_a_city_for_cloud_computing; siehe auch oben Kap. 2.1.1.

Diensten ausgesagt wird. Cluster sind demnach nur eine frühe Vorstufe des späteren Cloud Computing. Ein Zwischenschritt dazu war das Grid Computing.

2.3.6.3 Grid Computing

Grid Computing ist die lose Kopplung von mehreren Computerclustern über Weitverkehrsnetze (WAN[240]).[241] Der Begriff „Grid“ wird abgeleitet aus „Electrical Power Grid“ (Stromnetz), dessen Idee darin besteht, die Ressourcen den Benutzern so zur Verfügung zu stellen als ob sie Strom aus der Steckdose bekommen.[242]

Während früher Computercluster und Hochleistungsrechner (HPC[243]) üblicherweise lokal an einen einzigen physischen Standort gebunden waren und auch nur lokal vernetzt waren, führt Grid Computing mehrere dieser geographisch verteilten Einzeleinheiten zu einem „virtuellen Supercomputer“ zusammen. Dies führt zur Entstehung von Virtuellen Organisationen (VO). Der Begriff der Virtuellen Organisation beschreibt eine dynamische Allianz von Organisationen, die ein gemeinsames Interesse während der Nutzung des Grids vertreten.[244]

Oft werden die Grids genutzt, um eng definierte rechenintensive wissenschaftliche – insbesondere mathematische – Probleme zu lösen.[245] Grid Computing ist jedoch, im Gegensatz zu dessen kurzzeitigem Vorgänger, dem Metacomputing, nicht nur auf reine Rechenleistung beschränkt. So können über standardisierte Schnittstellen auch weitere IT-Ressourcen wie Software, Datenbanken, Speicherplatz oder spezielle Hardware miteinander vernetzt werden.[246]

Eine Definition, die alle diese Elemente enthält wurde von *Ian Foster* und *Carl Kesselman* formuliert. Sie lautet: „Die gemeinsame Nutzung von Ressourcen ist nicht primär der Austausch von Dateien, sondern vielmehr der direkte Zugriff auf Computer, Software, Daten und andere Ressourcen, wie sie bei einer Reihe von kollaborativen, problemlösenden und Ressourcen vermittelnden Strategien benötigt werden, die zurzeit in Industrie, Wissenschaft und im Ingenieurwesen auftauchen. Diese gemeinsame Nutzung von Ressourcen ist, notwendigerweise, in einem Höchstmaß kontrolliert, wobei die Anbieter und Konsumenten der Ressourcen klar und eindeutig festlegen, welche Ressourcen geteilt werden, wem die gemeinsame Nutzung erlaubt ist und unter welchen Bedingungen die gemeinsame Nutzung er-

---

240 Siehe oben Fn. 187.

241 *Büst*, Was ist Grid Computing?, http://clouduser.org/grundlagen/was-ist-grid-computing-156; ähnlich *Hoeren/Spittka*, MMR 2009, 589.

242 *Büst*, Was ist Grid Computing?, http://clouduser.org/grundlagen/was-ist-grid-computing-156; *Fuhrmann-Koch*, Grid Computing-Technologie: Rechenleistung wie Strom aus der Steckdose ziehen, http://idw-online.de/pages/de/news241139; wie einleitend ausgeführt, ist der Vergleich zum elektrischen Strom mittlerweile für Cloud Computing kennzeichnend.

243 High Performance Computing.

244 *Büst*, Was ist Grid Computing?, http://clouduser.org/grundlagen/was-ist-grid-computing-156.

245 *Wikipedia*, Grid-Computing, http://de.wikipedia.org/wiki/Grid-Computing.

246 *Büst*, Was ist Grid Computing?, http://clouduser.org/grundlagen/was-ist-grid-computing-156.

folgt. Eine Menge von Individuen und/oder Institutionen, die sich durch solche Richtlinien zur gemeinsamen Nutzung von Ressourcen ergeben, formen das, was wir eine Virtuelle Organisation nennen.“[247]

Ein entscheidender Vorteil von Grids liegt darin, dass der geographische Ort, an dem sich die Ressource befindet, nicht mehr von Bedeutung ist, vergleichbar mit den Webservern des World Wide Web. Grid Computing ist als Basistechnologie für die Koordination und Verarbeitung organisationsübergreifender Geschäftsprozesse und den gemeinschaftlichen Austausch und die Nutzung von Ressourcen anzusehen und damit ein Vorläufer des Cloud Computing.[248]

Je nach genutzter Ressource lassen sich unterschiedliche Arten von Grids klassifizieren. Die beiden wichtigsten Formen von Grids sind Rechengrids und Datengrids. Rechengrids (Computing Grids) erlauben den Zugriff auf verteilte Rechenressourcen und die Kombination der Rechenleistung, während Datengrids (Data Grids) den Zugriff auf verteilte Datenbanken und die gemeinsame Nutzung der enthaltenen Daten ermöglichen. Daneben gibt es noch sogenannte Application Grids, Ressource Grids, Service Grids und Knowledge Grids.[249]

Die Beschränkung auf die Lösung von – oft wissenschaftlichen – Problemen unter Ausnutzung der gemeinsamen, verteilten Ressourcen ist das wesentliche Unterscheidungsmerkmal zu Cloud Computing. Während bei Letzterem Unternehmensressourcen zusammengeführt werden, um eine optimale Auslastung und Ausnutzung der vorhandenen Hardware zu erreichen, liegt der Zusammenschluss von Hochleistungsrechnern bei Grid Computing hauptsächlich in der Steigerung der Kapazitäten, namentlich der Rechenleistung. Die Lösung eines (mathematischen) Problems würde die ursprünglich alleinstehenden und voneinander getrennten Computer überfordern. Was die Beteiligten anbelangt besteht eine große Ähnlichkeit zu Community Clouds, da bei Grid Computing häufig nur wenige verschiedene Akteure, meist wissenschaftliche Institutionen, beteiligt sind. Ein wesentliches Unterscheidungsmerkmal ist allerdings die fehlende Flexibilität bei Grid Computing. Die Zusammenschlüsse erfolgen nicht spontan und abhängig von der wirtschaftlichen Unternehmenssituation oder den vorhandenen Ressourcen, sondern werden unter den Beteiligten längerfristig geplant und – nicht selten in lang andauernden Rechenprozessen – durchgeführt, mit dem Ziel, ein spezifisches Problem zu lösen oder dessen Lösung zu erleichtern und zu beschleunigen. Außerdem sind Grids hie-

---

247 *Foster/Kesselman* 2003; so auch *Metzger/Reitz/Villar* 2011, 24.

248 *Büst*, Was ist Grid Computing?, http://clouduser.org/grundlagen/was-ist-grid-computing-156.

249 *Büst*, Was ist Grid Computing?, http://clouduser.org/grundlagen/was-ist-grid-computing-156; *Wikipedia*, Grid-Computing, http://de.wikipedia.org/wiki/Grid-Computing.

rarchisch strukturiert und es gibt immer eine koordinierende Instanz. Beides sind Merkmale, die in dieser Form bei Cloud Computing nicht vorkommen.[250]

2.3.6.4 Utility Computing

Der englische Begriff „utility“ bezieht sich auf Versorgungsleistungen wie Strom, Telefon, Wasser und Gas, die von einem Versorgungsbetrieb bereitgestellt werden. Ähnlich wie beim Strom- oder Telefonnetz bezieht der Kunde beim Utility Computing die Leistung „Computing“, also Rechenleistung, über ein Netz. Der Verbrauch wird gemessen und abgerechnet.[251] Es gilt das Pay-as-You-Go-Bezahlmodell.[252]

Utility Computing ist der unmittelbare Vorläufer des Cloud Computing und beinhaltet schon wesentliche Kriterien und Eigenschaften, die bei Cloud Computing noch deutlicher zum Vorschein kommen. Erwähnt seien die Skalierbarkeit, der nutzungsabhängige Preis, möglichst standardisierte Dienste oder auch die Virtualisierung und Automatisierung.[253] Service Level Agreements sind angesichts eines Anbieter-Kunden-Verhältnisses ebenfalls bereits von hoher Bedeutung.

Cloud Computing ist eine Form von Utility Computing, aber Utility Computing ist nicht Cloud Computing. Anders gesagt: Cloud Computing ist die größtmögliche praktische Umsetzung des Geschäftsmodells „Utility Computing“ angereichert um neue cloudtypische Merkmale. Insbesondere die bedarfsgerechte On-Demand-Anforderung der Leistungen bei Cloud Computing und die Flexibilität bei der Auswahl der Anbieter sind als Abgrenzungsmerkmale zu nennen. Diese sind eine Neuerung im Vergleich zur fortdauernden Bereitstellung beim Utility Computing. Strom, Gas oder Wasser werden dauernd bereitgestellt und man nutzt üblicherweise längerfristig einen bestimmten Anbieter, während bei Cloud Computing höchstmögliche Flexibilität bei der Anbieterauswahl und nur kurze Vertragslaufzeiten, entsprechend dem tatsächlichen Bedarf, Merkmal des Geschäftsmodells sind.

2.3.6.5 Klassisches IT-Outsourcing

Streng genommen ist Cloud Computing in Form von Software as a Service eine moderne und erweiterte Form des klassischen IT-Outsourcing, wie es schon seit etwa 20 Jahren praktiziert wird.[254] Der Begriff „Outsourcing“ ist ein Kunstwort, das

---

250 *Wikipedia*, Grid-Computing, http://de.wikipedia.org/wiki/Grid-Computing; allenfalls ein Cloudprovider einer Public Cloud mit unzähligen Subunternehmen kann mit einer solchen koordinierenden Instanz verglichen werden.

251 *Wikipedia*, Utility Computing, http://de.wikipedia.org/wiki/Utility_Computing.

252 *Tetzner* 2010, 32.

253 *Wikipedia*, Utility Computing, http://de.wikipedia.org/wiki/Utility_Computing.

254 *Schwarze/Müller*, HMD – Praxis der Wirtschaftsinformatik, Heft 245, 2005, 6 ff.; *Schwarze/Müller*, IT-Outsourcing - Erfahrungen, Status und zukünftige Herausforderungen, http://hmd.dpunkt.de/245/01.html.

sich aus den englischen Begriffen „outside“, „resource“ und „using“ zusammensetzt.[255]

Klassisches IT-Outsourcing bedeutete die Auslagerung von Teilen oder der kompletten Informationstechnik eines einzigen Unternehmens zu genau einem Outsourcinganbieter. Es wurde demnach die sogenannte One-to-One-Strategie angewandt. Der Kunde gab dabei seine Wünsche permanent an den Anbieter weiter, während sich dieser mit Hilfe des gewonnen fachlichen Wissens auf die individuellen Bedürfnisse des Kunden spezialisierte. Daraus resultierte meist eine intensive und langfristige Beziehung zwischen den Geschäftspartnern.[256]

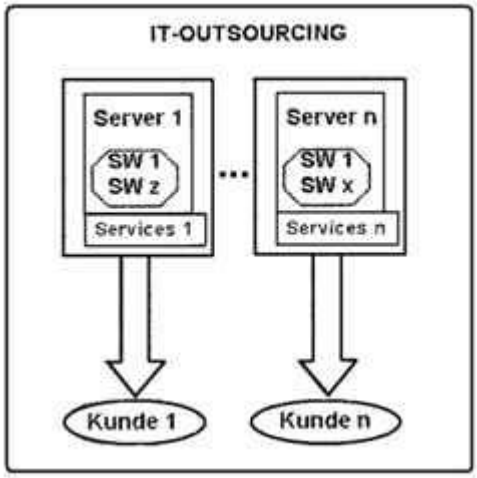

Abbildung 5: Beziehung zwischen Kunden und Anbietern beim IT-Outsourcing[257]

Die Unterschiede zu Cloud Computing und dabei insbesondere zu Software as a Service sind offensichtlich. Auffälligste Unterscheidungsmerkmale sind die Zuordnung physikalischer Ressourcen und die Möglichkeit der Prozessanpassung beim Outsourcing sowie die unterschiedlichen Vertragslaufzeiten.

Das klassische Outsourcing verfolgte das One-to-One-Prinzip und damit die feste Zuordnung von physikalischen Ressourcen in Hard- und Software an ganz bestimmte einzelne Kunden (Singletenancy-Prinzip[258]). Der Anbieter erarbeitete zudem mit dem Kunden gemeinsam die individuell auf diesen zugeschnittene Lösung.[259] Cloud Computing verfolgt demgegenüber den One-to-Many-Ansatz

---

255 *Schwarze/Müller*, HMD – Praxis der Wirtschaftsinformatik, Heft 245, 2005, 6 ff.

256 *Herold/Müller*, Cloud Computing und SaaS, http://knol.google.com/k/cloud-computing-und-saas.

257 Aus *Leonhard* 2009, 20; *Schmitt*, Software as a Service (SaaS), http://knol.google.com/k/software-as-a-service-saas?hl=de&lr=lang_en|lang_de.

258 *Essoh/Doubrava/Münch* 2011, 17.

259 *von Westerholt/Berger*, CR 2002, 82.

(Multitenancy-Prinzip) und die flexibilisierte Zuteilung und Skalierbarkeit der verfügbaren Ressourcen, ohne individuelle Abstimmung mit den einzelnen Cloudnutzern.[260]

Während beim klassischen IT-Outsourcing der Anbieter die Anwendungen durch die individuelle Betreuung an die Geschäftsprozesse anpasst, muss der Kunde dies bei Cloud Computing über Webschnittstellen selbst erledigen, da der Cloudprovider nur die Dienste bereitstellt und deren Betrieb verantwortet.[261] Ein Eingehen auf die spezifischen Eigenheiten der IT-Umgebung und die Wünsche des Kunden wird weder angeboten, noch ist diese enge Beziehung gewollt. Die Kunden nutzen nach dem One-to-Many-Ansatz alle die gleiche Plattform und Software. Lediglich die Abschottung der jeweiligen Einzelumgebungen mittels Virtualisierung erfolgt individuell.

Ein weiterer Unterschied besteht darin, dass für klassisches Outsourcing in der Regel der Nutzer Lizenzen für die Nutzung von Software erwirbt und diese dann an den Outsourcinganbieter weitergibt, während bei Cloud Computing ein solcher Softwareerwerb oder Lizenzerwerb durch den Cloudnutzer gerade nicht erfolgt oder allenfalls eine Unterlizenzierung, abhängig vom konkreten Einzelfall, nötig ist.[262]

Auch die Laufzeiten von klassischen Outsourcingvertragsverhältnissen unterscheiden sich von den Laufzeiten der Cloud-Computing-Vertragsverhältnisse. Während klassisches Outsourcing, wie oben dargestellt, auf mittel- bis längerfristige Laufzeiten ausgelegt ist, werden Cloudservices meist kurz und nur bei Bedarf genutzt.[263] Dieses kurzfristige Eingehen von Geschäftsbeziehungen hat zudem den Vorteil, Services unterschiedlicher Anbieter gleichzeitig oder nacheinander zu nutzen und somit im Sinne der serviceorientierten Architekturen (SoA) die Geschäftsprozesse bei unterschiedlichen Anbietern auszulagern und ablaufen zu lassen.[264] Im Idealfall existieren dafür Standards und offene Schnittstellen, so dass Vendor Lock-in,[265] das im Übrigen beim klassischen IT-Outsourcing durch die Bindung an den einen Anbieter dem Geschäftsprinzip quasi inhärent war, möglichst vermieden wird.

Nutzungsmodelle wie IaaS oder PaaS gab es beim klassischen IT-Outsourcing ebenfalls nicht. Der Nutzer war an die Infrastruktur des einen Anbieters gebunden. Softwareentwicklungsmöglichkeiten durch den Kunden waren gerade nicht vorgesehen. Die Software wurde vom Anbieter, anhand der spezifischen Wünsche und Anforderungen der Nutzer, selbst entwickelt.

---

260 *Schulz/Rosenkranz*, ITRB 2009, 233.

261 *Streitberger/Ruppel* 2009, 8; *Essoh/Doubrava/Münch* 2011, 18.

262 *von Westerholt/Berger*, CR 2002, 82; zu den lizenzrechtlichen Aspekten siehe die Ausführungen im urheberrechtlichen Teil in Kap. 3.7.1.

263 *Streitberger/Ruppel* 2009, 8.

264 Zu den serviceorientierten Architekturen siehe auch sogleich Kap. 2.3.6.7.

265 Zum Begriff und dessen Erläuterung siehe unten Kap. 2.4.1.2.2.

2.3.6.6 Application Service Providing (ASP)

Application Service Providing wird folgendermaßen definiert: „Die Zurverfügungstellung von Anwendungen, deren Funktionen und damit verbundenen Dienstleistungen über ein Netzwerk mit der Abrechnung der Software-Lizenz per effektiver Softwarenutzung (Pay as You Go)“.[266] Der Nutzer erhält vom Provider die Berechtigung auf Software im System des Providers zuzugreifen und diese zu nutzen.[267]

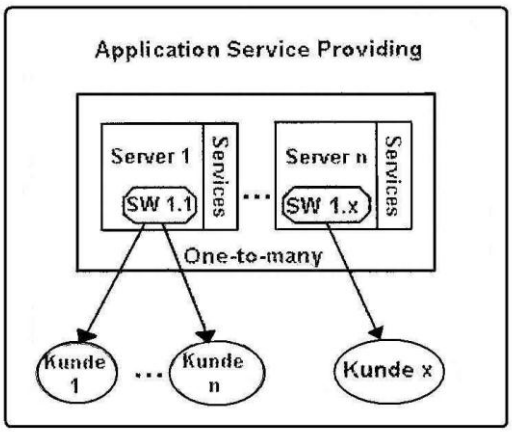

Abbildung 6: Beziehung zwischen Kunden und Anbietern bei ASP[268]

ASP ist eine Weiterentwicklung des klassischen Outsourcings und auch die Ähnlichkeiten zu Cloud Computing sind unverkennbar.[269] Insbesondere wird bei ASP bereits der One-to-Many-Ansatz verfolgt. Bei ASP teilen sich, wie bei Cloud Computing, mehrere Kunden den Gebrauch einer bestimmten Software und die IT-Infrastruktur des ASP-Anbieters. Dies hat zur Konsequenz, dass viele im Rahmen des ASP aufgetretene rechtliche Probleme und deren Lösungen auch für die rechtliche Bewertung des Cloud Computing weitergelten.[270]

Ebenfalls wie bei Cloud Computing liegen die Vorteile von ASP darin, dass die Kosten für die Softwarenutzung kalkulierbar werden, die Anschaffungskosten gesenkt werden können und es vermieden wird veraltete Software einzusetzen.

Oft werden und wurden zusätzliche Services zum eigentlichen ASP vereinbart, beispielsweise die Bereithaltung von Speicherplatz, die Sicherung und Pflege der Da-

---

266 *Röhrborn/Sinhart*, CR 2001, 69.

267 *Röhrborn/Sinhart*, CR 2001, 69.

268 Aus *Leonhard* 2009, 21; *Schmitt*, Software as a Service (SaaS), http://knol.google.com/k/software-as-a-service-saas?hl=de&lr=lang_en|lang_de.

269 *Söbbing*, MMR, 2008, Heft 5, XII; zu ASP als Weiterentwicklung siehe *Klimek*, K&R 2002, 633.

270 Siehe dazu beispielsweise *Röhrborn/Sinhart*, CR 2001, 70 ff.

ten des Nutzers (Dataproviding), die Erstellung und Pflege von Datenbanken (Datawarehousing) oder technische Unterstützung, Wartung und Hilfe (Support).[271]

Die Unterschiede zwischen ASP und Cloud Computing in Form von SaaS sind weitaus schwieriger zu differenzieren als die Unterschiede zwischen klassischem Outsourcing und Cloud Computing. Der wesentlichste Unterschied ist, dass sich ASP immer noch relativ individuelle Anpassungsmöglichkeiten der Software offen hält, während das SaaS-Konzept auf eine absolut homogene Dienstleistungspalette setzt.[272] Die Beziehung zwischen ASP-Anbietern und Kunden ist enger als bei Cloud Computing, jedoch loser als beim klassischen Outsourcing. Die Softwarebereitstellung bei ASP folgt demnach zwar dem One-to-Many-Ansatz, sie ist jedoch nicht stringent mehrmandantenfähig ausgelegt, wie bei SaaS. Trotz Nutzung einer gleichartigen Software beim ASP ist diese immer noch kundenspezifisch durch den Anbieter modifizierbar.

Zudem könnte die beim ASP-Provider genutzte Software ebenso gut inhouse auf den Servern des Kunden laufen, was bei SaaS nicht mehr möglich ist, da diese Art von Software für die Mehrmandantennutzung in virtualisierten Umgebungen und nicht für eine lokale Installation optimiert wurde. Die Implementierung und Nutzung der Möglichkeiten der Virtualisierung sind bei SaaS fortgeschrittener. ASP war somit mehr oder weniger die Remotenutzung einer Software, die genauso gut lokal beim Kunden hätte laufen können, während SaaS-optimierte Software für virtualisierte Umgebungen konzipiert ist und die lokal installierbare Software faktisch nur noch als Remotedienst nachbildet und darüber hinaus um netzwerkspezifische Merkmale ergänzt, die als lokale Software so überhaupt nicht umsetzbar wäre.

Ein weiterer Unterschied zwischen ASP und Cloud Computing ist der Umstand, dass beim ASP immer bekannt ist, wo die ausgelagerten Daten liegen, da der Anbieter eigene lokale Ressourcen speziell für die Software und Anwendungen der jeweiligen Kunden bereithält, während bei (Public) Cloud Computing für Außenstehende und Nutzer oft unklar ist, wo genau die Daten gespeichert oder verarbeitet werden.

Dem sogleich darzustellenden SoA-Paradigma folgend ist Software as a Service auch kleinteiliger und feingranularer ausgestaltet. Oft bildet eine Software nur einzelne Geschäftsprozesse ab (Business-Apps), die erst durch die Kombination mehrerer solcher „Apps“ eine zu einem herkömmlichen Softwarepaket, eben auch wie bei ASP, vergleichbare Funktionalität erhält. Im Gegensatz zu ASP ist also die Modifizierbarkeit und damit die kundenspezifische Nutzung nicht mehr durch den Anbieter durchzuführen, sondern der Nutzer sucht sich die passenden Apps aus und

---

271 *Röhrborn/Sinhart*, CR 2001, 70.

272 *Herold/Müller*, Cloud Computing und SaaS, http://knol.google.com/k/cloud-computing-und-saas.

kombiniert sie selbständig nach eigenen Bedürfnissen. Diese individuelle Zusammensetzung kann auch anbieterübergreifend erfolgen.

2.3.6.7 Verhältnis von Cloud Computing zu serviceorientierten Architekturen (SoA)

Serviceorientierte Architekturen und Cloud Computing sind zwei sich einander ergänzende, orthogonale Konzepte. Unternehmen, die SOA-Initiativen gestartet haben, werden Cloud Computing leichter nutzen können.[273] Cloud Computing nutzt die Fortschritte und Erfahrungen bei der Komposition, Choreographie und Orchestrierung von Webservices.[274] Die Architekturstrategie des Cloud Computing hat demzufolge eine serviceorientierte Basis im Sinne von SoA.[275]

Cloud-Computing-Systeme sind eher infrastrukturgetrieben, während serviceorientierte Architekturen vielmehr die Geschäftsprozesse im Fokus haben. Beiden ist jedoch gemein, dass sie auf den gleichen Technologien basieren und komplexe Systeme und Komponenten in Form einfacher Dienste kapseln.[276] Sie teilen außerdem die Idee der Wiederverwendbarkeit und Erweiterbarkeit dieser Dienste.[277] Durch serviceorientierte Architekturen sollen Programme und Schnittstellen wiederverwendet werden können, während Clouddienste möglichst von Anfang an breit aufzustellen sind, um einfach erweiterbar zu sein und damit eine gewisse Beständigkeit zu gewährleisten.[278] Diese Beständigkeit von Cloudumgebungen wird gerade auch durch die Implementierung des SoA-Paradigmas der Wiederverwendbarkeit erreicht und führt außerdem zur leichteren Nutzung von Cloudservices.

Auch die Fähigkeiten, Richtlinien (Policies) für Dienste definieren zu können und Änderungen an den Richtlinien verwalten zu können, sind in serviceorientierten Architekturen stark ausgeprägt. Ähnliche Werkzeuge müssen in Cloudumgebungen

---

[273] *Münzl/Przywara/Reti/Schäfer/Sondermann/Weber/Wilker* 2009, 12; *Ruppel*, Serviceorientierte Architekturen (SOA) und Cloud Computing, http://www.searchsecurity.de/themenbereiche/applikationssicherheit/web-application-security/articles/257175/index3.html; *Neumann*, Lazarus-Effekt: das Comeback von SOA, http://www.heise.de/newsticker/meldung/Lazarus-Effekt-das-Comeback-von-SOA-1133988.html.

[274] *Schuster/Reichl*, CR 2010, 39; ähnlich *Tietz/Blichmann/Hübsch*, Informatik Spektrum 2011, 346.

[275] *Neumann*, Lazarus-Effekt: das Comeback von SOA, http://www.heise.de/newsticker/meldung/Lazarus-Effekt-das-Comeback-von-SOA-1133988.html.

[276] *Ruppel*, Serviceorientierte Architekturen (SOA) und Cloud Computing, http://www.searchsecurity.de/themenbereiche/applikationssicherheit/web-application-security/articles/257175/index2.html.

[277] *Tietz/Blichmann/Hübsch*, Informatik Spektrum 2011, 346.

[278] *Ruppel*, Serviceorientierte Architekturen (SOA) und Cloud Computing, http://www.searchsecurity.de/themenbereiche/applikationssicherheit/web-application-security/articles/257175/index2.html.

erst entwickelt und in den Systemen verankert werden. Dabei kann auf die Erfahrungen in serviceorientierten Architekturen zurückgegriffen werden.[279]

2.3.7 Anwendungsbereiche, Anwendungsbeispiele und Einsatzszenarien

Um die anschließend darzustellenden Vor- und Nachteile in einen praktischen Kontext bringen zu können, bietet es sich an, vorab die praktischen Anwendungsfelder für Cloud Computing darzustellen.

Wie einleitend erwähnt, sind Cloudservices nicht völlig neu. Gerade im Privatanwenderbereich bestehen gewisse Services schon seit etlichen Jahren, wobei diese jedoch nicht als Cloudservices oder als Software as a Service bezeichnet wurden. Der Bereich der privaten Nutzung von Webdiensten war insoweit Vorreiter bei Cloud Computing, was nicht zuletzt in den kostenlosen oder werbefinanzierten Angeboten seine Ursache hat.[280]

2.3.7.1 Privatbereich

2.3.7.1.1 Mailservices

Die ältesten ausgelagerten Dienste dürften die kostenlosen Mailservices sein. E-Mailanbieter, wie zum Beispiel Hotmail, GMX, Web.de, Googlemail oder AOL, bieten die Speicherung auf ihren Systemen und den Webzugang mittels vorgefertigter Webseiten über jeden Internetzugang schon seit mehreren Jahren an. Diese über das Web verfügbaren Maildienste sind nichts anderes als Software as a Service. Die Webmailoberfläche bildet nämlich die lokal installierbaren Mailprogramme nach. Solche Mailprogramme, wie beispielsweise Outlook oder Thunderbird, sind für die Nutzung nicht mehr notwendig, können jedoch optional verwendet werden.

Was für Privatnutzer seit Jahren eine Selbstverständlichkeit ist, ist im Unternehmens- und Behördenumfeld eher die Ausnahme. Dort wurde dedizierte Hard- und Software, beispielsweise Microsofts Exchange Server, eingesetzt, die über weitere Funktionalitäten, zum Beispiel Groupwarefunktionen, verfügt. So erstaunt es auch nicht, dass zum Beispiel die Auslagerung der behördlich genutzten Mailservices der Stadt Los Angeles zu Googlemail eine Nachrichtenmeldung wert war.[281] Die damit verbundenen Einsparungen der Stadt sollen sich auf 5,5 Millionen US-Dollar über fünf Jahre belaufen.[282]

---

[279] *Ruppel*, Serviceorientierte Architekturen (SOA) und Cloud Computing, http://www.searchsecurity.de/themenbereiche/applikationssicherheit/web-application-security/articles/257175/index3.html.

[280] *Kurz*, Netzwoche 17/2008, 34.

[281] *Posdziech*, Los Angeles' Verwaltung setzt auf Google Mail, http://www.onlinekosten.de/news/artikel/36604/0/Los-Angeles-Verwaltung-setzt-auf-Google-Mail.

[282] *Williams*, Los Angeles City Council Approves Google E-Mail Plan, http://www.govtech.com/pcio/Los-Angeles-City-Council.html.

2.3.7.1.2 Fotodienste und Webalben

Zweitältester Anwendungsbereich dürften Webalben, wie zum Beispiel Flickr, oder bloße Bildhoster, wie Imageshack oder Imagevenue, sein. Anstatt seine digitale Fotosammlung wie früher nur auf Datenträgern zu speichern, lädt man die Digitalfotos zu spezialisierten Anbietern hoch, die die Bilder hosten und oft auch Zusatzdienstleistungen anbieten. Beispiele sind die Onlinebildbearbeitung und das „Entwickeln" der Digitalbilder zu realen Fotos gegen geringes Entgelt. Erfolgsfaktor der Bilderdienste war allerdings der Aspekt der Veröffentlichung im Web und die damit verbundene einfache Möglichkeit, Fotos jedermann oder auch nur bestimmten Personen zeigen zu können.

2.3.7.1.3 Filehosting und Storage

Ebenfalls als Cloud Computing ist das Filehosting bei sogenannten „One-Click-Hostern" oder Sharehostern anzusehen. Diese unterfallen dem Infrastrukturbereich (IaaS), genauer dem Storage-as-a-Service-Modell.[283] Die oben erwähnten Imagehoster sind übrigens als „Filehoster für Bilddateien" auch in die Filehostingkategorie einordenbar.

Bekannteste Anbieter sind Rapidshare, Megaupload oder Upload.to. Bei diesen weltweit aufgestellten Anbietern wird das Problem der „Wolke" besonders deutlich. Allenfalls der Hostingbetreiber kann durch Logs und Protokolle nachvollziehen wo genau und wann welche Datei gespeichert ist oder war. Mittels Load Balancing werden die Daten verteilt, so dass die Infrastruktur optimal ausgenutzt wird. Deshalb ist es auch oft unmöglich im Voraus vorherzusagen, wo genau die Daten gespeichert werden. Allenfalls eine manuelle Begrenzung auf bestimmte Server oder Regionen kann diese zufällige und weltweite Verteilung der Daten eingrenzen.

Juristisch war dies insofern ein Problem, weil die Anbieter ihren Sitz in zwielichtige Kleinststaaten verlegten und somit über das Sitzlandprinzip praktisch nicht greifbar waren. Die Anknüpfung an die Serverstandorte durch das Territorialitätsprinzip scheiterte gerade an dieser fehlenden örtlichen Transparenz der Speicherung. In Deutschland wurde aber durch das OLG Düsseldorf die Haftung der Hostinganbieter als Störer für die illegalen Handlungen der Nutzer verneint.[284] Einige Oberlandesgerichte urteilten zuvor differenzierter und waren der Ansicht, dass nur bei Kenntnis des unberechtigten Uploads urheberechtlich geschützter Dateien ein Sharehoster verpflichtet sei, die Dateien unverzüglich zu löschen, jedoch nicht zum

---

[283] Neben „Storage-as-a-Service" auch als „Data-Storage-as-a-Service" bezeichnet; so beispielsweise *Martens/Teuteberg/Gräuler*, HMD – Praxis der Wirtschaftsinformatik, Heft 275, 2010, 53.

[284] *Briegleb*, OLG Düsseldorf: Rapidshare haftet nicht für Urheberrechtsverletzungen, http://www.heise.de/newsticker/meldung/OLG-Duesseldorf-Rapidshare-haftet-nicht-fuer-Urheberrechtsverletzungen-992144.html.

Einsatz von Wortfiltern greifen müsse.[285] Im Gegensatz zum OLG Düsseldorf waren diese Gerichte der Ansicht, dass die Sharehoster die Uploads nach bekannten urheberrechtlich geschützten Dateien filtern müssten, um überhaupt die Möglichkeit der Kenntnisnahme zu haben.

Filehosting kann auch dazu dienen, Backups in der Cloud vorzuhalten. Solche Daten richten sich dann allerdings nicht an die Öffentlichkeit, sondern sind im Gegenteil, in der Regel verschlüsselt und, soweit der Filehoster dies ermöglicht, auch nur für den konkreten Nutzer zugänglich.

Storageanbieter, wie Amazons S3, sind auch von Privatleuten nutzbar, wobei diese Form der Nutzung wegen der eher komplizierten Bedienung noch eher selten ist. Es gibt allerdings Anbieter, die auf S3 aufsetzen und eine einfachere Benutzeroberfläche anbieten. Im Prinzip ist dies eine Erleichterung der Nutzung eines Infrastrukturservices durch vereinfachte SaaS-Oberflächen. Ein Beispiel hierfür wäre der Storageanbieter Dropbox, der in der Basisversion kostenlos genutzt werden kann.[286] Neben dem reinen S3-Service bietet Amazon auch das sogenannte „Cloud Drive“, einen Onlinespeicher für Mediendateien. Dieser bietet eine einfache Weboberfläche zur Verwaltung der Daten und die weitergehende Möglichkeit, diese Daten über Mobiltelefone mittels einer App abzurufen und zu streamen.[287]

2.3.7.1.4 Spiele (Cloud Gaming)

Cloud Computing ist in Form des Cloud Gaming gerade dabei, den Spielemarkt zu revolutionieren.[288] Dienste wie OnLive[289], Otoy[290] oder Gaikai[291] bieten die Möglichkeit Spiele nicht mehr lokal installiert zu spielen, sondern direkt aus und in der Cloud als Dienst, also als sogenannte „Cloud Games“.

Cloud Gaming funktioniert dergestalt, dass das Computerspiel auf den Servern des Cloud-Gaming-Anbieters ausgeführt wird und die Ausgabe komprimiert als Livestream an den Spieler über das Internet ausgeliefert wird. In der Gegenrichtung werden die Eingabe- und Steuerungsbefehle des Nutzers an den Gamingserver in der

---

285 OLG Köln, Az. 6 U 86/07, http://medien-internet-und-recht.de/volltext.php?mir_dok_id=1388; *Ermert*, Gericht schränkt Prüfpflichten für RapidShare ein, http://www.heise.de/newsticker/meldung/Gericht-schraenkt-Pruefpflichten-fuer-RapidShare-ein-177999.html; OLG Hamburg, Az. 5 U 73/07, *Heidrich*, OLG Hamburg: RapidShare haftet als Mitstörer für Urheberrechtsverletzungen, http://www.heise.de/newsticker/meldung/OLG-Hamburg-RapidShare-haftet-als-Mitstoerer-fuer-Urheberrechtsverletzungen-Update-209949.html.

286 http://www.dropbox.com.

287 https://www.amazon.com/clouddrive/learnmore.

288 *Austinat/Fechteler/Gieselmann*, c’t 21/2010, 76; *Gieselmann*, Interview: Otoy streamt Cloud Games und Hollywood-Effekte, http://www.heise.de/newsticker/meldung/Interview-Otoy-streamt-Cloud-Games-und-Hollywood-Effekte-1102483.html.

289 http://www.onlive.com.

290 http://www.otoy.com.

291 http://www.gaikai.com.

Cloud übermittelt. Das Spielerlebnis ist also von einer performanten Internetverbindung abhängig. Diese muss zum einen genug Bandbreite haben, um den Stream übertragen zu können, und möglichst geringe Latenzen hinsichtlich der Paketlaufzeiten aufweisen, um eine Echtzeitsteuerung zu gewährleisten. Die Bandbreite ist abhängig von der Auflösung, den genutzten Kompressionsalgorithmen und der Qualität des Streams. Bei OnLive sollte die Internetverbindung mindestens 6 MBit/s liefern und möglichst nicht 80 Millisekunden bei den Paketlaufzeiten vom Kunden-PC zum Spieleserver unterschreiten.[292] Die Anforderungen an die Laufzeiten der Pakete sind für die diversen Spielgenres unterschiedlich. Während beispielsweise 3D-Shooter und Rennspiele angesichts der innewohnenden Dynamik so geringe Latenzen wie möglich (maximal 80 - 100 ms) erfordern, sind beispielsweise Strategiespiele auch mit Latenzen von 1 bis 2 Sekunden (entspricht 1000 - 2000 ms) spielbar.[293]

Die Bereitstellungsmöglichkeit in der Cloud hat gewisse Vorteile. Der Nutzer braucht nicht mehr in regelmäßigen Abständen seine Hardware zu aktualisieren. Bisher war es üblich, mit jeder neuen Spielegeneration die Hardwareanforderungen hochzuschrauben. Um aktuelle Spiele flüssig und in annehmbarer Qualität spielen zu können, benötigte man eine zeitgemäße Grafikkarte (GPU) und einen möglichst neuen Prozessor (CPU). Bei Spielkonsolen galt und gilt übrigens das gleiche Prinzip, jedoch mit weniger Aktualisierungsphasen, da hierbei die Konsole komplett aktualisiert werden muss, während Personal Computer modular aufgerüstet werden können. Dieser Zwang zum stetigen Aufrüsten entfällt mit Cloud Gaming. Der Computer des Nutzers muss lediglich in der Lage sein, den Stream adäquat darstellen zu können, was nur vergleichsweise geringe Hardwareausstattungen beim Nutzer voraussetzt.

Der zweite Vorteil liegt in der Möglichkeit, neuartige Spiele in einer solchen Qualität und Komplexität anzubieten, die niemals auf einem Einzelrechner-PC laufen würden, da die Hardwareanforderungen zu hoch wären und einen leistungsfähigen Server voraussetzen. Solche Spiele werden künftig gerade für den Einsatz auf skalierbaren Cloudservern entwickelt werden.[294] Während heutige Spieleentwickler immer an die Leistungsfähigkeit der gegenwärtig verfügbaren PC-Hardware gebunden sind, gilt diese Begrenzung für Cloudspiele nicht mehr. Clouds sind, wie schon erwähnt, nach oben skalierbar.

Ein weiterer potentieller Vorteil liegt in der Bezahlung der Nutzung durch den Kunden. Die Ausgestaltung ist dabei noch flexibler als bei herkömmlichen Spielen. Neben der Abrechnung der tatsächlichen Nutzungszeit eines Spiels oder Teilen ei-

---

[292] *Austinat/Fechteler/Gieselmann*, c't 21/2010, 77, 80.
[293] *Austinat/Fechteler/Gieselmann*, c't 21/2010, 76, 77.
[294] *Austinat/Fechteler/Gieselmann*, c't 21/2010, 83.

nes Spiels, sind auch Flatrates oder sonstige Bezahlmodalitäten für gewisse Spiele möglich.

2.3.7.1.5 Weitere Dienste

Die Ausnutzung der enormen Rechenleistung und Skalierbarkeit einer Cloud sind auch für cloudbasierte Antivirenlösungen oder Spracherkennungsservices von Vorteil.[295]

Antivirenlösungen halten Virensignaturen zentral vor, so dass die lokale Installation einer Antivirensoftware entbehrlich ist. Zudem ist eine solche gemeinschaftsbasierte Echtzeitsammlung zirkulierender Malware immer aktueller als lokale Signaturen, die immer nur in Intervallen aktualisiert werden können. Der Nachteil ist, dass ohne Verbindung zum Internet auch kein Virenscanning möglich ist.

Cloudbasierte Spracherkennung bietet die Möglichkeit auch mit leistungsschwachen Geräten solche Funktionalitäten zu nutzen. So ist es bereits möglich, Sprache mittels Smartphone aufzuzeichnen, diese komprimiert an einen entsprechenden Dienstleister, beispielsweise Nuance,[296] zu schicken und die Auswertung auf dessen leistungsstarken Servern durchführen zu lassen. Das Ergebnis wird dem Kunden dann umgehend als Text zugeschickt. Wegen der geringen Reaktionszeit ergibt sich für den Nutzer der Eindruck, dass das genutzte Mobilgerät die Spracherkennungsfunktionalität bietet.[297] Noch beeindruckender ist die über Cloudservices in Echtzeit durchgeführte Sprachübersetzung, beispielsweise mit der Android-App „Talk to me Cloud“, die die Übersetzung nicht als Text, sondern wieder als Sprache ausgibt (sogenannte „Realtime Speech-to-Speech Translation“).[298] Auch die mit dem iPhone 4S nutzbare Spracherkennungssoftware „Siri“ funktioniert überwiegend cloudbasiert.[299]

Diese Services sind prinzipiell auch in sonstigen Bereichen, also Unternehmen oder Behörden einsetzbar, jedoch sind die aktuellen Dienste primär für Privatnutzer aus-

---

[295] *Weidemann*, Einsatzbeispiele zu Cloud Computing 1+2, http://www.pcwelt.de/ratgeber/Verschiedene-Einsatzbeispiele-zu-Cloud-Computing-Ratgeber-Internet-1124745.html; *Probst*, DSB 2009, Heft 7-8, 21; *Kalkuhl*, Clear skies ahead: cloud computing and in-the-cloud security, http://www.securelist.com/en/analysis?pubid=204792059; *Klatte*, <kes> Special - Sicheres Cloud Computing, März 2011, 18.

[296] http://www.nuance.com; *Skrbina*, Cloud computing – the secret weapon that enables massively scalable speech applications, http://community.nuance.com/blogs/expertsblog/archive/2009/12/09/cloud-computing-the-secret-weapon-that-enables-massively-scalable-speech-applications.aspx.

[297] *Weidemann*, Einsatzbeispiele zu Cloud Computing 1+2, http://www.pcwelt.de/ratgeber/Verschiedene-Einsatzbeispiele-zu-Cloud-Computing-Ratgeber-Internet-1124745.html.

[298] http://www.flaviuapps.com.

[299] *Kremp*, Mit diesem Handy wird man sprechen, http://www.spiegel.de/netzwelt/gadgets/0,1518,790986,00.html.

gestaltet. Neuerdings werden sogar in Schulen Clouddienste, meist unter dem Aspekt der Zusammenarbeit (Collaboration), eingesetzt.[300]

2.3.7.2 Unternehmensbereich

2.3.7.2.1 Startupunternehmen

Gerade neu gegründete Unternehmen benötigen innerhalb kurzer Zeit unkomplizierte und zuverlässige IT-Infrastruktur zur Umsetzung ihrer eigentlichen Geschäftsidee. Skalierbarkeit und Flexibilität sind bei solchen Unternehmen besonders von Bedeutung, da diese nicht selten schnell wachsen, so dass auch die Unternehmens-IT mit diesem Wachstum mithalten muss. Sei es weil die Informationstechnologie Teil der Geschäftsidee ist, beispielsweise bei Webshops oder Social Communities, oder weil sie Hilfsfunktionen zur Bewältigung der anfallenden Arbeiten bietet, zum Beispiel CRM- oder Collaborationlösungen.[301] Außerdem erspart sich ein Startup mit der Nutzung von Cloudservices hohe Investitionen in Hard- und Software, so dass das ersparte Kapital in die eigentlichen Kernaufgaben des Unternehmens fließen kann. Zu weiteren Vorteilen wird auf die Darstellung des Vorteils „Kostenersparnis“ verwiesen.[302]

2.3.7.2.2 Unternehmen mit bestehender Infrastruktur

Hauptanwendungsfälle des Cloud Computing für Unternehmen mit bestehender Infrastruktur sind zum einen das Abfedern von Lastspitzen durch Nutzung einer oder mehrerer Public Clouds und die Umwandlung der vorhandenen Ressourcen zu einer Private oder Community Cloud.

Anstatt die eigenen Server aufzurüsten, mieten die Unternehmen für Zeiten erhöhten Bedarfs Kapazitäten bei Cloudanbietern hinzu. Die zweite Anwendungsalternative ist das Zusammenführen der bisher getrennten Unternehmens- oder Konzerninfrastruktur und der verteilten Ressourcen in eine Private Cloud. Dadurch lassen sich diese Ressourcen besser ausnutzen und skalieren besser. Mit der Zusammenführung in einer Private Cloud geht gleichzeitig die Einführung von Virtualisierungstechniken einher, soweit solche nicht bereits vorher schon verwendet wird.

Für die praktische Umsetzung kann auf das Know-how von bestehenden Public Cloud Anbietern zurückgegriffen werden, indem diese ihre Cloudsoftware für den kleineren Einsatz in einer Private Cloud zum Kauf anbieten. Außerdem kann auch kostenlose und speziell vorgefertigte Open-Source-Software genutzt werden. Ein Beispiel für ersteres ist Microsofts Azure für Private Clouds, die sogenannte

---

[300] *Ondreka*, Lernen über die Wolken, http://www.taz.de/Datenclouds-an-Schulen/!75203.

[301] *Reti/Pauly* 2009, 14; *Böken*, iX 04/2011, 115.

[302] Siehe Kap. 2.4.1.1.1.

„Windows Azure Platform Appliance“.[303] Die bekannteste Open-Source-Software für den Aufbau einer Private Cloud ist „Eucalyptus“.[304] Der Name „Eucalyptus” ist dabei ein Akronym für “Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems”. Neben der kostenlosen Open-Source-Version gibt es eine in der Funktionalität erweiterte kostenpflichtige „Enterprise Edition“.[305] Eine weitere, im Jahr 2010 gestartete, Initiative namens „OpenStack“ hat die Bereitstellung von kostenloser Open-Source-Software und die Etablierung offener Standards zum Ziel.[306]

2.3.7.2.3 Konkrete Anwendungsbereiche in Unternehmen

In Unternehmen werden zum Teil die schon für den Privatbereich vorgestellten Dienste genutzt, zum Beispiel Mailservices oder herkömmliche Anwendungssoftware als Service, insbesondere Office- und Textverarbeitungssoftware, jedoch hauptsächlich unternehmensspezifische Software-as-a-Service-Dienstleistungen. Erwähnt seien das Kundenbeziehungsmanagement (CRM), Enterprise Resource Planning (ERP), also die Planung, wie Unternehmensressourcen eingesetzt und verwendet werden sollen, oder Software für das Lieferkettenmanagement[307] (Supply Chain Management). Einige Cloud- und SaaS-Anbieter, wie zum Beispiel Salesforce, haben sich auf die Bereitstellung von solcher Geschäftssoftware spezialisiert.

Mit dem im Privatbereich üblichen File- oder Imagehosting ist in Unternehmen die Datensicherung mittels Backups bei professionellen Anbietern vergleichbar.[308] Gerade Cloud Computing bietet neue Möglichkeiten die in Unternehmen massiv anfallenden Sicherungsdaten zu managen.[309]

Ein vergleichsweise neues Anwendungsfeld für Clouddienste tut sich im Automobilbereich auf. Fahrzeughersteller nutzen Cloudservices sowohl für die Fahrzeugproduktion als auch für den späteren Einsatz von IT im Fahrzeug. Während ersteres Daten und Berechnungen im Bereich Forschung, Fahrzeugentwicklung und Fahr-

---

303 http://www.microsoft.com/windowsazure/appliance.

304 http://www.eucalyptus.com.

305 *Eucalyptus*, On-premise and Hybrid Cloud Infrastructure as a Service, http://www.eucalyptus.com/products/eee.

306 http://www.openstack.org, *Kirsch*, Open-Source-Software für die Cloud, http://www.heise.de/newsticker/meldung/Open-Source-Software-fuer-die-Cloud-1040964.html.

307 Welche konkreten Vorteile sich durch cloudbasiertes SCM ergeben und welche Funktionen dabei cloudbasiert genutzt werden können, kann man bei *Grohmann*, JDA Software: Cloud-Computing eröffnet Herstellern neue Zugangsmöglichkeiten zum Supply Chain Management, http://www.cloud-computing-report.de/jda-software-cloud-computing-eroeffnet-herstellern-neue-zugangsmoeglichkeiten-zum-supply-chain-management/07-09-2010 nachlesen.

308 Siehe dazu oben beispielsweise Rackspace, GoGrid oder Linode; in Deutschland sind 1&1 oder Host Europe bekannte Cloudhoster.

309 Siehe hierzu beispielsweise *Gheri*, <kes> Special - Sicheres Cloud Computing, März 2011, 36 ff.

zeugherstellung betrifft, ist der Bereich „IT im Auto“ meist mit dem Infotainment der Fahrzeuginsassen oder der Verkehrstelematik verbunden.[310] Auch im Maschinenbau oder für CAD gewinnt Cloud Computing unter den Aspekten Forschung, Entwicklung, Design und Simulation immer größere Bedeutung.[311] Mittlerweile gibt es sogar deutsche Cloudanbieter, die sich auf die Bereitstellung von Rechenleistung für solche rechenintensive Anwendungsfelder spezialisiert haben.[312]

Andere kommerzielle Anwendungsbereiche finden sich in der Pharmaindustrie, aber auch in der Landwirtschaft oder der Logistik.[313] Im Laufe der Zeit wird Cloud Computing auf irgendeine Art und Weise für jedes Unternehmen Bedeutung erlangen.

2.3.7.3 Behörden und öffentliche Verwaltung

Ähnlich wie Unternehmen, können sich auch Behörden durch Nutzung von Cloudservices auf ihre eigentliche Behördentätigkeit konzentrieren. Allerdings stehen im öffentlichen Sektor die Störungen der Arbeitsabläufe und die Notwendigkeit von Investitionen nicht so im Vordergrund wie bei privatwirtschaftlichen Unternehmen. Zukunftspotential haben insbesondere Shared Services Center. Diese ermöglichen die Konsolidierung und Zentralisierung von Dienstleistungsprozessen einer Organisation, zum Beispiel einer Behörde. Dabei werden gleichartige Prozesse aus verschiedenen Bereichen einer Organisation zusammengefasst und von einer zentralen Stelle, nämlich dem Shared Services Center, erbracht.[314] Die gemeinsame Nutzung beschränkt sich meist auf die gemeinsame Speicherung von Daten mehrerer Behörden in einem einzigen Rechenzentrum oder die gemeinsame Nutzung von Datenbanken, so dass diese meist ohne die Ausnutzung der Vorteile der Cloudtechnologie funktionieren.

---

310 *Kaiser*, <kes> Special - Sicheres Cloud Computing, März 2011, 28 ff.

311 *Arrelano*, Autodesk U: CAD software company eyes the cloud, http://www.itworldcanada.com/news/autodesk-u-cad-software-company-eyes-the-cloud/108412.

312 http://cloudnumbers.com bietet die Möglichkeit HPC-Cluster als Cloud zusammenzustellen und zu nutzen.

313 *Handelsblatt*, Mit Cloud Computing gegen Krebs und Alzheimer, http://www.handelsblatt.com/technologie/it-tk/special-cloud-computing/mit-cloud-computing-gegen-krebs-und-alzheimer/4289308.html; *Proplanta*, Cloud Computing für die Landwirtschaft: Neue Anwendungen werden erforscht, http://www.proplanta.de/Agrar-Nachrichten/IT-Medien/Cloud-Computing-fuer-die-Landwirtschaft-Neue-Anwendungen-werden-erforscht_article1304883406.html; http://www.ccl.fraunhofer.de.

314 http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Technologie-und-Innovation/aktionsprogramm-cloud-computing,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf, S. 19; das Prinzip der Shared Services Center wird auch als „internes Outsourcing“ bezeichnet; *Maurer*, http://www.controllingportal.de/Fachinfo/Sonstiges/Shared-Service-Center.html.

Shared Services durch Cloud Computing sollen Vorteile bei den Kosten, in der Qualität der Leistungserbringung, bei der Dienstleistungsorientierung und der IT-Sicherheit ermöglichen.[315] Künftig könnte mit Cloud Computing, vorerst wahrscheinlich in Form von Private oder Community Clouds, die gesamte IT aus der Wolke kommen, wobei insbesondere die gemeinsame Nutzung zentralisierter Datenbestände leichter möglich wird.[316]

2.3.8 Ausgewählte Cloudprovider

Um die hohe wirtschaftliche Bedeutung zu verdeutlichen, die dadurch auch Einfluss auf das Gewicht der Rechtsfragen hat, wird im Folgenden die Markt- und Angebotslage bis zum Jahr 2012 mit den wichtigsten Cloudprovidern dargestellt. Es ist eine Auswahl ohne Anspruch auf Vollständigkeit. Unzählige kleinere Provider blieben dabei unberücksichtigt. Zudem kommen fortwährend neue Cloudanbieter hinzu. Unternehmen mit erheblichen Rechencenterkapazitäten, dem notwendigen Know-how und einer großen Kundenbasis können faktisch „aus dem Nichts“ zu größeren Anbietern auf dem Cloudmarkt aufsteigen. Bestes Beispiel hierfür sind Microsofts vergleichsweise kurzfristige und erfolgreiche Anstrengungen der Etablierung der Windows-Azure-Cloud.[317] Ähnlich schnelle Entwicklungen und Marktetablierungen sind für IBM oder Oracle, nicht zuletzt durch die Übernahme von Sun Microsystems, zu erwarten.[318]

Eine Übersicht der Leistungen der vier größten Cloudanbieter bietet die sogenannte „CloudMatrix“, ein graphisch aufbereiteter und interaktiver Service von T-Systems-Mitarbeitern.[319] Dieser erlaubt einen direkten Vergleich der jeweiligen Provider in verschiedenen Sparten, zum Beispiel Funktionsumfang, Performance, Sicherheitsniveau, Supportleistungen und anfallende Kosten. Zielsetzung des Angebots ist die Vereinfachung der Providerauswahl für Unternehmensentscheider und zukünftige Nutzer.[320]

---

315 *Bundesministerium für Wirtschaft und Technologie*, Aktionsprogramm Cloud Computing, http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Technologie-und-Innovation/aktionsprogramm-cloud-computing,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf, S. 19; die Zentralisierung durch „Verwaltungsclouds“ soll Einsparungen in Höhe von bis zu drei Milliarden Euro ermöglichen; siehe dazu *Krüger*, Datenwolke gegen virtuelle Kleinstaaterei, http://www.heute.de/ZDFheute/inhalt/6/0,3672,8241158,00.html.

316 Der gleichen Ansicht sind *Deussen/Strick/Peters*, 2010, iv, 22 und *Cattedu* 2010, 7.

317 Näheres dazu siehe weiter unten in Kap. 2.3.8.4.

318 Zu ersten Clouddiensten beider Unternehmen siehe http://cloud.oracle.com und http://www.ibm.com/cloud-computing.

319 http://www.thecloudmatrix.org.

320 http://www.thecloudmatrix.org.

2.3.8.1 Amazon

Amazon war der Pionier bei der Bereitstellung von Clouddienstleistungen.[321] Die Angebote von Amazon werden stetig ausgebaut, wobei es nicht nur neue Cloudservices gibt, sondern auch Webserviceangebote anderer Art, die jedoch in die unternehmenseigenen Cloudangebote integriert sind.[322] Das Leistungsangebot von Amazon, quasi vom Onlinebuchhändler bis hin zum Cloudprovider, hat sich im Laufe der Jahre stark verändert und erweitert.[323] Einen Überblick über die diversen Web- und Cloudservices bietet die folgende Grafik.

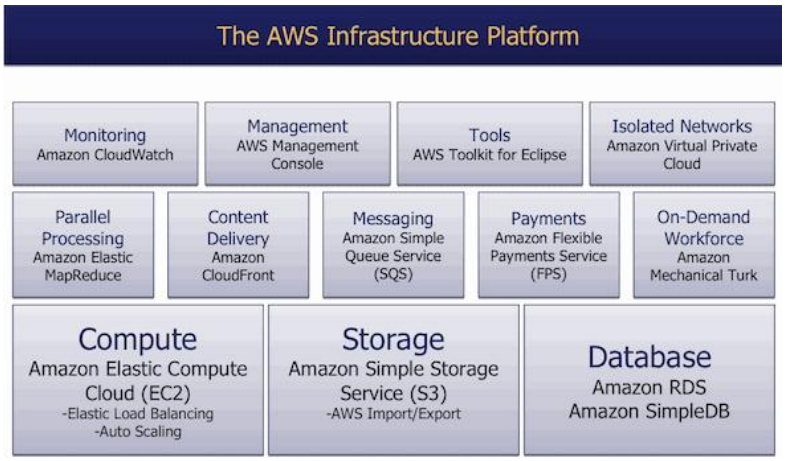

Abbildung 7: Übersicht über Amazons Web- und Cloudservices[324]

Auch die spezifischen Cloudangebote werden mit immer neueren Optionen und Angeboten erweitert. So können Kunden zwischen neun Betriebssystemen auswählen. Auch preislich werden die Angebote immer günstiger. Bei der Abrechnung wird zwischen vier Nutzungsmodellen unterschieden. Es gibt „On-Demand Instances“, die dem klassischen Pay-per-Use-Gedanken folgen, „Reserved Instances“, die als Prepaidangebot und wie der Name sagt, mit einer Reservierungsmöglichkeit von Rechen-, Speicher-, oder sonstigen Leistungen verbunden sind und die „Spot Instances“, die das Ersteigern von ungenutzten Kapazitäten für eine gewisse Zeit erlauben.[325] Durch Letztere lassen sich für den Kunden im Vergleich zu den beiden „regulären“ Angeboten Kosten sparen, während Amazon seine Hardwareinfrastruk-

---

321 Siehe dazu auch noch einmal Kap. 2.3.6.

322 Hierzu zählt beispielsweise auch das in Kap. 2.3.1.4 erwähnte Crowdsourcing mittels „Amazon Mechanical Turk“.

323 *Weiner/Renner/Kett* 2010, 98.

324 http://aws.amazon.com.

325 *Amazon*, EC2-Funktionen, http://aws.amazon.com/ec2/#features; *Amazon*, EC2 Spot Instances, http://aws.amazon.com/ec2/spot-instances; zu den „Reserved Instances” siehe auch Fn. 138.

tur optimal auslastet. Seit September 2010 gibt es zudem die sogenannten „Micro Instances“.

Um ein Gefühl für die Preise zu bekommen, sollen diese exemplarisch für Amazon in der folgenden Grafik dargestellt werden. Die Preise gelten für „On-Demand Instances“ in Europa im Herbst 2010.

EU – Irland

Standard On-Demand Instances	Linux/UNIX-Nutzung	Windows-Nutzung
Small (Vorgabe)	0,095 USD pro Stunde	0,12 USD pro Stunde
Large	0,38 USD pro Stunde	0,48 USD pro Stunde
Extra Large	0,76 USD pro Stunde	0,96 USD pro Stunde
High-Memory On-Demand Instances		
Extra Large	0,57 USD pro Stunde	0,62 USD pro Stunde
Double Extra Large	1,34 USD pro Stunde	1,44 USD pro Stunde
Quadruple Extra Large	2,68 USD pro Stunde	2,88 USD pro Stunde
High-CPU On-Demand Instances		
Medium	0,19 USD pro Stunde	0,29 USD pro Stunde
Extra Large	0,76 USD pro Stunde	1,16 USD pro Stunde

Abbildung 8: Beispiel für die Preisgestaltung eines Cloudangebots[326]

Billiger sind die später hinzugekommenen Mikroinstanzen („Micro Instances“). Während die bis dahin kleinste EC2-Instanz „Small“ mit Linux für 9,5 US-Cent pro Stunde in der EU genutzt werden kann, fallen für die Mikroinstanz nur 2 US-Cent pro Stunde an. Unter Windows sind es 3 US-Cent statt 12. Damit ist eine Mikroinstanz, die dauerhaft läuft, bereits für knapp 15 US-Dollar im Monat mit Linux und für rund 22 US-Dollar mit Windows zu haben.[327]

Um Entwicklern die Möglichkeit zu geben, mit Cloudanwendungen innerhalb von EC2 zu experimentieren, bietet Amazon zu diesem Zweck seit Anfang November 2010 ein kostenloses Angebot. Dieses gilt innerhalb gewisser Nutzungsgrenzen für ein Jahr und beinhaltet eine EC2-Mikroinstanz.[328] Näheres zu den Nutzungskonditi-

---

326 *Amazon*, EC2-Preise, http://aws.amazon.com/de/ec2/pricing.

327 *Ihlenfeld*, Mikroinstanzen zum kleinen Preis, http://www.golem.de/1009/77826.html; *Barr*, New Amazon EC2 Micro Instances - New, Low Cost Option for Low Throughput Applications, http://aws.typepad.com/aws/2010/09/new-amazon-ec2-micro-instances.html.

328 *Amazon*, Kostenloses Nutzungskontingent für AWS, http://aws.amazon.com/free; *Diercks*, Amazon bietet kostenlose Cloud-Instanz an, http://www.heise.de/newsticker/meldung/Amazon-bietet-kostenlose-Cloud-Instanz-an-1123577.html.

onen und den Leistungen im Detail findet sich auf der Webseite der Amazon Web Services.[329]

Weitere „Service Highlights“ beinhalten die typischen Cloudeigenschaften. Zu erwähnen wäre die Elastizität, komplette Kontrolle durch den Kunden, Flexibilität, größtmögliche Zuverlässigkeit und Verfügbarkeit.[330]

Eine Besonderheit, die der Rechtslage, aber auch den Latenzen bei den Paketlaufzeiten geschuldet ist, ist die Auswahlmöglichkeit zwischen mehreren physischen Standorten, an denen die Daten gespeichert und verarbeitet werden. So gibt es mehrere, voneinander unabhängige, sogenannte „Verfügbarkeitszonen“ (Availability Zones) in sieben Regionen mit Rechenzentren in Nord-Virginia für die US-Ostküste, in Oregon und Kalifornien für die US-Westküste, in Irland für Europa, in Tokio und Singapur für den asiatischen Raum und in Sao Paolo für Südamerika.[331] Außerdem existiert die sogenannte „AWS GovCloud“ für US-Behörden, deren Rechenzentren sich ebenfalls physisch in den USA befinden.[332]

Fehler und Ausfälle einer Zone tangieren dabei nicht die Funktionsfähigkeit und Verfügbarkeit der anderen Verfügbarkeitszonen.[333] In seinen SLAs garantiert Amazon eine Verfügbarkeit von 99,95% für die jeweilige Zone.[334] Mit der Verfügbarkeitszone in Irland ist eine strikt europäische Cloud einrichtbar, um den rechtlichen Einschränkungen im europäischen Datenschutzrecht hinsichtlich der Datenübermittlung und Speicherung gerecht zu werden.

Die Marktführerschaft Amazons äußert sich auch in der Adaption der Elastic Compute Cloud durch Dritte und der Kompatibilität zu dieser. Man kann mittlerweile davon ausgehen, dass sich die Amazon Web Services für Cloud Computing als ein De-Facto-Standard etabliert haben. So hat zum Beispiel der deutsche Cloud-Computing-Anbieter ScaleUp Technologies[335] die Amazon S3 API[336] vollständig adaptiert. Zudem gibt es mit der oben genannten Eucalyptus-Open-Source-Software oder der Ubuntu Enterprise Cloud „Klone“ von EC2, mit denen eine Private Cloud nach dem Muster von EC2 aufgebaut werden kann. Für Eucalyptus gibt es die so-

---

329 *Amazon*, Kostenloses Nutzungskontingent für AWS, http://aws.amazon.com/free.

330 *Amazon*, EC2-Servicemerkmale, http://aws.amazon.com/ec2/#highlights.

331 *Amazon*, EC2 – Funktionen, http://aws.amazon.com/de/ec2/#features.

332 Nach Vorgaben der US-Bundesregierung darf der Zugriff auf Daten in der GovCloud nur aus den USA möglich sein; siehe dazu *Amazon*, AWS GovCloud (US), http://aws.amazon.com/de/govcloud-us und die weiteren Ausführungen in Kap. 2.3.10.

333 *Amazon*, EC2 – Funktionen, http://aws.amazon.com/de/ec2/#features.

334 Rein rechnerisch dürfen somit die konsequenzlosen Ausfallzeiten pro Jahr maximal 4,38 Stunden, pro Monat 21,56 Minuten und pro Woche lediglich 5,04 Minuten betragen.

335 http://www.scaleup.it.

336 API steht für „Application Programming Interface“ und erlaubt es Softwareentwicklern, Anwendungen zu schreiben und dabei bereits vorhandene, standardisierte Bibliotheksroutinen zu nutzen; so *Kratz*, API, http://www.heinz-kratz.de/edilex/a.html.

genannten Euca2ools[337] als direkte EC2-API-Adaption. Berücksichtigt man zudem die Liste der sogenannten „AWS Solution Provider“,[338] so erkennt man schon an der reinen Anzahl dieser Provider die Bedeutung der Amazon Web Services.[339]

Weitere Cloudprojekte Amazons sind „Elastic Beanstalk“, ein kostenloses PaaS-Angebot im Betastatus, und die Möglichkeit die Amazoncloudinfrastruktur für den Mailversand zu nutzen.[340] Im Frühjahr 2011 ist zudem die Möglichkeit für Privatnutzer hinzugekommen, ihre Mediensammlung in die Amazoncloud auszulagern, um damit mit jedem internetfähigen Gerät Zugriff darauf zu erlangen. Eine Besonderheit liegt darin, dass der 5 GB umfassende kostenlose Speicherplatz beim Kauf eines Albums als MP3-Download über Amazon für ein weiteres Jahr auf 20 GB aufgestockt wird. Alternativ ist der individuelle Zukauf von Speicherplatz möglich, wobei ein Gigabyte einen Dollar pro Jahr kostet. Die Speichergrößen sind allerdings vorgegeben und nur stufenweise (20, 50, 100, 200, 500 oder 1000 GB) buchbar.[341]

2.3.8.2 Salesforce

Ein weiterer Pionier und ein weiteres Schwergewicht ist das Unternehmen Salesforce.[342] Dieses bietet seinen Kunden Customer Relationship Management-Services (CRM) unter den Namen und den Webseiten „Force.com“, „Salesforce.com“ und „Database.com“ an. „Salesforce.com“ und „Sales Cloud 2“ stellen das eigentliche Software-as-a-Service-Angebot für das Kundenbeziehungsmanagement dar, während „Force.com“ als Entwicklungsplattform (PaaS) für Geschäftsanwendungen und Webseiten anzusehen ist.[343] Mit seinem Angebot widerlegt Salesforce außerdem die These, dass nur hoch standardisierte Software als Service funktioniert, da die CRM-Software stark an die Kundenbedürfnisse angepasst werden kann.[344]

---

337 *Büst*, Eucalyptus: Die Euca2ools, http://clouduser.org/tutorials/eucalyptus-die-euca2ools-4879; *Eucalyptus*, Euca2ools User Guide, http://open.eucalyptus.com/wiki/Euca2oolsGuide_v1.3.

338 *Amazon*, AWS Solution Providers, http://aws.amazon.com/de/solutions/solution-providers/?preview=true&type=isv&category=all&region=all.

339 *Büst*, Sind die Amazon Web Services der Standard der Cloud?, http://clouduser.org/management/sind-die-amazon-web-services-der-standard-der-cloud-5869.

340 *Neumann*, Elastic Beanstalk: Amazon betritt PaaS-Bühne, http://www.heise.de/newsticker/meldung/Elastic-Beanstalk-Amazon-betritt-PaaS-Buehne-1172343.html; *Ungerer*, Amazons Cloud als Mailing-Plattform, http://www.heise.de/newsticker/meldung/Amazons-Cloud-als-Mailing-Plattform-1177238.html.

341 *Amazon*, Additional storage plans available: 20 GB to 1000 GB, https://www.amazon.com/clouddrive/learnmore; *Elzer*, Amazon Cloud Drive: Gratis Onlinespeicher für MP3s, http://www.chip.de/news/Amazon-Cloud-Drive-Gratis-Onlinespeicher-fuer-MP3s_48109194.html; *Zota*, Amazon: Musik liegt in der Cloud, http://www.heise.de/newsticker/meldung/Amazon-Musik-liegt-in-der-Cloud-1216593.html.

342 http://www.salesforce.com/de.

343 *Salesforce*, CRM Produkte & CRM Lösung, http://www.salesforce.com/de/crm/products.jsp; *Salesforce*, Die Plattform für das Social Enterprise, http://www.salesforce.com/de/platform.

344 *Weiner/Renner/Kett* 2010, 101.

Kerngeschäft ist die in der Cloud bereitgestellte Software für das Kundenbeziehungsmanagement. Das CRM-SaaS-Angebot wird sogar von Branchengrößen und potentiellen künftigen Konkurrenten im Cloudbereich, wie zum Beispiel Facebook, genutzt.[345]

Die Preise für die CRM-SaaS-Angebote gelten jeweils pro Benutzer und Monat. Es gibt unterschiedliche Sales-Cloud-Editionen, beginnend mit dem „Contact Manager“ für bis zu fünf Benutzer zu je 4 Euro pro Monat und das Angebot „Group“ für grundlegende Sales- und Marketingfunktionen für 27 Euro pro Monat bei maximal fünf Benutzern. Größere Angebote sind „Professional“, „Enterprise“ und „Unlimited“.

„Professional“ kostet 27 Euro pro Benutzer und bietet die vollständigen CRM-Funktionen. Die beiden Topangebote bieten als Alleinstellungsmerkmale die individuelle Anpassbarkeit der CRM-Software für ganze Unternehmen ohne Benutzerlimit. „Enterprise“ kostet 135 Euro pro Monat und Benutzer, während für „Unlimited“ 270 Euro pro Monat zu zahlen sind. „Enterprise“ richtet sich an größere Unternehmen und bietet die passenden Werkzeuge, insbesondere Möglichkeiten der Workflowautomatisierung. „Unlimited“ erlaubt maßgeschneidertes CRM, was für Clouddienste untypisch ist. Das Angebot beinhaltet sogar einen Rund-um-die-Uhr-Service durch ein „Premier-Support-Team“ das Anpassungen der Software an die Bedürfnisse des Kunden vornimmt.[346]

Die Plattform „Force.com“ ermöglicht freien Entwicklern cloudbasierte Geschäftsanwendungen selbst zu programmieren und anzubieten. Hierzu stellt Force.com alle Programmierwerkzeuge und Programmierfunktionen in einer Umgebung bereit. Über den Marktplatz namens „AppExchange“ können die entwickelten Geschäftsanwendungen kostenlos oder gegen Miete vertrieben werden. Mit Hilfe der Foren „DeveloperForce“ und „Salesforce.com Community“ können sich die Benutzer zwecks gegenseitiger Unterstützung vernetzen und Beratungsleistungen austauschen.[347]

Mit Force.com können auch Vertrieb, Marketing, Partnermanagement und Kundenservice („Service Cloud 2“) verwaltet werden.[348] Das neueste Collaborationangebot namens „Chatter“ ermöglicht die unternehmensweite Zusammenarbeit der Sales-

---

[345] *Cloudtweaks*, Facebook Selects Salesforce.com As Cloud Computing Provider, http://www.cloudtweaks.com/2010/07/facebook-selects-salesforce-com-as-cloud-computing-provider.

[346] *Salesforce*, Die richtige Sales Cloud-Edition wählen, http://www.salesforce.com/de/assets/pdf/datasheets/DS_SalesCloud_EdCompare.pdf

[347] *Manhart*, Die wichtigsten Cloud-Computing-Provider, http://www.pcwelt.de/start/dsl_voip/online/praxis/2347953/die-wichtigsten-cloud-computing-provider/index5.html.

[348] *Salesforce*, CRM Produkte & CRM Lösung, http://www.salesforce.com/de/crm/products.jsp; *Baun/Kunze/Nimis/Tai* 2009, 55.

forcekunden.[349] Stichworte in diesem Zusammenhang sind Mobilität und ubiquitäre Zusammenarbeit.

Die Preise für die Plattform werden, analog zum SaaS-Angebot, ebenfalls pro Benutzer und Monat erhoben. Im Gegensatz zum Softwareangebot gibt es allerdings eine kostenlose Nutzungsmöglichkeit („Free-Edition“). Daneben gibt es analog zur Sales Cloud die Editionen „Enterprise“ und „Unlimited“ für 54 Euro beziehungsweise 80 Euro pro Monat und Benutzer. Bei diesen Angeboten ist eine weitere Differenzierung zwischen der Nutzung einer oder mehrerer Entwicklungsanwendungen möglich.[350]

Die Service Cloud 2, die zum Teil auch nichtcloudbezogene Services, wie Call-Center-Funktionen bietet, kostet je nach Tarif zwischen 70 und 285 Euro pro Monat und Benutzer. Chatter, soweit nicht schon in den Service-Cloud-Tarifen enthalten, ist für 15 Euro pro Monat und Benutzer buchbar.[351]

Einen Datenbankservice, also eine Kombination aus SaaS und PaaS, stellt das Ende 2010 vorgestellte Angebot namens database.com dar.[352] Kunden erhalten mit Beginn des Angebots monatlich 100.000 Objekte, 50.000 Transaktionen und drei Nutzerlizenzen kostenlos. Zusätzliche 100.000 Objekte oder 150.000 Transaktionen kosten jeweils 10 Dollar pro Monat.[353]

2.3.8.3 Google

„Google Apps“[354] und „Google App Engine“[355] sind Googles Cloudservices. Sie sind in der Sparte „Google Code“ angesiedelt, die alle Entwicklungs- und Programmierumgebungen, also auch diejenigen ohne Cloudbezug, bündelt.

Unter Google Apps sind die diversen SaaS-Angebote des Konzerns zusammengefasst. Bekannteste Dienste innerhalb der Apps sind GMail (Google Mail), Docs (Text & Tabellen), Calendar und Sites. Am ehesten folgt dabei Google Docs dem klassischen Software-as-a-Service-Gedanken. Die online nutzbare Software ersetzt durch ihren Funktionsumfang oftmals lokal installierte Office- und Textverarbeitungspakete, beispielsweise die Officesuiten von Microsoft. Es gibt aber auch Ergänzungen zu Microsoft Office, zum Beispiel den kostenlosen

---

349 *Salesforce*, Chatter, http://www.salesforce.com/de/chatter.

350 *Salesforce*, Die richtige Sales Cloud-Edition wählen, http://www.salesforce.com/de/assets/pdf/datasheets/DS_CustomCloud_EdCompare.pdf.

351 *Salesforce*, Editionen und Preise in der Übersicht, http://www.salesforce.com/de/crm/customer-service-support/pricing-editions.jsp.

352 http://www.database.com.

353 *Neumann*, Database.com: “Database as a Service” von Salesforce, http://www.heise.de/newsticker/meldung/Database-com-Database-as-a-Service-von-Salesforce-1149468.html; http://www.database.com/pricing.

354 http://code.google.com/intl/de/googleapps.

355 http://code.google.com/appengine.

Collaborationsoftwareservice „Cloud Connect for Microsoft Office“, mit dem mehrere Anwender simultan MS-Officedateien bearbeiten können.[356]

Das Angebot hat etwa 30 Millionen Nutzer und ist in drei Ausführungen erhältlich.[357] Die „Standard Edition“ ist kostenlos, jedoch sind nicht alle Anwendungen nutzbar und es wird Werbung eingeblendet. Außerdem ist sie auf 10 Nutzer begrenzt.[358] Ähnliche Konditionen bietet die „Non Profit Edition“, die sich an gemeinnützige Organisationen richtet.[359] Die „Premier Edition“ ist die kommerzielle Version mit Preisen von 40 Euro pro Nutzungskonto und Jahr und unbegrenzter Nutzerzahl.[360] Ähnlich der Premier Edition, jedoch kostenlos, ist die „Education Edition“, die sich an Schulen und Universitäten richtet und zusätzliche Tools zum gemeinsamen Lernen beinhaltet.[361] Speziell an Behörden richtet sich die „Government Edition“, wobei die jeweiligen Leistungen von Staat zu Staat differieren.[362] So sind nationalstaatliche Zertifizierungen, beispielsweise in den USA gemäß dem Federal Information Security Management Act (FISMA)[363], auch logischerweise nur in den entsprechenden Staaten verfügbar. Diese Edition kostet zum Beispiel in den USA 50 US-Dollar pro Nutzer und Jahr.[364]

Google App Engine ist eine Serviceplattform und ermöglicht das Entwickeln und Hosten von Webanwendungen. Hierzu stellt Google eine Programmier- und Ausführungsumgebung sowie Werkzeuge zur Softwareentwicklung bereit. Damit lassen sich Webapplikationen entwickeln, ohne sich mit der Serveradministration beschäftigen zu müssen. Unterstützte Programmiersprachen sind Python und Java.[365] Die lokale Laufzeitumgebung erlaubt das probeweise Ausführen und Testen dieser Applikationen. Laufen die Anwendungen fehlerfrei, werden sie an die Googleinfrastruktur übergeben und dort ausgeführt. Dadurch profitiert die entwickelte Software

---

356 http://tools.google.com/dlpage/cloudconnect.

357 *Google*, How many customers does Google Apps have?, http://code.google.com/googleapps/faq.html#how_many (Stand: Oktober 2011).

358 *Google*, Google Apps kostenlos ausprobieren, http://www.google.com/apps/intl/de/group/index.html.

359 *Google*, Google Apps for Nonprofit, http://www.google.com/apps/intl/en/nonprofit/index.html.

360 *Google*, Google Apps for Business, http://www.google.com/apps/intl/de/business/index.html.

361 *Google*, Google Apps for Education, http://www.google.com/a/help/intl/de/edu/index.html.

362 *Google*, Google Apps for Government, http://www.google.com/apps/intl/en/government/index.html.

363 *Google*, Secure applications to meet the needs of government, http://www.google.com/apps/intl/en/government/trust.html.

364 *Google*, Google Apps lets you focus on your agency's mission - not complex IT, http://www.google.com/apps/intl/en/government.

365 *Google*, The Application Environment, http://code.google.com/appengine/docs/whatisgoogleappengine.html; *Manhart*, Die wichtigsten Cloud-Computing-Provider, http://www.pcwelt.de/start/dsl_voip/online/praxis/2347953/die-wichtigsten-cloud-computing-provider/index4.html.

unmittelbar von der Zuverlässigkeit und Skalierbarkeit dieser Infrastruktur. Zudem können bereits vorhandene Services und Vertriebskanäle, beispielsweise der „Google Apps Marketplace“, genutzt werden.[366]

Eine weitere Erweiterung der herkömmlichen „App Engine“ ist die „App Engine for Business“, die – wie der Name bereits andeutet – größere Unternehmen als Zielgruppe anspricht.[367] Für die nichtkommerzielle Softwareentwicklung und unter Einhaltung gewisser Mengenbeschränkungen ist die Nutzung der App Engine kostenlos.[368] Es gibt ein Freikontingent je Entwickler für Rechenleistung, Speichernutzung und Datentransfer, das pro Nutzungstag gilt. So dürfen zum Beispiel Applikationen maximal 6,5 CPU-Stunden pro Tag verwenden und der Datendurchsatz maximal 1 GByte pro Tag und 56 MByte pro Minute betragen. Weitere Ressourcen können hinzugekauft werden, wobei die Preise mit denen der Amazon Web Services vergleichbar sind. Die Abrechnung erfolgt entsprechend dem tatsächlichen Mehrverbrauch.[369] Die Preise für die App Engine for Business betragen bei deren Neueinführung 8 US-Dollar pro genutzter Anwendung pro Benutzer und Monat.[370]

Speicherplatz für Entwickler wird im Angebot „Google Storage for Developers“ gebündelt.[371] Eine kostenlose Testversion des Angebots mit 5 GB Speicherplatz war bis Dezember 2011 vorhanden.[372]

2.3.8.4 Microsoft

Microsofts Cloudservices sind unter der „Windows Azure Platform“ zusammengefasst und erst seit Anfang 2010 kommerziell nutzbar.[373] Microsoft hat trotz der Dominanz von Google und Amazon und angesichts des drohenden Bedeutungsverlusts sein Cloudangebot relativ kurzfristig aufgezogen. Trotz der vergleichsweise späten Positionierung am Markt hat sich Azure als drittwichtigster Anbieter durchgesetzt. Innerhalb eines Jahres hat Microsoft bereits 10.000 Kunden für sein Angebot gewinnen können.[374] Angesichts der Marktdominanz Microsofts in anderen Berei-

---

366 *Manhart*, Die wichtigsten Cloud-Computing-Provider, http://www.pcwelt.de/start/dsl_voip/online/praxis/2347953/die-wichtigsten-cloud-computing-provider/index4.html; *Baun/Kunze/Nimis/Tai* 2009, 52, 53.

367 http://code.google.com/intl/de/appengine/business.

368 *Google*, Billing and Budgeting Resources, http://code.google.com/appengine/docs/billing.html; *Baun/Kunze/Nimis/Tai* 2009, 53.

369 *Manhart*, Die wichtigsten Cloud-Computing-Provider, http://www.pcwelt.de/start/dsl_voip/online/praxis/2347953/die-wichtigsten-cloud-computing-provider/index4.html.

370 http://code.google.com/appengine/kb/business.html#cost.

371 http://code.google.com/intl/de/apis/storage/?lr=lang_en|lang_de.

372 *Google*, Cloud Storage - Pricing and Support, http://code.google.com/apis/storage/docs/pricingandterms.html.

373 http://www.microsoft.com/windowsazure.

374 *Cloer*, Steve Ballmer schwört auf Cloud Computing, http://www.computerwoche.de/management/cloud-computing/2349201.

chen, der vorhandenen Infrastruktur und des Know-hows ist dieser Erfolg nicht zufällig.

Zudem setzt Microsoft mit seiner Zukunftsstrategie und den aktuellen und künftig zu tätigenden Investitionen einen großen Schwerpunkt auf Cloud Computing.[375] Vor allem die Kombination aus kostenpflichtiger Software für den PC und kostenlosen Onlinefunktionen in der Cloud ist ein erster Schritt in diese Richtung.

Windows Azure richtet sich hauptsächlich an Softwareentwickler. Die Azure-Plattform besteht aus drei Kernbestandteilen, nämlich Windows Azure, SQL Azure und Windows Azure AppFabric. Sie verbindet cloudbasierte Entwicklungsfunktionen mit Infrastrukturdiensten und ist somit als PaaS und IaaS zu klassifizieren. Unternehmen, IT-Dienstleister und Entwickler können damit Webanwendungen, Webdienste und Speicherplatz ohne Administrationsaufwand in Microsofts Rechenzentren mieten und bereitstellen.[376]

Die Preise sind etwas höher als bei der Konkurrenz. Eine Stunde Prozessorleistung kostet beispielweise 12 Cent. Pro Gigabyte gespeicherter Daten werden zusätzlich 15 Cent pro Monat berechnet. Außerdem werden 10 Cent pro Gigabyte hochgeladener Daten und 15 Cent für den Download berechnet.[377]

Nicht unmittelbar unter Windows Azure firmierend ist das Software-as-a-Service-Angebot „Office 365“.[378] Es umfasst die Office-Komponenten Textverarbeitung, Tabellenkalkulation und Präsentation. Diese sind Onlinependants zu den herkömmlichen Offlineversionen von Word, Excel und Powerpoint. Hinzu kommen das webbasierte E-Mail-Programm Exchange und die Kollaborationssoftware Sharepoint. Alle Funktionen von „Office 365“ laufen SaaS-typisch in einem Browser ab.[379]

Unternehmenskunden mit bis zu 25 Mitarbeitern bezahlen 5,25 Euro pro Nutzer und Monat. Großunternehmen und Behörden können für die Nutzung der Online-Office-

---

375 Siehe dazu auch die in Kap. 2.1.1 zitierten Aussagen von Microsofts CEO *Steve Ballmer*.

376 *Manhart*, Die wichtigsten Cloud-Computing-Provider, http://www.pcwelt.de/start/dsl_voip/online/praxis/2347953/die-wichtigsten-cloud-computing-provider/index6.html.

377 *Microsoft*, Windows Azure Platform Offers, http://www.microsoft.com/windowsazure/offers; *Manhart*, Die wichtigsten Cloud-Computing-Provider, http://www.pcwelt.de/start/dsl_voip/online/praxis/2347953/die-wichtigsten-cloud-computing-provider/index6.html.

378 http://office365.microsoft.com/en-US/online-services.aspx.

379 *Mossdorf*, Office 365: Microsoft stellt Internet-basierte Office-Programme vor, http://www.teltarif.de/office-365-suite-microsoft-google-apps/news/40430.html; *Microsoft*, What Is Office 365?, http://www.microsoft.com/en-us/office365/what-is-office365.aspx.

Suite Monatsgebühren zwischen 1,75 Euro und 22,75 Euro, abhängig von den Leistungen des Kundendiensts, bezahlen.[380]

2.3.9 Weitere Cloudprovider

Die „Rackspace Cloud“[381] firmierte ursprünglich unter der Marke „Mosso“. Sie war eine der ersten Clouds auf dem Markt. Rackspace bietet Webhosting unter dem Namen „Cloud Sites“ und Onlinespeicher unter dem Namen „Cloud Files“. Rechenleistung und Infrastruktur (IaaS) wird als „Cloud Servers“ bereitgestellt.[382]

Der Provider Zoho[383] ist hauptsächlich für die Bereitstellung von Software as a Service bekannt. Zoho bietet eine Vielzahl von Softwareprogrammen als Service an. Bekannteste sind die „Zoho Office Suite“ als Teil von „Zoho Business“, „Zoho Docs“ oder „Zoho CRM“. Die bereitgestellten Softwareservices können sowohl von Privat- als auch von Geschäftskunden genutzt werden. Letztere können auf Software zurückgreifen, die speziell für den Unternehmenseinsatz entwickelt wurde.

Mit „Blue Cloud“ ist IBM kein klassischer Anbieter von umfänglichen Cloudservices, sondern hauptsächlich ein Anbieter von Software und Hilfsprogrammen für Cloudanbieter. Nichtsdestotrotz hat IBM auch eigene Cloudservices, in Form von Rechenleistung und Speicherkapazität, vormals als „Computing on demand“ bekannt, im Angebot.[384]

T-Systems, das Tochterunternehmen der Deutschen Telekom stellt seit längerem Rechenzentren für Großkonzerne bereit. Die Bereitstellung von Cloud Computing war somit der nächste logische Schritt. Seit November 2010 bietet T-Systems, zunächst als kostenlose viermonatige Pilottestphase, IaaS-Services für jedermann an. Alle Rechenzentren und Kundendaten befinden sich in Deutschland und sind gemäß ISO 27001[385] zertifiziert. Kunden sollen die Rechenzentren auch selbst auditieren können. Zwischen den Anwendungen der jeweiligen Kunden findet eine logische Trennung statt und weitere, nicht näher spezifizierte, Sicherheitsvorkehrungen sollen vor Zugriffen über das Internet schützen. Ausdrücklich erwähnt wird nur die Zugangskontrolle. Vertraglich sollen definierte Service Level Agreements eine große Rolle spielen.[386] Technisch stehen vorkonfigurierte Systeme auf Basis von x86-Prozessoren mit 32- und 64-Bit-Betriebssystemen zur Verfügung. Über ein

---

380 *Microsoft*, Office 365 Fact Sheet, http://office365.microsoft.com/uploadedFiles/Office365FactSheet.docx; *Meusers*, Ein Büro in der Wolke, http://www.spiegel.de/netzwelt/web/0,1518,724188,00.html.

381 http://www.rackspacecloud.com.

382 *Rackspace*, Cloud Products, http://www.rackspacecloud.com/cloud_hosting_products.

383 http://www.zoho.com.

384 http://www-03.ibm.com/systems/deepcomputing/cod/infrastructure.html.

385 Siehe dazu Kap. 3.1.9.9.8.

386 *Deutsche Telekom*, T-Systems startet „Infrastructure as a Service“ für Großkunden, http://www.telekom.com/dtag/cms/content/dt/de/595758?archivArticleID=953550; *Ihlenfeld*, Telekom bietet Infrastructure as a Service an, http://www.golem.de/1011/79570.html.

Webportal können Informationen zur Systemlaufzeit und über die genutzten Ressourcen einschließlich der Prozessor- und Speicherleistung abgefragt werden.[387]

Weitere bekannte Anbieter sind die Provider Linode, GoGrid und RightScale.[388] Apple hat erst Mitte 2011 einen Dienst namens iCloud gestartet, der aber lediglich Datensynchronisation zwischen mehreren Geräten und Streaming von Musik ermöglicht und deswegen nur mit gutem Willen als Clouddienst eingeordnet werden kann.[389]

2.3.10 Provider im öffentlichen Bereich

Wie bereits weiter oben geschildert,[390] ist absehbar, dass auch öffentliche Bundes-, Landes- oder Kommunalbehörden, Universitäten oder andere öffentliche Verwaltungseinheiten, neben der Einführung von Internal Clouds, mittelfristig vorhandene gemeinsame Ressourcen unterschiedlicher Verwaltungseinheiten als Community Clouds zusammenführen werden.[391] Beispielsweise ist denkbar, dass regional beschränkt genutzte Shared Services Center zu groß angelegten Cloudsystemen zusammengezogen werden. Beim Freiwerden von erheblichen Überkapazitäten durch dieses Zusammenführen ist nicht zuletzt ein privatwirtschaftliches Tätigwerden nicht auszuschließen, indem die frei werdenden Ressourcen als Public Cloud zugänglich gemacht werden oder komplette Rechenzentren an Private verkauft oder vermietet werden. Bei einem solchen Mischbetrieb ist erst recht auf eine strikte Trennung der jeweiligen Daten, vorzugsweise auf physischer Hardwareebene, zu achten.

Beispiele aus den Vereinigten Staaten zur Bereitstellung von Cloudservices für und durch US-Bundesbehörden wurden bereits weiter oben im Rahmen der Darstellung der Community Clouds genannt.[392] Insbesondere „Apps.gov“ der GSA ist in diesem Zusammenhang noch einmal erwähnenswert, da, trotz der vergleichsweise geringeren Sensitivität der Daten innerhalb der Clouds der GSA, zahlreiche Anforderungen und Voraussetzungen zu beachten sind, bevor Cloud Computing für US-Bundesbehörden zulässig ist. Hintergrund ist das Federal Risk and Authorization Management Program (FedRAMP), das eine standardisierte Sicherheits- und Risikoprüfung mitsamt Risikobewertung erfordert.[393] Daneben beinhaltet FedRAMP die

---

387 *Ihlenfeld*, Telekom bietet Infrastructure as a Service an, http://www.golem.de/1011/79570.html.

388 http://www.rightscale.com; Linode und GoGrid wurden weiter oben schon erwähnt.

389 http://www.apple.com/icloud.

390 Siehe dazu Kap. 2.3.7.3.

391 *Deussen/Strick/Peters*, 2010, iv, 22.

392 Siehe hierzu noch einmal Kap. 2.3.2.6.

393 *CIO Council*, Federal Risk and Authorization Management Program (FedRAMP), http://www.cio.gov/pages-nonnews.cfm/page/Federal-Risk-and-Authorization-Management-Program-FedRAMP; *CIO Council*, Proposed Security Assessment & Authorization for U.S.

zur Problemlösung notwendigen Sicherheitsanforderungen und Hinweise auf Basissicherheitsmaßnahmen. Für externe kommerzielle Cloudanbieter ist, wie der Name schon andeutet, eine besondere Autorisierung und insbesondere die Abnahme der Sicherheitsmaßnahmen durch das sogenannte Joint Authorization Board erforderlich, das aus je einem Vertreter der GSA, des US-Verteidigungsministeriums (DoD) und des Department of Homeland Security (DHS) besteht.[394]

Die Nutzung von kommerziellen Public Clouds durch Behörden und dabei insbesondere Staats- und Kommunalbehörden ist in den USA bereits alltägliche Praxis.[395] Googles „Gov Cloud“, die zum Beispiel von den Behörden der Stadt Los Angeles genutzt wird, ist Vorreiter in diesem Bereich.[396] Der Bundesstaat Minnesota nutzt für seine 33 000 Angestellten Cloudservices von Microsoft (Business Productivity Online Suite), die jedoch nicht nur spezifisch für Behörden, wie zum Beispiel Googles Gov Cloud, bereitgestellt werden. Eine Besonderheit dieser Cloudservices von Microsoft ist die territoriale Begrenzung auf US-Hoheitsgebiet.[397]

2.4 Soziale Folgen des Cloud Computing

Cloud Computing wird einen erheblichen Einfluss auf die künftige Nutzung und Bereitstellung von Informationstechnologie haben. Durch die immer fortschreitendere Vernetzung, die Verlagerung von Daten und Anwendungen ins Netz, die weltweite Verfügbarkeit der Dienste und die Nutzung immer präsenterer Hardware wird Informationstechnologie noch weitgehender in den Alltag der Menschen integriert werden als dies heute bereits der Fall ist. Die Nutzung von Smartphones, Tablets und des mobilen Internets sind heute schon ein erster Hinweis darauf, wie sich die IT-Welt fortentwickeln wird, um dann mit dem Ubiquitous Computing den vorläufigen Höhepunkt der Durchdringung des Alltags mit Informationstechnologie zu erreichen.

Government Cloud Computing, https://info.apps.gov/sites/default/files/Proposed-Security-Assessment-and-Authorization-for-Cloud-Computing.pdf.

394 *Spies*, USA: Cloud Computing - Nicht einfach, wenn Kunde die US-Regierung ist, http://blog.beck.de/2010/12/14/usa-cloud-computing-nicht-einfach-wenn-kunde-die-us-regierung-ist-fedramp; *Mell*, Federal Cloud Computing Strategy, https://isaca-washdc.sharepointsite.net/resources/Event%20Presentations/Conference-April2010-Session4.pdf.

395 Amazons Clouddienst speziell für US-Behörden namens „AWS GovCloud“ wurde beispielsweise bereits in Kap. 2.3.8.1 und Fn. 332 erwähnt.

396 *Claburn*, Google's Gov Cloud Wins 7.2 Million Los Angeles Contract, http://www.informationweek.com/news/services/saas/showArticle.jhtml?articleID=221100129.

397 *Kirsch*, Minnesota setzt auf Microsofts Cloud, http://www.heise.de/newsticker/meldung/Minnesota-setzt-auf-Microsofts-Cloud-1100600.html; *Henschen*, State of Minnesota Moves To Microsoft's Cloud, http://www.informationweek.com/news/government/cloud-saas/showArticle.jhtml?articleID=227500838&subSection=All+Stories; siehe auch Fn. 332.

2.4.1 Chancen und Risiken des Cloud Computing

Bei der Darstellung der Merkmale und Eigenschaften von Cloud Computing wurde bereits kurz auf einige Vor- und Nachteile eingegangen. Diese sollen nun näher dargestellt werden. Methodisch wird dieser Abschnitt zudem später im Rahmen der Anwendung der KORA-Methode Relevanz erlangen. Dabei ist insbesondere auf die Risiken und Nachteile einzugehen, die – soweit sie sicherheitsrelevant sind – später im Detail in Form einer Bedrohungsanalyse ermittelt und dargestellt werden sollen. Vorab ist bereits festzustellen, dass Cloudsysteme und deren Nutzung eigene spezifische Bedrohungen aufweisen, aber auch faktisch alle herkömmlichen Bedrohungen weiterhin akut sind. Angesichts der Kombination bereits bestehender Technologien ist dies kein überraschender Befund. Erfreulich ist, dass den meisten dieser klassischen Bedrohungen auch auf herkömmliche Art und Weise begegnet werden kann.

Bevor jedoch auf die Nachteile und die damit verbundenen Gefahren sowie deren mögliche Lösung eingegangen wird, sollen die einleitend angeführten Vorteile dargestellt werden.

2.4.1.1 Vorteile und Chancen

2.4.1.1.1 Kostenersparnis

Wie bereits angedeutet, ersparen sich Startups die Investitionen in eigene Hard- und Software.[398] Dies führt zu einer Reduktion der Markteintrittsbarrieren, so dass ein Startup direkt mit der Umsetzung seiner Geschäftsidee beginnen kann und nicht Zeit und Geld in den Aufbau der IT-Infrastruktur investieren muss. Die sogenannte „Time-to-Market“ wird durch die flexible und schnelle Anmietbarkeit von IT-Services erheblich reduziert. Dies betrifft nicht nur IT-Unternehmen, sondern faktisch alle Unternehmen, da diese heutzutage auf die Nutzung von EDV und IT angewiesen sind. Bei der Darstellung der Cloudanbieter wurde ersichtlich, dass die Services ihrerseits, abhängig von der Nutzungszeit und der Anzahl der Nutzer, Kosten verursachen. Diese On-Demand-Nutzung kann aber in vielen Fällen billiger sein als das Vorhalten eigener Ressourcen.

Diese Möglichkeit einer Kostenersparnis äußert sich aber nicht nur beim Markteintritt, sondern auch im späteren Unternehmensalltag, weil nur für den tatsächlich notwendigen Bedarf an IT-Leistungen Clouddienste angemietet werden müssen. Bei größerer Auftragslage werden die IT-Dienstleistungen schnell und einfach erweitert. Früher liefen Unternehmen Gefahr, entweder eine über- oder eine unterdimensionierte IT-Ausstattung vorzuhalten. Hierzu nötige Planungen, Prognosen und Berechnungen kosteten Zeit, Personalaufwand und dementsprechend Geld. Außerdem

[398] Siehe dazu auch die Ausführungen in der Einleitung.

gab es die Problematik der Über- oder Unterlizenzierung von Software.[399] Auch die Vorhaltung redundanter IT-Infrastruktur kostete Geld. Diese kann durch die Nutzung von Clouddiensten, bis auf redundante Internetzugangsmöglichkeiten, eingespart werden. Neben privatwirtschaftlichen Unternehmen kann auch der öffentliche Sektor Geld einsparen. So sollen durch den Einsatz von Cloud Computing in der Verwaltung Einsparungen im zweistelligen Prozentbereich erzielbar sein.[400]

Durch Cloud Computing lässt sich auch Personal einsparen.[401] Die bestehende IT-Abteilung kann auf ein Minimum reduziert werden, sobald die angemieteten Cloudservices in Betrieb genommen wurden. Bei der Umstellung eines Unternehmens von herkömmlicher IT auf Cloudtechnologie wird die unternehmensinterne IT-Abteilung jedoch für Planungen, die konkrete Umsetzung und für die Anfangsphase des Betriebs gebraucht werden. Problematisch erscheint der mit der Reduzierung der Personaldecke einhergehende Verlust von IT-Know-how im Unternehmen. Geht etwas im laufenden Betrieb schief, müssen Externe als Dienstleister beauftragt werden, die sich zunächst in die lokalen Gegebenheiten einarbeiten müssen. Angesichts der relativ homogenen Cloudservices ist diese Einarbeitungsphase aber nur noch von der unternehmensspezifischen IT-Ausstattung abhängig. In den meisten Fällen ist die bedarfsgerechte Anmietung von IT-Dienstleistern aber immer noch billiger als ständig eine eigene IT-Abteilung bereitzuhalten. So ist es bei kleineren Unternehmen oder Selbständigen schon immer üblich, IT-Supportdienstleistungen von spezialisierten IT-Unternehmen nur bei Bedarf einzukaufen. Je komplexer und größer ein IT-System, umso eher lohnt es sich allerdings eine eigene IT-Abteilung vorzuhalten. Ob Cloudservices im Übrigen einen Beitrag zu geringerer Komplexität der Unternehmens-IT leisten werden, muss die Zukunft zeigen.

Ein mit den Kosten und Lizenzen zusammenhängender Aspekt, ist der der Eindämmung von lizenzwidrig genutzter Software.[402] Nur online nutzbare Software kann nicht kopiert und unberechtigt genutzt werden. Potentielle Straf- und Schadensersatzzahlungen, die eine lizenzwidrige Nutzung nach sich zieht, sind keine Gefahr mehr für den Finanzhaushalt eines Unternehmens. Für Unternehmen, deren Angestellte absichtlich oder unabsichtlich nicht oder nicht ausreichend lizenzierte Software einsetzten, konnten das Aufdecken der unberechtigten Nutzung und die sich daran anschließenden Konsequenzen nicht selten den Untergang bedeuten. Mit online bereitgestellter Software, deren lizenzrechtliche Aspekte nur noch den Cloudanbieter betreffen, besteht das Problem nicht mehr.

---

399 Siehe dazu auch Kap. 2.3.5.10.

400 *Kien*, HP-Umfrage: Cloud-Computing für Verbraucher noch ohne Bedeutung, http://www.funkschau.de/telekommunikation/news/article/69108/0/HP-Umfrage_Cloud-Computing_fuer_Verbraucher_noch_ohne_Bedeutung.

401 So auch *Tetzner* 2010, 24.

402 Umgangssprachlich als „Raubkopien“ bezeichnet.

Zudem sind Skaleneffekte erkennbar, die die Kosten für die Implementierung von Sicherheitsmaßnahmen reduzieren. Die Kosten für Sicherheitsmaßnahmen steigen nämlich nicht proportional zur Implementierungsgröße.[403] Cloudprovider können Sicherheit für eine Vielzahl von Kunden erheblich günstiger anbieten verglichen mit der individuellen Implementierung durch die einzelnen Kunden. Aus Kundensicht sinken mit der Nutzung von Cloudservices die Kosten für IT-Sicherheit oder es wird bei gleichbleibenden Kosten ein höheres Sicherheitsniveau erreicht.[404]

2.4.1.1.2 Förderung des Wirtschaftswachstums

Cloud Computing hat Prognosen zufolge erheblichen Einfluss auf die Weltwirtschaft. Einer Studie des Londoner Centre for Economics and Business Research im Auftrag des US-amerikanischen IT-Unternehmens EMC, das einen Teil des Umsatzes selbst mit Clounddienstleistungen bestreitet, soll Cloud Computing der deutschen Volkswirtschaft bis zum Jahr 2015 jährliche Vorteile im Wert von bis zu 49 Milliarden Euro erbringen.[405] Insgesamt sollen in den fünf Jahren ca. 221 Milliarden erwirtschaftet werden.[406] Die Zahlen umfassen sowohl Public, Private als auch Hybrid Clouds. Die prognostizierten Vorteile umfassen Einsparungen, Geschäftsentwicklungsmöglichkeiten, Vorteile durch tatsächliche Geschäftsgründungen und Multiplikatoreffekte.[407]

Der Prognose zufolge soll Cloud Computing zudem bis zum Jahr 2015 allein in Deutschland zu Gründung von 39 000 neuen Unternehmen führen und in diesem Zeitraum voraussichtlich 789 000 Arbeitsplätze schaffen, die direkt oder indirekt mit Cloud Computing zusammenhängen.[408]

Neben Deutschland wurden auch für die Länder Frankreich, Großbritannien, Spanien und Italien Prognosen erstellt. Für diese fünf größten Volkswirtschaften Europas soll Cloud Computing zu Vorteilen in Höhe von 177 Milliarden Euro pro Jahr füh-

---

403 *Slamka/Georg*, in: Schartner/Weippl, D-A-CH Security 2010, 24.

404 *Slamka/Georg*, in: Schartner/Weippl, D-A-CH Security 2010, 25; *Helmbrecht*, DuD 2010, 554.

405 *EMC*, The Cloud Dividend - The economic benefits of cloud computing to business and the wider EMEA economy, http://uk.emc.com/collateral/microsites/2010/cloud-dividend/cloud-dividend-report.pdf; *Wilkens*, Forscher errechnen makroökonomische Vorteile des Cloud Computing, http://www.heise.de/newsticker/meldung/Forscher-errechnen-makrooekonomische-Vorteile-des-Cloud-Computing-1148384.html; *EMC*, The Cloud Dividend - Executive Summary: Germany, http://uk.emc.com/microsites/2010/cloud-dividend/germany.htm.

406 *EMC*, The Cloud Dividend - The economic benefits of cloud computing to business and the wider EMEA economy, http://uk.emc.com/collateral/microsites/2010/cloud-dividend/cloud-dividend-report.pdf, S. 7.

407 *EMC*, The Cloud Dividend - The economic benefits of cloud computing to business and the wider EMEA economy, http://uk.emc.com/collateral/microsites/2010/cloud-dividend/cloud-dividend-report.pdf, S.12 ff.

408 *Wilkens*, Forscher errechnen makroökonomische Vorteile des Cloud Computing, http://www.heise.de/newsticker/meldung/Forscher-errechnen-makrooekonomische-Vorteile-des-Cloud-Computing-1148384.html.

ren.[409] In den fünf Staaten sollen außerdem im Zeitraum zwischen 2010 und 2015 insgesamt knapp 2,4 Millionen Arbeitsplätze entstehen.[410]

2.4.1.1.3 Hohe Skalierbarkeit

Die „gute“ oder „hohe“ Skalierbarkeit als Merkmal von Cloudsystemen ist einer der großen Vorteile des Konzepts.[411] Cloudsysteme sind dynamisch skalierbar und können sowohl „nach oben“ als auch „nach unten“ gut skalieren, so dass die Entziehung von Ressourcen analog zur Steigerung derselben die annähernde Leistungsreduktion oder den annähernden Leistungszuwachs zur Folge hat.

Reduziert man die Ressourcen zum Beispiel um die Hälfte, so ist auch die Leistung nur noch halb so groß. Steigert man die Ressourcen um das Doppelte, so steigt auch die Leistung im Optimalfall um das Doppelte. In informationstechnischen Systemen ist dies nicht unbedingt immer der Fall, so dass die Skalierbarkeit einen erheblichen wirtschaftlichen Aspekt darstellt.

Mit der hohen Skalierbarkeit hängen auch die Flexibilität und die Möglichkeit der schnellen Bereitstellung zusammen. Es ist vor der Bereitstellung oder Entziehung absehbar, wie sich die Leistung entwickelt. Wäre dies nicht der Fall, müsste man nach langwierigen Tests und durch Kapazitätsplanungen im Vorfeld ermitteln, wie viele Ressourcen nötig sind, um einen benötigten Leistungszuwachs tatsächlich zu realisieren. Es wäre zudem unwirtschaftlich, einen doppelten Leistungszuwachs erst mit – beispielsweise – der zehnfachen Zuteilung von Ressourcen zu erreichen. Wie bereits ausgeführt, bedeutet „schlechtes Skalieren“ nicht selten, dass ab einer gewissen Ressourcenzuteilung oder Ressourcenentziehung ein System einfach nicht mehr funktioniert. Erhebliche Softwareanpassungen, um die Performance entsprechend der Ressourcenzuteilung zu verbessern oder das System überhaupt zum Funktionieren zu bringen, wären die Folge. Solche Probleme schlecht skalierbarer Systeme sind im Fall des Cloud Computing aufgrund erprobter Virtualisierungstechniken und den Erfahrungen mit Großrechenzentren weitestgehend gelöst.

Die hohe Skalierbarkeit hat aber auch Vorteile für die Sicherheit und Verfügbarkeit von Cloudsystemen. Im Falle eines Angriffs, beispielsweise einer DDoS-Attacke[412], können Ressourcen dynamisch und automatisiert umverteilt werden, so dass poten-

---

409 *EMC*, The Cloud Dividend - Executive Summary: Germany, http://uk.emc.com/microsites/2010/cloud-dividend/germany.htm.

410 *EMC*, The Cloud Dividend - The economic benefits of cloud computing to business and the wider EMEA economy, http://uk.emc.com/collateral/microsites/2010/cloud-dividend/cloud-dividend-report.pdf, S. 7.

411 Zur Definition und weiteren Einzelheiten der Skalierbarkeit sei auf die Ausführungen in Kap. 2.3.5.7 verwiesen.

412 Distributed-Denial-of-Service-Attacke; hierbei wird ein System mit Anfragen überhäuft, so dass es unter der Last entweder komplett zusammenbricht oder legitime Anfragen nicht mehr durchkommen oder nicht mehr beantwortet werden können, wodurch die Verfügbarkeit des Systems leidet.

tiell negative Auswirkungen auf die Verfügbarkeit des Systems reduziert und minimiert werden.[413]

2.4.1.1.4 Verfügbarkeit

Die Wahrscheinlichkeit, dass ein professionell geführtes Cloudunternehmen einen Datenverlust erleidet, dürfte im Vergleich zu Privatnutzern oder kleineren und mittleren Unternehmen geringer sein. Zum einen ist das Know-how der Beteiligten unterschiedlich groß und zum anderen ergeben sich in Cloudumgebungen erhebliche Redundanzen, indem Daten oder Datenfragmente auf mehreren physischen Systemen gespeichert und repliziert werden. Vermeintlich verlorene Daten sind deshalb bei Teilausfällen oder Löschungen oft dennoch wiederherstellbar.[414]

Techniken wie RAID[415] sind zwar auch im kleineren Maßstab bei Privaten oder kleinen Unternehmen einsetzbar, jedoch sind professionelle Cloud(storage)systeme auf einem höheren technischen Level. Außerdem ist ein großer Provider in der Lage abgestufte Sicherheits- und Preismodelle anzubieten und damit Risiken gewissermaßen kalkulationsfähig zu machen. Amazon bietet zum Beispiel abhängig von der garantierten Haltbarkeit und dem Replikationsaufwand unterschiedliche Endkundenpreise. Während Amazon für S3 eine Haltbarkeit und Verfügbarkeit der Daten von 99,999999999 Prozent angibt, sind es beim Reduced-Redundancy-Storage-Angebot nur 99,99 Prozent. In beiden Fällen wird die garantierte Haltbarkeit durch eine Überwachung der Systeme erreicht, die dafür sorgt, dass beim Ausfall einzelner Speichermedien die Daten automatisch auf weitere Systeme repliziert werden. In der S3-Standardversion gespeicherte Daten sollen den Ausfall von zwei Rechenzentren überstehen, während Amazon dies bei der Reduced-Redundancy-Storage-Version nur für den Ausfall eines Rechenzentrums garantiert.[416]

Auch bei der Verfügbarkeit im Sinne des Aufrechterhaltens des Betriebs sind verteilte Systeme und damit auch Clouds besser abgesichert. Achillesferse im Zusammenhang mit Cloud Computing ist der Zugang zum Internet und damit zu den Cloudservices an sich. Sobald dieser ausfällt, ist auch die in den SLAs garantierte

---

413 *Slamka/Georg*, in: Schartner/Weippl, D-A-CH Security 2010, 25.

414 So konnten beim bisher größten Vorfall eines Datenverlusts in einer Cloud, nämlich beim Anbieter T-Mobile USA, die meisten Daten wiederhergestellt werden; *Fried/Beiersmann*, T-Mobile kann verlorene Sidekick-Daten teilweise wiederherstellen, http://www.zdnet.de/news/mobile_wirtschaft_t_mobile_kann_verlorene_sidekick_daten_teilweise_wiederherstellen_story-39002365-41515733-1.htm; eine ebenfalls erfolgreiche Wiederherstellung gab es Anfang 2011 beim zeitweisen Verlust von Emails bei Googlemail; *Braun*, Verschwundene Google-Mails werden wiederhergestellt, http://www.heise.de/newsticker/meldung/Verschwundene-Google-Mails-werden-wiederhergestellt-1200083.html.

415 *Luther/Vilsbeck/Haluschak*, RAID im Überblick, http://www.tecchannel.de/storage/extra/401665/raid_sicherheit_level_server_storage_performance_festplatten_controller.

416 *Ihlenfeld*, Amazon startet Billigversion von S3, http://www.golem.de/1005/75217.html.

Verfügbarkeit eines Clouddienstes hinfällig. Mit der Etablierung von Clouddiensten wird es notwendig, auch den Internetzugang redundant auszulegen. Denkbar ist, dass ein Unternehmen mehrere physische Leitungen oder Zugänge über Mobilfunk, Satellit oder Richtfunk anmietet, so dass alternative Internetzugangsmöglichkeiten beim Ausfall eines physischen Zugangs vorhanden sind.

2.4.1.1.5 Elastizität und Flexibilität

Elastizität und Flexibilität sind das Ergebnis der schnellen Bereitstellungsmöglichkeit. Kurzfristig auftretender Ressourcenbedarf (hohe Last) kann schnell und effektiv aufgefangen werden, indem zusätzliche Ressourcen eines oder mehrerer Cloudanbieter angemietet werden, während in Zeiten geringer Last Kapazitäten ebenso schnell reduziert und gekündigt werden können.

Im Gegensatz zu früheren Outsourcingmodellen führt diese erleichterte Buchbarkeit von Cloudleistungen auch zu einer flexiblen Auswahl des zu nutzenden Providers. Der faktische Zwang zur Bindung an einen bestimmten Provider entfällt oder wird auf ein Minimum reduziert. Cloud Computing fördert ein situativeres Eingehen von Geschäftsbeziehungen und reduziert langfristige Geschäftspartnerschaften. Die Geschwindigkeit der Entstehung und Lösung von Geschäftsbeziehungen, aber auch die Freiheit, Entscheidungen rückgängig zu machen, wenn sich Rahmenbedingungen ändern, geben Cloud Computing einen Vorteil gegenüber der Anbahnung und Aufrechterhaltung traditioneller Outsourcingpartnerschaften. Die Entscheidungsfreiheit der Nutzer wird größer. In dem Maße, wie die Freiheit wächst, müssen Unternehmen aber auch Entscheidungskompetenz aufbauen.[417]

2.4.1.1.6 Energieeffizienz und Umweltschutz

Durch Cloud Computing sind Energieeinsparungen absehbar, so dass Cloud Computing auch zum Schutz der Umwelt beitragen könnte. Der Betrieb von wenigen zentralen Rechenzentren und lediglich schlanken und vergleichsweise sparsamen Client-PCs ist energiesparender als das dauernde Bereithalten einer Vielzahl leistungsfähiger Einzel-PCs und kleinerer Rechenzentren, die zudem nur zum Teil ausgelastet sind und ohne Notwendigkeit Energie verbrauchen. Die Energieeffizienz wird durch die optimale Auslastung gesteigert. Ein neuartiger Aspekt der optimalen Auslastung ist die modulare Zusammenstellung und Erweiterbarkeit von ganzen Rechenzentren durch Container.[418]

Darüber hinaus ist auch die Produktion von schlanken Client-PCs, Tablets oder Smartphones weniger ressourcenschädigend als die Herstellung von überdimensionierten „Desktopboliden“. Bis vor wenigen Jahren war die Steigerung der Pro-

---

[417] *Reti/Pauly* 2009, 13.

[418] Microsoft nutzt neuerdings auch Rechenzentren, die auf solchen Servercontainern basieren, die sogar mit Lastkraftwagen transportiert werden können; siehe dazu *Manhart*, Rechnen im Baukastenprinzip, http://www.computerwoche.de/management/cloud-computing/2489154.

zessorleistung gleichbedeutend mit einem höheren Energieverbrauch. Seit einigen Jahren gibt es allerdings rechenstarke und gleichzeitig vergleichsweise sparsame Prozessormodelle. Auch bei den weiteren Rechnerkomponenten (zum Beispiel beim Grafikprozessor oder Chipsatz) wurde, nicht zuletzt wegen der Durchsetzung von Notebooks und Netbooks, auf eine möglichst energiesparende Arbeitsweise der Hardware seitens der Hersteller geachtet. Trotz dieser Bemühungen der Hersteller zur Entwicklung sparsamer Komponenten bleibt das Problem des weitgehenden Leerlaufs dieser Komponenten und des unnötigen Stromverbrauchs, so dass die Energieeffizienz von Cloudumgebungen trotzdem vorteilhafter ist. Außerdem zeigt das Beispiel der Smartphones, Netbooks und Tablets, dass die Akzeptanz von leistungsschwachen und mobilen Clients durch die Nutzer, noch vor der Durchsetzung des Cloudgeschäftsmodels, bereits hoch ist.

Trotz der erwarteten Einsparungen werden die Rechenzentren der größten Internetunternehmen um das Jahr 2020 nach Prognosen von Greenpeace den Verbrauchswert von Staaten erreichen und dreimal höher sein als heutzutage.[419] Im Jahr 2020 werden sie mehr Energie verbrauchen als Frankreich, Deutschland, Kanada und Brasilien im Jahr 2010 zusammen. In der Modellrechnung wird davon ausgegangen, dass die Zahl der Server jährlich um neun Prozent wächst.[420] Als Ursache und Antreiber dieser Entwicklung wird die immer stärkere Durchsetzung von Cloud Computing ausgemacht.[421] Die Prognosen sagen jedoch nichts darüber aus, wie hoch der Verbrauch wäre, wenn sich Cloud Computing nicht durchsetzen würde, also der Status quo mit unzähligen dezentralen und energieineffizienten Desktoprechnern und Rechenzentren weiterbestünde. Ein positiver Aspekt ist zudem darin zu sehen, dass große Internetunternehmen einige ihrer Rechenzentren mit Wasserkraft betreiben und dadurch nicht zu CO2-Emissionen beitragen.[422] Setzt sich dieses Modell der Nutzung erneuerbarer Energien für Cloudrechenzentren weiter durch, so ist ein noch größerer Beitrag zum Umweltschutz möglich.

Eine solche Erhöhung der Nutzung erneuerbarer Energien ist auch deshalb anzuraten, weil sich bereits in der näheren Vergangenheit, nämlich zwischen 2000 und

---

419 *Beiersmann*, Greenpeace: Stromverbrauch von Rechenzentren steigt bis 2020 um Faktor drei, http://www.zdnet.de/news/wirtschaft_unternehmen_business_greenpeace_stromverbrauch_von_rechenzentren_steigt_bis_2020_um_faktor_drei_story-39001020-41529895-1.htm; *Greenpeace*, Make IT Green, http://www.greenpeace.org/raw/content/usa/press-center/reports4/make-it-green-cloud-computing.pdf.

420 *Sawall*, Rechenzentren brauchen mehr Strom als Industriestaaten, http://www.handelsblatt.com/technologie/energie_technik/co-sub-2-sub-bilanz-rechenzentren-brauchen-mehr-strom-als-industriestaaten;2554827; *Greenpeace*, Make IT Green, http://www.greenpeace.org/raw/content/usa/press-center/reports4/make-it-green-cloud-computing.pdf.

421 *Greenpeace*, Make IT Green, http://www.greenpeace.org/raw/content/usa/press-center/reports4/make-it-green-cloud-computing.pdf, S. 1.

422 *Greenpeace*, Make IT Green, http://www.greenpeace.org/raw/content/usa/press-center/reports4/make-it-green-cloud-computing.pdf, S. 3.

2005, der Energieverbrauch von Servern weltweit verdoppelt hat.[423] Nach einer Studie des Borderstep-Instituts hat sich auch der Energiebedarf von Rechenzentren in Deutschland zwischen 2000 und 2006 auf rund 8,7 Milliarden Kilowattstunden mehr als verdoppelt. Die Stromkosten haben sich im gleichen Zeitraum aufgrund der gestiegenen Energiepreise auf 867 Millionen Euro sogar mehr als verdreifacht.[424] Neben den Umweltgesichtspunkten wird mit umweltfreundlich ausgestaltetem Cloud Computing folglich auch eine Reduzierung der Energiekosten einhergehen. Diese sind in vielen Rechenzentren die größten Kostenfaktoren.

Konkrete Prognosen hinsichtlich der Reduzierung des Energiebedarfs und damit der Energiekosten und des CO2-Ausstoßes bietet eine von Microsoft in Auftrag gegebene Studie.[425] Diese kam zum Ergebnis, dass sich die Einsparungen zwischen 30 und 90 Prozent bewegen werden, wenn Software anstatt lokal installiert aus der Cloud bezogen wird.[426]

Die Studie vergleicht drei weit verbreitete Microsoftanwendungen für E-Mail, virtuelle Zusammenarbeit und CRM, die einmal jeweils lokal installiert und ein anderes Mal aus der Cloud genutzt werden. Konkret wurde die CO2-Bilanz von Netzwerk-, Server- und Speicherinfrastruktur für Einheiten von 100, 1000 und 10000 Nutzern ermittelt. Die Studie besagt, dass je kleiner das Unternehmen ist, umso größer dürfte der Nutzen durch die Umstellung auf Cloudservices sein. Kleine Unternehmen mit 100 Nutzern, die Clouddienstleistungen verwenden, könnten die CO2-Bilanz um bis zu 90 Prozent reduzieren, größere und große Unternehmen um immerhin noch ca. 30 Prozent.[427] Ursachen für die Energieeinsparungen sind die positiven Skaleneffekte und die effizientere Nutzung der Infrastruktur bei Cloud Computing. Die Studie stellt zudem fest, dass, trotz der Energiesparbemühungen in unternehmenseigenen lokalen Datenzentren, die Umweltverträglichkeit bei Anbie-

---

423 *Berl/Fischer/De Meer*, Informatik Spektrum 2010, 192.

424 *Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit/BITKOM*, Energieverbrauch in Rechenzentren senken, http://www.bmu.de/benutzerhinweise/impressum/doc/3537.php.

425 *Accenture*, Cloud Computing and Sustainability, http://download.microsoft.com/download/A/F/F/AFFEB671-FA27-45CF-9373-0655247751CF/Cloud%20Computing%20and%20Sustainability%20-%20Whitepaper%20-%20Nov%202010.pdf.

426 *Wilkens*, Microsoft: Cloud Computing hilft der Umwelt, http://www.heise.de/newsticker/meldung/Microsoft-Cloud-Computing-hilft-der-Umwelt-1131304.html.

427 *Microsoft*, Studie: erhebliches Potenzial zur Senkung des Energiebedarfs durch Cloud Computing, http://www.pressebox.de/pressemeldungen/microsoft-deutschland-gmbh-0/boxid/387296; *Accenture*, Cloud Computing and Sustainability, http://download.microsoft.com/download/A/F/F/AFFEB671-FA27-45CF-9373-0655247751CF/Cloud%20Computing%20and%20Sustainability%20-%20Whitepaper%20-%20Nov%202010.pdf, S. 6.

tern einer großen Public Cloud wegen diesen positiven Skaleneffekten dennoch besser sein soll.[428]

2.4.1.1.7 Ortsunabhängigkeit

Ortsunabhängigkeit meint die Möglichkeit, von überall, wo ein Zugang zum Internet besteht, auf die in der Cloud vorgehaltenen Daten zugreifen zu können. Zwar ist das an sich nichts Neues, da es auch bisher schon möglich war Daten ins Netz zu stellen, jedoch erfordert das Onlinestellen bislang einen zusätzlichen Schritt des aktiven und gezielten Hochladens durch den Datennutzer. Vergaß dieser beispielsweise auf dem Unternehmensrechner gespeicherte Daten online zu stellen, konnte er auch nicht von außerhalb auf diese zugreifen. Clouddaten hingegen sind von Anfang an „im Netz“. Kompliziertes Synchronisieren mit verschiedenen Rechnern und verschiedenen Dateiversionen entfällt.

Im Grunde genommen kommt es durch die Nutzung von Cloudservices zu einer Umkehrung des Verhaltens. Während früher Daten lokal vorgehalten wurden und nur optional online gestellt wurden, wird es zukünftig mit der vermehrten Nutzung von Clouds umgekehrt sein. Daten sind dann überwiegend online in der Cloud und nur sekundär und optional lokal gespeichert. Die zusätzliche lokale Speicherung hat den Sinn einer zusätzlichen Datensicherung oder die fortbestehende Nutzbarkeit der Daten beim Ausfall des Cloudservices oder des Internetzugangs. Diese parallele Datenhaltung bringt jedoch wieder den Aufwand des Abgleichs und auch erhöhte Hardwareanforderungen (Speicherplatz) mit sich. Als Übergangsphase, insbesondere wenn die lokale Hardware ohnehin schon vorhanden ist, ist diese „Doppelnutzung“ ratsam. Nicht zuletzt deshalb, weil anzunehmen ist, dass Cloud Computing als Technologie in seiner Anfangsphase auch mit Ausfällen und Unterbrechungen zu kämpfen haben wird. Auch die Errichtung redundanter Internetzugänge braucht Zeit und entsprechendes Know-how. Je zuverlässiger und fehlerunanfälliger die Dienste funktionieren, umso eher kann man die Daten und Dienste exklusiv in die Clouds migrieren.

Richtet man für ausgelagerte Daten und Dienste entsprechende Freigaben ein, sind auch Kollaborationen mehrerer Mitarbeiter möglich. Neue ausgeklügelte Lösungen hierfür werden mit der Verbreitung der Clouds immer nutzerfreundlicher und „intelligenter“ funktionieren. In gewissem Sinne sind bereits Chats und herkömmliche Internetforen Vorläufer dieser mitarbeitsfähigen Verfügbarkeit von Daten. Auch hierbei wird also deutlich, dass durch Cloudservices und Cloudapplikationen „das

---

[428] *Microsoft*, Studie: erhebliches Potenzial zur Senkung des Energiebedarfs durch Cloud Computing, http://www.pressebox.de/pressemeldungen/microsoft-deutschland-gmbh-0/boxid/387296; *Accenture*, Cloud Computing and Sustainability, http://download.microsoft.com/download/A/F/F/AFFEB671-FA27-45CF-9373-0655247751CF/Cloud%20Computing%20and%20Sustainability%20-%20Whitepaper%20-%20Nov%202010.pdf, S. 2.

Rad nicht neu erfunden wird“, sondern vorhandene Technik und Methoden zusammengeführt, verbessert und weiterentwickelt werden.

2.4.1.1.8 Einfachheit

Einfachheit bedeutet zum einen, die möglichst einfache Nutzung der Services und zum anderen die Möglichkeit des situativen Eingehens von Geschäftsbeziehungen mit unterschiedlichen Cloudprovidern. Außerdem entfallen der zeitintensive Aufbau und die Einrichtung von lokaler IT.

Die Nutzung von Cloudservices sollte mindestens genauso einfach sein, wie die Nutzung lokaler IT. Sollen jedoch vorhandene lokale Ressourcen durch Services ersetzt werden oder in die Cloud migriert werden, so kann dies dem Gedanken der Einfachheit entgegenstehen. Dies ist beispielsweise dann der Fall, wenn die zu nutzenden Schnittstellen uneinheitlich sind und Standards fehlen, so dass eine Migration mit Schwierigkeiten verbunden ist.

Einfachheit ist hingegen ein klarer Vorteil für Unternehmen, die „neu starten“. Startups konzentrieren sich nur noch auf ihr Kerngeschäft, anstatt Geld und Zeit für das Planen, Dimensionieren, Ankaufen, Einrichten oder für sonstige Tätigkeiten im Zusammenhang mit der Anschaffung lokaler IT zu investieren.

Der zweite Punkt der Einfachheit betrifft die kurzfristig und situativ eingehbaren Geschäftsbeziehungen zwischen Kunden und Cloudprovidern. Im Gegensatz zum klassischen IT-Outsourcing oder ASP hat der Kunde die Auswahl, wann und wie lange er welchen Provider nutzen will. Nicht selten werden die Nutzer unterschiedliche Cloudservices unterschiedlicher Provider kombinieren, um möglichst effizient, unabhängig und kostengünstig agieren zu können. Einfachheit ist folglich Voraussetzung der oben angeführten Flexibilität.

Dieses situative und einfache Eingehen und Lösen von Geschäftsbeziehungen muss auch in den Verträgen zum Tragen kommen und rechtlich machbar sein. Zwingendes Recht ist dabei selbstredend nicht modifizierbar.

Ein weiterer Aspekt der Einfachheit ist auch das erleichterte Patchmanagement. Das zentrale Planen und Einspielen der Updates ist in Clouds effizienter, erheblich einfacher und wegen der Virtualisierung oft ohne Ausfall der Services möglich.[429]

2.4.1.1.9 Unabhängigkeit von proprietären Betriebssystemen

Ein ganz wesentlicher Vorteil von Software as a Service als Teil des Cloud Computing ist die Ausgestaltung als Webapplikation. Dies hat den Vorteil, dass solche webbasierten Applikationen auf jedem internetfähigen Gerät mit einem Webbrowser genutzt werden können. Die Anwendung wird damit vom zugrundeliegenden Betriebssystem unabhängig. Nutzer können damit auf unterschiedlichen Geräten

---

[429] *Slamka/Georg*, in: Schartner/Weippl, D-A-CH Security 2010, 25; siehe auch Kap. 2.3.1.3.

und völlig frei von proprietären Zwängen die Software als Service nutzen. Entwickler müssen diese nur einmal programmieren und nicht mehr aufwendig an unterschiedliche Betriebssysteme anpassen oder gänzlich neuprogrammieren. Der Pro-Programmieraufwand verringert sich, während sich die Anzahl der potentiellen Nutzer sogar noch erhöht.

2.4.1.1.10 Sicherheit

Es ist umstritten, ob eine Auslagerung von Daten und Diensten ins Internet, also auch in Cloudsysteme, einen Sicherheitsvorteil oder einen Sicherheitsnachteil darstellt. Angesichts der weiter unten darzustellenden Bedrohungen ist es nicht verwunderlich, dass bei einer nur oberflächlichen Betrachtung die Datenauslagerung als Nachteil aufgefasst wird. Auch der Aspekt des „aus der Hand Gebens" der Daten durch die Unklarheit der örtlichen Speicherung in Clouds bereitet vielen Sicherheitsverantwortlichen Unbehagen. Zieht man jedoch in Betracht, dass die Daten in einer Cloud regelmäßig verschlüsselt sind oder zumindest eine Verschlüsselung anzustreben ist, so relativieren sich diese Bedenken teilweise.[430] Es gibt aber auch weitere Erwägungen und Konstellationen, die bei einer Beurteilung als Vor- oder Nachteil in Betracht kommen.

So muss man nämlich beachten, welche Umstände miteinander verglichen werden. Vergleicht man ein professionell geführtes Cloudunternehmen mit eigens dazu ausgebildeten Mitarbeitern mit Privatrechnern oder Servern eines kleineren Unternehmens, in dem allenfalls sporadisch ein Fachmann die Sicherheitseinstellungen und Sicherheitsmaßnahmen überprüft und aktualisiert, so kann man davon ausgehen, dass das Know-how zur Absicherung der Daten in Cloudumgebungen höher ist.[431] Nicht jeder Privatmann oder Kleinunternehmer kann sich die allerneuesten Sicherheitskenntnisse und -anwendungen aneignen oder leisten. Insofern wird durch die Nutzung eines Clouddienstes sicherheitsrelevantes Know-how und tatsächlicher technisch-organisatorischer Schutz der Daten mit eingekauft. Dies ist mit der Situation vergleichbar, dass man sein Geld lieber einem Banksafe anvertraut, anstatt es im Sparstrumpf zu lagern, weil die Sicherheit Kernkompetenz einer Bank ist.[432]

Geschieht ein Fehler im Verantwortungsbereich des Anbieters, so ist dieser – soweit er dies nicht ausdrücklich gesetzlich ausschließen kann – im Übrigen auch scha-

---

430 Siehe hierzu auch Verschlüsselung als technisches Gestaltungsziel in Kap. 4.5.1.

431 Siehe dazu auch bereits Kap. 2.3.5.6; so im Übrigen auch *Goldmann*, Datenschutz-Berater 11/2010, 18; ein Beleg für diese These sind die professionellen Botnetze und deren Trojaner, die überwiegend auf Privatrechner abzielen und vorwiegend auch auf solchen zu finden sind; siehe dazu *Hensel*, Ungeschützte Privatrechner in Botnetzen sind Spam-Hauptursache, http://www.searchsecurity.de/themenbereiche/bedrohungen/phishing-und-spam/articles/136936; *Tsvihun/Stephanow/Streitberger* 2010, 7; *Helmbrecht*, DuD 2010, 554.

432 *Tsvihun/Stephanow/Streitberger* 2010, 7.

densersatzpflichtig.[433] Schädigt sich der Privatmann oder Kleinunternehmer selbst, indem er die nötigen Sicherheitsmaßnahmen vernachlässigt hat, so kann er auch niemanden dafür zur Verantwortung ziehen. Professionelle Angreifer sind faktisch nie zu überführen, so dass er den entstandenen Schaden alleine tragen muss.

Es ist also, ohne dies empirisch nachweisen zu können, allein aus der allgemeinen Lebenserfahrung wahrscheinlicher, dass die Daten aus kleineren Rechnerumgebungen entwendet oder auch ungewollt zerstört werden als in einem professionellen Rechenzentrum mit mehrfachen Redundanzen und aktuellen Sicherheitsmechanismen, dessen Kernaufgabe gerade darin besteht, die Daten möglichst sicher aufzubewahren und zu verarbeiten.

Für große Unternehmen, die eigene Großrechenzentren betreiben und deshalb nur bedingt auf öffentliche Cloudservices angewiesen sind, sieht es jedoch anders aus. Da das Sicherungs-Know-how bei Großkonzernen und Public Clouds auf dem gleichen Niveau ist, besteht aus der Sicherheitsperspektive eines solchen Unternehmens in der Regel kein zwingender Grund, Public Clouds zu nutzen. Ein konkretes Sicherheitsassessment und der Vergleich mit den Sicherheitsmaßnahmen eines Providers kann diese Frage jedoch am besten beantworten.

Ein weiterer wichtiger Sicherheitsaspekt ist die physische Herrschaftsgewalt und Kontrolle über die Daten und Infrastrukturen. Die Ansicht, dass die Aufgabe der physischen Kontrolle zu einem Sicherheitsnachteil führt, ist jedoch nicht verallgemeinerbar. So sind die beiden Alternativen, dass ein über das Internet agierender Angreifer die Schutzmechanismen im online angebundenen Unternehmen oder in einer gesicherten Cloudumgebungen angreift und überwindet als gleichartig anzusehen. Sicherheit ist in diesen Fällen keine Frage des physischen Standorts der Daten und der physischen Herrschaftsgewalt über die Daten, sondern eine Frage des Onlinezugangs, den der Angreifer ausnutzt, um auf die Daten zuzugreifen.

Es lässt sich also festhalten, dass bei der Nutzung kryptographisch sicher verschlüsselter Daten der physische Speicherort für die Wahrscheinlichkeit des unberechtigten Zugangs zum Informationsgehalt nur eine geringe bis gar keine Relevanz hat, wenn diese Daten ohnehin in irgendeiner Form online zugänglich sind. Für Daten, die wegen ihrer Sensitivität fortwährend in Offlineumgebungen vorgehalten wurden gilt diese Aussage allerdings nicht. Bei stringent offline gespeicherten Daten muss ein Angreifer sich der Daten physisch bemächtigen, was bedeutend schwieriger ist als das Abgreifen über Netzwerke.

Es gibt allerdings noch weitere Argumente, die für einen Sicherheitsvorteil von Cloud Computing sprechen. Die lokale Vorhaltung der Daten schützt geringer vor der mutwilligen oder zufälligen physischen Zerstörung von Daten. In Cloudsystemen werden Daten redundant gespeichert. Zudem ist für Außenstehende prinzipbe-

[433] Zu Haftungsfragen siehe auch Kap. 3.5.3.3.

dingt meist unklar, wo genau die Daten gerade gespeichert sind, so dass eine (nicht nur physische) Kompromittierung dieser Systeme schwieriger wird. Zudem dürften Cloudrechenzentren auch physisch besser geschützt sein als die Rechner eines kleineren oder mittleren Unternehmens.[434] Im Umkehrschluss kann also die lokale Speicherung in einem Unternehmen oder Privathaushalt die gezielte oder gezieltere Datenzerstörung ermöglichen. Zerstört ein Angreifer alle Festplatten in einem Unternehmen, beispielsweise indem er ein Gebäude in Brand setzt, so ist die Wahrscheinlichkeit sehr hoch, dass er die unternehmensrelevanten Daten unwiederbringlich zerstört. In Clouds ist diese Angriffsform praktisch nicht durchführbar. Alleine das – eher unwahrscheinliche – Zerstören aller Cloudrechenzentren eines Anbieters oder sogar von Subunternehmen würde einen vergleichbaren „Erfolg“ nach sich ziehen.

2.4.1.1.11 Verringerung von Datensätzen und Verarbeitungsvorgängen durch Zentralisierung

Ein Vorteil im Sinne des Datenschutzprinzips der Datenvermeidung und Datensparsamkeit ist der Aspekt der Zentralisierung von Datensätzen und die damit einhergehende Reduzierung von Verarbeitungsvorgängen.[435] Die dezentrale Nutzung eines „Fat Client“ hat im Vergleich zu einem „Thin Client“ und der zentralen Vorhaltung und Verarbeitung den Nachteil, dass die Daten auf jedem einzelnen „Fat Client“ vorrätig sein müssen und auch auf jedem einzelnen dieser Geräte verarbeitet werden müssen.[436]

Soweit also die gleichen personenbezogenen Daten von mehreren genutzt werden, ist es bei funktionierendem Zugriffsschutz grundrechtsschonender, diese nur einmal auf dem Cloudserver vorzuhalten und zu verarbeiten, statt mehrfach auf den einzelnen Clients der Nutzer. Insbesondere Datenbanken, beispielsweise in Unternehmen oder Behörden sind dadurch grundrechtsschonender nutzbar. Dies darf andererseits jedoch nicht dazu führen, dass ehemals isoliert und begrenzt nutzbare Datensätze auch von Nichtberechtigten einsehbar werden.[437]

Während die lokalen Verarbeitungsvorgänge reduziert werden, steigen allerdings im Gegenzug die Übermittlungsvorgänge zwischen Nutzern und Providern und umgekehrt, so dass besonders auf die Absicherung des Datentransports geachtet werden muss. Unter Umständen kann die Zahl der notwendigen Übermittlungen die Zahl der, ansonsten lokal stattfindenden, Verarbeitungen erheblich übersteigen, so dass

---

[434] Zum Beispiel indem die Örtlichkeiten möglichst geheim gehalten werden, nur schwer zugänglich sind und durch Wachpersonal überwacht werden.

[435] Zum Prinzip siehe Kap. 3.1.6.5.

[436] Siehe hierzu auch das Beispiel bei *Roßnagel*, in: Eifert/Hoffmann-Riem, Innovation, Recht und öffentliche Kommunikation, 2011, 47.

[437] Siehe auch das Beispiel der beabsichtigten Zusammenführung von lokalen Einwohnermeldedaten zu einem zentralen Melderegister in Kap. 3.1.7.1.

bei gewissen Diensten die Zentralisierung mindestens als neutral, wenn nicht sogar als nachteilig angesehen werden kann.

Der angesprochene Vorteil ergibt sich außerdem auch nicht bei der klassischen Umsetzung der Mehrmandantenfähigkeit. Dabei werden die Daten immer noch durch mehrere Stellen mehrfach verarbeitet. Die einzelnen Verarbeitungen erfolgen dann nicht mehr jeweils lokal, sondern immer noch einzeln und voneinander abgeschottet auf der Infrastruktur des Providers, so dass die Anzahl der Verarbeitungsvorgänge die gleiche ist.

2.4.1.1.12 Demokratisierung und Innovationsförderung

Nicholas Carr ist der Ansicht, dass mit Cloud Computing eine „Demokratisierung von IT-Systemen“ einhergeht. Während die Erfindung des Personal Computers Individuen den Zugang zu Computern gebracht hat, bringt Cloud Computing ihnen künftig den Zugang zu einem ganzen Rechenzentrum. Der Zugriff durch jedermann auf quasi unendliche Computerkapazitäten zu sehr geringen Kosten soll der Kreativität von Programmierern, Designern und Wissenschaftlern künftig keine Grenzen mehr setzen. Er ist der Ansicht, dass man künftig eine wahre Explosion an innovativen Ideen auf Basis der Cloudtechnologie sehen wird und dass diese neuen Möglichkeiten dem Einzelnen im Ergebnis mehr Macht geben werden.[438]

Dass die Bezeichnung als „Demokratisierung“ nicht unpassend gewählt ist, zeigt der Vergleich zum Grid und High Performance Computing. Während bei diesen Formen nur wissenschaftliche Institutionen oder Großkonzerne leistungsfähige Rechenzentren nutzen konnten, ist dies mit Cloud Computing jedermann möglich. Durch die geringen Kosten ist eine breitere Nutzung potentiell unbegrenzter Rechenleistung oder Speicherkapazität möglich. Unternehmen, insbesondere Entwicklungs- und Forschungsabteilungen, können ihre Berechnungen, zum Beispiel Crash-Test-Simulationen in der Automobilindustrie oder Genomanalysen in der Pharmazie kostengünstiger oder überhaupt erstmalig durchführen, so dass auch diese Aspekte innovationsfördernd wirken.[439]

Eine Vorahnung dieser Innovationsfreundlichkeit des Cloud Computing im Privatbereich bietet das Web 2.0 mit den Social Communities, wie zum Beispiel Facebook. Ohne die Demokratisierung bei der Nutzung wären solche Modelle der sozialen Vernetzung nicht möglich gewesen. Private Cloudarchitekturen ebneten den Weg bei der technischen Umsetzung. Facebooks immense Kapazität an Rechenzentren ist eine große Private Cloud mit öffentlichen Elementen, nämlich der Möglichkeit der kostenlosen Nutzung innerhalb eines vorgegebenen Rahmens. Die-

---

[438] Vergleiche dazu *Peer*, Aufbruch in ein neues IT-Zeitalter, http://www.handelsblatt.com/datenwolke-aufbruch-in-ein-neues-it-zeitalter;2708100;3.

[439] Ähnlich *Peer*, Aufbruch in ein neues IT-Zeitalter, http://www.handelsblatt.com/datenwolke-aufbruch-in-ein-neues-it-zeitalter;2708100;3; http://www.news-medical.net/news/20100909/20/German.aspx; siehe dazu bereits oben Kap. 2.3.7.2.3.

ser Nutzungsrahmen ist technisch in Form einer Webseite und rechtlich durch Nutzungsbedingungen begrenzt.

Ein weiterer Aspekt der Demokratisierung kommt in Verbindung mit Mobile Computing, also der Nutzung von Smartphones und Tablets mittels Internetbrowser und schlanker Apps, zum Tragen. In Entwicklungsländern können sich weniger Menschen einen ausgewachsenen Rechner mit Internetzugang leisten als ein Handy oder Smartphone. So haben bei einer Milliarde Menschen in Indien nur etwa 80 Millionen einen Zugang zum Internet, gleichzeitig besitzen aber 600 Millionen ein Mobiltelefon.[440] Es wird offensichtlich, dass mit Cloud Computing, das die Anforderungen an die Clienthardware reduziert, mehr Menschen an der globalen Informationsgesellschaft teilhaben können. Informationsfreiheit als Basis jeder Demokratie hat nämlich immer die Voraussetzung diese auch effizient wahrnehmen zu können. Mit Cloud Computing wird in dieser Hinsicht ein großer Sprung nach vorne getan.

2.4.1.1.13 Zukunftssicherheit

Glaubt man den Prognosen, so wird man in Zukunft als Privatanwender, aber auch als Unternehmen, Cloud Computing nicht ignorieren können. Cloud Computing soll demnach eine der zukunftssichersten Technologien sein. In diesem Zusammenhang wird darauf hingewiesen, dass Clouds den Vorteil der „Selbsterneuerung“ haben. Eine Cloud besteht aus vielen, oft hunderttausenden, einzelnen Serverkomponenten, die laufend ausgetauscht und durch neuere Modelle ersetzt werden. Eine Cloudumgebung regeneriert sich so in kleinsten Schritten und entwickelt sich dadurch permanent weiter.[441] Diese Selbsterneuerung betrifft jedoch nicht nur die verwendete Hardware, sondern auch die den Systemen zugrundeliegende Software (beispielsweise Hypervisoren). Diese Weiterentwicklung und Aufrüstung erfolgt für die Nutzer möglichst ungestört und unbemerkt, so dass diese im Optimalfall immer von und mit der neuesten und effizientesten Technologie versorgt werden. Voraussetzung für die Zukunftssicherheit ist jedoch die Möglichkeit der Nutzer, einen alternativen Cloudprovider auswählen zu können, also die Daten migrieren zu können, um damit Lock-In-Effekte[442] zu vermeiden. Trotz Zukunftssicherheit des Konzepts, ist es nicht auszuschließen, dass einzelne Anbieter ihre Angebote einstellen müssen, zum Beispiel nach einer Insolvenz.

Für Softwareentwickler, die sich Cloudplattformen bedienen, bieten die oft daran gekoppelten Marktplätze eine höhere Reichweite bei den Kunden, so dass die ent-

---

440 *Scaglia*, Wie Cloud und Mobile Computing unser Leben verändern, http://www.handelsblatt.com/gastbeitrag-wie-cloud-und-mobile-computing-unser-leben-veraendern;2726192;2.

441 *Batlogg*, Die 10 größten Vorteile des Cloud Computing, http://www.zehn.de/zukunftssicherheit-7241-3.

442 Siehe zum Begriff Kap. 2.4.1.2.2.

wickelte Software auch tatsächlich genutzt wird, dadurch die Erlöse steigen und andere Entwickler zu Verbesserungen oder daraus abgeleiteten neuen Softwareapplikationen inspiriert werden.[443] Insbesondere die Marktplätze für Smartphoneapps von Apple namens „App Store“ oder „Google Play“ für Androidapps boomen.[444]

Auch die umweltverträglichere Nutzung von Informationstechnologie durch die Etablierung von Cloudservices ist ein Aspekt der Zukunftssicherheit. Umweltschädliche Technologien und Konzepte haben mittel- bis langfristig keine Chance weiterzubestehen. Nach dem Verursacherprinzip müssen Verursacher von Umweltschäden für die Kosten aufkommen, so dass ein Interesse besteht möglichst umweltfreundliche Technologie auf den Markt zu bringen.

Zukunftssicherheit muss aber auch rechtlich gewährleistet sein. Ebenso wie umweltschädliche Technologie untergehen wird, haben nicht rechtsgemäße oder sogar rechtswidrige Technologieanwendungen ebenso keine Zukunft. Um diese Zukunftssicherheit zumindest für einen absehbaren Zeitraum gewährleisten zu können, bietet es sich an, die Technik im Vorfeld so zu gestalten, dass nachträgliche Änderungen oder das „Einstampfen“ der Technik nicht notwendig werden.

Teilweise gestaltet aber auch die pure Faktizität vorhandener Technologien die aktuellen und zukünftigen gesetzlichen Normen und Regelungen. Dies ist aber relativ selten der Fall und nur dann erfolgreich, wenn die Technologien weltweit eingesetzt werden, am Markt oder in der Gesamtbevölkerung überaus beliebt und aus dem Alltag nicht mehr wegzudenken sind. Als Beispiele seien der Erfolg des Personal Computers oder des Internets genannt. Große Teile des heutigen IT-Rechts sind erst nach dem Aufkommen der Technologien entstanden oder angepasst worden, wobei diese Anpassungen auch in viele andere Rechtsbereiche ausstrahlten.[445] Im Fall des Cloud Computing könnte dies erneut der Fall sein. Um mit der technischen Entwicklung Schritt halten zu können, ist neben rechtlicher Technikgestaltung auch die frühzeitige Gestaltung von Rechtsregeln notwendig.[446]

Insbesondere sind diverse Forderungen nach einem einheitlichen, internationalen Rechtsrahmen im Datenschutz- und Strafverfolgungsbereich laut geworden. So hat Microsoft eine Eingabe bei der Federal Communications Commission (FCC) eingebracht, die die wesentlichen rechtlichen Probleme in der internationalen Anwen-

---

443 Ähnlich *Kurz*, Netzwoche 17/2008, 35.

444 Rein statistisch hat mehr als jeder Vierte in Deutschland (28 %) schon einmal Apps aus einem solchen Marktplatz heruntergeladen und 19 Prozent aller Mobiltelefonbesitzer nutzten täglich Apps; siehe hierzu *Winter*, Jeder Vierte hat bereits eine App aufs Smartphone geladen, http://www.teltarif.de/markt-mobile-app-appstore-smartphone-mobilfunk-technologie/news/40724.html.

445 Man denke beispielsweise an die Auswirkungen des Formanpassungsgesetzes auf die Formvorschriften des BGB oder ähnlich alte Gesetzeswerke wie das HGB oder die ZPO.

446 Zu Vorschlägen zur Rechtsgestaltung siehe Kap. 3.10.

dung von Cloudservices enthält.[447] Microsoft fordert von der US-Regierung, dass sich diese stärker engagiert, um auf internationaler Ebene einen Rechtsrahmen zu finden, der die bestehenden Ungleichgewichte und rechtlichen Widersprüche möglichst weitgehend beseitigt und das Geschäftsmodell Cloud Computing nachhaltig fördert. Ansätze auf der Ebene der Wirtschaft allein hätten bislang kaum Lösungen erbracht.[448]

2.4.1.2 Nachteile und Risiken

2.4.1.2.1 Unvorhersehbare Fehler

Unstreitig ein Nachteil, wie bei allen neuen Konzepten oder Technologien, ist die Problematik von unvorhersehbaren und unvorhergesehenen Fehlern. Angesichts der Komplexität der verwendeten Techniken und der Abhängigkeit von zuverlässigen Infrastrukturen ist dies ein nicht zu verachtender Punkt. Zwar kann man mit Sicherheits- und Risikoanalysen sowie Simulationen oder Simulationsstudien die gröbsten Fehler antizipieren und beseitigen, jedoch ist neue Technik immer fehleranfälliger als über Jahre hinweg in der Praxis etablierte. Je komplexer ein System, umso geringer ist der Einfluss der Neuartigkeit. In hochkomplexen Umgebungen ist unabhängig von der Neuartigkeit immer mit Fehlern zu rechnen.

Zielsetzung in solchen neuen und komplexen Systemen muss es zunächst sein die möglichen Schäden zu begrenzen und damit das Schadenspotential zu reduzieren. Im Zusammenhang mit Cloud Computing ist damit die Frage des Ob und des Wie der Nutzung verbunden. Es besteht die Möglichkeit die auszulagernden Daten in einem ersten Schritt auszusondern, anschließend zu klassifizieren und letztlich nur unwichtige oder weniger wichtige Daten in Clouds auszulagern. Die Betrachtung sollte unter dem Aspekt des Datenverlusts aufgrund mangelnder Funktionssicherheit der Cloudumgebungen und nicht unter dem Aspekt des Verlusts der physischen Verfügungsgewalt über die Daten erfolgen. Es muss auch nicht unbedingt zum Verlust im Sinne einer Zerstörung oder eines Abhandenkommens der Daten kommen. Bereits die fehlende Zugriffsmöglichkeit, beispielsweise durch Ausfall der Clouddienste, kann Schäden verursachen. Der Verlust oder der gestörte Zugriff auf unwichtige Daten produziert nur geringe Schäden, während der Verlust wichtiger Daten oder die zeitweise Unmöglichkeit des Zugriffs in Extremfällen die Insolvenz eines Unternehmens oder einer Person bedeuten kann. Das Schadenspotential orientiert sich also unmittelbar an der Sensitivität und Bedeutung der Daten für ein Unternehmen oder für eine Person.

---

447 *Microsoft*, Written Ex Parte Communication, NBP Public Notice 21, Data Portability and Its Relationship to Broadband, https://portal.neca.org/portal/server.pt/gateway/PTARGS_0_0_307_206_0_43/http%3B/prodnet.www.neca.org/publicationsdocs/wwpdf/1231microsoft.pdf.

448 *Spies*, MMR-Aktuell 2010, 297791.

Cloudtechnologie ist kein Ersatz herkömmlicher lokaler Speicherung und Nutzung, sondern eine Ergänzung, mithin eine Option, die dem Nutzer zusätzlich zur Verfügung steht, so dass er frei entscheiden kann, ob und inwieweit er Cloud Computing nutzen will. Die Nutzung kann auch stufenlos erfolgen, abhängig davon, wie detailliert er seine Anforderungen definiert. Langfristig ist jedoch absehbar, dass die einleitend aufgezeigten Zukunftsszenarien einer weitverbreiteten Cloudnutzung eintreten werden. Insbesondere ist der Aspekt zu beachten, dass sich die Technologie im Laufe der Zeit etabliert und gerade durch die Nutzung die Funktionstüchtigkeit und Zuverlässigkeit ansteigt.

2.4.1.2.2 Lock-In-Effekte und fehlende Standards

Als sogenanntes „Vendor Lock-in“ oder nur „Lock-in“, also „Einsperren“ bezeichnet man den Umstand, dass sich ein Nutzer von einem Anbieter derart abhängig macht, dass er keine Wahl mehr hat. Dies kann dadurch geschehen, dass er die Daten und Services nicht anderweitig portieren und nutzen kann. Lock-In-Effekte und daraus folgende Abhängigkeitsverhältnisse entstehen durch proprietäre Software und Schnittstellen eines Anbieters. Lock-in kann sogar so weit gehen, dass ein Nutzer die Daten nicht nur nicht zu Konkurrenzanbietern, sondern auch nicht mehr auf eigene lokale IT-Systeme migrieren kann.

Eine besondere Gefahr entsteht dann durch das Scheitern der Geschäftsbeziehung, sei es im Streit oder einfach durch das Einstellen der Services des Cloudproviders, beispielsweise indem dieser insolvent wird. Im Streitfall kann der Anbieter den Kunden mit den Daten unter Druck setzen, indem er diese „in Geiselhaft“ nimmt. Der Kunde ist dann dem Provider ausgeliefert. Bei einer Insolvenz des Cloudanbieters besteht die Gefahr, dass die bei ihm vorgehaltenen Daten für den Kunden entweder überhaupt nicht mehr nutzbar sind oder mit hohem finanziellem und personellem Aufwand kompatibel gemacht werden müssen. Notfalls muss der Kunde hierfür Hardware des ehemaligen Anbieters ankaufen oder aus der Insolvenzmasse erwerben.

Einheitliche, möglichst offene Standards und normierte Schnittstellen sind daher Voraussetzung, um ein solches Einsperren zu verhindern und die Daten flexibel zu anderen Anbietern oder auf lokale Systeme übertragen zu können.[449] Ist eine solche Standardisierung der Schnittstellen jedoch einmal realisiert, so wird sich dieser Umstand als Vorteil darstellen, da dadurch die Flexibilität der Kunden durch erleichterte Anbieterwechsel gesteigert wird.[450] Allerdings ist auch trotz offener Standards weiterhin eine Abhängigkeit des Kunden von einem oder mehreren Anbietern gege-

---

[449] *Fickert*, in: Taeger/Wiebe, Inside the Cloud, 419; offene Standards sollen beispielsweise die Mitte 2011 gegründete Open Cloud Initiative (http://www.opencloudinitiative.org) oder OpenStack gewährleisten; zu OpenStack siehe auch Fn. 306.

[450] *Slamka/Georg*, in: Schartner/Weippl, D-A-CH Security 2010, 25.

ben, weil er prinzipbedingt keinen direkten administrativen Zugriff auf die Hard- und Software hat.[451]

Einen ähnlichen technischen Aspekt führt *Vinton Cerf*, der Mitbegründer des Internetprotokolls, an. Ihm zufolge ergibt sich Vendor Lock-in auch aus dem Aspekt, dass sich die Fülle der im Laufe der Zeit in eine Cloud geladenen Daten schon wegen des immensen Umfangs nicht mehr oder nur schwer portieren lassen. Erschwert wird dies zudem durch den eben angesprochenen Aspekt fehlender Standards zur Kommunikation zwischen Providern, aber auch wegen der fehlenden unmittelbaren technischen Verbindung zwischen ihnen. Jeder Cloudanbieter verhalte sich zudem so, als sei er der einzige auf dem Markt.[452] Dies führt dazu, dass Nutzer die Daten erst mühselig herunterladen müssen, um sie dann anschließend beim nächsten Provider wieder hochzuladen oder per Datenträger einzuschicken. Die Hauptschwierigkeit der Portierung ergibt sich für die Endnutzer vor allem aus dem Umstand, dass die ihnen zur Verfügung stehenden Bandbreiten noch oft zu gering sind.[453]

2.4.1.2.3 Oligopolbildung und marktbeherrschende Stellung

Insbesondere auf dem Markt der Public Clouds besteht die Gefahr eines Oligopols weniger Anbieter und einer oder mehrerer marktbeherrschender Stellungen. Angesichts der Notwendigkeit von Großrechenzentren ist auch nicht absehbar, dass sich neue und große Cloudanbieter kurzfristig am Markt positionieren. Eine vergleichsweise schnelle Positionierung gelingt nur Unternehmen, die ihre vorhandenen Rechenzentren und Serverparks für Cloud Computing umrüsten, was jedoch ebenfalls ein Mindestmaß an Zeit und Investionen erfordert.[454] Mit der Etablierung des Geschäftsmodells wird aber auch mittelfristig die Zahl der größeren Anbieter steigen. Im Jahr 2011 ist die Zahl der großen Cloudanbieter und Cloudangebote überschaubar und wird von den altbekannten IT-Branchengrößen dominiert. Diese verfügen über die nötige Infrastruktur, das Know-how, qualifizierte Mitarbeiter und die Bekanntheit am Markt.[455]

2.4.1.2.4 Gefahr der Profilbildung und Weitergabe von Daten

Weil die On-Demand-Nutzung für die Abrechnung protokolliert werden muss, ist es nicht auszuschließen, dass ein Provider oder ein beteiligtes Subunternehmen Nutzungsprofile erstellt. Außerdem könnten Inhaltsdaten eingesehen und ausgewertet

---

451 *Münch/Essoh/Doubrava*, <kes> Special - Sicheres Cloud Computing, März 2011, 10.

452 *Biermann*, Cloud-Dienste sind noch am Anfang, http://www.zeit.de/digital/internet/2011-05/cloud-vint-cerf.

453 *Biermann*, Cloud-Dienste sind noch am Anfang, http://www.zeit.de/digital/internet/2011-05/cloud-vint-cerf/seite-2.

454 So zum Beispiel Microsoft mit dem Aufbau seiner Azurecloud; siehe dazu Kap. 2.3.8.4.

455 Siehe dazu auch oben Kap. 2.3.8.

werden. Die Situation ist mit einem Internetprovider vergleichbar, der in der Lage ist die Internetnutzung seiner Kunden detailliert zu analysieren und auszuwerten.[456]

Eine weitere Gefahr besteht darin, dass sich der Provider die Auswertung der Nutzungs- oder sogar von Inhaltsdaten zu eigenen Zwecken, zum Beispiel der Optimierung der Dienste, vom Cloudnutzer einräumen lässt und dann diese zunächst erlaubt zustande gekommenen Erkenntnisse unerlaubt an Dritte, oft Werbeunternehmen, weitergibt.

Hinsichtlich eines solchen missbräuchlichen Vorgehens ist allerdings zu beachten, dass strafrechtliche und datenschutzrechtliche Vorschriften bestehen, die eine gewisse Hemmschwelle bilden. Es ist allerdings nicht auszuschließen, dass Vorschriften im Ausland die Profilbildung oder Weitergabe erlauben, ohne dass ein Nutzer im Inland rechtlich effektiv dagegen vorgehen könnte.

2.4.1.2.5 Bedrohungen

Als weiteren Nachteil gibt es, jeder Informationstechnologie inhärente, allgemeine Bedrohungen und daneben zusätzlich spezifische und neuartige Bedrohungen, die der Cloudtechnologie eigen sind.[457] Letztere ergeben sich nicht nur für die Daten in der Cloud, sondern die Cloudtechnologie selbst erzeugt ihrerseits neue Bedrohungen, beispielsweise den Missbrauch der enormen Rechenleistung. Vor allem die übliche Praxis der Anmeldung mittels Kreditkartendaten ermöglicht den anonymen Missbrauch von Clouddiensten, wenn diese Kreditkartendaten gestohlen wurden.[458]

Neben informationstechnischen Auswirkungen haben Bedrohungen auch regelmäßig einen darüberhinausgehenden negativen Effekt, beispielsweise indem finanzielle Schäden entstehen oder Persönlichkeitsrechte von Betroffenen beeinträchtigt werden.

---

[456] Zur Auswertungsmöglichkeit durch den Internetprovider siehe auch unten die Ausführungen zur Deep Packet Inspection in Kap. 3.8.1.1.

[457] Siehe dazu ausführlich Kap. 3.1.9.8.

[458] Siehe hierzu auch *Galante/Yasu*, Amazon.com Server Said to Have Been Used in Sony Attack, http://www.bloomberg.com/news/2011-05-13/sony-network-said-to-have-been-invaded-by-hackers-using-amazon-com-server.html und Kap. 4.5.6.

3 Rechtsrahmen und rechtliche Aspekte des Cloud Computing

Die rechtlichen Aspekte und der rechtliche Rahmen, innerhalb dessen sich die relevanten Rechtsfragen zu Cloud Computing abspielen, sind nicht gänzlich neu. Ähnliche Rechtsfragen wurden bereits im Rahmen des klassischen IT-Outsourcings oder beim Application Service Providing thematisiert.[459] Cloud Computing hat jedoch die klare Beziehung zwischen Anbieter und Nutzer bei den herkömmlichen Verfahren, insbesondere die Art und den Ort der Leistungserbringung und die Verarbeitung der Daten, intransparent werden lassen und weitgehend globalisiert, so dass die rechtlichen Ausführungen zu den Vorgängermodellen auf Cloud Computing nicht ungeprüft und nur eingeschränkt übertragbar sind. Zu den bisherigen rechtlichen Problemen der Vorgängermodelle kommen außerdem eine Reihe cloudspezifischer Rechtsprobleme hinzu.

Cloud Computing ist auch nicht ein einzelnes kohärentes Bereitstellungsmodell, sondern unterteilt sich in drei Schichten,[460] die unterschiedliche Aspekte (Hardware, Plattformen, Software) betreffen, so dass bereits diese Aufteilung eine direkte Übernahme der rechtlichen Lösungen hinsichtlich der Vorgängermodelle weitgehend ausschließt.

Die rechtlichen Aspekte umfassen dabei Datenschutzrecht, Vertragsrecht, aber auch Urheberrecht, Kartellrecht oder Strafprozessrecht. Auch rechtliche Bezüge zum Recht anderer Staaten, namentlich den USA, sind näher zu beleuchten. Abschließend sollen Empfehlungen zur Rechtsgestaltung formuliert werden.

Bevor auf die für Cloud Computing relevanten Datenschutzvorschriften eingegangen wird, sollen das Datenschutzrecht, dessen Entwicklung und die völker- und europarechtlichen Grundlagen dargestellt werden.

3.1 Datenschutzrecht

3.1.1 Entwicklung des Datenschutzrechts

Die Ursprünge des modernen Datenschutzrechts liegen in den Vereinigten Staaten von Amerika. In den 60er Jahren des vorherigen Jahrhunderts waren „Right to Privacy“ und „Right to be let alone“ Schlagworte in Diskussionen zwischen Soziologen und Publizisten.[461] Diese Abwehrrechte wurden bereits 1890 von Juristen in einem Artikel formuliert und gelten als Ausgangspunkt der Privatheitsdebatte.[462] Die Diskussionen hierüber sensibilisierten eine breitere Öffentlichkeit über die Gefahren elektronischer Datenverarbeitung. Die Debatte mündete schließlich in zwei

---

459 Siehe dazu auch die Abgrenzungsfragen in Kap. 2.3.6.

460 Siehe dazu oben Kap. 2.3.1.

461 *Abel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 2.7, Rn. 9; *Grimm/Roßnagel*, DuD 2000, 447.

462 *Warren/Brandeis*, Harvard Law Review 4, 1890, 198 ff.

sektoralen Datenschutzgesetzen, nämlich dem Fair Credit Reporting Act[463] aus dem Jahr 1970 und dem Privacy Act aus dem Jahr 1974.[464]

Im Gegensatz zur amerikanischen Sicht zielt der europäisch geprägte Datenschutz nicht auf den Ausschluss von Kommunikation, der vor allem im „Right to be let alone“ seinen Ausdruck findet, sondern auf die Ermöglichung selbstbestimmter Kommunikation ab. Datenschutz soll nicht den Schutz des Sonderlings, der sich von der Außenwelt abschotten will, sondern den Schutz von selbstbestimmt in der Gesellschaft agierenden und kommunizierenden Individuen ermöglichen.[465]

Das weltweilt erste Datenschutzgesetz trat am 30.9.1970 im Land Hessen in Kraft. Dieses Gesetz verwendete auch erstmalig das Wort „Datenschutz“, dessen eigentlicher Ursprung allerdings nicht bekannt ist.[466] Als zweites Bundesland erließ Rheinland-Pfalz am 24.1.1974 ein Landesdatenschutzgesetz.[467] Auf Bundesebene trat am 1.1.1978 das Bundesdatenschutzgesetz in Kraft.[468] Das weltweit erste, national geltende, Datenschutzgesetz gab es bereits schon fünf Jahre früher, nämlich im Jahr 1973, in Schweden.[469]

Ein weiterer Meilenstein und Höhepunkt in der Entwicklung des nationalen Datenschutzrechts war das Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983. Dieses entwickelte und benannte die informationelle Selbstbestimmung als Grundrecht. Dessen Grundgedanke ist das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.[470]

Ein letztes großes Kapitel in der Ausbildung des europäischen Datenschutzrechts war der Erlass der Allgemeinen Datenschutzrichtlinie[471] (DSRL) am 24.10.1995 und das damit einhergehende einheitliche Datenschutzniveau innerhalb der EU und des EWR.

---

463 Title 15 U.S.C., § 1681, http://www.law.cornell.edu/uscode/15/1681.html.

464 Title 5 U.S.C., § 552a, http://www.law.cornell.edu/uscode/5/552a.html; *Abel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 2.7, Rn. 10; zu Letzterem siehe auch weiter unten Kap. 3.1.12.5.3.

465 *Roßnagel* 2007, 112.

466 *Abel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 2.7, Rn. 12.

467 *Gola/Schomerus* 2010, Einleitung, Rn. 1.

468 Eine chronologische Übersicht über die einzelnen Datenschutzgesetze findet sich beim *Landesdatenschutzbeauftragten des Landes Baden-Württemberg*, Datenschutzentwicklung im Zeitraffer, http://www.baden-wuerttemberg.datenschutz.de/aktuell/ldsg/zeitraffer.htm.

469 *Burkert*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 2.3, Rn. 14.

470 BVerfGE 65, 1; weitere Einzelheiten zum Urteil siehe auch in Kap. 3.1.3.1.

471 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html; auch als „Europäische Datenschutzrichtlinie“ bekannt; zu Einzelheiten siehe sogleich Kap. 3.1.2.2.1.

Im Laufe der letzten Jahre ist der Regelungsgehalt und die Regelungsfähigkeit des einfachen Datenschutzrechts im Vergleich zur technischen Entwicklung und der damit verbundenen sozialen Durchdringung im Alltag ins Hintertreffen geraten. Insbesondere das Internet mit seinen vielfältigen Diensten und Nutzungsmöglichkeiten hat dabei einen wesentlichen Anteil. Zwar gab es sporadische Novellierungen der Datenschutzgesetze, jedoch wurden umfassende und in sich kohärente Modernisierungsansätze[472] nie umgesetzt, so dass das Datenschutzrecht, neben der immer weitläufigeren sektoralen Auffächerung, auch inhaltlich immer unübersichtlicher wird und mit den unzähligen Ausnahmen und Einzelfallregelungen unmittelbar davor steht in sich widersprüchlich zu werden.

3.1.2 Zwischenstaatliche Regelungen zum Datenschutz

Das nationale Datenschutzrecht basiert auf unterschiedlichen normativen Ebenen und wird von diesen unterschiedlich stark beeinflusst.[473] Dabei kann zwischen international geltenden Regeln und Abkommen, also Völkerrecht, und europarechtlichen Regelungen, überwiegend Gemeinschaftsrecht, unterschieden werden.

3.1.2.1 Internationale Abkommen

Regelungen zum Datenschutz oder zum Umgang und Schutz personenbezogener Daten finden sich in grundlegenden völkerrechtlichen Abkommen nicht unmittelbar und können lediglich aus allgemeineren Normen abgeleitet werden kann. So garantiert beispielsweise Art. 12 der Allgemeinen Erklärung der Menschenrechte[474] der Vereinten Nationen (UN) den Schutz der Freiheitssphäre des Einzelnen, wozu nach Satz 1 auch ausdrücklich das Privatleben gehört. Wegen der fehlenden Bindungswirkung hat diese Garantiefunktion allerdings nur symbolischen Charakter.[475]

Ein weiterer im Rahmen der Vereinten Nationen zustande gekommener völkerrechtlicher Vertrag mit Menschenrechtsgarantien und Bezügen zum Datenschutzrecht ist der Internationale Pakt über bürgerliche und politische Rechte (IPbpR)[476] vom 16.12.1966. Art. 17 des Pakts verbietet willkürliche oder rechtswidrige Eingriffe in das Privatleben und ist damit ähnlich offen formuliert wie die Allgemeine Erklärung der Menschenrechte. Im Gegensatz zu dieser ist der Pakt allerdings rechtsverbind-

---

472 Zum Beispiel *Roßnagel/Pfitzmann/Garstka* 2001, 1 ff. oder auch das Eckpunktepapier der Konferenz der Datenschutzbeauftragten des Bundes vom 18.3.10; eine zeitliche Übersicht über bisherige Ansätze und die Forderungen nach einer Modernisierung findet sich beim *Bundesbeauftragten für Datenschutz*, Modernisierung des Datenschutzrechts - eine zeitliche Übersicht, http://www.bfdi.bund.de/DE/Schwerpunkte/ModernisierungDS/Artikel/Chronologie.html;jsessionid=9720E50C93DD6CD5BE870804FD552769.1_cid134?nn=1091786.

473 *Hornung* 2005, 131.

474 Resolution 217 A (III) vom 10.12.1948, http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=ger.

475 *Schnabel* 2009, 44.

476 Resolution 220 A (XXI) vom 16.12.1966, http://www2.ohchr.org/english/law/ccpr.htm; auch als UN-Zivilpakt bekannt.

lich, weil dieser durch die unterzeichnenden Staaten ratifiziert werden musste.[477] Betroffene Bürger können, soweit der nationale Rechtsweg erschöpft ist und ein Zusatzprotokoll[478] unterzeichnet wurde, mittels Individualbeschwerde den UN-Menschenrechtsausschuss anrufen. Nicht zuletzt wegen dieser Rechtswegserschöpfung wird allerdings deutlich, dass die völkerrechtlichen Abkommen in der Datenschutzpraxis keine Rolle spielen.

Daneben sind noch die Richtlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten[479] der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) zu erwähnen. Als Leit- oder Richtlinien sind diese unverbindlich.[480]

3.1.2.2 Europarecht und Europäische Abkommen

3.1.2.2.1 EU-Ebene

Eine wichtige Regelung auf EU-Ebene ist Art. 8 der Europäischen Grundrechtecharta (GRC).[481] Die Charta ist seit dem 1.12.2009 rechtlich bindend soweit die Mitgliedsstaaten Unionsrecht ausführen. Art. 8 GRC regelt ausdrücklich den „Schutz personenbezogener Daten“. In Art. 8 Abs. 2 GRC werden sogar einige Datenschutzprinzipien, wie beispielsweise die Zweckbindung, angeführt. Flankiert wird Art. 8 GRC durch den allgemeineren Art. 7 GRC, nämlich die „Achtung des Privat- und Familienlebens“. Vor der verbindlichen Geltung der Grundrechtecharta und der Bezugnahme des bis 30.11.2009 geltenden Art. 6 Abs. 2 EUV a. F. auf die EMRK war bereits die Rechtsprechung des EuGH durch die Aufstellung allgemeiner Rechtsgrundsätze, die den Rechtsordnungen der Mitgliedsstaaten gemeinsam sind, schon früh auch datenschutzorientiert. Dieser hat bereits im Jahr 1969 die Grundrechtsqualität des Datenschutzes anerkannt.[482]

Im Sekundärrecht ist die Allgemeine Datenschutzrichtlinie als wichtigste Regelung zu nennen.[483] Sie erzeugt in den Mitgliedsstaaten Datenschutzmindeststandards und damit zugleich ein einheitliches Basisniveau für den Datenschutz. Die Harmonisierung soll allerdings nicht dazu führen, dass eine „Angleichung nach unten“ erfolgt, so dass die Mitgliedsstaaten auch höhere und über die Richtlinie hinausgehende

---

477 Die Bundesrepublik hat den Pakt am 17.12.1973 ratifiziert.

478 5. optionales Zusatzprotokoll vom 23.3.1976, http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-5&chapter=4&lang=en.

479 Richtlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten vom 23.9.1980, http://www.oecd.org/dataoecd/16/7/15589558.pdf

480 Näheres dazu bei *Schnabel* 2009, 49.

481 Eigentlich „Charta der Grundrechte der Europäischen Union“, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0001:0016:DE:PDF.

482 EuGH, Slg.1969, I-419 (Stauder/Stadt Ulm); *Hornung* 2005, 136.

483 Siehe Fn. 471.

Datenschutzstandards etablieren können.[484] In der Bundesrepublik ist die Datenschutzrichtlinie erst nach der Einleitung eines Vertragsverletzungsverfahrens durch das Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18.5.2001 umgesetzt worden. Ein später eingeleitetes Vertragsverletzungsverfahren betraf die mangelnde Unabhängigkeit der Datenschutzaufsichtsbehörden.[485] Für datenschutzrechtlich relevante Sachverhalte hat die Richtlinie als Auslegungshilfe Bedeutung, soweit nationale Vorschriften nicht eindeutig sind. Behörden und Gerichte sind nach der EUGH-Rechtsprechung zudem zur richtlinienkonformen Auslegung verpflichtet.[486]

Eine weitere Regelung zum Datenschutz, die im Zusammenhang mit Cloud Computing erwähnenswert erscheint, ist die Datenschutzrichtlinie für elektronische Kommunikation, die im Telekommunikationsbereich Anwendung findet.[487]

3.1.2.2.2 Europaratsebene

Die Mitgliedsstaaten des Europarats haben bereits am 4.11.1950 die Europäische Menschenrechtskonvention[488] (EMRK), auf die die EU-Grundrechtecharta zum Teil verweist, unterzeichnet. Die EMRK ist seit der Ratifikation am 5.12.1952 in Deutschland geltendes Recht. Die Einhaltung der Konvention wird durch den Europäischen Gerichtshof für Menschenrechte (EGMR) gewährleistet. Im Gegensatz zur Grundrechtecharta fehlt eine spezielle Regelung über den Schutz personenbezogener Daten. Es ist lediglich eine mit Art. 7 GRC vergleichbare Norm in Art. 8 EMRK, die ganz ähnlich als „Recht auf Achtung des Privat- und Familienlebens“ beschrieben ist, vorhanden. Der EGMR hat allerdings mehrfach geurteilt, dass die Sammlung und Speicherung personenbezogener Daten in die Rechte aus Art. 8 Abs. 1 EMRK eingreift und einer Rechtfertigung bedarf, die ihrerseits den Anforderungen aus Art. 8 Abs. 2 EMRK genügen muss.[489] Zudem haben die Mitgliedsstaaten des Europarats am 28.1.1981 das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten[490] vereinbart, das in

---

484 *Simitis*, NJW 1998, 2473; *Roßnagel/Pfitzmann/Garstka* 2001, 55 ff.; *Schnabel* 2009, 44.

485 Einzelheiten dazu und zum entsprechenden EUGH-Urteil, siehe bei *Briegleb*, EU-Kommission mahnt unabhängige Datenschutzaufsicht an, http://www.heise.de/newsticker/meldung/EU-Kommission-mahnt-unabhaengige-Datenschutzaufsicht-an-1223241.html.

486 EuGH, Slg. 1984, I-1891 (Colson, Kamann/Land Nordrhein-Westfalen).

487 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:DE:NOT.

488 Sie trat am 3.9.1953 allgemein in Kraft; die deutsche Fassung ist unter http://conventions.coe.int/Treaty/ger/Treaties/Html/005.htm abrufbar.

489 *Hornung* 2005, 134; maßgebliche Urteile waren Leander/Schweden, Urteil vom 26.3.1987, Z./Finnland, Urteil vom 25.2.1997 und Amann/Schweiz, Urteil vom 16.2.2000.

490 Abrufbar unter http://conventions.coe.int/treaty/ger/treaties/html/108.htm.

Deutschland am 19.6.1985 ratifiziert wurde. Zum Abkommen wurden noch weitere Zusatzprotokolle vereinbart.[491]

Ebenso wie die EMRK ist die Europäische Datenschutzkonvention[492] vom 28.1.1981 ein völkerrechtlicher Vertrag, der von den Mitgliedsstaaten des Europarats vereinbart wurde. Die Konvention beinhaltet grundlegende Datenschutzprinzipien, zum Beispiel den Zweckbindungsgrundsatz (Art. 5 b.) oder das Erforderlichkeitsprinzip (Art 5 e.), die von den Unterzeichnerstaaten in nationales Recht umzusetzen sind.[493] Sie ist die einzige bindende völkerrechtliche Vereinbarung, die ausschließlich den Datenschutz als Regelungsinhalt hat.[494] Für Cloud Computing hat sie insoweit Bedeutung, dass sie zukünftig auch gerade darauf und auf soziale Netzwerke angepasst werden soll.[495]

3.1.3 Nationales Verfassungsrecht

Das nationale Datenschutzrecht hat seine Grundlagen im Verfassungsrecht und der Rechtsprechung des Bundesverfassungsgerichts. Auch für Cloud Computing und die KORA-Methode spielt Verfassungsrecht eine erhebliche Rolle, so dass sich im Folgenden die Darstellung und Erläuterung der einschlägigen Grundrechte anbietet.

3.1.3.1 Recht auf informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung ist dem Volkszählungsurteil zufolge „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“.[496] Er soll dadurch in die Lage versetzt werden, selbstbestimmt entscheiden zu können, welche Daten und damit letztlich welches Bild er von sich selbst preisgeben und darstellen will.[497] Wer nämlich „nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt

---

491 Zu weiteren Einzelheiten siehe *Hornung* 2005, 134 ff

492 Eigentlich „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108)“, http://conventions.coe.int/Treaty/GER/Treaties/Html/108.htm.

493 Der Konvention sind bisher 38 Staaten beigetreten; http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=2&DF=10/4/2006&CL=GER.

494 *Schnabel* 2009, 48; ähnlich der Hinweis in der Resolution Nr. 3 der 30. Justizministerkonferenz vom 26.11.2010, dort Nr. 10, http://www.coe.int/t/dghl/standardsetting/minjust/mju30/MJU-30%20_2010_%20RESOL%203%20E%20final.pdf.

495 Resolution Nr. 3 der 30. Justizministerkonferenz vom 26.11.2010, http://www.coe.int/t/dghl/standardsetting/minjust/mju30/MJU-30%20_2010_%20RESOL%203%20E%20final.pdf; siehe dazu auch Kap. 3.10.

496 BVerfGE 65, 1; siehe auch bereits weiter oben die Erwähnung bei der historischen Entwicklung des Datenschutzes.

497 Zum Gedanken der Selbstdarstellung und der Rückspiegelung siehe *Roßnagel* 2007, 109 und *ders.* MMR 2003, 693.

sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.“[498]

Das aus dem allgemeinen Persönlichkeitsrecht entwickelte Recht ist als ungeschriebenes Grundrecht anerkannt.[499] Das Volkszählungsurteil erging 1983 und damit 13 Jahre, nachdem das einfache Datenschutzrecht bereits existierte.[500] Das Urteil baute auf rechtsdogmatischen Vorarbeiten von Datenschutzexperten auf und ist im Kontext der damaligen Diskussion um die, ursprünglich bereits für 1981 geplante, Volkszählung zu sehen.[501]

Während sich die dem Urteil zugrundeliegende Verfassungsbeschwerde gegen eine staatliche Maßnahme richtete, hat der Schutz der informationellen Selbstbestimmung mittlerweile vor allem gegenüber Privaten Bedeutung erlangt. Das Fortschreiten der Technik und daraus resultierende neuartige Gefährdungslagen sind damit nur selten staatlichem Handeln geschuldet.[502] Nicht zuletzt deshalb, weil Technik, wie zum Beispiel Cloud Computing, primär von Privaten entwickelt und eingesetzt wird.

Das Grundrecht hat, neben der subjektiven Komponente der selbstbestimmten Entwicklung und Entfaltung des Einzelnen, auch, wie die meisten Grundrechte, einen objektiven Einschlag.[503] Informationelle Selbstbestimmung ist „zugleich die Grundlage einer freien und demokratischen Kommunikationsverfassung“.[504] Sie ist nämlich „eine elementare Funktionsbedingung eines auf Handlungs- und

---

498 BVerfGE 65, 43.

499 Siehe zum Beispiel *Roßnagel*, MMR 2003, 693 oder *ders.* 2007, 108, der sogar eine ständige Rechtsprechung des Bundesverfassungsgerichts zur Frage der Grundrechtsqualität sieht; andere sind allerdings der Auffassung, dass das Recht auf informationelle Selbstbestimmung kein neues Grundrecht sei, sondern eine bloße Fortschreibung des allgemeinen Persönlichkeitsrechts; so beispielsweise *Schiedermair*, in: Dörr/Kreile/Cole, Handbuch Medienrecht, 286; für diese Auffassung könnte auch der Wortlaut des § 1 Abs. 1 BDSG sprechen, der den Zweck des Gesetzes im Schutz vor Beeinträchtigungen des Persönlichkeitsrechts sieht; das BVerfG erwähnt allerdings in BVerfGE 34, 280 ausdrücklich das „Grundrecht auf Datenschutz“ oder spricht in BVerfGE 67, 143 von „grundrechtlichem Datenschutz“, so dass die abweichende Ansicht nur schwer aufrechtzuerhalten sein dürfte und einiges für eine ständige Rechtsprechung spricht; unstreitig dürfte allerdings sein, dass der Datenschutz Verfassungsrang hat; so auch *Hornung* 2005, 138 und dortige Fn. 752.

500 Siehe dazu oben die historische Entwicklung in Kap. 3.1.1.

501 *Roßnagel*, MMR 2003, 693, der in diesem Zusammenhang *Podlech*, *Steinmüller* und *Mallmann* erwähnt; siehe dazu *Podlech*, DVR 1976, 23 ff., *ders*. 1976, 313, *ders.* 1982, 453 und *Steinmüller/Lutterbeck/Mallmann/Harbort/Kolb/Schneider* 1971, 88 ff.

502 Der Staat macht sich allerdings solche Techniken manchmal zueigen; zu denken wäre beispielsweise an die Vorratsdatenspeicherung und maschinelle Auswertung der Vorratsdaten oder auch die Onlinedurchsuchung mittels staatlicher Trojanersoftware, bei der sich der Staat den Methoden von Cyberkriminellen bedient.

503 *Roßnagel* 2007, 110 f.; zum objektiven Aspekt der Grundrechte siehe Kap. 3.2.2.

504 *Roßnagel*, MMR 2003, 694; *ders.* 2007, 110.

Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens".[505] Als Grundrecht ist sie Teil einer „objektiven Wertordnung, die als verfassungsrechtliche Grundentscheidung für alle Bereiche des Rechts gilt und Richtlinien und Impulse für Gesetzgebung, Verwaltung und Rechtsprechung gibt".[506]

Informationelle Selbstbestimmung soll demzufolge zweierlei gewährleisten, nämlich den selbstbestimmten Informationsaustausch und eine freie demokratische Willensbildung.[507]

3.1.3.2 Vertraulichkeit und Integrität informationstechnischer Systeme

Weniger klassisch datenschutzbezogen, aber mit Bedeutung für den technischen Datenschutz und Daten an sich, ist das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme. Dieses im Jahr 2008 vom Bundesverfassungsgericht ebenfalls aus dem allgemeinen Persönlichkeitsrecht abgeleitete (neue) Grundrecht ist als eine Art Auffanggrundrecht ausgestaltet, das Schutzlücken füllen soll, die im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse aufgetreten sind.[508]

Vom Grundrecht ist nach dem Urteil des Gerichts zunächst „das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben" gegeschützt.[509] Daneben ist, wie die Benennung des Grundrechts bereits besagt, auch das Integritätsinteresse vom Schutzbereich umfasst. In die Integrität eines informationstechnischen Systems wird dann eingegriffen, „wenn auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen".[510]

Das Grundrecht beschränkt sich auf IT-Systeme, „die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten". Vertraulichkeits- und Integritätsinteresse sind allerdings nur geschützt, „soweit der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen

---

505 BVerfGE 65, 43.

506 BVerfGE 7, 205; BVerfGE 39, 41; BVerfGE 35, 114 mwN.

507 *Roßnagel* 2007, 110.

508 *Roßnagel/Schnabel*, NJW 2008, 3534; BVerfG, NJW 2008, 824.

509 BVerfG, NJW 2008, 824; von *Roßnagel/Schnabel*, NJW 2008, 3534 prägnant als „Vertraulichkeitsinteresse" bezeichnet.

510 BVerfG, NJW 2008, 827.

zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt".[511]

Für Cloud Computing stellt sich die Frage, ob ein Cloudnutzer über die genutzten Services und Systeme „verfügt". Das Gericht hat dieses allgemeine – nicht nur cloudspezifische –Problem jedoch erkannt. Soweit nämlich „die Nutzung des eigenen informationstechnischen Systems über informationstechnische Systeme stattfindet, die sich in der Verfügungsgewalt anderer befinden, erstreckt sich der Schutz des Nutzers auch hierauf".[512] Der Cloudnutzer hat auf allen Cloudebenen einen gewissen Einfluss auf die Dienste und Systeme, beispielsweise indem er Daten in eine Onlinemaske eingibt oder Daten hochlädt, so dass diese Systeme, nicht zuletzt auch wegen der Anmietung, als „eigene" anzusehen sind. Die eigene Nutzung und Verfügung wird bei IaaS-Angeboten mit ihren umfassenden Steuerungsmöglichkeiten durch den Nutzer besonders deutlich.

3.1.3.3 Telekommunikationsgeheimnis

Durch Cloud Computing ist, wenn auch nur am Rande, das Telekommunikationsgeheimnis[513] aus Art. 10 GG betroffen.[514] Clouddienste werden über das Internet und damit über Telekommunikationsdienste vermittelt. Das Grundrecht „gewährleistet die Vertraulichkeit der individuellen Kommunikation, wenn diese wegen der räumlichen Distanz zwischen den Beteiligten auf eine Übermittlung durch andere angewiesen ist und deshalb in besonderer Weise einen Zugriff Dritter ermöglicht".[515] Es hat somit für den Schutz der in und aus der Cloud übermittelten Daten Bedeutung. Der Datentransport über Telekommunikationsleitungen und durch Telekommunikationsunternehmen ermöglicht Ausspähungen und Manipulationen, insbesondere durch Bedienstete der Telekommunikationsunternehmen, die gerade durch das Grundrecht und seine einfachgesetzlichen Ausprägungen in § 88 TKG oder § 206 StGB verhindert werden sollen. Wegen des engen Anwendungsbereichs des Fernmeldegeheimnisses handelt es sich im Vergleich zur informationellen Selbstbestimmung lediglich um ergänzenden Grundrechtsschutz.

3.1.3.4 Wirtschaftsgrundrechte

Während die eben dargestellten Grundrechte persönlichkeitsrechtlich geprägt sind und im Cloudkontext den Schutz personenbezogener Daten gewährleisten, haben die Eigentumsfreiheit aus Art. 14 Abs. 1 GG und die Berufs- und Betätigungsfrei-

---

511 BVerfG, NJW 2008, 827.

512 BVerfG, NJW 2008, 827; siehe dazu auch *Hornung*, CR 2008, 303 oder *Roßnagel/Schnabel*, NJW 2008, 3538, die als Beispiel eine Onlinefestplatte, also Cloudstorage, als „eigenes System" ansehen.

513 Auch als Fernmeldegeheimnis bekannt.

514 Einzelheiten zur Nebenläufigkeit des TK-Rechts siehe sogleich in Kap. 3.1.4.1.

515 BVerfGE 115, 181.

heit aus Art. 12 Abs. 1 GG als sogenannte Wirtschaftsgrundrechte für den Schutz von Geschäfts- und Betriebsgeheimnissen Bedeutung.[516]

Die Heranziehung der beiden Grundrechte als verfassungsrechtliche Grundlage für den Schutz der Geschäfts- und Betriebsgeheimnisse ist umfassend anerkannt, allerdings ist umstritten, welches Grundrecht genau anwendbar sein soll.[517] Viele differenzieren allerdings überhaupt nicht und sehen beide Grundrechte gleichermaßen, meist ohne nähere Begründung, als einschlägig an.[518] Im Folgenden sollen dennoch kurz die Argumente der differenzierenden Meinungen dargestellt werden.

Die Befürworter der Eigentumsgarantie stellen auf die große wirtschaftliche Bedeutung der Betriebs- und Geschäftsgeheimnisse für Unternehmen ab und betonen die mit Immaterialgüterrechten vergleichbare Funktion. Immaterialgüterrechte habe das Bundesverfassungsgericht aber in Form von Urheberrechten[519] und patentierten Erfindungen[520] als Eigentum im Sinne des Art. 14 Abs. 1 GG anerkannt.[521] Darüber hinaus habe ihre Funktion als „geronnene wirtschaftliche Leistung“ in Form der einfachgesetzlichen Schutzvorschriften Anerkennung gefunden.[522]

Die Befürworter des Art. 12 Abs. 1 GG als Grundlage argumentieren hingegen damit, dass die rechtliche Zuordnung der Betriebs- und Geschäftsgeheimnisse darauf beruhe, den Berechtigten vor einer Ausspähung zu schützen und dies gerade keine Zuordnung eines Rechtsobjekts zu einem Rechtsinhaber bewirke, sondern gerade deswegen erst notwendig werde, weil das Schutzobjekt, nämlich die geschützte Information, dem Inhaber gerade nicht rechtlich, sondern nur tatsächlich zugeordnet sei und damit Art. 14 Abs. 1 GG nicht einschlägig sein könne.[523]

Die vorgebrachten Argumente, die gegen Art. 14 Abs. 1 GG sprechen, sind berechtigt, da es gerade darum geht, die unbefugte Verwertung von Geheimnissen (Know-How) zu unterbinden. „Normale“ Immaterialgüterrechte sind aber in der Regel öffentlich, zum Beispiel Patente, so dass es bei diesen gerade nicht auf den Schutz vor Ausspähung ankommt. Know-how ist außerdem oft keine patentfähige Erfindung und erfüllt auch meistens nicht die Kriterien für andere Schutzrechte, wie etwa Ur-

---

516 *Breuer*, NVwZ 1986, 174; *Wolff*, NJW 1997, 99; Art. 14 i.V.m. Art. 19 Abs. 3 GG schützt außerdem auch das Steuergeheimnis, soweit Unternehmen als Grundrechtsträger betroffen sind; siehe dazu auch Kap. 4.3.

517 Zu den einzelnen Positionen siehe *Wolff*, NJW 1997, 99, insbesondere Fn. 17 ff.; zu den Befürwortern des Art. 14 als Grundlage siehe auch *Brammsen*, DÖV 2007, 11 und Fn. 5.

518 Beispielsweise so auch der Gesetzgeber in der Gesetzesbegründung zum Gesetz zur Verbesserung der gesundheitsbezogenen Verbraucherinformation (VIG) in BT-Drs. 16/1408, 11 oder auch durch die Rechtsprechung, beispielsweise OVG Schleswig, NVwZ 2007, 1449; siehe dazu auch *Polenz*, DÖV 2010, 351 f.

519 BVerfGE 31, 238 ff.

520 BVerfGE 36, 290 f.

521 *Wolff*, NJW 1997, 99; *Brammsen*, DÖV 2007, 11, 12.

522 *Wolff*, NJW 1997, 99; zu den einzelnen Schutzvorschriften siehe auch Kap. 3.8.1.2.

523 *Wolff*, NJW 1997, 100 f.

heberrechte oder Gebrauchs- und Geschmacksmuster.[524] Vor allem Verfahren können nicht als Gebrauchsmuster, sondern nur als Patente geschützt werden.

Somit kommt nur Art. 12 Abs. 1 GG als einschlägiges Grundrecht in Betracht.[525] Dieses bietet (auch) Schutz vor der Beeinträchtigung der unternehmerischen Betätigungsfreiheit.[526] Durch den Erlass der einfachgesetzlichen Schutzvorschriften durch den Gesetzgeber, insbesondere die §§ 17 UWG und 203, 204 StGB, ist dem Grundrecht auch einfachrechtlich zwischen Privaten zu seiner mittelbaren Wirkung verholfen worden. Daneben kann durch angepasste Technikgestaltung dem Datenverlust durch Ausspähen vorgebeugt werden, so dass auch dadurch die Grundrechtsverwirklichung gefördert wird.

3.1.4 Cloud Computing als Telekommunikation oder Telemedium?

Vor einer möglichen Anwendung des Bundesdatenschutzgesetzes ist zu prüfen, ob bereichsspezifisches Datenschutzrecht gemäß § 1 Abs. 3 Satz 1 BDSG vorrangig ist. In Betracht kommt zum einen Telekommunikationsrecht und damit das Telekommunikationsgesetz (TKG) und zum anderen Telemedienrecht, mithin bereichsspezifische Vorschriften im Telemediengesetz (TMG).

3.1.4.1 Cloud Computing als Telekommunikationsdienstleistung?

Telekommunikationsdienste sind gemäß § 3 Nr. 24 TKG in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen. Cloud Computing ist kein Telekommunikationsdienst in diesem Sinne. TK-Dienste sind allerdings zwingende Voraussetzung, um Cloudservices über das Internet mittels Telekommunikation, zum Beispiel über Glasfaserstandleitungen, Richtfunk, Fernsehkabel, DSL oder Mobilfunk, anbieten und nutzen zu können. Erst mit der flächendeckenden Durchsetzung breitbandiger Telekommunikationsdienste konnte sich Cloud Computing durchsetzen.[527]

Auch das kombinierte Angebot von TK-Dienstleistungen und Cloudservices durch einen Generalunternehmer ändert nichts an diesem Ergebnis, da die einzelnen Dienstleistungen und Dienste wegen ihrer unterschiedlichen Eigenart getrennt zu betrachten sind.

Clouddienste sind schließlich auch keine telekommunikationsgestützten Dienste im Sinne des § 3 Nr. 25 TKG, weil durch Clouddienste keine mit der Telekommunikationsverbindung zeitgleiche Inhaltsleistung erfüllt wird. Clouddienste sind zudem

---

524 *Schubert*, Know-how-Schutz, http://www.unternehmenswerkstatt-bb.de/K/Know-how-Schutz.html.

525 Ähnlicher Ansicht ist auch das BVerfG, MMR 2006, 375, 382; *Polenz*, DÖV 2010, 357.

526 Zur unternehmerischen Betätigungsfreiheit aus Art. 12 GG siehe BVerfG, MMR 2006, 375 und BVerwGE 71, 183 ff.

527 Siehe oben Kap. 2.3.4.4.

zeitlich und räumlich von der TK-Dienstleistung getrennt. Telekommunikationsgestützte Dienste sind in der Regel Mehrwertdienste, wie zum Beispiel Dienste, die über kostenpflichtige 0900er-Nummern bezogen werden können.

3.1.4.2 Cloud Computing als Telemediendienst?

Schwieriger ist hingegen die Abgrenzung zu den Telemediendiensten. Telemedien oder Telemediendienste werden negativ definiert und sind gemäß § 1 Abs. 1 Satz 1 TMG alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages darstellen.

Bei Telemedien muss es sich also um elektronische Informations- und Kommunikationsdienste handeln. Dies bedeutet, dass die Dienstleistung selbst elektronisch erbracht werden muss. Da Telemediendienste nicht den Bereich der Übertragung, also Telekommunikation, betreffen, muss sich die elektronische Erbringung auf die Bereitstellung der Inhalte für den Dienst beziehen. Entscheidend ist somit, ob die für den Dienst erforderlichen Inhalte elektronisch bereitgestellt werden.[528]

Die meisten Clouddienste sind demnach als Telemedien anzusehen.[529] Insbesondere Software-as-a-Service- und Platform-as-a-Service-Anwendungen sind wegen der Bereitstellung von Inhalten, sprich der zu nutzenden Software, als Telemedien einzuordnen. Infrastructure as a Service hingegen wird dagegen, je nach webseitiger Implementierung, nicht als Telemedium anzusehen sein.[530] Es werden dabei keine Inhalte im Sinne von Informationsdiensten bereitgestellt, sondern das Management von entfernt verfügbaren Infrastrukturen und Ressourcen ermöglicht. Allerdings ist zuzugestehen, dass dieses Management kommunikationsorientiert über das Internet erfolgt, so dass man auch die Ansicht vertreten kann, dass diese ebenfalls Telemedien darstellen. Je feingranularer und detaillierter die Steuerung über die Weboberfläche und je höher der darin enthaltende Informationsgehalt, umso eher ist rechtlich ein Telemedium annehmbar.

3.1.4.3 Konsequenzen für den Datenschutz und Abgrenzung

Rechtlich hat diese Einordnung für die hier zu behandelnden personenbezogenen Daten *in* den Clouddiensten allerdings keine Bedeutung. Die Datenschutzvorschrif-

---

528 *Holznagel/Ricke*, in: Spindler/Schuster, Recht der elektronischen Medien, 12. Teil, TMG, § 1, Rn. 4.

529 So auch *Heidrich/Wegener*, MMR 2010, 805; zum Teil („in der Regel“) anderer Auffassung und ohne weitere Begründung *Nägele/Jacobs*, ZUM 2010, 290.

530 So auch *Heidrich/Wegener*, MMR 2010, 805, die für IaaS die Parallele zu einem Content Provider gemäß § 10 TMG ziehen, soweit Hosting im Vordergrund steht.

ten der §§ 11 ff. TMG und insbesondere die §§ 14 und 15 TMG regeln nämlich nur die Bestands-, Nutzungs- und Abrechnungsdaten, die im Rahmen der Bereitstellung und Nutzung eines Telemediendienstes anfallen.[531] Dies wären die Nutzungs- und Bestandsdaten der die Cloudservices nutzenden Kunden. Diese sind, soweit natürliche Personen betroffen sind, auch schützenswert, jedoch stellen sie keine Inhaltsdaten dar.[532] Inhaltsdaten sind alle Daten, die mit Hilfe eines Telemediendienstes übermittelt werden, um die durch den Telemediendienst begründeten Leistungs- und Rechtsverhältnisse zu erfüllen.[533]

Solche Inhaltsdaten, also die konkreten personenbezogenen Daten der von der ausgelagerten Datenverarbeitung Betroffenen, die in den Cloudrechenzentren genutzt, verarbeitet und an diese und die Cloudnutzer übermittelt werden, unterfallen nach herrschender Meinung den allgemeinen Grundsätzen und damit dem Regelungsregime des Bundesdatenschutzgesetzes oder der Landesdatenschutzgesetze.[534]

Ein Teil der Literatur ordnet die Inhaltsdaten als Unterfall von Nutzungsdaten ein, was sich aus § 12 Abs. 1 TMG ergeben soll. Nutzungsdaten seien solche personenbezogenen Daten, die erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen.[535] Es gehe dabei um die Nutzung an sich.[536]

Gegen diese Sicht spricht aber, dass Inhaltsdaten, im Gegensatz zu Nutzungsdaten, gerade nicht notwendigerweise während oder durch die Nutzung der Telemedien anfallen und sie auch nicht erforderlich sind, um die Inanspruchnahme der Telemedien zu ermöglichen.[537] Die zum Cloudprovider übermittelten personenbezogenen Daten werden überwiegend schon vor der Nutzung erhoben und grundsätzlich mittels eines Telemediums in die Cloud eingebracht, so dass sie nur ausnahmsweise während der Nutzung anfallen, beispielsweise wenn Daten „live“ in eine Eingabemaske eingetragen werden, um einen Datensatz neu anzulegen. Sie sind auch nicht erforderlich, um die Inanspruchnahme oder die Abrechnung zu ermöglichen. Die Inhaltsdaten werden übermittelt, um den Vertrag zwischen dem Provider und dem Nutzer zu erfüllen. Der Provider soll die, regelmäßig bereits erhobenen, Daten des Nutzers speichern oder in irgendeiner Form (weiter)verarbeiten. Dass dabei zeitwei-

---

[531] *Spindler/Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, 12. Teil, TMG, § 11, Rn. 6; *Heidrich/Wegener*, MMR 2010, 805.

[532] Zum Begriff und dem vermeintlichen Streit darum siehe *Spindler/Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, 12. Teil, TMG, § 11, Rn. 6 und § 15, Rn. 3.

[533] *Roßnagel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 7.9, Rn. 59.

[534] *Spindler/Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, 12. Teil, TMG, § 15, Rn. 3; *Schaar* 2002, Rn. 247 ff.; *Ernst*, NJOZ 2010, 1918; *Heidrich/Wegener*, MMR 2010, 805; *Schmitz*, in: Hoeren/Sieber, Handbuch Multimediarecht, Kap. 16.4, Rn. 99.

[535] *Spindler/Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, 12. Teil, TMG, § 15, Rn. 2.

[536] *Ernst*, NJOZ 2010, 1918.

[537] *Spindler/Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, 12. Teil, TMG, § 15, Rn. 3.

se möglicherweise ein Telemedium eine Rolle spielt, begründet nicht die Anwendbarkeit des TMG auf die übermittelten personenbezogenen Inhaltsdaten.

Kurz zusammengefasst lässt sich festhalten, dass Clouddienste, genauer deren Anwendungsoberflächen und Eingabemasken, in der Regel Telemedien darstellen, jedoch die in der Cloud verarbeiteten personenbezogenen Daten Inhaltsdaten darstellen, auf die das TMG nicht anzuwenden ist.

3.1.5 Anwendungs- und Geltungsbereich des Bundesdatenschutzgesetzes

Als zentrales Normgefüge für den nationalen Datenschutz bei Cloud Computing ist somit das Bundesdatenschutzgesetz anzusehen. Unter welchen Umständen dieses zur Anwendung kommt, soll im Folgenden kurz dargestellt werden.

3.1.5.1 Normadressaten

Grundsätzlich gilt gemäß § 1 Abs. 2 Nr. 1 und 3 BDSG, dass das Bundesdatenschutzgesetz für nichtöffentliche Stellen und öffentliche Stellen des Bundes anzuwenden ist. Öffentlich-rechtliche Wettbewerbsunternehmen, die im Wettbewerb zu privaten Unternehmen stehen, werden wie nichtöffentliche Stellen behandelt.

Öffentliche Stellen der Länder wenden hingegen Landesdatenschutzrecht an, soweit nicht die Ausnahmen in § 1 Abs. 2 Nr. 2 BDSG greifen, also wenn diese Bundesrecht ausführen oder als Organe der Rechtspflege tätig werden.

3.1.5.2 Sachlicher Anwendungsbereich

Das Bundesdatenschutzgesetz gilt gemäß § 1 Abs. 2 Nr. 1 bis 3 BDSG für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die soeben erwähnten Stellen.

Gemäß § 3 Abs. 3 BDSG ist Erheben das Beschaffen von Daten über den Betroffenen. Die Verarbeitung ist gemäß § 3 Abs. 4 Satz 1 BDSG der Sammelbegriff für das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten.

§ 3 Abs. 4 Satz 2 Nr. 1 BDSG definiert Speichern als das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung. Da in eine Cloud ausgelagerte (personenbezogene) Daten zu irgendeinem Zeitpunkt in eben dieser aufbewahrt werden müssen, ist der Begriff des Speicherns für Cloud Computing besonders relevant.

Ein weiterer zentraler Begriff, der auch und gerade für Cloud Computing erhebliche Bedeutung hat, ist der der Übermittlung. Übermitteln ist gemäß § 3 Abs. 4 Satz 2 Nr. 3 BDSG das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden (§ 3 Abs. 4 Satz 2 Nr. 3 lit. a) BDSG) oder der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft (§ 3

Abs. 4 Satz 2 Nr. 3 lit. b) BDSG). Cloud Computing betrifft dabei unter anderem die Weitergabe an Dritte gemäß § 3 Abs. 4 Satz 2 Nr. 3 lit. a) BDSG.

„Dritter“ ist gemäß § 3 Abs. 8 Satz 1 BDSG jede Person oder Stelle außerhalb der verantwortlichen Stelle. Verantwortliche Stelle ist gemäß § 3 Abs. 7 BDSG jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Außerdem ist zu beachten, dass gemäß § 3 Abs. 8 Satz 2 BDSG keine Dritten der Betroffene sowie Personen und Stellen sind, die im Inland oder einem anderen EU- oder EWR-Staat personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.[538]

Weitere für Cloud Computing relevante Formen der Verarbeitung sind das Verändern und das Löschen von personenbezogenen Daten. Das Verändern ist für alle Cloudservices relevant, die nicht nur bloße Speicherung im Sinne von Cloudstorage anbieten. Verändern ist gemäß § 3 Abs. 4 Satz 2 Nr. 2 BDSG das inhaltliche Umgestalten gespeicherter personenbezogener Daten, während das Unkenntlichmachen gespeicherter personenbezogener Daten gemäß § 3 Abs. 4 Satz 2 Nr. 5 BDSG als Löschen definiert wird. Löschen betrifft alle Arten von Clouddiensten, da einmal eingebrachte personenbezogene Daten auch irgendwann wieder gelöscht werden müssen.

Die letzte Unterform der Verarbeitung, nämlich das Sperren von personenbezogenen Daten, hat für Cloud Computing nur untergeordnete Bedeutung. Sperren in diesem Sinne wird als das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken, legaldefiniert.

Nutzen ist gemäß § 3 Abs. 5 BDSG jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

3.1.5.3 Personenbezogene Daten

3.1.5.3.1 Definition gemäß § 3 BDSG und Relativität des Personenbezugs

Der Anwendungsbereich des Bundesdatenschutzgesetzes ist eröffnet, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Daten sind gemäß § 3 Abs. 1 BDSG dann personenbezogen, wenn sie als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person anzusehen sind. Durch diese beiden Alternativen wird gleichzeitig der Berechtigte des Datenschutzrechts, nämlich der Betroffene, definiert.

Eine Person ist bestimmt, wenn die Daten mit dem Namen des Betroffenen verbunden sind oder sich aus dem Inhalt oder dem Zusammenhang der Bezug unmittelbar

[538] Zu den Auswirkungen siehe vor allem die Ausführungen weiter unten zur Auftragsdatenverarbeitung und zu den internationalen Aspekten in den Kap. 3.1.8 und 3.1.12.

herstellen lässt.[539] Sie ist bestimmbar, wenn die speichernde Stelle den Bezug mit den ihr normalerweise zur Verfügung stehenden Hilfsmitteln und ohne unverhältnismäßigen Aufwand durchführen kann. Folglich kommt es auf die Kenntnisse, Mittel und Möglichkeiten der speichernden Stelle an.[540] Der Personenbezug ist deswegen relativ.[541] Für die Feststellung des Personenbezugs ist die Relation zwischen Daten und Datenverwender zu betrachten, wobei nur für denjenigen Verwender die Datenschutzgesetze gelten, der durch sein – mit vertretbarem Aufwand erwerbbares – Zusatzwissen den Bezug zwischen den Daten und dem Betroffenen herstellen kann.[542]

3.1.5.3.2 Einordnung verschlüsselter personenbezogener Daten

Da Kryptographie ein wirksames Mittel für technischen Datenschutz darstellt und gerade für den Erfolg des Cloud Computing ein wesentlicher Aspekt sein wird, stellt sich die Frage, wie verschlüsselte personenbezogene Daten datenschutzrechtlich zu behandeln sind.[543] Konkret stellt sich die praxisrelevante Frage, ob Datenschutzrecht eingreift, wenn der Cloudprovider keinen Schlüssel zur Dekodierung hat, sondern dieser nur dem Cloudnutzer oder dem vom Umgang mit den Daten Betroffenen zur Verfügung steht.[544]

Kryptografisch verschlüsselte personenbezogene Daten sind pseudonymisierte Daten. Die Daten werden durch eine Zuordnungsvorschrift, nämlich den kryptografischen Schlüssel in Verbindung mit dem Verschlüsselungsalgorithmus, derart verändert, dass die Einzelangaben ohne Kenntnis oder Nutzung dieser Zuordnungsvorschrift nicht mehr einer natürlichen Person zugeordnet werden können.[545] Der Inhaber des kryptografischen Schlüssels ist dabei der Inhaber der Zuordnungsregel. Auch für alle Angreifer, die die genutzte Verschlüsselung mit vertretbarem Auf-

---

539 *Gola/Schomerus* 2010, § 3, Rn. 10.

540 *Gola/Schomerus* 2010, § 3, Rn. 10.

541 *Gola/Schomerus* 2010, § 3, Rn. 10; *Dammann*, in: Simitis, BDSG, § 3, Rn. 32 ff.; *Roßnagel/Scholz*, MMR 2000, 723; *Spindler/Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, 2008, 12. Teil, TMG, § 11, Rn. 5b; a. A. sind die Anhänger der objektiven Theorie; siehe dazu *Pahlen-Brandt*, DuD 2008, 34; *Pahlen-Brandt*, K&R 2008, 289 und AG Berlin Mitte, K&R 2007, 601; begrifflich und inhaltlich unklar *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3, Rn. 13.

542 *Roßnagel/Scholz*, MMR 2000, 723.

543 Siehe auch *Spies*, Cloud Computing und Datenschutz - macht die Verschlüsselung einen Unterschied?, http://blog.beck.de/2011/01/14/cloud-computing-und-datenschutz-macht-die-verschluesselung-einen-unterschied.

544 *Spies*, MMR-Aktuell 2011, 313727.

545 So allgemein für den Vorgang der Pseudonymisierung *Gola/Schomerus* 2010, § 3, Rn. 46.

wand brechen können, sind die Daten personenbezogen.[546] Für alle anderen sind sie anonyme Daten.[547] Anonyme Daten sind aber keine personenbezogenen Daten.[548]

Daraus folgt beispielsweise, dass in Fällen in denen anonyme Daten an eine Stelle übermittelt wird, die in der Lage ist, den Personenbezug (wieder)herzustellen, der Übermittlungstatbestand des Bundesdatenschutzgesetzes erfüllt ist.[549] Bei verschlüsseltem Cloud Computing ist also zu differenzieren, wer den Schlüssel zur Entschlüsselung kennt oder besitzt. Unproblematisch in dem Sinne, dass kein Personenbezug besteht, ist demzufolge nur der Fall, wenn nur der Cloudnutzer oder – noch besser – der Betroffene selbst die Daten entschlüsseln kann.

Daraus folgt, dass vom Betroffenen oder zumindest vom Cloudnutzer kryptografisch auf dem Stand der Wissenschaft und Technik verschlüsselte personenbezogene Daten ohne Beachtung datenschutzrechtlicher Vorschriften in die Cloud verbracht werden dürfen. Diese Feststellung betrifft aber nur die bereits verschlüsselte Übermittlung und die anschließende verschlüsselte Speicherung. Wie bereits erwähnt, ist es für eine Verarbeitung notwendig, dass der Verarbeitende, also in der Regel der Cloudprovider, die Daten entschlüsseln können muss.[550]

3.1.5.4 Räumlicher Geltungsbereich

Wegen den internationalen Aspekten des Cloud Computing ist es wichtig zu wissen, wann und inwieweit deutsches Datenschutzrecht gilt.[551] Das Bundesdatenschutzgesetz gilt, soweit nicht bereichsspezifische oder landesgesetzliche Vorschriften vorgehen, für jede Verwendung personenbezogener Daten innerhalb Deutschlands.[552] Auch ausländische Unternehmen, die in Deutschland personenbezogene Daten verarbeiten, sind an die deutschen Datenschutzgesetze gebunden. Es ist dabei sogar unerheblich, dass „nur“ Daten von und über Ausländer verwendet werden. Das Bundesdatenschutzgesetz unterscheidet nämlich nicht nach der Nationalität der Betroffenen. Entscheidend ist der Verwendungsort.[553]

Daneben ist § 1 Abs. 5 Satz 1 BDSG zu beachten, der nach seinem ersten Halbsatz nicht mehr auf das Territorialitätsprinzip, sondern das Sitzprinzip abstellt, wenn Datenverkehr zwischen EU- oder EWR-Staaten stattfindet. Eine Gegenausnahme

---

546 Dafür dürfte der Stand der Technik und der kryptologischen Forschung entscheidend sein; die Wiederherstellung des Personenbezugs wird auch als Reanonymisierung bezeichnet.

547 *Roßnagel*, in: Eifert/Hoffmann-Riem, Innovation, Recht und öffentliche Kommunikation, 2011, 49; *Roßnagel/Scholz*, MMR 2000, 725.

548 *Roßnagel*, in: Eifert/Hoffmann-Riem, Innovation, Recht und öffentliche Kommunikation, 2011, 48.

549 *Gola/Schomerus* 2010, § 3, Rn. 10.

550 Siehe dazu auch weiter unten Kap. 4.6.4.

551 Zur Datenübermittlung ins Ausland siehe Kap. 3.1.12.

552 *Simitis*, in: Simitis, BDSG, § 4b, Rn. 8.

553 *Simitis*, in: Simitis, BDSG, § 4b, Rn. 9, 13.

besteht nach § 1 Abs. 5 Satz 1 Halbsatz 2 BDSG, wenn die aus einem EU-Staat tätige Stelle eine Niederlassung im Inland hat und von dieser Niederlassung aus agiert, so dass wieder das Territorialitätsprinzip gilt. Für Erhebungen, Verarbeitungen und Nutzungen durch eine solche Niederlassung gilt dann wiederum deutsches Datenschutzrecht.[554] Nach § 1 Abs. 5 Satz 4 BDSG hat das Sitzlandprinzip schließlich wieder Bedeutung, wenn bereits erhobene und gespeicherte Daten über deutsches Territorium lediglich transportiert werden, also ein Datentransfer erfolgt, ohne dass die Daten in Deutschland zur Kenntnis genommen werden.[555]

Soweit eine außereuropäische Stelle, zum Beispiel ein Cloudprovider oder Cloudnutzer in den USA ohne Sitz in Deutschland, personenbezogene Daten gerade nicht im deutschen Inland erhebt, verarbeitet oder nutzt, ergibt sich im Umkehrschluss aus § 1 Abs. 5 Satz 2 BDSG, dass in solchen Fällen ebenfalls kein deutsches Datenschutzrecht gelten kann.[556] § 1 Abs. 5 Satz 2 BDSG lässt zudem offen, wie genau die Erhebung, Verarbeitung oder Nutzung im Inland erfolgen muss, um deutsches Recht für anwendbar anzusehen. Es fällt dabei auf, dass die deutsche Vorschrift Art. 4 Abs. 1 lit. c) DSRL nicht vollständig umsetzt. Dieser verlangt eine Anwendung des nationalen Rechts nämlich nur dann, wenn die im Drittland angesiedelte Stelle „auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind“.

So ist beispielsweise umstritten, ob der PC eines Nutzers eines Onlinedienstes als in Europa oder Deutschland belegenes Mittel ausreicht.[557] Für Cloud Computing wird in der Regel davon auszugehen sein, dass die personenbezogenen Daten bereits im Inland erhoben wurden und nur noch die Frage der Zulässigkeit der Übermittlung ins außereuropäische Ausland im Raum steht.[558] Problematisch sind nur die Fälle, in denen erstmalig personenbezogene Inhaltsdaten in einen in einem Drittland belegenen Clouddienst vom Cloudnutzer als Betroffenen eingegeben und damit rechtstechnisch „erhoben“ werden. Für eine solche Erhebung personenbezogener Daten mit Hilfe eines Webformulars des Cloudproviders wird aber die Auffassung vertreten, dass die datenschutzrelevanten Handlungen in vollem Umfang vom Betroffenen ausgehen und demnach die im Drittland befindliche Stelle, also der Cloudprovider, nicht auf im Hoheitsgebiet des Nutzers belegene Mittel im Sinne des Art. 4 Abs. 1 lit. c) DSRL zurückgreift.[559]

---

554 *Gola/Schomerus* 2010, § 1, Rn. 28.

555 *Gola/Schomerus* 2010, § 1, Rn. 30.

556 So auch *Hoeren*, ZRP 2010, 252 für das Beispiel „Facebook“.

557 *Dammann*, in: Simitis, BDSG, § 1, Rn. 217 mit weiteren Beispielen; siehe dazu auch *Hoeren*, ZRP 2010, 252.

558 Siehe dazu weiter unten Kap. 3.1.12, wobei dort unterstellt wird, dass die Daten im Inland erhoben wurden und somit unter den Anwendungsbereich des BDSG fallen.

559 *Dammann*, in: Simitis, BDSG, § 1, Rn. 223.

Der Vollständigkeit halber sei erwähnt, dass § 1 Abs. 5 Satz 2 BDSG als internationalrechtliche Spezialkollisionsnorm den Rom-Verordnungen vorgeht.[560]

3.1.6 Datenschutzprinzipien

Im modernen Datenschutzrecht sind einige zentrale und grundlegenden Prinzipien und Grundsätze verankert. Diese sollen im Folgenden kurz vorgestellt werden. Sie sind primär bei der Rechtsanwendung zu beachten, haben aber auch bei der Anwendung der KORA-Methode erhebliche Bedeutung.[561]

3.1.6.1 Notwendigkeit eines Erlaubnistatbestands und Gedanke der Selbstbestimmung

Für deutsches und europäisches Datenschutzrecht gilt der Grundsatz, dass eine Datenverarbeitung eines Erlaubnistatbestands bedarf, um rechtmäßig zu sein. Ein solcher Erlaubnistatbestand kann sich gemäß § 4 Abs. 1 BDSG aus einer gesetzlichen Erlaubnisnorm oder der Einwilligung des Betroffenen ergeben.

Insbesondere der Grundgedanke der Selbstbestimmung des Betroffenen wird aus dem Einwilligungserfordernis deutlich. Die übrigen Legitimationsnormen sind hingegen oft Ausdruck eines überwiegenden Allgemeininteresses, zum Beispiel der Strafverfolgung, oder erfordern das Abwägen mit sonstigen Interessen Einzelner, wie beispielsweise in § 28 BDSG zu sehen ist.[562]

3.1.6.2 Transparenz

Das Transparenzprinzip ist eine verfassungsrechtlich begründete Ausprägung des Rechts auf informationelle Selbstbestimmung.[563] Es soll dem Einzelnen Einsicht in die ihn betreffenden Datenverarbeitungsvorgänge und die Umstände der Datenverarbeitung gewähren. Kurz zusammengefasst, soll der Transparenzgrundsatz dem Betroffenen das Wissen verschaffen, das er benötigt, um wissen zu können, wer was wann über ihn weiß.[564] Wenn man auf das Ziel der informationellen Selbstbestimmung abstellt, kann er bei Gewährleistung des Transparenzprinzips überprüfen, ob das Bild das durch die Datenverarbeitung von ihm entworfen wurde, auch dem entspricht, das er selbst von sich preisgeben möchte.

Die Transparenz wird einfachgesetzlich durch Informationspflichten des Datenverarbeiters, zum Beispiel in § 4 Abs. 3 BDSG, gegenüber dem Betroffenen und um-

---

560 *Dammann*, in: Simitis, BDSG, § 1, Rn. 216; *Jotzo*, MMR 2009, 233; zu den Rom-Verordnungen siehe die Ausführungen zum internationalen Privatrecht in Kap 3.4.

561 Siehe dazu die Ausführungen in Kap. 4.4.3 und Kap. 4.4.6.

562 Ähnlich *Schnabel* 2009, 135; zu den Interessen, insbesondere bei außereuropäischen Übermittlungen, siehe Kap. 3.1.12.1.4.

563 *Hornung*, MMR 2006, XXII; *Gola/Schomerus* 2010, § 33, Rn. 1.

564 *Spindler/Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Teil, BDSG, § 4, Rn. 6; *Hornung* 2005, 164, 198.

gekehrt durch Auskunftsrechte des Betroffenen (§§ 19, 34 BDSG) gegenüber dem Datenverarbeiter gewährleistet.[565] Diese Rechte des Betroffenen sind gemäß § 6 Abs. 1 BDSG unabdingbar.

Im Cloudkontext geht es wegen der Komplexität, der Fülle der Verarbeitungsvorgänge und nicht zuletzt wegen des prinzipinhärenten intransparenten „Wolkencharakters“ bei der Forderung nach Transparenz im Wesentlichen um die Offenlegung der Struktur des Datenverarbeitungsverfahrens[566] und der nachträglichen Nachvollziehbarkeit der, oft von Zufällen geprägten, Aktionen in der Cloud. Eine Benachrichtigung und Einwilligung für jede einzelne Aktion, würde angesichts der Fülle und Vielfalt der Vorgänge und der beteiligten Stellen zu einer Überforderung der Beteiligten führen, so dass die Ursprungsintention des Transparenzprinzips in modernen IT-Systemen an seine Grenzen stößt.[567]

3.1.6.3 Grundsatz der Direkterhebung

Mit der Transparenz zusammenhängend, beziehungsweise aus dieser ableitbar, ist der Grundsatz der Direkterhebung. Dieser ist in § 4 Abs. 2 Satz 1 BDSG kodifiziert und besagt, dass personenbezogene Daten beim Betroffenen zu erheben sind, so dass dieser von der Erhebung Kenntnis erlangt und entsprechend reagieren kann. Ohne die Mitwirkung des Betroffenen dürfen sie nur erhoben werden, wenn die Ausnahmen in § 4 Abs. 2 Satz 2 BDSG eingreifen. Der Direkterhebungsgrundsatz wurde im Volkszählungsurteil formuliert und findet sich auch in Erwägungsgrund 38 und Art. 10 der Datenschutzrichtlinie.

3.1.6.4 Erforderlichkeit

Der Erforderlichkeitsgrundsatz steht in engem Zusammenhang mit der Zweckbindung. Erforderlichkeit bedeutet, dass eine konkrete Datenverarbeitung auf das für die Erreichung des konkreten Zwecks erforderliche Maß hinsichtlich Datenumfang, Verarbeitungsform und Verarbeitungszeit beschränkt wird. Nur wenn unter Berücksichtigung dieser drei Umstände nicht auf die konkrete Datenverarbeitung verzichtet werden kann, ist diese tatsächlich erforderlich.[568] Für die Beurteilung der Erforderlichkeit ist ein strenger Maßstab anzulegen.[569] Insbesondere kommen hinsichtlich der Aufgabenerfüllung die Geeignetheit und Zweckmäßigkeit als weitere Voraus-

---

565 Zur Transparenz siehe auch Kap. 3.1.9.5.7 und 4.4.3.

566 So bereits die allgemeine Forderung von *Roßnagel*, MMR 2005, 74 in einer Welt allgegenwärtiger Datenverarbeitung; zu dieser Struktur gehören insbesondere auch vom Provider möglicherweise genutzte Subunternehmen.

567 So *Roßnagel*, MMR 2005, 72 für Ubiquitous Computing, wobei die Wertung auch für Cloud Computing gilt; in diesem Zusammenhang sind auch die Ausnahmen nach § 33 Abs. 2 BDSG zu erwähnen.

568 *Roßnagel*, in: Eifert/Hoffmann-Riem, Innovation, Recht und öffentliche Kommunikation, 2011, 44.

569 *Sokol*, in: Simitis, BDSG, § 13, Rn. 26.

setzungen hinzu. Das Fehlen der Geeignetheit und Zweckmäßigkeit führt in der Regel dazu, dass es auch an der Erforderlichkeit mangelt.[570]

Der Grundsatz ist ein Mittel zur Abwehr von Grundrechtseingriffen.[571] Er durchzieht das gesamte Datenschutzrecht und findet sich zum Beispiel in den §§ 13 Abs. 1, 14 Abs. 1, 15 Abs. 1, 16 Abs. 1 Nr. 1, 20 Abs. 2 Nr. 2 BDSG oder im Zusammenhang mit Abwägungsklauseln in § 28 Abs. 1 Nr. 2 und 3 BDSG. So ist beispielsweise die Speicherung, Veränderung oder Nutzung von Daten nach § 14 BDSG dann erforderlich, wenn die Aufgabe ansonsten nicht oder nicht vollständig erfüllt werden könnte.[572] Im Rahmen des § 15 Abs. 1 Satz 1 Nr. 1 BDSG muss es der Stelle sogar unmöglich sein, ihre Aufgabe ohne die Kenntnis der übermittelten personenbezogenen Daten zu erfüllen, um dem Erforderlichkeitsprinzip zu genügen.[573]

Auch § 9 Satz 1 BDSG beinhaltet einen Erforderlichkeitsaspekt. Danach sind nur die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die in der Anlage zu § 9 BDSG genannten Anforderungen zu gewährleisten. In Satz 2 wird der Erforderlichkeitsmaßstab näher konkretisiert. Nach § 9 Satz 2 BDSG sind Maßnahmen nur dann erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Damit wird die Notwendigkeit einer Sicherungsmaßnahme im Sinne des § 9 BDSG durch das Verhältnismäßigkeitsprinzip begrenzt.

3.1.6.5 Datenvermeidung und Datensparsamkeit

Mit der Erforderlichkeit hängen die in § 3a BDSG ausdrücklich gesetzlich angeführten Prinzipien der Datenvermeidung und Datensparsamkeit zusammen.[574] Sie sind Teil des Systemdatenschutzes.[575] Ein erster Ansatz zur Datenvermeidung und Datensparsamkeit findet sich bereits im Volkszählungsurteil in Form der Forderung des Gerichts nach gesetzlichen Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung.[576] Die Prinzipien sind somit zentrale Ausprägung und Umsetzung des Vorsorgegedankens im Datenschutzrecht.[577]

---

570 *Sokol*, in: Simitis, BDSG, § 13, Rn. 26.

571 *Roßnagel*, in: Eifert/Hoffmann-Riem, Innovation, Recht und öffentliche Kommunikation, 2011, 44.

572 *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 14, Rn. 5.

573 *Dammann*, in: Simitis, BDSG, § 15, Rn. 11, 15.

574 *Simitis*, DuD 2000, 725 sieht diese als Unterfall des Erforderlichkeitsprinzips; a. A. *Roßnagel*, in: Eifert/Hoffmann-Riem, Innovation, Recht und öffentliche Kommunikation, 2011, 44, der darin den zentralen Ansatz zur Umsetzung des Vorsorgeprinzips im Datenschutz erkennt.

575 *Gola/Schomerus* 2010, Einleitung, Rn. 12; *Roßnagel/Scholz*, MMR 2000, 722.

576 BVerfGE 65, 43 ff.; *Roßnagel*, in: Eifert/Hoffmann-Riem, Innovation, Recht und öffentliche Kommunikation, 2011, 42.

577 *Roßnagel*, in: Eifert/Hoffmann-Riem, Innovation, Recht und öffentliche Kommunikation, 2011, 44.

Zielsetzung der Prinzipien ist es gemäß § 3a BDSG, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Zudem sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies möglich ist und im Verhältnis zum angestrebten Schutzzweck kein unverhältnismäßiger Aufwand dafür erforderlich ist. Soweit es also verhältnismäßig und technisch möglich ist, sind Systeme und Verfahren datenvermeidend und datensparsam zu gestalten. Die Datenvermeidung als Gestaltungsaufgabe kann sogar zu einer Rechtspflicht erwachsen.[578]

Die beiden Prinzipien haben für Cloud Computing besondere Bedeutung, da die Frage, ob personenbezogene Daten überhaupt in die Cloud ausgelagert werden sollten, eine solche des datenvermeidenden Umgangs ist. Die „Globalisierung der Datenverarbeitung" führt zu einer besonderen Erhöhung der Grundrechtsrisiken, weil der Umgang mit personenbezogenen Daten innerhalb von vernetzten IT-Systemen für den Betroffenen faktisch nicht mehr kontrollierbar ist.[579] Dies ist auch und gerade bei Public Cloud Computing der Fall, da die Cloudnutzer und Provider mit Daten von betroffenen Dritten umgehen. Selbst diese Nutzer und Provider haben eine vergleichsweise eingeschränkte Kontrollfähigkeit und Beherrschbarkeit über diese Daten Dritter. Die eigentlich Betroffenen sind nicht nur faktisch nicht in der Lage den Umgang zu kontrollieren, sondern oft auch rechtlich schutzlos gestellt, da der Umgang mit ihren Daten außerhalb des Einflussbereichs deutscher und europäischer Gesetze und entsprechender Kontrollstellen erfolgen kann.[580]

Im Sinne des Vorsorgegedankens kann demnach – unter bestimmten Umständen – nur die Datenvermeidung als einzig verbleibendes Mittel mit dem Ziel der informationellen Selbstbestimmung übrigbleiben.[581] Wenn auf eine Verarbeitung von Daten nicht verzichtet werden kann, sind die in § 3a Satz 2 BDSG angeführten Alternativen der Pseudonymisierung und Anonymisierung in Betracht zu ziehen, mit denen ebenfalls Persönlichkeitsschutz erreicht werden kann.[582] Beide sind Mittel zur Umsetzung des System- und Selbstdatenschutzes.

---

578 *Roßnagel*, in: Eifert/Hoffmann-Riem, Innovation, Recht und öffentliche Kommunikation, 2011, 45.

579 *Roßnagel*, in: Eifert/Hoffmann-Riem, Innovation, Recht und öffentliche Kommunikation, 2011, 44.

580 Allgemein dazu auch *Roßnagel*, in: Eifert/Hoffmann-Riem, Innovation, Recht und öffentliche Kommunikation, 2011, 44.

581 *Roßnagel*, in: Eifert/Hoffmann-Riem, Innovation, Recht und öffentliche Kommunikation, 2011, 44.

582 Zur Anonymisierung und Pseudonymisierung siehe auch Kap. 3.1.5.3.2 und *Roßnagel/Scholz*, MMR 2000, 721 ff.

3.1.6.6 Zweckfestlegung, Zweckbindung, informationelle Gewaltenteilung

Das Zweckbindungsprinzip, das als Reaktion auf das Volkszählungsurteil[583] im Jahr 1990 durchgängig ins Bundesdatenschutzgesetz eingeführt wurde, soll sicherstellen, dass personenbezogene Daten grundsätzlich nur zu dem Zweck verarbeitet werden dürfen, zu dem sie erhoben oder gespeichert wurden. Der Zweck muss außerdem im Voraus festgelegt sein. Auch ein Empfänger einer Datenübermittlung ist an den jeweils vorher festgelegten Übermittlungszweck gebunden.[584] Anknüpfungspunkte für zulässige Zwecke ergeben sich aus den legitimierenden Normen für eine konkrete Erhebung oder Speicherung.[585]

Vorschriften in denen das Zweckbindungsprinzip zum Vorschein kommt sind im Bundesdatenschutzgesetz zum Beispiel die §§ 14, 15 Abs. 3, 28 Abs. 5 und 39 BDSG. Die Zweckbindung ist zudem eng mit der Trennungskontrolle gemäß Nr. 8 der Anlage zu § 9 BDSG verbunden.[586] Der Zweckbindungsgrundsatz ist somit auch durch technische Maßnahmen zu unterstützen.

Einer besonderen Zweckbindung unterliegen die in § 31 BDSG erwähnten Daten. Im Cloudkontext sind vor allem personenbezogene Daten zu Datensicherungszwecken oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage besonders erwähnenswert.

Aus dem Zweckbindungsgebot folgt auch der vom Bundesverfassungsgericht entwickelte Grundsatz der informationellen Gewaltenteilung. Dieser besagt, dass eine Übermittlung personenbezogener Daten zwischen Behörden den üblichen Voraussetzungen unterliegt, mithin ein Erlaubnistatbestand vorliegen muss.[587] Umgekehrt folgt das Gebot die personenbezogenen Daten der unterschiedlichen Stellen voneinander abzuschotten. Der Grundsatz geht allerdings noch weiter und verlangt, dass eine Zweckbindung nicht nur zwischen verschiedenen datenverarbeitenden Stellen, sondern auch bei der Verfolgung verschiedener Aufgaben durch eine einzelne Stelle gilt. Nimmt diese nämlich unterschiedliche Aufgaben wahr, so sind diese organisatorisch so voneinander zu trennen, dass kein Informationsaustausch stattfinden kann.[588]

---

583 BVerfGE 65, 46: „Die Verwendung der Daten ist auf den gesetzlich bestimmten Zweck begrenzt. Schon angesichts der Gefahren der automatischen Datenverarbeitung ist ein – amtshilfefester – Schutz gegen Zweckentfremdung durch Weitergabeverbote und Verwertungsverbote erforderlich.“.

584 *Dammann,* in: Simitis, BDSG, § 15, Rn. 34.

585 *Dammann,* in: Simitis, BDSG, § 14, Rn. 40; BVerfGE 65, 46: „Ein Zwang zur Angabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt.“.

586 Siehe dazu Kap. 3.1.9.3.2.8.

587 BVerfGE 65, 68; BVerfG, NJW 1988, 961.

588 *Polenz,* in: Kilian/Heussen, Computerrechtshandbuch, Teil 13, Rn. 9.

3.1.7 Cloud Computing und Behörden

Während sich die Darstellung der Rechtslage im Zusammenhang mit Cloud Computing im Wesentlichen an Unternehmen orientiert, sollen im Folgenden einige Besonderheiten bei der Nutzung von Cloud Computing durch Behörden oder öffentlich-rechtliche Anstalten aufgezeigt werden.

3.1.7.1 Datenschutzrecht

Bei Behörden ist zu prüfen, ob eine Bundesbehörde oder Landesbehörde tätig wird. Ist Letzteres der Fall ist zudem zu differenzieren welches Recht sie ausführt.

Eine gesetzliche Aufzählung und Legaldefinition der öffentlichen Stellen des Bundes und der Länder findet sich in § 2 BDSG. Beachtenswert ist zudem die Spezialvorschrift in Absatz 3, wonach privatrechtlich organisierte Vereinigungen[589] von öffentlichen Stellen des Bundes und der Länder (Bund-Länder-Mischvereinigungen), die Aufgaben der öffentlichen Verwaltung wahrnehmen, als öffentliche Stellen des Bundes gelten, wenn sie die Voraussetzungen der Nr. 1 oder 2 erfüllen. Ansonsten gelten sie als öffentliche Stellen der Länder.

Bei gemischt ausgestalteten Behördenclouds, die der Erledigung öffentlicher Aufgaben dienen, könnte insbesondere die Ausnahme in Nr. 1 relevant werden, wonach eine solche Vereinigung über den Bereich eines Landes hinaus tätig wird. § 2 Abs. 3 Nr. 2 BDSG besagt außerdem, dass bei einer absoluten Mehrheit des Bundes an der privatrechtlichen Vereinigung ebenfalls Bundesrecht und damit das BDSG gilt.

Beim Zusammenschluss von öffentlichen Ressourcen ist künftig zu erwarten, dass sich unterschiedliche Behörden zusammentun und somit Bundes- und Landesbehörden oder Behörden unterschiedlicher Bundesländer mit dem gleichen Tätigkeitsschwerpunkt eine privatrechtliche Community Cloud bilden. Dies erfolgt am einfachsten, wenn bereits vorhandene (Shared) Services Center zu effizienten Cloudsystemen zusammengefasst werden. Die Anwendbarkeit von Landes- oder Bundesrecht ist in solchen Fällen nicht vom Standort der Server und dem Ort der Verarbeitung abhängig, sondern von den Beteiligten.

Bei einer Zentralisierung von Daten und IT-Services ist darauf zu achten, dass die Zusammenführung rechtlich erlaubt ist, technisch die Zugriffsberechtigungen und die konkrete Nutzung nur innerhalb des rechtlichen Rahmens erfolgt und keine über den Gesetzeswortlaut hinausgehenden Begehrlichkeiten geweckt werden. Insbesondere ist datenschutzrechtlich der Grundsatz der informationellen Gewaltenteilung zu wahren.[590]

---

589 Der Begriff der „Vereinigung“ ist weit auszulegen, so dass darunter sogar Personengesellschaften fallen; siehe hierzu *Dammann*, in: Simitis, BDSG, § 2, Rn. 34 ff.

590 Zum Grundsatz siehe auch oben Kap. 3.1.6.6.

Die zentrale(re) Nutzung darf insbesondere nicht zu einem Dammbruch führen, was die jeweiligen Nutzungsmöglichkeiten angeht. Ein Beispiel wären die bisher voneinander getrennten Melderegister auf Kommunalebene, die in einer zentralen Cloud vorgehalten werden und dadurch die Begehrlichkeit nach einem zentralen Melderegister schafft, das die Gefahr der Totalerfassung in sich trägt.[591] So ist denkbar, dass Polizeibehörden oder Geheimdienste die zentralen Daten für ihre Zwecke nutzen und dabei bereits die Ermächtigungsgrundlagen vom Gesetzgeber zu weit ausgestaltet sind. Zu denken sei beispielsweise an die Erfahrungen mit der Rasterfahndung, der Onlinedurchsuchung oder dem KFZ-Kennzeichenscanning.

Durch die zentrale Vorhaltung in leistungsstarken Serverfarmen, wobei die Daten physisch tatsächlich eher dezentral in Einzelrechenzentren gespeichert werden, sind auch Data-Mining-Prozesse erheblich einfacher oder überhaupt erst möglich. Die Nutzung von Cloud Computing durch staatliche Einrichtungen darf demzufolge nicht dazu führen, dass der Grundrechtsschutz der Bürger geschmälert wird, indem neuartige Methoden zur Anwendung kommen, nur weil diese technisch überhaupt erst möglich wurden.

Problematische Rechtsbereiche im Zusammenhang mit der Nutzung von Cloud Computing durch Behörden sind neben dem allgemeinen Datenschutzrecht, das Sozialrecht, das Abgaben- und Steuerrecht, das Melderecht und der rechtliche Rahmen der Justiz- und Polizeiverwaltung und der Geheimdienste.[592] Insbesondere das jeweilige sektorspezifische Datenschutzrecht ist zu beachten. Beispielsweise gilt für die Sozialverwaltung bei der Erhebung, Verarbeitung und Nutzung von Sozialdaten das Sozialgeheimnis und damit die Vorschriften in § 35 SGB Abs. 1 i.V.m. den §§ 67 ff. SGB X.

3.1.7.2 Verbot der Mischverwaltung gemäß Art. 83 GG

Die Zusammenfassung von bundes- und landeseigenen Services Center und allgemeinen IT-Ressourcen stellt keinen Verstoß gegen das Verbot der Mischverwaltung gemäß Art. 83 ff. GG dar. Als Mischverwaltung sind solche Verwaltungstätigkeiten zu klassifizieren, bei denen die sachlichen Entscheidungen im Zusammenwirken der beteiligten Behörden getroffen werden.[593] Gemäß der Rechtsprechung des Bundesverfassungsgerichts müssen Verwaltungen des Bundes und der Länder „organisatorisch und funktionell im Sinne in sich geschlossener Einheiten prinzipiell

---

591 So gab es bereits Pläne für ein „Bundesmelderegister“, die jedoch, nicht zuletzt wegen grundgesetzlichen Kompetenzfragen und Kritik von Datenschützern, nicht realisiert wurden; siehe dazu *Krempl*, Datenschützer gegen zentrales Bundesmelderegister, http://www.heise.de/newsticker/meldung/Datenschuetzer-gegen-zentrales-Bundesmelderegister-167713.html.

592 *Deussen/Strick/Peters*, 2010, 55.

593 *Schulz*, MMR 2010, 77; *ders.*, VM 1/2010, 38.

voneinander getrennt sein“. Sachentscheidungen müssen einem verantwortlichen Träger zugeordnet werden können.[594]

Bei der Nutzung gemeinsamer Infrastrukturen geht es jedoch nicht um die Erledigung von Sachaufgaben und dem Treffen von Sachentscheidungen, sondern um die Erfüllung von sonstigen Funktionen und die Klärung von verwaltungsinternen Fragestellungen, beispielsweise die Entscheidung, wie die behördeninterne IT-Infrastruktur aufgebaut sein soll. Es geht dabei gerade nicht um Gesetzesvollzug und die Sachentscheidungen werden durch die gemeinsame Nutzung von IT-Ressourcen auch nicht tangiert, so dass eine Kooperation in diesem Bereich verfassungsrechtlich unproblematisch möglich ist. Die Zielsetzung der Kooperationen ist, wie in allen Fällen der Nutzung von Cloud Computing, die Reduzierung der anfallenden Kosten durch die gemeinsame Nutzung von IT-Ressourcen. [595]

3.1.7.3 IT-Zusammenarbeit gemäß Art. 91c GG

Im Zusammenhang mit Behördenkooperationen ist auch Art. 91c GG von Bedeutung. Der Grundgesetzartikel gilt seit dem 1.8.2009 und wurde durch die „Föderalismusreform II“ eingefügt. Er behandelt die IT-Zusammenarbeit zwischen dem Bund und den Ländern.[596] Art. 91c Abs. 1 GG besagt, dass diese bei der Planung, der Errichtung und dem Betrieb der für ihre Aufgabenerfüllung benötigten informationstechnischen Systeme zusammenwirken können. Das Bemerkenswerte an dieser Vorschrift ist außerdem, dass damit erstmals Bestimmungen über Informationstechnologie Eingang ins Grundgesetz gefunden haben.[597]

In Art. 91c Abs. 2 Satz 1 GG steht zudem, dass Bund und Länder die für die Kommunikation zwischen ihren informationstechnischen Systemen notwendigen Standards und Sicherheitsanforderungen miteinander vereinbaren können. Damit würden einheitliche Standards und Sicherheitsanforderungen für Clouds im öffentlichen Sektor die Unterstützung durch das Grundgesetz finden. Für Sicherheitsanforderungen im IT-Bereich ist eine solche prominente Erwähnung in der Verfassung ein Novum.

3.1.8 Auftragsdatenverarbeitung

Die arbeitsteilige Wirtschaft in Deutschland macht vielfältige Weitergaben personenbezogener Daten erforderlich.[598] Früher wurden ganze IT-Abteilungen aus Unternehmen ausgegliedert, heutzutage werden Daten und Datensätze in Clouds ausgelagert. Die Bandbreite der Verarbeitungen im Auftrag kann die bloße Datener-

---

594 *Schulz*, MMR 2010, 77; *ders.*, VM 1/2010, 38; BVerfG, DVBl 2008, 173.

595 *Schulz*, MMR 2010, 77; *ders.*, VM 1/2010, 38.

596 *Schulz*, DÖV 2010, 225 und *Seckelmann*, DÖV 2009, 753 beschreiben die Hintergründe der Vorschrift.

597 *Siegel*, NVwZ 2009, 1128; *Schulz*, DÖV 2010, 225.

598 *Sutschet*, RDV 2004, 97.

fassung bis hin zur Abwicklung der gesamten Datenverarbeitungen eines Unternehmens umfassen.[599]

Vor Erlass des § 11 BDSG war die Auftragsdatenverarbeitung im BDSG 1977 an verschiedenen Stellen im Gesetz geregelt. Maßgebliche Vorschriften waren die §§ 8, 22 Abs. 2, 31 Abs. 2 und 37 BDSG 1977. Zur besseren Übersichtlichkeit wurden die verstreuten Regelungsinhalte im Jahr 1990 in § 11 BDSG zusammengefasst.[600] Auf die im Jahr 2009 erfolgte teilweise Neufassung und Erweiterung des Wortlauts der Vorschrift soll im Folgenden bei der Darstellung der Einzelheiten der Auftragsdatenverarbeitung eingegangen werden.

Von Datenverarbeitung im Auftrag oder Auftragsdatenverarbeitung spricht man, wenn sich eine Stelle für ihre Datenverarbeitung eines in ihrem Auftrag stehenden Hilfsorgans bedient, um diese „außer Haus“ durchführen zu lassen.[601] Für Cloud Computing bedeutet dies, dass der Cloudnutzer als verantwortliche Stelle die Datenverarbeitung durch das externe Hilfsorgan „Cloudprovider“ durchführen lässt. Die Vorschrift in § 11 BDSG normiert die Aufgaben- und Pflichtenverteilung zwischen Auftraggebern und Auftragnehmern.[602] Sie soll sicherstellen, dass der einer datenverarbeitenden Stelle auferlegte Datenschutz- und Datensicherungsstandard durch die Verarbeitung bei einer „außer Haus“ befindlichen, beauftragten Stelle nicht eingeschränkt wird.[603] Damit wird auch der Bezug zwischen § 11 BDSG und § 9 BDSG deutlich. Die Einzelheiten der Datenverarbeitung im Auftrag und ihre rechtlichen Implikationen, insbesondere Abgrenzungsfragen und die Neuregelungen seit dem 1.9.2009 sollen sogleich näher dargestellt werden.

Neben der in § 11 BDSG geregelten Auftragsdatenverarbeitung finden sich auch in anderen bereichsspezifischen Gesetzen Regelungen dazu. Diese sind oft mit dem Wortlaut oder dem Regelungsgehalt des § 11 BDSG identisch. Soweit Unterschiede bestehen, wie beispielsweise in § 80 Abs. 3 und Abs. 5 SGB X, soll auf diese kurz eingegangen werden.

3.1.8.1 Auftrag

Der Begriff „Auftrag“ ist weitergehender als der in § 662 BGB.[604] Auch die Art des der Auftragsdatenverarbeitung zugrunde liegenden Rechtsverhältnisses ist unerheblich. Es kann privatrechtlich, öffentlich-rechtlich, entgeltlich oder unentgeltlich

---

599 *Wächter*, CR 1991, 333.

600 *Wächter*, CR 1991, 333; *Gola/Schomerus* 2010, § 11, Rn. 1; *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 11, Rn. 1.

601 *Wächter*, CR 1991, 333.

602 *Petri*, in: Simitis, BDSG, § 11, Rn. 2.

603 *Petri*, in: Simitis, BDSG, § 11, Rn. 1.

604 *Elbel*, RDV 2010, 206; *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 11, Rn. 5; *Wank*, in: Müller-Glöge/Preis/Schmidt, ErfK, BDSG, § 11, Rn. 1.

sein. Es ist nicht einmal erforderlich, dass es rechtswirksam ist.[605] Entscheidend ist, dass der Auftrag allein auf die Erhebung, Verarbeitung und Nutzung von Daten gerichtet ist.[606] Ein Auftrag in diesem Sinne bedarf gemäß § 11 Abs. 2 Satz 2 BDSG der Schriftform (§§ 126, 126a BGB).[607]

3.1.8.2 Beteiligte, Privilegierungsfunktion und Rechtsstellung

Bei der Auftragsdatenverarbeitung gibt es zwei Hauptbeteiligte. Dies sind zum einen der Auftraggeber und zum anderen der Auftragnehmer, also die die tatsächliche Datenverarbeitung durchführende Stelle. Daneben sind noch die von der Datenverarbeitung Betroffenen zu erwähnen, deren personenbezogene Daten und damit deren Persönlichkeitsrecht durch die Vorschriften in § 11 BDSG geschützt werden sollen.[608]

Die Auftragsdatenverarbeitung privilegiert den Auftragnehmer. Sie ist dadurch gekennzeichnet, dass sich eine verantwortliche Stelle eines Dienstleistungsunternehmens bedient, das lediglich weisungsgebunden mit den Daten umgeht. Dieses Hilfsunternehmen fungiert als „verlängerter Arm“ oder als ausgelagerte Abteilung der weiterhin verantwortlichen Stelle, die als „Herrin der Daten“ die volle Verfügungsgewalt behält und damit auch allein über die Erhebung, Verarbeitung oder Nutzung bestimmt.[609] Auftraggeber und Auftragnehmer bilden dabei eine rechtliche Einheit.[610] Hauptmerkmal und Grund der Privilegierung des Auftragnehmers (Hilfsunternehmen) ist also die beim Auftraggeber (Nutzer) verbleibende Verantwortlichkeit. Die ursprünglich verantwortliche Stelle bleibt damit weiterhin verantwortlich.

Der Vollständigkeit halber sei erwähnt, dass es nicht notwendig ist, dass der Auftraggeber die Datenverarbeitung insgesamt „außer Haus“ durchführen lässt. Es reicht aus, dass eine der in § 3 Abs. 4 BDSG genannten Verarbeitungsphasen dem Auftragnehmer übertragen wird.[611]

Während üblicherweise alle Stellen außerhalb der verantwortlichen Stelle „Dritte“ im Sinne des § 3 Abs. 8 Satz 2 BDSG sind, werden gemäß § 3 Abs. 8 Satz 3 BDSG Personen und Stellen, die im Inland oder in einem Mitgliedsstaat der EU oder des

---

605 *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 11, Rn. 5; *Wank*, in: Müller-Glöge/Preis/Schmidt, ErfK, BDSG, § 11, Rn. 1.

606 *Wank*, in: Müller-Glöge/Preis/Schmidt, ErfK, BDSG, § 11, Rn. 1.

607 *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 11, Rn. 4.

608 *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 11, Rn. 6.

609 *Gola/Schomerus* 2010, § 11, Rn. 3; *Söbbing/Wöhlermann*, HMD – Praxis der Wirtschaftsinformatik, Heft 245, 2005, 50.

610 *Gola/Schomerus* 2010, § 11, Rn. 4.

611 *Petri*, in: Simitis, BDSG, § 11, Rn. 12.

EWR[612] personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen, nicht als Dritte angesehen. Wird also im Umkehrschluss einer Stelle außerhalb des Geltungsbereichs der EU-Datenschutzrichtlinie der Umgang mit Daten übertragen, so greift die Privilegierung des § 11 BDSG für solche außereuropäischen Stellen, unabhängig von einem angemessenen Datenschutzniveau, gerade nicht ein.[613] Dabei kommt es hinsichtlich des Auftragnehmers und seiner Rechenzentren auf den Ort der Datenverarbeitung und nicht auf den Sitz oder die Nationalität des Unternehmens an.[614]

Aus § 11 BDSG i.V.m. § 3 Abs. 8 Satz 3 BDSG folgt außerdem, dass Datentransfers zu und vom Auftragsdatenverarbeiter nicht als Übermittlung im Sinne von § 3 Abs. 4 Nr. 3 BDSG verstanden werden. In Fällen, in denen die Privilegierung durch § 11 BDSG nicht greift und eine Übermittlung, insbesondere in ein Drittland, anzunehmen ist, sind die für die Zulässigkeit einer solchen Übermittlung allgemein geltenden Bestimmungen, also vor allem die Notwendigkeit des Eingreifens eines Erlaubnistatbestands, zu beachten.[615]

3.1.8.3 Theorie der Funktionsübertragung

Nach herrschender Auffassung[616] ist eine Auftragsdatenverarbeitung von der sogenannten „Funktionsübertragung“ abzugrenzen. Der Ende der 70er Jahre des vorigen Jahrhunderts geprägte Begriff ist allerdings gesetzlich, von ein paar Verwaltungsvorschriften abgesehen, ungeregelt und in der Literatur umstritten.[617] Die Funktionsübertragung soll Fallgestaltungen umfassen, in denen Daten an einen Auftragnehmer nicht nur zur Verarbeitung weitergegeben werden, sondern diese als Hilfsmittel zur Erledigung einer gesamten Aufgabe dienen, die dem Auftragnehmer vom Auftraggeber übertragen wurde.[618] Es wird mithin eine ganze Funktion oder Aufgabe und nicht lediglich Daten übertragen. Die Stelle, der die Funktion übertragen wurde, hat im Gegensatz zur Auftragsdatenverarbeitung alle datenschutzrechtli-

---

612 Der Europäische Wirtschaftsraum (EWR) umfasst die EU-Staaten und zusätzlich Island, Norwegen und Liechtenstein.

613 *Pohle/Ammann*, CR 2009, 276; *Niemann/Hennrich*, CR 2010, 688; *Petri*, in: Simitis, BDSG, § 11, Rn. 8; *Dammann*, in: Simitis, BDSG, § 3, Rn. 246; *Gola/Schomerus* 2010, § 11, Rn. 16; *Geis* 2009, 4; *Schulz*, in: Taeger/Wiebe, Inside the Cloud, 413; *Heidrich/Wegener*, MMR 2010, 806; siehe dazu auch die genaueren Ausführungen in Kap. 3.1.12.6.

614 *Niemann/Hennrich*, CR 2010, 687; *Dammann*, in: Simitis, BDSG, § 3, Rn. 246; *Gabel*, in: Taeger/Gabel, BDSG, § 11, Rn. 25.

615 *Petri*, in: Simitis, BDSG, § 11, Rn. 8; siehe hierzu im internationalen Kontext Kap. 3.1.12.1.

616 *Petri*, in: Simitis, BDSG, § 11, Rn. 22; *Gola/Schomerus* 2010, § 11, Rn. 9; Aufsichtsbehörden Baden-Württemberg, Hinweise zum BDSG Nr. 26, Staatsanzeiger 1987, Nr. 1/2, S. 7; a. A. *Sutschet*, RDV 2004, 102, der § 11 BDSG unabhängig von der Übertragung von etwaigen Funktionen immer anwenden will, wenn ein Auftragsverhältnis vorliegt.

617 *Kramer/Hermann*, CR 2003, 938.

618 *Sutschet*, RDV 2004, 97; *Kramer/Hermann*, CR 2003, 938.

chen Pflichten und ist Dritter im Sinne des BDSG.[619] Zudem ist die Weitergabe eine Übermittlung im Sinne des § 3 Abs. 4 Satz 2 Nr. 3 BDSG, die einer Rechtsgrundlage als Übermittlungsvoraussetzung bedarf.

Von den obigen Fällen, dass keine Auftragsdatenverarbeitung vorliegt und damit die vollständige Verantwortung beim Nutzer verbleibt, sind die Fälle der Funktionsübertragung abzugrenzen, bei denen die Stelle, an die die Funktion übertragen wurde, voll verantwortlich ist. Zwischen diesen beiden Polen ist die Auftragsdatenverarbeitung angesiedelt, die die prinzipielle Verantwortlichkeit gegenüber dem Betroffenen beim Auftraggeber (Cloudnutzer) belässt und den Auftragnehmer (Cloudprovider) privilegiert, aber im Innenverhältnis dem Auftragnehmer gewisse, in § 11 BDSG näher beschriebene Pflichten auferlegt.[620]

Im Folgenden sollen nun die Abgrenzungskriterien zwischen Auftragsdatenverarbeitung und Funktionsübertragung kurz dargestellt und gewürdigt werden.

Das Abgrenzungskriterium der „Übertragung einer Funktion“ ist nach der ablehnenden Meinung untauglich, weil der Begriff der „Funktion“ unklar sei. Identische Datenweitergaben mit vergleichbaren Zwecksetzungen seien eher willkürlich einmal als Auftragsdatenverarbeitung und ein anderes Mal als Funktionsübertragung anzusehen. Als Beispiel wird die Datenweitergabe an einen Steuerberater zum Zweck der Gehaltsabrechnung (Auftragsdatenverarbeitung) und zur steuerlichen Beratung (Funktionsübertragung) eines Arbeitnehmers angeführt. Die Differenzierung sei nicht begründbar, weil die Gefährdungslage für den Betroffenen in beiden Fällen gleich sei.[621]

Nach dem Gedanken, dass derjenige die datenschutzrechtliche Verantwortung tragen soll, der die Entscheidung trifft, soll das Kriterium der eigenverantwortlichen Tätigkeit eine Auftragsdatenverarbeitung ausschließen. Kritik wird aber daran geübt, dass die Eigenverantwortung bei der Durchführung der Tätigkeit nicht zwingend mit der datenschutzrechtlichen Verantwortlichkeit identisch ist. So ist das Beispiel eines Datenvernichters, der in eigener Verantwortung die Art und Weise der Löschung der Datenträger bestimmt und gegenüber dem Auftraggeber für den Erfolg verantwortlich ist, nach allgemeiner Auffassung trotz dieser Eigenverantwortung datenschutzrechtlich dennoch eine Auftragsdatenverarbeitung und gerade keine Funktionsübertragung. Das Kriterium ist demzufolge untauglich.[622]

Weitere in der Literatur erwähnte Abgrenzungskriterien sind der Gefahrengedanke und die Überwachbarkeit. Demnach liegt eine Auftragsdatenverarbeitung immer

---

619 *Wächter*, CR 1991, 333.

620 *Kramer/Hermann*, CR 2003, 938, 940 sehen vor allem die Sicherungsmaßnahmen nach § 9 BDSG samt Anlage als wesentliche Pflicht des Auftragnehmers.

621 *Sutschet*, RDV 2004, 99.

622 *Sutschet*, RDV 2004, 99.

dann vor, wenn durch die rein mechanische Datenerhebung oder Datenverwendung des Dienstleisters keine zusätzlichen Gefahren geschaffen werden (Gefahrengedanke) und der Dienstleister bei seiner Tätigkeit der Aufsicht und den Weisungen des Auftraggebers unterliegt (Überwachbarkeit).[623] Unklar ist jedoch, was „mechanischer Umgang“ bedeuten soll, zumal mit den Daten elektromagnetisch umgegangen wird. Manche sehen im Begriff „mechanisch“ den Gegensatz zum eigenverantwortlichen Umgang mit Daten.[624] Dieses Kriterium wurde aber bereits oben als untauglich eingeordnet, so dass die beiden Kriterien „Gefahrengedanke“ und „Überwachbarkeit“ nicht in der Lage sind, die Funktionsübertragung von der Auftragsdatenverarbeitung klar und eindeutig abzugrenzen.

Eine neuere Literaturmeinung will die Abgrenzung nicht anhand des rechtlichen Dürfens, sondern anhand der tatsächlichen Umstände vornehmen. Je stärker die tatsächliche Fähigkeit des Auftraggebers ist, Datenmissbrauch und mangelhaften Datenschutz durch den Auftragnehmer zu verhindern, desto eher ist von einer Auftragsdatenverarbeitung auszugehen. Kriterien sollen die Komplexität des ausgelagerten Verfahrens, die tatsächliche Einwirkungsmöglichkeit und die Fachkunde des Auftraggebers sein.[625]

Bei dieser Methode ist allerdings nur nachträglich und unter größten Schwierigkeiten ermittelbar, ob die jeweiligen Kriterien vorliegen. Das beste Beispiel ist die fehlende Fachkunde des Auftraggebers. Würde man dieser Ansicht folgen, so wäre es mehr oder weniger vom Zufall, nämlich den Eigenbemühungen des Auftraggebers sich weiterzubilden, abhängig, wie ein rechtliches Verhältnis ausgestaltet ist. Wie genau diese Fachkunde ermittelt und festgestellt werden kann, ist ein weiteres Problem.

Ebenso ist das Kriterium der Komplexität nicht weiterführend. Es ist nicht ersichtlich, wieso ein komplexes Verfahren anders behandelt werden soll. Komplexität bedeutet nämlich nicht zwingend verminderte Einwirkungsmöglichkeit. Bestes Beispiel ist gerade Cloud Computing. Die Komplexität steigt zwar mit jedem zusätzlichen Subunternehmer, jedoch kann eine sorgfältige Auswahl und Überwachung die Gefahren für die Daten der Betroffenen geringer halten als bei einer direkten Geschäftsbeziehung zwischen einem Auftraggeber und einem Auftragnehmer, bei der der Auftraggeber seine Pflichten völlig außer Acht lässt.

Bei der tatsächlichen Einwirkungsmöglichkeit soll insbesondere die geographische Entfernung eine maßgebliche Rolle spielen.[626] Angesichts moderner Kommunikationsmöglichkeiten ist dies kein zeitgemäßes Kriterium. Bis auf die Frage der persön-

---

623 *Kramer/Hermann*, CR 2003, 938; *Sutschet*, RDV 2004, 99.
624 *Sutschet*, RDV 2004, 99.
625 *Elbel*, RDV 2010, 208.
626 *Elbel*, RDV 2010, 208.

lichen Begehbarkeit der Datenverarbeitungsanlagen durch den Auftraggeber, spielt diese faktisch keine Rolle. Der Auftraggeber kann in Zeiten moderner Kommunikationsmittel auch trotz großer Entfernungen effektiv auf den Auftragnehmer einwirken.

Trotz der Vielfalt an Kriterien ist die Funktionsübertragung demnach immer noch sehr schwer von der Auftragsdatenverarbeitung abzugrenzen. Das Hauptproblem am Konzept einer Funktionsübertragung ist der Umstand, dass diese im Gesetz keinen Anklang gefunden hat. So sind vor allem mögliche Grenzen der Auftragsdatenverarbeitung und der damit verbundenen Privilegierung gesetzlich nicht festgelegt.[627]

Am ehesten ist weiterhin das namensgebende Kriterium der Übertragung einer Funktion heranzuziehen, um diese Grenze zu ziehen, auch wenn diese Grenzziehung im Einzelfall oft willkürlich geschieht und der Funktionsbegriff alles andere als eindeutig ist. Im Zusammenhang mit Cloud Computing ist beispielsweise an den Fall zu denken, dass mit der Bereitstellung von spezieller Software als Service ganze Geschäftsprozesse, wie das Kundenbeziehungsmanagement (CRM) oder Enterprise Resource Planning (ERP), von einem spezialisierten Provider (mit)erledigt werden. In solchen Fällen einer sehr weiten Übernahme von ursprünglichen Aufgaben des Auftraggebers ist nur schwer zu begründen, wieso der Provider privilegiert werden sollte und die datenschutzrechtliche Verantwortlichkeit alleine beim Nutzer verbleiben sollte.

Für den weit überwiegenden Teil der Clouddienste scheidet eine Funktionsübertragung aus, so dass sich die Frage stellt, ob für Cloud Computing Auftragsdatenverarbeitung in Betracht kommt. Bei der Betrachtung dieser Fragestellung bietet es sich an, die unterschiedlichen Schichten gesondert zu betrachten.

3.1.8.4 Cloud Computing als Auftragsdatenverarbeitung?

Ob Cloud Computing mit seinen drei Unterformen als Datenverarbeitung im Auftrag eingeordnet werden kann, hängt maßgeblich vom genauen Schutzumfang des § 11 BDSG ab. Zum Schutzzweck und Schutzumfang des § 11 BDSG im Kontext von Rechenzentren und Rechenkapazität gibt es in der Literatur zwei Auffassungen.

Nach einer Auffassung sollen vom Schutzzweck des § 11 BDSG die Fälle umfasst sein, in denen externe Stellen personenbezogene Daten des Auftraggebers zur Kenntnis nehmen oder auf diese einwirken.[628] Keine Auftragsdatenverarbeitung ist dieser Ansicht zufolge gegeben, wenn kein Eingriff der Mitarbeiter in die eigentliche Datenverarbeitung erfolgt. Die erhöhte Schutzbedürftigkeit des Betroffenen

---

[627] *Sutschet*, RDV 2004, 100; *Kramer/Hermann*, CR 2003, 939.

[628] *Müthlein*, RDV 1993, 167; *von Sponeck*, CR 1992, 595.

liegt in der selbständigen Erledigung durch einen Dritten, außerhalb der eigentlichen Stelle.[629]

Zudem sei es für die Annahme einer Auftragsdatenverarbeitung notwendig, dass die beauftragte Person oder Stelle unterstützend tätig wird, was bei einem Rechenzentrum, das online und ausschließlich durch den Auftraggeber gesteuert wird, nicht der Fall sein soll.[630] Die bloße Sachherrschaft über die Rechenanlage und notwendige Hilfsdienste, um diese am Laufen zu halten, sollen nicht ausreichend sein.[631] Die bloße Anmietung von Rechenzentren und Rechenkapazität soll also gerade keine Auftragsdatenverarbeitung darstellen.[632] Für die Annahme einer Auftragsdatenverarbeitung reicht es nicht aus, dass Rechenkapazität durch einen Dritten zur Verfügung gestellt wird und nur der reine Maschinenbetrieb ausgelagert wird.[633]

Zusammengefasst soll nach der ersten Auffassung keine Auftragsdatenverarbeitung dann vorliegen, wenn drei Voraussetzungen vorliegen. Dem Kunden wird die reine Rechenleistung überlassen, die Verarbeitung oder Nutzung erfolgt ausschließlich durch den Kunden und der Dienstleister wird bei der Datenverarbeitung nicht unterstützend tätig.

Konsequenz der Ablehnung einer Auftragsdatenverarbeitung ist der Verbleib der kompletten Verantwortung für den Datenschutz und die Datensicherheit beim Nutzer als verantwortliche Stelle. Er selbst oder sein Beauftragter für den Datenschutz muss sowohl bei der Auswahl des Rechenzentrums, aber vor allem auch bei der folgenden Verarbeitung der Daten, alle gebotenen Datenschutzmaßnahmen treffen.[634]

Die zweite Literaturansicht lässt dagegen die bloße Möglichkeit des Datenzugriffs, beispielsweise durch die beim Auftragnehmer beschäftigten Mitarbeiter, ausreichen, um eine Datenverarbeitung im Auftrag annehmen zu können.[635]

Aber auch nach der ersten, restriktiven Auffassung kann Auftragsdatenverarbeitung dann angenommen werden, wenn der Betreiber des Rechenzentrums die Fertigung von Sicherungskopien und deren Aufbewahrung übernimmt, mithin also unterstützend tätig wird.[636]

3.1.8.4.1 Infrastructure as a Service

Folgt man der ersten Auffassung, wird Infrastructure as a Service (IaaS), je nach Ausgestaltung der Services, regelmäßig nicht als Auftragsdatenverarbeitung anzu-

---

629 *von Sponeck*, CR 1992, 595.
630 *Müthlein*, RDV 1993, 167.
631 *von Sponeck*, CR 1992, 595.
632 *Müthlein*, RDV 1993, 168; *von Sponeck*, CR 1992, 595.
633 *Müthlein*, RDV 1993, 168; *Gola/Schomerus* 2010, BDSG, § 11, Rn. 8.
634 *Gola/Schomerus* 2010, § 11, Rn. 8; *Böken*, iX 04/2011, 115; *Engels*, K&R 2011, 549.
635 *Walz*, in: Simitis, BDSG, 2006, § 11, Rn. 14.
636 *Müthlein*, RDV 1993, 168; *Gola/Schomerus* 2010, § 11, Rn. 8; *Engels*, K&R 2011, 549.

sehen sein, da hierbei der Nutzer die volle Kontrolle über die Datenverarbeitung behält und der Anbieter nur die Hardwarekapazitäten, wie eben Rechenleistung oder Speicherplatz, bereitstellt.[637] Der Anbieter nimmt die Daten nicht zur Kenntnis und wird bei der eigentlichen Datenverarbeitung nicht unterstützend tätig und wirkt auf diese auch nicht ein.

Jedoch wird man dieser Auffassung entgegenhalten müssen, dass die Bereitstellung der Infrastruktur über das Internet bereits eine Unterstützungshandlung darstellen könnte, aber auf alle Fälle durch die physische und lokale Verarbeitung der Daten in den Servern des Anbieters auf die Daten eingewirkt wird. Bestes Beispiel für eine Einwirkung ist der Umstand, dass bei der Verarbeitung etwas schief gehen kann, beispielsweise dass durch einen Stromausfall Daten zerstört werden. Demzufolge ist es mit der zweiten Literaturmeinung ausreichend, dass eine Möglichkeit zur Einwirkung besteht. Gleiches gilt für die bloße Möglichkeit der Kenntnisnahme durch die Mitarbeiter des Cloudproviders.

Der ersten Auffassung zufolge soll jedoch die bloße Möglichkeit, Daten zur Kenntnis zu nehmen, nicht ausreichen, da diese Kenntnisnahme auch bei der Datenverarbeitung im eigenen Haus immer möglich sei.[638] Allerdings ist diese Annahme insoweit falsch, weil bei einer eigenen lokalen Datenverarbeitung die Mitarbeiter unmittelbar überwachbar und instruierbar sind, während eine solche unmittelbare Überwachung bei einem externen Rechenzentrumsbetreiber faktisch ausscheidet, so dass bei der Betrachtung der Kenntnisnahmemöglichkeiten differenziert werden muss.

Im Übrigen werden die IaaS-Services auch regelmäßig so ausgestaltet sein, dass der Provider Sicherungskopien und Backups der Daten macht, die auf seinen Infrastrukturen vorgehalten werden, oft sogar in einem identischen Spiegelrechenzentrum, so dass meist auch nach der ersten Auffassung bei IaaS Auftragsdatenverarbeitung anzunehmen ist und somit die beiden Auffassungen zum gleichen Ergebnis, nämlich der Anwendbarkeit des § 11 BDSG, kommen.[639]

3.1.8.4.2 Restliche Services (PaaS, SaaS)

Auch bei den beiden Formen Platform as a Service (PaaS) und Software as a Service (SaaS) wird die Nutzung von Cloudservices eines Cloudproviders durch einen Cloudnutzer regelmäßig nach beiden Auffassungen ein Auftragsdatenverarbeitungsverhältnis im Sinne des § 11 BDSG darstellen. Insbesondere greifen die ausschließenden Voraussetzungen der ersten Auffassung nicht, weil die Daten auch beim Anbieter und nicht ausschließlich beim Nutzer verarbeitet werden und ersterer dabei üblicherweise auch noch unterstützend tätig wird. Bei SaaS ist diese Unter-

[637] So auch *Engels*, K&R 2011, 550.
[638] *von Sponeck*, CR 1992, 596.
[639] So auch *Engels*, K&R 2011, 549.

stützung durch die komplette anbieterseitige Bereitstellung der Software sogar die Grundlage des Geschäftsmodells.

Viele sehen daher für Cloud Computing, ohne jedoch detailliert zwischen den Schichten und Nutzungsmodellen zu differenzieren, unproblematisch die Anwendbarkeit der Vorschriften über die Auftragsdatenverarbeitung als gegeben an, soweit diese innerhalb der EU oder des EWR stattfindet.[640]

Zusammenfassend lässt sich feststellen, dass Cloud Computing mit seinen Unterformen das gesamte streitige Spektrum rund um die Auftragsdatenverarbeitung abdeckt. An einem Ende ist manchmal unklar, ob überhaupt Auftragsdatenverarbeitung vorliegt, wie dies für IaaS gezeigt wurde, während am anderen Ende Dienstleistungen erbracht werden können, die so weit gehen, dass an eine Funktionsübertragung zu denken ist (CRM oder ERP). Der weit überwiegende Teil der praktisch verfügbaren Clouddienste ist aber in Form der Auftragsdatenverarbeitung benutzbar.

3.1.8.5 Detailstruktur der Auftragsdatenverarbeitung

3.1.8.5.1 Pflichten des Auftraggebers und wesentliche Merkmale einer Auftragsdatenverarbeitung den Auftraggeber betreffend

Der Auftraggeber einer Datenverarbeitung bleibt gemäß § 11 Abs. 1 Satz 1 BDSG und § 3 Abs. 7 3. Alternative BDSG datenschutzrechtlich als „Herr über die Daten“ verantwortlich, er hat gemäß § 11 Abs. 2 Satz 1 BDSG den Auftragnehmer sorgfältig auszuwählen und muss die Auftragserteilung gemäß § 11 Abs. 2 Satz 2 BDSG schriftlich erteilen.

Der schriftlichen Auftragserteilung geht gemäß § 11 Abs. 2 Satz 2 Nr. 1 BDSG als erster Punkt des Katalogs die „Pflicht“ voraus, den Gegenstand und die Dauer des Auftrags festzulegen. Dies ist jedoch keine Pflicht im klassischen Sinne, da bei einer Auftragserteilung im Rahmen einer Datenverarbeitung im Auftrag ohnehin eine Spezifizierung der Vereinbarung hinsichtlich des Auftragsgegenstands und der Dauer erfolgen muss.[641]

Weitere Pflichten des Auftraggebers sind die Erteilung von Weisungen zur Verarbeitung oder Nutzung der Daten gemäß § 11 Abs. 2 Satz 2 und § 11 Abs. 3 Satz 1 BDSG oder die Überprüfung der Einhaltung der erteilten Weisungen gemäß § 11 Abs. 1 Satz 1 BDSG. Mit der Neufassung des § 11 BDSG wurden weitere Pflichten in den Gesetzeswortlaut mit aufgenommen.

---

[640] *Pohle/Ammann*, CR 2009, 273; *Niemann/Paul*, K&R 2009, 449; *Schulz*, MMR 2010, 75; *Schuster/Reichl*, CR 2010, 38; *Gola/Schomerus* 2010, § 11, Rn. 8; *Schulz*, in: Taeger/Wiebe, Inside the Cloud, 411; *Karger/Sarre*, in: Taeger/Wiebe, Inside the Cloud, 434; *Heidrich/Wegener*, MMR 2010, 805 f.; *Petri*, in: Simitis, BDSG, § 11, Rn. 30; *Hennrich*, CR 2011, 548; eine differenzierte Betrachtung erfolgt aber durch *Engels*, K&R 2011, 548.

[641] *Hoeren*, DuD 2010, 689.

Die bis zum 1.9.2009 gültige Fassung enthielt weitgehend unkonkrete und allgemeine Vorgaben, wie ein Auftragsdatenverarbeitungsverhältnis zustande kommen sollte und welche Anforderungen nötig waren. Auch die notwendigen Inhalte eines Vertrages zwischen Auftraggeber und Auftragnehmer waren nur in Ansätzen geregelt. Konkret waren gemäß § 11 Abs. 2 Satz 2 Halbsatz 2 BDSG die Datenerhebung, -verarbeitung oder -nutzung, die technisch-organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen.

Mit der sogenannten „Datenschutznovelle II“[642] aus dem Jahr 2009 wurde die Regelung der Auftragsdatenverarbeitung in § 11 BDSG vom Gesetzgeber neu strukturiert und modernisiert. Die Neuregelung des § 11 BDSG erfolgte zusammen mit neuen Regelungen zum Direktmarketing und basierte auf einer Bundesratsinitiative.[643] Der aufgetrennte Entwurf des Bundesinnenministeriums, der ursprünglich auch einen Vorschlag für ein Datenschutzauditgesetz enthielt, wurde am 3.7.2009 vom Bundestag als Gesetz verabschiedet.[644]

Die, auch nach altem Recht, bereits bestehenden Pflichten der Auftraggeber wurden durch einen nicht abschließenden „10-Punkte-Katalog“ in § 11 Abs. 2 Satz 2 BDSG konkretisiert.[645]

Regelungsziel der Neufassung des Gesetzeswortlauts war somit nicht die Ausweitung der Verpflichtungen, sondern die bessere Erkennbarkeit der Pflichten für die Rechtsanwender und Adressaten der Regelung, also die an der Auftragsdatenverarbeitung beteiligten Auftraggeber und Auftragnehmer.[646] Datenschutzaufsichtsbehörden zufolge konnten die Adressaten in den alten Regelungen nur schwer erkennen, was genau von ihnen verlangt wurde.[647]

Konkreter Hintergrund für die Neustrukturierung waren die gehäuft auftretenden Datenskandale in Callcentern. Der Bundesrat war der Ansicht, dass mit den alten Regelungen den Unsitten, die insbesondere in Callcentern vorherrschten, wonach nähere Festlegungen zu einem Auftrag mündlich oder überhaupt nicht erfolgten, nicht beizukommen war.[648] Nicht zuletzt deswegen wurde auch die Neueinführung

---

642 Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Bestimmungen, BR-Drs. 4/09 vom 2.1.2009.

643 BT-Drs. 16/12011, 40; *Hoeren*, DuD 2010, 688.

644 BT-Drs. 16/12011 und BT-Drs. 16/13657; *Hoeren*, DuD 2010, 688; zum Entwurf eines Gesetzes zur Regelung des Datenschutzaudits siehe auch Kap. 3.1.10 und Fn. 642.

645 *Hoeren*, DuD 2010, 689 bezeichnet die Aufzählung in § 11 Abs. 2 Satz 2 BDSG sogar als „eine Art Mustervertrag“.

646 *Vander*, K&R 2010, 293; *Eckhart*, DuD 2009, 588.

647 BR-Drs. 4/1/09, 8; *Vander*, K&R 2010, 293.

648 BR-Drs. 4/09, 7, 8; *Hoeren*, DuD 2010, 688.

einer Bußgeldbewehrung bei Verstößen gegen § 11 Abs. 2 Satz 2 BDSG durch den Bundesrat begrüßt.[649]

Vor der Neuregelung wurden insbesondere die gesetzlichen Erfordernisse einer ordnungsgemäßen, hinreichend spezifizierten und detaillierten schriftlichen Auftragserteilung kaum beachtet.[650] Hierbei ist nicht nur der Auftrag an sich schriftlich zu fixieren, sondern auch und gerade die datenschutzrechtlichen Anforderungen. Pauschale Verweisungen auf den Gesetzeswortlaut reichen dabei nicht aus. Die schriftliche Ausgestaltung muss die konkreten Maßnahmen im jeweiligen Auftragsverhältnis explizit nennen.[651] Auch die bloße Wiedergabe des Gesetzeswortlauts genügt, ausweislich der Gesetzesmaterialien, gerade nicht.[652] Für die Praxis bedeutet dies, dass die Verträge nach der Neuregelung deutlich bestimmter und konkreter gefasst werden müssen.

Zur Erleichterung der Anpassung haben verschiedene Verbände und Behörden Musterverträge für Auftragsdatenverarbeitungen nach dem neuen § 11 BDSG im Internet veröffentlicht. So hat unter anderem das Regierungspräsidium Darmstadt einen solchen Mustervertrag entworfen, der aber mittlerweile wieder aus dem Netz entfernt wurde, da er als überarbeitungsbedürftig erkannt wurde. Außerdem ist bei der Gesellschaft für Datenschutz und Datensicherung e.V. (GDD)[653] ein auf Grundlage des neuen § 11 BDSG erstellter Vertrag abrufbar und auch der BITKOM[654] hat ein solches Muster veröffentlicht, das zudem auch Übersetzungshilfen in englischer Sprache enthält.[655] Beachtenswert ist, dass die Muster an die individuellen Verträge und Vertragsumstände angepasst werden müssen.

Nach § 11 Abs. 2 Satz 2 Nr. 4 BDSG sind die Berichtigung, Löschung und Sperrung ebenfalls vertraglich zu regeln. Die Neuregelung ist dabei so zu verstehen, dass der Auftraggeber sicherstellt, dass der Auftragnehmer die Berichtigung, Löschung und Sperrung ausführt, wenn der Auftraggeber hierzu gegenüber dem Auftragnehmer verpflichtet ist.[656] In Cloudumgebungen führt dies zu einer erheblichen Erleichterung, da es dann ausreicht, dass der Cloudnutzer die Berichtigung, Löschung oder Sperrung per Webinterface oder sonstige Software anweist und der

---

649 BR-Drs. 4/09, 8.

650 BR-Drs. 4/09, 7.

651 *Vander*, K&R 2010, 294.

652 BR-Drs. 4/1/09, 9; *Eckhart*, DuD 2009, 588.

653 *GDD*, Muster: Auftrag gemäß § 11 BDSG, https://www.gdd.de/nachrichten/arbeitshilfen/Mustervereinbarung%20a7%2011%20BDSG_final1.doc.

654 *BITKOM*, Mustervertragsanlage zur Auftragsdatenverarbeitung, http://www.bitkom.org/files/documents/Mustervertragsanlage_zur_Auftragsdatenverarbeitung_v_3_0.pdf.

655 *Moos*, Musterverträge zur Auftragsdatenverarbeitung nach § 11 BDSG, http://blog.dlapiper.com/detechnology/entry/mustervertr%C3%A4ge_zu_11_bdsg_n.

656 *Eckhart*, DuD 2009, 589.

Auftragnehmer, also der Cloudprovider, die Daten dann anschließend tatsächlich berichtigt, sperrt oder physisch löscht.

Mit der Neuregelung stellt sich außerdem die Frage, ob der Auftraggeber einseitig die Vertragsmodalitäten vorgeben oder sogar durchsetzen muss oder ob diese, wie bisher, zwischen Auftraggeber und Auftragnehmer ausgehandelt werden können.[657] Der Wortlaut und die Gesetzesbegründung geben nichts für eine einseitige Vorgabe her, so dass eine einvernehmliche Abstimmung weiterhin möglich ist. Insbesondere bei den technischen und organisatorischen Maßnahmen gemäß § 11 Abs. 2 Satz 2 Nr. 3 BDSG muss eine solche Abstimmung möglich sein.[658]

Für Datenverarbeitungen im Auftrag sind zudem die zu regelnden Vorgaben des § 11 Abs. 2 Satz 2 Nr. 2 BDSG zu beachten. Während die Art und der Zweck der Datenverwendung im Vorhinein festlegbar sind, sind der Umfang der Datenverarbeitung und der Kreis der Betroffenen nicht so einfach festzustellen, da sich diese Merkmale im Laufe der Geschäftsbeziehung ändern können. Allerdings sind spätere Änderungen nicht cloudspezifisch und nachträglich im Vertrag anpassbar.

Gleiches gilt für die Berechtigung zur Begründung möglicher Unterauftragsverhältnisse gemäß § 11 Abs. 2 Satz 2 Nr. 6 BDSG. Dabei ist zu beachten, dass lediglich die Berechtigung an sich, nicht aber der einzelne Unterauftragnehmer einer näheren vorlaufenden Spezifizierung bedarf. Es reicht also aus, im Vorhinein das „Ob“ und das „Wie“ einer Unterbeauftragung festzulegen. In der Praxis kommen zum Beispiel die Unterbeauftragung durch Weisung oder nach schriftlicher Zustimmung des Cloudnutzers als Auftraggeber in Frage.[659] Weil der Nutzer auch für die vom Provider genutzten Subunternehmen verantwortlich bleibt, kann es angebracht sein, dass er sich einen Zustimmungsvorbehalt vor der Inanspruchnahme eines konkreten Subunternehmens sichert.[660] So kann er konkrete vom Provider zur Unterauftragsdatenverarbeitung ausgesuchte Subunternehmen überprüfen und gegebenenfalls ablehnen.

Es erscheint aber fraglich, ob, insbesondere bei großen Public Clouds, eine solche „Einmischung“ der Kunden in den Betrieb der Cloud vom Provider erwünscht ist. Im Grunde genommen müsste dieser vor der Nutzung von Subunternehmen die Zustimmung aller Kunden einholen oder überhaupt erst nach deren Weisung ein solches Subunternehmen beauftragen. Bisher sind keine Fälle bekannt, dass auch nur ein Cloudprovider in der Alltagspraxis so vorgehen würde.

Da ein solcher genereller Zustimmungsvorbehalt oder Tätigwerden nur nach Weisung in der Praxis wohl nur schwer umgesetzt werden kann, wird in der Literatur

---

657 *Eckhart*, DuD 2009, 588.

658 *Eckhart*, DuD 2009, 589.

659 *Gola/Schomerus* 2010, § 11, Rn. 18e.

660 *Eckhart*, Information Management und Consulting 4/2010, 59.

als Lösungsansatz die Klassifizierung von Subunternehmen und der Aufbau von Kategorien vorgeschlagen. Während bestimmte Kategorien unter Zustimmungsvorbehalt im Einzelfall gestellt werden, können andere generell und sogar vorab genehmigt werden, sofern bestimmte vorher vom Cloudnutzer festgelegte Parameter und Voraussetzungen vom Subunternehmen erfüllt sind.[661]

Im Zusammenhang mit § 11 Abs. 2 Satz 2 Nr. 2 BDSG fordern einige Stimmen in der Literatur, dass ein Auftraggeber „Art und Umfang der Datenverarbeitung sowie Ort und Zeit vollständig kennen (beherrschen) muss".[662] Indes ist festzustellen, dass solche Anforderungen im Gesetzeswortlaut nicht zu finden sind. Man könnte diese gesetzlich unbestimmten Anforderungen allenfalls aus dem Umstand, dass der Auftraggeber „Herr der Auftragsdatenverarbeitung" sein sollte, herleiten.

Folgt man dieser Literaturmeinung und nimmt eine solche Anforderung an, so wäre dabei genauer zwischen Kenntnis und Beherrschung durch den Auftraggeber zu differenzieren. Hinsichtlich der Kenntnis ist zudem zwischen vorlaufender und nachträglicher Kenntnis des Auftraggebers zu unterscheiden.

Es stellt sich die Frage, ob der Auftraggeber im Vorhinein wissen muss, wo und wann genau die Datenverarbeitung durch den Auftragnehmer stattfindet. Zudem stellt sich die weitere Frage, ob es ausreicht, dass der Ort und die Zeit im Vertrag festgelegt werden oder ob der Auftraggeber jedes Detail jeder einzelnen Verarbeitung vorher kennen muss.

Dem Auftragnehmer obliegt „die tatsächliche technische Ausführung der Datenverarbeitung".[663] Es ist daher ausreichend, wenn der Auftraggeber die groben örtlichen und zeitlichen Umstände kennt. Bei Cloud Computing wäre dies zum Beispiel hinsichtlich des Ortes gewahrt, wenn die Daten innerhalb einer abgegrenzten Region, zum Beispiel der EU, verbleiben. Anknüpfungspunkt wäre demnach die potentielle Änderung von rechtlichen Rahmenbedingungen. So müsste man bei einer Möglichkeit des Verlassens des EU-Raumes, nicht zuletzt wegen der erheblichen rechtlichen Folgen, dem Auftraggeber eine vorherige Kenntnisnahmemöglichkeit einräumen oder ihn darauf hinweisen. Im Beispielsfall der EU-Cloud würde es demzufolge dann ausreichen, wenn der Auftraggeber nachträglich über Logs und Protokolldaten die Einhaltung der räumlichen Beschränkung überprüfen oder allgemein den örtlichen und zeitlichen Verlauf der Datenverarbeitung und -übermittlung nachvollziehen kann.

Neben den rechtlichen Umständen hinsichtlich der Orte der Datenverarbeitung kann auch die IT-Sicherheit für den Ort der Datenverarbeitung Relevanz haben. So kann ein Auftraggeber die Nutzung ganz bestimmter Rechenzentren vorgeben und andere

---

661 *Eckhart*, Information Management und Consulting 4/2010, 60.

662 *Schuster/Reichl*, CR 2010, 41; *Heidrich/Wegener*, MMR 2010, 806.

663 *Gola/Schomerus* 2010, § 11, Rn. 4.

ausschließen wollen, beispielsweise weil bei einem bestimmten Rechenzentrum des Auftragnehmers oder eines Subunternehmens in der Vergangenheit vergleichsweise viele oder schwerwiegende Datenverluste aufgrund mangelhafter IT-Sicherheitsmaßnahmen aufgetreten sind. Solche Vorbehalte müssen im Voraus vertraglich festgeschrieben werden und deren Einhaltung durch Monitoring, also auch wieder durch Logs und Protokolldaten, überprüfbar sein. Aus den Logs ergeben sich im Regelfall auch die Zeiten der Verarbeitung. Insofern ergeben sich rein praktisch für Clouddienstleistungsverhältnisse keine Besonderheiten. Ob ein Anbieter auf solche spezifischen Wünsche des Kunden als Auftraggeber eingehen wird, ist in der Praxis angesichts der standardisierten und homogenen Bereitstellung als Massengeschäft eher zu bezweifeln. Die aktuelle Praxis zeigt, dass allenfalls eine Beschränkung auf die EU-Region dem Nutzer als Option zur Verfügung steht.

Neben der Kenntnis wird auch die Beherrschung und Beherrschbarkeit als Merkmal und Möglichkeit einer Auftragsdatenverarbeitung in der Literaturmeinung erwähnt.[664] Diese soll wohl bedeuten, dass der Auftraggeber in Echtzeit auf die Verarbeitung beim Auftragnehmer Einfluss nehmen können muss. Eine solche weite Einflussmöglichkeit ist aber weder gesetzlich vorgesehen, noch ist eine solche in herkömmlichen Auftragsdatenverarbeitungsverhältnissen der Fall. Der Auftraggeber beauftragt gerade deshalb Auftragnehmer, um sich gerade nicht mit der tatsächlichen Durchführung auseinandersetzen zu müssen. Hätte er die volle Verfügungsgewalt über den Ort und die Zeit der Datenverarbeitung, wäre der Aufwand für die Echtzeitüberwachung des Auftragnehmers durch den Auftraggeber, um bei Bedarf steuernd eingreifen zu können, oft genauso hoch, wie wenn der Auftraggeber die Datenverarbeitung selbst durchführt. Die Forderung nach der Beherrschung ist demnach auch dann gewahrt, wenn er bereits im Voraus oder nachträglich steuernd auf die Prozesse beim Auftragnehmer Einfluss nehmen kann.

Bei Cloud Computing besteht das vermeintliche Problem, dass auch ein Cloudprovider nicht vorhersagen könne, wo und wann eine Datenverarbeitung stattfindet. Tatsächlich ist es aber so, dass der Cloudprovider immer steuernd eingreifen und beispielsweise die Verarbeitung in bestimmten Rechenzentren von vornherein ausschließen kann, so dass dadurch die Beherrschung gewahrt ist. Mangelnde exakte Vorhersehbarkeit bedeutet nicht mangelnde Steuerungsfähigkeit. Der Nutzer als Auftraggeber kann seinerseits auf den Provider vertraglich oder tatsächlich einwirken und somit die Datenverarbeitung mindestens mittelbar beherrschen. Dass diese Steuerungsmöglichkeiten heutzutage von den Cloudprovidern nicht oder nur ansatzweise eingeräumt werden, bedeutet jedoch nicht, dass Cloud Computing an sich nicht beherrscht werden könnte.[665]

---

[664] Vergleiche obiges Zitat, wonach ein Auftraggeber „Art und Umfang der Datenverarbeitung sowie Ort und Zeit vollständig kennen (*beherrschen*) muss“.

[665] Wohl anderer Auffassung *Heidrich/Wegener*, MMR 2010, 806.

Zudem hat der Auftraggeber anderweitige Kontrollpflichten, die von Gesetzes wegen vorgesehen sind und mit Pflichten des Auftragnehmers korrelieren, um die Steuerungsfähigkeit des Auftraggebers zu gewährleisten.

Für Cloud Computing ist die Konkretisierung der Kontrollpflichten besonders relevant. Während sich in § 11 Abs. 2 Satz 4 BDSG a. F. der Auftraggeber allgemein von der Einhaltung der technisch-organisatorischen Maßnahmen überzeugen musste, hat sich der Auftraggeber mit der Neufassung der Vorschrift „vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen“. Hintergrund der Neuregelung waren die oftmals unzureichenden Kontrollen der Auftraggeber, insbesondere wenn Call-Center Auftragnehmer waren. Die von diesen begangenen schwerwiegenden Datenschutzverletzungen hielten die Öffentlichkeit zeitweise wochenlang in Atem.[666]

Die Kontrollpflichten gelten damit sowohl bei als auch nach Auftragserteilung. Außerdem sind nach der Neuregelung in § 11 Abs. 2 Satz 5 die Ergebnisse der Kontrollen durch den Auftraggeber zu dokumentieren. Unklar ist allerdings welche Anforderungen an die Dokumentation der Kontrollen zu stellen sind.[667] Der Gesetzeswortlaut gibt diesbezüglich, trotz der Bemühung um eine Konkretisierung und Vereinfachung für den Gesetzesanwender, leider nichts her.

Für Cloud Computing in Public Clouds ist die Klärung der Art und Weise der Überzeugungsbildung im Sinne des § 11 Abs. 2 Satz 4 BDSG besonders relevant, da eine Überzeugung vor Ort und in Person des Auftraggebers regelmäßig und zum Teil prinzipbedingt unmöglich ist. Zum einen ist vorab meist unklar, wo und wann genau die Daten gespeichert werden und zum anderen werden die Cloudanbieter ihre Rechenzentren kaum für den Kundenverkehr öffnen wollen, da eine Vor-Ort-Begehung ihrerseits ein Sicherheitsrisiko schafft. Durch die Besichtigung vor Ort können nämlich physische Angriffe auf die Hardware und Infrastruktur ermöglicht werden. Auch das Auskundschaften von möglichen Lücken im Sicherheitskonzept wird durch eine Besichtigung vor Ort erleichtert.

Üblicherweise unterliegen die Standorte und genauen Einzelheiten über die Belegung mit Servern, der tatsächliche Auf- und Ausbau und die Art und Weise der Stromversorgung oder der Kühlung der Datenzentren der Geheimhaltung. Auf die physische Abschottung der Serverparks und die Überwachung wird ebenfalls großen Wert gelegt. Wie oben bereits dargelegt, liegt auch gerade in dieser Art der Datenaufbewahrung die erhöhte Sicherheit gegenüber der lokalen Speicherung in Unternehmen oder bei Privatnutzern auf herkömmlichen Rechnern und Servern. Der Ausfall eines Großrechenzentrums durch einen Angriff ist zwar wegen der de-

---

666 *Vander*, K&R 2010, 294.

667 *Vander*, K&R 2010, 295.

zentralen Ausgestaltung und redundanten Speicherung in Clouds oft weniger gravierend wie bei der Zerstörung eines dedizierten Unternehmensrechenzentrums, jedoch kann ein physischer Angriff auf ein Cloudrechenzentrum trotzdem zu erheblichen Beeinträchtigungen und Datenverlusten für die Cloudnutzer führen. Beispiele sind die Zerstörung der Hardware durch Bombenangriffe oder die vorsätzlich herbeigeführte Unterbrechung der Stromversorgung oder der Kühlsysteme. Die Geheimhaltung der Standorte folgt demnach dem Prinzip der „Security by Obscurity". Zudem wird klar, dass die physische Abschottung auch für Cloud Computing Relevanz hat, wenn auch weniger für die Sicherheit konkreter Daten, sondern die allgemeine Datensicherheit und insbesondere für die Funktionstüchtigkeit und damit Verfügbarkeit der Dienste. Die Überzeugungsbildung vor Ort wäre demnach für die Datensicherheit kontraproduktiv.

Ausweislich der Gesetzesmaterialien ist vom Gesetzgeber eine solche Vor-Ort-Begehung allerdings auch nicht vorgeschrieben. Es wird davon abgesehen, dass sich der Auftraggeber unmittelbar beim Auftragnehmer vor Ort oder selbst in Person überzeugen muss.[668] Gesetzlich wird auch keine Prüfung im klassischen Sinne, sondern nur die Überzeugungsbildung verlangt.[669] Begründet wird dies damit, dass eine Vor-Ort-Begehung regelmäßig nicht angemessen und mit einem Verlust an Flexibilität verbunden wäre. Für die Überzeugungsbildung beim Auftraggeber soll demnach beispielsweise die Einholung eines Testats eines Sachverständigen oder sogar nur die schriftliche Auskunft des Auftragnehmers ausreichen.[670] Hinsichtlich des letzten Beispiels in den Gesetzesmaterialien ergibt sich jedoch ein Wertungswiderspruch zur davor geäußerten Gesetzesintention, die eine mittelbare Kontrollmöglichkeit durch den Auftraggeber für erforderlich erachtet.[671] An diesem Beispiel wird ersichtlich, dass die vom Gesetzgeber intendierten Anforderungen für die Überzeugungsbildung sehr niedrig sind. Demnach wird die Kontrolle durch Sachverständige im Rahmen von Audits und Zertifizierungen ausreichend sein und künftig wahrscheinlich der Regelfall der Überzeugungsbildung werden.[672]

Eine solche externe Überprüfung ist meist auch effektiver, da den Cloudnutzern das Know-how fehlt, um bei Kontrollen Mängel zu identifizieren und vom Anbieter abstellen zu lassen. Für die sachverständige Prüfung kann auf existierende Standards zurückgegriffen werden. Um spezifischen Problemen des Cloud Computing

---

668 BT-Drs. 16/13657, 18; gleicher Ansicht *Eckhart*, DuD 2009, 589; *ders.*, Information Management und Consulting 4/2010, 59; *Weichert*, DuD 2010, 682; *Essoh/Doubrava/Münch* 2011, 63; *Dorschel*, in: Schartner/Weippl, D-A-CH Security 2010, 182; *Gaul/Koehler*, Betriebsberater 2011, 2231.

669 *Eckhart*, DuD 2009, 589.

670 BT-Drs. 16/13657, 18.

671 *Vander*, K&R 2010, 295.

672 Ähnlich *Heidrich/Wegener*, MMR 2010, 806; das Unterwerfen unter ein anerkanntes Zertifizierungsverfahren wird auch von den Aufsichtsbehörden als ausreichend angesehen; siehe hierzu *Budszus/Heibey/Hillenbrand-Beck/Polenz/Seifert/Thiermann* 2011, 9.

gerecht zu werden, können auch die Entwicklung neuer cloudspezifischer Standards vorangetrieben werden oder vorhandene Standards ergänzt werden.[673]

Bei der Art und Weise der Kontrollen ist außerdem zu beachten, dass der Gesetzgeber vor allem an die erstmalige Kontrolle der technischen und organisatorischen Maßnahmen hohe Anforderungen stellt. Die Gesetzesmaterialien sprechen von der „besonderen Bedeutung“ der ersten Kontrolle vor Beginn der Datenverarbeitung und davon, dass der Auftraggeber zu diesem Zeitpunkt „noch Unzulänglichkeiten abstellen“ kann und die „erste Kontrolle daher besonders umfassend“ erfolgen müsse. Bei den nachgelagerten weiteren Kontrollen sollen dagegen nur Veränderungen seit der letzten Kontrolle geprüft werden.[674] Zudem hat eine erste Kontrolle immer stattzufinden, während Folgekontrollen von der Dauer der Auftragsdatenverarbeitung abhängig sind und unter Umständen entfallen können.[675] Bei den regelmäßig nur situativ eingegangenen Vertragsverhältnissen bei Cloud Computing sind vom Auftraggeber initiierte regelmäßige Folgekontrollen eher die Ausnahme. Dass ein Cloudprovider von sich aus Folgekontrollen anstößt, liegt in seinem Interesse. In der Praxis wird der Provider ohnehin eine durchgängige Zertifizierung vorweisen, da er logischerweise nicht bei jedem Eingehen einer neuen, oft nur kurzzeitigen Geschäftsbeziehung eine Neuzertifizierung anstoßen kann. In großen Public Clouds mit unzähligen Nutzern und einer entsprechenden Fluktuation wäre dies zudem auch praktisch unmöglich.

Hinsichtlich der Häufigkeit der Kontrollen fällt auf, dass der Gesetzgeber es unterlassen hat, starre Fristen, beispielsweise die halb- oder jährliche Kontrolle, festzusetzen. Starre Fristen würden nämlich nicht der in der Praxis vorkommenden Bandbreite an Auftragsdatenverarbeitungen gerecht werden.[676]

Die gleichen Erwägungen gelten den Gesetzesmaterialien zufolge hinsichtlich der näheren Ausgestaltung der Art und des Umfangs der Dokumentation der Kontrollen. So kann zum Beispiel der Umfang einer Dokumentation je nach Größe und Komplexität der Auftragsdatenverarbeitung variieren.[677] Das grundsätzliche Erfordernis einer Dokumentation wird hingegen deutlich herausgestellt, denn nur durch eine Dokumentation lässt sich der Handlungszeitpunkt nachweisen und nur dadurch kann sich ein Auftraggeber gegenüber einer Aufsichtsbehörde entlasten.[678] Taugliche Dokumentationen dürften vor allem Zertifikate anerkannter externer Prüf- und

---

673 Zu bereits existierenden Standards und der bereits erfolgten Zertifizierung von einigen Providern nach aktuellen Standards siehe auch Kap. 3.1.9.9.8.

674 BT-Drs. 16/13657, 22; *Vander*, K&R 2010, 295.

675 BT-Drs. 16/13657, 22.

676 BT-Drs. 16/13657, 18; *Vander*, K&R 2010, 295.

677 BT-Drs. 16/13657, 18.

678 BT-Drs. 16/13657, 18.

Zertifizierungsgesellschaften sowie standardisierte „Checklisten“ zur Verwendung durch den Auftraggeber sein.[679]

Für Cloud Computing bedeutet dies, dass die Häufigkeit und der Umfang der Dokumentation der Kontrollen – wie allgemein – vom jeweiligen Auftragsverhältnis abhängig sind. Als Indikatoren und Kriterien für die Kontrollhäufigkeit und den Prüfumfang könnten der Umfang einer Auslagerung, die Sensitivität der betroffenen Daten oder die geplante Laufzeit eines Auftrages herangezogen werden.[680] Vertragslaufzeiten von bis zu einem Jahr sollen wohl keine wiederholte Prüfung der technischen und organisatorischen Sicherheitsvorkehrungen nötig machen.[681]

Wie oben bereits angedeutet, sollte die regelmäßige Rezertifizierung des Providers durch Sachverständige den meisten Anforderungen der Nutzer als Auftraggeber in der Praxis gerecht werden. Soweit die Intervalle für einige Nutzer, wegen den eben angesprochenen individuellen Kriterien, zu lang sind, müssen diese auf den Provider einwirken und eine kurzfristigere Rezertifizierung verlangen oder die Nutzung des Dienstes einstellen. Im Optimalfall, also bei vorab bereits absehbar engen Kriterien und einer verstärkten Kontrollhäufigkeit, ist es geboten die Providerauswahl hiernach vorzunehmen und die Prüfhäufigkeit vertraglich abzusichern.

3.1.8.5.2 Kontrollrechte des Auftraggebers

Neben Kontrollpflichten räumt § 11 Abs. 2 Satz 2 Nr. 7 BDSG dem Auftraggeber Kontrollrechte ein, ohne dass diese im Wortlaut näher spezifiziert werden. Eine solche Spezifizierung kann allerdings im Vertrag zwischen dem Auftraggeber und dem Auftragnehmer festgehalten werden.[682]

Die Regelung wird so verstanden, dass sich der Auftraggeber ein Recht zur Kontrolle vor Ort, also in den Rechenzentren des Providers, vorbehalten muss. Im Einklang mit dem vorhin Gesagten ist es somit nicht notwendig, dass der Auftraggeber diese dann auch tatsächlich durchführt. Es reicht aus, dass er ein solches Kontrollrecht ausüben könnte. Hierfür ist es allerdings notwendig, dass der Cloudprovider als Auftragnehmer dem Cloudnutzer als Auftraggeber einige Informationen zukommen lässt, beispielsweise die Orte der genutzten Rechenzentren.[683] In der Praxis mangelt es sehr oft an diesem Erfordernis, da die Provider, wie bereits erwähnt, die Standor-

---

679 *Vander*, K&R 2010, 296.

680 *Vander*, K&R 2010, 295.

681 So zumindest *Vander*, K&R 2010, 295.

682 *Dorschel*, in: Schartner/Weippl, D-A-CH Security 2010, 181.

683 *Eckhart*, Information Management und Consulting 4/2010, 59.

te ihrer Rechenzentren geheim halten. Erste Ansätze eines Umschwungs sind aber erkennbar.[684]

3.1.8.5.3 Pflichten des Auftragnehmers

Mit den eben erwähnten Kontrollrechten des Auftraggebers korrespondiert, wie sich aus § 11 Abs. 2 Satz 2 Nr. 7 BDSG ergibt, die Pflicht des Auftragnehmers diese Kontrollen zu dulden und daran mitzuwirken.[685]

Besonders relevant, nicht zuletzt hinsichtlich der vertraglichen Ausgestaltung, ist die konkrete Festlegung der praxis- und sicherheitsrelevanten technisch-organisatorischen Maßnahmen und Zielvorgaben aus § 9 BDSG samt Anlage gemäß § 11 Abs. 2 Satz 2 Nr. 3 BDSG. Der Auftragnehmer ist nämlich gemäß § 11 Abs. 4 i.V.m. § 9 BDSG verpflichtet, in Eigenverantwortung die Maßnahmen zur Datensicherung zu treffen, die den vom BDSG geforderten Schutz der personenbezogenen Daten sicherstellen.[686] Die Sicherungsmaßnahmen sind vor Einsatz des Datenverarbeitungsverfahrens vorzunehmen, soweit diese nicht ohnehin kontinuierlich während der Datenverarbeitung anzuwenden und zu wahren sind. Die konkret getroffenen Maßnahmen muss der Auftragnehmer, also ein Cloudprovider mit Sitz in Deutschland, der zuständigen Aufsichtsbehörde in geeigneter Form darlegen können.

Neben die Verpflichtung zur Datensicherung und den Duldungs- und Mitwirkungspflichten tritt auch die Pflicht zur Wahrung des Datengeheimnisses gemäß § 11 Abs. 4 i.V.m. § 5 BDSG.[687] Zudem haben Auftragnehmer gemäß § 11 Abs. 2 Satz 2 Nr. 5 und Abs. 4 Nr. 2 i.V.m. §§ 4f, 4g und 38 BDSG einen Datenschutzbeauftragten zu bestellen.

Der Auftragnehmer ist schließlich gemäß § 11 Abs. 3 Satz 1 BDSG verpflichtet, die Daten nur „im Rahmen“ der Weisungen des Auftraggebers zu verarbeiten oder zu nutzen. Der Auftragsdatenverarbeiter ist demnach nicht strikt an die Weisungen des Auftraggebers gebunden, sondern agiert innerhalb des vorgegebenen Rahmens. So bildet zum Beispiel die Beauftragung eines Unternehmens zur Löschung von Datenträgern und die entsprechende Weisung den Rahmen dieser Weisung. Wie das Unternehmen die Daten dann letztlich löscht, ist ihm überlassen.[688] In diesem Zusammenhang ist auch auf die Auftragskontrolle gemäß Nr. 6 der Anlage zu § 9 BDSG hinzuweisen, so dass der Auftragnehmer durch technisch-organisatorische

---

684 *Chip Online*, Premiere: Erster Blick auf ein Cloud-Rechenzentrum, http://business.chip.de/news/Premiere-Erster-Blick-auf-ein-Cloud-Rechenzentrum_48757521.html; siehe hierzu insbesondere auch Fn. 738 mwN.

685 So auch *Hoeren*, DuD 2010, 690.

686 *Wächter*, CR 1991, 335; auf die Einzelheiten der zu treffenden Maßnahmen und Zielvorgaben wird weiter unten in einer umfassenden Darstellung in Kap. 3.1.9 einzugehen sein.

687 Zum Datengeheimnis siehe Kap. 3.1.11.

688 *Sutschet*, RDV 2004, 101.

Maßnahmen gewährleisten muss, dass Datenverarbeitungen nur im Rahmen der Weisungen des Auftraggebers möglich sind.[689]

Hinsichtlich der Weisungsgebundenheit des Auftragnehmers ist auch ausdrücklich darauf hinzuweisen, dass diese eine Rechtsfolge der Auftragsdatenverarbeitung und nicht deren Voraussetzung ist. Auch wenn der Auftraggeber sich jeder Weisung enthält und die Durchführung dem Auftragnehmer überlasst, liegt eine Datenverarbeitung im Auftrag vor.[690]

Wegen der datenschutzrechtlichen Verantwortlichkeit des Auftraggebers ist der Auftragnehmer außerdem nicht verpflichtet, die Weisungen auf ihre Übereinstimmung mit dem Bundesdatenschutzgesetz oder anderen datenschutzrechtlichen Vorschriften zu überprüfen. Allerdings kann er offensichtlich gegen datenschutzrechtliche Bestimmungen verstoßende Weisungen ablehnen und ihre Durchführung verweigern. Er ist dann jedoch verpflichtet, den Auftraggeber darauf hinzuweisen.[691]

Inwieweit von diesen Ablehnungsmöglichkeiten in der alltäglichen Praxis des Cloud Computing Gebrauch gemacht werden wird, muss die Zukunft zeigen. Es ist nur schwer vorstellbar, dass sich ein Cloudprovider nachträglich in die Feinheiten der vertraglichen Abrede einmischen wird, um mögliche Missstände beim Nutzer zu suchen und diesem solche zu melden. Dazu hat ein Provider nicht die nötigen Mitarbeiter und es entspricht auch nicht dem Geschäftsmodell, das, insbesondere bei Public Cloud Computing, auf ein standardisiertes Massengeschäft setzt. Der Vorteil für den Provider, aber auch den Kunden, ist gerade der, dass sich ersterer nicht um datenschutzrechtliche Belange kümmern muss und dies auch nicht will. Solange der Provider die Weisungen im Rahmen der Vorgaben des Auftraggebers ausführt, ist allen Beteiligten gedient.

Wegen des standardisierten Vorgehens der Cloudprovider wird es allerdings im Regelfall kaum bis gar keine Weisungsmöglichkeiten der auftraggebenden Nutzer geben. Dieses Fehlen von Weisungsmöglichkeiten muss dadurch kompensiert werden, dass Nutzern Optionsangebote, wie die Auswahl bestimmter Ressourcen, Regionen, Sicherheitsniveaus sowie sonstiger Anbieter- und Nutzungsmerkmale eröffnet werden.[692]

Sind Weisungen möglich, stellt sich das weitere Praxisproblem, dass die Weisungen missachtet, nicht vollständig oder falsch ausgeführt werden könnten. Dem wird der Provider jedoch im Vorfeld dadurch begegnen, indem er individuelle Weisungsmöglichkeiten durch den Auftraggeber, also den Kunden und Nutzer, nur be-

---

689 Siehe hierzu Kap. 3.1.9.3.2.6.

690 *Sutschet*, RDV 2004, 101.

691 *Wächter*, CR 1991, 335.

692 So auch *Weichert*, DuD 2010, 685.

schränkt oder überhaupt nicht (technisch) ermöglicht, beispielsweise, indem die softwareseitigen Einfluss- und Direktionsmöglichkeiten über Benutzereingabeschnittstellen vereinheitlicht, den vertraglichen Abreden angepasst und auf eine bestimmte Anzahl und Form der Einflussnahme reduziert werden.

Konkrete Einzelabreden und individuelle Weisungsmöglichkeiten sind allenfalls bei Community Clouds denkbar. Bei Private Clouds wird es bereits regelmäßig an einem Auftraggeber-Auftragnehmer-Verhältnis fehlen, so dass unternehmensintern keine Auftragsdatenverarbeitung möglich und nötig ist, so dass sich bei dieser Unterform des Cloud Computing das Weisungsproblem auch nicht stellt.

3.1.8.5.4 Wartungs- und Servicearbeiten

Der Vollständigkeit halber soll noch erwähnt werden, dass weder Auftragsdatenverarbeitung noch Funktionsübertragung bei der Tätigkeit von Wartungs- und Serviceunternehmen gemäß § 11 Abs. 5 BDSG gegeben sind. Da der Schutzbedarf jedoch mit dem eines Auftragsdatenverarbeitungsverhältnisses vergleichbar ist, sind die Vorschriften des § 11 Abs. 1 bis 4 BDSG nach dem Wortlaut des Abs. 5 entsprechend anzuwenden. Insbesondere die Einhaltung der Maßnahmen nach § 9 BDSG samt Anlage ist dabei zu gewährleisten.[693]

Cloudprovider, die sich demnach externer Dritter für solche Servicearbeiten bedienen, haben auch im Verhältnis zu diesen die eben erwähnten Vorkehrungen zu treffen. Dabei ist zu beachten, dass ein „Rollenwechsel“ stattfindet. Während der Cloudprovider als Auftragnehmer im Verhältnis zu den Cloudkunden agiert, tritt er im Verhältnis zu den Servicebetrieben entsprechend einem Auftraggeber auf. Diese Zuordnung hat erhebliche Bedeutung für die jeweiligen Rechte und Pflichten. Soweit wartungsspezifische Maßnahmen oder Pflichten auftreten, die einer klassischen Auftragsdatenverarbeitung fremd sind, sind diese zusätzlich im schriftlichen Auftrag festzuhalten.[694]

3.1.8.5.5 Bußgeldtatbestände

Eine zweite wesentliche Änderung der Datenschutznovelle II, die die Auftragsdatenverarbeitung betrifft, ist der Erlass eines neuen Bußgeldtatbestandes in § 43 Abs. 1 Nr. 2b BDSG. Dieser enthält zwei Begehungsalternativen. Ordnungswidrig handelt demzufolge, wer entgegen § 11 Abs. 2 Satz 2 BDSG einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Absatz 2 Satz 4 BDSG sich nicht vor Beginn der Datenverarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt. Verantwortlich für die Regelung der Auftragsmodali-

---

693 *Gola/Schomerus* 2010, § 11, Rn. 14; siehe hierzu auch die Ausführungen im Zusammenhang mit § 203 StGB in Kap. 3.8.1.2.

694 *Petri*, in: Simitis, BDSG, § 11, Rn. 102.

täten ist demzufolge der Auftraggeber, auch wenn die Abstimmung einvernehmlich mit dem Auftragnehmer erfolgen kann.[695] Nicht bußgeldbewehrt sind somit Verstöße gegen die Pflicht zur regelmäßigen Kontrolle der Sicherheitsvorkehrungen und gegen die Dokumentationspflicht aus § 11 Abs. 2 Satz 5 BDSG.[696]

Weitere Neuerungen bei den datenschutzrechtlichen Bußgeldern sind die Verdopplung des Maximalbetrags von 25 000 Euro auf 50 000 Euro bezogen auf die Tatbestandsalternativen in § 43 Abs. 1 BDSG, die Erhöhung von 250 000 Euro auf 300 000 Euro bezogen auf § 43 Abs. 2 BDSG sowie die, lediglich klarstellende, Einführung einer Gewinnabschöpfungsregelung entsprechend § 17 Abs. 4 OWiG, der auch bisher im Rahmen von datenschutzrechtlichen Geldbußen zur Anwendung kommen konnte.[697] Die Geldbuße soll gemäß § 43 Abs. 3 Sätze 2 und 3 BDSG den wirtschaftlichen Vorteil, den der Täter aus einer Ordnungswidrigkeit gezogen hat, übersteigen. Sollten die in § 43 Abs. 3 Satz 1 BDSG genannten Beträge hierfür nicht ausreichen, so können sie im Einzelfall überschritten werden.[698]

Zielsetzung der neuen Bußgeldvorschriften ist die bessere Durchsetzbarkeit der gesetzlichen Vorgaben. Allerdings bestehen erhebliche Zweifel an der Bestimmtheit einiger Tatbestandsalternativen. Insbesondere die Verpflichtungen gemäß § 11 Abs. 2 Satz 2 BDSG werfen erhebliche Unwägbarkeiten auf. Während man noch klar bestimmen kann, ob ein Auftrag schriftlich erteilt wurde, ist weitgehend unklar, wann von einer „vollständigen“ oder gar „nicht richtigen“ Auftragserteilung ausgegangen werden kann. Bei der Aufzählung in § 11 Abs. 2 Satz 2 BDSG handelt es sich, wie oben bereits erwähnt, um Regelbeispiele für Pflichten, die nicht abschließend sind, so dass es trotz Erfüllung aller dort aufgeführten Pflichten in Einzelfällen dennoch zu einer „unvollständigen“ Auftragserteilung führen kann. Dieser Bußgeldtatbestand dürfte deshalb wegen Verstoßes gegen das Bestimmtheitsgebot aus Artikel 103 Abs. 2 GG nichtig sein.[699]

3.1.8.6 Mögliches Transparenzproblem und Problem der Unterbeauftragung (Auslagerungsketten)

Mit der Weisungsgebundenheit des Auftragnehmers (Cloudproviders) steht die Grundkonzeption des Public Cloud Computing im Dissens. Der Auftragnehmer und vor allem der Auftraggeber haben nicht die gleiche Kontrollmöglichkeit wie bei einer Private Cloud. Es ist Merkmal des Public Cloud Computing, dass die Daten nach Verfügbarkeit von Ressourcen verteilt werden. Insbesondere die flexible Nutzung von externen Ressourcen bei Subunternehmen ist Kennzeichen hierfür.[700] Eine

---

695 Siehe oben Kap. 3.1.8.5.1.
696 *Vander*, K&R 2010, 296.
697 *Hanloser*, MMR 2009, 598.
698 *Vander*, K&R 2010, 296.
699 *Hanloser*, MMR 2009, 597; *Vander*, K&R 2010, 296.
700 Siehe dazu auch die Kap. 2.3.3.2 und 3.1.8.5.1.

solche mehr oder weniger zufällige Eingehung von Unterauftragsverhältnissen ist zudem mit der Gefahr von Auslagerungsketten verbunden. Der Provider bedient sich der Subunternehmen, die ihrerseits nachgelagerte Unternehmen beauftragen. Solche Auslagerungsketten und nachgelagerte Subprovider sind in § 11 BDSG jedoch nicht vorgesehen. Zwar ist in § 11 Abs. 2 Satz 2 Nr. 6 BDSG generell von Unterauftragsverhältnissen die Rede, allerdings sind damit die unmittelbar vom Auftragnehmer unterbeauftragten Subunternehmen gemeint.

Die Möglichkeit, Ketten von Subunternehmen zu bilden, besteht allerdings mit den neuerlassenen EU-Standardvertragsklauseln.[701] Die Unterbeauftragung in Kette ist aber grundsätzlich nur mit Zustimmung des Auftraggebers zulässig.[702] Wenn bereits die unmittelbare Inanspruchnahme von Subunternehmen an Voraussetzungen gebunden ist, gilt dies erst recht, wenn diese ihrerseits weitere Subunternehmen unterbeauftragen. Mit jedem „Glied in der Kette“ schwindet die Transparenz und Beherrschbarkeit des verantwortlichen Cloudnutzers als Auftraggeber.

Für Cloudprovider ist es deshalb vorteilhaft im Vorfeld eines Vertragsverhältnisses mit den Kunden eine schriftliche Festlegung aller Subunternehmen und eine Kategorisierung im oben erwähnten Sinne vorzunehmen und für die vorab genehmigten Unternehmen die schriftliche Zustimmung durch die Kunden einzuholen.[703] Das hat zwar einen Verlust von Flexibilität zur Folge, jedoch wird auch in der Praxis der Cloudprovider die jeweiligen Betreiber sorgsam auswählen, Verträge mit diesen abschließen und diese letztlich auch bezahlen müssen. Zudem hat er ein eigenes Interesse, dass diese sich nicht ihrerseits dubioser Subunternehmen bedienen, weil dadurch auch seine Kontrollfähigkeit eingeschränkt würde.

Für die weitere Auslagerung durch die Subunternehmen gelten dann erst recht die gleichen Voraussetzungen, wie für den Cloudprovider, sprich die Zustimmung durch den Cloudnutzer oder die Vereinbarung von sicheren und nicht zustimmungspflichtigen Subunternehmerkategorien und die jeweilige Einordnung der weiteren Subunternehmen.

Eine von Kontrollverlust gekennzeichnete Cloud kann im Geschäftsumfeld zu Vertrauensverlust und dem Verlust von Kunden führen, insbesondere wenn der Ernstfall eintritt und Daten bei einem Subunternehmen abhandenkommen. In letzter Konsequenz trifft der Kundenverlust dann den Cloudanbieter. Die Zufälligkeit der Datenverteilung ist demnach nur auf die vorher festgelegten und nachträglich vertraglich eingebundenen und zugestimmten Subunternehmen beschränkt. Alles ande-

---

701 Siehe dazu weiter unten Kap. 3.1.12.5.1.2.

702 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 148; zu den neuen EU-Standardvertragsklauseln vom 5.2.2010 siehe Kap. 3.1.12.5.1.2.

703 Siehe auch oben Kap. 3.1.8.5.1; *Eckhart*, Information Management und Consulting 4/2010, 60; hinsichtlich der schriftlichen Zustimmungsbedürftigkeit allgemein und nicht nur auf Cloud Computing bezogen *Ernestus*, in: Simitis, BDSG, § 9, Rn. 148.

re, insbesondere die unregulierte Nutzung von freien Kapazitäten Dritter, hätte letztlich auch den Verlust der Privilegierung durch § 11 BDSG zur Folge. Eine Weisung durch den Nutzer ist nicht mehr möglich, wenn noch nicht einmal der Provider genau weiß, wer in seinem Cloudverbund agiert. Auch die Unklarheit, in welchen Ländern die Subunternehmen agieren, hätte erhebliche datenschutzrechtliche Implikationen zur Folge.

Es ist also festzuhalten, dass die flexible Nutzung von Ressourcen in der Praxis tatsächlich nicht so leicht und unbeschwert erfolgt, wie oft angepriesen oder befürchtet wird. Bevor Daten in einem Pool von eigenen und angemieteten Ressourcen tatsächlich auf Zufälligkeiten (unterschiedliche Lastverteilungsalgorithmen, freie Kapazitäten, Nachfrage) basierend verteilt werden, müssen diese verfügbar sein. Die externen Ressourcen müssen angemietet, netzwerktechnisch angebunden und nicht zuletzt durch den Provider bezahlt werden.

Ein Transparenzproblem oder ein Problem des Kontrollverlusts hinsichtlich der Cloudinfrastruktur und der damit zusammenhängenden Geschäftsbeziehungen ergibt sich folglich für den Provider nicht. Das infrastrukturelle Geflecht einer Cloud ist für den Provider immer klar. Im Voraus unklar sind nur die Zeit und zum Teil der Ort einer Datenverarbeitung in dieser abgegrenzten Cloud. Hätte der Provider nicht die entsprechende Abgrenzungsmöglichkeit, wären auch regionale Clouds nicht möglich.

Rechtlich und in der künftigen alltäglichen Praxis ist allerdings zu gewährleisten, dass nicht nur der Provider, insbesondere in Fällen der Auftragsdatenverarbeitung, entscheidet, welche Subunternehmen oder Server genutzt werden, sondern der Cloudnutzer hierbei mitentscheiden können muss. Durch diese Mitentscheidungsmöglichkeit wird auch die Transparenz gefördert, was nicht zuletzt die Vorbehalte gegen Cloud Computing senken dürfte. Es ist allerdings einzugestehen, dass durch diesen Zusatzaufwand die Flexibilität leidet.

3.1.8.7 Spezialregelungen

Einige Besonderheiten und Beschränkungen der Auftragsdatenverarbeitung, auch hinsichtlich der Auslagerung in Clouds, bestehen für Sozialdaten. Sozialdaten sind durch das Sozialgeheimnis in § 35 SGB Abs. 1 i.V.m. § 67 ff. SGB X geschützt.

Gemäß § 80 Abs. 3 SGB X hat der Auftraggeber zum einen gegenüber seiner Aufsichtsbehörde erhebliche schriftliche Anzeigepflichten hinsichtlich gewisser zu erfüllender Voraussetzungen beim Auftragnehmer, beispielsweise die getroffenen technisch-organisatorischen Maßnahmen gemäß Nr. 1. Zudem unterliegt die Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag durch nichtöffentliche Stellen, also auch durch privatrechtliche Cloudanbieter, gemäß § 80 Abs. 5 SGB X gewissen Beschränkungen und ist als Ausnahme von der Regel anzusehen. Nach § 80 Abs. 5 Nr. 1 SGB X ist die Auslagerung erlaubt, wenn ansons-

ten Störungen im Betriebsablauf zu erwarten sind. Die zweite Ausnahme in § 80 Abs. 5 Nr. 2 Satz 1 SGB X erlaubt die Auslagerung, wenn die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden können und der Auftrag dabei nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst. Gemäß § 80 Abs. 5 Nr. 2 Satz 2 SGB X muss der überwiegende Teil der Speicherung des gesamten Datenbestandes beim Auftraggeber verbleiben. Im Übrigen kann die Datenverarbeitung im Auftrag den gesamten Datenbestand erfassen, soweit sie nicht Speicherung ist.[704] Durch die Beschränkungen wird die Auslagerung von Sozialdaten in eine Cloud zwar nicht unmöglich gemacht, jedoch dürfte sie unwirtschaftlich sein.[705]

In diesem Zusammenhang soll noch kurz erwähnt werden, dass es noch weitere Spezialvorschriften hinsichtlich der Auslagerung von Daten für bestimmte Branchen gibt, die jedoch keine Datenschutzvorschriften darstellen. Diese betreffen die interne Organisation und das betriebliche Risikomanagement und werden dementsprechend im Rahmen der Darstellung der Compliance kurz thematisiert.[706]

Auch strafrechtliche Vorschriften sind spezialgesetzlich zu beachten.[707] Die Weitergabe von fremden Geheimnissen an einen Auftragnehmer durch Ärzte, Apotheker, Angehörige der privaten Kranken- oder Lebensversicherungen, Rechtsanwälte, Steuerberater oder sonstige Berufsgeheimnisträger gemäß § 203 Abs. 1 Nr. 1 bis 6 StGB erfüllt eine unbefugte Offenbarung, so dass Auftragsdatenverarbeitung in solchen Fällen grundsätzlich nur mit Einwilligung der Betroffenen möglich ist, da sich ansonsten die Berufsgeheimnisträger gemäß § 203 Abs. 1 StGB strafbar machen.[708]

Eine nicht strafbare Weitergabe von Daten ohne Einwilligung der Betroffenen ist nur an Gehilfen der Berufsgeheimnisträger im Sinne des § 203 Abs. 3 Satz 2 StGB möglich. Einige sind der Ansicht, dass ein Cloudprovider als Auftragnehmer als ein solcher Gehilfe eingeordnet werden könnte. Dabei soll der Umstand, dass der schweigepflichtige Berufsgeheimnisträger die Herrschaft über die Auftragsdatenverarbeitung behält, den Ausschlag geben.[709] Der Provider würde „in den informationellen Schutzbereich eingebunden und als zum Kreis der zum Wissen Berufenen

---

704 *Bieresborn*, in: von Wulffen, SGB X, § 80, Rn. 12.

705 *Dix*, Datenschutz und IT-Sicherheit beim Cloud Computing, http://www.datenschutz-berlin.de/attachments/585/2008-datenschutzbericht_verlinkt_READER_vom_03.04.09.pdf, S. 16.

706 Siehe dazu Kap. 3.6.2.

707 Zu weiteren Strafvorschriften siehe auch Kap. 3.8.1.2.

708 *Ministerium des Innern des Landes Sachsen-Anhalt/Landesbeauftragte für den Datenschutz Sachsen-Anhalt*, Handreichung zur Auslagerung von Aufgaben (Outsourcing), http://www.sachsen-anhalt.de/index.php?id=20554.

709 *Eckhart/Giebichenstein/Helbing/Hilber/Niemann/Weiss* 2010, S. 20 f.; *Kühl*, in: Lackner/Kühl, StGB, § 203, Rn. 11b vertritt hingegen den Standpunkt, dass eine „organisatorische Anbindung der Datenverwalter an den Auftraggeber erforderlich ist"; zum Streitstand siehe außerdem *Lenckner/Eisele*, in: Schönke/Schröder, StGB, § 203, Rn. 64a.

gehörig angesehen werden".[710] Bei Einhaltung der strengen Kriterien des § 11 BDSG könnte demzufolge die Auslagerung von durch besondere Berufsgeheimnisse geschützten Daten in eine Cloud als Ausnahme der Weitergabe an Gehilfen nicht verboten sein.[711]

Ob sich diese Ansicht allerdings durchsetzen wird, muss die Zukunft zeigen. Insbesondere ist noch fraglich, welche genauen Maßstäbe an die tatsächliche Herrschaft des Schweigepflichtigen über die ausgelagerten Geheimnisse anzulegen sind. Angesichts dieser Zweifel und den strafrechtlichen Konsequenzen ist es für Berufsgeheimnisträger sicherer, wenn sie die Einwilligung der Betroffenen bei einer geplanten Auslagerung einholen.

3.1.8.8 Datenschutzrechtlicher Reformbedarf

Insbesondere für Cloud Computing sind die deutschen Vorschriften über die Verantwortlichkeit noch unzureichend, weil diese, anders als die Europäische Datenschutzrichtlinie, keine Möglichkeit der Verantwortlichkeit mehrerer Stellen (Joint Controllership) vorsehen.[712] Gerade bei Public Cloud Computing mit der Möglichkeit der Beteiligung einer Vielzahl von Subunternehmen wäre es wünschenswert, diese ebenfalls in den Verantwortungsbereich als „Joint Controller" mit einzubeziehen und dadurch die Schwierigkeiten einer effektiven Kontrolle des Providers als Auftragnehmer und des – nach geltender Rechtslage – allein verantwortlichen Nutzers als Auftraggeber zu reduzieren.

Die Verteilung der Verantwortlichkeiten ist in Cloudkonstellationen weder mit Auftragsdatenverarbeitung noch mit der Funktionsübertragung befriedigend zu regeln. Die Datenschutzaufsichtsbehörden schlagen vor, den Begriff der verantwortlichen Stelle auch im deutschen Datenschutzrecht an Art. 2 lit. d) DSRL anzupassen und damit „Joint Controllership" zu ermöglichen. Bei der Beteiligung mehrerer Stellen, also insbesondere bei Cloud Computing, fordern sie außerdem die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung von den tatsächlichen Einflussmöglichkeiten und der Interessenlage der Betroffenen abhängig zu machen. Die datenschutzrechtliche Verantwortlichkeit kann zum Beispiel auch nach einer Übermittlung fortbestehen, wenn wirtschaftliche oder tatsächliche Einwirkungsmöglichkeiten auf die Empfänger vorhanden sind. Die Betroffenen sollen zudem ihre Rechte gegenüber jeder verantwortlichen Stelle geltend machen können.[713]

---

710 *Eckhart/Giebichenstein/Helbing/Hilber/Niemann/Weiss* 2010, S. 20.

711 *Eckhart/Giebichenstein/Helbing/Hilber/Niemann/Weiss* 2010, S. 20.

712 Zur kollektiven Verantwortlichkeit für die Datenverarbeitung in Social Networks siehe *Roßnagel/Jandt*, ZD 2011, 160 ff.

713 Eckpunktepapier „Ein modernes Datenschutzrecht im 21. Jahrhundert" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18.3.2010, S. 15 f.

3.1.9 Technisch-organisatorische Maßnahmen zur IT- und Datensicherheit

3.1.9.1 IT-Sicherheit und Datensicherheit

IT-Sicherheit oder Informationssicherheit und Datensicherheit sind gleichzusetzen.[714] IT-Sicherheit und Informationssicherheit sind Begriffe der Informationstechnik, während die Datensicherheit und Datensicherung im juristischen Bereich, insbesondere in § 9 BDSG und der Anlage zu § 9 Satz 1 BDSG rechtlich thematisiert werden. Die Überschneidung ergibt sich folglich aus der in sich zusammenhängenden Bedeutung der beiden Begriffe „Information“ und „Daten“. Nach DIN 44300 Nr. 19 und DIN ISO/IEC 2382 sind Daten „Gebilde aus Zeichen oder kontinuierliche Funktionen, die aufgrund bekannter oder unterstellter Abmachungen Informationen darstellen“.[715] Informationen werden demnach aus Daten abgeleitet.

Im Zusammenhang mit § 9 BDSG wird unter IT-Sicherheit der Zustand verstanden, der durch organisatorische und technische Vorkehrungen bezogen auf Systeme, Systemkomponenten oder Verfahren der betreffenden Informationstechnik ein vorher bestimmtes Maß der Vertraulichkeit, Integrität und Verfügbarkeit von automatisiert zu verarbeitenden Informationen (Daten) gewährleistet.[716]

Datensicherheit meint die Gesamtheit aller organisatorischen und technischen Regelungen und Maßnahmen, mit denen ein unzulässiger Umgang mit personenbezogenen Daten verhindert und die Integrität sowie Verfügbarkeit der Daten und die zu deren Verarbeitung eingesetzten technischen Einrichtungen erhalten werden. Der ähnliche Begriff der Datensicherung bedeutet hingegen nur die Doppelung und Auslagerung (Backup) von Daten. Die Begriffe „Datensicherheit“ und „Datensicherung“ hängen insoweit zusammen, als durch die Datensicherungsmaßnahmen die Herstellung von Datensicherheit erreicht werden soll.[717]

Eine Zusammenführung der beiden Disziplinen Informationstechnik und Recht stellt § 2 Abs. 2 BSIG dar, der eine Legaldefinition der „Sicherheit in der Informationstechnik“, kurz gefasst also der „IT-Sicherheit“ beinhaltet. Sicherheit in der Informationstechnik im Sinne der Vorschrift bedeutet demnach die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen. Die Legaldefinition vermeidet es jedoch, diese verwendeten Begriffe ihrerseits näher zu beschreiben.[718] Ähnliches gilt im Übrigen für das neue Grundrecht auf Vertraulichkeit und Integrität eigengenutzter

---

[714] Wohl ähnlicher Ansicht *Schneider*, ZD 2011, 7.

[715] *Ernestus*, in: Simitis, BDSG, § 9, Rn. 2.

[716] *Ernestus*, in: Simitis, BDSG, § 9, Rn. 2; zur Vertraulichkeit, Integrität und Verfügbarkeit siehe Kap. 3.1.9.5.

[717] *Ernestus*, in: Simitis, BDSG, § 9, Rn. 2.

[718] Näheres dazu siehe in Kap. 3.1.9.5.

informationstechnischer Systeme, das jedoch zumindest durch das Urteil des Bundesverfassungsgerichts konkretisiert wird.

Aus dem Rückgriff auf das Bundesdatenschutzgesetz und das BSI-Gesetz wird deutlich, dass es kein IT-Sicherheitsgesetz in Deutschland gibt, sondern IT-Sicherheitsrecht eine heterogene Querschnittsmaterie und eine Gemengelage aus unterschiedlichen Rechtsgebieten und Vorschriften darstellt.[719] Hintergrund sind die unterschiedlichen Anwendungsbereiche und Schutzrichtungen der Gesetze, bei denen IT-Sicherheit allenfalls einen Teilaspekt ausmacht.[720] Man kann dabei grob zwischen produkt-, dienstleistungs- und organisationsbezogenen Regelungen unterscheiden.[721] Das aktuelle IT-Sicherheitsrecht orientiert sich außerdem an den spezifischen Bedürfnissen an die jeweils eingesetzte Informationstechnologie.[722] Einige halten es trotz dieser unterschiedlichen Zielrichtungen und Regelungshintergründe dennoch für angebracht über ein allgemeines und kohärentes IT-Sicherheitsgesetz nachzudenken.[723]

3.1.9.2 Bedeutung der Sicherheit allgemein und für den weiteren Gang der Untersuchung

Bevor auf die konkreten Regelungen mit Bezügen zum Datenschutz und zur Datensicherheit eingegangen werden soll, bietet es sich an, die einleitend erwähnte Bedeutung der Sicherheit allgemein und speziell als IT- und Datensicherheit für Cloud Computing in einen Gesamtzusammenhang zu bringen. Auch die Darstellung des weiteren Vorgehens ist nur in einem solchen übergreifenden und interdisziplinären Kontext verständlich.

Sicherheit ist ein Grundbedürfnis des Menschen und der Gesellschaft. Gerade in Zeiten der Globalisierung und der ansteigenden Abhängigkeit von Informations- und Kommunikationstechnik nimmt das Sicherheitsbedürfnis stetig zu.[724] Mit der Durchdringung der alltäglichen Belange mit Informationstechnologie geht die steigende Verwundbarkeit der Gesellschaft und des Einzelnen einher. Neben immensen wirtschaftlichen Schäden durch mangelnde IT-Sicherheit[725] sind sichere und funkti-

---

719 *Schmidl*, NJW 2010, 477; *Gaycken/Karger*, MMR 2011, 6; *Spindler*, MMR 2008, 9.

720 Zum Beispiel eben im BDSG oder dem BSIG; *Schmidl*, NJW 2010, 477.

721 *Spindler*, MMR 2008, 9.

722 *Heckmann*, MMR 2006, 281.

723 *Gaycken/Karger*, MMR 2011, 6; wohl auch *Spindler*, MMR 2008, 7 ff.; *Holznagel* 2002, 50.

724 *BSI*, Leitfaden Informationssicherheit, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile, S. 7.

725 Nach einer Mitteilung des Statistischen Bundesamtes hatte 2010 mehr als jedes zehnte Unternehmen in Deutschland Probleme mit der Sicherheit seiner Informationssysteme, so dass es durch fehlende Verfügbarkeit der Systeme oder die Zerstörung von Daten zu wirtschaftlichen Schäden kam; siehe dazu *Statistisches Bundesamt*, 11% der Unternehmen haben IT-Sicherheitsprobleme, http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/ Internet/DE/Presse/pm/2010/12/PD10__448__52911%2CtemplateId%3DrenderPrint.psml.

onierende kritische Infrastrukturen für den Bestand der Gesellschaft essentiell.[726] Aber auch ohne dieses gesteigerte Sicherheitsbedürfnis einer kritischen Infrastruktur muss Cloud Computing sicher sein. Risiken und Bedrohungen von Schutzgütern müssen analysiert werden, um im Lebenszyklus einer Technologie möglichst frühzeitig beseitigt zu werden. Im Optimalfall werden solche Probleme noch vor oder mit der Technikentwicklung beseitigt.

Ziele sind die Reduktion der Schadenswahrscheinlichkeit und – wesentlich bedeutsamer – die Verminderung des Schadenspotentials. So kann sich eine Bedrohung oder ein Risiko unproblematisch mit hoher Wahrscheinlichkeit verwirklichen, wenn gewährleistet ist, dass der zu erwartende Schaden vernachlässigbar ist.[727] Wegen der Komplexität von IT-Systemen und nicht vorhersehbaren Folgen, ist es jedoch immer ratsam, auch die Wahrscheinlichkeit eines Schadens, sprich die konkrete Ausnutzung eines Sicherheitsrisikos, zu minimieren. So kann zwar der Schaden durch die Ausnutzung einer Schwachstelle gering sein, jedoch besteht immer die Gefahr dass sich mit deren Ausnutzung weitere Bedrohungen für Rechtsgüter auftun, so dass zumindest mittelbar ein hohes Schadenspotential entsteht.[728]

Bedrohte Rechtsgüter sind insbesondere die informationelle Selbstbestimmung von Betroffenen, aber auch die Vertraulichkeit und Integrität der Systeme, die ebenfalls dem Schutz des allgemeinen Persönlichkeitsrechts des Einzelnen dienen. Auch die hohen Investitionen in Cloudtechnologien und -infrastrukturen rechnen sich nur, wenn die Sicherheit dieser Systeme und Daten in möglichst hohem Maße gewährleistet ist, so dass auch Aspekte des Eigentums nach Art. 14 GG eine Rolle spielen.

Weil ohne IT-Sicherheit kein effektiver Datenschutz und Schutz der informationellen Selbstbestimmung möglich ist, ist IT- und Datensicherheit ein wesentliches Ziel der rechtlichen Technikgestaltung. Wie zu sehen sein wird, werden zwar einzelne IT-Sicherheitsmaßnahmen rechtlich vorgegeben, jedoch sind diese rechtlichen Vorgaben völlig unzureichend und weitgehend veraltet, so dass es notwendig ist auf eine aktuelle informatische Betrachtung mit dem Ziel der Erreichung von IT-Sicherheit abzustellen. Diese erfolgt durch eine Darstellung und Systematisierung der anerkannten IT-Schutzziele.

Dabei müssen auch die Kernprobleme des Cloud Computing im Zusammenhang mit den IT-Schutzzielen erörtert werden. Im Anschluss wird in Form einer Bedrohungsanalyse auf die Bedrohungen, Gefahren und Risiken für die IT-Sicherheit allgemein und speziell in Cloudumgebungen einzugehen sein.[729] Die Gestaltung von

---

[726] Näheres zu kritischen Infrastrukturen siehe in Kap. 3.2.

[727] *Hammer* 1999, 112 ff., 268; *Roßnagel/Wedde/Hammer/Pordesch* 1990, 71, 74, 211.

[728] *Roßnagel/Wedde/Hammer/Pordesch* 1990, 209.

[729] Neben der technischen Gestaltung hat die Bedrohungsanalyse auch erhebliche Bedeutung für die Compliance von bestehenden IT-Systemen und Organisationsstrukturen; siehe dazu insbesondere Kap. 3.1.9.8 und Kap. 3.6.

Technik kann nur dann technisch optimal und rechtsgemäß erfolgen, wenn man die Gefahren und Gefährdungen möglichst umfassend kennt. Maßnahmen zur Gewährleistung und Erreichung der Sicherheit sollen bei der Darstellung der Schutzziele ebenfalls eine Rolle spielen, um dann schließlich noch einmal gesondert die wichtigsten Sicherheitsmaßnahmen als Ergebnis der Analyse darzustellen.

Der Hintergrund für die Trennung in allgemeine und cloudspezifische Bedrohungen hängt damit zusammen, dass die allgemeinen Bedrohungen regelmäßig auch Cloudsysteme betreffen. Nicht zuletzt der Umstand, dass bei Cloud Computing mehrere unterschiedliche Technologien zusammengeführt werden, lässt es angebracht erscheinen, diese, bei IT-Systemen praktisch immer vorzufindenden, Bedrohungen und Gefahren bildlich gesprochen „vor die Klammer“ zu ziehen. Die spezifischen Gefahren ergeben sich dagegen zum einen aus der Neuartigkeit der Technologie und zum anderen aus der eben erwähnten Kombination unterschiedlicher Technologien, die ihrerseits neue Sicherheitsprobleme erzeugt. Kombinationen von Technologien und Systemen führen außerdem zu einer Erhöhung der, bereits so schon relativ hohen, Komplexität. Ebenso sind Neukombinationen immer in der Lage lose vorhandene Kopplungen einzelner Untersysteme zu verstärken und damit das Schadenspotential im Fall eines Fehlers erheblich zu erhöhen.

Neben technischen Aspekten wird aus den einschlägigen Normen ein weiterer wesentlicher Aspekt von Sicherheit abgeleitet, nämlich Organisation. Dazu gehören frühzeitiges und möglichst umfassendes Risikomanagement, die aus einer Bedrohungsanalyse abgeleitete Erarbeitung von Sicherheitskonzepten, aber auch die Rollenverteilung in einem Unternehmen mit den entsprechenden Nutzungs- und Zugriffsbefugnissen. Die Befolgung von rechtlichen oder internen Vorgaben (Compliance) ist nur möglich, wenn klar ist, wer verantwortlich ist. Diese Verantwortlichkeit erhöht die Sicherheit, weil der Verantwortliche darauf achten wird, möglichst nicht gegen Regeln zu verstoßen. Außerdem wird er durch die Organisation von Abläufen und durch Weisungen andere dazu anhalten.

Neben der informatischen, organisatorischen und rechtlichen Absicherung gibt es jedoch auch weitere Aspekte wie die Nutzungskompetenz der beteiligten Personen und die Ergonomie der zu nutzenden Systeme. Unsichere Technologie ist nicht nur solche, die gegen Angriffe verwundbar ist, sondern auch solche, die durch Fehlbedienungen Schäden verursachen kann.

3.1.9.3 Geltende Rechtslage

Zentrale Vorschriften, die technische und organisatorische Maßnahmen und Sicherheitskonzepte rechtlich regeln, sind § 9 BDSG und die Anlage zu § 9 Satz 1 BDSG sowie § 109 TKG. § 78a SGB X ist im Sozialrecht die Parallelvorschrift zu § 9 BDSG und hat eine identische Anlage mit den gleichen Maßnahmen, die speziell für die Absicherung von Sozialdaten gilt.

3.1.9.3.1 Regelungsinhalt des § 9 BDSG und der Anlage zu Satz 1

§ 9 BDSG und die Anlage zu § 9 Satz 1 BDSG haben erhebliche Bedeutung für die Absicherung informationstechnischer Systeme mit dem Hauptziel des Schutzes personenbezogener Daten. Im Vordergrund steht zwar die Gewährleistung und Wahrung der Datensicherheit, jedoch dienen die Maßnahmen mittelbar auch dem Datenschutz. Wenn personenbezogene Daten ungesichert in einem Cloudrechenzentrum lagern oder verarbeitet werden und von Unberechtigten entwendet werden, weil der Zutritt zu diesem Rechenzentrum für jedermann möglich ist, so tangiert die fehlende Gebäudeabsicherung auch die Persönlichkeitsrechte der von dem Datenverlust Betroffenen. Für sicherheitsrelevante Fragestellungen im Rahmen von Cloud Computing, insbesondere welche konkreten Anforderungen und Maßnahmen zur Absicherung nötig sind, ist § 9 BDSG samt der Anlage zu Satz 1 somit eine zentrale Vorschrift. Die Vorschrift symbolisiert den technischen Datenschutz.[730]

Aus § 9 Satz 1 BDSG ergibt sich die Verpflichtung für öffentliche und nichtöffentliche Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um ein hohes Maß an Datensicherheit zu gewährleisten. Die Vorschrift richtet sich nicht nur an Stellen, die selbst Daten verarbeiten, sondern auch ausdrücklich an im Auftrag datenverarbeitende Stellen, wie im Wortlaut der Vorschrift erkennbar ist. Mit dem Ausdruck „haben“ wird auch die Pflicht zur Einhaltung und Gewährleistung der Anforderungen bekräftigt. Relativiert wird diese Verpflichtung mit Satz 2 der Vorschrift, wonach die Maßnahmen nur dann erforderlich sind, wenn ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht.

Die Anlage, auf die in Satz 1 verwiesen wird, konkretisiert die notwendigen Anforderungen und Maßnahmen. Sie stellt somit gleichzeitig die Mittel (Maßnahmen) als auch die notwendigen Voraussetzungen (Anforderungen oder Zielvorgaben) für die zu realisierende Datensicherheit dar. Während in § 9 Satz 1 BDSG die nichtabschließende Auflistung in der Anlage („insbesondere“) als „Anforderungen“ bezeichnet werden, ist in der Anlage selbst in den Sätzen zwei und drei von „Maßnahmen“ die Rede. Die acht Punkte in der Aufzählung werden untechnisch auch als „acht Gebote des Datenschutzes“ bezeichnet, was indes eine abschließende Wirkung suggeriert, die jedoch gesetzlich nicht gewollt ist.

Der Katalog in der Anlage zu § 9 BDSG enthält zwar, wie sogleich zu sehen ist, bereits wichtige Maßnahmen, jedoch sind diese sehr allgemein gehalten und können eine situationsspezifische Bedrohungsanalyse und die Einleitung und Gewährleistung von spezifischen Maßnahmen zur Beseitigung oder Vorbeugung von Bedrohungen und dementsprechenden Schäden nicht ersetzen. Sie geben aber grobe

---

730 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 1.

Hinweise für den Rechtsanwender, welche Bereiche er absichern muss, um einen Basisschutz der Daten zu erreichen.

Außerdem ist beachtlich, dass die Maßnahmen nicht nur technischer Natur sind, sondern und gerade auch die Organisation von datenverarbeitenden Stellen, also auch Cloudunternehmen, ein wesentlicher Aspekt der Datensicherheit ist. Insbesondere die betriebsinternen Abläufe und Zugangs- und Zutrittsberechtigungen sind hierbei von eminenter Bedeutung. Auch wenn interne Angreifer eher die Ausnahme bei Angriffen darstellen und damit Angriffe von innen einer geringen Wahrscheinlichkeit unterliegen,[731] haben die internen Angreifer durch ihre Einbindung in die Organisation und die damit einhergehende Kenntnis der Umstände oder sogar entsprechende Berechtigungen, wie beispielsweise Administratoren, die Möglichkeit durch ihre bösartig motivierten Handlungen besonders hohe Schäden zu verursachen. Betrachtet man also das Schadenspotential, so sind interne Angriffe regelmäßig mit einem höheren Schaden verbunden, als externe Angriffe.[732]

In Cloudumgebungen wird dies umso deutlicher. Neben dem Zugang zu den physischen Servern, können die internen Mitarbeiter auch die Absicherung durch die Hypervisoren umgehen. Im ersten Szenario kann beispielsweise ein wichtiger Rechner physisch zerstört werden, so dass mittelbar der komplette Cloudservice für längere Zeit ausfällt. Im Extremfall kann ein interner Angreifer die gesamten Datenbestände löschen oder unbrauchbar machen. Die Auswahl und Überwachung der Mitarbeiter ist somit ein wesentlicher sicherheitsrelevanter Kernpunkt der innerbetrieblichen Organisation.

Flankierend zu § 9 BDSG samt Anlage ist die Regelung des § 9a BDSG, wonach zur Verbesserung des Datenschutzes und der Datensicherheit Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen können.[733]

3.1.9.3.2 Maßnahmen gemäß der Anlage

Vorab ist festzuhalten, dass die notwendigen Schutzmaßnahmen in *allen* Rechenzentren eines Cloudproviders und eventuell beteiligter Subunternehmen getroffen werden müssen. Es muss also schon vor der Datenverarbeitung klar sein, in welchen Rechenzentren die Daten gespeichert oder verarbeitet werden könnten. Zwar ist bei

---

[731] In einer Studie kam der britische Sicherheitsdienstleister 7Safe zusammen mit der University of Bedfordshire zum Ergebnis, dass nur zwei Prozent der untersuchten Einbrüche auf interne Angreifer zurückzuführen waren, siehe hierzu *Bachfeld*, Studie bestätigt das Ende der Legende vom internen Angreifer, http://www.heise.de/security/meldung/Studie-bestaetigt-das-Ende-der-Legende-vom-internen-Angreifer-914773.html; *7Safe*, UK Security Breach Investigations Report, http://www.7safe.com/breach_report/Breach_report_2010.pdf.

[732] *Holznagel* 2003, 26; *Eckert* 2006, 16; siehe dazu auch Kap. 3.1.9.8.4 und Fn. 959.

[733] Siehe dazu ausführlich Kap. 3.1.10.

Cloud Computing in der Regel im Voraus unklar, wann und wo genau Daten gespeichert oder verarbeitet werden, jedoch ist immer klar, welche Rechenzentren insgesamt an der Speicherung oder Verarbeitung von Daten beteiligt sein werden, so dass die Umsetzung der Maßnahmen auch vorab praktisch möglich ist. Im Übrigen dürfte ein professionell geführtes Rechenzentrum die Maßnahmen, die vorab umsetzbar sind, ohnehin von sich aus in irgendeiner Form umsetzen. Wichtiger ist allerdings die fortwährende Beachtung und Umsetzung der auf Dauer angelegten Maßnahmen. Im Folgenden sollen nun die einzelnen Maßnahmen aufgezeigt und ihre Tauglichkeit im Hinblick auf Cloudumgebungen erörtert werden.

3.1.9.3.2.1 Zutrittskontrolle (Nr. 1)

Zutrittskontrolle bedeutet, dass Unbefugten der körperliche und räumliche Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, verwehrt wird. Es soll damit verhindert werden, dass unbefugte Personen unkontrolliert in die Nähe von oder in Datenverarbeitungsanlagen gelangen, wodurch sich Möglichkeiten unbefugter Kenntnis- oder Einflussnahme ergeben.[734] Die dafür tauglichen Maßnahmen sind vielfältig. Erwähnt seien die Einteilung in Sicherheitszonen und Sperrbereiche, Schranken, Closed-Shop-Betriebe, Chipkarten, Transponderkarten, Berechtigungsausweise, Schlüsselregelungen, Personenkontrollen durch Pförtner oder Vereinzelungsanlagen.[735] Im Ergebnis also übliche Zutrittsberechtigungskonzepte und bauliche Gebäude- und Raumsicherungsmaßnahmen, wobei unter Umständen auch eine optische Abschirmung in Betracht kommen kann.[736]

Hinsichtlich der Cloudrechenzentren ergeben sich keine Besonderheiten oder Abweichungen zu herkömmlichen Rechenzentren. Insbesondere sind nicht zwingend Maßnahmen nötig, um den Kunden den Zutritt zwecks Besichtigung zu ermöglichen, weil diese Vor-Ort-Besichtigungen im Rahmen von Auftragsdatenverarbeitungsverhältnissen regelmäßig nicht notwendig sind, da die bloße Überzeugungsbildung laut Gesetzesbegründung ausreicht. Diese kann auch schriftlich durch den Auftragnehmer oder durch beauftragte Sachverständige als Prüfer erfolgen.[737] Dadurch wird auch die Zutrittskontrolle erleichtert, weil kein „Publikumsverkehr“ durchgeschleust werden muss, sondern nur noch die zwingend notwendigen Rechenzentrumsmitarbeiter und einige wenige Sachverständige die Räumlichkeiten betreten müssen.

---

[734] *Gola/Schomerus* 2010, § 9, Rn. 22; *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 9, Rn. 6; *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5, Rn. 39.

[735] *Gola/Schomerus* 2010, § 9, Rn. 22.

[736] *Roth*, ITRB 2010, 60, 61.

[737] Siehe dazu Kap. 3.1.8.5.1.

Soweit ein Anbieter, was wohl äußerst selten vorkommen dürfte, auch den Kunden die Möglichkeit der persönlichen Besichtigung[738] vor Ort einräumen will, muss er entsprechende Vorkehrungen treffen, zum Beispiel die Durchführung von Personenkontrollen, die Einrichtung von Sicherheitszonen oder die Ausgabe von Berechtigungsausweisen, um dem Zutrittskontrollgebot zu genügen. Auch flankierende Maßnahmen, wie die Überwachung der Besucher mittels Überwachungskameras oder die Begleitung durch Sicherheitspersonal sind angezeigt, um nach dem Passieren des Zutrittskontrollpunkts weiterhin auf die in der Anlage befindlichen Personen einwirken zu können. Dabei spielt insbesondere das Szenario eine Rolle, dass sich Angreifer als Kunden tarnen, um bei einer Besichtigung vor Ort Schäden an der physischen Infrastruktur zu verursachen.

3.1.9.3.2.2 Zugangskontrolle (Nr. 2)

Durch Zugangskontrollen soll sichergestellt werden, dass nur Berechtigte die Datenverarbeitungsanlagen und IT-Systeme nutzen können.[739] Es geht dabei nicht, wie bei der Zutrittskontrolle, um die räumliche Annäherung, sondern um den technisch-organisatorischen Zugang und die faktische Nutzungsmöglichkeit der IT-Systeme.[740] Demnach ist nicht nur auf die Hardware, im Sinne einer physischen Annäherungsmöglichkeit, sondern auf ein „Datenverarbeitungs*system*“, mithin also auf eine Kombination von Hardware, Software und Daten, abzustellen.

Nutzung ist jede im Wege der Datenverarbeitung sich vollziehende Einflussnahme auf den Verarbeitungsprozess.[741] Die Möglichkeit hierzu reicht bereits aus, wie anhand der Formulierung „genutzt werden können“ ersichtlich ist. Zweck der Zugangskontrolle ist es also, das Risiko einer unbefugten Kenntnisnahme oder von Änderungen oder Löschungen personenbezogener Daten zu reduzieren.[742]

---

738 Eine oberflächliche Besichtigung per Video ermöglichen Google und Facebook, die jeweils ein Rechenzentrum und dessen Ausstattung und sogar einige wichtige Sicherheitsvorkehrungen in Videos präsentieren, was angesichts der bisher gepflegten Geheimhaltung der Rechenzentrumsbetreiber besonders erwähnenswert ist; *Wilkens*, Google gibt Einblicke in Rechenzentrum, http://www.heise.de/newsticker/meldung/Google-gibt-Einblicke-in-Rechenzentrum-1234222.html; *Google*, Google data center security, http://www.youtube.com/v/1SCZzgfdTBo?fs=1&hl=de_DE&rel=0; *Facebook*, Prineville Data Center, http://www.facebook.com/prinevilledatacenter; http://opencompute.org. In Deutschland hat die DATEV die Eröffnung eines Cloudrechenzentrums genutzt, um dieses näher vorzustellen; siehe dazu *Chip Online*, Premiere: Erster Blick auf ein Cloud-Rechenzentrum, http://business.chip.de/news/Premiere-Erster-Blick-auf-ein-Cloud-Rechenzentrum_48757521.html.

739 *Gola/Schomerus* 2010, § 9, Rn. 23.

740 *Roth*, ITRB 2010, 61; *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5, Rn. 42; früher umfasste die Zugangskontrolle auch den Zutrittsschutz; siehe dazu *Hammer/Pordesch/Roßnagel* 1993, 191 f.

741 *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 9, Rn. 7.

742 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 88, 91, 92, 94, 96.

Die Zugangskontrolle betrifft nicht nur den persönlichen und unmittelbaren Zugang zu Systemen, sondern vor allem den Zugang über Netzwerke, in der Regel also über das Internet.[743] Zugangskontrolle über Netzwerke bedeutet, dass ein IT-System die Identitäten der Kommunikationspartner prüft und nur mit Berechtigten weiterkommuniziert.[744] Für Cloud Computing ist außerdem relevant, dass die Zugangskontrolle unabhängig davon gilt, ob die verantwortliche Stelle ein eigenes Datenverarbeitungssystem benutzt oder sich, wie bei Cloud Computing üblich, externer Rechenkapazität bedient.[745]

Die technisch-organisatorischen Maßnahmen im Rahmen der Zugangskontrolle sollen die fehlende menschliche Einzelfallentscheidung ersetzen.[746] Konkrete Maßnahmen für Cloudrechenzentren sind die Absicherung mittels Firewalls und der Schutz unterschiedlicher Accounts mittels Passwörtern, um unbefugte Einflüsse auf die in den Rechenzentren stattfindenden Rechenprozesse zu verhindern. Satz 3 der Anlage zu § 9 BDSG erwähnt außerdem dem Stand der Technik entsprechende Verschlüsselungsmethoden, die auch bei der Zugangskontrolle eine sinnvolle Vorkehrung darstellen. Hierdurch wird eine Einflussnahme auf den Datenverarbeitungsprozess zumindest erschwert, da die Daten zwar während der Verarbeitung unverschlüsselt im Arbeitsspeicher und dem Prozessor vorhanden sind, jedoch davor und danach, also bei der Speicherung und der Übermittlung, oft ohne größeren zusätzlichen Aufwand, verschlüsselt werden können. Auch die Protokollierung der Nutzung ist eine sinnvolle Maßnahme, um nachträglich nachvollziehen zu können, wer in welcher Weise auf welche Verarbeitungs- und Nutzungsmöglichkeiten tatsächlich zugegriffen hat.[747]

Vor der prinzipiellen Nutzung eines Systems hat der Systemverantwortliche zu prüfen, ob er es verantworten kann, dass die Daten im System genutzt und verarbeitet werden. Diese Prüfung hat vor dem Hintergrund der Sensitivität der Daten und des Risikos eines unberechtigten Zugangs zu den Daten zu geschehen. Nicht zuletzt aus Verhältnismäßigkeitserwägungen kann es also geboten sein, schützenswerte Daten nicht in dem anvisierten System, zum Beispiel in einem offenen Cloudsystem, verarbeiten zu lassen, sondern stattdessen ein abgeschottetes Stand-alone-System zu benutzen.[748]

Bei dieser Abwägung ist auf die aktuelle technische Entwicklung zu achten, da diese immer neue und verbesserte Sicherungstechniken hervorbringt, so dass die Ent-

---

743 *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5, Rn. 43; *Ernestus*, in: Simitis, BDSG, § 9, Rn. 89.

744 *Federrath/Pfitzmann*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 2.2, Rn. 30.

745 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 90; *Schaffland/Wiltfang*, BDSG, 2010, § 9, Rn. 87.

746 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 94.

747 Protokollierung als Maßnahme ist damit sowohl für die Zugangskontrolle als auch die Zugriffskontrolle relevant; *Ernestus*, in: Simitis, BDSG, § 9, Rn. 94.

748 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 95.

scheidung vom Entscheidungszeitpunkt und der ab dann absehbaren technischen Entwicklung abhängt.[749] Gleiches gilt für den gegenteiligen Fall, nämlich wenn absehbar ist, dass ein Sicherungsmittel mittelfristig untauglich werden wird. Bestes Beispiel ist das absehbare Brechen von Verschlüsselungsalgorithmen, indem entweder ein Algorithmus mathematisch ausgehebelt wird oder die schiere Rechenleistung ein zeitlich und finanziell vertretbares Brechen der Schlüssel ermöglicht. Hinsichtlich der Nutzung von Cloudservices können daher manche Unternehmensentscheider und -verantwortliche jederzeit zum Ergebnis kommen, dass für die ihnen anvertrauten Daten aus obigen Erwägungen eine Nutzung und Verarbeitung in der Cloud nicht in Frage kommt.

3.1.9.3.2.3 Zugriffs- und Speicherkontrolle (Nr. 3)

Im Gegensatz zur Zugangskontrolle, die den Unbefugten von der Benutzung des Datenverarbeitungssystems ausschließt, ist bei der Zugriffskontrolle der Benutzer zur Benutzung an sich berechtigt, jedoch beschränkt auf die seiner Zugriffsberechtigung unterliegenden personenbezogenen Daten.[750] Die Vorschrift richtet sich folglich hauptsächlich an die Beschäftigten datenverarbeitender Stellen.

Die früher gesondert aufgeführte Speicherkontrolle ist ebenfalls Teil der Nr. 3 der Anlage zu § 9 BDSG und bedeutet, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung von Mitarbeitern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.[751]

Im Rahmen der datenschutzgerechten Organisation ist sicherzustellen, dass der Zugriff nur auf solche Daten ermöglicht wird, die ein Mitarbeiter zur Erledigung der ihm übertragenen Aufgaben benötigt.[752] Das Berechtigungskonzept muss dazu möglichst feingranular und individuell festlegbar sein. Hierzu ist eine klare, möglichst schriftlich festgehaltene, Aufgaben- und Zugriffstrennung nötig. Besondere Beachtung erfordert die lückenlose Protokollierung der Zugriffe, wobei revisionssicher nachvollzogen werden kann, wer wann welche Zugriffe und Aktionen getätigt hat. Die Zugangsberechtigten müssen identifizierbar sein. Zugriffskontrolle ist demnach nicht nur Vorbeugung des Datenmissbrauchs, sondern soll auch die Möglichkeit eröffnen, zuwiderhandelnde Personen zur Verantwortung ziehen zu können.

Die Gewährleistung, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, betrifft auch die Abschottung der verschiedenen virtuellen Maschinen durch Hypervisoren (Virtual Machine Monitor). Die virtuellen Maschinen

---

749 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 95.

750 *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 9, Rn. 7; ähnlich *Roth*, ITRB 2010, 61.

751 *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 9, Rn. 8; *Roth*, ITRB 2010, 61; siehe dazu auch *Hammer/Pordesch/Roßnagel* 1993, 195 ff.

752 *Gola/Schomerus* 2010, § 9, Rn. 24.

und Hypervisoren müssen so ausgestaltet und abgesichert sein, dass ein Ausbrechen aus einer Maschine und der Zugriff auf Daten einer anderen Maschine nicht möglich sind. Zwar existiert niemals ein absoluter Schutz hiergegen, jedoch sind gegenwärtige Virtualisierungslösungen so weit entwickelt und in der Praxis erprobt, dass eine Absicherung der virtuellen Maschinen in Cloudsystemen vor Fremdzugriffen effektiv zu verhindern ist.

Zudem muss in Cloudumgebungen und Rechenzentren allgemein sichergestellt sein, dass die handelnden Administratoren niemals alleinigen Vollzugriff auf die Daten bekommen. Dies ist durch begrenzte Zuständigkeiten und das Mehr-Augen-Prinzip zu erreichen.

3.1.9.3.2.4 Weitergabekontrolle (Nr. 4)

Die Vorschrift fasst sämtliche Aspekte der Weitergabe personenbezogener Daten zusammen. Darunter fallen die elektronische Übertragung, die Speicherung, der Datenträgertransport und die Datenübermittlung. Zusätzlich soll überprüft und festgestellt werden können, an welche Stellen eine Übermittlung personenbezogener Daten vorgesehen ist.[753] Die Vorschrift unterteilt sich demnach in die Sicherung von Datenträgern und Übertragungswegen und in die Übermittlungskontrolle.[754] Für Cloud Computing haben beide Aspekte erhebliche Relevanz.

Nicht nur die elektronische Übermittlung mittels Telekommunikation muss abgesichert erfolgen, sondern auch der herkömmliche Transport von Datenträgern. Zum einen können Kunden Daten mittels des Zusendens von Festplatten oder sonstigen Datenträgern, wie zum Beispiel USB-Sticks, DVDs oder Speicherkarten, in die Cloud einbringen, zum anderen ist aber auch der Transport zwischen den Rechenzentren manchmal über herkömmliche Festplatten billiger und schneller, als über Datenleitungen. Zum Beispiel bei der nachträglichen Spiegelung von Daten in einem zweiten Rechenzentrum.

Diese physische Übermittlung betrifft meist das erstmalige Migrieren von Daten in die Cloud, weil dabei die meisten Daten anfallen. Spätere Änderungen am ausgelagerten Datenbestand durch die Nutzung im täglichen Praxiseinsatz sind meist weniger datenintensiv. Sowohl die leitungsgebundene als auch die postalische Übermittlung darf nur verschlüsselt erfolgen. Für die leitungsgebundene Übermittlung bietet sich die SSL-Verschlüsselung über normale Webzugänge oder IPSEC-Verschlüsselung mittels VPN als Transportverschlüsselung an, während beim Datenträgertransport im Optimalfall sämtliche Daten auf der Festplatte oder dem Speicherstick vollverschlüsselt sind.[755] Insbesondere die personenbezogenen Daten

---

[753] *Roth*, ITRB 2010, 61; *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 9, Rn. 9; *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5, Rn. 51 ff.

[754] *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 9, Rn. 10 f.

[755] Siehe auch Kap. 4.6.1.

müssen verschlüsselt werden, da im Fall des Abhandenkommens des Datenträgers erhebliche und nicht wiedergutmachbare Schäden für die Persönlichkeitsrechte der Betroffenen drohen.

Die Sicherung von Datenträgern geht aber noch weiter. Auch und gerade die im Rechenzentrum vorhandenen Datenträger müssen vor Entwendung oder sonstiger unbefugter Kenntnisnahme geschützt werden. Dazu gehört auch die sichere Löschung der Daten, insbesondere wenn die Datenträger verkauft oder ausgemustert werden sollen.[756] Technisch-organisatorische Maßnahmen sind die bauliche Absicherung vor Entwendung, die kontrollierte Vernichtung oder Löschung von Datenträgern, Regelung zur Anfertigung von Kopien oder die Festlegung der zur Verwaltung und zum Umgang mit Datenträgern befugten Personen.[757]

Analog zur Sicherung der Datenträger müssen die leitungsgebundenen Übertragungswege mittels Firewalls, zum Beispiel Web Application Firewalls oder Application Layer Firewalls, Intrusion-Detection-Systemen (IDS), Intrusion-Prevention-Systemen (IPS), Data-Loss-Prevention-Systemen und dedizierten Weitergabeberechtigungen für die Daten, soweit dies technisch möglich ist, abgesichert werden. Letzteres beispielsweise so, dass personenbezogene Daten im Cloudsystem durch Mitarbeiter nur gelesen, aber nicht kopiert werden können.

Durch die Übermittlungskontrolle soll als vorbeugende Maßnahme die Prüfbarkeit der Übermittlung gesichert werden.[758] Es ist nicht nötig zu prüfen, an welche Stellen die Daten tatsächlich übermittelt wurden, sondern es soll ausreichen zu prüfen, an wen die Übermittlung vorgesehen ist. Das Aufzeichnen von Übermittlungsprotokollen ist damit zwar hilfreich, aber nicht zwingend notwendig.[759] Der Empfänger ist dabei so konkret zu bestimmen, dass eine eindeutige Feststellung zur Zulässigkeit der Übermittlung getroffen werden kann. Gefordert ist nicht lediglich die Angabe einer Unternehmensgruppe oder einer öffentlich-rechtlichen Körperschaft mit mehreren Behörden, sondern die Angabe der konkreten Person.[760] In offenen Systemen, wie dem Internet und damit insbesondere auch bei Public Cloud Umgebungen, in denen eine Vielzahl von Subunternehmen oder weltweit verteilte Server genutzt werden, ist diese Voraussetzung problematisch. Für diese Fälle ist dann nur noch die zwingende vollständige Protokollierung taugliches Mittel. Anders ist das

---

756 Siehe zur Problematik des Recyclings von Datenträgern auch *Jandt/Wilke* UPR 2010, 433 ff.

757 *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 9, Rn. 10.

758 *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5, Rn. 54; *Ernestus*, in: Simitis, BDSG, § 9, Rn. 113; *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 9, Rn. 11.

759 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 116; *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 9, Rn. 11; a. A. *Wank*, in: Müller-Glöge/Preis/Schmidt, ErfK, BDSG, § 9, Rn. 5.

760 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 119.

Risiko für die personenbezogenen Daten in offenen Kommunikationsnetzen nicht zu beherrschen.[761]

Bei Public Cloud Computing, das jedermann gegen Entgelt nutzen kann, wird diese Form der Protokollierung als Übermittlungskontrolle der Regelfall sein, da prinzipbedingt im Voraus nicht absehbar ist, ob überhaupt, wann und wohin genau personenbezogene Daten übermittelt werden.[762] Zwar ist, wie einleitend erwähnt, eingrenzbar, welche (Sub)Unternehmen beteiligt sind, jedoch ist es bei mehr als drei beteiligten Rechenzentren oft vom Zufall abhängig ob, wann und insbesondere in welches Rechenzentrum genau personenbezogene Daten übermittelt werden.

Der Betreiber hat darauf zu achten, dass die Protokollierung auch über seinen Einflussbereich hinaus möglich ist, gerade wenn er sich Subunternehmen bedient, so dass diese die weiteren Übermittlungen im Auftrag des Providers protokollieren. Zudem werden die Daten sowohl vom Provider selbst als auch von möglichen Subunternehmen an die Kunden des Cloudservices oder sogar Dritte (zurück)übermittelt. Ein Umstand, der erst recht eine Protokollierung erfordert.

3.1.9.3.2.5 Eingabekontrolle (Nr. 5)

Die Eingabekontrolle hat die Nachvollziehbarkeit der innerhalb eines Verarbeitungssystems durchgeführten Aktionen zum Ziel. Nach der Legaldefinition muss gewährleistet sein, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in das Datenverarbeitungssystem eingegeben, verändert oder entfernt worden sind. Lediglich auf den genauen Zeitpunkt kann verzichtet werden, wenn der Aufwand dafür zu hoch ist.[763] Diese nachträgliche Überprüfbarkeit setzt die eindeutige Identifizierbarkeit der am Datenverarbeitungsprozess Beteiligten voraus.[764] Die Vorschrift zielt auf die individuelle Verantwortung der mit der Eingabe betrauten Person ab.[765] Dazu zählen auch Externe, zum Beispiel Kunden, eines Cloudservices. Nutzer des Datenverarbeitungssystems müssen sich demnach mittels Credentials[766] authentifizieren. Die Authentifizierung und die oben aufgeführten Einzelheiten der Nutzung sind durch automatisierte Protokolle aufzuzeichnen.

Hierbei ist allerdings zu bedenken, dass mit einer solchen umfangreichen Protokollierung eine neue Sammlung von möglicherweise sehr sensitiven Daten entsteht. Die Protokolle sind deswegen selbst abzusichern und nur zweckgebunden zu ver-

---

761 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 117, 119.

762 Bei Private Clouds ist hingegen im Regelfall bekannt, an wen die Daten übermittelt werden, da diese meist nur unternehmens- oder konzernintern ausgetauscht werden.

763 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 134.

764 *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 9, Rn. 12.

765 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 135.

766 Siehe hierzu auch die Ausführungen zum Schutzziel der Authentizität in Kap. 3.1.9.5.9.

wenden.[767] Protokolldaten stellen Vorratsdaten über die Nutzung der Services dar und erlauben erhebliche Rückschlüsse auf persönlichkeitsrechtlich geschützte Umstände, zum Beispiel den genauen Zeitpunkt der Nutzung oder die Nutzung über einen gewissen Zeitraum durch eine bestimmte Person. Beispielsweise kann in Beschäftigungsverhältnissen dadurch das Arbeitsverhalten überwacht werden.[768]

Demnach bietet es sich an, diese Protokolldaten zu pseudonymisieren und möglichst nicht auf Rechnern des Cloudsystems, sondern von diesen getrennt abzuspeichern. Besonders kritisch ist in diesem Zusammenhang der Umstand, dass der Gesetzgeber keine Mindest- oder Höchstdauer der Speicherfristen für die Protokolldaten festgelegt hat. Entscheidend soll sein, ob der wirtschaftliche Aufwand verhältnismäßig ist und ob der Zweck, die Prüfbarkeit zu garantieren, erfüllt ist.[769]

Für die in den Cloudrechenzentren Beschäftigten ergeben sich dabei keine zusätzlichen Besonderheiten. Auch deren Protokolldaten sind getrennt von der Cloudinfrastruktur zu speichern und möglichst zu pseudonymisieren.

3.1.9.3.2.6 Auftragskontrolle (Nr. 6)

Die Auftragskontrolle betrifft Fälle der Auftragsdatenverarbeitung und ist daher im Zusammenhang mit § 11 BDSG zu sehen, der seinerseits in § 11 Abs. 2 Satz 1 und § 11 Abs. 2 Satz 2 Nr. 3 BDSG auf die Maßnahmen der Anlage zu § 9 BDSG Bezug nimmt.[770] Kurz zusammengefasst kann man feststellen, dass die Auftragskontrolle der Durchführung der Vorschriften über die Datenverarbeitung dient.[771] Sie richtet sich in erster Linie an die beauftragte Stelle, also den Auftragnehmer, und nur mittelbar an den Auftraggeber, der seinerseits dafür verantwortlich ist, dass die Weisungen widerspruchfrei und genau gegeben werden.[772] Die beauftragte Stelle hat die ihr erteilten Weisungen zu beachten und für die lückenlose Befolgung der Weisungen Maßnahmen zu treffen.[773] Der Auftraggeber muss die Einhaltung der gegebenen Weisung sicherstellen. Die Auftragskontrolle erfordert also sowohl beim Auftraggeber als auch beim Auftragnehmer technische und organisatorische Maßnahmen, die die lückenlose Einhaltung des Weisungsprinzips gewährleisten.[774]

So ist es zum Beispiel hilfreich für eine klare, genaue und widerspruchsfreie Auftragserteilung passend ausgestaltete Formulare zu benutzen. Mündlich erteilte Aufträge sind schnellstmöglich abzufassen. Schulungen und Arbeitsrichtlinien können

---

767 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 143.

768 *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5, Rn. 59.

769 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 139.

770 Siehe hierzu auch oben Kap. 3.1.8.5.3.

771 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 146.

772 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 147; *Roth*, ITRB 2010, 62; *Gola/Schomerus* 2010, § 9, Rn. 27.

773 *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 9, Rn. 13.

774 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 149.

dazu beitragen, dass diese Maßnahmen beachtet werden.[775] Kontrollen sollen die Einhaltung der technischen und organisatorischen Maßnahmen gewährleisten und sind sowohl vom Auftraggeber, als auch vom Auftragnehmer durchzuführen.[776]

Eindeutige Regelungen zur Zweckbindung der Datennutzung nebst effektiven Kontrollmaßnahmen und Regelungen zu Zugriffsbeschränkungen, zur Aufbewahrung von Datenträgern, zum Verlust von Datenträgern, zu Löschverfahren und zur vollständigen Herausgabe im Fall der Auftragsbeendigung sind in die Verträge zwischen Anbieter und Kunden mit aufzunehmen.[777] Zudem sollte die Heranziehung von Subunternehmen im Vertrag schriftlich festgelegt sein.[778]

Im Jahr 2011 angebotenen Cloudservices mangelt es an dem in Nr. 6 festgelegten wechselseitigen Zusammenspiel zwischen Auftraggeber und Auftragnehmer. Derzeit ist es eher so, dass die Cloudprovider als Auftragnehmer ihre Leistungen vorgefertigt anbieten, ohne jedoch dem Kunden Spielraum bei der Gestaltung oder abweichende Aufträge zu erlauben. Insbesondere bestehen nur selten Kontrollbefugnisse des Kunden hinsichtlich der Durchführung und der Einhaltung der vom Betreiber vorgegebenen Maßnahmen.

3.1.9.3.2.7 Verfügbarkeitskontrolle (Nr. 7)

Die Verfügbarkeitskontrolle soll sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.[779] Es sind deshalb nur solche Maßnahmen zu ergreifen, die darauf abzielen eine zufällige Zerstörung der Hardware oder den Verlust von Daten,[780] zum Beispiel durch Wasserschäden, Brand, Blitzschlag oder Stromausfall, zu verhindern.[781] Beispiele für taugliche Sicherungsmaßnahmen sind die Auslagerung von Sicherungskopien, das Bereithalten von Notstromaggregaten und von unterbrechungsfreier Stromversorgung (USV), das Aufstellen eines Katastrophenplans oder das Ausarbeiten und Einhalten eines Sicherungskonzepts inklusive der Dokumentation der Sicherungsläufe.[782]

Für Cloudrechenzentren gelten diese Maßnahmen ebenso. Allerdings sind angesichts der Fülle von Daten und deren Bedeutung für eine Vielzahl von Kunden erheblich höhere Anforderungen an die Sicherungsmaßnahmen zu stellen. Das geht so

---

775 *Roth*, ITRB 2010, 62; *Ernestus*, in: Simitis, BDSG, § 9, Rn. 150.

776 *Gola/Schomerus* 2010, § 9, Rn. 27; *Ernestus*, in: Simitis, BDSG, § 9, Rn. 154.

777 *Böken*, Cloud Computing und Auftragsdatenverarbeitung, http://www.linuxtag.org/2010/fileadmin/www.linuxtag.org/slides/Arnd%20B%C3%B6ken%20-%20Cloud-Computing%20und%20Auftragsdatenverarbeitung.pdf, S. 22.

778 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 148.

779 *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5, Rn. 67.

780 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 156.

781 *Gola/Schomerus* 2010, § 9, Rn. 28.

782 *Gola/Schomerus* 2010, § 9, Rn. 28; *Ernestus*, in: Simitis, BDSG, § 9, Rn. 159.

weit, dass Daten in einem zweiten gespiegelten Rechenzentrum an einem anderen Ort parallel vorgehalten werden.

3.1.9.3.2.8 Trennungsgebot (Nr. 8)

Datentrennung ist ein Aspekt des Zweckbindungsgrundsatzes. Sie soll gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. So soll eine verantwortliche Stelle schon bei der Konzeption von Systemen diese so auslegen, dass personenbezogene Daten auch tatsächlich getrennt verarbeitet werden können.[783] Die praktische Umsetzung der Vorschrift ist somit der erste Schritt für einen funktionierenden Systemdatenschutz.[784]

Die Trennung kann physisch oder logisch erfolgen.[785] Bei Cloud Computing erfolgt die Trennung aufgrund der Mehrmandantennotwendigkeit zum einen physisch, indem unterschiedliche physische Server beteiligt sind, zum anderen virtuell, indem Hypervisoren unterschiedliche virtuelle Maschinen bereitstellen und voneinander abschotten.[786] Die Virtualisierungstechnik ist mittlerweile so ausgereift, dass damit die Forderungen aus Nr. 8 der Anlage zu § 9 BDSG erfüllt werden können. Allerdings ergeben sich die cloudspezifischen Sicherheitsbedrohungen gerade in diesem Regelungsfeld des Trennungsgebots.[787]

3.1.9.3.3 Spezialvorschrift des § 109 TKG

§ 109 TKG ist gegenüber § 9 BDSG eine Spezialvorschrift, die die notwendigen Sicherheitsmaßnahmen für Telekommunikationsanbieter präzisiert und teilweise erweitert, um damit sichere und zuverlässige Telekommunikation zu gewährleisten.[788] Nicht zuletzt wegen der strukturellen Ähnlichkeit zwischen TK- und Cloudanbietern, nämlich einem Gemenge aus verteilten eigenen und mitbenutzten Einrichtungen und technischen Ressourcen, ist die Vorschrift mittelbar auch für Cloud Computing relevant.

§ 109 TKG schützt gemäß Abs. 1 Nr. 1 nicht nur das Fernmeldegeheimnis, sondern auch personenbezogene Daten, so dass sich auch der Bezug zu § 9 BDSG erklärt. Ein weiteres Schutzgut ist die Telekommunikationsinfrastruktur.[789] Wegen der hohen Bedeutung des Fernmeldegeheimnisses und des Datenschutzes sowie der Infra-

---

783 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 161.

784 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 160.

785 *Ernestus*, in: Simitis, BDSG, § 9, Rn. 161.

786 Dass die Abstraktion von physischen Gegebenheiten und damit die Trennung nur mittels Software nicht minder effektiv ist, wurde weiter oben im Rahmen der Darstellung der Virtualisierung dargelegt; siehe dazu auch Kap. 2.3.4.2.1.

787 Siehe Kap. 3.1.9.10 und zu den konkreten Maßnahmen Kap. 3.1.9.9.3.

788 *Schommertz*, in: Scheurle/Mayen, TKG, § 109, Rn. 1; *Bock*, in: Beck'scher TKG-Kommentar, § 109, Rn. 7, 10.

789 *Graulich*, in: Arndt/Fetzer/Scherer, TKG, § 109, Rn. 3.

strukturbedeutung der Telekommunikationsdienste, hat sich der Gesetzgeber für eine gesetzliche Regelung der Sicherheitsmaßnahmen entschieden.[790]

Gemäß § 109 Abs. 1 Nr. 1 TKG sind technische Vorkehrungen und sonstige Maßnahmen zu treffen. Diese müssen angemessen sein. Welche Schutzmaßnahmen angemessen sind, muss anhand des Einzelfalls entschieden werden, wobei der Stand der technischen Entwicklung zu beachten ist. Rentabilitäts- oder Wirtschaftlichkeitsbetrachtungen spielen ebenfalls eine Rolle, da die Maßnahmen bezahlbar sein müssen. Als übliche und angemessene technische Vorkehrungen werden Firewalls, Intrusion-Detection-Systeme, Überbrückungsaggregate oder der Betrieb redundanter Systeme angesehen.[791] Die Vorkehrungen umfassen neben der unternehmensinternen Organisation, folglich auch und gerade Maßnahmen gegen Zugriffe von außen.[792] Auch Zutritts- und Zugangskontrollen oder das Abtrennen von internen und externen Netzen sind weitere wichtige technische Vorkehrungen. Dadurch besteht eine große Übereinstimmung mit den Datensicherungsmaßnahmen, die in § 9 BDSG und der zugehörigen Anlage vorgesehen sind.[793] Darüber hinaus sind gemäß § 109 Abs. 2 Satz 1 TKG Maßnahmen gegen Katastrophen zu treffen und gemäß § 109 Abs. 3 Satz 1 TKG ein Sicherheitskonzept zu erstellen. Ein solches Sicherheitskonzept im Sinne der Vorschrift ist ein unternehmensinternes Konzept und muss nach § 109 Abs. 3 Satz 2 TKG der Bundesnetzagentur unverzüglich nach Aufnahme der Telekommunikationsdienste zur Prüfung vorgelegt werden.

Das Sicherheitskonzept muss nach § 109 Abs. 3 Satz 2 Nr. 1 bis 3 TKG gewisse Voraussetzungen erfüllen. Auf Cloud Computing übertragen, sind vor allem Nr. 2 und Nr. 3 bedeutsam. Gemäß § 109 Abs. 3 Satz 2 Nr. 2 TKG ist festzuhalten, von welchen Gefährdungen oder Bedrohungen[794] auszugehen ist. Dazu zählen beispielsweise Witterungseinflüsse, technische Störungen, menschliche Fehlhandlungen oder organisatorische Mängel.[795]

§ 109 Abs. 3 Satz 2 Nr. 3 TKG zielt auf die Beseitigung der Gefährdungen ab. Demnach ist im Konzept festzuhalten welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen geplant und praktisch getroffen werden.[796] Diese müssen

---

790 BR-Drs. 80/96, 54; *Bock*, in: Beck'scher TKG-Kommentar, § 109, Rn. 8.

791 *Gaycken/Karger*, MMR 2011, 6; *Bock*, in: Beck'scher TKG-Kommentar, § 109, Rn. 19.

792 *Schommertz*, in: Scheurle/Mayen, TKG, § 109, Rn. 7.

793 *Bock*, in: Beck'scher TKG-Kommentar, § 109, Rn. 19.

794 Zu den Begriffen und deren Abgrenzung siehe Kap. 3.1.9.8.1.

795 Siehe dazu insbesondere den von der Bundesnetzagentur veröffentlichten „Leitfaden zur Erstellung eines Sicherheitskonzeptes gemäß § 109 TKG", S. 16 ff., http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Bundesnetzagentur/AmtsblattPublikationen/DruckschriftenAllgemein/SicherheitTelekommunikation/LeitfadenSicherheitskonzeptId4552pdf; *Graulich*, in: Arndt/Fetzer/Scherer, TKG, § 109, Rn. 11; siehe hierzu auch die detaillierte Klassifizierung in Kap. 3.1.9.8.2.

796 TK-spezifische Schutzmaßnahmen finden sich auch im „Leitfaden zur Erstellung eines Sicherheitskonzeptes gemäß § 109 TKG", S. 26 ff., http://www.bundesnetzagentur.de/Shared

zur Beseitigung oder Vorbeugung von Gefährdungen und Bedrohungen geeignet sein.[797]

Zusammenfassend lässt sich festhalten, dass § 109 TKG für die weitere Untersuchung der IT-Sicherheitsaspekte von Cloud Computing als gesetzlich basierte Orientierungshilfe herangezogen werden kann.[798] Gerade die Feststellung der Bedrohungen und Gefährdungen, deren Abwehr durch Sicherheitsmaßnahmen und die Aufstellung eines in sich schlüssigen und umfassenden Sicherheitskonzepts sind damit nicht nur als informationstechnisch notwendig, sondern auch als rechtlich geboten anzusehen.

3.1.9.3.4 Wertungen des Bundesverfassungsgerichts zur Vorratsdatenspeicherung

Die Bedeutung der Datensicherheit für personenbezogene Daten lässt sich auch am Urteil des Bundesverfassungsgerichts zur Vorratsspeicherung von Telekommunikationsverbindungsdaten erkennen.[799] Die Speicherung dieser Daten durch die verpflichteten TK-Unternehmen ist dem Gericht zufolge nur dann verfassungsgemäß, wenn diese eine Reihe von technisch-organisatorischen Sicherheitsmaßnahmen einhalten. Das Gericht ging dabei so weit, die notwendigen Maßnahmen konkret vorzugeben, was für verfassungsgerichtliche Urteile eine Ausnahme darstellt, weil dadurch der Beurteilungsspielraum des Gesetzgebers eingeschränkt wird.

Die Situation zwischen den zur Speicherung auf Vorrat verpflichteten Telekommunikationsunternehmen und Cloudprovidern ist fast identisch, so dass die Einschätzungen aus dem Urteil auch auf die Absicherung von Clouddaten übertragbar sind. In beiden Konstellationen geht es um Unternehmen, denen eine Fülle von sensitiven Daten anvertraut wurde, die diese durch Sicherungsmaßnahmen vor Verlust oder unbefugter Kenntnisnahme schützen müssen. Der einzige Unterschied besteht darin, dass die TK-Unternehmen die Daten selbst erheben, während ein Cloudprovider diese in der Regel vorwiegend von seinen Kunden zugeleitet bekommt. Die Speicherung als Teil des Umgangs mit den Daten ist somit identisch. Dabei sind nicht nur die technischen, sondern auch und gerade die organisatorischen Maßnahmen direkt vergleichbar und übertragbar. Auch die Maßnahmen zur Absicherung des Datentransports sind identisch.

Das Gericht konnte bei der Formulierung der Sicherungsmaßnahmen auf bereits vorhandene Forschungen und Gestaltungsvorschläge, sowie auf die Gutachten der

---

Docs/Downloads/DE/BNetzA/Bundesnetzagentur/AmtsblattPublikationen/DruckschriftenAllgemein/SicherheitTelekommunikation/LeitfadenSicherheitskonzeptId4552pdf; zu allgemeinen Schutz- und Sicherheitsmaßnahmen siehe auch Kap. 3.1.9.9.

797 *Graulich*, in: Arndt/Fetzer/Scherer, TKG, § 109, Rn. 11.

798 Eine direkte Anwendung scheitert, wie einleitend ausgeführt, an der Spezialität der Vorschrift.

799 BVerfGE 125, 260.

bestellten Sachverständigen zurückgreifen.[800] Wichtige Maßnahmen sind die Trennung unterschiedlicher Datenarten,[801] die Verschlüsselung der gespeicherten Daten, die Implementierung von Manipulationserkennungsverfahren sowie von Fehlererkennungs- und Fehlerkorrekturverfahren oder die sichere Löschung obsolet gewordener Daten. Weitere wichtige Maßnahmen sind die Umsetzung des Vieraugenprinzips oder sonstiger anerkannter Zugangs-, Zutritts- und Zugriffsregelungen und die Protokollierung des tatsächlichen Umgangs mit den Daten.[802]

3.1.9.4 Datenschutzrechtlicher Reformbedarf

Im Eckpunktepapier zur Konferenz der Datenschutzbeauftragten des Jahres 2010 forderten die Beteiligten eine Modernisierung der Anlage zu § 9 BDSG. Die Maßnahmen stammen aus Zeiten von Großrechentechnologie und sind heutzutage nur mit Mühe auf moderne und vernetzte Systeme anwendbar. Sie fordern deswegen die komplette Ersetzung der dortigen Maßnahmen mit grundlegenden IT-Schutzzielen und nicht nur das Einfließen von deren Wertungen. Dabei werden im Papier ausdrücklich die Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität, Transparenz und Nicht-Verkettbarkeit erwähnt.[803]

Eine sehr ähnliche Auswahl und auf Landesebene bereits früher erfolgte Umsetzung der Forderungen findet sich beispielsweise in den Landesdatenschutzgesetzen der Länder Berlin und Sachsen-Anhalt in § 5 Abs. 2 Nr. 1 bis 6 Berliner Datenschutzgesetz und § 6 Abs. 2 Nr. 1 bis 6 DSG LSA. Beide erwähnen die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz und beinhalten bezüglich des Umgangs mit personenbezogenen Daten ansatzweise eine Legaldefinition der jeweiligen Schutzziele. Wie an der anschließenden Klassifizierung der Schutzziele zu sehen sein wird, stellt die Auswahl im Eckpunktepapier und in den Landesdatenschutzgesetzen aber nur einen Bruchteil der bisher anerkannten Schutzziele dar.[804]

Die Schutzziele sollten dem Eckpunktepapier der Datenschutzbeauftragten zufolge zudem gewisse Bedingungen erfüllen. Insbesondere sollten sie einfach, verständlich und praxistauglich sein. Sie sollen außerdem an den Vorgaben des Datenschutzes zu messen sein, müssen längere Zeit Bestand haben und dürfen sich, trotz aller Überschneidungen, nicht allein an den Vorgaben der IT-Sicherheit orientieren. Außer-

---

800 Zum Beispiel *Ziebarth*, DuD 2009, 25; *Roßnagel/Bedner/Knopp*, DuD 2009, 536; die gutachterlichen Stellungnahmen sind unter http://www.vorratsdatenspeicherung.de/content/view/51/70/lang,de, dortige Nr. 40 ff. zu finden.

801 Siehe dazu insbesondere *Ziebarth*, DuD 2009, 25 ff.

802 BVerfGE 125, 325 ff.; siehe dazu auch *Roßnagel/Bedner/Knopp*, DuD 2009, 539 ff.

803 Eckpunktepapier „Ein modernes Datenschutzrecht im 21. Jahrhundert“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18.3.2010, S. 19; *Schneider*, ZD 2011, 6 ff. plädiert ebenfalls für eine umfassende Reform des § 9 BDSG samt Anlage.

804 Zur Klassifizierung siehe sogleich Kap. 3.1.9.5.

dem sollen sich aus den Schutzzielen die konkret in der Praxis zu treffenden Maßnahmen ableiten lassen. Die Maßnahmen sind dem Stand der Technik anzupassen, während die Schutzziele nachhaltig und technologieunabhängig zu formulieren sind.[805]

Flankierend sollten Risikoanalysen und Sicherheitskonzepte die Maßnahmen konzeptionell absichern. Letztere sind nach dem Stand der Technik regelmäßig fortzuschreiben und sollten zu einem möglichst frühen Zeitpunkt ansetzen.[806] Zielsetzung ist die Stärkung der Eigenverantwortung und des Selbstdatenschutzes der Betroffenen und die Förderung datenschutzfreundlicher Technologien.[807]

3.1.9.5 Schutzziele der IT-Sicherheit

Im Folgenden sollen die IT-Schutzziele ermittelt, systematisiert und näher erläutert werden.[808] Diese haben sich im Laufe der letzten zwanzig Jahre parallel zum technischen Fortschritt entwickelt. Bei der Systematisierung ist zwischen übergeordneten und untergeordneten Schutzzielen zu unterscheiden. Untergeordnete IT-Schutzziele sind aus einem oder mehreren übergeordneten Schutzzielen abgeleitet oder stehen mit solchen im Zusammenhang. Zur besseren Vergleichbarkeit werden jeweils auch die entsprechenden englischen Begriffe der Schutzziele genannt. Zusätzlich erfolgt eine Nennung geläufiger Maßnahmen, die eingesetzt werden, um die Ziele zu erreichen. Dadurch soll auch das Verständnis für das jeweilige Schutzziel und die Notwendigkeit seiner Einhaltung geschärft werden. Soweit rechtliche Grundlagen für ein Schutzziel vorhanden sind, sollen diese erwähnt und deren Bedeutung für das jeweilige Schutzziel verdeutlicht werden.

3.1.9.5.1 Vertraulichkeit

Vertraulichkeit (Confidentiality), als übergeordnetes Schutzziel, ist bei einem IT-System gewährleistet, wenn die darin enthaltenen Informationen nur Befugten zugänglich und vor Ausspähung geschützt sind.[809] Dies bedeutet, dass die sicherheitsrelevanten Elemente nur einem definierten Personenkreis bekannt werden.[810] Dazu sind Maßnahmen zur Festlegung sowie zur Kontrolle zulässiger Informationsflüsse zwischen den Subjekten des Systems nötig (Zugriffsschutz und Zugriffsrechte), so

---

805 Eckpunktepapier „Ein modernes Datenschutzrecht im 21. Jahrhundert“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18.3.2010, S. 18 ff.

806 Eckpunktepapier „Ein modernes Datenschutzrecht im 21. Jahrhundert“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18.3.2010, S. 19 ff.

807 Eckpunktepapier „Ein modernes Datenschutzrecht im 21. Jahrhundert“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18.3.2010, S. 20.

808 Dieses Kapitel geht im Wesentlichen auf *Bedner/Ackermann*, DuD 2010, 323 ff. zurück und wurde im Rahmen dieser Arbeit inhaltlich geändert und ergänzt.

809 *Holznagel* 2003, 13; *Heckmann*, MMR 2006, 281; Vertraulichkeit ist Teil der sogenannten „CIA-Triad“, die sich aus den drei Schutzzielen Confidentiality, Integrity, Availability ergibt.

810 *Stelzer* 1993, 35.

dass ausgeschlossen werden kann, dass Informationen zu unautorisierten Subjekten „durchsickern".[811] Zu den Schutzobjekten der Vertraulichkeit gehören unter anderem die gespeicherten oder transportierten Nachrichteninhalte, die näheren Informationen über den Kommunikationsvorgang sowie die Daten über den Sende- und Empfangsvorgang.[812] Andere unterscheiden zwei Bereiche, nämlich den „Schutz des Informationsverhaltens",[813] also den Schutz des Benutzers vor Beobachtung, Aufzeichnung und Auswertung seines Verhaltens während der Nutzung eines IT-Systems und den „Schutz der Informationsinhalte".[814]

Das zentrale Instrument zur Gewährleistung der Vertraulichkeit ist, neben einem wirksamen Zugriffsschutz, die Verschlüsselung von Daten.[815] Das Ziel der Verschlüsselung liegt darin, die Daten geeignet zu transformieren, so dass unautorisierte Dritte ohne den korrekten Schlüssel nicht in der Lage sind, die Daten sinnvoll zu interpretieren.[816] Die Verschlüsselung kann symmetrisch oder asymmetrisch erfolgen.[817]

Im Gegensatz zu den meisten anderen IT-Schutzzielen ist der Schutz der Vertraulichkeit von Daten und Informationen rechtlich vergleichsweise gut abgesichert. Regelungen zum Schutz der Vertraulichkeit finden sich in Art. 10 GG und einfachgesetzlich in § 88 TKG und § 206 StGB, soweit das Fernmeldegeheimnis betroffen ist. Datenschutzrechtlich sind insbesondere § 5 BDSG (Verpflichtung der Mitarbeiter auf das Datengeheimnis) und die technisch-organisatorischen Maßnahmen in der Anlage zu § 9 BDSG, insbesondere die Nummern 1 bis 3 (Zutritts-, Zugangs- und Zugriffskontrolle), erwähnenswert.[818] Als Vorschriften zum Schutz von Privat- oder Betriebsgeheimnissen sind § 203 StGB und § 17 UWG zu erwähnen.[819]

3.1.9.5.2 Unverkettbarkeit

Unverkettbarkeit[820] (Unlinkability) soll gewährleisten, dass mehrere kommunikative Ereignisse, etwa aufeinander folgende Abrufe von Informationen auf verschiedenen Webservern im Internet, nicht miteinander in Verbindung gebracht werden können.[821] Allgemeiner formuliert bedeutet die Unverkettbarkeit von Subjekten, Objekten oder Aktionen, dass durch Beobachtungen des Szenarios die Wahrscheinlichkeit

---

811 *Eckert* 2006, 9.
812 *Holznagel* 2003, 13 f.
813 *Grochla/Weber/Albers/Werhahn*, Angewandte Informatik, 1983, 189.
814 *Grochla/Weber/Albers/Werhahn*, Angewandte Informatik, 1983, 192.
815 Für viele *Witt* 2006, 67; *Eckert* 2006, 9; zu Details siehe auch die Kap. 3.1.9.9.1 und 4.5.1.
816 *Eckert* 2006, 9.
817 *Witt* 2006, 67.
818 Vergleiche oben Kap. 3.1.9.3.2.
819 Siehe dazu auch Kap. 3.8.1.2.
820 Auch als „Unverknüpfbarkeit" bekannt.
821 *WEKA*, Unverkettbarkeit, http://www.weka.de/datenschutz/4742978-Unverkettbarkeit.html.

einer Relation zwischen enthaltenen Elementen unverändert bleibt.[822] Zu beachten ist, dass auch der Gegenbegriff, nämlich die Verkettbarkeit, im Zusammenhang mit der Zurechenbarkeit als Ziel angesehen werden kann.

Eine Maßnahme zur Gewährleistung der Unverkettbarkeit ist die Nutzung von sogenannten „Mixen“, das heißt Servern, die die einzelne Zuordnung eines Datenpakets zu einem Nutzer verschleiern, indem Nachrichten nicht direkt vom Sender zum Empfänger, sondern über mehrere Zwischenstationen (eben diese „Mix“-Server) übertragen und untereinander verwürfelt werden.[823] Begründer dieses Konzepts war der Informatiker und Ökonom *David Chaum*[824] im Jahr 1981.[825]

Unverkettbarkeit ist ein wichtiger Aspekt der informationellen Selbstbestimmung und für den Selbstdatenschutz essentiell. Der Betroffene hat es bei Erfüllung des Schutzziels selbst in der Hand, dass Dritte seine Handlungen im obigen Sinne nicht auf ihn zurückführen können.

3.1.9.5.3 Nicht-Verfolgbarkeit

Eng mit der Unverkettbarkeit und damit ebenso der informationellen Selbstbestimmung zusammenhängend ist die Nicht-Verfolgbarkeit (Untraceability), auch als Unverfolgbarkeit oder Nicht-Rückverfolgbarkeit bekannt. Im Unterschied zur Unverkettbarkeit, die allgemein auf die fehlende Möglichkeit der Relation von Subjekten, Objekten oder Aktionen abstellt, meint Nicht-Verfolgbarkeit die Unmöglichkeit, Handlungen oder Kommunikationsinhalte einer ganz bestimmten identifizierbaren Person nachverfolgen zu können. Nicht-Verfolgbarkeit weist auch Bezüge zur Zurechenbarkeit, aber auch insbesondere zur Anonymität und Pseudonymität im Sinne des § 3a BDSG und § 13 Abs. 6 Satz 1 TMG auf.[826]

Ein Beispiel für die Umsetzung von Anonymität durch Nicht-Verfolgbarkeit ist die Abwicklung von E-Commerce-Geschäften durch den digitalen Zahlungsverkehr. Ist dieser entsprechend ausgestaltet, beispielsweise bei der Geldkarte, können Teilnehmer in einer computerisierten Umgebung genauso agieren wie bei herkömmlichen Bargeschäften des täglichen Lebens. Sie bezahlen mit digitalem Geld, ohne ihre Identität offenbaren zu müssen,[827] da die Zahlungsströme nicht mehr nachträglich einzelnen identifizierbaren Personen zugeordnet werden können.

---

822 *Stritter* 2006, 11.

823 Siehe *Federrath/Pfitzmann*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 2.2, Rn. 74 und *JAP*, Technischer Hintergrund von JAP, http://anon.inf.tu-dresden.de/JAPTechBgPaper.pdf für eine genauere Beschreibung; *Holznagel* 2003, 31.

824 *Chaum*, Communications of the ACM, 1981, 84.

825 *Danz/Federrath/Köhntopp/Kritzenberger/Ruhl* 1999, 60 f.

826 Zur Anonymität und Pseudonymität siehe Kap. 3.1.9.5.6 und zur Zurechenbarkeit Kap. 3.1.9.5.8.

827 *Biskup* 2009, 44.

3.1.9.5.4 Unbeobachtbarkeit

Die Unbeobachtbarkeit (Unobservability) ist gewährleistet, wenn sich nicht erkennen lässt, wer Daten sendet oder empfängt,[828] aber auch wenn der oben erwähnte Schutz des Informationsverhaltens gewährleistet ist. Dritte können weder die Nutzung der Systeme noch das eigentliche Senden und Empfangen von Nachrichten beobachten.[829] Das Problem an Letzterem ist, dass in den bestehenden Netzen die Ereignisse des Sendens oder Empfangens eines Datenpaketes stets beobachtbar sind. Allerdings kann durch das Generieren von „Dummy Traffic“ ein Angreifer daraus keinen Nutzen ziehen. „Dummy Traffic“ bedeutet, dass ein Nutzer Leernachrichten, die für einen Beobachter von außen nicht von echten Botschaften zu unterscheiden sind, sendet, solange er keine echten Nachrichten zu senden hat.[830] Damit wären zumindest das Senden und der Erhalt von einzelnen konkreten Nachrichten verheimlicht. Um die eigentliche Dienstenutzung an sich durch einen bestimmten Nutzer unbeobachtbar zu gestalten, bietet sich das oben dargestellte Mix-Verfahren an, das mehrere Beteiligte beinhaltet, so dass aufgrund der verwendeten Verwürfelungsmethoden nicht auf einen einzelnen Nutzer geschlossen werden kann.

Soweit das Schutzziel die Unbeobachtbarkeit der Nutzung von Systemen betrifft, beispielsweise durch heimliches Beobachten oder Abhören des Nutzers mittels Kameras, Mikrofonen oder Auffangen von elektromagnetischer Abstrahlung, so sind die Maßnahmen der optischen und elektromagentischen Abschirmung, zum Beispiel fensterlose und als Faradayscher Käfig ausgestaltete Räume und die Überprüfung dieser Räume auf Abhörgeräte in Betracht zu ziehen.

Das Schutzziel findet in § 13 Abs. 6 Satz 1 TMG oder dem Fernmeldegeheimnis gemäß § 88 Abs. 1 TKG rechtlich Anklang. Diensteanbieter sollen die möglichst anonyme Nutzung der Dienste ermöglichen, während Telekommunikationsanbieter die Beteiligung an einem Telekommunikationsvorgang geheim halten müssen. Zudem dient auch dieses Schutzziel dem Schutz der informationellen Selbstbestimmung.

3.1.9.5.5 Verdecktheit

Während bei der Unbeobachtbarkeit klar ist, dass irgendwann eine Datenübertragung stattfindet, diese jedoch hinsichtlich der Sender und Empfänger, des genauen Zeitpunkts und des Inhalts für Angreifer nicht auszumachen ist, geht die Verdecktheit (Covertness, Obscurity) einen Schritt weiter. Diese bedeutet, dass niemand außer den Kommunikationspartnern überhaupt weiß, dass Kommunikation stattfindet. Steganographie, also das Verstecken von Informationen im Datenrauschen von

---

828 *Roßnagel/Pfitzmann/Garstka* 2001, 230; *Biskup* 2009, 43.

829 *Federrath/Pfitzmann*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 2.2, Rn. 66.

830 *Danz/Federrath/Köhntopp/Kritzenberger/Ruhl* 1999, 60.

Bild- oder Musikdateien, ist ein Beispiel für eine reale Anwendung. Durch solche Maßnahmen zur Gewährleistung von Verdecktheit wird der Selbstdatenschutz auf ein sehr hohes Niveau gehoben. Die rechtlichen Grundlagen sind im Übrigen die gleichen, wie bei der Unbeobachtbarkeit.

3.1.9.5.6 Anonymität und Pseudonymität

Anonymität (Anonymity) meint den Schutz vor Identifizierung.[831] Sie ist Folge der Unverkettbarkeit. Demgemäß werden auch Dienste, die die Verkettbarkeit unterbrechen als Anonymisierungsdienste bezeichnet. Das Wort „anonym“ kommt aus dem Griechischen und bedeutet „namenlos“ oder „ohne Namensnennung“.[832]

Die Anonymität erlangt rechtlich im Rahmen des Datenschutzrechts Bedeutung. Wie bereits bei dem Schutzziel der Nicht-Verfolgbarkeit erwähnt, ist sie in den §§ 3a Satz 2 BDSG und 13 Abs. 6 Satz 1 TMG gesetzlich erwähnt. In § 3 Abs. 6 BDSG wird der Vorgang des Anonymisierens legaldefiniert als das derartige Verändern personenbezogener Daten, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Kurz gefasst sind anonyme Daten zwar immer noch Einzelangaben über eine Person, allerdings können diese von niemandem zugeordnet werden und sind demzufolge auch nicht mehr datenschutzrelevant, da die Person gerade nicht mehr bekannt ist.[833]

Pseudonymität (Pseudonymity) bedeutet Schutz vor namentlicher Identifizierung. „Pseudonym“ entspringt ebenfalls dem Griechischen und bedeutet „mit falschem Namen auftretend“, „fälschlich so genannt“ oder nach modernem Verständnis „erfundener Name“, „fingierter Name“ oder „Deckname“.[834] Die datenschutzrechtliche Maßnahme der Pseudonymisierung ist beispielsweise in § 3 Abs. 6a BDSG geregelt und meint „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren“. Im Gegensatz zur Anonymisierung wird bei der Pseudonymisierung der Bezug zu einer bestimmten Person jedoch nicht endgültig aufgehoben, denn es besteht immer eine Aufdeckungsmöglichkeit. Durch eine Zuordnungsregel kann das Pseudonym nachträglich wieder dieser bestimmten Person zugeordnet werden. Derjenige, der die Zuordnungsregel kennt, kann Pseudonyme mit realen Personen verketten, diese Personen wiedererkennen und soweit nötig zur Verantwortung ziehen. Pseudonymität ist folglich ein Kompromiss aus Vertraulich-

---

831 *Biskup* 2009, 44.

832 *Duden Online*, Anonym, http://www.duden.de/zitieren/10010349/1.6.

833 *Roßnagel/Scholz*, MMR 2000, 723; Näheres hierzu siehe auch weiter unten in Kap 3.1.5.3.2.

834 *Duden Online*, Pseudonym, http://www.duden.de/zitieren/10028922/1.5.

keit und Transparenz. Wenn die Zuordnungsregel verloren geht oder bewusst vernichtet wird, dann entsteht Anonymität im obigen Sinne.

Anonymisierung und Pseudonymisierung haben auch für den Grundsatz der Datenvermeidung und Datensparsamkeit Bedeutung. Gemäß § 3a Satz 2 BDSG sollen personenbezogene Daten, soweit der Verwendungszweck dies erlaubt und keinen unverhältnismäßigen Aufwand darstellt, anonymisiert oder pseudonymisiert werden. Gemäß § 13 Abs. 6 Satz 1 TMG soll die Nutzung und Bezahlung von Telemediendiensten auch anonym und pseudonym möglich sein.

3.1.9.5.7 Transparenz

Transparenz (Transparency) ist das Gegenstück zur Vertraulichkeit und somit ebenfalls ein übergeordnetes IT-Schutzziel. Im Gegensatz zur Computer- und Netzwerktechnik, in der ein transparenter Teil eines Systems nicht wahrgenommen werden soll, hat Transparenz im Kontext der Schutzziele die entgegengesetzte Bedeutung. Analog zum datenschutzrechtlichen und politischen Verständnis bedeutet Transparenz Klarheit, Erkennbarkeit und Nachverfolgbarkeit.[835] Systeme und ihr technischer Aufbau sollen möglichst durchschaubar und ihre Funktions- und Arbeitsweise nachvollziehbar und verständlich sein (Gegenteil einer „Blackbox“). Die darin verarbeiteten Daten und insbesondere die beteiligten Personen und deren Handlungen sollen erkennbar sein.

Einige der Transparenz untergeordneten Schutzziele lassen sich als Gegenbegriffe der Vertraulichkeitsschutzziele bezeichnen. So kann es erwünscht oder nötig sein, dass Handlungen verkettbar und nachverfolgbar sind oder Kommunikation beobachtbar und unverdeckt erfolgt.

Maßnahmen zur Gewährleistung von Systemtransparenz sind Audits, Code Review oder die Nutzung von Open-Source-Software. Nutzungstransparenz wird beispielsweise durch die Authentisierung von Personen oder die Protokollierung von Ereignissen unter Verwendung von digitalen Signaturen und Zeitstempeln sichergestellt.

Transparenz ist datenschutzrechtlich äußerst bedeutsam und nicht zuletzt deshalb als eigenständiges Datenschutzprinzip ausgestaltet.[836] Als unmittelbar Informationstechnologie und Datenschutz verbindende Transparenzvorschrift ist das Datenschutzaudit gemäß § 9a BDSG zu erwähnen.[837] Datenschutzrechtliche Unterrichtungspflichten nach § 13 Abs. 1 TMG oder § 4 Abs. 3 BDSG sind ebenfalls als Transparenzvorschriften bedeutsam.

---

835 Ähnlich *Rost/Pfitzmann*, DuD 2009, 355.

836 Näheres zur Transparenz als Datenschutzprinzip ist in Kap. 3.1.6.2 zu finden.

837 Einzelheiten dazu siehe auch weiter unten in Kap. 3.1.10.

3.1.9.5.8 Zurechenbarkeit

Die Zurechenbarkeit (Accountability) hat Bezüge zur Transparenz, Authentizität, Integrität und Nicht-Verfolgbarkeit. Sie wird auch als Nachweisbarkeit (Detectability), Unleugbarkeit oder Nicht-Abstreitbarkeit (Non-repudiation) bezeichnet. Sie hatte ursprünglich nur für Kommunikationsbeziehungen Bedeutung und meinte, dass Sendern und Empfängern von Informationen das Senden und der Empfang der Informationen nachgewiesen werden können.[838] Im Umkehrschluss sollen die Beteiligten ihre jeweilige Beteiligung nicht abstreiten können und somit das Gegenüber geschützt werden. Die Nachweisbarkeit der Identität des Absenders schützt den Empfänger davor, dass der Absender den Versand der Nachricht abstreitet, wohingegen die Nachweisbarkeit des Versendens den Absender davor schützt, dass der Versand der Nachricht bestritten wird (Nicht-Abstreitbarkeit der Herkunft). Die Nachweisbarkeit der Zustellung und des Empfangs schützt den Absender und den Empfänger davor, dass die Zustellung oder der Empfang bestritten werden können (Nicht-Abstreitbarkeit des Versands oder des Erhalts).[839]

Mittlerweile wurde die Definition allgemein um Handlungen und Transaktionen erweitert. Zurechenbarkeit bezeichnet demnach den Umstand, dass Aktionen oder Dokumente den urhebenden Personen oder Institutionen zugeordnet werden können, so dass diese Personen ihre durchgeführte Handlung oder Transaktion nachträglich nicht mehr bestreiten können.[840] Es muss bei jeder in einem IT-System ausgeführten Aktion während ihres Ablaufs und danach feststellbar sein, welcher Person eine Aktion zuzuordnen ist und wer sie letztlich zu verantworten hat.[841] Zurechenbarkeit ist somit das Gegenstück der Nicht-Verfolgbarkeit angereichert um den Aspekt der Verantwortlichkeit. Die rechtliche Bedeutung der Zurechenbarkeit ist damit offensichtlich und äußert sich insbesondere im Zusammenhang mit Rechtsgeschäften und der Zurechenbarkeit von Willenserklärungen oder Handlungen. Sie hat Bedeutung für die Beweisbarkeit und damit letztlich für die rechtliche Verantwortung und Haftung von Personen.

Maßnahmen zur Gewährleistung der Zurechenbarkeit sind, wie bei der Transparenz allgemein, die Protokollierung und der Einsatz von digitalen Signaturen und Zeitstempeln.

---

838 *Roßnagel/Pfitzmann/Garstka* 2001, 230; *Biskup* 2009, 42.

839 *Hungenberg*, Nachweisbarkeit, http://www.demonium.de/th/home/sicherheit/grundlagen/sachziele.phtml#nachweisbarkeit.

840 *Muntermann/Roßnagel, H./Rannenberg*, in: Knop/Haverkamp/Jessen: E-Science und GRID, Ad-hoc-Netze und Medienintegration 2004, 369.

841 *Dierstein*, Informatik Spektrum 2004, 349.

3.1.9.5.9 Authentizität

Authentizität[842] (Authenticity) ist gewährleistet, wenn durch geeignete Kontrollmaßnahmen sichergestellt wird, dass Daten und Informationen wirklich aus der angegebenen Quelle stammen und dass die Identität eines Benutzers oder eines angeschlossenen Systems korrekt ist. Im Rahmen einer Kommunikationsbeziehung muss außerdem sichergestellt sein, dass diese Identität über die Dauer einer Kommunikationsbeziehung erhalten bleibt.[843] Die Identifikation eines Benutzers basiert auf der Vergabe von eindeutigen Benutzerkennungen. Charakterisierende Eigenschaften zum Nachweis der Identität (Authentisierung) sind beispielsweise Passwörter, deren Kenntnis der Benutzer beim Systemzugang nachweisen muss, oder biometrische Merkmale, zum Beispiel Fingerabdrücke.[844] Auch der Besitz von Chip- oder Magnetstreifenkarten gehört dazu.[845] Identitätsnachweise werden häufig allgemein als „Credentials“ bezeichnet.[846]

Im Zusammenhang mit dem Schutzziel der Authentizität sind auch die Begriffe „Authentifizierung“, „Authentisierung“ und „Autorisierung“ voneinander abzugrenzen. Durch eine erfolgreiche Authentisierung identifiziert sich ein Benutzer oder ein System an einem anderen System. Benutzer oder anfragendes System werden bei erfolgreichem Abgleich der Credentials vom angefragten System authentifiziert. Bei der Autorisierung erhalten Nutzer meist aufgrund ihrer Zugehörigkeit zu festgelegten Gruppen oder Rollen bestimmte Rechte im IT-System zugewiesen.

Rechtlich ist die Authentizität mit der Zurechenbarkeit vergleichbar, weil diese ebenfalls die Beweisbarkeit und die Verantwortlichkeit von Personen betrifft.

3.1.9.5.10 Revisionsfähigkeit

Revisionsfähigkeit (Reviewability) bedeutet Nachprüfbarkeit und Nachvollziehbarkeit und wird durch Protokollierung und Dokumentation von Handlungen gewährleistet und lässt sich demzufolge als Unterfall der Transparenz einordnen.[847] In der Literatur wird die Revisionsfähigkeit als „Eigenschaft eines Systems, die Funktionsweise lückenlos nachzuvollziehen und damit feststellen zu können, wer, wann, welche Daten in welcher Weise verarbeitet hat (prüfende Wiederdurchsicht)“ beschrieben.[848]

Nach den Verwaltungsvorschriften zum Datenschutzgesetz des Landes Sachsen-Anhalt sind Daten revisionsfähig, „wenn nachprüfbar ist, wie sie in einen Datenbe-

---

842 Auch als „Echtheit“ bezeichnet.
843 *Holznagel* 2003, 14; *Biskup* 2009, 42.
844 *Eckert* 2006, 7.
845 *Holznagel* 2003, 14.
846 *Eckert* 2006, 7.
847 *Rost/Pfitzmann*, DuD 2009, 355.
848 *Pohl*, DuD 2004, 680.

stand gelangt sind und welche Veränderungen sie im Laufe der Zeit erfahren haben. Nachprüfbar muss sein, wer für das Aufnehmen bestimmter Daten in einen Datenbestand oder ihr Entfernen daraus die Verantwortung trägt“.[849]

Die Begriffe Zurechenbarkeit und Revisionsfähigkeit sind nicht vollkommen trennscharf voneinander, jedoch kann man eine grobe Abgrenzung dahingehend vornehmen, dass Zurechenbarkeit überwiegend Personen und deren Handlungen zum aktuellen Zeitpunkt und nachträglich betrifft, während Revisionsfähigkeit eher auf das System abstellt und nur die nachträgliche, auf die Vergangenheit bezogene, Möglichkeit der Überprüfbarkeit und die Sicherung von Kontrollrechten meint. Oft ist es so, dass durch diese Überprüfungsmöglichkeit, also vorwiegend durch Protokollierung, auch gleichzeitig eine Zurechenbarkeit von Handlungen zu Personen ermöglicht wird.

Wie bei der Zurechenbarkeit und Authentizität geht es demzufolge auch bei der Revisionsfähigkeit, wenn auch nur mittelbar, um die rechtliche Beweisbarkeit von Handlungen oder Zuständen und die sich daraus ergebenden rechtlichen Folgen und Sanktionen.

3.1.9.5.11 Verfügbarkeit

Verfügbarkeit (Availability) ist ein weiteres übergeordnetes IT-Schutzziel und meint den Schutz vor Informationsverlust, Informationsentzug oder Informationsblockade.[850] Sie betrifft sowohl informationstechnische Systeme als auch die darin verarbeiteten Daten und bedeutet, dass die Systeme jederzeit betriebsbereit sind und auf die Daten wie vorgesehen zugegriffen werden kann.[851] Zum einen muss die Datenverarbeitung inhaltlich korrekt sein und zum anderen müssen alle Informationen und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden.[852]

Im Geschäftsleben wird die Verfügbarkeit eines Systems oder Dienstes als das Verhältnis der Zeit innerhalb eines vereinbarten Zeitraums, in der das System tatsächlich zur Verfügung stand (sogenannte Betriebszeit oder „Operation Time“) zu der gesamten vereinbarten Zeit verstanden. Dieses Verhältnis wird üblicherweise in Prozent angegeben. Idealzustand sind 100 Prozent, also die jederzeitige Verfügbarkeit. Dieses Verhältnis hat Auswirkungen bei der Vereinbarung von Service Level Agreements und darin eventuell festgelegte Strafzahlungen im Fall von Vertragsverstößen.[853] Der Zeitraum ohne Verfügbarkeit des Systems wird als Ausfallzeit (Downtime) bezeichnet. Die Verfügbarkeit und Funktionsfähigkeit der Systeme

---

[849] Anweisungen zu § 6, Unterpunkt 6.2.5.

[850] *Heckmann*, MMR 2006, 281.

[851] *Dustar/Gall/Hauswirth* 2003, 217.

[852] *Holznagel* 2003, 13.

[853] Zu SLAs siehe Kap. 3.5.3.

hat somit unmittelbaren Einfluss auf die Erfüllung von rechtlichen Vereinbarungen. Eine Maßnahme zur Erhöhung der Verfügbarkeit ist der Einsatz redundanter Systeme.

3.1.9.5.12 Integrität

Integrität oder Unversehrtheit[854] (Integrity) als viertes übergeordnetes Schutzziel bedeutet Schutz vor jeglicher Form ungewollter Informationsveränderung.[855] Es beinhaltet zweierlei, nämlich die Vollständigkeit und Korrektheit der Daten (Datenintegrität) und die korrekte Funktionsweise des Systems (Systemintegrität).[856] Vollständig bedeutet, dass alle Teile der Information verfügbar sind. Korrekt sind Daten, wenn sie den bezeichneten Sachverhalt unverfälscht wiedergeben.[857] Integrität bedeutet demnach, dass Daten im Laufe der Verarbeitung oder Übertragung mittels des Systems nicht beschädigt oder durch Nichtberechtigte unbefugt verändert werden können.[858] Beschädigungs- oder Veränderungsmöglichkeiten sind das Ersetzen, Einfügen und Löschen von Daten oder Teilen davon. Rechtlich hat die Integrität für die Beweissicherung und die Beweisbarkeit von Umständen, insbesondere in der IT-Forensik, erhebliche Bedeutung. Nur unveränderte und vollständige Daten und korrekt funktionierende Systeme bieten die Gewähr, dass die zu beweisenden Umstände der Realität entsprechen.

Manipulationen dürfen nicht unbemerkt bleiben.[859] Das bedeutet, dass Techniken erforderlich sind, mit deren Hilfe unautorisierte Manipulationen nachträglich erkennbar sind. So kann verhindert werden, dass unautorisiert manipulierte Daten weiterverarbeitet werden, so dass der mögliche Schaden begrenzt wird.[860] Zur Erkennung von durchgeführten Datenveränderungen werden kryptographisch sichere Hashfunktionen eingesetzt.[861] Neben der Erkennbarkeit ist auch die (automatische) Verbesserung verfälschter Inhalte, sprich die Wiederherstellung des Ausganszustands, wünschenswert, was jedoch nicht immer technisch realisierbar ist.[862]

3.1.9.5.13 Verlässlichkeit

Mit der Integrität und Verfügbarkeit hängen die Verlässlichkeit und die Beherrschbarkeit von Systemen zusammen. Unter Verlässlichkeit eines Systems versteht man

---

854 So zum Beispiel in § 2 Abs. 2 BSIG.

855 *Heckmann*, MMR 2006, 281.

856 *Hungenberg*, Sachziele der Informationssicherheit, http://www.demonium.de/th/home/sicherheit/grundlagen/sachziele.phtml.

857 *Holznagel* 2003, 13; *Biskup* 2009, 41.

858 *Holznagel/Schumacher*, MMR 2009, 3; *Holznagel* 2003, 13; *Biskup* 2009, 42; *Heckmann*, MMR 2006, 281.

859 *Biskup* 2009, 42.

860 *Eckert* 2006, 8.

861 *Eckert* 2006, 8.

862 *Biskup* 2009, 42.

die Eigenschaft, keine unzulässigen oder undefinierten Zustände anzunehmen (Dependability) und die Gewährleistung, dass die spezifizierte Funktion zuverlässig erbracht wird (Reliability).[863] Die tatsächlich vorhandene Ist-Funktionalität soll folglich mit der vorher bestimmten Soll-Funktionalität übereinstimmen. Dieser Verlässlichkeitsaspekt wird auch als Funktionssicherheit oder Ordnungsmäßigkeit bezeichnet. Alternativ wird Verlässlichkeit als eine Sachlage definiert, bei der weder die Systeme noch die mit ihnen verarbeiteten Daten (Informationen) noch die Datenverarbeitung (Funktionen und Prozesse) in ihrem Bestand, ihrer Nutzung oder ihrer Verfügbarkeit unzulässig beeinträchtigt werden.[864] Wie bei der Integrität geht es unter rechtlichen Gesichtspunkten um die Beweisbarkeit von Umständen und Zuständen.

Um eine hohe Verlässlichkeit zu erzielen, werden in der Praxis verschiedene Testverfahren eingesetzt, wie etwa Unit Tests, die Nutzungsszenarien einer Software simulieren und auf eventuell vorhandene Abweichungen zur Soll-Funktionalität prüfen.[865]

3.1.9.5.14 Beherrschbarkeit

Im Unterschied zur Verlässlichkeit, welche die Sicherheit des Systems betrifft, bezieht sich die Beherrschbarkeit (Controllability) auf die Sicherheit des Betroffenen. Beherrschbarkeit wird auch als „Freiheit von Nebenwirkungen“ ausgelegt und bedeutet konkret, dass das IT-System kein „Eigenleben“ entwickelt und damit keine nichttolerierbaren Nebenwirkungen auftreten. Ein IT-System ist beherrschbar, wenn der Einzelne und die Gesellschaft vor unerwünschten oder ungewollten Auswirkungen des Einsatzes des IT-Systems im Rahmen des vorzugebenden Grenzrisikos bewahrt bleiben.[866] Dabei ist auch zu beachten, dass nur beherrschbare Systeme rechtlich effektiv regulierbar sind. Insbesondere die Durchsetzung und Wahrung von Rechten gestaltet sich schwierig, wenn die beteiligten Systeme nicht so funktionieren, wie vorgesehen und zu negativen Auswirkungen bei den Nutzern und Betroffenen führen.

Maßnahmen um unerwünschte Nebenwirkungen zu reduzieren sind die gründliche Validierung von Eingabedaten und das bewusste Abfangen von ungültigen Daten, die zu fehlerhaften Zuständen führen könnten.

3.1.9.5.15 Nicht-Vermehrbarkeit

Nicht-Vermehrbarkeit (Non-propagation) von Informationen bedeutet, dass diese von Unberechtigten nicht kopiert oder im Rahmen von sogenannten „Replay-Angriffen“ nicht unerkannt wiederholt werden können. Im Falle eines Replay-

---

863 *Eckert* 2006, 6.

864 *Dierstein* 2004, 346.

865 *Frankl/Hamlet/Littlewood/Strigini* 1997, 68 ff.

866 *Dierstein* 2004, 348.

Angriffs sammelt der Angreifer zuvor aufgezeichnete Daten, um diese später gezielt wieder einzuspielen und eine fremde Identität vorzutäuschen. Dies kann zum Beispiel zur missbräuchlichen Wiederholung einer finanziellen Transaktion führen.[867] Aus einer rechtlichen Perspektive dient das Schutzziel somit allgemein dazu den Missbrauch von bestehenden Rechten zu vermeiden und Rechtsgüter gegen Beschädigung zu schützen. Eine verbreitete Gegenmaßnahme gegen Replay-Angriffe ist die Verwendung von großen, nicht vorhersagbaren und nur einmalig gültigen Zeichenketten, sogenannten Nonces.[868]

3.1.9.5.16 Kontingenz und glaubhafte Abstreitbarkeit

Kontingenz (Contingency) als letztes übergeordnetes Schutzziel soll gegen Einengungen durch Technik fungieren und ist im Zusammenhang mit der Integrität zu sehen. Trotz des Technikeinsatzes soll es möglich sein, Inhalte und Umstände der Technikanwendung in der Schwebe zu halten, um nicht durch diesen Technikeinsatz ohne Interventionsmöglichkeit eingeengt zu werden.[869] Inhalt des Schutzziels ist die Möglichkeit festzustellen, dass „etwas anders sein könnte, als es scheint“, während die Integrität als Schutzziel immer nur die Feststellung erlaubt, dass „etwas so ist, wie es ist“.[870]

Diese Möglichkeit, dass etwas anders ist, als es erscheint, erinnert stark an das durch Kryptographie ermöglichte Konzept der glaubhaften Abstreitbarkeit (Plausible Deniability) und kann als, aus der Kontingenz abgeleitetes IT-Schutzziel angesehen werden.

Softwaretechnisch wird glaubhafte Abstreitbarkeit beispielsweise in der Verschlüsselungssoftware „Truecrypt“[871] oder beim sogenannten „Off-the-Record Messaging“[872] umgesetzt. Mit der Nutzung von Truecrypt wird es beispielsweise unmöglich gemacht nachzuweisen, dass überhaupt Verschlüsselung eingesetzt wird. Die verschlüsselten Daten sehen wie Zufallszahlen[873] aus. Eine daraus abgeleitete Umsetzung ist die Möglichkeit der Nutzung von versteckten Datencontainern oder ganzen Betriebssystemen innerhalb eines äußeren Dummycontainers. Wird der Nutzer beispielsweise mit Gewalt dazu gezwungen, das vermeintlich richtige Passwort zu verraten, so kann er das Passwort des äußeren Containers angeben, ohne dass die

---

867 *Repges*, Internetspezifische Angriffe, http://www.repges.net/IPSec/Angriffe_IPSec/INTERN_1/intern_1.htm.

868 *Kappes* 2007, 208.

869 *Rost/Pfitzmann*, DuD 2009, 353 f.

870 *Rost/Pfitzmann*, DuD 2009, 354.

871 *Truecrypt*, Protection of Hidden Volumes, http://www.truecrypt.org/docs/hidden-volume-protection.

872 *Cypherpunks*, Off-the-Record Messaging, http://www.cypherpunks.ca/otr.

873 Datenträger werden beispielsweise mit Zufallszahlen überschrieben, um die darauf enthaltenen Daten zu vernichten.

Daten im inneren Container sichtbar werden. Weil die verschlüsselten Daten der beiden Container immer wie Zufallszahlen aussehen, ist es möglich, die Existenz des versteckten Containers plausibel abzustreiten. Ein Angreifer kann nicht beweisen, dass neben dem Dummycontainer weitere versteckte Container existieren. Es scheint ein Container vorhanden zu sein, es könnten aber auch überhaupt keiner (lediglich Zufallszahlen) oder mehr als einer vorhanden sein.

Rechtlich wird durch glaubhafte Abstreitbarkeit einerseits der Selbstdatenschutz gestärkt, andererseits kann dadurch auch eine möglicherweise erwünschte Beweisführung unmöglich gemacht werden.

3.1.9.6 Konzept der mehrseitigen Sicherheit

Wenn mehrere Subjekte an der Nutzung eines IT-Systems beteiligt sind, ergeben sich Konflikte, da alle Beteiligten individuelle Sicherheitsbedürfnisse haben. Einen Versuch des Ausgleichs auf der Ebene der Sicherheit liefert das sogenannte Konzept der mehrseitigen oder multilateralen Sicherheit.[874]

Mit der verstärkten Vernetzung der Informationstechnologie im Alltag, die nicht zuletzt durch Cloud Computing noch weiter verstärkt wird, hat sich der Komplexitätsgrad von Sicherheitsproblemen erheblich gesteigert. Es handeln verschiedene Subjekte, die entweder miteinander kooperieren oder konkurrieren und dementsprechend jeweils unterschiedliche Sicherheitsanforderungen an die IT stellen. So möchte oder muss ein Cloudanbieter beispielsweise möglichst viele Daten der Nutzung seines Dienstes protokollieren, um gegebenenfalls Sicherheitsvorfälle analysieren und aufklären zu können. Die Nutzer sind demgegenüber daran interessiert möglichst wenige Daten preiszugeben. Neben die anbieterbezogene Systemsicherheit treten somit die Sicherheitsinteressen der Benutzer oder derjenigen, die von der Informationsverarbeitung betroffen sind.[875] Dieser Erkenntnis der unterschiedlichen Interessen bei der Nutzung eines IT-Systems liegt das Konzept der mehrseitigen Sicherheit zugrunde. Dementsprechend wird mehrseitige Sicherheit als die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung definiert.[876] Später wurde diese Definition um den Aspekt des gegenseitigen Vertrauens ergänzt.[877]

---

874 Das Konzept wurde von *Rannenberg*, *Pfitzmann* und *Müller* begründet; siehe dazu insbesondere *Rannenberg*/*Pfitzmann*/*Müller*, in: Müller/Pfitzmann, Mehrseitige Sicherheit in der Kommunikationstechnik 1998, 21 ff. und *Federrath/Pfitzmann* 1998, 319 ff.

875 *Holznagel* 2003, 12 f.

876 *Federrath/Pfitzmann* 1998, 328; *Federrath/Pfitzmann*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 2.2, Rn. 16.

877 *Roßnagel/Pfitzmann/Garstka* 2001, 228.

Sicherheit ergibt sich somit aus einem mindestens bilateralen Ansatz, wobei eine Wechselwirkung zwischen den jeweiligen individuellen Schutzinteressen besteht.[878] Sind die Systeme oder Techniken nicht nur unilateral nutzbar, sondern bilateral, trilateral oder sogar multilateral, Letzteres ist wegen der Mehrmandantenfähigkeit bei Clouddiensten der Fall, so ist die Sicherheit nur gewährleistet, wenn alle Beteiligten kooperieren und zusammenwirken. Dies setzt in einem großen Maß Koordination und Aushandlung voraus.[879] Die Koordination erfolgt bei Clouddiensten überwiegend durch den Anbieter, indem er Verträge mit den Kunden schließt (bilateral) und beispielsweise Hypervisoren einsetzt, um die mehrmandantenfähigen virtuellen Serversysteme für die unterschiedlichen Kunden einzuteilen und möglichst sicher abzuschotten (multilateral).

Außerdem ist zu beachten, dass mehrseitige Sicherheit nicht nur den Kommunikationspartnern selbst dient, sondern auch all denjenigen, die mit den Kommunikationspartnern oder mit dem jeweiligen Kommunikationsinhalt in Beziehung stehen oder die Kommunikationsmittel bereitstellen.[880]

Die Realisierung von mehrseitiger Sicherheit führt auch nicht zwangsläufig dazu, dass die Interessen aller Beteiligten erfüllt werden. Möglicherweise offenbart sie sogar gegensätzliche, unvereinbare Interessen, die den Beteiligten vorher nicht bewusst waren. Sie führt jedoch letztlich dazu, dass die Partner einer mehrseitig sicheren Kommunikationsbeziehung in einem (rechtlich) geklärten Kräfteverhältnis miteinander interagieren.[881] Bei Cloud Computing beispielsweise durch das Anpassen von Verträgen an geänderte Rahmenbedingungen und sich ändernde Interessen und Bedürfnisse.

Während die Schutzziele ein systematisches und planvolles Vorgehen bei der Absicherung und Gestaltung der Cloudsysteme an sich ermöglichen, bedeutet mehrseitige Sicherheit, dass primär die jeweiligen Interessen der Beteiligten (Cloudanbieter, Cloudnutzer, Betroffene, Subunternehmen oder sonstige Dritte) ermittelt und beachtet werden müssen. Während im Anbieter-Nutzer-Verhältnis eher vertragliche Lösungen mit Sanktionsmöglichkeiten im Vordergrund stehen, sind im Verhältnis der Nutzer untereinander technische Lösungen zur Wahrung der jeweiligen Sicherheitsinteressen nötig, zum Beispiel die oben erwähnten Hypervisoren und deren Absicherung. Die Nutzung durch mehrere Parteien führt nämlich zwangsläufig dazu, dass sich neue Sicherheitsschwachstellen, beispielsweise durch fehlerhaft implementierte Hypervisoren, auftun.[882] Technische Lösungen im Anbieter-Nutzer-Verhältnis sind beispielsweise technische Protokollierungen, so dass sowohl die

---

878 Siehe dazu auch das Schaubild bei *Roßnagel/Pfitzmann/Garstka* 2001, 231.

879 *Roßnagel/Pfitzmann/Garstka* 2001, 237.

880 *Roßnagel/Schneider*, it+ti 1996, 15.

881 *Federrath/Pfitzmann* 1998, 328.

882 *Slamka/Georg*, in: Schartner/Weippl, D-A-CH Security 2010, 24.

Nutzer als auch die Anbieter ihre vertraglich festgelegten Interessen wechselseitig überprüfen und durchsetzen können, und somit – neben Sicherheitsverbesserungen – auch wechselseitige Transparenz erreicht wird.

3.1.9.7 Zentrale Probleme des Cloud Computing

Cloud Computing tangiert wegen seiner technischen und strukturellen Ausgestaltung unmittelbar oder mittelbar alle IT-Schutzziele. Diese sind bei der rechtlichen Technikgestaltung[883] und der Aufstellung von notwendigen Sicherheitsmaßnahmen zu beachten.[884]

Die neuartigen und zentralen Probleme des (Public) Cloud Computing bestehen aber darin, die Vertraulichkeit und Integrität der Daten zu gewährleisten.[885] Durch die Verarbeitung und Speicherung der Daten beim Cloudanbieter, ohne dass die Kunden nachvollziehen können, wie diese Verarbeitungsvorgänge ablaufen und wo genau die Daten gespeichert werden, ist außerdem die Transparenz betroffen.

3.1.9.7.1 Vertraulichkeit

In Cloudsystemen, insbesondere in Public Clouds, sind die Daten häufig in Bewegung, weil die Anbieter zur Optimierung ihrer Ressourcen und der Infrastruktur sowie zur Sicherstellung der Performanz die Daten auf unterschiedliche Rechner im Serververbund kopieren und duplizieren. Diese Vorgänge liegen regelmäßig außerhalb der Einflussmöglichkeiten der Kunden und können zu Vertraulichkeitsproblemen führen, wenn die Daten beispielsweise Landesgrenzen überschreiten oder auf (unsicheren) Systemen von Subunternehmen gespeichert werden.[886]

Aufgrund der eingesetzten Algorithmen und Dateisysteme der Cloudanbieter kann nicht immer garantiert werden, dass die Daten dauernd verschlüsselt auf einem Speichermedium vorliegen. In den Geschäftsbedingungen der meisten Cloudanbieter gibt es zudem nur selten Zusicherungen darüber, wo die Daten gespeichert werden und wie ihre Vertraulichkeit geschützt wird. Dem Kunden ist es selbst überlassen, die Daten mit eigenen Mitteln und Verfahren zu verschlüsseln.[887] Außerdem sind die Daten während einer Verarbeitung unverschlüsselt, so dass sie the-

---

[883] Wie weiter unten zu sehen sein wird, sind die Kriterien Transparenz, Integrität und Verfügbarkeit weitgehend mit den entsprechenden Schutzzielen identisch; siehe dazu die Kap. 4.4.3, 4.4.11 und 4.4.12.

[884] Bei einer zukünftigen Reform des § 9 BDSG samt Anlage oder nach den oben erwähnten Landesdatenschutzgesetzen sind die Schutzziele sogar unmittelbar rechtlich relevant, soweit mit personenbezogenen Daten in einer Cloud umgegangen wird; vergleiche Kap. 3.1.9.4.

[885] *Weichert*, DuD 2010, 680.

[886] *Ruppel*, Vertraulichkeit, Integrität und Verfügbarkeit beim Cloud Computing, http://www.searchsecurity.de/themenbereiche/applikationssicherheit/web-application-security/articles/249238.

[887] *Ruppel*, Vertraulichkeit, Integrität und Verfügbarkeit beim Cloud Computing, http://www.searchsecurity.de/themenbereiche/applikationssicherheit/web-application-security/articles/249238.

oretisch vom Anbieter, von Subunternehmen oder von Externen zur Kenntnis genommen werden können. Erfolgt die Verschlüsselung mit Schlüsseln der Cloudanbieter oder der Subunternehmen ist eine Kenntnisnahme auch von gespeicherten Daten möglich.

Neben dem Schutz von ruhenden Daten umfasst das Schutzziel Vertraulichkeit auch den Datentransport. Zwar ist die Datenübertragung primär Aufgabe des Telekommunikationsanbieters und nicht die des Cloudproviders, jedoch betrifft dies nur die Bereitstellung der technischen Infrastruktur, wie zum Beispiel Router und Leitungen. Die verwendeten Protokolle oder Verschlüsselungsmethoden auf der Transport- und Anwendungsschicht (OSI-Layer 6 und 7) werden hingegen vom Cloudprovider vorgegeben oder mit dem Kunden vereinbart, beispielsweise indem die weitverbreitete SSL/TLS-Verschlüsselung[888] genutzt wird. Dies ist angesichts der Möglichkeiten aktueller Deep-Packet-Inspection-Verfahren durch Provider oder Behörden und der Bedrohung durch Man-in-the-Middle-Angriffe ein nicht zu unterschätzender Aspekt zur Wahrung der Vertraulichkeit der Kommunikationsinhalte.[889]

3.1.9.7.2 Integrität

Das Schutzziel Integrität umfasst bekanntermaßen die Vollständigkeit und Korrektheit der Daten (Datenintegrität) und die korrekte Funktionsweise des Systems (Systemintegrität).[890] Vollständigkeit und Korrektheit im Sinne der Datenintegrität bedeutet für Cloudsysteme, dass die Daten nicht unautorisiert und unbemerkt verändert oder gelöscht werden können. Die Cloudsystemkomponenten, also alle Komponenten, die Daten speichern, verarbeiten oder übertragen, müssen wie beabsichtigt funktionieren, um die Systemintegrität zu gewährleisten.

Mögliche Maßnahmen zur Sicherung der Integrität betreffen nicht nur den Cloudanbieter, sondern alle Beteiligten, inklusive möglicher Subunternehmen als Ressourcenanbieter, die Nutzer und eingeschränkt sogar die Telekommunikationsanbieter. In einem komplexen, verteilten System, zum Beispiel einem Cloudsystem, kann die Gewährleistung der Integrität eine sehr komplizierte Aufgabe darstellen, die die Abstimmung aller Beteiligten erfordert, primär jedoch den Cloudanbieter betrifft.[891]

Cloudspezifisch ist demzufolge die Unübersichtlichkeit über die Beteiligten und die Vielzahl von Subsystemen. Dies ist insbesondere in Public Clouds der Fall, wenn

---

[888] Secure Socket Layer (SSL) und Transport Layer Security (TLS).

[889] Zu Deep Packet Inspection siehe auch Kap. 3.8.1.1.1.

[890] Siehe Kap. 3.1.9.5.12.

[891] *Ruppel*, Vertraulichkeit, Integrität und Verfügbarkeit beim Cloud Computing, http://www.searchsecurity.de/themenbereiche/applikationssicherheit/web-application-security/articles/249238/index2.html.

Ressourcen bei Subunternehmen kurzfristig durch den Cloudanbieter hinzugebucht werden und vor der Buchung nicht geprüft wurde, ob diese die Daten- und Systemintegrität gewährleisten können. So können beispielsweise die lokalen Administratoren der Ressourcenanbieter Zugriff auf die vom Cloudprovider ausgelagerten Daten erhalten und diese manipulieren, duplizieren oder löschen.

Gleiches gilt im Übrigen auch für sonstige Angreifer. Einmal in die metaphorische Wolke eingebrachte Daten sind nur beschränkt überwachbar, so dass die Wahrscheinlichkeit einer Manipulation der Daten und damit eine Integritätsverletzung wahrscheinlicher ist als bei lokal und offline vorgehaltenen Daten. Vor allem verschlüsselte Daten können durch geringste Änderungen, beispielsweise durch Änderung eines einzigen Bits,[892] unbrauchbar werden. Auch Fehler in den Konfigurationen der (virtuellen) Cloudsysteme können zu Integritätsverletzungen führen.

Dem Schutzziel Integrität ist auch das folgende Problem geschuldet. Daten können durch die Nutzung von Cloud Computing so aufgespalten werden, dass die Einzelteile über mehrere Server verstreut sind und erst im zusammengesetzten Zustand wieder als Daten ihren Informationsgehalt offenbaren. Hintergrund dieser Aufspaltung ist zum einen die flexible Nutzung von vorhandenen Ressourcen und zum anderen die Datensicherung. Die aufgespaltenen Datenbruchstücke werden vermehrt und anschließend mehrfach redundant und (potentiell weltweit) gespeichert. Gehen Fragmente verloren oder werden sie beschädigt, so kann im Idealfall aus den noch verfügbaren Fragmenten der Datensatz wieder rekonstruiert werden.[893] Insofern ist dieses auf den ersten Blick destruktive Vorgehen zunächst eine Maßnahme zur Wahrung der Datenintegrität. Durch die Verteilung steigt zudem gleichzeitig auch die Verfügbarkeit der Daten. Allerdings kann Korrektheit der Daten im Kontext der Integrität auch bedeuten, dass nur ein einziger Datensatz vorhanden sein darf. Eine Vielzahl von Datensätzen kann die Integrität aller Datensätze in Frage stellen, wenn einzelne Teile oder ganze Duplikate durch Beschädigungen sich inhaltlich widersprechen.[894] Um solchen Fehlern vorzubeugen bietet es sich an Checksummen und Hashwerte zu verwenden.

3.1.9.7.3 Transparenz

Ein weiteres Problem des Cloud Computing ist die mangelnde Transparenz der Datenverarbeitung. Dieser Mangel ist zum Teil technikinhärent, jedoch hauptsächlich

---

892 Teilweise auch technisch bedingt, beim sogenannten „Kippen“ eines Bits.

893 Nach dem gleichen Prinzip funktioniert zum Beispiel das kommerzielle Storageangebot von „Amplidata“ mit dessen „BitSpread-Mechanismus“; *Rüdiger*, Datenverwaltung: innovative Produkte für die Cloud, http://www.zdnet.de/it_business_technik_datenverwaltung_innovative_produkte_fuer_die_cloud_story-11000009-41539940-3.htm; http://www.amplidata.com; siehe dazu auch die Ausführungen in Kap. 3.1.9.9.6.

894 Zum Beispiel durch das „Kippen“ eines Bits; siehe dazu Fn. 892.

der regelmäßig anzutreffenden Verweigerungshaltung der Anbieter geschuldet. Diese verweigern ihren Kunden üblicherweise die Herausgabe der Details über die Art und Weise der Datenverarbeitung, deren Ort und wohin genau die Daten übermittelt werden.

3.1.9.7.3.1 Technikbedingte Intransparenz

Prinzipbedingt ist gerade in großangelegten Public Clouds, zum Beispiel wegen der Lastverteilung[895] (Load Balancing), nicht vorhersagbar, wie, wie oft und wo genau Daten oder Teile von Daten oder Datenfragmente gespeichert werden. Die einzige effektive Möglichkeit Vorhersagbarkeit zu gewährleisten besteht darin, bestimmte Serverstandorte oder Rechenzentren von der Datenverarbeitung auszuschließen oder von vornherein auf bestimmte Server oder Rechenzentren zu begrenzen. Auch diese Information der Nutzer über die Handhabung und Begrenzung auf Serverstandorte ist Teil der Transparenz. Bei den Anbietern setzt sich allerdings langsam die Erkenntnis durch, dass es insbesondere datenschutzrechtliche Regelungen gibt, die auf den Speicherort oder Ort der Verarbeitung abstellen und dementsprechend Relevanz für die Nutzer haben. Ein Beispiel hierfür ist Amazon mit seiner EU-belegenen Availability Zone.

3.1.9.7.3.2 Anbieterbedingte Intransparenz

Im Gegensatz zu Vorhersagen ist die nachträgliche Nachvollziehbarkeit der stattgefundenen technisch bedingten Ereignisse und menschlichen Handlungen innerhalb des Cloudsystems problemlos möglich. Mittel hierfür sind die Protokollierung und Erstellung von Logdateien oder Data Tracking Tools.[896] Zwar bedeutet die Protokollierung einen gewissen administrativen Aufwand, jedoch ist dieser notwendig, nicht zuletzt um Angriffe auf ein System oder Fehler in der Verarbeitung der Daten nachvollziehen zu können. Das Transparenzproblem besteht allerdings nicht darin, technisch und tatsächlich die Protokolle zu erstellen, sondern darin, dass Protokollergebnisse und Monitoring Tools den Nutzern vorenthalten oder nicht angeboten werden. Kunden müssten bei vertraglichen Vereinbarungen darauf hinwirken, dass sie Einsicht und die nötigen Mittel zur Verfügung gestellt bekommen.

Diese Form der Intransparenz betrifft weniger IaaS, aber umso mehr SaaS und ist auch mit dem Schutzziel der Beherrschbarkeit verknüpft. Je weniger Möglichkeiten dem Nutzer zur Steuerung und Beherrschbarkeit des ihm zur Verfügung gestellten Systems oder der Anwendung bleiben, umso eher ist er auf den Cloudanbieter und dessen Protokolle und Auswertungen angewiesen. Im Prinzip widerspricht diese verbraucher- und nutzerunfreundliche Haltung auch dem Self-Service-Prinzip. Es

---

[895] *Elektronik Kompendium*, Load Balancing, http://www.elektronik-kompendium.de/sites/net/0906201.htm.

[896] Data Tracking Tools sollen die Nachverfolgbarkeit hinsichtlich des physischen Speicherorts und der Speicherzeit von Daten ermöglichen.

ist aber bereits absehbar, dass sich aufgrund der Konkurrenzsituation auf dem Cloudmarkt die Stellung der Nutzer immer weiter verbessert, da der Service für den Kunden und Transparenzaspekte wichtige Abgrenzungsmerkmale darstellen.

3.1.9.7.4 Bedeutung sonstiger Schutzziele

Wie einleitend angedeutet, sind neben der Vertraulichkeit, Integrität und Transparenz auch alle anderen über- und untergeordneten Schutzziele für Cloud Computing und dessen praktischen Einsatz relevant. Wegen der Interaktion und Kommunikation zwischen Server- und Clientsystemen über das Internet sind sowohl die Schutzziele, die schwerpunktmäßig die Absicherung der Einzelsysteme zum Ziel haben, als auch die die Kommunikation absichernden Schutzziele gleichermaßen bedeutsam.

Die bei der Erörterung der Schutzziele gewonnenen Erkenntnisse können dazu beitragen, die in Cloudumgebungen eingesetzte Technik und Sicherheitslösungen anhand dieser Sicherheitszielsetzungen zielführend zu gestalten und damit die Datensicherheit und auch den Schutz von Daten zu erhöhen. Außerdem dürften die meisten der dort angeführten Maßnahmen zur Zielerreichung auch in Cloudumgebungen ihre Wirkung beibehalten.

3.1.9.8 Bedrohungsanalyse

Um sichere Cloudsysteme gestalten und die möglichen Risiken in Form von Schadenswahrscheinlichkeiten oder Schadenspotentialen abschätzen und adäquate Sicherheitsmaßnahmen treffen zu können, benötigt man einen Überblick über die existierenden und potentiellen Bedrohungen. Diese müssen so konkret wie möglich bestimmt werden. Die rechtlich begründete Gestaltung kann nämlich nur dann gelingen, wenn man die problematischen Aspekte und Ansatzpunkte kennt. Die Gestaltung erfolgt am aktuellen und kurzfristig absehbaren Stand der Technik und somit auch am Stand der aktuellen Sicherheitstechniken.

Die rechtlichen Anforderungen an die IT-Sicherheit sind nur im Zusammenspiel mit diesem Stand der Sicherheitstechnik richtig zu verstehen und vor allem ziel- und zweckgerichtet interpretierbar. Rechtsverträglichkeit ist somit, genauso wie die Sicherheit eines Systems, ein Prozess, der zwar die Gestaltung des Systems als Ausgangspunkt hat, jedoch nicht damit endet. Die Gestaltung zu Beginn gibt jedoch „den Weg vor“. Fehler in der Gestaltung oder die Nichtbeachtung von rechtlichen Vorgaben können dazu führen, dass eine spätere Anpassung nicht mehr oder nur mit unverhältnismäßigen Aufwand möglich ist.

Die Durchführung einer Bedrohungsanalyse ist jedoch nicht nur für die Technikgestaltung bedeutsam, sondern kann vor allem für Unternehmen in der Rechtsform einer Kapitalgesellschaft unmittelbar rechtlich vorgegeben sein. Insbesondere die

Etablierung von Risikomanagement- und Risikofrüherkennungssystemen[897] im Rahmen der Compliance hat zwingend die Durchführung einer Bedrohungsanalyse als Voraussetzung. Ebenso wie bei der technischen Gestaltung sind die Abwendung von Bedrohungen und die Einschätzung von potentiellen und konkreten Risiken nur möglich, wenn man diese vorher ermittelt und zur Kenntnis nimmt. Maßgebliche Vorschriften sind insbesondere § 91 Abs. 2 AktG und § 43 Abs. 2 GmbHG.[898] Eine weitere, ebenfalls nur mittelbare, rechtliche Regelung zur Notwendigkeit einer Bedrohungsanalyse findet sich in § 109 Abs. 3 Satz 1 Nr. 2 TKG.[899] Adressaten der Vorschrift sind ebenfalls Unternehmen, dabei speziell Telekommunikationsunternehmen mit der entsprechenden technischen Infrastruktur.

Während die Technikgestaltung überwiegend auf die technisch zu treffenden Maßnahmen abzielt, sind bei unternehmensbezogenen Bedrohungsanalysen auch und gerade organisatorische Faktoren, nicht nur im Rahmen der Prüfung der IT-Sicherheit, Teil einer solchen Analyse. Zudem hat die vorlaufende Technikgestaltung auch auf ein solches unternehmensbezogenes Risikomanagement Einfluss, so dass die beiden Aspekte nicht völlig zusammenhanglos nebeneinander stehen. Rechtsgemäß und sicher gestaltete Technik erleichtert auch das Management von Risiken beim Einsatz von Unternehmensinformationstechnologie. Wegen der umfassenden Nutzung und Abhängigkeit von IT in Unternehmen kann unsichere Technik und ein entsprechender Sicherheitsvorfall verbunden mit dem Ersatz von Schäden oder durch Reputationsverluste oft zur Insolvenz einer Gesellschaft führen.

Angesichts dieser Erwägungen sollen nun im Anschluss die allgemeinen Bedrohungen der IT-Sicherheit aufgezeigt werden, die zudem auch für Cloud Computing relevant sind. Diesen vorausgehend erfolgt die Definition und Abgrenzung der in diesem Zusammenhang oft verwendeten Begriffe. Für die später anzuwendende KORA-Methode stellt die Bedrohungsanalyse und -darstellung den informationssicherheitsrelevanten Risikenteil der „Chancen und Risiken des Cloud Computing“ dar. Die bereits oben dargestellten Nachteile betreffen vorwiegend wirtschaftliche oder konzeptionelle Nachteile, während nunmehr auf die technikbedingten Risiken und Nachteile einzugehen ist. Konzeptionelle oder ökonomische Fehlentwicklungen, also solche, die nicht die Technik betreffen oder diese als Ursprung haben, sind auch nicht oder nur sehr eingeschränkt durch Technikgestaltung zu beseitigen oder zu steuern.

Die mit Cloud Computing neu entstandenen Bedrohungen und die zu ihrer Beseitigung notwendigen Sicherheitsmaßnahmen werden, zwecks besseren Verständnisses, nach der Darstellung der allgemeinen Bedrohungen und der wichtigsten

---

[897] Manchmal auch als „Security Management Systeme“ oder „Information Security Management Systeme“ (ISMS) bezeichnet.

[898] Zu Einzelheiten hierzu siehe Kap. 3.6.1.

[899] Siehe dazu weiter oben Kap. 3.1.9.3.3.

Sicherheitsmaßnahmen gesondert erläutert.[900] Diese Vorgehensweise bietet, wie bei der Darstellung der Schutzziele, den Vorteil, dass die Maßnahmen im unmittelbaren Zusammenhang mit den spezifischen Bedrohungen aufgezeigt werden können.

3.1.9.8.1 Begriffsdefinitionen und gegenseitige Abgrenzung

Bevor auf die diversen Bedrohungsarten und die konkreten Bedrohungen der allgemeinen IT-Sicherheit eingegangen wird, ist es notwendig die damit zusammenhängenden Begriffe zu definieren, näher zu erläutern und voneinander abzugrenzen. Soweit Cloud Computing dabei eine ganz besondere und spezifische Rolle spielt, soll die Erläuterung einiger Begriffe im Cloudkontext erfolgen.

3.1.9.8.1.1 Bedrohung, Gefährdung und verwandte Begriffe

Bedrohungen im IT-Kontext sind Umstände oder Ereignisse, die prinzipiell die Schutzziele der IT-Sicherheit oder Rechtsgüter verletzen und zu einem Schaden führen können.[901] Beispiele für Bedrohungen sind höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen.[902]

Die Bedrohung ist abzugrenzen vom Begriff der Gefährdung. Eine Gefährdung ist die Folge aus einer Bedrohung und einer Schwachstelle.[903] Eine Bedrohung allein, wie sie durch einen Hacker, einen Spion, jegliche Form von Schadsoftware (Viren, Würmer, Trojaner, usw.)[904] oder aber auch durch höhere Gewalt besteht, wäre für ein perfektes IT-System, sofern es ein solches gäbe, nicht gefährlich. Erst dadurch, dass das System oder die das System umgebenden Personen, Räumlichkeiten oder Regelungen eine Schwachstelle aufweisen, die durch eine Bedrohung ausgenutzt werden kann, entsteht eine Gefährdung.[905] Kurz zusammengefasst wird also eine Bedrohung erst durch die Ausnutzung einer vorhandenen Schwachstelle zur Gefährdung.

Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der

---

900 Siehe dazu die Ausführungen in Kap. 3.1.9.10.

901 *Sackmann*, IT-Sicherheit, http://www.enzyklopaedie-der-wirtschaftsinformatik.de/wi-enzyklopaedie/lexikon/technologien-methoden/Informatik--Grundlagen/IT-Sicherheit; *BSI*, Glossar und Begriffsdefinitionen, https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/glossar/04.html; zum Schadensbegriff siehe Kap. 3.1.9.8.1.3.

902 Siehe dazu auch die Ausführungen zu den Bedrohungsklassifizierungen in Kap. 3.1.9.8.2.

903 *BSI*, Gefährdungen: Begriffserläuterung, Einführung, https://www.bsi.bund.de/DE/Themen/InternetSicherheit/Gefaehrdungen/gefaehrdungen_node.html.

904 Zu deren Erläuterung siehe beispielsweise *Federrath/Pfitzmann*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 2.2, Rn. 35 ff.

905 *BSI*, Gefährdungen: Begriffserläuterung, Einführung, https://www.bsi.bund.de/DE/Themen/InternetSicherheit/Gefaehrdungen/gefaehrdungen_node.html; zum Risikobegriff siehe Kap. 3.1.9.8.1.4.

Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam und ein System geschädigt wird. Durch eine Schwachstelle wird das System anfällig für Bedrohungen.[906]

Eine Verwundbarkeit ist eine Schwachstelle, über die die Sicherheitsdienste des Systems umgangen, getäuscht oder unautorisiert modifiziert werden können.[907] Eine Verwundbarkeit ist somit ein Unterfall einer Schwachstelle. Synonym für „Verwundbarkeit“ ist der Begriff der „Sicherheitslücke“. Ein sogenannter „Exploit“ ist eine Software oder Sequenz von Befehlen, die eine solche Sicherheitslücke ausnutzt.[908]

3.1.9.8.1.2 Bedeutungen des Gefahrbegriffs und Abgrenzung zur Gefährdung

Gefahr im informationstechnischen Sinne ist als potentielles Eintreten einer Bedrohung gegen ein IT-System, unabhängig vom Vorhandensein eventueller Schwachstellen oder von Sicherheitsmaßnahmen, zu verstehen.[909] Der Gefahrenbegriff ist jedoch nicht nur informatisch belegt, sondern gerade auch rechtlich bedeutsam und hat im Polizei- und Ordnungsrecht seine eigene Bedeutung. Eine Gefahr liegt demnach vor, wenn eine Sachlage oder ein Verhalten bei ungehindertem Ablauf des objektiv zu erwartenden Geschehens in absehbarer Zeit und mit hinreichender Wahrscheinlichkeit ein polizeilich geschütztes Rechtsgut schädigen wird.[910] Es wird darauf abgestellt, ob eine Sachlage oder ein Verhalten gegeben ist, aus dem die Wahrscheinlichkeit einer Schädigung nach bewährten Erfahrungssätzen folgt, also eine objektiv gegebene Gefahr vorliegt, in Abgrenzung zu einer nur vorstellbaren, subjektiven Gefahr. Im Laufe der Zeit wurde der Gefahrenbegriff immer weiter unterteilt. Erwähnt seien die Begriffe der abstrakten und konkreten Gefahr, der Anscheins- und Putativgefahr oder der sogenannte Gefahrenverdacht. Auf einige dieser Begriffe wird sogleich näher einzugehen sein.

Der Gefahrbegriff muss von der Gefährdung abgegrenzt werden. Es wird vertreten die Gefahr als übergeordneten Begriff anzusehen, wohingegen unter einer Gefährdung eine genauer beschriebene Gefahr, die räumlich und zeitlich bestimmt ist, verstanden wird.[911]

Gefahren und Bedrohungen für die IT-Sicherheit sind somit noch relativ abstrakt und auch noch als bloße Möglichkeiten zu verstehen, während Gefährdungen schon

---

906 *BSI*, Glossar und Begriffsdefinitionen, https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/glossar/04.html.

907 *Eckert* 2006, 14.

908 *Wikipedia*, Exploit, http://de.wikipedia.org/wiki/Exploit.

909 *Pohl* 2004, 682.

910 BVerwGE 45, 51.

911 *BSI*, Glossar und Begriffsdefinitionen, https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/glossar/04.html.

konkret werden und sich real in Sicherheitslücken und Verwundbarkeiten manifestieren, die durch Exploits faktisch ausgenutzt werden können.

Am ehesten sind die Unterfälle des rechtlichen Gefahrbegriffs der konkreten und abstrakten Gefahr und des Gefahrenverdachts im IT-Sicherheitsbereich nutzbar zu machen. Inhaltliche Parallelen zwischen den eben dargestellten informatischen und den, sogleich darzustellendenen, Rechtsbegriffen drängen sich geradezu auf.

In § 2 Nr. 1 lit. a) Nds. SOG ist die konkrete Gefahr als „Sachlage, bei der im einzelnen Fall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ein Schaden für die öffentliche Sicherheit oder Ordnung eintreten wird“ legaldefiniert. Sie ist also mit der Gefährdung, die gerade räumlich und zeitlich bestimmt ist, vergleichbar.

Die konkrete Gefahr hat, wie an der Definition ersichtlich ist, ein Wahrscheinlichkeitselement inne, nämlich die hinreichende Wahrscheinlichkeit. Die Umschreibung der „Verletzung der geschützten Güter“ ist nichts anderes als der Eintritt eines Schadens. In § 2 Nr. 1 lit. a) Nds. SOG, § 3 Nr. 3 lit. a) SOG LSA und § 54 Nr. 3 lit. a) ThürOBG ist die konkrete Gefahr dementsprechend auch als „Sachlage, bei der im einzelnen Fall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ein Schaden für die öffentliche Sicherheit oder Ordnung eintreten wird“ legaldefiniert. Die konkrete Gefahr betrifft demgemäß immer einen real existierenden Einzelfall. In der Sprache der Informatik wäre dies das Bestehen einer ganz bestimmten und real ausnutzbaren Verwundbarkeit oder Sicherheitslücke.

Die abstrakte Gefahr knüpft gemäß den Legaldefinitionen in den drei obigen Polizei- und Ordnungsgesetzen an „eine nach allgemeiner Lebenserfahrung oder den Erkenntnissen fachkundiger Stellen mögliche Sachlage, die im Fall ihres Eintritts eine konkrete Gefahr darstellt“ an. Sie ist mit dem informatischen Begriff der Gefahr vergleichbar, der ebenso an eine unkonkrete Sachlage anknüpft und nur potentielle Bedrohungen betrifft.

Dementsprechend ist die Bedrohung in gewisser Weise mit dem sogenannten Gefahrenverdacht vergleichbar. Beim Gefahrenverdacht wird eine Gefahr für möglich gehalten, auch wenn subjektiv noch Zweifel vorhanden sind und objektiv der Schadenseintritt nicht hinreichend wahrscheinlich, jedoch möglich ist.[912] Beim Gefahrenverdacht liegen objektive Anhaltspunkte für eine Gefahr vor, die aber für eine endgültige Beurteilung nicht ausreichend sind.[913] Mit dem Gefahrenverdacht zusammenhängend ist die Notwendigkeit der Gefahrerforschung, die diese endgültige Beurteilung ermöglichen soll. Die Gefahrerforschung ist im IT-Kontext somit am ehesten mit einer Bedrohungsanalyse vergleichbar.

---

912 *Wikipedia*, Gefahr, http://de.wikipedia.org/wiki/Gefahr#Rechtswissenschaft.2FVerwaltung.

913 *Rechtswörterbuch*, Gefahrenverdacht, http://www.rechtswoerterbuch.de/recht/g/gefahrenverdacht.

3.1.9.8.1.3 Schadensbegriff

Der Begriff des Schadens ist inhärent juristischer Natur und hatte bereits im Römischen Recht eine zentrale Bedeutung.[914] Allerdings ist der in den Rechtswissenschaften aktuell verwendete Schadensbegriff nicht legaldefiniert, sondern folgt gemäß der herrschenden Meinung dem sogenannten „natürlichen Schadensbegriff".[915] Folgt man der Literatur, so ist ein Schaden in diesem Sinne jeder Verlust, den ein Rechtssubjekt an seinen Rechtsgütern erleidet und der im Rechtsverkehr als ersatzfähige Einbuße angesehen wird.[916] Der natürliche Schadensbegriff orientiert sich demnach am allgemeinen Sprachgebrauch, wonach ein Schaden Nachteile und Einbußen an Lebensgütern darstellt.[917] Solche Schäden an Rechts- oder Lebensgütern sind nicht nur finanzieller Art, sondern auch und gerade Beeinträchtigungen von Grundrechten oder den politischen Zielsetzungen eines demokratischen und sozialen Rechtsstaats.[918] Zentrale Vorschriften im Zusammenhang mit Schäden und der Haftungsausfüllung sind die §§ 249-254 BGB. Technische Schäden an IT-Systemen sind nur ein Teilaspekt im Sinne des allgemeinen und juristischen Schadensbegriffs. Die Nachteile und Verluste für ein Subjekt äußern sich an Rechts- oder Lebensgütern, indem IT-Systeme in ihrer Funktionsfähigkeit beeinträchtigt werden. Eine sicherheitstechnisch orientierte Definition des Schadens ist demzufolge nicht notwendig.

Neuartige Technik kann nicht nur zu neuartigen Schäden, sondern auch zu neuartigen Schadensverteilungen führen. Es wird zwischen Kumulationsschäden, Multiplikationsschäden und Kopplungsschäden unterschieden.[919]

Bei kumulierten Schäden werden die Schäden vervielfacht, weil die Technik voneinander unabhängige Handlungen ermöglicht. Hinzu kommen Multiplikationsschäden, in Form der Nutzung eines defekten oder manipulierten Systems durch eine Vielzahl von Nutzern.[920] Gerade die Vielzahl von Nutzern und die standardisierte und homogene Bereitstellung von Clouddiensten lässt diese beiden Schadensklassifikationen bei Cloud Computing besonders akut werden. Unterschiedliche Angreifer können voneinander unabhängige Angriffe auf unterschiedliche Nutzer ausführen, so dass sich die Angriffe kumulieren. Alternativ können sie die Provider-

---

914 Beispielsweise bereits 450 v. Chr. Die TABVLA VIII der sogenannten „Zwölftafelgesetze" (http://de.wikipedia.org/wiki/Zw%C3%B6lftafelgesetz) oder auch das erheblich ältere Talionsprinzip („Auge um Auge"), das den Ausgleich von Schäden zum Inhalt hatte.

915 *Fischer* 1903, 1 ff.; *Lange/Schiemann* 2003, § 1 I, 26 ff.; *Oetker*, in: Münchner Kommentar zum BGB, Band 2, § 249, Rn. 17; *Schubert*, in: Bamberger/Roth, BeckOK, Edition 18, § 249, Rn. 9.

916 *Schubert*, in: Bamberger/Roth, BeckOK, Edition 18, § 249, Rn. 9.

917 *Schulze*, in: Schulze, Handkommentar zum BGB, Vorbemerkung zu §§ 249-253, Rn. 5.

918 So zum Beispiel *Roßnagel/Wedde/Hammer/Pordesch* 1990, 7.

919 *Roßnagel/Wedde/Hammer/Pordesch* 1990, 73 f.

920 *Roßnagel/Wedde/Hammer/Pordesch* 1990, 73.

infrastruktur angreifen und die einheitlich bereitgestellten Dienste, meist Software, manipulieren, so dass sich die Schäden bei den Nutzern multiplizieren.

Die Vernetzung und Virtualisierung führt zudem zur dritten Art der Schadensverteilung, nämlich den Kopplungsschäden. Diese treten zum gleichen Zeitpunkt auf.[921] In Cloudsystemen treten diese Schäden auch gehäuft auf, weil Cloudsysteme wegen der Vernetzung aller Beteiligten eng gekoppelt sind. Eine noch engere und vergleichsweise neue Form der Kopplung erfolgt durch die virtualisierte Bereitstellung auf wenigen physischen Systemen und die Abhängigkeit einer Vielzahl von Nutzern von der Funktionsfähigkeit dieser physischen Basissysteme. Der Ausfall eines Servers hat den gleichzeitigen Ausfall für eine Vielzahl von Nutzern zur Folge.

Weitere wichtige Begriffe im Zusammenhang mit Schäden sind die Schadenswahrscheinlichkeit und das Schadenspotential. Die Schadenswahrscheinlichkeit, auch als Eintrittswahrscheinlichkeit bezeichnet, beschreibt die vorab geschätzte oder berechnete Wahrscheinlichkeit des Eintritts eines zukünftigen Schadens. Demgegenüber ist das Schadenspotential die Größe oder Höhe eines möglichen, aber (noch) nicht realisierten, Schadens.[922] Es entspricht dem potentiellen Maximalschaden für ein Rechtsgut bei Eintritt eines künftigen Ereignisses und stellt eine Prognose über das mögliche Schadensausmaß dar. Das Schadenspotential wird, wie die Schadenswahrscheinlichkeit, unter Zugrundelegung der zum Zeitpunkt der Beurteilung bekannten Umstände geschätzt oder berechnet. Das Schadensausmaß beschreibt die tatsächliche Schwere eines Schadens und wird dementsprechend auch als Schadensschwere bezeichnet. Das Schadensausmaß ergibt sich aus einer Ex-post-Betrachtung, während das Schadenspotential vor Eintritt des schädigenden Ereignisses geschätzt oder berechnet wird. Das tatsächliche Schadensausmaß kann vom Schadenspotential nach oben oder nach unten abweichen.

Im Zusammenhang mit der Schadenswahrscheinlichkeit und dem Schadenspotential sind auch der Schadeneintritt, die Schadensverhinderung und die Schadensminimierung zu erwähnen. Der Eintritt eines Schadens hängt, wie eben erwähnt, von der Schadenswahrscheinlichkeit ab, während die potentielle Höhe oder Größe eines Schadens durch das Schadenspotential beschrieben wird. Um einen Schaden an sich zu verhindern, ist es notwendig, auf die Wahrscheinlichkeit des Eintritts eines schädigenden Ereignisses einzuwirken. In der Regel ist eine hierfür notwendige Steuerung oder Antizipierung von schädigenden Ereignissen jedoch entweder gar nicht oder nur mit unverhältnismäßigem Aufwand in Relation zur drohenden Schadenshöhe möglich. Um die negativen Auswirkungen von Schäden zu minimieren, ist es deswegen einfacher, das Schadenspotential zu reduzieren.[923]

---

921 *Roßnagel/Wedde/Hammer/Pordesch* 1990, 74.

922 *Roßnagel/Wedde/Hammer/Pordesch* 1990, 8.

923 *Roßnagel/Wedde/Hammer/Pordesch* 1990, 71 ff.; *Hammer* 1999, 112 ff.

Im Szenario des Cloud Computing geht es um potentielle Schäden an Rechtsgütern, beispielsweise an der informationellen Selbstbestimmung. Im Cloudszenario ist regelmäßig unklar, wie hoch die Wahrscheinlichkeit des Abhandenkommens oder der unbefugten Kenntnisnahme von Daten ist. Diese hängt vom Vernetzungsgrad, der Komplexität der genutzten Cloud, Zugriffsbefugnissen der Mitarbeiter, Wartungsintervallen, Anzahl der genutzten Subunternehmen, potentiellen und tatsächlichen Angriffsversuchen, Naturereignissen und einer nahezu unendlichen Vielzahl von weiteren Einflüssen und Variablen ab. Im Gegensatz dazu ist das Schadenspotential eingrenzbar. Dieses hängt von der Wichtigkeit der Daten ab. Dabei spielt auch das Prinzip der Datenvermeidung eine wichtige Rolle. Aus nicht erhobenen Daten können nämlich auch keine Schäden, zum Beispiel für die informationelle Selbstbestimmung, erwachsen, so dass der Verzicht auf die Erhebung von Daten das Schadenspotential auf Null reduziert.

Um zum Beispiel des Cloud Computing zurückzukehren, bedeutet dies, nicht nur alle möglichen Sicherheitsmaßnahmen umzusetzen, sondern vor allem gewisse Daten erst gar nicht auszulagern oder überhaupt nicht zu erheben. Weil aber in der Praxis regelmäßig bereits erhobene Daten betroffen sind, geht es nur noch um die Frage, ob sie ausgelagert werden sollen oder nicht.

Zusammengefasst ist also festzuhalten, dass die Wichtigkeit der auszulagernden Daten, also das Schadenspotential, vor einer Auslagerung berücksichtigt werden muss. Eine solche Betrachtung und Bewertung kann dazu führen, dass eine Auslagerung von Daten unterbleiben muss. Werden Daten trotz eines absehbar hohen Schadenspotentials dennoch ausgelagert, gewinnt die Schadenseintrittswahrscheinlichkeit erst in einem zweiten Schritt an Bedeutung. Dann ist es angebracht, diese durch entsprechende Maßnahmen so gering wie möglich zu halten. Dabei ist auch auf das Verhältnis zwischen dem Aufwand und den Kosten der durchzuführenden Maßnahmen und der tatsächlich erreichten Reduktion zu achten.

3.1.9.8.1.4 Risiko und Risikovorsorge

Der Risikobegriff wird sowohl in der Alltagssprache als auch in der Wissenschaft verwendet. Noch weitergehender als der Gefahrbegriff, ist der Risikobegriff in der Wissenschaft von der ihn verwendenden Disziplin abhängig. Die jeweiligen Risikobegriffe sind vom jeweiligen wissenschaftlichen Hintergrund geprägt und nicht immer miteinander kompatibel und vergleichbar.[924]

In der Mathematik ist Risiko das Produkt aus der Eintrittswahrscheinlichkeit und dem Ausmaß eines negativen Ereignisses.[925] Für die hier zu betrachtenden Risiken hat die Definition insoweit Bedeutung, als die technischen Wissenschaften, also

---

[924] *Jonen*, in: Lingnau, Beiträge zur Controlling-Forschung 2006, 7; *Hammer*, DuD 2000, 167.

[925] *Muschick/Müller* 1987, 108; *Roßnagel*, UPR 1986, 46; *Jonen*, in: Lingnau, Beiträge zur Controlling-Forschung 2006, 9.

auch die Informatik, dieser mathematischen Formel der Risikobeschreibung folgen.[926] Das „Ausmaß eines negativen Ereignisses“ ist mit dem obigen Begriff des „Schadenspotentials“ gleichzusetzen.

Zwar wird in diversen Gesetzen, zum Beispiel im Gentechnikgesetz oder dem Aktiengesetz der Risikobegriff erwähnt und ist damit den Rechtswissenschaften nicht unbekannt, allerdings stützen sich diese auch auf den mathematisch-technischen Risikobegriff. In den Gesetzen geht es, wie schon an Gesetzesnamen ersichtlich, auch hauptsächlich um die gesetzliche Regelung von technisch bedingten Risiken. Recht kann nämlich technische Risiken nicht völlig verbieten, sondern diese nur steuern und lediglich festlegen unter welchen Umständen sich ein zulässiges Risiko verwirklichen darf. Absolute Sicherheit – und damit völlige Risikofreiheit – ist im Zusammenhang mit Technik unmöglich. Recht kann technische Risiken nur begrenzen.[927]

Die Regelung von technischen Risiken und der damit verbundene Schutz von Rechtsgütern ist im Übrigen auch verfassungsrechtlich, beispielsweise in Art. 2 Abs. 1 Satz 1 GG, und durch die Rechtsprechung des Bundesverfassungsgerichts untermauert.[928] Letzteres hat sich beispielsweise 1978 in der Kalkarentscheidung ausführlich mit dem Begriff und Inhalt des Restrisikos von Atomkraft befasst.[929] Maßstab für ein verbleibendes Restrisiko ist dabei der „Stand der Wissenschaft“.[930] Auch in der europäischen Rechtsprechung ist der Risikobegriff Gegenstand von Entscheidungen geworden. So vertritt das Europäische Gericht erster Instanz (EuG) einen weiten Risikobegriff. Es sieht als Risiko jede „nachteilige Wirkung für ein Rechtsgut“ und spricht auch von einer „Funktion der Wahrscheinlichkeit“.[931]

Letztlich sind die diversen Risikobegriffe aber nicht nur disziplin-, sondern auch kontextabhängig und an dem jeweiligen Zweck orientiert zu verstehen.[932] Für die weiteren Betrachtungen ist aber alleinig der mathematisch-technische Risikobegriff heranzuziehen.

---

926 Vergleiche beispielsweise DIN EN 1050, DIN IEC 62198 und die zurückgezogene DIN VDE 31000; *Jonen*, in: Lingnau, Beiträge zur Controlling-Forschung 2006, 9.

927 *Roßnagel*, UPR 1986, 46, 47.

928 Siehe beispielsweise BVerfGE 39, 41, BVerfGE 46, 164 oder BVerfGE 53, 57.

929 Zu den Einzelheiten siehe BVerfGE 49, 89, insbesondere BVerfGE 49, 140 ff.

930 BVerfGE 49, 89 ff.; zu den unbestimmten Rechtsbegriffen „Stand der Wissenschaft“, „Stand der Technik“ oder „Stand von Wissenschaft und Technik“ und deren Bedeutung für Normanwender siehe *Roßnagel*, UPR 1986, 48 f.; zu Unsicherheiten bei der wissenschaftlichen Beurteilung siehe *Roßnagel/Neuser* UPR 1993, 401 ff.

931 EuG, Slg. 2002, II-3305, Rn. 147 (Pfizer Animal Health); *Scherer/Heselhaus*, in: Dauses, EU-Wirtschaftsrecht, Teil O (Umweltrecht), Rn 38.

932 *Renn/Zwick* 1997, 89; *Jonen*, in: Lingnau, Beiträge zur Controlling-Forschung 2006, 53.

Zielsetzung der rechtlichen Befassung mit Risiken ist die Risikovorsorge. Diese zielt darauf ab, technische Risiken zu vermindern.[933] Das Risikovorsorgeprinzip,[934] das insbesondere im Umwelt- und Gemeinschaftsrecht (bei Letzterem in Form von Produktsicherheitsrecht und Verbraucherschutzrecht) Bedeutung hat, kann auch in der IT-Sicherheitsforschung angewendet werden. Ein Beispiel dafür ist die Anwendung der KORA-Methode. Vorlaufende Technikgestaltung, insbesondere im IT-Sicherheitsbereich, folgt damit zum Teil den umweltrechtlich begründeten Grundsätzen der Vorbeugung und Vorsorge.[935]

Eine Berufung auf das Vorsorgeprinzip ist dann möglich, wenn potentielle Gefahren durch eine objektive wissenschaftliche Bewertung ermittelt wurden, sich das Risiko aber nicht mit hinreichender Sicherheit bestimmen lässt. Das Prinzip kommt folglich dann zur Anwendung, wenn noch Unsicherheit besteht oder keine umfassenden wissenschaftlichen Informationen über das potentielle Risiko vorliegen.[936] Vorsorge ist demzufolge zukunftsbezogen und betrifft Maßnahmen, die zeitlich vor der Gefahrentstehung zu treffen sind.[937] Diese Vorsorgemaßnahmen stellen Antworten auf die Risiken der Unkenntnis und der Unbekanntheit von künftigen Schadensereignissen dar.[938] Risikovorsorge ist damit Schadensvorsorge, wie sie umweltrechtlich beispielsweise in § 7 Abs. 2 Nr. 3 AtomG und § 5 Abs. 1 Nr. 2 BImSchG zum Ausdruck kommt.

Übertragen auf die IT-Sicherheitsforschung bedeutet dies, dass es sich um neuartige Informationstechnologie handeln muss, von der Risiken ausgehen, die noch nicht bestimmbar sind. Da sich das Vorsorgeprinzip in der Regel auf eminent wichtige Rechtsgüter, wie beispielsweise Leben oder körperliche Unversehrtheit, bezieht, muss der betroffenen Informationstechnologie eine ähnlich hervorgehobene Bedeutung zukommen. Als Beispiel seien kritische Infrastrukturen erwähnt.[939]

Im Kontext Cloud Computing ist also, abhängig vom Einzelfall und der Wichtigkeit der Daten, von einer Auslagerung abzusehen, wenn damit noch nicht absehbare Risiken für Rechtsgüter bestehen. Für solche „Restrisiken“, die nicht wissenschaftlich abschätzbar sind, gebietet das Vorsorgeprinzip, etwas Bestimmtes zu tun oder zu

---

933 *Roßnagel*, UPR 1986, 46.

934 Vergleiche dazu auch die Erwähnung als „Grundsätze der Vorbeugung und Vorsorge“ in Art. 191 Abs. 2 Satz 2 AEUV.

935 Siehe dazu ausführlich *Roßnagel*, in: Koch/Pache/Scheuing 2011, GK-BImSchG, § 5, Rn. 415 ff.

936 *EU-Kommission*, Mitteilung vom 2.2.2000 zur Anwendbarkeit des Vorsorgeprinzips, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=de&type_doc=COMfinal&an_doc=2000&nu_doc=1.

937 *Roßnagel*, in: Koch/Pache/Scheuing, GK-BImSchG 2011, § 5, Rn. 423.

938 *Roßnagel*, in: Koch/Pache/Scheuing, GK-BImSchG 2011, § 5, Rn. 449.

939 Zu kritischen Infrastrukturen siehe auch Kap. 3.2.1.

unterlassen. Die EU-Kommission formuliert dies entsprechend so, dass „das Vorsorgeprinzip zu einer Entscheidung für oder gegen ein Tätigwerden führen muss“.[940] Dies führt dazu, dass bei der Frage, ob Daten ausgelagert werden, nicht nur das einzelne Datum oder jeder einzelne Vorgang betrachtet werden muss, sondern manchmal auch die Gesamtheit der Daten, wenn die Kombination einzelner „harmloser“ Daten einen übergeordneten Informationsgehalt entwickelt, der Rechtsgüter des Betroffenen, namentlich die informationelle Selbstbestimmung, beeinträchtigen kann. Ein Beispiel im Cloudkontext wäre die Erstellung von Profilen anhand einzelner ausgelagerter, für sich genommen harmloser, Datensätze. Auch aus der Zusammenführung von einzelnen Nutzungshandlungen in Nutzungsprotokollen kann ein Profil erstellt werden.

3.1.9.8.2 Bedrohungsklassifizierungen

Im Folgenden sollen die Vielzahl der IT-spezifischen Bedrohungen einer ersten Systematisierung und Klassifizierung zugeführt werden und bereits einige typische Bedrohungen in Grundzügen dargestellt werden.

In der IT-Sicherheitsforschung wird üblicherweise zwischen unbeabsichtigten und beabsichtigten Eingriffen unterschieden, wobei letztere Eingriffe auch als Angriffe bezeichnet werden.

3.1.9.8.2.1 Unbeabsichtigte Eingriffe

Zu den unbeabsichtigten Eingriffen gehören die höhere Gewalt, technisches Versagen und menschliche Fehlhandlungen. Der Schutz vor solchen unbeabsichtigten Eingriffen wird im englischen Sprachraum mit „Safety“ bezeichnet.[941]

Als höhere Gewalt bezeichnet die Rechtsprechung ein von außen kommendes, nicht voraussehbares und auch durch äußerste vernünftigerweise zu erwartende Sorgfalt nicht abwendbares Ereignis.[942] Beispiele sind Naturkatastrophen jedweder Art, insbesondere Unwetter (Sturm, Blitzschlag[943], Starkregen, etc.), Erdbeben, Überschwemmungen, Vulkanausbrüche, aber auch Brände, Verkehrsunfälle oder Kriege. Als höhere Gewalt gelten auch der Ausfall von Weitverkehrsnetzen (für Dienste

---

940 Mitteilung der EU-Kommission vom 2.2.2000 zur Anwendbarkeit des Vorsorgeprinzips (KOM 2000/1).

941 *Christmann/Hilpert/Thöne/Hagenhoff*, HMD – Praxis der Wirtschaftsinformatik, Heft 275, 2010, 63; *Witt* 2006, 66 ff.; im Englischen wird in Abgrenzung zum Begriff „Safety“ der Schutz vor beabsichtigten Angriffen als „Security“ bezeichnet.

942 BGHZ 100, 157.

943 Dass Blitzeinschlag auch für Cloud Computing erhebliche Auswirkungen haben kann, zeigte sich im August 2011 als ein Blitz in der Nähe eines Rechenzentrums in Irland einschlug und zu Teilausfällen von Amazons und Microsofts Cloudangeboten führte; siehe dazu *Ihlenfeld*, Blitzeinschlag macht Amazon und Microsoft Probleme, http://www.golem.de/1108/85549.html und *Kirsch*, Blitz stört Amazons und Microsofts Cloud in Irland, http://www.heise.de/newsticker/meldung/Blitz-stoert-Amazons-und-Microsofts-Cloud-in-Irland-1319332.html.

besonders relevant, wenn die Netzinfrastruktur nicht mehr funktioniert), der Personalausfall, unzulässige Temperaturen und Luftfeuchten, Staub und Verschmutzung, Datenverluste durch starkes Licht bei optischen Datenträgern oder starke Magnetfelder, die zur Zerstörung der Datenstruktur auf magnetischen Datenträgern führen.[944]

In Abgrenzung zur höheren Gewalt ist das technische Versagen in gewissem Rahmen vorhersehbar, weil technikimmanent und unter Beachtung der üblichen Sorgfalt, zum Beispiel durch Austausch anfälliger oder veralteter Komponenten, eingeschränkt beherrschbar. Hauptversagensgrund ist der Ausfall von Hardware und damit verbundene Datenverluste durch Defekte, Alterung, Stromausfall oder Spannungsschwankungen. Zum technischen Versagen gehören aber auch unsichere oder im Laufe der Zeit unsicher gewordene kryptographische Algorithmen und deren Implementierung. Letztere werden zum Beispiel durch die stetige Steigerung der Rechenleistung von Prozessoren oder durch neue Kryptoanalysemethoden unsicher, weil sie in vertretbarer Zeit gebrochen werden können. Einen weiteren Fall technischen Versagens stellt die unkontrollierte Ausbreitung von Funkwellen dar. Dies ist dann der Fall, wenn auch außerhalb der eigentlichen Nutzreichweite des Funknetzes Daten empfangen und abgehört werden können. Ebenfalls als technisches Versagen einzuordnen ist der Fall, wenn es in Kommunikationsnetzen zu fehlerhaften Datenübertragungen aufgrund von Fehlschaltungen durch Hardwarekomponenten oder zum Übersprechen von Leitungen kommt.[945]

Menschliche Fehlhandlungen sind vielfältig. Zahlenmäßig am weitesten verbreitete Fehlhandlung dürfte die Fehlbedienung von technischen Systemen und Komponenten sein. Zu den Fehlhandlungen gehören aber auch unbeabsichtigte Schädigungen und Verluste von Hardware oder Daten, die Fehlinterpretation von Ereignissen oder die Sorglosigkeit im Umgang mit Informationen. Die Nichtbeachtung von notwendigen Sicherheitsmaßnahmen fällt ebenso darunter wie die ungeeignete Konfiguration eines Risikomanagementsystems. Auch Fehleinschätzungen in rechtlicher Hinsicht können Auswirkungen auf die IT-Sicherheit haben.[946]

3.1.9.8.2.2 Beabsichtigte Eingriffe

Ein weiteres Ziel der IT-Sicherheitsforschung ist die Abwehr von beabsichtigten Angriffen in Form von vorsätzlichen Handlungen. Unter einem Angriff versteht man einen nicht autorisierten Zugriff oder Zugriffsversuch auf ein IT-System[947] oder die unmittelbare oder mittelbare Störung desselben. Absicht ist, vergleichbar

---

944 *BSI*, G 1 Höhere Gewalt, http://www.bsi.de/gshb/deutsch/g/g01.htm.

945 BSI, G 4 Technisches Versagen, http://www.bsi.de/gshb/deutsch/g/g04.htm mit vielen weiteren, teils sehr konkreten, Beispielen.

946 *BSI*, G 3 Menschliche Fehlhandlungen, http://www.bsi.de/gshb/deutsch/g/g03.htm mit weiteren Beispielen.

947 *Eckert* 2006, 16.

zum dolus directus ersten Grades im Strafrecht, dann gegeben, wenn der Angreifer von seiner fehlenden Autorisierung oder Berechtigung weiß und die Angriffsdurchführung auf das Zielsystem will. Hinsichtlich möglicher Schäden oder Folgeschäden ist dolus eventualis, also die Erkenntnis eines potentiellen Schadens und das Sich-damit-Abfinden, ausreichend. Die Abwehr ist erfolgreich, wenn der Zugriffs- oder Störungsversuch scheitert und dieser Versuch seinerseits keine Auswirkungen auf das IT-System hatte.

Die Unterscheidung zwischen Zugriffsversuch und bloßer Störung eines Systems ist nicht immer eindeutig. So kann beispielsweise eine herbeigeführte Überlastung eines IT-Systems sowohl ein Zugriffsversuch, als auch eine gezielte Störung sein. In der ersten Alternative versucht der Angreifer beispielsweise durch einen Brute-Force-Angriff[948] Zugriff auf das System zu erlangen, wodurch dieses wegen der Verarbeitung der Anfragen für Berechtigte unbenutzbar wird, während in der zweiten Alternative die Störung das Hauptziel des Angriffs ist, zum Beispiel durch eine DDoS-Attacke, die gerade nicht die Erlangung des Zugriffs zum Ziel hat. Eine solche Störung ist auch mittelbar möglich, indem nicht das Zielsystem, sondern ein vorgeschaltetes oder nachgeschaltetes System gestört wird, so dass das eigentliche Zielsystem nicht mehr seine Aufgabe erfüllen kann.

Ein cloudspezifisches Beispiel für diese zweite Alternative wäre die Störung der administrativen Rechner (Management Interfaces), wodurch mittelbar auch die Produktivsysteme in Mitleidenschaft gezogen werden. Allerdings können auch Brute-Force-Angriffe auf die Management Interfaces mit dem Ziel der Zugriffserlangung deren Benutzbarkeit unmöglich machen, so dass unter Umständen und zeitlich versetzt die gleichen Folgewirkungen, nämlich nicht mehr verfügbare Produktivsysteme, entstehen.

3.1.9.8.3 Komplexität und IT-Sicherheit

Komplexität kann die Sicherheit von Systemen negativ beeinflussen. Komplexe Systeme sind dabei von sogenannten „linearen Systemen“ abzugrenzen. Erstere zeichnen sich dadurch aus, dass Subsysteme Mehrfachfunktionen übernehmen und räumlich nah beieinander angesiedelt sind, während den linearen Systemen diese Mehrfachfunktionen und die damit verbundene enge Nachbarschaft fehlen. Bei linearen Systemen haben Ausfälle von Teilkomponenten folglich nur geringe Auswirkungen auf das Gesamtsystem, weil die wechselseitigen Abhängigkeiten und Wechselwirkungen der Komponenten viel geringer sind.[949]

---

948 „Brute Force“ bedeutet übersetzt „rohe Gewalt“; bei dieser Methode werden alle möglichen Kombinationen durchprobiert, zum Beispiel komplette Wörterbücher bei Passwörtern, bis die richtige Kombination gefunden ist.

949 *Perrow* 1987, 125 ff.

Bei den Abhängigkeiten und der Verbindung von Komponenten und Systemen spielt auch die Kopplung eine Rolle. Es wird zwischen enger und loser Kopplung unterschieden. Enge Kopplung bedeutet, dass es zwischen zwei verbundenen Teilen kein Spiel, keine Pufferzone oder Elastizität gibt, so dass sich Vorgänge des einen Teils unmittelbar auf den anderen Teil auswirken.[950]

Weitere Aspekte komplexer (IT-)Systeme sind, neben den bereits angesprochenen Wechselwirkungen (Relationen zwischen den Elementen), zudem die Heterogenität (Unterschiedlichkeit der Elemente) und die Größe (Anzahl der Elemente) eines Systems.[951]

Für die Sicherheit eines IT-Systems sind alle diese Aspekte relevant. Für die weiteren Betrachtungen der IT-Sicherheit von Cloud Computing ist es angebracht, diese Merkmale speziell in diesen Kontext zu stellen.

Als erstes fällt auf, dass Clouds große Systeme sind, die sich aus einer Vielzahl von Elementen in Form von Rechenzentren, Servern, Routern, Leitungen, bis hin zu den einzelnen Komponenten dieser Einzelsysteme, zusammensetzen. Dabei erkennt man sowohl enge Kopplungen, in Form von Rechenzentren, Teilkomponenten und Virtualisierung, als auch lose Kopplungen durch die Verbindungen über das Internet. Letztere vermindern allerdings nicht die Komplexität, trotz einer nur losen Kopplung, sondern erhöhen diese für das Gesamtsystem „Cloud“, da durch die Vernetzung neue und weitere Wechselwirkungen entstehen. Angriffe auf ein Teilsystem können durch die Vernetzung die Sicherheit des Gesamtsystems beeinträchtigen.

Ähnliches gilt für die mit der Mehrmandantenfähigkeit einhergehende Virtualisierung. Hierbei wird die enge Kopplung besonders deutlich. Angriffe auf den physischen Server haben unmittelbare Auswirkungen auf die virtuellen Systeme, beispielsweise wenn der Server ausfällt. Aber auch unzureichend abgesicherte Hypervisoren führen zu einer engen Kopplung, so dass Vorgänge in einer virtuellen Maschine direkte Auswirkungen auf weitere Maschinen haben.

Bei vernetzten IT-Systemen ist zudem der mit der Linearität einhergehende Gesichtspunkt der engen Nachbarschaft zwischen Systemen eher vernachlässigbar. Dieser gewinnt nur bei physischen Angriffen gegen die Infrastruktur oder bei höherer Gewalt Bedeutung. Allerdings sind die Aspekte der Heterogenität und Homogenität für die IT-Sicherheit umso relevanter. Während Heterogenität für Komplexität spricht, ist Homogenität das Gegenteil dazu. Unter Sicherheitsaspekten ist diese Sichtweise jedoch zu differenzieren. Homogene Systeme, die die Komplexität reduzieren, können andererseits Angriffe oder Fehler erleichtern. Gleichartige Systeme sind einfacher überwindbar, da eine gefundene Sicherheitslücke mehrfach ausgenutzt werden kann. Analog dazu äußern sich Fehler mehrfach, so dass sich deren

---

950 *Perrow* 1987, 131.

951 *Meinhold*, IT-Komplexität, http://www.guenther-meinhold.de/html/it-komplexitat.html.

Wirkung multipliziert.[952] Vor allem Rechenzentren sind eine Anhäufung von gleichartigen Servern und Komponenten. Auch die Bereitstellung homogener Dienste in Clouds ist der Reduzierung der Komplexität geschuldet.[953]

Es fällt also auf, dass die Reduzierung der Komplexität mit dem Ziel, Wechselwirkungen und damit einhergehende Fehler zu verringern, demgegenüber gezielte Angriffe erleichtert, da die Angriffswirkungen unmittelbarer und stärker zum Tragen kommen. Die eigentlich unerwünschte Komplexität von Systemen kann sich demnach auch als Sicherheitsvorteil äußern. In komplexen Systemen muss sich ein (vor allem externer[954]) Angreifer zunächst zurechtfinden und die ausnutzbaren Wechselwirkungen ausloten, um das Angriffsziel auszumachen und die Angriffswirkung zu maximieren. Je spezieller die Zielsetzung eines Angriffs, umso hinderlicher ist die Komplexität für die Durchführung des Angriffs und die Erreichung der Zielsetzung. Cloud Computing mit seinen Intransparenzen erschwert folglich auch gezielte Angriffe, beispielsweise auf ein ganz bestimmtes virtualisiertes Mandantensystem und die darin enthaltenen Daten.[955]

Unter Umständen wird ein gezielter Angriff in komplexen Systemen faktisch technisch unmöglich oder zu teuer, weil der notwendige finanzielle und tatsächliche Aufwand in keiner Relation zum erwarteten Ergebnis steht.[956] Andererseits erhöht ein komplexes System aber auch die Ansatzpunkte für Angriffe. Neben der erwähnten Anzahl der Elemente können die gehäuften Wechselwirkungen Fehler verursachen, die zu unbekannten Sicherheitslücken und einer allgemeinen Häufung derselben führen. Diese können dann wiederum gezielte Angriffe befördern.

Der Einfluss der Komplexität auf ungezielte und breit gestreute Angriffe, wie zum Beispiel DDoS-Attacken, ist ebenfalls nicht eindeutig als positiv oder negativ beantwortbar. Einerseits können die Wechselwirkungen in komplexen Systemen den Verfügbarkeitsausfall beschleunigen, andererseits kann die Komplexität dazu genutzt werden, um solche Angriffe ins Leere laufen zu lassen, indem weitere Ressourcen hinzugefügt werden, so dass die Verfügbarkeit des Gesamtsystems dennoch

---

952 Siehe dazu auch Kap. 3.1.9.8.1.3.

953 Diese ist allerdings durch Kosteneinspareffekte motiviert.

954 Siehe dazu sogleich Kap. 3.1.9.8.4.

955 Siehe dazu auch das Beispiel der sogenannten Exfiltration-Angriffe in Kap. 3.1.9.10.1.2.

956 Ein praktisches Beispiel für hohe Komplexität und den erheblichen Aufwand, um die gewünschten Wirkungen zu erzielen, war der Angriff mit der Stuxnet-Malware auf Atomanlagen im Iran; siehe dazu *Rieger*, Der digitale Erstschlag ist erfolgt, http://www.faz.net/s/RubCEB3712D41B64C3094E31BDC1446D18E/Doc~E8A0D43832567452FBDEE07AF579E893C~ATpl~Ecommon~Scontent.html; *Falliere/Murchu/Chien*, W32.Stuxnet Dossier, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf; *Pluta*, Fünf Ziele und 12.000 Infektionen, http://www.golem.de/1102/81402.html.

gewährleistet ist. Durch das Hinzufügen zusätzlicher Ressourcen wird die Komplexität paradoxerweise sogar noch weiter gesteigert.

Gerade diese Erwägungen zur Ambivalenz der Komplexität zeigen, dass es einhundertprozentige Sicherheit in IT-Systemen niemals geben kann. Sicherheit ist nicht nur von der Gestaltung und Funktion des Systems, sondern auch von der Motivation und der Art der Angreifer abhängig. Diese unterschiedlichen Arten von Angreifertypen sollen im Folgenden dargestellt werden.

3.1.9.8.4 Angreifertypen

Im Zusammenhang mit Angriffen lassen sich zunächst zwei Arten von Tätern unterscheiden, nämlich interne und externe Täter. Interne Täter werden auch als Berechtigte oder Insider bezeichnet. Sie können meist größere Schäden anrichten als Externe. Sie kennen die Infrastruktur und deren Schwachstellen und wissen, wo sie für einen erfolgreichen Angriff ansetzen müssen. Komplexität ist für Insider folglich kein Hinderungsgrund, einen gezielten Angriff durchzuführen. Zudem können sie den richtigen Zeitpunkt für den Angriff abwarten und dadurch ihre Entdeckung erschweren oder den Schaden erhöhen.[957]

Externe Täter, auch als Dritte oder Outsider umschrieben, sind Personen, die organisatorisch (und meist auch räumlich) außerhalb des Unternehmens oder der Organisation stehen. Sie haben meist keinen unmittelbaren Zugang zu den IT-Systemen und verfügen nicht über das gleiche Wissen über die Systeme wie Insider. Um diesen Wissensmangel zu kompensieren, können externe Angreifer Insider erpressen oder durch Social Engineering für sich ausnutzen.[958]

Bezüglich der Unterscheidung zwischen internen und externen Tätern fällt auf, dass in den Medien suggeriert wird, dass überwiegend externe Täter, in diesem Zusammenhang meist als Hacker oder Cracker bezeichnet, die Daten- und Systemsicherheit bedrohen und dadurch Schäden verursachen. Tatsächlich sind in der Praxis allerdings interne Täter, nämlich Administratoren oder sonstiges Personal, für den Großteil der Schäden verantwortlich.[959] Dies hängt mit dem erwähnten Insiderwissen und den besseren Ansatzpunkten für erfolgreiche Angriffe zusammen. Die Häufigkeit interner Angriffe ist aber vergleichsweise gering. So gibt es Studien, die nur von zwei Prozent der Angriffe durch Insider ausgehen.[960]

---

957 *Roßnagel/Wedde/Hammer/Pordesch* 1990, 146.

958 *Roßnagel/Wedde/Hammer/Pordesch* 1990, 154.

959 *Holznagel* 2003, 26; *Eckert* 2006, 16; *PC-Welt*, Eigene Mitarbeiter bleiben größtes Sicherheitsrisiko, http://www.pcwelt.de/start/sicherheit/sicherheitsluecken/news/2343708/eigene-mitarbeiter-bleiben-groesstes-sicherheitsrisiko; siehe auch Kap. 3.1.9.3 und Fn. 731 und 732.

960 *Bachfeld*, Studie bestätigt das Ende der Legende vom internen Angreifer, http://www.heise.de/security/meldung/Studie-bestaetigt-das-Ende-der-Legende-vom-internen-Angreifer-914773.html; *7Safe*, UK Security Breach Investigations Report, http://www.7safe.com/breach_report/Breach_report_2010.pdf.

Bei den durch Insider verursachten Schadensarten kann zwischen destruktiven Verhaltensweisen und gezieltem Abgreifen von Daten und Geschäftsgeheimnissen unterschieden werden. Während erstere eher auf Frustration oder Langeweile der Beschäftigten zurückzuführen sind und oft nur geringe Schäden verursachen, kann die Veräußerung von Betriebsgeheimnissen durch (ehemalige) Mitarbeiter zur Insolvenz eines Unternehmens führen. Umfragen zeigen, dass 60 Prozent der Mitarbeiter beim Verlassen des ehemaligen Arbeitgebers Daten unberechtigt mitnehmen.[961] Diese erhoffen sich von der Entwendung der Daten einen Vorteil bei der Arbeitssuche oder nutzen das entwendete Know-how als Selbständige. Auch Rache kann ein Motiv sein, so dass Daten an Konkurrenten weitergeben oder verkauft werden.[962]

3.1.9.8.5 Angriffsarten

Angriffe sind sowohl passiv, zum Beispiel durch Mithören, Mitlesen oder die Analyse des Kommunikationsverhaltens, als auch aktiv, beispielsweise durch die Manipulation von Daten oder die Zusendung von Malware, möglich.[963]

3.1.9.8.5.1 Passive Angriffe

Passive Angriffe bedrohen die Vertraulichkeit der Kommunikation, beeinflussen aber nicht die Kommunikation oder den Nachrichteninhalt an sich. Sie zielen ausschließlich auf die (unerlaubte) Informationsbeschaffung ab.[964] Über einen passiven Angriff kann ein Angreifer weitere Ansatzpunkte, zum Beispiel Passwörter, für einen späteren aktiven Angriff erlangen. Das Problem bei internetbasierten und auf Cloud Computing abzielenden passiven Angriffen besteht darin, dass ein Abhören der Kommunikation aufgrund der offenen Struktur des Internets sehr leicht möglich ist. Um passive Angriffe effektiv abzuwehren, muss daher die Kommunikation anonymisiert, verschlüsselt oder versteckt erfolgen.[965]

Ein klassisches Beispiel für einen passiven Angriff ist das sogenannte „Packet-Sniffing“.[966] Der englische Ausdruck „Packet“ steht für ein im Netzwerk verschicktes Datenpaket.[967] „Sniffing“ bedeutet übersetzt „(Aus)schnüffeln“. Bekannte Packet-Sniffer (auch als „Packet Analyzer“ oder „Network Analyzer“ bezeichnet) sind beispielsweise WireShark[968] (ehemals Ethereal) oder Tcpdump.[969] Die Programme

---

961 *Bube*, Nach der Kündigung: 60 Prozent nehmen Daten mit, http://www.crn.de/panorama/artikel-35535.html.

962 *Bube*, Nach der Kündigung: 60 Prozent nehmen Daten mit, http://www.crn.de/panorama/artikel-35535.html.

963 *Witt*, 2006, 68; Einzelheiten zu den Beispielen siehe sogleich.

964 *ITWissen.info*, Angriff, http://www.itwissen.info/definition/lexikon/Angriff-attack.html.

965 *Holznagel* 2003, 25.

966 *Holznagel* 2003, 25; *Eckert* 2006, 16.

967 Siehe dazu auch Kap. 3.8.1.1.1.

968 http://www.wireshark.org.

dienen eigentlich der Netzwerkanalyse und Netzwerkwartung, können aber auch zum Ausspähen und Abhören missbraucht werden. Insbesondere unverschlüsselte WLANs oder GSM-Handykommunikation[970] sind leicht abhörbar, weil ein Angreifer die abgestrahlten Funkwellen lediglich empfangen und auswerten muss.

Physischer Zugang ist nur bei LAN-gestützer Kommunikation nötig. In einem solchen Fall werden Sniffer auf einem Router auf dem Transportweg (Netzwerkknoten) installiert und die übermittelten Paketdaten darüber abgegriffen.[971] Wegen der Dezentralität des Internets ist die Route, also die Abfolge an Servern, die die Daten des Senders an den Empfänger weiterleiten und umgekehrt, nicht immer gleich, so dass ein solcher Angriff auch scheitern kann. Je näher jedoch der mitschneidende Server netztopologisch beim Empfänger steht, umso wahrscheinlicher wird es, dass der Angreifer an die gewünschten Daten gelangt. Außerdem besteht das grundlegende Problem mit dem sogenannten „Border Gateway Protocol"[972] (BGP), dass durch Fehler oder auch die absichtliche „Fehlkonfiguration" (dann aktiver Angriff) von Servern Datenverkehr zwingend über gewisse Routen und Server im Internet geleitet werden muss, so dass auch das gezielte Mitschneiden erheblich erleichtert wird.[973] Vor allem mittels Deep-Packet-Inspection-Technologien sind sehr tiefgehende Trafficanalysen auch in Echtzeit möglich.[974]

Diese Angriffsform des Packet-Sniffings wird auch als Unterform eines Man-in-the-Middle-Angriffs (MITM) bezeichnet. Typischerweise begnügen sich Angreifer, die MITM-Angriffe durchführen, nicht mit dem bloßen Mitlesen von Daten, sondern versuchen dem Opfer manipulierte Daten unterzuschieben. Daher wird diese Angriffsform, soweit sie über das bloße Mitlesen von Daten hinausgeht, als aktive Angriffsform eingeordnet.

Nicht netzwerkbasiert und dementsprechend in der Praxis eher selten, sind folgende Angriffsmethoden. Die erste Methode besteht darin, die elektromagnetische Abstrahlung von Computern, Bildschirmen oder Leitungen aufzufangen und auf diese

---

969 http://www.tcpdump.org.

970 Dies betrifft aber nur GSM-Mobiltelefonie, da die bei GSM verwendeten Verschlüsselungsalgorithmen A5/1 bis A5/3 nicht (mehr) sicher sind; siehe dazu *Rütten*, Lauschgelegenheit, http://www.heise.de/ct/07/24/090.

971 *Holznagel* 2003, 25.

972 *RFC Archive*, RFC 4271, http://www.rfc-archive.org/getrfc.php?rfc=4271.

973 Erwähnt seien der weitreichende Ausfall von YouTube, nachdem ein pakistanischer Zensurserver fehlkonfiguriert wurde und das ähnliche Problem am 8.4.2010, als 15 % des weltweiten Internettraffics für 18 Minuten über chinesische Server geleitet wurden; siehe hierzu die Meldungen bei *McMillan*, YouTube outage underscores big Internet problem, http://www.infoworld.com/t/applications/youtube-outage-underscores-big-internet-problem-702 und *Neumann*, China: Man-in-the-middle-Angriff auf die ganze Welt?, http://www.netzpolitik.org/2010/china-man-in-the-middle-angriff-auf-die-ganze-welt.

974 Zur Deep-Packet-Inspection-Technologie siehe unten 3.8.1.1.

Weise den Kommunikationsinhalt zu rekonstruieren.[975] Neuerdings kann man auch per Lasermikrofon die Tastenklicks eines PCs oder Notebooks registrieren. Eine Software, die ähnlich funktioniert wie ein Texterkennungsprogramm, extrapoliert dann aus den jeweiligen Klickgeräuschen, welche Taste gedrückt wurde, gleicht ihre Ergebnisse mit einem Wörterbuch ab und versucht so sinnvolle Wörter zusammenzusetzen.[976] Ebenfalls zu den neueren Methoden zählen die sogenannten „Seitenkanalangriffe“, die die physikalische Implementierung eines Kryptosystems in einem Gerät angreifen und Rückschlüsse auf den verwendeten Schlüssel erlauben. Passive Formen sind die Messung der vergangenen Rechenzeit (Timing Attacks), die Beobachtung der genutzten Speicherbereiche oder die Messung des Stromverbrauchs während gewisser Kryptovorgänge. Ein weiterer passiver Angriff ist das Webseiten- und Nutzertracking. Dabei wird das Nutzungsverhalten einer Person, zum Beispiel beim Surfen über mehrere Webseiten hinweg, analysiert, um daraus Erkenntnisse für spätere aktive Angriffe zu gewinnen.

3.1.9.8.5.2 Aktive Angriffe

Bei aktiven Angriffen werden IT-Systeme, aber auch das Verhalten natürlicher Personen, so manipuliert, dass Daten entwendet oder verfälscht werden können.[977] Zu den klassischen aktiven Angriffen gehört das Übermitteln von Viren, Würmern, Spyware und Trojanern, also von Programmen, die unter den Sammelbegriff „Schadsoftware“ (Malware) fallen. Weitere verbreitete aktive Angriffe sind die bereits erwähnten (Distributed)-Denial-of-Service-Angriffe (DDoS)[978] oder Angriffe auf das Domain-Name-System, indem Verknüpfungen zwischen Domains und IP-Adressen gefälscht werden (Pharming und IP-Spoofing). Social Engineering zielt auf Personen ab und wird genutzt, um an Passwörter oder sonstige Zugangsdaten oder angriffsrelevante Informationen zu gelangen. Auch die bereits geschilderten Brute-Force-Attacken sind aktive Angriffe.[979] Öffentlich noch weitgehend unbeachtet sind neuartige Angriffe, die in der Lage sind, Hardware irreparabel zu schädigen. Dabei werden die implementierten Möglichkeiten für Firmwareupdates missbraucht. In Anlehnung an die DDoS-Angriffe werden diese Angriffe als „Permanent Denial of Service“ (PDOS) bezeichnet.[980]

---

975 *Holznagel* 2003, 25.

976 *Kremp*, Der Laser liest mit, http://www.spiegel.de/netzwelt/tech/0,1518,614887,00.html.

977 Ähnlich *ITWissen.info*, Angriff, http://www.itwissen.info/definition/lexikon/Angriff-attack.html.

978 Siehe dazu Fn. 412.

979 Siehe auch Fn. 948.

980 *Greif*, Neue Angriffsmethode legt Hardware dauerhaft lahm, http://www.zdnet.de/news/wirtschaft_sicherheit_security_neue_angriffsmethode_legt_hardware_dauerhaft_lahm_story-39001024-39191173-1.htm.

3.1.9.9 Allgemeine Sicherheitsmaßnahmen

Das Ergebnis einer Bedrohungsanalyse ist die Zusammenstellung von Maßnahmen zur Gewährleistung von IT-Sicherheit. Nachdem taugliche Sicherheitsmaßnahmen bereits als Maßnahmen zur Wahrung der IT-Schutzziele erwähnt wurden, sollen im Folgenden die wichtigsten Maßnahmen zur Absicherung von IT- und Cloudsystemen zusammenfassend und überblicksartig dargestellt werden.

Das Verständnis für die Sicherheitsmaßnahmen entfaltet sich zwar am Besten im direkten Zusammenhang mit der jeweiligen Bedrohung oder dem zu erreichenden Schutzziel, jedoch ist ein Überblick hilfreich, um die allgemeinen und wichtigsten Möglichkeiten einer Absicherung von IT-Systemen abschätzen zu können. Insbesondere die Beantwortung der Frage, ob Daten einem ausgelagerten IT-System anvertraut werden, ist davon abhängig, ob die Bereitschaft und die Fähigkeiten vorhanden sind, um die notwendigen Schutzmaßnahmen zu treffen. Bevor allerdings notwendige Maßnahmen eingeleitet werden können, müssen diese bekannt sein.

Die sogleich darzustellenden Maßnahmen entfalten auch für die technischen Gestaltungsziele und Gestaltungsvorschläge im Rahmen der KORA-Methode Relevanz, so dass hinsichtlich des konkreten praktischen Einsatzes nicht nur auf die bereits oben erwähnten Maßnahmen im direkten Zusammenhang mit den IT-Schutzzielen zu verweisen ist, sondern auch auf die späteren Ausführungen im Rahmen der Anwendung der KORA-Methode.

Die Sicherheitsmaßnahmen sind im Grunde ein disziplinenverbindendes Element und eine Schnittmenge zwischen der informatisch geprägten Sicht (IT-Bedrohungen, IT-Schutzziele) und den rechtlichen Vorgaben (Grundrechte bis hin zur Anlage zu § 9 BDSG). Sie haben ihren Ursprung sowohl in der Informatik, zum Beispiel am Stand der Sicherheitstechnik und Best Practices, als auch im Recht. Beispielsweise sind die rechtlich vorgegebenen Zugangs-, Zugriffs- und Weitergabekontrollen im Sinne des Satz 2 Nr. 2 bis 4 der Anlage zu § 9 BDSG gemäß Satz 3 durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren zu erreichen. Taugliche und bewährte Sicherheitsmaßnahmen sind „gelebter“ Rechtsgüterschutz.

Die wichtigsten Maßnahmen sind die Verschlüsselung von Daten, die Trennung von Systemen, Daten und Rollen, die Protokollierung von Systemzuständen und des Nutzungsverhaltens, der Aufbau von Redundanz, aber auch die Förderung der Nutzungs- und Sicherheitskompetenz und entsprechende Schulungen der Anwender und Administratoren. Letztere schärfen das Sicherheitsbewusstsein dieser Personengruppen. Audits und Zertifizierungen sind eine übergreifende Sicherheitsmaßnahme und ermöglichen die Überprüfung der bereits getroffenen Maßnahmen. Das

standardisierte Vorgehen erleichtert außerdem das Auffinden bis dahin noch nicht umgesetzter Sicherheitsmaßnahmen.

3.1.9.9.1 Verschlüsselung

Wie man an der gehäuften Erwähnung des Themas im Rahmen der Schutzziele und der Bedrohungsanalyse ersehen konnte, ist die Verschlüsselung der zu schützenden Daten eine der wichtigsten Maßnahmen zum Schutz der geheimen oder personenbezogenen Daten.

Bei der Verschlüsselung oder Kryptografie werden mittels Algorithmen und eines Schlüssels verständliche Informationen, der sogenannte Klartext, in unverständliche Zeichen, den Geheimtext, umgesetzt.[981] Eine Legaldefinition des Verschlüsselungsbegriffs mit ähnlichem Inhalt findet sich in § 3a Abs. 4 Nr. 3 des Berliner Datenschutzgesetzes. Danach ist Verschlüsselung „das Ersetzen von Klartextbegriffen oder Zeichen durch andere in der Weise, dass der Klartext nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft wieder lesbar gemacht werden kann“.[982]

Ziel einer Verschlüsselung ist somit, die verständlichen Informationen nur noch von Berechtigten durch den umgekehrten Weg der Entschlüsselung erkennbar zu machen und Angreifer oder Nichtberechtigte an der Erfassung des geschützten Informationsgehalts zu hindern.

Nach dem Prinzip *von Kerckhoffs* soll die Sicherheit nicht von der Geheimhaltung des verwendeten Algorithmus, sondern der Geheimhaltung des Schlüssels abhängig sein. Der Algorithmus sollte öffentlich sein, damit dessen Schwachstellen in öffentlichen Diskussionen und Analysen entdeckt werden können und der Algorithmus verbessert oder gegen einen sichereren ersetzt werden kann.[983]

Besonders erwähnenswert ist der Umstand, dass es, außer bei der mathematischen Einmalverschlüsselung mit dem sogenannten „One-Time-Pad“, keine absolute Sicherheit für Verschlüsselungsverfahren gibt. Die nur relative Sicherheit kryptographischer Verfahren basiert auf zwei Faktoren, nämlich der Wahrscheinlichkeit und der Zeit. Primär beruht diese Sicherheit darauf, dass es sehr unwahrscheinlich ist, dass mathematische Umkehrungen der genutzten Algorithmen und Funktionen gefunden werden. Der Faktor Zeit spielt bei der Dauer der Umkehrung der Funktionen oder bei Brute-Force-Angriffen eine Rolle. Für einen Angreifer muss die Zeitspanne zur Umkehrung oder für eine erfolgreiche Brute-Force-Attacke unangemessen lange dauern und damit praktisch unmöglich werden.[984] Auch die entstehenden Kosten

---

981 *ITWissen.info*, Verschlüsselung, http://www.itwissen.info/definition/lexikon/Verschluesselung-encryption.html.

982 *Gerhards* 2010, 87.

983 *Holznagel* 2003, 89.

984 *Gerhards* 2010, 35, 37.

und die notwendige Arbeitskraft sind limitierende Faktoren, so wie dies auch in der Legaldefinition des Berliner Datenschutzgesetzes zum Ausdruck kommt.

Neben der Absicherung des Übertragungsweges[985] ist vor allem die Speicherung von Daten mittels Kryptografie absicherbar. Der oft notwendige Zwischenschritt der Verarbeitung von Daten, in Cloudsystemen alle Vorgänge außer Cloudstorage, ist mit den herkömmlichen Methoden der Verschlüsselung (noch) nicht abzusichern.[986]

Im Lebenszyklus der Daten ist diese Sicherungsmaßnahme, trotz der Schwächen im Zusammenhang mit der Verarbeitung von Daten, von größter Bedeutung, da die Übermittlung und vor allem die Speicherung die längste zeitliche Dauer, gerade im Vergleich zur nur kurzzeitigen Phase der unverschlüsselten Verarbeitung, aufweisen und dadurch Angriffe bereits aus zeitlichen Gesichtspunkten erschwert werden. Das Zeitfenster für einen Angriff auf die unverschlüsselten Daten in Prozessoren, Speichern oder Caches ist damit im Vergleich zu einer dauernd unverschlüsselten Vorhaltung der Daten sehr klein. In Clouds eingebrachte Daten werden in der Regel nicht fortwährend (weiter)verarbeitet, sondern ruhen als gespeicherte Daten auf Datenträgern oder werden über Netze zwischen dem Nutzer und Cloudprovider transportiert.

3.1.9.9.2 Systemtrennung, Abschottung und Kanalisierung von Datenströmen

Wie vor allem im Anschluss bei den cloudspezifischen Bedrohungen im Detail zu sehen sein wird, ist die Trennung und (teilweise) Abschottung von Systemen, die über Netzwerke oder mittels Virtualisierung verbunden sind, eine erprobte Maßnahme. Die sogenannte „Entnetzung“ ist die extremste Form einer solchen Trennung.[987] Dabei werden einmal verbundene Systeme komplett getrennt oder autarke Systeme von vornherein niemals verbunden. In Zeiten des Internet und der IP-Fähigkeit von immer mehr Geräten ist jedoch zurzeit der gegenteilige Trend vorherrschend, nämlich die immer weiter fortschreitende Vernetzung.

Firewalls, die Aufteilung in Subnetze, auch virtualisiert in Form von VLANs oder Network Address Translation[988] (NAT) sind technische Möglichkeiten, um eine Vernetzung bei einer teilweisen Abschottung und Trennung zu ermöglichen. Auch Hypervisoren sind eine solche technische Lösung der Systemtrennung. Durch diese technischen Möglichkeiten sind Datenströme zwischen unterschiedlichen Systemen gezielt steuer- und eingrenzbar.

---

985 Zum Beispiel mittels SSL; siehe hierzu Kap. 3.1.9.7.1 und Fn. 888.

986 Siehe dazu die Problematik im Zusammenhang mit homomorpher Verschlüsselung in Kap. 4.6.5 und die Fn. 1505.

987 Zum Begriff der „Entnetzung“ siehe *Gaycken/Karger*, MMR 2011, 3 ff.

988 *RFC Archive*, RFC 3022, http://www.rfc-archive.org/getrfc.php?rfc=3022.

Die Wahrung der physischen IT-Sicherheit ist die ursprünglichste Form der Systemtrennung. Dadurch soll die unmittelbare Einwirkung auf die zu schützenden Systeme verhindert werden. Anerkannte konkrete Maßnahmen sind die Gewährleistung des unmittelbaren Besitzes am geschützten Gerät, das Einschließen von Rechnern oder das Umzäunen von Rechenzentren.

3.1.9.9.3 Datentrennung

Datentrennung in Anlehnung an Nr. 8 der Anlage zu § 9 BDSG betrifft im Gegensatz zur Systemtrennung die Speicherung und Aufbewahrung von Daten. Hierbei sind unterschiedliche Datenarten voneinander abzugrenzen.[989]

Analog zur Systemtrennung sind die Daten der unterschiedlichen Kunden voneinander getrennt abzuspeichern. Inhaltsdaten, also die von den Nutzern hochgeladenen Daten, sind von deren Nutzungs- und Bestandsdaten getrennt zu speichern. Insbesondere die Bestandsdaten, vor allem Kredit- und Bankdaten, erfordern einen besonders hohen Schutz.[990] Protokoll- und Nutzungsdaten sind ebenfalls von sonstigen Daten getrennt zu speichern.

Zu unterschiedlichen Zwecken gespeicherte Daten sind somit im Sinne des Zweckbindungsgrundsatzes getrennt aufzubewahren.[991] Im Falle eines Angriffs sollen so wenig wie möglich miteinander verknüpfte oder verknüpfbare Daten in die Hände des Angreifers fallen, so dass dessen Angriff im Optimalfall ins Leere läuft oder sogar den Angriffsversuch an sich unterbindet, weil der erwartete „Ertrag“ für den Angreifer zu gering ist.

Neben diesen sicherheitsrelevanten Aspekten dient die Datentrennung auch der Verhinderung einer Profilbildung. Das Erschweren einer solchen Profilbildung ist weniger potentiellen Angreifern geschuldet, sondern soll im Wesentlichen verhindern, dass der Cloudprovider ein zu umfassendes Bild über seine Nutzer gewinnt. Nicht selten werden solche Nutzerprofile, beispielsweise nach einer Insolvenz des Providers, an Dritte verkauft. Datentrennung soll damit auch einer potentiell missbräuchlichen Verwendung vorbeugen.

Eine Kombination von zwei Maßnahmen wäre die Trennung und unterschiedliche Verschlüsselung von unterschiedlichen Arten von Datensätzen. So sollten beispielsweise die eigentlichen Inhaltsdaten in der Cloud anders verschlüsselt werden als die Bestandsdaten der Nutzer. Bei gleichen Verschlüsselungsverfahren müssen sich die Schlüssel für die jeweiligen Daten unterscheiden.

---

989 Zu den rechtlichen Aspekten diverser Datenarten siehe auch Kap. 3.1.4.2.

990 Für Kreditkarten gilt der Payment Card Industry Data Security Standard, der verschärfte Anforderungen an die Aufbewahrung und den Umgang mit diesen Daten stellt.

991 Näheres zum Zweckbindungsgrundsatz siehe in Kap. 3.1.6.6.

3.1.9.9.4 Rollentrennung

Die Rollentrennung zielt auf die Befugnisse der beteiligten Personen im Umgang mit den Systemen und Daten ab. Neben der Unterscheidung zwischen Beschäftigten (Insidern) und Nutzern, ist zudem die Trennung von Befugnissen der einzelnen Mitarbeiter eine wesentliche Maßnahme zur Erreichung von IT-Sicherheit. So sollten für unterschiedliche IT-Systeme, wie physische Server, Router, Switches, virtuelle Maschinen oder Netze unterschiedliche Personen zuständig sein. Server- und Netzadministration sollten getrennt sein.[992] Stimmen in der Literatur unterscheiden zwischen Infrastrukturadministratoren und Sicherheitsadministratoren, wobei die einen nur Infrastrukturen modifizieren und die anderen lediglich Verfahren definieren können, ohne weitere Rollen auszuüben.[993] Im Ergebnis sollte also jeder Administrator nur solche Rechte innehaben, die für die Erfüllung seiner Aufgabe erforderlich sind. Nutzer sollten nur die ihnen zugewiesenen Ressourcen nutzen können. Man spricht dabei auch von Rechteminimierung oder dem „Principle of Least Privilege“.[994]

Neben Authentisierungs-, Zugriffs-, Zugangskontrollen und ähnlichen Maßnahmen sollte es unmöglich sein, sich erhöhte Rechte oder andere Rollen zuweisen zu können, beispielsweise indem Administratoren als Insider oder externe Angreifer entsprechende Verzeichnisse mit den Rollenzuweisungen abändern.[995]

3.1.9.9.5 Protokollierung

Mit der Rollentrennung wird auch die Protokollierung von Handlungen und Zuständen notwendig. Die Handlungen der beteiligten Personen sind nur mittels Protokollierung überprüfbar. Überschreitungen der Berechtigung oder fehlerhafte Handlungen sind nachträglich mittels Logdateien und Protokollen leichter nachvollziehbar und unmittelbar dem Falschagierenden zuordenbar. Gleiches gilt für unzulässige Systemzustände und sich daraus möglicherweise ergebende Sicherheitsvorfälle.

Bei der Protokollierung ist zu beachten, dass diese nicht nur eine Sicherheitsmaßnahme, sondern auch ein Sicherheitsrisiko darstellen kann. Angreifer können beispielweise aus Logdateien Rückschlüsse auf die technisch-organisatorische Ausgestaltung der Systeme ziehen und Angriffs(zeit)punkte ausforschen. Gleichzeitig können sie durch Manipulation der Protokolle bereits abgeschlossene Angriffe verschleiern. Die Protokollierung ist demnach ihrerseits durch andere Sicherungsmaßnahmen abzusichern. Nicht zuletzt hat die Protokollierung auch datenschutz-

---

992 Ähnlich *Münch/Doubrava/Essoh*, DuD 2011, 325 f.

993 *Marnau/Schirmer/Schlehahn/Schunter*, DuD 2011, 334.

994 *Marnau/Schirmer/Schlehahn/Schunter*, DuD 2011, 334.

995 *Münch/Doubrava/Essoh*, DuD 2011, 324 am Beispiel Private Clouds, wobei die Gefährdung aber nicht cloudspezifisch ist, sondern für alle IT-Systeme gilt, die solche Verzeichnisse zur Rollenzuweisung nutzen.

rechtliche Relevanz, da aus den Protokollen der Nutzungshandlungen Nutzungsprofile von Personen erstellt werden können.

Für Cloud Computing ergeben sich dabei keine Besonderheiten. Die Protokollierung sollte sowohl Handlungen der Administratoren als auch der Cloudnutzer umfassen und Systemzustände nachvollziehbar machen.

3.1.9.9.6 Redundanz

Die mehrfache und redundante Vorhaltung von Daten und Systemen ist eine erprobte und lange bekannte Möglichkeit, auf zukünftige Sicherheitsvorfälle oder Ausfälle zu reagieren. Gerade verteilte Systeme sind prädestiniert, um Redundanzen aufzubauen und zu nutzen. In Cloudsystemen wird der Gedanke der Redundanz auf ein neues und bis dahin unbekanntes Niveau gehoben. Neuartige Redundanzen durch die schiere Vielzahl physischer Systeme, die Abstraktion von diesen mittels Virtualisierung und die damit verbundenen einfachen Möglichkeiten der Replizierung von Daten und virtuellen Systemen stellen einen großen Fortschritt beim Redundanzaufbau dar. Je weitgehender die Redundanzbemühungen sind, umso geringer ist die Schadenswahrscheinlichkeit.

Eine spezielle Form der Redundanz ist die Aufteilung von Daten in Datenfragmente und deren Replizierung. Der Vorteil dieser Vorgehensweise ist der Schutz der Vertraulichkeit des Informationsgehalts bei gleichzeitiger Erhöhung der Verfügbarkeit und Integrität der Daten.[996]

3.1.9.9.7 Nutzungskompetenz und IT-Sicherheitsbewusstsein

Sicherheit kommt auch dadurch zustande, dass die bei einem Anbieter Beschäftigten und die Nutzer die Dienste ordnungsgemäß administrieren und nutzen können. Gerade Administratoren müssen sich angesichts der technischen Entwicklung und dem Aufkommen immer neuer Bedrohungen fortbilden. Administratoren und Nutzer müssen durch Schulungen und Einweisungen in die Lage versetzt werden, die Systeme und Dienste nach dem intendierten Zweck nutzen zu können. Insbesondere Fehlbedienungen können neue Sicherheitslücken auftun oder existierende verstärken. Bei der Gestaltung der Dienste sind ergonomische Erkenntnisse zu nutzen. Einfache und leicht zu nutzende Systeme und Dienste vermindern die Gefahr von Fehlbedienungen, fördern die Beherrschbarkeit und sind insgesamt ein Beitrag zur Sicherheit.

Neben dem Aneignen von Nutzungskompetenz muss sowohl bei den Nutzern als auch und gerade bei den Beschäftigten das Bewusstsein für die Etablierung von IT-Sicherheit und den sicheren Umgang mit Daten und Diensten kontinuierlich sensibilisiert und weiterentwickelt werden. Außerdem müssen die beteiligten Personen in

---

[996] Vergleiche auch nochmal oben Kap. 3.1.9.7.2 und die Ausführungen zur technischen Umsetzung im Rahmen der KORA-Methode in Kap. 4.6.8.

die Lage versetzt werden, auf Sicherheitsvorfälle angemessen zu reagieren. Parallel zu technisch-organisatorisch geprägten Sicherheitskonzepten ist im alltäglichen Umgang mit Daten und Systemen eine „IT-Sicherheitskultur“ notwendig. Gerade in diesem Zusammenhang ist die Formel, dass Sicherheit nicht punktuell ist, sondern einen andauernden Prozess darstellt, besonders treffend.

3.1.9.9.8 Audits und Zertifizierungen

Eine letzte bedeutende Maßnahme zur Gewährleistung von IT-Sicherheit ist die Zertifizierung und Auditierung von IT-Systemen. Ein solches Vorgehen findet sogar in § 9a BDSG als Datenschutzaudit rechtlich Anklang. Während auf die Rechtsnorm später noch einzugehen sein wird, sollen im Folgenden die Grundlagen für Zertifizierungen in Form von Standards, Normen und Best Practices kurz dargestellt sowie deren Bedeutung für Cloud Computing aufgezeigt werden.[997]

Zur Erreichung und Förderung der Schutzziele und zur Etablierung bewährter und erprobter Sicherheitsmaßnahmen haben sich im Laufe der Zeit diverse Standards und Verfahren im Sinne von Best Practices etabliert. Diese ermöglichen Organisationen einen möglichst sicheren und (datenschutz)rechtskonformen Umgang mit den ihnen anvertrauten Daten.

Ein Standard ist ein öffentlich zugängliches technisches Dokument, das auf Ergebnissen aus Wissenschaft und Technik beruht, unter Beteiligung aller interessierten Parteien entwickelt wird und deren Zustimmung findet.[998]

Der Begriff der Norm wird selbst durch eine Norm definiert, nämlich DIN EN 45020, und ist dieser Definition zufolge „ein Dokument, das mit Konsens erstellt und von einer anderen Institution angenommen wurde und das für die allgemeine und wiederkehrende Anwendung Regeln, Leitlinien oder Merkmale für Tätigkeiten oder deren Ergebnisse festlegt“.[999] Nach ständiger Rechtsprechung sind beispielsweise DIN-Normen keine Rechtsnormen, sondern private technische Regelungen mit Empfehlungscharakter und können die anerkannten Regeln der Technik wiedergeben oder hinter diesen zurückbleiben.[1000]

Best Practices sind bewährte und kostengünstige Verfahren, technische Systeme oder Geschäftsprozesse, die das verwendende Unternehmen zum Musterbetrieb für andere machen.[1001]

Primär erlauben die Standards die Überprüfung des Sicherheitszustands eines Systems. Diese erfolgt anhand von vorformulierten und standardisierten Vorgehenswei-

---

997 Zu § 9a BDSG siehe Kap. 3.1.10.
998 *Lensdorf/Mayer-Wegelin*, CR 2009, 545.
999 *Hübner*, DuD 2011, 56.
1000 BGHZ 139, 16; *Hübner*, DuD 2011, 56.
1001 *Lensdorf/Mayer-Wegelin*, CR 2009, 545.

sen, die in Audits und bei Zertifizierungen abgeprüft werden.[1002] Dabei wird auf Erfahrungen und im Laufe der Zeit angesammeltes Wissen zurückgegriffen. Einige Standards haben auch für Cloud Computing Relevanz. Insbesondere können Cloudprovider mit einer Zertifizierung das Vertrauen in ihre Geschäftstätigkeit erhöhen und im Optimalfall die Einhaltung und Wahrung von rechtlich notwendigen Maßnahmen, beispielsweise nach § 9 BDSG, nachweisen. Mittlerweile gibt es sogar cloudspezifische Gütesiegel, wie zum Beispiel das sogenannte „EuroCloud SaaS-Star Audit Certificate".[1003] Am bekanntesten dürfte der Standard ISO/IEC 27001 aus der ISO/IEC 27000-Serie[1004] sein. Dieser beinhaltet Best Practices im Umgang mit Informationssicherheitsmanagementsystemen (ISMS). ISO/IEC 27001 hat auch unmittelbar für die Praxis des Cloud Computing Bedeutung. So sind einige Cloudprovider nach ISO/IEC 27001 zertifiziert.[1005]

Die IT-Grundschutzkataloge des BSI sind national bedeutend und stellen eine Methodik dar, um Informationssicherheit in der Praxis strukturiert und planmäßig umzusetzen. Sie sind wie die ISO/IEC 27000-Reihe als Best Practices anzusehen und unterstützen die Aufstellung und Umsetzung von Sicherheitskonzepten und Informationssicherheitsmanagementsystemen. Den Grundschutzkatalogen stehen mittlerweile vier BSI-Standards zur Seite.[1006] Ein direkter Zusammenhang zwischen ISO/IEC 27001 und dem BSI-Grundschutz besteht seit dem Jahr 2005 in der Form, dass eine Zertifizierung nach ISO/IEC 27001 auf Basis von IT-Grundschutz erfolgen kann.[1007] Eine Zertifizierung nach den BSI-Standards erfüllt damit gleichzeitig die Voraussetzungen von ISO/IEC 27001.

Ebenfalls bedeutsam ist der Payment Card Industry Data Security Standard[1008] (PCI DSS), der speziell für die Absicherung von Bezahlvorgängen mittels Kreditkarte entwickelt wurde.

1002 Ähnlich *Hübner*, DuD 2011, 56.

1003 Näheres dazu bei *Weiss*, <kes> Special - Sicheres Cloud Computing, März 2011, 16 und *Giebichenstein/Weiss*, DuD 2011, 338.

1004 http://www.27000.org.

1005 Zum Beispiel die Cloudservices von Salesforce und die Amazon Webservices; siehe *Salesforce*, ISO 27001 certified security, http://www.salesforce.com/platform/cloud-infrastructure/security.jsp und *Barr*, AWS Receives ISO 27001 Certification, http://aws.typepad.com/aws/2010/11/aws-receives-iso-27001-certification.html.

1006 BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS); BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise; BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz; BSI-Standard 100-4 Notfallmanagement; https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html.

1007 *BSI*, IT-Grundschutz: Ziel, Idee und Konzeption, https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Allgemeines/Einstiegskapitel/einstiegskapitel_node.html.

1008 https://www.pcisecuritystandards.org/security_standards/index.php.

Kein Standard, aber eine Spezifikation ist DIN SPEC 1401, die weiter unten näher dargestellt wird, da diese speziell Outsourcingvorhaben betrifft.[1009] Im Gegensatz zu den bisher erwähnten Standards geht es bei DIN SPEC 1401 nicht um die nachträgliche Überprüfung bestehender Systeme, sondern um die Abschätzung und Erleichterung geplanter und noch durchzuführender Outsourcingvorhaben. Dabei besteht eine gewisse Ähnlichkeit zum Outsourcingbaustein B 1.11 des BSI-Grundschutzkatalogs.

Für potentielle Cloudnutzer sind Zertifizierungen nach gewissen Standards ein wichtiger Anhaltspunkt für die Professionalität und Vertrauenswürdigkeit eines Anbieters. Sie erleichtern die Anbieterauswahl und werden daher nicht selten als Teil der Eigenwerbung der Anbieter an die potentiellen Nutzer kommuniziert.

3.1.9.10 Neuartige cloudspezifische Bedrohungen und notwendige Sicherheitsmaßnahmen

Nach der Darstellung der allgemeinen Bedrohungen, die im Wesentlichen alle auch die Sicherheit von Cloudsystemen tangieren, gibt es spezielle neuartige Bedrohungen, die sich erst mit der Bereitstellung von Cloudsystemen offenbaren.[1010] Entsprechend dem bisherigen Vorgehen sollen konkrete Sicherheitsmaßnahmen unmittelbar im Zusammenhang mit den cloudspezifischen Bedrohungen erläutert werden.

Hauptursache für die Neuartigkeit der Bedrohungen ist vor allem die Implementierung von Virtualisierung mit dem Zweck der Realisierung von Mehrmandantenfähigkeit. Neben der vergleichsweisen Neuartigkeit der Virtualisierung an sich, ist vor allem der Umstand neu, dass diese dazu verwendet wird, um eine Vielzahl von Cloudnutzern, deren Systeme lediglich virtuell voneinander getrennt sind, bedienen zu können.

3.1.9.10.1 Bedrohungen durch unzureichende Trennung und Segmentierung

Die wichtigste kernspezifische Bedrohung des Cloud Computing ist in einer unzureichenden Trennung von Daten und Zugriffsberechtigungen zu sehen. Bei den Bedrohungen durch mangelhafte Trennung geht es bei Cloud Computing hauptsächlich um die virtuellen Systeme und die darin verarbeiteten Daten. Während Virtualisierung in lokalen Rechenzentren üblicherweise dazu eingesetzt wird, um die vorhandenen Ressourcen zusammenzuführen und besser auszunutzen, kommt bei Cloud Computing die Ermöglichung der Nutzung durch viele Kunden und deren gegenseitige Abschottung hinzu.

[1009] Siehe dazu Kap. 3.5.4.

[1010] Eine komplette Risikoanalyse, nicht nur technischer Natur, hat die ENISA durchgeführt; siehe dazu *Catteddu/Hogben* 2010, 1 ff.

3.1.9.10.1.1 Hypervisorsicherheit

Die Hypervisorsicherheit ist notwendige Voraussetzung, um ein Übertreten von Daten zwischen mehreren virtuellen Maschinen zu verhindern.[1011] Bedrohungen dieser Sicherheit können darin bestehen, dass eine virtuelle Maschine auf Speicherbereiche des Hypervisors oder anderer virtueller Maschinen zugreifen kann (Virtual Machine Escape).[1012] Erleichtert oder ermöglicht wird ein solcher Angriff durch Fehler in der Systemarchitektur, insbesondere durch mangelhafte Isolation der virtuellen Maschinen oder Fehler im Design und in der Umsetzung der Virtualisierungssoftware, insbesondere im Hypervisor. Solche Schwachstellen in der Virtualisierungssoftware sind wegen dem zwingenden Erfordernis einer effektiven Trennung als sehr kritisch anzusehen.

Neben dem Zugriff aus einer virtuellen Maschine auf Daten einer anderen, besteht die noch größere Bedrohung der Übernahme des Hypervisors und damit die Möglichkeit des Zugriffs auf alle Daten des zugrundeliegen physischen Systems. Außerdem sind nach einer solchen Übernahme auch Störungen des Clouddienstes wahrscheinlich. Zum Beispiel indem durch Angreifer virtuelle Maschinen abgeschaltet oder gelöscht werden.[1013] Auch die bösartige Implementierung von virtuellen Rootkits, vergleichbar mit den schon existierenden Kits für herkömmliche PCs namens Blue Pill oder SubVirt, ist bei Fehlern innerhalb des Hypervisors leichter möglich.[1014] Während Blue Pill und SubVirt auf herkömmlichen Rechnern das auf der Hardware laufende Betriebssystem in ein virtuelles System überführen, ist es bei Servern ebenso denkbar, dass eine zusätzliche virtuelle Abstraktionsschicht eingebaut wird, um die bösartig motivierte Kontrolle des Gesamtsystems oder einzelner virtueller Maschinen durch einen Angreifer zu tarnen. Bei einer Vielzahl von abstrahierten Schichten fällt eine zusätzliche Schicht weniger auf.

Zielsetzung eines virtuellen Rootkits ist also die Erschwernis der Detektierbarkeit durch Antivirenprogramme oder sonstige Malwareerkennungsmaßnahmen und das erleichterte Abfangen aller Ein- und Ausgaben, zum Beispiel von Passwörtern oder Schlüsseln.[1015]

Es soll allerdings nicht unerwähnt bleiben, dass solche Rootkitangriffe, insbesondere durch externe Angreifer, nur sehr schwer umzusetzen sind. Wegen der hohen

---

[1011] Siehe dazu auch die Kap. 2.3.4.2.1 und 2.3.5.1.

[1012] *Grobauer/Walloschek/Stöcker* 2010, 15; *Deussen/Strick/Peters*, 2010, 64; *Münch/Doubrava/Essoh*, DuD 2011, 324.

[1013] *Slamka/Georg*, in: Schartner/Weippl, D-A-CH Security 2010, 27.

[1014] *Curry/Darbyshire/Fisher/Hartman/Herrod/Kumar/Martins/Orrin/Wolf* 2010, 5; *Bachfeld*, Rootkit verschiebt Windows in virtuelle Maschine, http://www.heise.de/newsticker/meldung/Rootkit-verschiebt-Windows-in-virtuelle-Maschine-173214.html.

[1015] *Curry/Darbyshire/Fisher/Hartman/Herrod/Kumar/Martins/Orrin/Wolf* 2010, 5, 6.

Komplexität ist diese Gefahr zurzeit eher theoretischer Natur. Praktische Erfahrungen hinsichtlich eines solchen Angriffs bestehen bisher (noch) nicht.[1016]

Als Gegenmaßnahme können durch einen „Hardware Root of Trust“, also ein aus Hardware bestehendes Trusted Platform Module (TPM), Rootkitangriffe reduziert oder gänzlich unterbunden werden. Dabei werden regelmäßig stattfindende Programmabfolgen und Systemzustände, zum Beispiel der Bootvorgang, mit vordefinierten im TPM gespeicherten Zuständen verglichen. Weil diese bei der Herstellung des Computers oder der Computerkomponente „in Hardware gegossene“ Vergleichsbasis nicht softwareseitig manipuliert werden kann, ist ein Angriff umso schwerer, da der Angreifer einen Weg finden muss, diese Systemzustandsvergleiche zu unterbinden.[1017]

Viel einfacher und wahrscheinlicher sind die eingangs erwähnten Übernahmen von unsicheren virtuellen Maschinen oder Hypervisoren. Indem der Angreifer eine virtuelle Maschine als vorgeblicher Cloudkunde anmietet, kann er insbesondere bei IaaS wegen der erheblichen Steuerungsmöglichkeiten, aber auch bei PaaS und SaaS, inhärente Lücken ausnutzen, um darüber Angriffe auf das Gesamtsystem oder benachbarte virtuelle Maschinen zu starten. So gibt es schon theoretische Überlegungen und ein praktisches Experiment wie ein solcher Angriff in der Praxis konkret ablaufen könnte.[1018] Insbesondere hochkoordinierte „Exfiltration-Angriffe“[1019] im Rahmen von IaaS-Angeboten dürften zukünftig problematisch werden. Dabei sind Daten eines bestimmten Cloudnutzers, beispielsweise eines Unternehmens oder einer Privatperson, Ziel des Angriffs. Zwischenziel des Angriffs ist die Anmietung mindestens einer virtuellen Maschine auf dem gleichen physischen Server wie das Angriffsziel. Um dies zu erreichen, werden parallel DDoS-Angriffe auf die Infrastruktur ausgeführt, um damit den Cloudprovider zu zwingen, neue virtuelle Maschinen bereitzustellen und feststehende Ressourcen umzuverteilen, während der Angreifer gleichzeitig eine Vielzahl von virtuellen Maschinen anmietet. So soll sich die Wahrscheinlichkeit erhöhen, dass sich mindestens eine der angemieteten Maschinen auf dem gleichen physischen Server wie das anvisierte Angriffsziel befindet. Im Anschluss können dann mögliche Fehler im Hypervisor ausgenutzt werden,

---

[1016] *Curry/Darbyshire/Fisher/Hartman/Herrod/Kumar/Martins/Orrin/Wolf* 2010, 6.

[1017] *Curry/Darbyshire/Fisher/Hartman/Herrod/Kumar/Martins/Orrin/Wolf* 2010, 6; *Berger*, The TPM, Trust and the Cloud: Making Trust Real, http://cloudcomputing.sys-con.com/node/1411630.

[1018] Zum praktischen Experiment mit Amazons EC2 siehe das Schaubild bei *Talbot*, Technology Review 03/2010, 41.

[1019] „Exfiltration“ bedeutet übersetzt das Ausschleusen oder Herausschleusen und ist ein Begriff aus dem Militärjargon.

um auf die Speicherbereiche und Daten der benachbarten Maschinen zuzugreifen und diese auszulesen.[1020]

Je komplexer und virtuell abstrahierter ein System ist, umso schwieriger ist die Absicherung mittels TPM. TPMs überwachen üblicherweise nur die Basiszustände und Bootabfolgen physischer Systeme. Anwendungssoftware oder mehrfach abstrahierte virtuelle Maschinen sind wegen der damit einhergehenden Komplexität des TPM und den notwendigen Restriktionen bei der Softwarenutzung nur schwer überwachbar. Es ist aber gerade bei standardisierten und gleichförmigen Cloudumgebungen nicht unwahrscheinlich, dass ein solches Modul entwickelt werden kann, da die Gleichförmigkeit der Bereitstellung und Nutzung die Komplexität reduziert.[1021] Zudem könnten durch ein solches neuartiges Modul mittelfristig auch die Angriffe auf Hypervisoren erschwert werden, weil der Zustand des Hypervisors oder sogar die Zustände der laufenden virtuellen Maschinen mit den vordefinierten Zuständen im TPM abgleichbar wären.

3.1.9.10.1.2 Absicherung des Management Interfaces und des Datenverkehrs durch Trennung

Cloudservices müssen durch Angestellte des Cloudproviders kontrolliert und administriert werden. Mit dem sogenannten Management Interface werden Maschineninstanzen verwaltet, gestartet, gestoppt und erzeugt sowie die Fernwartung der Virtualisierungsumgebung ermöglicht.[1022] Das Schadenspotential durch interne Angreifer ist damit bei Cloud Computing in der Regel höher als bei herkömmlichen IT-Diensten und Rechenzentren. Bei einer Public Cloud mit tausenden von Nutzern können bei absichtlichen schädigenden Eingriffen durch Administratoren erhebliche Schäden entstehen.[1023] Betroffen sind nicht nur die Integrität der Kundendaten, sondern auch die Verfügbarkeit der Dienste an sich. Eine strenge Rechteverwaltung und Rechtetrennung und die Implementierung des Mehraugen-Prinzips sind unerlässlich. Außerdem ist der Kundendatenverkehr vom administrativen Datenverkehr zu trennen. Insbesondere darf der Zugriff von virtuellen Maschinen auf Management Interfaces unter keinen Umständen möglich sein.[1024] Auch der Missbrauch von Gastwerkzeugen wie XenTools oder VMware Tools, um damit kundeneigene virtu-

---

[1020] *Curry/Darbyshire/Fisher/Hartman/Herrod/Kumar/Martins/Orrin/Wolf* 2010, 8, 9; *Talbot*, Technology Review 03/2010, 41; *Münch/Doubrava/Essoh*, DuD 2011, 324.

[1021] Ähnlich *Curry/Darbyshire/Fisher/Hartman/Herrod/Kumar/Martins/Orrin/Wolf* 2010, 6.

[1022] *Slamka/Georg*, in: Schartner/Weippl, D-A-CH Security 2010, 27; *Jaster/Collier de Mendoca/Slamka/Radmacher* 2010, 16; je eher es sich um ein IaaS-Angebot handelt, umso eher kann auch ein Nutzer solche Handlungen für „seine“ virtuellen Nutzerinstanzen vornehmen; siehe dazu auch das Beispiel der „AWS Management Console“ in Fn. 213.

[1023] Die Bedrohung gilt allerdings auch für Private Clouds; so zum Beispiel *Münch/Doubrava/Essoh*, DuD 2011, 324.

[1024] *Jaster/Collier de Mendoca/Slamka/Radmacher* 2010, 16; *Slamka/Georg*, in: Schartner/Weippl, D-A-CH Security 2010, 27.

elle Maschinen bei IaaS selbst steuern zu können, darf nicht dazu führen, dass diese Werkzeuge unerlaubt Systemrechte und damit mit einem Management Interface vergleichbare Möglichkeiten der Administration von virtuellen Maschinen anderer Nutzer erlangen.[1025]

Netzwerke sind abhängig von der Art der übertragenen Daten, beispielsweise nach administrativen und produktiven Daten oder nach Datenströmen unterschiedlicher Nutzer, durch physische Isolierung mittels Switches und Router oder virtuell durch die Nutzung unterschiedlicher VLANs aufzutrennen.[1026] Um gegen PDOS-Angriffe auf die Hardware oder gegen allgemeine Hardwarefehler gewappnet zu sein, müssen die Rechner für die Management Interfaces redundant vorhanden sein.

3.1.9.10.2 Kontrollverlust durch Verteilung

Was einerseits ein Vorteil sein kann, indem Daten, Datenfragmente und Systeme getrennt und redundant vorgehalten werden, birgt andererseits die Gefahr des Kontrollverlusts. Diese wird bei Cloud Computing dadurch verstärkt, dass ein Provider Subunternehmen zur Erbringung seiner Dienste heranziehen kann. Das kurzzeitige und flexible Eingehen von solchen Geschäftsbeziehungen birgt immer die Gefahr, dass Daten auf den kurzzeitig genutzten Ressourcen nicht oder nicht vollständig gelöscht werden, so dass der Provider oder Nutzer nach der Provisionierung und Nutzung der Systeme nicht mehr auf diese zugreifen können. Im Extremfall werden solche Subressourcen nur für Millisekunden genutzt, beispielsweise indem Daten kurzzeitig zwischengespeichert werden. Bei einer durch Algorithmen geprägten Verteilung der Daten ist zudem nicht immer vorhersagbar, wo und wann Daten in einer solchen breit aufgestellten Cloud gespeichert oder verarbeitet werden. Data Tracking Tools können aber die Nachvollziehbarkeit und Nachverfolgbarkeit der Datenverteilung in Echtzeit und nachträglich erleichtern.[1027]

Diese Gefahren sind jedoch mit weiteren, vergleichsweise einfachen, Maßnahmen minimierbar. Die ausschließliche Nutzung eigenkontrollierter Ressourcen ist die einfachste Maßnahme und entspricht im Prinzip dem Model der Private Cloud. Weitere Maßnahmen sind die Beibehaltung der Kontrolle durch vertragliche Verpflichtung der Subunternehmen und die Einräumung von Weisungs- und Kontrollrechten.[1028] Diese Rechte sind technisch zu unterstützen, zum Beispiel durch APIs und Schnittstellen oder die automatisierte Zusendung von Protokollen. Erwähnenswert ist in diesem Zusammenhang, dass solche Schnittstellen bei unzureichender

---

[1025] So auch *Münch/Doubrava/Essoh*, DuD 2011, 324 für Private Clouds.

[1026] *Slamka/Georg*, in: Schartner/Weippl, D-A-CH Security 2010, 26; *Jaster/Collier de Mendoca/Slamka/Radmacher* 2010, 15; *Münch/Doubrava/Essoh*, DuD 2011, 325.

[1027] *Schneider*, IT-Grundschutz 2010, 12; zu Data Tracking Tools siehe auch Kap. 4.6.11.

[1028] Zu Einzelheiten siehe auch die Ausführungen zu Auslagerungsketten in Kap. 3.1.8.6 und die obige Fn. 896.

Implementierung auch von Angreifern für ihre Zwecke ausgenutzt werden können.[1029]

3.1.9.10.3 Kontrollverlust durch die Weiterübermittlung von Daten

Nicht technischer, sondern eher faktischer oder rechtlicher Natur ist die zweite Form des Kontrollverlusts, nämlich die Übermittlung von Daten durch den Provider an Dritte. Eine solche Übermittlung oder Datenweitergabe kann missbräuchlich erfolgen oder mit der Zustimmung des Nutzers. Letztere erfolgt durch intransparent gestaltete Nutzungsbedingungen oft unbewusst.

So hatte beispielsweise Facebook Anfang 2009 eine Klausel in seinen Nutzungsbedingungen, wonach die von den Mitgliedern generierten Inhalte genutzt, kopiert, veröffentlicht, gestreamt, gespeichert, aufbewahrt, öffentlich aufgeführt oder gezeigt, ausgestrahlt, gescannt oder umformatiert werden durften. Die Erlaubnis galt sogar, nachdem der Nutzer sein Profil gelöscht hatte.[1030] Später wurde diese Klausel insoweit relativiert, dass die Nutzung durch Facebook trotz Löschung weiterhin möglich ist, wenn die einmal eingestellten Inhalte weiterhin mit anderen Nutzern geteilt werden und diese sie nicht gelöscht haben.[1031] Der Twitterbilderdienst Twitpic lässt sich sogar Nutzungsrechte zum Weiterverkauf der hochgeladenen Bilder einräumen.[1032]

3.1.9.10.4 Abhängigkeit der Nutzer vom Provider in Sicherheitsfragen

Keine klassische Bedrohung, jedoch cloudspezifisch und Folge der zentralen Bereitstellung sowie ebenfalls ein Aspekt des Kontrollverlusts, ist die verstärkte Abhängigkeit des Nutzers vom Cloudprovider in Sicherheitsfragen. Während bei eigener IT-Infrastruktur der Eigentümer diese nach eigenem Ermessen absichern kann, ist ein Cloudnutzer, insbesondere bei SaaS, kaum in der Lage eigene Sicherheitsmaßnahmen zu implementieren.[1033] Der Vorteil eines zentralen Patchmanagements durch den Provider wird dann zur Bedrohung, wenn dieser die notwendigen Sicherheitsupdates nicht oder nicht rechtzeitig durchführt.

Zusätzlich können Diskrepanzen zwischen beworbenen und tatsächlich vorhandenen Sicherheitsfeatures bestehen. Zertifizierungen und Audits durch externe Dritte

---

[1029] *Münch/Doubrava/Essoh*, DuD 2011, 324.

[1030] *Weis*, Bei Facebook ist nichts mehr sicher, http://www.tagesschau.sf.tv/Nachrichten/Archiv/2009/02/17/Vermischtes/Bei-Facebook-ist-nichts-mehr-sicher.

[1031] Siehe dazu ausführlich *Wagenknecht*, Facebook: was passiert mit unseren Bildern? – Ein Einblick in die Nutzungsbestimmungen, http://www.rechtambild.de/2011/05/facebook-was-passiert-mit-unseren-bildern-%E2%80%93-ein-einblick-in-die-nutzungsbestimmungen.

[1032] *Reißmann*, Twitpic reicht Nutzer-Fotos an Vermarkter weiter, http://www.spiegel.de/netzwelt/web/0,1518,761721,00.html; *Reißmann*, Twitpic lässt Nutzer im Unklaren, http://www.spiegel.de/netzwelt/web/0,1518,761838,00.html.

[1033] Solche Maßnahmen sind meist nur noch beim eigengenutzten Client möglich.

ermöglichen aber eine Einschätzung der beim Provider tatsächlich gepflegten Sicherheitskultur.

3.1.9.10.5 SoA-bedingte Bedrohungen

Eine Bedrohung, die auf dem SoA-Paradigma und dem damit einhergehenden Wiederverwenden und Kombinieren von Programmcode beruht, ist das entsprechend bezeichnete Problem des „Shared Code in Service-Oriented-Architectures". Verteilte Systeme, also auch Cloudsysteme „erben" dabei die Schwachstellen des bereits genutzten Programmcodes.[1034] Insbesondere die standardisierte und homogene Bereitstellung von Services in Clouds befördert dieses Problem. Auch die Portierung von lokalen Geschäftsprozesslösungen in Cloudumgebungen kann das Problem aufkommen lassen. Zum Beispiel dann, wenn ein Cloudanbieter seine Angebote nicht von Grund auf neu programmiert, sondern dem SoA-Gedanken folgend aus bereits vorhandenem Quellcode kombiniert.

Gegenmaßnahmen sind entweder der Verzicht auf die Wiederverwendung von älterem Code oder die Durchführung von Code Reviews zur Prüfung auf etwaige Sicherheitslücken oder Programmierfehler. Die Nutzung von Open Source kann bei der Überprüfung Vorteile bieten, da unter Umständen schon andere Personen den Quellcode geprüft und ausgebessert haben und zudem offener Code allgemein leichter überprüfbar ist, da dieser öffentlich verfügbar ist.

3.1.9.10.6 Bedrohungen für Rechtsgüter Dritter durch Clouddienste

Mit Cloud Computing ergeben sich nicht nur Bedrohungen für die in den Clouddiensten gespeicherten und verarbeiteten Daten, sondern auch Bedrohungen die von den Clouddiensten selbst ausgehen. So kann die beträchtliche Rechenleistung beispielsweise Brute-Force-Angriffe auf Sicherungsmechanismen wie Passwörter oder Schlüssel erheblich beschleunigen.[1035] Je nach Budget des Angreifers und Länge der Passwörter oder Schlüssel können dadurch sicher geglaubte Verschlüsselungsmaßnahmen in vergleichsweise kurzer Zeit umgangen werden.

Ein weiteres Szenario ist die, oft durch einen Angriff auf die Cloudinfrastruktur initiierte, Nutzung von Cloudressourcen zur Kontrolle oder „bedarfsgerechten" Erweiterung von illegalen Botnetzen oder zur Verteilung von Spam oder Malware.[1036]

[1034] *Rahmel*, Einführung in die Informationssicherheit, http://www.iis.uni-hildesheim.de/files/teaching/Wintersemester20062007/VorlesungIS/Folien/EIS-1-Informationssicherheit.pdf, dort Folie 10.

[1035] *Kremer*, WPA-PSK: Erfolgreicher Bruteforce dank Amazon-Cloud, http://www.gulli.com/news/wpa-psk-erfolgreicher-bruteforce-dank-amazon-cloud-2011-01-11; *Kremer*, Hacker demonstriert Bruteforce von SHA-1 in der Amazon-Cloud, http://www.gulli.com/news/hacker-erstellt-rainbow-tables-f-r-sha-1-in-der-amazon-cloud-2010-11-18.

[1036] So hat beispielsweise das Zeus-Botnet Ende 2009 Amazons EC2 infiltriert und die Cloudressourcen mit genutzt; siehe *Kremer*, Amazons Cloud-Dienst als Botnet-Server,

Dieser Missbrauch kann sogar Folgen für normale Cloudnutzer haben, wenn die IP-Adressbereiche (IP-Ranges) der vermeintlichen Botnetz- oder Spamserver von anderen Internetprovidern blockiert werden.[1037] Darunter kann im Extremfall die Verfügbarkeit eines kompletten Cloudangebots leiden. Oft ist es jedoch so, dass solche IP-Adressen, gerade wegen der hohen Bedeutung der Cloudservices, nur selten auf Blacklists landen und demzufolge die Cloudangebote für Botnetzbetreiber noch attraktiver werden.[1038]

3.1.9.11 Sicherheitskonzept

Die strukturierte und fortwährende Umsetzung von Sicherheitsmaßnahmen kann mittels eines konkreten Sicherheitskonzepts gewährleistet und gefördert werden.[1039] Bei einem solchen Vorgehen werden passgenaue Maßnahmen für identifizierte Bedrohungen ermittelt und unter regelmäßiger Prüfung des Erfolgs praktisch umgesetzt. Sicherheitskonzepte sind am effektivsten, wenn sie sich auf eine spezifische Einzelsituation oder -organisation mit ihren jeweiligen Besonderheiten beziehen.

Für Clouddienste aufzustellende Sicherheitskonzepte müssen, neben den jeweiligen providerspezifischen Eigenheiten, alle beteiligten Kommunikationsverhältnisse und Systeme im Blick behalten. Es reicht nämlich nicht aus, ein Teilsystem, zum Beispiel die Rechenzentren der Cloudprovider, höchst sicher zu gestalten, während der Datentransport oder die Handhabung beim Kunden erhebliche Schutzlücken offen lässt. Zum Beispiel die Fälle und Konstellationen, dass die Kommunikation abhörbar ist, sich Dritte als Kunden ausgegeben können oder über Clients der Nutzer Daten aus dem Cloudrechenzentrum abgegriffen werden.

Die Schwierigkeit der Absicherung ergibt sich damit aus dem Zusammenspiel der unterschiedlichen Beteiligten. Ein Cloudprovider kann nicht im Alleingang Sicherheit garantieren, wenn der Kunde nicht „mitspielt“. Auf Sicherheit bedachte Cloudnutzer müssen demnach ihr eigenes Nutzungsverhalten immer an das Sicherheitskonzept des Providers anpassen.[1040]

---

http://www.gulli.com/news/amazons-cloud-dienst-als-botnet-server-2009-12-10; auch der Angriff auf das Playstationnetwork Mitte 2011 soll unter anderem mit Hilfe der Amazoncloud erfolgt sein; siehe dazu *Karthaus*, PSN-Hack: Hacker nutzten angeblich Amazons Cloud für ihren Angriff, http://www.hddaily.de/2011/05/15/psn-hack-hacker-nutzten-angeblich-amazons-cloud-fur-ihren-angriff-29296.html.

[1037] Zur Problematik des Blacklistings von Cloudprovider-IP-Ranges siehe auch unten die Ausführungen zur „Essential-Facilities-Doktrin“ in Kap. 3.3.

[1038] *Kremer*, Amazons Cloud-Dienst als Botnet-Server, http://www.gulli.com/news/amazons-cloud-dienst-als-botnet-server-2009-12-10; weitere Beispiele für Bedrohungen durch Cloudservices siehe bei *Garfinkel*, Angriff aus der Wolke, http://www.heise.de/tr/artikel/Angriff-aus-der-Wolke-1363872.html.

[1039] Zum Sicherheitskonzept für TK-Unternehmen siehe Kap. 3.1.9.3.3.

[1040] Ähnlich *Tsvihun/Stephanow/Streitberger* 2010, 7.

3.1.10 Datenschutzaudit

Im Zusammenhang mit den Maßnahmen in § 9 BDSG samt Anlage ist § 9a BDSG zu sehen. Zielsetzung und Zweck der Regelung ist die Verbesserung des Datenschutzes und der Datensicherheit durch die Möglichkeit, Datenschutzkonzepte, Datenschutzmanagementsysteme und technische Einrichtungen durch unabhängige Gutachter überprüfen und bewerten zu lassen und das Ergebnis der Prüfung zu veröffentlichen.[1041] Die mit Hilfe von § 9 BDSG und der Anlage getroffenen Maßnahmen können durch externe Gutachter geprüft und die erfolgreiche Umsetzung zertifiziert werden. Ein weiteres Ziel der Regelung in § 9a BDSG ist die Förderung datenschutzfreundlicher Produkte und Dienstleistungen.[1042] Anbieter solcher Produkte und Dienstleistungen können mit dem erfolgreichen Audit werben.[1043] In diesem Zusammenhang ist ausdrücklich erwähnenswert, dass ein Datenschutzaudit kein Produktaudit darstellt und die Produkte oder Dienstleistungen lediglich im Rahmen der Auditierung eines konkreten Datenschutzkonzepts oder Datenschutzmanagementsystems (mit)geprüft werden. Streng genommen ist zwischen der Zertifizierung von Produkten (Produktaudit) und der Auditierung von Datenschutzmanagementsystemen (Systemaudit) zu unterscheiden.[1044]

Wie am Tatbestandsmerkmal „können“ ersichtlich ist, beinhaltet die Vorschrift keine zwingende Vorgabe, sondern überlässt es dem jeweiligen Anbieter, ob er sein Datenschutzkonzept mitsamt den technischen Einrichtungen auditieren lässt. Mit diesem auf Freiwilligkeit und damit auf Selbstregulierung basierenden Angebot an die Anbieter soll nach dem Willen der Länder in Anlehnung an das Umwelt-Audit-Verfahren die unternehmerische Selbstverantwortung eines Anbieters hinsichtlich der Beachtung des Gebots der Datenvermeidung und der Sicherung eines hohen Datenschutzniveaus betont werden.[1045] Die Freiwilligkeit umfasst auch die Beendigung des Datenschutzaudits. Es ist einem Anbieter unbenommen auf ein erneutes Audit zu verzichten.[1046]

Im Gegensatz zu ordnungsrechtlichen Stichproben ist das Datenschutzaudit auf die Sicherstellung einer kontinuierlichen Verbesserung des Datenschutzes und der Da-

---

[1041] *Roßnagel*, in: Hempel/Krasmann/Bröckling, Sichtbarkeitsregime – Überwachung, Sicherheit und Privatheit im 21. Jahrhundert, Leviathan Sonderheft 2010, 267; *Scholz*, in: Simitis, BDSG, § 9a, Rn. 1, 38; BT-Drs. 14/4329, 30, 38; zu den diversen Zertifikaten und Standards siehe Kap. 3.1.9.9.8.

[1042] *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 9a.

[1043] *Gola/Schomerus* 2010, § 9a, Rn. 1; *Scholz*, in: Simitis, BDSG, § 9a, Rn. 3; Zwischenbericht der Enquete-Kommission, BT-Drs. 11002, 104.

[1044] Näheres hierzu bei *Roßnagel*, in: Hempel/Krasmann/Bröckling, Sichtbarkeitsregime – Überwachung, Sicherheit und Privatheit im 21. Jahrhundert, Leviathan Sonderheft 2010, 267.

[1045] *Gola/Schomerus* 2010, § 9a, Rn. 1; *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 9a; BT-Drs. 14/1191, 14.

[1046] *Bizer*, in: Simitis, BDSG, 2006, § 9a, Rn. 38.

tensicherheit ausgerichtet und damit struktur- und insbesondere prozessbezogen.[1047] Es ist außerdem ein präventives Instrument des Datenschutzes, mit dem die Auswahl und Gestaltung datenvermeidender und datensparsamer Techniken sowie Lernprozesse zum Schutz der Daten gefördert werden.[1048] Ein Datenschutzaudit unterstützt zudem die öffentliche und betriebliche Datenschutzkontrolle und fördert und stärkt die Selbstverantwortung des Datenverarbeiters für den Schutz der ihm anvertrauten Daten.[1049]

Gerade Cloudprovider können mit einer solchen auf Kontinuität ausgelegten Überprüfung der getroffenen Maßnahmen ihre Vertrauenswürdigkeit und die Akzeptanz ihrer Angebote bei den Kunden stärken, weil letztere in der Praxis äußerst selten oder nie die Einhaltung von Sicherheitsmaßnahmen überprüfen können. Zudem sind Wettbewerbsvorteile gegenüber unzertifizierten Anbietern, wie oben bereits angedeutet, gesetzlich intendiert.[1050]

Auch die internationale Akzeptanz von ehemals nationalen Auditverfahren ist nicht selten. So könnten gerade im Cloudumfeld nationale oder europäische Auditverfahren mittelfristig auch beispielsweise in den USA und anderen Staaten akzeptiert werden. Neben Wettbewerbsvorteilen stehen dann zusätzlich Standortvorteile für zertifizierte Anbieter im Raum. Umgekehrt können ausländische Anbieter, zum Beispiel Cloudprovider, ihre Produkte und Dienstleistungen nach deutschem Recht zertifizieren lassen und auf dem nationalen oder internationalen Markt damit werben.[1051]

Das in § 9a Satz 2 BDSG erwähnte und das Auditverfahren konkretisierende Ausführungsgesetz ist bisher noch nicht verabschiedet.[1052] Der Entwurf des sogenannten „Bundesdatenschutzauditgesetzes“[1053] wurde vom federführenden Bundesinnenministerium in einem Paket mit weiteren datenschutzrechtlich relevanten Vorschriften als sogenanntes „Gesetz zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften“ vorgelegt, jedoch beschloss der

---

[1047] *Scholz*, in: Simitis, BDSG, § 9a, Rn. 4; BT-Drs. 14/1191, 14; nach *Roßnagel*, in: Hempel/Krasmann/Bröckling, Sichtbarkeitsregime – Überwachung, Sicherheit und Privatheit im 21. Jahrhundert, Leviathan Sonderheft 2010, 266, 267 auch in Abgrenzung zu einem lediglich statischen und objektbezogenen Produktaudit.

[1048] *Scholz*, in: Simitis, BDSG, § 9a, Rn. 7; Zum Aspekt als Lernsystem siehe *Roßnagel*, in: Hempel/Krasmann/Bröckling, Sichtbarkeitsregime – Überwachung, Sicherheit und Privatheit im 21. Jahrhundert, Leviathan Sonderheft 2010, 266 f.

[1049] *Roßnagel*, in: Hempel/Krasmann/Bröckling, Sichtbarkeitsregime – Überwachung, Sicherheit und Privatheit im 21. Jahrhundert, Leviathan Sonderheft 2010, 266.

[1050] *Gola/Schomerus* 2010, § 9a, Rn. 1; *Scholz*, in: Simitis, BDSG, § 9a, Rn. 6.

[1051] *Scholz*, in: Simitis, BDSG, § 9a, Rn. 6.

[1052] Die Verabschiedung eines Datenschutzauditgesetzes hat *Roßnagel* bereits in einem unveröffentlichten Gesetzentwurf im Jahr 1999 gefordert; siehe dazu *Roßnagel* 2000, 1 ff. und *Roßnagel/Pfitzmann/Garstka* 2001, 134 f.

[1053] BT-Drs. 16/12011.

Deutsche Bundestag am 3.7.2009 das Auditgesetz nicht zu verabschieden, nachdem es zwei Tage zuvor schon vom Innenausschuss aus dem Gesetzentwurfspaket herausgenommen wurde. Die restlichen datenschutzrechtlichen Vorschriften wurden am gleichen Tag als „Gesetz zur Änderung datenschutzrechtlicher Vorschriften" vom Bundestag verabschiedet.[1054] Zu diesen Vorschriften gehörte im Übrigen auch der neu strukturierte § 11 BDSG.

Für Cloud Computing wird das externe Audit einen erheblichen Bedeutungsgewinn erleben. Angesichts der faktischen Unmöglichkeit der persönlichen Überprüfung durch den Auftraggeber, wird es das Mittel der Wahl sein, um die Voraussetzungen des § 11 BDSG praktisch umsetzen zu können.[1055]

3.1.11 Verpflichtung der Mitarbeiter auf das Datengeheimnis

Neben den technisch-organisatorischen Maßnahmen ist § 5 BDSG, die Verpflichtung auf das Datengeheimnis der bei der datenverarbeitenden Stelle Beschäftigten, ein wichtiger Aspekt in einem ganzheitlichen Sicherheitskonzept.

Der Begriff des Datengeheimnisses ist in § 5 Satz 1 BDSG legaldefiniert und bedeutet, dass den bei der Datenverarbeitung beschäftigten Personen untersagt ist, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Satz 2 schließt mit dem Gebot an, dass diese Personen bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten sind. Die Verpflichtung muss in jedem Einzelfall und persönlich erfolgen.[1056] Sie richtet sich demzufolge an natürliche Personen und greift unabhängig von der Qualifikation und der Wirksamkeit des zwischen den Beschäftigten und der verantwortlichen oder verarbeitenden Stelle bestehenden Rechtsverhältnisses.[1057]

Das Datengeheimnis gilt neben anderen Berufs- oder Amtsgeheimnissen und lässt diese unberührt.[1058] Allerdings ist es zum allgemeinen Amtsgeheimnis aus § 67 Abs. 1 BBG und den entsprechenden Landesgesetzen die speziellere Norm.

Die Bezeichnung als „Datengeheimnis" hat nicht nur die aus dieser Bezeichnung ableitbaren Verbote der Weitergabe und Offenbarung von Daten zum Inhalt, sondern betrifft alle Phasen der Datenverarbeitung, mithin auch die unberechtigte Erhebung, Speicherung, Veränderung, Sperrung, Löschung oder jede andere Art und Weise unzulässiger Verwendung.[1059] Erst mit Beendigung der Tätigkeit gemäß Satz 3 wird daraus ein Verbot der Weitergabe und Offenbarung, da der Mitarbeiter üblicherweise mit dem Ausscheiden die anderen unzulässigen Verarbeitungsfor-

---

[1054] BT-Drs. 16/13657.
[1055] *Weichert*, DuD 2010, 683; siehe dazu auch Kap. 3.1.8.5.1.
[1056] *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 5, Rn. 6.
[1057] *Ehmann*, in: Simitis, BDSG, § 5, Rn. 5, 6, 14.
[1058] *Ehmann*, in: Simitis, BDSG, § 5, Rn. 7.
[1059] *Ehmann*, in: Simitis, BDSG, § 5, Rn. 21.

men, zum Beispiel die unzulässige Speicherung oder Veränderung, mangels Zugangs zu den Datenbeständen nicht mehr durchführen kann.[1060] Das Datengeheimnis gilt somit gemäß § 5 Satz 3 BDSG auch nach Beendigung des Be-Beschäftigungsverhältnisses fort.

Bei Cloud Computing betrifft die Vorschrift die Beschäftigten in den Rechenzentren eines Providers. Soweit also ein Cloudprovider in Deutschland ansässig ist, hat dieser das Gebot zur einzelnen und persönlichen Verpflichtung seiner Mitarbeiter auf das Datengeheimnis zu beachten. Auch Auftragnehmer bei einer Auftragsdatenverarbeitung sind gemäß § 11 Abs. 4 Satz 1 BDSG dieser Verpflichtung unterworfen, so dass auch hieraus deutsche Cloudprovider zur Geheimniswahrung durch ihre Mitarbeiter verpflichtet sind. Es hat außerdem Bedeutung im Zusammenhang mit der Übermittlung von Daten in Drittstaaten (§§ 4b, 4c BDSG) und der Verarbeitung sensitiver Daten im Sinne von § 3 Abs. 9 BDSG.[1061]

Die Belehrung über das Datengeheimnis besteht aus zwei Teilen. Sie muss zum einen eine hinreichende Information beinhalten, was genau die Pflicht zur Wahrung des Datengeheimnisses konkret und tätigkeitsspezifisch beinhaltet und zum anderen auf drohende Schadenersatzforderungen sowie auf mögliche Sanktionen arbeits-, dienst- und strafrechtlicher Natur hinweisen, die aus einem Verstoß gegen das Datengeheimnis resultieren können.[1062] Zusätzlich ist die Aufforderung, das Datengeheimnis stets gewissenhaft zu wahren, erforderlich.[1063]

Die Befugnis zum Datenumgang ergibt sich aus den intern zugewiesenen Zugriffsberechtigungen. Jede Datennutzung ist unbefugt, die nicht in der dem Mitarbeiter zugewiesenen Aufgabenstellung liegt, selbst wenn die Verarbeitung aus der Sicht der verantwortlichen Stelle rechtmäßig ist.[1064] Eine Nutzung ist immer unbefugt, wenn sie rechtswidrig ist. Die Rechtswidrigkeit kann sich nicht nur aus datenschutzrechtlichen, sondern auch aus anderen rechtlichen Vorgaben ergeben.[1065]

Bei Zuwiderhandlungen gegen das Datengeheimnis können auch Strafen für die dagegen verstoßenden Mitarbeiter in Betracht kommen. Eine Strafbarkeit ergibt sich insbesondere aus § 44 BDSG und §§ 203, 206 StGB.[1066] Die Verfolgung einer solchen Straftat erfolgt allerdings nur auf Antrag.[1067]

[1060] *Ehmann*, in: Simitis, BDSG, § 5, Rn. 32.

[1061] *Ehmann*, in: Simitis, BDSG, § 5, Rn. 3.

[1062] *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 5, Rn. 6; zu einschlägigen Strafnormen siehe sogleich.

[1063] *Ehmann*, in: Simitis, BDSG, § 5, Rn. 28.

[1064] *Gola/Schomerus* 2010, § 5, Rn. 6.

[1065] *Gola/Schomerus* 2010, § 5, Rn. 5.

[1066] *Gola/Schomerus* 2010, § 5, Rn. 2.

[1067] *Ambs*, in: Erbs/Kohlhaas/Ambs, Strafrechtliche Nebengesetze, BDSG, § 5, Rn. 3 und 7; *Ehmann*, in: Simitis, BDSG, § 5, Rn. 34.

3.1.12 Datenübermittlung ins außereuropäische Ausland

Neben datenschutzrechtlichen Kollisionsnormen und Fragen des räumlichen Anwendungsbereichs betrifft Cloud Computing auch und gerade datenschutzrechtliche Fragen, wenn Daten ins Ausland übermittelt werden sollen.[1068] Ein solcher grenzüberschreitender Datenverkehr gestaltet sich besonders schwierig, wenn das Zielland des Datentransfers ein Staat im außereuropäischen Ausland ist. Bei einer elektronischen Übersendung personenbezogener Daten in Staaten, die nicht der EU oder dem EWR angehören, liegt eine datenschutzrechtliche Übermittlung vor, die, genau wie die anschließende Nutzung der Daten im Ausland, einer besonderen Rechtfertigung bedarf. Für eine solche Übermittlung und Nutzung ist demnach ein Erlaubnistatbestand als Zulässigkeitsvoraussetzung notwendig, soweit nicht eine Einwilligung des Betroffenen vorliegt. Dies entspricht der Rechtslage gemäß § 4 Abs. 1 BDSG und gilt, wie mehrfach erwähnt, allgemein und immer im Umgang mit Daten, unabhängig von einem internationalen Bezug.[1069]

Als Erlaubnisnormen kommen für öffentliche Stellen § 16 Abs. 1 BDSG und für nicht-öffentliche Stellen die allgemeinen Zulässigkeitsvorschriften gemäß §§ 28 ff. BDSG in Betracht. Eine Besonderheit bei § 28 BDSG ist die Verquickung der Interessenabwägung aus den Erlaubnisnormen, zum Beispiel § 28 Abs. 1 Satz 1 Nr. 2 BDSG, mit der aus § 4b Abs. 2 Satz 2 Halbsatz 1 BDSG.[1070] § 4b Abs. 2 Satz 2 Halbsatz 1 BDSG zufolge unterbleibt eine Übermittlung, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Ein solches entgegenstehendes schutzwürdiges Interesse ist gemäß § 4b Abs. 2 Satz 2 Halbsatz 2 BDSG insbesondere dann anzunehmen, wenn bei den empfangenden Stellen ein angemessenes Datenschutzniveau nicht gegeben ist. Neben dem Schutzniveau können demzufolge auch andere schutzwürdige Interessen des Betroffenen einer Datenübermittlung in Drittländer entgegenstehen.[1071] Fehlt es an einem angemessenen Schutzniveau, so sind allerdings die Ausnahmen nach § 4c Abs. 1 Nr. 1 bis 6 und gemäß Abs. 2 BDSG zu beachten, die ein solches Fehlen des Niveaus kompensieren.

Aus der Gesetzessystematik ergibt sich demnach ein zweistufiger Prüfungsaufbau, der in der zweiten Stufe die oben angeführten Fragen des angemessenen Datenschutzniveaus und die möglichen Ausnahmen dazu beinhaltet.[1072] Bei der zweistufigen Prüfung ist zu beachten, dass Fragestellungen der zweiten Stufe bereits bei der

---

[1068] Zu ersteren Aspekten siehe die Ausführungen in Kap. 3.4.

[1069] Siehe dazu insbesondere Kap. 3.1.6.1.

[1070] Zu Einzelheiten hierzu siehe sogleich Kap. 3.1.12.1.4

[1071] *Gola/Schomerus* 2010, § 4b, Rn. 8.

[1072] *Simitis*, in: Simitis, BDSG, § 4b, Rn. 38, 39; *Gola/Schomerus* 2010, § 4c, Rn. 3; *Duisberg*, in: Picot/Götz/Hertz, Trust in IT, 63.

Prüfung der Interessenabwägung auf der ersten Stufe von Bedeutung sein können, so dass es regelmäßig zu einer Überschneidung der Prüfungsebenen kommt.[1073]

3.1.12.1 Erlaubnisnormen und Zusammenwirken mit §§ 4b und 4c BDSG

Im ersten Prüfungsschritt muss demzufolge geprüft werden, ob die üblichen Erlaubnistatbestände eingreifen. Die grenzüberschreitende Übermittlung ist zunächst also nach den Maßstäben zu beurteilen, die auch an inländische oder innereuropäische Übermittlungen anzulegen sind.[1074] Durch § 4b BDSG werden allerdings die, bei direkter Anwendung der Erlaubnisvorschriften, inländischen Empfänger der Übermittlung durch eine entsprechende Anwendung der Vorschrift in ausländische Empfänger modifiziert. Die Voraussetzungen der Erlaubnistatbestände sind aber weiterhin die gleichen, zusätzlich um die spezielleren Voraussetzungen aus den §§ 4b und 4c ergänzt.

In der Literatur wird allerdings auch die Auffassung vertreten, dass die Ausnahmen in § 4c Abs. 1 BDSG eigenständige Erlaubnisnormen darstellen. Diese Ausnahmen in Abs. 1 sollen demnach aus sich heraus die Zulässigkeit einer Übermittlung begründen.[1075] Diese Auffassung ist aber wegen der systematischen Stellung, insbesondere im Zusammenhang mit § 4b BDSG, dem Wortlaut der Vorschrift („auch wenn bei ihnen ein angemessenes Datenschutzniveau nicht gewährleistet ist“) sowie dem Wortlaut des zugrundeliegenden Art. 26 DSRL („Drittland, das kein angemessenes Schutzniveau im Sinne des Artikels 25 Absatz 2 gewährleistet“) abzulehnen.

3.1.12.1.1 Öffentliche und nichtöffentliche Stellen als Übermittler

§ 4b Abs. 2 Satz 1 BDSG ordnet im Wortlaut die entsprechende Anwendung des Abs. 1 an, der wiederum auf § 16 Abs. 1 BDSG verweist, so dass auch im Gesetz der zweistufige Prüfungsaufbau angelegt ist. Auch § 4b Abs. 4 BDSG nimmt auf § 16 BDSG Bezug.

§ 16 BDSG hat für öffentliche Stellen des Bundes, also Bundesbehörden im Sinne des § 12 Abs. 1 BDSG, Bedeutung. Für öffentliche Stellen der Länder muss im Übrigen das jeweilige Datenschutzrecht des Landes herangezogen werden, in Hessen zum Beispiel § 17 HDSG. Bei einer direkten Anwendung regelt § 16 BDSG die Übermittlung personenbezogener Daten durch eine öffentliche Stelle an nichtöffentliche Stellen. Durch die entsprechende Anwendung gemäß § 4b Abs. 2 Satz 1 i.V.m. Abs. 1 BDSG ist eine Übermittlung durch eine öffentliche Stelle an ausländische oder über- oder zwischenstaatliche Stellen gemeint. Diese Vorschriften betreffen demnach die Nutzung von ausländischen Clouds durch deutsche Behörden, soweit personenbezogene Daten betroffen sind.

[1073] *Gola/Schomerus* 2010, § 4c, Rn. 3; siehe dazu den soeben erwähnten Aspekt der Verquickung der Interessenprüfungen.

[1074] *Simitis*, in: Simitis, BDSG, § 4b, Rn. 38, 39; *Scholz/Lutz*, CR 2011, 427.

[1075] *Duisberg*, in: Picot/Götz/Hertz, Trust in IT, 63.

Entsprechend zu § 16 BDSG sind die §§ 28 ff. BDSG in Verbindung mit § 4b Abs. 2 Satz 1 i.V.m. Abs. 1 BDSG so zu lesen, dass nicht-öffentliche Stellen an ausländische oder über- oder zwischenstaatliche Stellen personenbezogene Daten übermitteln. Diese Konstellation umfasst demnach die Fälle, dass deutsche Unternehmen personenbezogene Daten in ausländische Clouds übermitteln.

3.1.12.1.2 Erforderlichkeit

Bevor auf mögliche Interessenabwägungen abgestellt werden kann, ist gemäß § 16 Abs. 1 Nr. 1 und § 28 Abs. 1 Nr. 1 und 2 Halbsatz 1 BDSG zu prüfen, ob eine Übermittlung ins außereuropäische Ausland überhaupt erforderlich ist.

In den allermeisten Fällen scheitert eine Übermittlung in eine außereuropäische Cloud aber bereits an der Erforderlichkeit im Sinne des § 28 Abs. 1 Nr. 1 und 2 Halbsatz 1 BDSG. Gleiches gilt für die Erforderlichkeit gemäß § 16 Abs. 1 Nr. 1 BDSG bei öffentlichen Stellen. Es ist nämlich nicht zwingend notwendig, Clouddienste außerhalb des EU- und EWR-Raums zu nutzen, da es für die meisten Bedürfnisse der Cloudnutzer vermehrt auch innerhalb Europas adäquate Cloudangebote gibt. Der Umstand, dass außereuropäische Cloudangebote möglicherweise kostengünstiger sind, genügt für die Erforderlichkeit nicht.[1076]

3.1.12.1.3 Weitere Voraussetzungen

Fehlt es allerdings an adäquaten europäischen Clouddiensten oder ist die Inanspruchnahme ausländischer Anbieter aus anderen Gründen erforderlich, so sind die weiteren Voraussetzungen in § 16 Abs. 1 Nr. 1 und 2 oder § 28 Abs. 1 Nr. 1 und 2 BDSG zu prüfen.

§ 16 Abs. 1 Nr. 1 BDSG erlaubt die Übermittlung, wenn neben der Erforderlichkeit zur Aufgabenerfüllung die Voraussetzungen zur Nutzung nach § 14 BDSG vorliegen. § 16 Abs. 1 Nr. 2 BDSG regelt den Fall, dass der Dritte an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten hat. Für Cloud Computing ist diese Erlaubnisalternative allerdings nie einschlägig, da ein solcher Dritter der Cloudprovider wäre und dieser kein Interesse an den an ihn übermittelten Daten hat.

Nach § 28 Abs. 1 Nr. 1 BDSG muss sich die Erforderlichkeit der Übermittlung auf die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses zwischen Cloudnutzer und Betroffenem beziehen. In der Regel werden aber keine unmittelbaren vertraglichen Regelungen zwischen dem Cloudnutzer und dem Betroffenen hinsichtlich der Übermittlung von personenbezogenen Daten des Betroffenen in eine außereuropäi-

[1076] *Weichert*, DuD 2010, 683.

sche oder überhaupt eine irgendwie geartete Cloud bestehen.[1077] Deswegen wird in der Regel § 28 Abs. 1 Nr. 2 BDSG als Erlaubnisnorm heranzuziehen sein.

Die Erforderlichkeit bei § 28 Abs. 1 Nr. 2 BDSG bezieht sich auf die Wahrung berechtigter Interessen der verantwortlichen Stelle, also des cloudnutzenden Unternehmens. Unterstellt man dieses Interesse mit obigen Erwägungen, also zum Beispiel beim Fehlen adäquater europäischer Clouds, so muss man das schutzwürdige Interesse des Betroffenen am Ausschluss einer solchen Übermittlung in eine außereuropäische Cloud betrachten. Dabei ist § 4b Abs. 2 Satz 2 BDSG zu beachten.

3.1.12.1.4 Interesse des Betroffenen an einem Ausschluss der Übermittlung

Während § 28 Abs. 1 Nr. 2 BDSG eine Abwägung zwischen den Interessen des Betroffenen und der verantwortlichen Stelle vorsehen („überwiegt“), beschränkt sich § 4b Abs. 2 Satz 2 BDSG alleinig auf das Interesse des Betroffenen an einem Ausschluss der Übermittlung („hat“), ohne eine Interessenabwägung vorzusehen.[1078]

§ 28 Abs. 1 Nr. 2 BDSG wird also durch § 4b Abs. 2 Satz 2 BDSG insoweit modifiziert, dass keine Interessenabwägung stattfindet und ein Interesse des Betroffenen am Ausschluss der Übermittlung immer vorrangig ist.[1079] Hierdurch wird der zweistufige Prüfungsaufbau durchbrochen. Die Prüfung des Interesses an einem Ausschluss der Übermittlung muss daher nur einmalig erfolgen.

§ 28 Abs. 2 Nr. 2 BDSG, § 29 Abs. 1 Nr. 1 BDSG und § 16 Abs. 1 Nr. 2 BDSG lassen ebenfalls ein schutzwürdiges Interesse des Betroffenen am Ausschluss der Übermittlung ausreichen, ohne dass eine Abwägung der Interessen nötig wäre. Eine Modifizierung durch § 4b Abs. 2 Satz ist bei diesen Vorschriften also nicht nötig, so dass die Durchbrechung der zweistufigen Prüfung im Vergleich zu § 28 Abs. 1 Nr. 2 BDSG noch deutlicher wird. Das Interesse des Betroffenen am Ausschluss der Übermittlung im Rahmen der Erlaubnisnorm bedeutet gleichzeitig die Tatbestandserfüllung von § 4b Abs. 2 Satz 2 BDSG.

[1077] *Weichert*, DuD 2010, 683.

[1078] § 28 Abs. 1 Nr. 2 spricht im Zusammenhang mit dem Betroffeneninteresse im Übrigen nur von „Verarbeitung oder Nutzung“ und nicht unmittelbar von Übermittlung. Da jedoch die Gesamtumstände zu betrachten sind (*Gola/Schomerus* 2010, § 28, Rn. 27), ist auch die vorgelagerte Übermittlung als Datenumgangsform gemeint. Dies ergibt sich im Übrigen auch aus der Formulierung zu Beginn des § 28 Abs. 1 Satz 1 BDSG, wonach dieser „das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke“ regelt. Letztlich kommt es aber auf die Frage des Umgangs auch nicht an, wie sogleich zu sehen ist, da § 4b Abs. 2 Satz 2 BDSG als Spezialnorm abschließend wirkt.

[1079] Der gleichen Ansicht wohl *Simitis*, in: Simitis, BDSG, § 4b, Rn. 45, der allgemein von einer „letztlich allein entscheidenden Zulässigkeitsbedingung“ spricht.

3.1.12.1.5 Einwilligung

Die datenschutzrechtlichen Beschränkungen können in der überwiegenden Mehrzahl der Anwendungsfälle durch die Einwilligung des Betroffenen aufgehoben werden und damit die Verarbeitung, Speicherung oder einen sonstigen Datenumgang erlauben. Erforderlich ist jedoch, dass der Betroffene den Zweck, den detaillierten Sachverhalt und die konkreten Umstände der Datenverarbeitung kennt und die Einwilligung freiwillig, also ohne sozialen oder wirtschaftlichen Druck, erfolgt.[1080] Als Spezialvorschrift im internationalen Kontext, die die Einwilligung des Betroffenen regelt, ist § 4c Abs. 1 Nr. 1 BDSG anzusehen.[1081]

3.1.12.1.6 Zwischenergebnis

In der Regel ist eine Übermittlung von personenbezogenen Daten in außereuropäische Clouds rechtlich unzulässig. Die Interessen der Betroffenen dürften regelmäßig dahin tendieren, die Übermittlung zu unterlassen. Sehr oft wird die Übermittlung schon vorher an der fehlenden Erforderlichkeit einer außereuropäischen Auslagerung scheitern, da es meistens auch passende rein europäische Cloudangebote gibt.

Die Angemessenheit des Datenschutzniveaus und die Ausnahmen nach § 4c BDSG, die im Anschluss dargestellt werden sollen, werden nur dann relevant, wenn diese eben genannten Voraussetzungen der Erlaubnisnormen eingehalten wurden, mithin also die Übermittlung zulässig ist.

3.1.12.2 Besondere Arten personenbezogener Daten

In § 3 Abs. 9 BDSG werden besonders sensitive Angaben unter dem Begriff „besondere Arten von personenbezogenen Daten“ erwähnt, die unter anderem gemäß § 28 Abs. 6 ff. und § 29 Abs. 5 BDSG nur unter engen Vorgaben zu den dort geregelten Zwecken erhoben, verarbeitet, genutzt oder übermittelt werden dürfen. Die Erhebung, Verarbeitung und Nutzung von Daten aus bestimmten Datenkategorien unterliegt damit besonderen Restriktionen.[1082] Der Wortlaut der Vorschrift erwähnt als solche Datenkategorien enumerativ und abschließend Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder das Sexualleben.

Neben den §§ 28, 29 BDSG werden die besonderen Arten personenbezogener Daten noch in weiteren Vorschriften des BDSG erwähnt. Die Erhebung solcher Daten ist in § 13 Abs. 2 BDSG geregelt und enthält diverse Zulässigkeitsvoraussetzungen, zum Beispiel das Erfordernis der Einwilligung des Betroffenen (§ 13 Abs. 2 Nr. 2 BDSG) gemäß § 4a Abs. 3 BDSG.

[1080] *Harder/Maruhn* 2010, 62.
[1081] Siehe dazu auch Kap. 3.1.12.5.
[1082] *Gola/Schomerus* 2010, § 3, Rn. 56.

Dabei ist zu beachten, dass sich die Einwilligung gemäß § 4a Abs. 3 BDSG ausdrücklich auf solche Daten im Sinne des § 3 Abs. 9 BDSG beziehen muss, soweit mit solchen Daten umgegangen wird. Außerdem ist die Schriftform und die Benennung der Daten im Einwilligungstext erforderlich.[1083] Das zwingende Schriftformerfordernis soll der Sensitivität der Daten gerecht werden.[1084]

Eine Ausnahme vom Einwilligungserfordernis nach § 4a BDSG postuliert § 28 Abs. 6 BDSG beim Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten für eigene Geschäftszwecke in den Nr. 1 bis 4, zum Beispiel Daten, die der Betroffene offenkundig veröffentlicht hat (Nr. 2). Auch wenn die Daten für die wissenschaftliche Forschung benötigt werden und diese Forschungen das Interesse des Betroffenen am Ausschluss der Daten überwiegen (Nr. 4) ist die Einwilligung nicht nötig. Weitere Regelungen finden sich in § 28 Abs. 7 bis 9 BDSG. Gemäß § 29 Abs. 5 BDSG gelten die Absätze 6 bis 9 des § 28 BDSG entsprechend auch bei § 29 BDSG.

Für öffentliche Stellen gibt es Regelungen zu besonderen Arten personenbezogener Daten in § 14 Abs. 5 und 6 BDSG sowie § 16 Abs. 1 Nr. 2 Satz 2 BDSG, die auf die erwähnten Voraussetzungen in § 13 Abs. 2 Nr. 1 bis 7 und Nr. 9 BDSG verweisen. Diese sind ähnlich restriktiv, wie die Voraussetzungen in § 28 Abs. 6 BDSG.

Die Auslagerung von sensitiven Daten im Sinne des § 3 Abs. 9 BDSG ist somit in Cloudumgebungen, die nicht als Auftragsdatenverarbeitung klassifiziert werden kann, erheblich erschwert. Das auslagernde Unternehmen muss sich die schriftliche Einwilligung der Betroffenen geben lassen oder einen der sehr restriktiven Ausnahmetatbestände erfüllen.[1085]

3.1.12.3 Bereichsspezifische Vorschriften außerhalb des BDSG

Bereichsspezifische Regelungen zum Datentransfer ins Ausland finden sich beispielsweise in § 92 TKG oder § 77 SGB X. § 92 TKG erlaubt eine Übermittlung ins Ausland nur dann, wenn diese für die Erbringung von Telekommunikationsdiensten, für die Erstellung oder Versendung von Rechnungen oder für die Missbrauchsbekämpfung erforderlich ist. Im Sozialrecht ist § 77 SGB X einschlägig.[1086] Während sich § 77 Abs. 1 und 2 SGB X an der Parallelvorschrift des § 4b BDSG orientieren, ist § 77 Abs. 3 Satz 1 SGB X eher mit § 4c BDSG vergleichbar, wobei die sozialrechtlichen Aspekte im Vordergrund stehen. Die Ähnlichkeit des § 77 Abs. 3 SGB X zu § 4b BDSG kommt durch die dort ebenfalls zu beachtenden Interessen des Betroffenen am Ausschluss einer Übermittlung zum Vorschein. Ähnlich wie in § 4b Abs. 2 BDSG ist in § 77 Abs. 2 und 3 SGB X die Angemessenheit des

---

[1083] *Gola/Schomerus* 2010, § 3, Rn. 57 und § 4a, Rn. 16a.
[1084] *Gola/Schomerus* 2010, § 4a, Rn. 16a.
[1085] Siehe dazu auch weiter unten Kap. 3.1.12.6.
[1086] Näheres dazu siehe bei *Steinbach*, NZS 2002, 21 f.

Datenschutzniveaus ein Aspekt, der Einfluss auf die Zulässigkeit einer Übermittlung ausübt.

3.1.12.4 Angemessenheit des Datenschutzniveaus als Interessensaspekt

Nach § 4b Abs. 2 Satz 2 BDSG überwiegt das schutzwürdige Interesse an dem Ausschluss der Übermittlung insbesondere dann, wenn ein angemessenes Datenschutzniveau im Empfängerland nicht gewährleistet ist. Diese Angemessenheit des Schutzniveaus wird in § 4b Abs. 3 BDSG präzisiert. Die Angemessenheit „wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen von Bedeutung sind." Kriterien sind gemäß § 4b Abs. 3 Halbsatz 2 BDSG die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen.[1087]

Ein zum EWR vergleichbares Niveau gibt es in der Schweiz, Kanada, Argentinien, Guernsey, Jersey und der Isle of Man.[1088] Seit dem 31.1.2011 zählt auch Israel dazu.[1089] Die restlichen Staaten sind sogenannte „Drittstaaten".[1090] Im Vergleich zur EU, dem EWR und Deutschland besteht zu diesen (unsicheren) Drittstaaten ein „Datenschutzgefälle".[1091]

3.1.12.5 Ausnahmen gemäß § 4c BDSG

Nach § 4c BDSG ist es ausnahmsweise möglich Daten in Drittstaaten ohne angemessenes Datenschutzniveau zu übermitteln, wenn die dort aufgeführten Voraussetzungen und Ausnahmetatbestände erfüllt sind.

In § 4c Abs. 1 Satz 1 Nr. 1 BDSG findet sich die Ausnahme, wonach die Übermittlungsmöglichkeit in Staaten ohne ausreichendes Datenschutzniveau dann zulässig ist, wenn die Einwilligung des Betroffenen vorliegt. Diese muss, wie ansonsten auch, den Anforderungen des § 4a BDSG genügen.

[1087] *Erd*, K&R 2010, 625.

[1088] *Pohle/Ammann*, CR 2009, 277; *Erd*, K&R 2010, 625; diese werden zum Teil auch als „sichere Drittstaaten" bezeichnet; die Entscheidung über die Angemessenheit des Datenschutzniveaus trifft die EU-Kommission (sogenannte „Adäquanzentscheidungen"); für Israel siehe beispielsweise den Beschluss gemäß der nachfolgenden Fußnote.

[1089] Beschluss der Kommission vom 31.1.2011 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus im Staat Israel im Hinblick auf die automatisierte Verarbeitung personenbezogener Daten, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:027:0039:0042:DE:PDF.

[1090] Auch als „Drittländer" oder, in Abgrenzung zu den „sicheren Drittstaaten", als „unsichere Drittstaaten" bezeichnet; diese Unterscheidung wird insbesondere später bei der Frage der Europarechtswidrigkeit von § 3 Abs. 8 Satz 3 BDSG relevant; siehe dazu Kap. 3.1.12.6.

[1091] *von Sponeck*, CR 1992, 596.

Oft ist in der späteren Praxis der Umstand problematisch, dass beim Erheben der Daten, der Aspekt der außereuropäischen Übermittlung noch nicht abzusehen ist und der Betroffene folglich auch nicht einwilligen kann. In Betracht kommt aber eine (nachträgliche) Einholung der Einwilligung bevor eine Auslagerung der bereits erhobenen Daten in eine Cloud in Erwägung gezogen wird.

§ 4c Abs. 1 Satz 1 Nr. 2 BDSG betrifft die Ausnahme, dass die Übermittlung für die Erfüllung eines Vertragsverhältnisses zwischen verantwortlicher Stelle und Betroffenem erforderlich ist. Wie erwähnt, ist in Cloudkonstellationen jedoch vorab nur selten klar, dass die erhobenen Daten in die Cloud verlagert werden sollen, so dass die spätere Übermittlung für das Vertragsverhältnis keine Rolle spielt.

In Cloudkonstellationen könnte § 4c Abs. 1 Satz 1 Nr. 3 BDSG bedeutsam sein. Demnach ist eine Übermittlung ins außereuropäische Ausland zulässig, wenn diese Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen wurde, erforderlich ist.

Dreh- und Angelpunkt ist die Klärung der Frage, ob der Abschluss des Vertrages zwischen dem Cloudnutzer als verantwortliche Stelle und dem Cloudprovider als Dritten im Interesse des Betroffenen liegt. Ein solches Interesse soll nach Art. 26 Abs. 1 lit. c) DSRL dann vorliegen, wenn der Betroffene begünstigt wird, beispielsweise, wenn ein Vertrag zugunsten Dritter vorliegt.[1092] Eine Auslagerung der Daten begünstigt jedoch nicht die Betroffenen, sondern den Cloudnutzer, so dass die Ausnahme nicht eingreift.

Die Ausnahmen in § 4c Abs. 1 Satz 1 Nr. 4 bis 6 BDSG sind hingegen kaum auf Cloud Computing beziehbar. Allenfalls § 4c Abs. 1 Satz 1 Nr. 4 Alt. 1 BDSG, nämlich die Wahrung eines öffentlichen Interesses, könnte für Behörden einschlägig sein. Die Vorschrift ist restriktiv auszulegen, so dass das Interesse von erheblichem Gewicht sein muss.[1093] Als Beispiel wäre denkbar, dass Rechenleistung oder Speicherplatz für eine Behörde nicht ausreichend vorhanden ist, um kurzfristig und möglichst schnell ein Problem zu lösen und damit eine Gefahr für überragende Rechtsgüter nicht anders abwendbar ist, als durch die Inanspruchnahme eines leistungsfähigen ausländischen Public-Cloudanbieters.

Für Cloud Computing bedeutet dies zusammenfassend, dass nur selten Ausnahmetatbestände eingreifen und oft nur eine auf Freiwilligkeit basierende Einwilligung der Betroffenen die Datenübermittlung ins Ausland ermöglicht.

Weitere wichtige und vor allem praxisrelevante, allerdings genehmigungspflichtige, Ausnahmen finden sich in § 4c Abs. 2 Satz 1 BDSG. Der Vorschrift zufolge ist es möglich, über einzelfallbezogene vertragliche Verpflichtungen die Schutzdefizite

---

[1092] *Simitis*, in: Simitis, BDSG, § 4c, Rn. 17; *Gola/Schomerus* 2010, § 4c, Rn. 6.

[1093] *Simitis*, in: Simitis, BDSG, § 4c, Rn. 19 f.

im Zielland zu kompensieren und individuell ein angemessenes Schutzniveau herzustellen.[1094] Im zweiten Halbsatz werden ausdrücklich Vertragsklauseln oder verbindliche Unternehmensregelungen erwähnt. Diese stellen flexible Formen des Selbstdatenschutzes dar und sollen im Folgenden näher erläutert werden.[1095]

3.1.12.5.1 EU-Standardvertragsklauseln

3.1.12.5.1.1 Inhalt und Bedeutung

Die EU-Standardvertragsklauseln für Auftragsverarbeiter regeln die Übermittlung von personenbezogenen Daten an Auftragsverarbeiter in Drittländer. Hierbei ist zu beachten, dass der Begriff des „Auftragsverarbeiters" im Sinne von Art. 2 lit. e) der EU-Datenschutzrichtlinie zu verstehen ist, da nach § 3 Abs. 8 BDSG gerade keine Auftragsdatenverarbeitung im Sinne des BDSG in Drittländern möglich sein soll.[1096]

Die Vertragsklauseln bieten einen angemessenen Schutz der Daten und enthalten eine rechtlich durchsetzbare Garantie, nach der sich sowohl der Exporteur als auch der Importeur der Daten in gesamtschuldnerischer Haftung gegenüber dem Betroffenen verpflichten, die für ein angemessenes Datenschutzniveau maßgebenden Datenschutzgrundsätze einzuhalten.[1097]

Werden die Standardvertragsklauseln unverändert vereinbart, ist eine aufsichtsbehördliche Genehmigung nicht notwendig.[1098] Die Aufsichtsbehörden müssen jedoch in die Lage versetzt werden, die tatsächliche Verwendung der authentischen Klauseln überprüfen zu können. Dazu reicht eine Vorlage des Vertragswerks nach Aufforderung der Behörde aus. Falls jedoch die Musterklauseln modifiziert werden oder selbst gestaltete, individuelle Vertragsklauseln verwendet werden, kann nicht ohne Weiteres vom Vorliegen ausreichender Schutzgarantien ausgegangen werden. In solchen Fällen ist eine aufsichtsbehördliche Genehmigung notwendig.[1099] Eine Ausnahme eines solchen Genehmigungserfordernisses, mit der Konsequenz einer bloßen Anzeige der Änderungen eines Standardvertrags, ist in den Fällen anzunehmen, in denen die Klauseländerungen eindeutig zugunsten des Betroffenen ausfallen.[1100]

[1094] *Nielen/Thum*, K&R 2006, 172; *Rittweger/Schmidl*, DuD 2004, 617; *Schulz*, in: Taeger/Wiebe, Inside the Cloud, 413; *Karger/Sarre*, in: Taeger/Wiebe, Inside the Cloud, 435; *Grapentin*, CR 2011, 102 f.

[1095] *Heil*, DuD 2009, 228.

[1096] *Grapentin*, CR 2011, 104; zu § 8 Abs. 3 siehe auch Kap. 3.1.12.6.

[1097] *Gola/Schomerus* 2010, § 4c, Rn. 12.

[1098] *Gola/Schomerus* 2010, § 4c, Rn. 14; Innenministerium Baden-Württemberg, Hinweise zum BDSG für die Privatwirtschaft Nr. 40, B 2.8 – Bekanntmachung vom 18.2.2002, Az.: 2–0552.1/17.

[1099] *Gola/Schomerus* 2010, § 4c, Rn. 14.

[1100] Beschluss des Düsseldorfer Kreises vom 19./20.4.2007; *Gola/Schomerus* 2010, § 4c, Rn. 14.

3.1.12.5.1.2 Möglichkeit der Unterauftragsverarbeitung

Am 5.2.2010 hat die EU-Kommission neue Standardvertragsklauseln beschlossen.[1101] Die bisher geltenden EU-Standardvertragsklauseln wurden vor allem von US-Unternehmen als zu umständlich und zu belastend kritisiert. Diesem Umstand hat die EU-Kommission Rechnung getragen und in das neue Klauselwerk Vorschläge der Internationalen Handelskammer[1102] einfließen lassen.[1103] Bereits die Änderungen der EU-Standardvertragsklauseln im Jahr 2004 waren durch die internationale Handelskammer mit erarbeitet worden. Deswegen wurden diese manchmal auch, etwas missverständlich, als „ICC-Standardvertragsklauseln" bezeichnet.

Eine der wichtigsten Neuregelungen aus dem Jahr 2010 und ganz besonders für Cloud Computing relevant, ist die Möglichkeit des weiteren Outsourcings durch den Auftragsverarbeiter, den sogenannten Datenimporteur, in einem Drittland.[1104] Ein Datenimporteur ist nämlich nach Art. 3 lit. d) des Klauselbeschlusses der EU-Kommission „der in einem Drittland niedergelassene Auftragsverarbeiter".[1105] Im Fall des Cloud Computing wäre dies ein Cloudprovider im außereuropäischen Ausland.

Konkret bedeutet die Neuregelung, dass der Empfänger im Ausland (Datenimporteur) die Daten seinerseits an einen Subunternehmer als Unterauftragsverarbeiter transferieren darf, sofern der, im EU- oder EWR-Raum ansässige, Datenexporteur gemäß der Klausel 11 lit. a) schriftlich eingewilligt hat und sich der Drittempfänger nach lit. b) zusätzlich unter die Standardvertragsklauseln unterwirft.[1106] Daneben erfordern lit. c) und d) der Klausel eine Vereinbarung einer Drittbegünstigtenklausel gemäß Klausel 3 und die Anlegung und Führung eines Verzeichnisses der Unterauftragsverarbeiter durch den Datenexporteur. Das Verzeichnis ist jährlich zu aktualisieren. Der Begriff „Datenexporteur" bezeichnet dabei gemäß Art. 3 lit. c) des Klauselbeschlusses den für die Verarbeitung Verantwortlichen, der die personenbe-

---

[1101] Entscheidung der *EU-Kommission*, Abl. EU 2010 Nr. L 39, S. 5 ff., http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:DE:PDF; *Gola/Schomerus* 2010, § 4c, Rn. 14.

[1102] International Chamber of Commerce (ICC), http://www.iccwbo.org.

[1103] *Kläner*, Neue EU-Standardvertragsklauseln, http://www.telemedicus.info/article/1752-Neue-EU-Standardvertragsklauseln.html.

[1104] *Lensdorf*, CR 2010, 735 ist der Ansicht, dass eine Unterbeauftragung im außereuropäischen Ausland wohl nicht möglich sein soll.

[1105] *Lensdorf*, CR 2010, 736; Entscheidung der *EU-Kommission*, Abl. EU 2010 Nr. L 39, S. 8, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:DE:PDF.

[1106] *Schmidl/Krone*, DuD 2010, 839; *Europäische Union*, Sicherere Standards für die Übermittlung von Daten europäischer Bürger an Auftragsverarbeiter in Drittländern, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/130&format=HTML&aged=0&language=DE&guiLanguage=de; *Kläner*, Neue EU-Standardvertragsklauseln, http://www.telemedicus.info/article/1752-Neue-EU-Standardvertragsklauseln.html.

zogenen Daten übermittelt.[1107] Im Cloudszenario ist dies also der in der EU ansässige Cloudnutzer.

Im Ergebnis entstehen mit dem Einhalten dieser vier Vorgaben sogenannte Auslagerungsketten, die nach den alten Klauseln so nicht möglich waren. Auch Äußerungen der Artikel-29-Datenschutzgruppe zu den alten Klauseln waren nicht eindeutig, so dass die Neufassung der Klauseln durch die Kommission die Rechtssicherheit bezüglich der Unterbeauftragung im außereuropäischen Ausland erhöht.[1108]

Dem Unterauftragsverarbeiter werden nach dem eben Geschilderten in der schriftlichen Vereinbarung die gleichen Pflichten auferlegt, wie dem Auftragsverarbeiter. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, bleibt der Datenimporteur gegenüber dem Datenexporteur für die Erfüllung der Pflichten des Unterauftragsverarbeiters uneingeschränkt verantwortlich. Darüber hinaus umfasst die Unterauftragsverarbeitung ausschließlich die Verarbeitungstätigkeiten, die im ursprünglichen Vertrag zwischen dem Datenexporteur aus der EU und dem Datenimporteur im Ausland vereinbart wurden.[1109]

Bestehende Verträge, die nach den alten Klauseln geschlossen wurden, bleiben so lange gültig, wie die Übermittlung und die Datenverarbeitungstätigkeiten unverändert fortgeführt werden. Falls die Vertragsparteien Änderungen vornehmen oder Vereinbarungen zur Unterauftragsverarbeitung einführen wollen, sind sie allerdings verpflichtet, einen neuen Vertrag zu schließen, der die neuen und geänderten Standardvertragsklauseln berücksichtigt.[1110]

3.1.12.5.1.3 Anwendbarkeit bei innereuropäischer Unterauftragsdatenverarbeitung?

Angesichts der Vereinfachung der Vereinbarungen zwischen den Beteiligten durch die Klauselvorgaben und das entsprechende Vertragsmuster stellt sich die Frage, ob diese nicht auch als Basis intraeuropäischer Auftragsdatenverarbeitung genutzt werden könnten.[1111] Der Vorteil liegt in der europaweiten Akzeptanz der Regelungen und der Verfügbarkeit der Klauseln in 22 der 23 Amtssprachen der EU, so dass

---

[1107] Entscheidung der *EU-Kommission*, Abl. EU 2010 Nr. L 39, S. 8, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:DE:PDF.

[1108] Siehe auch *Lensdorf*, CR 2010, 735; allgemein zur Problematik der Kettenauslagerung vor der Neufassung siehe *Fischer/Steidle*, CR 2009, 632.

[1109] *Europäische Union*, Sicherere Standards für die Übermittlung von Daten europäischer Bürger an Auftragsverarbeiter in Drittländern, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/130&format=HTML&aged=0&language=DE&guiLanguage=de.

[1110] *Europäische Union*, Sicherere Standards für die Übermittlung von Daten europäischer Bürger an Auftragsverarbeiter in Drittländern, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/130&format=HTML&aged=0&language=DE&guiLanguage=de.

[1111] *Schmidl/Krone*, DuD 2010, 838 ff.

sich die Kosten für die Erstellung und Übersetzung von Individualverträgen reduzieren ließen. Zudem würde diese Vorgehensweise international tätigen Konzernen ermöglichen ihre Auftragsdatenverarbeitungsbeziehungen konzernweit einheitlich zu regeln.[1112]

So praxisbezogen diese Ansicht jedoch ist, so wenig lässt sie sich mit der Realität des Wortlauts der neuen EU-Standardvertragsklauseln in Übereinstimmung bringen. Danach ist es notwendig, dass sich der Datenimporteur in einem Drittland befindet. Auch Art. 2 des Klauselbeschlusses spricht von „Empfängern, außerhalb der Europäischen Union, die als Auftragsverarbeiter fungieren". Ähnliches steht in Erwägungsgrund Nr. 23, wonach die Klauseln keine Anwendung finden, „wenn ein in der Europäischen Union niedergelassener Auftragsverarbeiter (…) einen in einem Drittland niedergelassenen Unterauftragsverarbeiter mit der Verarbeitung beauftragt".[1113]

Die neuen Standardvertragsklauseln finden demzufolge weder dann Anwendung, wenn alle Beteiligten in der EU ansässig sind noch dann, wenn der „Datenimporteur" (Auftragsverarbeiter), also der Cloudprovider, in der EU sitzt und nur der Unterauftragsverarbeiter seinen Sitz in einem Drittland hat.[1114]

Allerdings wird mit der Neufassung die in der aktuellen Cloudnutzungspraxis relevanteste Konstellation, nämlich diejenige, dass alle Cloudbeteiligten außer dem Nutzer in einem Drittland ansässig sind, über die neuen Vertragsklauseln unmittelbar handhabbar. Schließlich sitzen die größten Cloudprovider in den USA, wobei sich diese meist solcher Subunternehmer als Unterauftragsdatenverarbeiter bedienen, die ebenfalls oft außerhalb der EU ihren Sitz haben.

Einige halten zumindest die zweite Konstellation, in der der Cloudprovider in der EU und das Subunternehmen in einem Drittland ansässig ist, analog mittels der genehmigungsfreien Standardvertragsklauseln regelbar, weisen aber zurecht darauf hin, dass angesichts zweier Stellungnahmen[1115] der Artikel-29-Datenschutzgruppe die planwidrige Regelungslücke als Voraussetzung einer analogen Anwendung fehlen könnte.[1116]

Hauptargument für eine potentiell analoge Anwendung ist allerdings, dass bei der von der Kommission intendierten Konstellation, wonach sowohl der Datenimporteur als auch der Unterauftragsverarbeiter in einem Drittland sitzen, die Gefährdung für die personenbezogenen Daten höher ist, als bei der Konstellation, in der zumin-

---

[1112] *Schmidl/Krone*, DuD 2010, 838, 839.

[1113] *Lensdorf*, CR 2010, 737.

[1114] *Lensdorf*, CR 2010, 736.

[1115] *Artikel-29-Datenschutzgruppe*, WP 161 vom 5.3.2009, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp161_de.pdf und WP 176 vom 12.7.2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp176_de.pdf.

[1116] *Lensdorf*, CR 2010, 737.

dest der „Datenimporteur“, also der Cloudprovider als Auftragsverarbeiter, in der EU sitzt.

Treibt man allerdings diesen Gedanken weiter, so müsste man auch die innereuropäische Datenverarbeitung erst recht erlauben, da bei dieser dritten Konstellation alle Beteiligten in der EU sitzen. Allerdings gehen auch die vermeintlichen Verfechter dieser Ansicht nicht so weit, sich komplett gegen den Wortlaut zu stellen, sondern nehmen die Klauseln als Ausgangspunkt für die einfachere Erstellung von Individualverträgen.[1117]

Lehnt man eine analoge Anwendung der Klauseln auch für die zweite Konstellation ab, bleibt noch die Klärung der Frage was gilt, wenn der Auftragsverarbeiter in der EU und der Unterauftragsverarbeiter im Drittland sitzen. Hierzu existiert kein rechtliches Instrument. Die Artikel-29-Datenschutzgruppe hat aber in ihrem Working Paper 176 drei Vorschläge unterbreitet, wie man vorgehen könnte.[1118]

Die erste Möglichkeit besteht darin, einen direkten Vertrag zwischen „Data Controllern“, also dem Auftraggeber (Cloudnutzer) und dem Unterauftragsverarbeiter (Subunternehmen) im Drittland zu schließen. Dabei wäre der im Drittland ansässige Unterauftragsverarbeiter wie ein Auftragsverarbeiter zu behandeln, mit der Konsequenz, dass dieser zur Erfüllung des direkten Vertrages lediglich die neuen Standardvertragsklauseln als Datenimporteur abschließen müsse. Davon abzugrenzen ist der Hauptvertrag zwischen Auftraggeber und dem in der EU ansässigen eigentlichen Auftragsverarbeiter, der die Weisungen des Auftraggebers enthalten und den Anforderungen der EU-Datenschutzrichtlinie genügen müsse.[1119]

Für Cloud Computing könnte dieser Lösungsvorschlag allerdings erhebliche praktische Probleme bedeuten. Während der Hauptvertrag zwischen dem Auftraggeber, also dem Cloudnutzer und dem Auftragsverarbeiter als Auftragsnehmer, faktisch wie üblich aussieht und sich in Deutschland nach § 11 BDSG richtet, bedeutet jedoch die Hinzuziehung eines Subunternehmens durch den Provider in einem Drittland, dass der Cloudnutzer mit diesem Subunternehmen einen direkten Vertrag schließen müsste. Daran hat der Nutzer jedoch regelmäßig kein Interesse, weil dadurch der Cloudnutzungsvorteil der Flexibilität erheblich leiden würde. Außerdem würde der Cloudprovider das Subunternehmen als Unterauftragsverarbeiter auswählen und den Cloudnutzer als Auftraggeber mehr oder weniger vor vollendete Tatsachen stellen. Lehnt der Nutzer das Subunternehmen ab, dürfte auch der Hauptvertrag nicht mehr aufrechterhalten werden können, wenn der Provider auf Ressourcen von Subunternehmen in Drittländern angewiesen ist.

[1117] *Schmidl/Krone*, DuD 2010, 838 ff.

[1118] Siehe auch *Lensdorf*, CR 2010, 739 sowie *Artikel-29-Datenschutzgruppe*, WP 176 vom 12.7.2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp176_de.pdf.

[1119] *Lensdorf*, CR 2010, 739.

Die zweite Möglichkeit ähnelt der ersten, wobei jedoch kein direkter Vertrag mehr zwischen dem Auftraggeber und dem Unterauftragsverarbeiter im Drittland geschlossen wird, sondern der in der EU ansässige Auftragsverarbeiter für den Auftraggeber, beispielsweise im Wege einer Stellvertretung gemäß §§ 164 ff. BGB oder in Form eines Auftrags gemäß § 662 BGB, den Vertrag, ebenfalls in Form der neuen Standardvertragsklauseln, abschließt. Im Hauptvertrag müsste dazu eine entsprechende Vereinbarung geschlossen werden.[1120]

Diese Lösung wäre auch wieder für Cloud Computing gangbar, da der Kontakt zwischen Cloudnutzern und Subunternehmen entbehrlich wird. Der Cloudprovider agiert in dem Fall für den Nutzer und kann sich zudem im Auftrag des Nutzers der vorformulierten und nicht genehmigungspflichtigen Standardvertragsklauseln bedienen.

Der dritte Vorschlag sieht einen Ad-hoc-Einzelfallvertrag zwischen Auftragsverarbeiter und Unterauftragsverarbeiter vor, der die gleichen Prinzipien und Sicherheiten wie die EU-Standardvertragsklauseln, insbesondere die Einhaltung eines angemessenen Datenschutzniveaus, beinhalten müsse. Zwischen Auftraggeber und Auftragnehmer wird wie in den obigen Fällen ein Hauptvertrag geschlossen.[1121] Diese Alternative hat mithin keine direkte Anwendbarkeit der Klauseln zum Inhalt und entspricht dem üblichen Vorgehen in Fällen, in denen die Klauseln nicht angewendet werden. Gerade die Vorteile der Einfachheit und Genehmigungsfreiheit der Klauseln gehen dadurch verloren. Die Einzelverträge sind nämlich durch die Aufsichtsbehörden zu genehmigen.[1122]

Die dritte Alternative wäre auch im Cloudumfeld gangbar. Die Einzelfallverträge müssten für jede Geschäftsbeziehung in der Kette geschlossen werden und die oben erwähnten Voraussetzungen gewahrt werden. Bedient sich der Provider dabei immer der gleichen Verträge, so muss er diese auch nur einmal genehmigen lassen. Der Nachteil liegt in der Notwendigkeit eines erstmaligen Entwurfs der Verträge und der Genehmigungspflichtigkeit. Abweichungen aufgrund individueller Vereinbarungen sind erneut genehmigungspflichtig.

Die Ausführungen zeigen, dass die Komplexität der rechtlichen und insbesondere vertraglichen Beziehungen bei Kettenauslagerungen wegen der Internationalität und unvollständigen Regelungen erheblich zunimmt. Die Standardvertragsklauseln sind zwar ein erster guter Ansatz, jedoch regeln sie nicht alle Konstellationen zufriedenstellend, so dass ihre intendierten Vereinfachungs- und Erleichterungseffekte nicht voll zum Tragen kommen. Komplexität ist aber meistens kontraproduktiv für den

[1120] *Lensdorf*, CR 2010, 739.
[1121] *Lensdorf*, CR 2010, 739 f.
[1122] *Lensdorf*, CR 2010, 740.

Schutz personenbezogener Daten.[1123] Eine Erhöhung der Komplexität kommt zudem dadurch zustande, dass einige deutsche Datenschutzbehörden bei der Nutzung von Standardvertragsklauseln zusätzlich die Einhaltung der Voraussetzungen des § 11 BDSG einfordern.[1124]

3.1.12.5.2 Binding Corporate Rules und Codes of Conduct

Bindende Unternehmensrichtlinien (Binding Corporate Rules) und Verhaltenskodizes (Codes of Conduct) sind für konzernrechtlich verbundene Cloudprovider und für Private Clouds in länderübergreifenden Konzernen relevant.[1125] Beiden liegt die Idee zugrunde, dass anstelle einer Einzelprüfung von Datenübertragungen auf der Ebene des Konzerns ein für den gesamten Konzern gültiger, verbindlicher Verhaltenskodex oder Arbeitsanweisungen erstellt werden. Diese betreffen die Datenverwendung als auch die Datenübermittlung innerhalb eines Konzerns. Innerhalb aller Teilunternehmen gelten damit standortunabhängig die gleichen verbindlichen Verhaltensregelungen. Diese müssen allerdings den zuständigen Datenschutzbehörden auf Übereinstimmung mit den europäischen Datenschutzstandards vorgelegt und von diesen überprüft und genehmigt werden.[1126] Änderungen des Code of Conduct erfordern eine erneute Prüfung durch die Aufsichtsbehörden, weil nach einer Änderung die inhaltlichen Anforderungen des BDSG oder der Datenschutzrichtlinie nicht mehr erfüllt sein könnten.[1127]

Ziel der Etablierung von bindenden Unternehmensrichtlinien ist es, innerhalb eines über die Grenzen der EU oder des EWR hinausreichenden Unternehmens ein vergleichbares und angemessenes Schutzniveau im Sinne des Art. 25 DSRL zu schaffen. Binding Corporate Rules werden zwar als solche nicht in der Richtlinie erwähnt, allerdings sieht diese in Abs. 2 die Herstellung eines angemessenen Schutzniveaus im Wege von Vertragsklauseln vor.[1128] In § 4c Abs. 2 Satz 1 Halbsatz 2 BDSG sind die verbindlichen Unternehmensregelungen ausdrücklich erwähnt.

Weder § 4c BDSG, noch die Datenschutzrichtlinie enthalten inhaltliche Vorgaben bezüglich der inhaltlichen Ausgestaltung. Allerdings enthalten die vier Kommissi-

---

[1123] So auch *Lensdorf*, CR 2010, 740.

[1124] Einzelheiten dazu siehe weiter unten in Kap. 3.1.12.6.

[1125] *Rath*, in: Schartner/Weippl, D-A-CH Security 2010, 189; *Karger/Sarre*, in: Taeger/Wiebe, Inside the Cloud, 435.

[1126] *Wunderlich*, Datenschutzrechtliche Aspekte des Cloud Computing, http://www.worldwidewundi.de/wordpress/?page_id=98#_ftn9; *Heil*, DuD 2009, 228; *Karger/Sarre*, in: Taeger/Wiebe, Inside the Cloud, 435.

[1127] *Räther/Seitz*, MMR 2002, 527.

[1128] *Wunderlich*, Datenschutzrechtliche Aspekte des Cloud Computing, http://www.worldwidewundi.de/wordpress/?page_id=98#_ftn9.

onsentscheidungen zu den Standardvertragsklauseln indirekt Anhaltspunkte für die inhaltliche Ausgestaltung von Binding Corporate Rules oder Codes of Conduct.[1129]

Welche Rechtsqualität die Arbeitsanweisungen und Verhaltenskodizes als Selbstregulierungsformen haben oder wie Missachtungen derselben sanktioniert werden, ist allerdings noch weitgehend ungeklärt.[1130] Die rechtliche Einordnung ist aber auch weniger entscheidend als die konkrete Umsetzung im Unternehmen. Sie sind als Handlungsanweisungen des Arbeitgebers im Rahmen seines Direktionsrechts gegenüber allen Arbeitnehmern auszugestalten und dementsprechend auch bekannt zu machen. Eine Möglichkeit ist beispielsweise die Umsetzung durch eine Betriebsvereinbarung.[1131]

Neben den rechtlichen Voraussetzungen sollten Codes of Conduct und Binding Corporate Rules eine weitere Anforderung erfüllen, nämlich dem Kunden die Position des Cloudproviders im Hinblick auf den Datenschutz verdeutlichen. Sie sind damit auch ein Marketinginstrument.[1132] Damit können zumindest die Bedenken hinsichtlich des Datenschutzes bei der Übertragung der Daten innerhalb eines Cloudkonzerns zerstreut werden. Dies betrifft neben den Inhaltsdaten Dritter insbesondere auch die Nutzungs- und Bestandsdaten der Cloudkunden.

Nachteilig im Vergleich zu Vertragsklauseln ist der Umstand, dass Codes of Conduct und Binding Corporate Rules nicht für spezielle Anforderungen im Einzelfall tauglich sind. Diese können nicht wie Verträge individuelle und differenzierte Lösungen bereitstellen.[1133] Da diese jedoch ohnehin nur konzernintern verwendet werden, ist der Bedarf an einer individuellen Abstimmung, im Vergleich zu einem Geschäftsverhältnis zwischen externen Kunden und einem Provider, viel geringer.

3.1.12.5.3 Safe-Harbor-Übereinkommen

Die letzte Ausnahme, die ein fehlendes Datenschutzniveau kompensiert, betrifft Datenübermittlungen in die Vereinigten Staaten. Grundlage hierfür ist das sogenannte Safe-Harbor-Abkommen. Es ist ein Abkommen zwischen den Vereinigten Staaten, vertreten durch das US-Handelsministerium (U.S. Department of Com-

---

1129 *Wunderlich*, Datenschutzrechtliche Aspekte des Cloud Computing, http://www.worldwidewundi.de/wordpress/?page_id=98#_ftn9, Entscheidungen der *EU-Kommission* in Abl. EU 2001 Nr. L 181, S. 19, Abl. EU 2002 Nr. L 6, S. 52, Abl. EU 2004 Nr. L 385, S. 74 und Abl. EU 2010 Nr. L 39, S. 5, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:DE:PDF.

1130 *Heil*, DuD 2009, 228; *Räther/Seitz*, MMR 2002, 526.

1131 *Räther/Seitz*, MMR 2002, 527.

1132 *Räther/Seitz*, MMR 2002, 527.

1133 *Räther/Seitz*, MMR 2002, 527.

merce) und der Europäischen Kommission und soll gewährleisten, dass die strengen Datenschutzanforderungen der Datenschutzrichtlinie gewahrt werden.[1134]

Mit dem Inkrafttreten der Richtlinie und dem Fehlen eines angemessenen Datenschutzniveaus in den USA bestand die Gefahr der Störung aller Datentransfers in die USA. Um dieses Problem anzugehen wurde ein Dialog zwischen dem amerikanischen Handelsministerium und der EU-Kommission (Generaldirektion XV) initiiert, dessen Ergebnis das Safe-Harbor-Übereinkommen vom 27.7.2000 darstellt.[1135] Es trat im gleichen Sommer in Kraft und wurde ab November 2000 in der Praxis angewandt.[1136]

Die vereinbarten Regelungen richten sich an US-Unternehmen, so dass auch nur solche die Privilegierung in Anspruch nehmen können. Die teilnehmenden Unternehmen sollen nach der Bezeichnung des Übereinkommens als „Safe Harbor“ einen „sicheren Hafen“ für die übermittelten Daten schaffen. Dem Abkommen sind bisher mehr als 1000 Unternehmen beigetreten, die auf einer Liste[1137] des US-Handelsministeriums geführt werden.[1138] Die daran teilnehmenden Unternehmen verpflichten sich im Rahmen einer Selbstverpflichtung und einer Meldung an die Federal Trade Commission (FTC) zur Einhaltung von strengen Datenschutzregelungen. Erstmalige oder weitere, regelmäßig stattfindende, Überprüfungen und Evaluierungen der Unternehmen durch Datenschutzaufsichtsbehörden erfolgen allerdings nicht. Trotz dieses Mangels einer Überprüfung durch Dritte hat die Kommission im Rahmen des Abschlusses der Verhandlungen festgestellt, dass Safe Harbor ein angemessenes Schutzniveau im Sinne des Artikel 25 Abs. 2 DSRL gewährleistet.[1139]

Hintergrund für das Übereinkommen ist der mangelnde rechtliche Schutz von personenbezogenen Daten in den Vereinigten Staaten. Ein einheitliches Datenschutz-

---

[1134] *US-Handelsministerium*, http://www.export.gov/safeharbor/eu; Entscheidung der *EU-Kommission*, Abl. EU 2000 Nr. L 215, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:DE:NOT.

[1135] *Räther/Seitz*, MMR 2002, 427.

[1136] Vorgelegt vom US-Handelsministerium am 21.7.2000; die Veröffentlichung der Entscheidung der EU-Kommission erfolgte im Europäischen Amtsblatt am 25.8.2000; *Erd*, K&R 2010, 625.

[1137] *US-Handelsministerium*, http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.

[1138] *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, Erfolgreicher transatlantischer Dialog zum Datenschutz, http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2006/PM-41-06ErfolgreicherTransatlantischerDialogZumDatenschutz.html; *Düsseldorfer Kreis*, Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile.

[1139] Entscheidung der *EU-Kommission*, Abl. EU 2000 Nr. L 215, S. 7; *Räther/Seitz*, MMR 2002, 428.

recht existiert dort nämlich nicht. Es gibt lediglich wenige sektorale Datenschutzgesetze, beispielsweise den sehr speziellen Video Privacy Protection Act,[1140] der untersagt, dass Daten von Personen herausgegeben werden dürfen, die Videos ausleihen oder kaufen oder den (Data) Privacy Act,[1141] der für Datenverarbeitungen durch Bundesbehörden gilt.[1142] Die Vereinigten Staaten verfolgen beim Datenschutz einen Selbstregulierungsansatz, der sich auf freiwillige Selbstverpflichtungen der Unternehmen stützt und auf staatliche Kontrollen, von Ausnahmen abgesehen, verzichtet.[1143] Diesem Verständnis entsprechend ist auch das Safe-Harbor-Abkommen ausgestaltet.

Wesentlicher Inhalt des Abkommens sind die sieben Prinzipien (Safe Harbor Privacy Principles) und die Frequently Asked Questions (FAQ). Die Unternehmen haben diesen zufolge gewisse Grundsätze zu beachten, beispielsweise müssen sie auch angemessene Sicherheitsmaßnahmen zur Datensicherheit gewährleisten. Neben diesem als „Security“ bezeichneten Prinzip gibt es noch die Prinzipien „Notice“, „Choice“, „Onward Transfer“, „Access“, „Data Integrity“ und „Enforcement and Dispute Resolution“.[1144]

Kernforderung des Abkommens ist das Ausweisen von sogenannten „Privacy Policies“, also Datenschutzrichtlinien oder Datenschutzerklärungen, durch die beteiligten Unternehmen. Dies kann zum Beispiel auf den öffentlich zugänglichen Websites der Unternehmen geschehen.[1145] Anhand dieser Richtlinien soll für die Nutzer eines Angebots nachvollziehbar sein, was genau mit personenbezogenen Daten geschieht. Zudem sollen sie eine Vergleichbarkeit der Unternehmen bezüglich des Datenhandlings ermöglichen. Bei Verstößen zwischen den darin gemachten Angaben und der tatsächlichen Praxis kann die FTC Sanktionen aussprechen.[1146]

In letzter Zeit kam das Safe-Harbor-Abkommen vermehrt in die Kritik.[1147] Einige plädieren dafür das Abkommen komplett aufzukündigen und grundlegend neu zu

---

[1140] Title 18 U.S.C., § 2710, http://www.law.cornell.edu/uscode/18/2710.html.

[1141] Title 5 U.S.C., § 552a, http://www.law.cornell.edu/uscode/5/552a.html.

[1142] *Räther/Seitz*, MMR 2002, 427; *Büllesbach/Höss-Löw*, DuD 2001, 136; *Abel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 2.7, Rn. 10; *Grimm/Roßnagel*, DuD 2000, 447.

[1143] Ausführlich dazu *Grimm/Roßnagel*, DuD 2000, 448 ff.; *Räther/Seitz*, MMR 2002, 427; *Marnau/Schlehahn*, DuD 2011, 312.

[1144] Zu den Prinzipien im Einzelnen siehe *Räther/Seitz*, MMR 2002, 428, *Erd*, K&R 2010, 625 und *US-Handelsministerium*, U.S.-EU Safe Harbor Overview, http://www.export.gov/safeharbor/eu/eg_main_018476.asp.

[1145] *Büllesbach/Höss-Löw*, DuD 2001, 138.

[1146] *Connolly* 2008, 11.

[1147] Eine Zusammenfassung der Kritikpunkte findet sich bei *Erd*, K&R 2010, 624 f.

verhandeln[1148] oder einer grundlegenden Revision zu unterziehen.[1149] Die Bundesregierung sah jedoch im Herbst 2010 keinen Reformbedarf.[1150]

Auslöser der harschen Kritik war eine Untersuchung aus dem Dezember 2008, die zum Ergebnis kam, dass es nicht nur Vollzugsdefizite gibt, sondern sogar 206 Unternehmen auf ihrer Webseite angaben am Abkommen beteiligt zu sein, obwohl dies tatsächlich nicht der Fall war.[1151] Auch war die vom Handelsministerium geführte Liste zum Zeitpunkt der Untersuchung nicht aktuell. Von 1597 Unternehmen auf der Liste waren faktisch nur 1109 Mitglieder des Abkommens. Die Unternehmen, die zu Unrecht auf der Safe-Harbor-Liste standen, hatten entweder die Zertifizierung nicht erneuert oder die Unternehmen existierten nicht mehr. Außerdem enthielt die Liste doppelte Einträge. Lediglich 348 Unternehmen erfüllten die grundlegendsten Minimalanforderungen, nämlich die Einhaltung des siebten Prinzips „Enforcement and Dispute Resolution“.[1152] Unter diesen 348 Unternehmen waren nur 54 oder 3% aller Unternehmen, die einen umfassenden Schutz der Daten gewährleisteten.[1153]

Die in der Studie aufgedeckten Missstände blieben für die Unternehmen im Übrigen folgenlos. Zwar wurde ein einziges Unternehmen wegen der Falschangabe, Mitglied des Safe-Harbor-Abkommens zu sein, verurteilt, allerdings ergaben sich aus der Verurteilung keinerlei Sanktionen.[1154]

Angesichts dieser Studienergebnisse und der lediglich ungeprüften Selbstzertifizierung stellen die deutschen Datenschutzbehörden mit dem Beschluss des „Düssel-

---

[1148] So *Weichert*, 10 Jahre Safe Harbor – viele Gründe zum Handeln, kein Grund zum Feiern, http://netzpolitik.org/2010/10-jahre-safe-harbor-%E2%80%93-viele-grunde-zum-handeln-kein-grund-zum-feiern.

[1149] *Erd*, K&R 2010, 627.

[1150] BT-Drs. 17/3375; *Krempl*, Bundesregierung: Kein Korrekturbedarf beim transatlantischen Datenschutz, http://www.heise.de/newsticker/meldung/Bundesregierung-Kein-Korrekturbedarf-beim-transatlantischen-Datenschutz-1128049.html.

[1151] *Schulzki-Haddouti*, Safe-Harbor-Abkommen: Freibrief für amerikanische Datenschutz-Sünder?, http://www.heise.de/newsticker/meldung/Safe-Harbor-Abkommen-Freibrief-fuer-amerikanische-Datenschutz-Suender-933700.html; *Connolly* 2008; *Erd*, K&R 2010, 625 f.

[1152] *Connolly* 2008, 4 f; in der Studie wurde lediglich auf Konformität mit einem der insgesamt sieben Prinzipien, nämlich „Enforcement and Dispute Resolution“, geprüft, so dass bei einer Prüfung aller Vorgaben von den 348 Unternehmen wahrscheinlich noch weniger konform im Sinne des Abkommens gewesen wären.

[1153] Siehe auch *Connolly* 2008, 8 und *Erd*, K&R 2010, 626, 627 mit jeweils weiteren Erkenntnissen aus der Studie.

[1154] *Galexia*, First US Prosecution for false web claim of Safe Harbor status, http://www.galexia.com/public/about/news/about_news-id168.html; *Schulzki-Haddouti*, Safe-Harbor-Abkommen: Freibrief für amerikanische Datenschutz-Sünder?, http://www.heise.de/newsticker/meldung/Safe-Harbor-Abkommen-Freibrief-fuer-amerikanische-Datenschutz-Suender-933700.html.

dorfer Kreises“[1155] vom 29.4.2010 verschärfte Anforderungen an die Übermittlung personenbezogener Daten an US-Unternehmen, die sich dem Abkommen unterworfen haben. Demnach soll für Unternehmen in Deutschland eine Verpflichtung bestehen, gewisse Mindestkriterien zu prüfen, bevor sie personenbezogene Daten an ein auf der Safe-Harbor-Liste geführtes US-Unternehmen übermitteln. Zudem sollen sich datenexportierende Unternehmen nicht allein auf die Behauptung einer Safe-Harbor-Zertifizierung des Datenimporteurs verlassen können. Vielmehr muss sich das Daten exportierende Unternehmen nachweisen lassen, dass die Safe-Harbor-Selbstzertifizierung vorliegt und noch gültig ist und deren Grundsätze auch tatsächlich eingehalten werden. Beim Fehlen dieser Voraussetzungen empfiehlt der Düsseldorfer Kreis die Verwendung von Standardvertragsklauseln oder von bindenden Unternehmensrichtlinien zur Gewährleistung eines angemessenen Datenschutzniveaus.[1156]

Neben Vollzugsdefiziten hat das Übereinkommen, was erheblich schwerer wiegt, auch inhärente konzeptionelle Schwächen, die nur schwer mit europäischen Datenschutzgrundsätzen vereinbar sind. So ist beispielsweise der Betroffene vor der Datenerhebung oder Datenverarbeitung nicht zwingend zu benachrichtigen. Die Benachrichtigung kann auch „so bald wie möglich danach“ erfolgen.[1157] Auch der Zweckbindungsgrundsatz ist nicht gewährleistet. Änderungen des Zwecks sind nämlich ohne ausdrückliche Einwilligung möglich. Es gilt das Opt-Out-Prinzip, so dass bei Passivität des Betroffenen eine Zweckänderung möglich ist. Lediglich bei einigen wenigen sensitiven Daten gilt das Opt-In-Prinzip. Auch das Auskunftsrecht des Betroffenen ist nur in Ansätzen vorhanden. Dieses steht nämlich unter dem Vorbehalt der Verhältnismäßigkeit und Zumutbarkeit.[1158]

Ein mit Safe Harbor zusammenhängender Kritikpunkt betrifft den vermehrten Zugriff öffentlicher US-Stellen, insbesondere von Sicherheitsbehörden, auf Daten, die von Unternehmen für eigene Geschäftszwecke gespeichert werden. Erwähnt seien die Zugriffe von US-Behörden auf Flugpassagierdaten, Daten des internationalen Zahlungsverkehrsnetzwerks SWIFT[1159] und die Zugriffsmöglichkeiten durch den

---

[1155] Der „Düsseldorfer Kreis“ ist die Bezeichnung für den Zusammenschluss von Datenschutzaufsichtsbehörden nichtöffentlicher Stellen; *Erd*, K&R 2010, 624.

[1156] *Düsseldorfer Kreis*, Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile.

[1157] *Erd*, K&R 2010, 624.

[1158] *Räther/Seitz*, MMR 2002, 429, 430 mit weiteren Einzelheiten zu den datenschutzrechtlichen Defiziten.

[1159] SWIFT ist ein Akronym für „Society for Worldwide Interbank Financial Telecommunication“; SWIFT ist durch eine Selbstverpflichtung auch dem Safe-Harbor-Abkommen unterworfen; zu Einzelheiten siehe *SWIFT*, SWIFT Safe Harbor Policy, http://www.swift.com/about_swift/legal/compliance/data_protection_policies/swift_safe_harbor_policy.page.

USA PATRIOT Act.[1160] Durch diese Zugriffsmöglichkeiten der US-Behörden wird das, bereits so schon unzureichende, Safe-Harbor-Abkommen noch weiter ausgehöhlt.

Nach all diesen Erwägungen erscheint es mehr als fraglich, ob Safe Harbor ein angemessenes Datenschutzniveau gewährleistet.[1161] Dies gilt insbesondere für die im Abkommen angeführten Mindestanforderungen. Es ist allerdings nicht ausgeschlossen, dass einzelne Unternehmen über die Gestaltung ihrer Datenschutzrichtlinien ein zu Europa vergleichbares Datenschutzniveau erreichen können. Deswegen ist es auch verständlich, dass die Bundesregierung und die EU-Kommission an der bisherigen Übereinkunft festhalten wollen.

Für Cloud Computing kann folglich die Erkenntnis gewonnen werden, dass zum einen die Vorgaben des Düsseldorfer Kreises zu beachten sind und über diese Vorgaben hinaus Nutzer mit US-Cloudanbietern individuelle Vereinbarungen hinsichtlich des Schutzes personenbezogener Daten treffen sollten, die europäischen Standards genügen. Dies kann beispielsweise auch über die vom Kreis vorgeschlagenen Standardvertragsklauseln oder Verhaltenskodizes erfolgen. Dabei ist insbesondere darauf zu achten, dass bei der Inanspruchnahme von Ressourcenanbietern durch den Cloudprovider innerhalb einer Leistungskette das Datenschutzniveau entsprechend den Garantien des Providers oder den individuellen Vereinbarungen gewahrt bleibt. Insbesondere muss der Betroffene schon vorher in Kenntnis gesetzt werden, dass solche Übermittlungen an Dritte möglich und nötig sind.

Die Alternative zu den obigen Lösungsansätzen wäre die Nutzung von auf die EU oder den EWR begrenzte Cloudangebote, da es auf den Ort der Datenerhebung oder Datenverarbeitung ankommt. Eine solche regionale Begrenzung löst jedoch nicht das Problem der Zugriffsbefugnisse der US-Behörden, soweit der Cloudanbieter ein US-Unternehmen ist.[1162]

3.1.12.6 Verhältnis zur Auftragsdatenverarbeitung

Die Übermittlung von Daten ins außereuropäische Ausland hat auf den ersten Blick für die Auftragsdatenverarbeitung keine Bedeutung. Die Privilegierung nach § 11 BDSG greift nämlich gemäß § 3 Abs. 8 Satz 3 Halbsatz 2 BDSG nur dann, solange die Daten innerhalb der EU oder des EWR verbleiben und dort erhoben, verarbeitet oder genutzt werden.[1163] Nach geltender Rechtslage ist das angemessene Daten-

---

[1160] Letzterer wird wegen seiner erheblichen Relevanz für Cloud Computing weiter unten in Kap. 3.9.2 näher erläutert und genauer untersucht.

[1161] *Erd*, K&R 2010, 627 findet angesichts der Kritikpunkte die polemische Bezeichnung „Unsafe Harbor“ passender.

[1162] Siehe dazu Kap. 3.9.2.

[1163] *Pohle/Ammann*, CR 2009, 276; *Niemann/Hennrich*, CR 2010, 688; *Petri*, in: Simitis, BDSG, § 11, Rn. 8; *Dammann*, in: Simitis, BDSG, § 3, Rn. 244 f; Gola/Schomerus 2010, § 11, Rn. 7; *Geis* 2009, 4; *Schulz*, in: Taeger/Wiebe, Inside the Cloud, 413.

schutzniveau, also der Umstand, ob es sich um ein „sicheres Drittland“ handelt, für eine Datenverarbeitung im Auftrag irrelevant.

Einige sehen in dieser Einengung durch § 3 Abs. 8 Satz 3 BDSG auf den EU- und EWR-Raum das Bestehen einer europarechtswidrigen Situation.[1164] Sie fordern deshalb, gerade vor dem Hintergrund von Globalisierung und der Internationalität von Geschäftsbeziehungen, eine Gleichstellung zwischen sicheren Drittstaaten sowie der EU und dem EWR, so dass die Auftragsdatenverarbeitung auch in solchen sicheren Drittstaaten ermöglicht wird.[1165]

Die Befürworter sind der Auffassung, dass sich aus den Beschlüssen der Kommission über die Angemessenheit des Datenschutzniveaus in den oben genannten sicheren Drittstaaten ein Gleichstellungs- und Gleichbehandlungsgebot diesen Staaten gegenüber ergibt, das durch die nationale Norm in § 3 Abs. 8 Sätze 2 und 3 BDSG unterlaufen wird. Die Adäquanzentscheidungen der Kommission sollen Vorgaben enthalten, die die Mitgliedsstaaten dazu verpflichten, „die Übermittlung personenbezogener Daten an Stellen in ‚sicheren Drittstaaten‘ unter denselben Voraussetzungen zuzulassen wie den Transfer personenbezogener Daten an Stellen in den Mitgliedsstaaten der EU und des EWR“.[1166] Allerdings findet sich ein derart unmittelbares und zwingendes Gleichbehandlungsgebot nicht im Wortlaut der Entscheidungen. Dort steht lediglich, dass „personenbezogene Daten aus den Mitgliedstaaten übermittelt werden können, ohne dass zusätzliche Garantien erforderlich sind“.[1167]

Für die Auffassung der Befürworter soll außerdem sprechen, dass dadurch auch das problematische Ergebnis vermieden werden kann, dass eine Übermittlung von sensitiven Daten im Sinne des § 3 Abs. 9 BDSG gemäß § 28 Abs. 6 BDSG in sichere Drittstaaten ohne Einwilligung der Betroffenen regelmäßig unzulässig und damit kaum durchführbar ist. Während nämlich die Übermittlung sensitiver Daten im Rahmen einer Auftragsdatenverarbeitung innerhalb der EU und des EWR gemäß § 11 BDSG an keine weiteren Voraussetzungen geknüpft ist, müssen für eine Übermittlung in einen sicheren Drittstaat, ebenso wie in einen unsicheren Drittstaat, die umfangreichen Voraussetzungen des § 28 Abs. 6 BDSG erfüllt sein.[1168]

Gerade dieses Beispiel der sensitiven Daten zeigt jedoch, dass eine vermittelnde und abgestufte Position dem Schutzbedürfnis des Betroffenen im Verhältnis zur praktischen Handhabbarkeit am ehesten gerecht werden würde. Während die gel-

---

[1164] *Erd*, DuD 2011, 275 ff.; ähnlich, aber mit anderen Argumenten, *Nielen/Thum*, K&R 2006, 172, 174.

[1165] *Erd*, DuD 2011, 275; zu den sicheren Drittstaaten siehe oben Kap. 3.1.12.4.

[1166] *Erd*, DuD 2011, 276.

[1167] Erwägungsgrund Nr. 2 in den jeweiligen Entscheidungen oder Beschlüssen der Kommission.

[1168] *Nielen/Thum*, K&R 2006, 174; *Erd*, DuD 2011, 277; zu § 28 Abs. 6 BDSG siehe auch noch einmal oben Kap. 3.1.12.2.

tende Rechtslage die Angemessenheit des Niveaus vollkommen außer Betracht lässt, gehen die Befürworter von einer Identität des Schutzniveaus mit dem der Datenschutzrichtlinie aus, was jedoch bereits der Bezeichnung als „Angemessenheit“ oder „Adäquanz“ des Datenschutzniveaus widerspricht. Zudem sind die Datenschutzregelungen in den jeweiligen „sicheren Drittstaaten“ unterschiedlich, so dass eine Pauschalisierung hinsichtlich sensitiver Daten bereits aus diesem Grund nicht angebracht ist.

Vermittelnd wäre es daher vorzugswürdig, die Übermittlung sensitiver Daten weiterhin an bestimmte Erlaubnisvoraussetzungen, zum Beispiel die ausdrückliche Einwilligung, zu knüpfen, während die nichtsensitiven Daten ohne besondere Erlaubnisnorm entsprechend einer innereuropäischen Auftragsdatenverarbeitung übermittelt werden könnten. Die Voraussetzungen für sensitive Daten sollten zudem nicht mehr den besonders strengen und einschränkenden Voraussetzungen des § 28 Abs. 6 BDSG unterliegen, sondern der Angemessenheit des Datenschutzniveaus in den sicheren Drittstaaten Rechnung tragen. Nur bei einer Übermittlung in unsichere Drittstaaten sollte die aktuelle Regelung zum Zug kommen.

Folgt man der Auffassung der Befürworter oder der vermittelnden Ansicht, so würde die Nutzung von Cloud Computing in und mit solchen sicheren Drittstaaten erheblich erleichtert werden. Insbesondere bei der Übermittlung sensitiver Daten würde das gesteigerte Schutzniveau rechtlich berücksichtigt werden.

Für eine solche differenzierte Regelung der Übermittlung sensitiver Daten müsste allerdings der Gesetzgeber tätig werden. Erste Ansätze für eine Regelungsbedürftigkeit hinsichtlich sicherer Drittstaaten haben deutsche Gesetzgebungsorgane erkannt, so dass mit einer baldigen Anpassung der Vorschriften des Bundesdatenschutzgesetzes gerechnet werden kann.[1169] Während der Bundesrat[1170] diese Anpassung bereits 2010 sektoral im Rahmen der Modernisierung des Beschäftigtendatenschutzes angehen wollte, lehnte die Bundesregierung[1171] diese mit dem Argument ab, dass die allgemeinen Regeln der Auftragsdatenverarbeitung und das Bundesdatenschutzgesetz insgesamt betroffen sind und diese nicht im Rahmen der Neuregelung des Beschäftigtendatenschutzes thematisiert werden sollte.[1172] Einen eigenen Gesetzesvorschlag hat die Regierung bislang allerdings nicht unterbreitet.

Der Vollständigkeit halber sei erwähnt, dass einige Stimmen in der Literatur noch weiter gehen und die Auftragsdatenverarbeitung durch eine analoge Anwendung der

---

[1169] Siehe auch *Erd*, DuD 2011, 277 f.

[1170] Stellungnahme des Bundesrates vom 5.11.2010 zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, BT-Drs. 17/4230, Anlage 3, 28, http://dipbt.bundestag.de/dip21/btd/17/042/1704230.pdf.

[1171] Gegenäußerung der Bundesregierung zur Stellungnahme des Bundesrates zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, BT-Drs. 17/4230, Anlage 4, 38.

[1172] Siehe auch *Erd*, DuD 2011, 278.

§§ 3 Abs. 8 Satz 3 und 11 BDSG auch hinsichtlich unsicherer Drittstaaten als zulässig ansehen und dabei mit der Existenz der EU-Standardvertragsklauseln und der Möglichkeit, über diese ein gleichwertiges Datenschutzniveau zu erreichen, argumentieren.[1173] Außerdem dürfe dieser Ansicht zufolge die Regelung in § 3 Abs. 8 Satz 3 BDSG auch nicht zwingend als abschließende Regelung in Bezug auf die Auftragsdatenverarbeitung nach § 11 BDSG verstanden werden, da auch die Europäische Datenschutzrichtlinie die Begriffe „Auftragsverarbeiter“ und „Dritte“ nicht auf den innereuropäischen Bereich begrenze.[1174] Der außereuropäische Auftragsdatenverarbeiter dürfe deshalb auch nicht als „Dritter“ im Sinne des BDSG angesehen werden.[1175]

Es ist allerdings fraglich, ob diese sehr weitgehenden Ansichten, insbesondere über eine analoge Anwendung des § 11 BDSG zulässig sind, da eine Regelungslücke allenfalls für die Auftragsdatenverarbeitung in sicheren Drittstaaten besteht, wie man an den erwähnten neueren Initiativen der Gesetzgebungsorgane erkennen kann. Eine Ausweitung im Sinne der Befürworter der weitergehenden Ansicht ist aber von den Gesetzgebungsorganen gerade nicht geplant.

Im Zusammenhang mit Standardvertragsklauseln besteht zudem eine vollkommen gegensätzliche Rechtsauffassung. So wird von den Datenschutzbehörden des Bundes und der Länder die Ansicht vertreten, dass bei der Benutzung von Standardvertragsklauseln zusätzlich die Anforderungen des § 11 BDSG einzuhalten seien.[1176] Dabei sollen nur die Pflichten aus § 11 Abs. 2 BDSG gelten. Im völligen Gegensatz zu den obigen Meinungen soll diese Geltung der Pflichten nämlich nicht zu einer Privilegierung des Auftraggebers führen. Die Ansicht der Aufsichtsbehörden widerspricht aber der Gesetzessystematik, da § 11 BDSG i.V.m. § 3 Abs. 8 Satz 3 BDSG, wie mehrfach erwähnt, nicht für Stellen außerhalb des EWR gilt, so dass eine solche Forderung nicht mit dem Bundesdatenschutzgesetz in Einklang zu bringen ist.[1177]

Im Ergebnis ist festzuhalten, dass man weder eine Privilegierung von außereuropäischen Stellen in unsicheren Drittstaaten mit § 11 BDSG begründen, noch solchen Stellen und dem innereuropäischen Auftraggeber ausschließlich die Pflichten des § 11 BDSG auferlegen kann.

3.2 Infrastrukturrecht

Neben dem Datenschutzrecht könnte auch das Infrastrukturrecht als öffentliches Recht einschlägig sein, wenn Cloud Computing als kritische Infrastruktur anzuse-

---

[1173] *Rittweger/Schmidl*, DuD 2004, 620; *Räther*, DuD 2005, 461 ff.; *Nielen/Thum*, K&R 2006, 172, 174.

[1174] *Nielen/Thum*, K&R 2006, 174; *Räther*, DuD 2005, 465.

[1175] *Nielen/Thum*, K&R 2006, 176.

[1176] *Budszus/Heibey/Hillenbrand-Beck/Polenz/Seifert/Thiermann* 2011, 11, 12; *Scholz/Lutz*, CR 2011, 424; kritisch *Schröder/Haag*, ZD 2011, 150; a. A. *Weber/Voigt*, ZD 2011, 76.

[1177] Ähnlich *Scholz/Lutz*, CR 2011, 427 f.

hen ist.[1178] Eine solche Einordnung hätte möglicherweise auch staatliche Schutzpflichten zur Folge.

3.2.1 Cloud Computing als kritische Infrastruktur?

Bevor jedoch eine solche Einordnung des Cloud Computing möglich ist, müsste vorab geklärt werden, was rechtlich und tatsächlich unter kritischen Infrastrukturen zu verstehen ist. Die Definitionen des Begriffspaars sind alle sehr ähnlich und auf EU-Ebene in Art. 2 lit. a) der EU-Infrastrukturschutzrichtlinie[1179] und national in § 17 Abs. 1 Nr. 3 ZSKG, einer Datenschutzvorschrift, legaldefiniert. § 3 Abs. 1 Nr. 15 BSIG[1180] erwähnt zudem den nicht näher definierten Begriff der „kritischen Informationsinfrastrukturen“.[1181]

Kritische Infrastrukturen sind solche Infrastrukturen, denen eine lebenswichtige Bedeutung für das Gemeinwesen zukommt.[1182] Es sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.[1183] Das auf Katastrophen abzielende ZSKG definiert kritische Infrastrukturen in § 17 Abs. 1 Nr. 3 ZSKG als solche, bei deren Ausfall die Versorgung der Bevölkerung erheblich beeinträchtigt wird.

Der Zusammenbruch von solchen essentiellen Infrastrukturen hat demnach erhebliche negative Folgewirkungen für das Dasein des Einzelnen und den Bestand der Gesellschaft als Ganzes.[1184] Für die Einordnung als kritische Infrastruktur ist es im Übrigen irrelevant, ob diese von der öffentlichen Hand oder von Privatunternehmen aufgebaut und betrieben wird.[1185]

Die erste Frage, die sich dabei stellt, ist die, ob Cloudsysteme eine „Infrastruktur“ im obigen Sinne darstellen. Cloud Computing basiert auf der Nutzung von Diensten über die – zweifellos kritische – Infrastruktur „Internet“.[1186] Indes sind für die Be-

---

[1178] Das Infrastrukturrecht wird als Querschnittsmaterie angesehen.

[1179] RL 2008/114/EG.

[1180] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz).

[1181] *Gaycken/Karger*, MMR 2011, 5.

[1182] *Holznagel/König* 2005, 3; *Schmidt-Preuß*, in: Kloepfer, Schutz kritischer Infrastrukturen, 47.

[1183] *BSI*, Definition Kritische Infrastrukturen, https://www.bsi.bund.de/ContentBSI/Themen/Kritis/Einfuehrung/KritisDefinitionen/definitionen.html; ähnlich *Schmidt-Preuß*, in: Kloepfer, Schutz kritischer Infrastrukturen, 47; *Gaycken/Karger*, MMR 2011, 5; siehe auch Art. 2 lit. a) der RL 2008/114/EG.

[1184] So auch *Schmidt-Preuß*, in: Kloepfer, Schutz kritischer Infrastrukturen, 47; Art. 2 lit. a) der RL 2008/114/EG spricht allgemeiner von „Auswirkungen auf die Mitgliedstaaten“.

[1185] *Gaycken/Karger*, MMR 2011, 5.

[1186] Die Bundesregierung hat zum Beispiel, um dieser Bedeutung des Internets als kritische Infrastruktur gerecht zu werden, Ende Februar 2011 eine Sicherheitsstrategie für den Cyberraum beschlossen; siehe dazu *Bundesministerium des Innern*, Bundesregierung beschließt Sicher-

reitstellung der Dienste auch Server und Rechenzentren nötig, die ebenfalls eine „Infrastruktur“ darstellen. Nicht zuletzt das Infrastructure-as-a-Service-Nutzungsmodell besagt schon im Namen, dass dabei Infrastruktur genutzt und angemietet wird. Infrastruktur in diesem technischen Sinne ist allerdings vom Begriff der (kritischen) Infrastrukturen abzugrenzen, der auf Einrichtungen und Organisationen abzielt und nicht auf technische Komponenten.

Nach dieser Unterscheidung der Infrastrukturbegriffe stellt sich die Ausgangsfrage, ob Cloudinfrastrukturen und Cloudsysteme, also nicht nur das zugrundeliegende Internet, sondern die damit verbundene Art der Bereitstellung von IT-Dienstleistungen, wichtige Bedeutung für die Gesellschaft und das staatliche Gemeinwesen haben. Im Jahr 2011 ist eine solche gesamtgesellschaftliche Wichtigkeit und Abhängigkeit noch nicht anzunehmen. Glaubt man jedoch den Prognosen und blickt man auf die getätigten und zu tätigenden Investitionen sowie die Erfahrungen bei der Entwicklung der herkömmlichen Internetdienstleistungen, so ist es nur eine Frage der Zeit, bis die Schwelle zum „Kritischen“ überschritten wird. Falls sich die Prognosen bewahrheiten und zukünftig fast jede IT-Operation in Unternehmen, Behörden oder bei privaten Nutzern von Cloudsystemen abhängt, wird eine Einordnung als kritische Infrastruktur somit nur eine Frage der Zeit sein. Ausfälle von Cloudinfrastrukturen hätten dann beachtliche, insbesondere wirtschaftliche, Auswirkungen. Als IT-Infrastrukturen wären Clouds auch kritische Informationsinfrastrukturen im Sinne des § 13 Abs. 1 Nr. 15 BSIG, mit der rechtlichen Konsequenz, dass sich private Unternehmen, in diesem Fall die Cloudprovider, mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) über den Infrastrukturschutz abstimmen und mit dem Bundesamt zusammenarbeiten müssten.[1187]

Wegen dieser absehbar erheblichen Bedeutung für das Gemeinwesen und die Gesellschaft sind auch die Anforderungen an die vorlaufende Technikgestaltung höher als bei unkritischen Strukturen. Deshalb ist die frühzeitige Einordnung als kritische Infrastruktur auch kein Selbstzweck, sondern soll dem Technikgestalter die Verantwortung und die meist erheblichen Konsequenzen bei einer unreflektierten Umsetzung der Technik vor Augen führen. Das Schadenspotential ist umso höher, je kritischer eine Infrastruktur ist. Nicht selten hängt das Leben von Menschen davon ab.

---

heitsstrategie für den Cyber-Raum, http://www.bmi.bund.de/cln_174/SharedDocs/Pressemitteilungen/DE/2011/mitMarginalspalte/02/cyber.html;jsessionid=095B210BC545B77D917040EF50320CB6.

[1187] Siehe zu dieser Koordinierungsbefugnis des BSI auch *Kuri*, Innenministerium: Mehr Biss für die IT-Sicherheit des Bundes, http://www.heise.de/newsticker/meldung/Innenministerium-Mehr-Biss-fuer-die-IT-Sicherheit-des-Bundes-189162.html.

3.2.2 Staatliche Schutz- und Gewährleistungspflicht für Cloudinfrastruktur?

In der Literatur wird vertreten, dass der Staat eine Schutzpflicht für die allgemeine IT-Infrastruktur hat, die sich aus dem neuen Grundrecht auf Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme ergeben soll. Das Internet – und damit mittelbar und zum Teil auch Cloud Computing – als Teil dieser allgemeinen Infrastruktur soll als informationstechnisches System vom Schutzbereich des Grundrechts mit umfasst sein.[1188]

Auch wenn diese Ansicht mit guten Gründen bestritten werden kann, weil primär eigengenutzte Systeme, wie Personal Computer oder Smartphones davon umfasst sind, ist ihr aber zuzugestehen, dass es bei den Grundrechten als objektive Wertordnung gerade nicht auf den Einzelnen und in diesem Fall auf dessen eigengenutztes System ankommen wird, sondern darauf, dass sich der Staat schützend vor die Grundrechte stellt und diese auch vor Angriffen Privater schützt.[1189] Ob allerdings gerade aus diesem neuen Grundrecht eine Schutzpflicht für IT-Infrastrukturen ableitbar ist, müssen der künftige wissenschaftliche Diskurs oder weitere Rechtsprechung des Bundesverfassungsgerichts zeigen.

Soweit es um den Vertraulichkeitsaspekt von Cloudinfrastrukturen geht, kann man beim Abstellen auf die objektive Dimension der Grundrechte auch das Telekommunikationsgeheimnis aus Art. 10 GG als schutzbegründendes Grundrecht heranziehen. Durch die einfachgesetzlichen Schutzvorschriften (§§ 88 ff. TKG, § 206 StGB) hat der Staat in diesem Zusammenhang seine Schutzpflicht erfüllt.

Keine grundrechtliche Schutzpflicht, aber eine Vorschrift des Grundgesetzes, ist Art. 87f Abs. 1 GG. Hiernach gewährleistet der Bund im Bereich der Telekommunikation flächendeckend angemessene und ausreichende Dienstleistungen. Zu den sonst üblichen Schutzpflichten kommt durch Art. 87f Abs. 1 GG eine grundgesetzliche Gewährleistungspflicht des Staates hinzu. Die Vorschrift ist die Grundlage für die sogenannten Universaldienste und hat maßgeblichen Anteil an der flächendeckenden Durchsetzung von TK-Infrastruktur in Form von Festnetztelefonie und damit zusammenhängend auch für breitbandige Internetzugänge. Für Letztere wird diskutiert, ob diese künftig als Universaldienst anerkannt werden sollen, was nicht zuletzt für Cloud Computing erhebliche Bedeutung haben würde, weil dadurch auch infrastrukturell weniger gut ausgebaute Regionen relativ kurzfristig Breitbanddienste und damit mittelbar Cloudservices nutzen könnten.[1190]

[1188] So *Höhne/Pöhls*, in: Schartner/Weippl, D-A-CH Security 2010, 54.

[1189] BVerfGE 7, 198; BVerfGE 39, 1 ff.; *Holznagel/König* 2005, 3.

[1190] Die Regierungskoalition ist aber gegen eine solche Anerkennung; siehe dazu *Krempl*, Bundestag verabschiedet Reform des Telekommunikationsgesetzes, http://www.heise.de/newsticker/meldung/Bundestag-verabschiedet-Reform-des-Telekommunikationsgesetzes-1367636.html.

Während man anhand der bisherigen Ausführungen noch an einer staatlichen Schutzpflicht für TK-Infrastrukturen zweifeln konnte, muss man eine solche beim Überschreiten der Schwelle zur „kritischen“ Infrastruktur bejahen.[1191] Rechtlich kommt, neben der körperlichen Unversehrtheit aus Art. 2 Abs. 2 Satz 1 GG, vor allem das Sozialstaatsprinzip aus Art. 20 Abs. 1 GG in Form der Daseinsvorsorge[1192] und der staatlichen Grundversorgung zum Tragen. Dabei kommt es zu einer Vermengung zwischen Schutz- und Gewährleistungspflichten des Staates. Neben Fragen der staatlichen Gewährleistung von Infrastrukturen treten in letzter Zeit vermehrt die Gefahren- und Risikovorsorge im Zusammenhang mit Infrastrukturen in den Vordergrund.[1193] Diese auf Sicherheit bedachten Vorsorgeaspekte sind eine unmittelbare Ableitung aus der staatlichen Schutzpflicht für kritische Infrastrukturen.

Nicht zuletzt wegen der künftigen Bedeutung des Cloud Computing für die Gesellschaft und wegen dem Zusammenhang zur Gefahr- und Risikovorsorge ist auch die IT-Sicherheit rechtlich und praktisch in Form der tatsächlichen Gestaltung der Systeme bedeutsam. Nur möglichst sichere Cloudsysteme können der künftigen Bedeutung, insbesondere als potentiell kritische Infrastruktur, gerecht werden.

Dieses Potential zur kritischen Infrastruktur der Clouddienste führt dazu, dass der Staat beim Überschreiten des „Kritischen“ oder sogar vorher seine Schutzpflichten ausüben und die Funktionstüchtigkeit und Verfügbarkeit der Clouddienste gewährleisten muss. Ohne IT-Sicherheit ist aber eine solche Gewährleistung nicht möglich. Die staatliche Schutzpflicht könnte sich somit im Laufe der Zeit sogar auf die Gewährleistung von IT-Sicherheit konkretisieren.[1194]

3.3 Deutsches und europäisches Kartellrecht

Im Zusammenhang mit Cloud Computing und öffentlichem Recht ist auch an Wettbewerbs- und Kartellrecht, als Teil des Wirtschaftsverwaltungsrechts, zu denken. Bei einer solchen kartellrechtlichen Betrachtung verdient die Möglichkeit des Missbrauchs einer marktbeherrschenden Stellung gemäß Art. 102 AEUV (ex-Art. 82 EGV) besondere Aufmerksamkeit. Insbesondere die möglicherweise gerade stattfindende „Aufteilung“ des Marktes zwischen den drei großen Anbietern für Public

---

[1191] Näheres zur Pflicht zur Sicherung kritischer Infrastrukturen siehe bei *Holznagel/König* 2005, 1 ff.

[1192] Mittlerweile ist sogar eine sogenannte „E-Daseinsvorsorge“ im Hinblick auf den Zugang zum Internet anerkannt; ausführlich dazu *Luch/Schulz*, VM 2/2011, 104 ff.

[1193] Siehe dazu auch *Greve*, DuD 2009, 756; ein Beispiel dafür ist die sogenannte KRITIS-Strategie; siehe dazu *Bundesministerium des Innern*, Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), http://www.bmi.bund.de/cae/servlet/contentblob/544770/publicationFile/27031/kritis.pdf.

[1194] Wie wichtig und relevant IT-Sicherheit für risikobehaftete Infrastrukturen werden kann, zeigte der Stuxnet-Angriff auf iranische Atomanlagen; siehe dazu Fn. 956.

Cloud Computing, nämlich Amazon, Google und Microsoft, lässt solche Überlegungen nicht unplausibel erscheinen.

Für große Public-Cloud-Provider könnte die „Essential-Facilities-Doktrin“, also die Annahme, dass IaaS-Cloudservices eine „wesentliche Einrichtung“ (Essential Facility) darstellen, einschlägig sein.[1195] Die Doktrin besagt, dass marktbeherrschende Unternehmen nach Art. 102 AEUV verpflichtet sind, Dritten Zugang zu solchen Einrichtungen zu gewähren, ohne deren Nutzung ein Wettbewerber seinen Kunden keine Dienste anbieten kann.[1196]

Die Doktrin der Verweigerung des Zugangs zu wesentlichen Einrichtungen wurde ursprünglich in nahezu neun Jahrzehnten in den Vereinigten Staaten entwickelt.[1197] Sie ist seit einigen Jahren Teil des europäischen Rechtsverständnisses und wurde durch die Europäische Kommission erstmals in den Sealink-Entscheidungen von 1992 und 1993 und später in der Entscheidung „Hafen von Rødby“ herangezogen.[1198] Der Fall „Magill“ wurde als implizite Bestätigung der Essential-Facilities-Doktrin durch den EuGH angesehen.[1199] Später präzisierte das Gericht Erster Instanz (EuG) in seinem Urteil „European Night Services Ltd.“ die Voraussetzungen für das Vorliegen einer „Essential Facility“ im Rahmen der Überprüfung einer Kommissionsentscheidung,[1200] noch vor dem EuGH, der später in der Rechtssache „Bronner“ den Anwendungsbereich der Essential-Facilities-Doktrin festlegte. Der Gerichtshof stellte dabei hohe Anforderungen an das Vorliegen eines Anspruchs auf Zugang zu den Einrichtungen eines marktbeherrschenden Unternehmens.[1201] Eine weitere Bestätigung der Kommissionspraxis erfolgte im EuGH-Urteil zum Fall „IMS Health“.[1202] Die konkreten Voraussetzungen der Doktrin sind jedoch, trotz dieser Urteile, noch nicht abschließend herausgebildet.[1203]

Da eine „wesentliche Einrichtung“ als eine Einrichtung oder Infrastruktur definiert wird, ohne deren Nutzung ein Wettbewerber seinen Kunden keine Dienste anbieten

---

1195 *Nägele/Jacobs*, ZUM 2010, 291.

1196 *Müller*, EuZW 1998, 232; *Nägele/Jacobs*, ZUM 2010, 291.

1197 *Scherer*, MMR 1999, 315 und dortige Fn. 2; Ausgangspunkt war das Urteil zum Fall „United States vs. Terminal Railroad Association“ aus dem Jahr 1912. Der Fall betraf die Weigerung marktbeherrschender Eisenbahngesellschaften, Wettbewerbern den Zugang zu dem von den marktbeherrschenden Unternehmen gekauften Bahnhof von St. Louis zu gewähren.

1198 *Scherer*, MMR 1999, 315; zum Teil als „Hafenentscheidungen“ bekannt; Entscheidungen der *Kommission*, B&I Line Plc. v. Sealink Harbours Ltd., Abl. EG Nr. 6, 1992, Ziffer 1.3.30 (Sealink I) und 94/19/EG, Sea Containers v. Stena Sealink, Abl. EG 1994 Nr. L 15, S. 8 (Sealink II); Entscheidung der *Kommission*, „Verweigerung des Zugangs zu den Anlagen des Hafens von Rødby“, Abl. EG 1994 Nr. L 55, S. 52.

1199 *Scherer*, MMR 1999, 316; EuGH, Slg. 1995, I-743, Rn. 50.

1200 *Scherer*, MMR 1999, 316; EuG, Slg. 1998, II-3141.

1201 *Scherer*, MMR 1999, 316, 317.

1202 EuGH, Slg. 2004, I-5039 (IMS Health/NDC Health).

1203 *Möschel*, in: Immenga/Mestmäcker, Wettbewerbsrecht: EG, Art. 82 EGV, Rn. 239.

kann, besteht die Befürchtung, dass ein IaaS-Cloudanbieter seine Kontrolle über die Cloudinfrastruktur dazu nutzen könnte, Wettbewerbern den Zugang zu verweigern, um dadurch seine Stellung auf einem nachgelagerten Markt zu schützen.[1204]

Als hypothetisches Beispiel wäre denkbar, dass ein Onlineshop Amazons Infrastrukturservice EC2 für die Bereitstellung seines Webshops nutzen möchte, Amazon aber diese Nutzung verweigert, um nicht die eigenen Onlineshoppingangebote zu untergraben. Zwar gibt es mit Google und Microsoft Konkurrenzangebote, jedoch sind diese, wie oben dargestellt, meist auf gewisse Dienstleistungen spezialisiert, so dass ein Wechsel zur Konkurrenz nur mit erheblichen Anpassungen und Schwierigkeiten verbunden wäre (Problematik der Interoperabilität, fehlender Standards und des Vendor Lock-in). Nicht selten ist so ein Wechsel überhaupt nicht möglich, weil die nötigen Services nur bei dem marktbeherrschenden Anbieter angeboten werden. Außerdem gibt es die Konstellation einer kollektiven Marktbeherrschung, wenn mehrere Unternehmen gemeinsam eine marktbeherrschende Stellung besitzen und somit ein Wechsel zur Konkurrenz nichts ändern würde, wenn diese Cloudanbieter genauso ablehnend reagieren, wie der zuerst ausgewählte Cloudprovider.[1205]

Um der Ausnutzung einer marktbeherrschenden Stellung wirksam zu begegnen, besteht ein aus der Doktrin abgeleiteter Kontrahierungszwang. Unternehmen die den Zugang zu vorgelagerten oder nachgeordneten Märkten beherrschen, müssen anderen Unternehmen die Mitbenutzung dieser Einrichtungen gestatten, selbst wenn ihnen davon eine Konkurrenz auf dem genannten anderen Markt droht.[1206] Hierbei ist zu beachten, dass die Tangierung des Eigentums des Cloudbetreibers durch das gezahlte Nutzungsentgelt kompensiert wird.[1207]

Eine Zugangsverweigerung kann allerdings durch objektive Gründe gerechtfertigt sein. Anerkannte Rechtfertigungsgründe sind die Erreichung von Kapazitätsgrenzen, die Ablehnung von Wettbewerbern, denen die zur Nutzung der Einrichtung notwendigen Eigenschaften fachlicher, technischer oder wirtschaftlicher Art fehlen, die Sicherung der Funktionsfähigkeit der Einrichtung und der Betriebssicherheit oder der Schutz von Verbrauchern.[1208] Insbesondere der erste und bedeutendste

---

[1204] *Nägele/Jacobs*, ZUM 2010, 291.

[1205] Zur kollektiven Marktbeherrschung siehe *Immenga/Körber* in: Immenga/Mestmäcker, Wettbewerbsrecht: EG, 2007, VO (EG) 139/2004, Art. 2, Rn. 413. Eine Definition der kollektiven Marktbeherrschung durch die EU-Kommission findet sich im Glossar der Wettbewerbspolitik der EU, 2002, S. 10: „Zwei oder mehr eigenständige Wirtschaftseinheiten, die durch eine wirtschaftliche Verbindung auf einem bestimmten Markt zusammenhängen, können ebenfalls gemeinsam eine beherrschende Stellung innehaben. Diese Situation wird als kollektive (gemeinsame oder oligopolistische) beherrschende Stellung bezeichnet.“.

[1206] *Emmerich* in: Dauses, EU-Wirtschaftsrecht, 2010, Art. 81 und 82 EGV, Rn. 393.

[1207] *Nägele/Jacobs*, ZUM 2010, 291.

[1208] *Möschel*, in: Immenga/Mestmäcker, Wettbewerbsrecht: EG, Art. 82 EGV, Rn. 242; *Nägele/Jacobs*, ZUM 2010, 291.

Rechtfertigungsgrund dürfte bei großen öffentlichen Cloudprovidern aufgrund der vermeintlich unbegrenzten Ressourcenkapazität nur durch klare Nachweise über die tatsächlich vorhandenen Kapazitäten zu begründen sein. Wegen der Fluktuation der genutzten Ressourcen, insbesondere bei Ressourcenanbietern als Subunternehmern, ist dies kein leichtes Unterfangen. Zudem wird in der Regel ein wirtschaftlich vernünftig handelnder Cloudprovider niemals zulassen, dass die Ressourcen bis zum Anschlag ausgenutzt werden. Dadurch wird die Nutzbarkeit für die Kunden eingeschränkt, weil eine Skalierung nach oben nicht mehr möglich und die Verfügbarkeit des Dienstes mangels Überlastung nicht mehr gewährleistet ist. Auch die restlichen Rechtfertigungsgründe dürften selten einschlägig sein. Hinsichtlich der Sicherheit ist allerdings denkbar, dass ein Unternehmen, das die Verbreitung von Spammails oder sogar Malware als „Geschäftsmodell“ zum Inhalt hat, mit dem Argument abgelehnt werden kann, dass durch Blacklisting von IP-Adressbereichen des Cloudproviders auch alle anderen Kunden in Mitleidenschaft gezogen würden. Allerdings dürfte es bei solchen dubiosen Unternehmen ohnehin am Wettbewerbsverhältnis auf einem vor- oder nachgelagerten Markt fehlen.

Mittelfristig könnte ein solcher Kontrahierungszwang für Cloudprovider dazu führen, dass Probleme der fehlenden Interoperabilität zwischen verschiedenen Cloudservices und das damit verbundene Problem des Vendor Lock-in durch einheitliche (De-Facto-)Standards reduziert würden. Wenn ein marktbeherrschendes Unternehmen im Umfeld einer kollektiven Marktbeherrschung mit anderen Unternehmen ohnehin quasi jedem Zugang zu seinen Angeboten ermöglichen muss, ist es kontraproduktiv, das Angebot durch proprietäre Schnittstellen und Software abzuschotten, wenn dadurch die Nutzer gezwungen werden zu einem Konkurrenzunternehmen zu wechseln und dadurch dessen Marktstärke noch weiter steigern. Zudem kann die mangelnde Kompatibilität den Kontrahierungszwang faktisch unterlaufen, was eventuelle Strafzahlungen nach sich ziehen würde. Insbesondere wenn keine kollektive, sondern eine alleinige Markbeherrschung besteht, ist es zwingend notwendig, dass die Dienste von potentiellen Konkurrenten auch tatsächlich genutzt werden können.

3.4 Internationales Privatrecht

Neben internationalen Bezügen im Datenschutzrecht ist auch im Zivilrecht zu klären, welches Recht bei internationalen Sachverhalten anzuwenden ist. Da die Grundkonzeption von Cloud Computing in Form von Public Cloud Computing regelmäßig grenzüberschreitenden Charakter hat, ist dies ein nicht zu vernachlässigender rechtlicher Gesichtspunkt. Insbesondere das internationale Privatrecht (IPR) hat hierbei Bedeutung. Das sind im Wesentlichen die Vorschriften der Art. 27 ff. EGBGB, soweit diese nicht durch die sogenannten „Rom-Verordnungen“ verdrängt

werden.[1209] Während die Rom-I-VO gemäß Art. 1 für vertragliche Schuldverhältnisse in Zivil- und Handelssachen gilt, die eine Verbindung zum Recht verschiedener Staaten aufweisen, ist die Rom-II-VO nach deren Art. 1 für Schuldverhältnisse außervertraglicher Art anzuwenden.

Bei kollisionsrechtlichen Fragestellungen hat das Verhältnis zwischen den Beteiligten Bedeutung. Es muss zwischen der Anbieterseite und der Nutzerseite differenziert werden. Während die Rechtsstellung der Cloudanbieter unproblematisch ist, muss bei den Cloudkunden unterschieden werden, ob Verbraucher oder Unternehmer auf der Nutzerseite beteiligt sind, da erstere nach den Vorstellungen des Gesetzgebers ein erhöhtes Schutzbedürfnis haben. Verbraucher sind gemäß § 13 BGB und Art. 6 Abs. 1 Rom-I-VO natürliche Personen, die ein Rechtsgeschäft zu einem Zweck abschließen, der weder ihrer gewerblichen noch ihrer selbständigen beruflichen Tätigkeit zugerechnet werden kann. Unternehmer sind gemäß § 14 BGB und Art. 6 Abs. 1 Rom-I-VO natürliche oder juristische Personen oder rechtsfähige Personengesellschaften, die bei Abschluss eines Rechtsgeschäfts in Ausübung ihrer gewerblichen oder selbständigen beruflichen Tätigkeit handeln. Auf der Anbieterseite muss immer ein Unternehmen handeln, um die erhöhte Schutzbedürftigkeit der Verbraucherseite zu begründen. Die Cloudanbieter sind Unternehmer in diesem Sinne.

Eine ähnliche Anknüpfung an die gewerbliche Tätigkeit enthält Art. 14 Abs. 1 lit. b) Rom-II-VO, der bei Erfüllung dieser Voraussetzung eine freie Rechtswahl erlaubt.[1210] Eine solche Rechtswahl bei gewerblich genutzten Clouds ist zudem nach Art. 3 Rom-I-VO auch für vertragliche Schuldverhältnisse möglich. Ohne eine solche Rechtswahl ist an die Vermutungsregelungen des Art. 4 Rom-I-VO anzuknüpfen. Als Ausprägung des erhöhten Schutzbedürfnisses gilt bei Verbraucherbeteiligung außerdem ein Günstigkeitsvergleich zwischen Verbraucherschutzvorschriften des gewählten Rechts und des Staats des gewöhnlichen Aufenthalts des Verbrauchers.[1211]

Außerdem ist zu beachten, dass die Rom II-VO gemäß Art. 1 Abs. 2 lit. g) nicht für Schuldverhältnisse gilt, die sich aus der Verletzung von Persönlichkeitsrechten ergeben. Für Persönlichkeitsrechtsverletzungen bleibt Art. 40 EGBGB die maßgebliche Kollisionsnorm.[1212]

[1209] Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Kurzbezeichnung: Rom-I-Verordnung) und Verordnung (EG) Nr. 864/2007 des Europäischen Parlaments und des Rates über das auf außervertragliche Schuldverhältnisse anzuwendende Recht (Kurzbeschreibung: Rom-II-Verordnungen), beide zukünftig als Rom-I-VO und Rom-II-VO abgekürzt.

[1210] Siehe hierzu auch die Ausführungen im Rahmen des Urheberrechts in Kap. 3.7.4.2.1.

[1211] *Nägele/Jacobs*, ZUM 2010, 283.

[1212] *Jotzo*, MMR 2009, 233.

3.5 Vertragsrecht

Im Rahmen von Cloud Computing haben Verträge zwischen Anbietern und Nutzern und damit das Vertragsrecht eine besondere Bedeutung. Im Rahmen der Überwindung von Datenschutzdefiziten wurde bereits auf vertragliche Regelungen eingegangen, beispielsweise die EU-Standardvertragsklauseln oder Binding Corporate Rules.[1213] Auch bei der Erläuterung des § 11 BDSG wurde mehrfach auf vertragliche Notwendigkeiten hingewiesen.[1214]

Zentral sind jedoch die Service Level Agreements (SLA), die die Leistungserbringung und deren Einzelheiten sowie die jeweiligen Rechte und Pflichten festlegen. Ein damit zusammenhängender Aspekt ist die Sicherheit der Datenverarbeitung. Sicherheitszusagen können über Security-Service Level Agreements (SSLA) verabredet werden. SLA und SSLA haben dabei in der Regel den Charakter von allgemeinen Geschäftsbedingungen (AGB).[1215]

Erster Ansatzpunkt bei einer vertragsrechtlichen Betrachtung des Cloud Computing ist die Klärung der Frage, welche Vertragstypen eine Rolle spielen können.

3.5.1 Vertragstypologische Einordnung

Diese vertragstypologische Einordnung hat nicht nur für die Auslegung von vertraglichen Bestimmungen oder die Ausfüllung möglicher Lücken im Vertrag, sondern vor allem auch für das Mängelgewährleistungsrecht Bedeutung.[1216] Wegen der großen Bandbreite der Cloudleistungen und deren Kombinationsmöglichkeiten ist eine pauschale Zuordnung zu einem der gängigen Vertragstypen des Schuldrechts nicht möglich. Die Zuordnung ist vom Einzelfall abhängig und bedarf einer individuellen Analyse.[1217] Diese Einordnung richtet sich nach der tatsächlich geschuldeten Leistung.[1218]

Als einschlägige Vertragstypen kommen Werkverträge gemäß §§ 631 ff. BGB, Mietverträge gemäß §§ 535 ff. BGB oder auch die Leihe gemäß §§ 598 ff. BGB in Betracht. Dienstverträge gemäß §§ 611 ff. BGB sind dagegen, trotz der Einordnung von „Cloud Computing als Dienstleistung“, wenig tauglich, da diese nur ein „Bemühen“ schulden, womit aber dem Cloudnutzer nicht gedient ist, da dieser die konkrete Erbringung einer Leistung und eines Erfolgs benötigt. Zudem wird durch Dienstverträge menschliche Arbeit Teil des Rechtsverkehrs, so dass der Dienstver-

---

[1213] Vergleiche Kap. 3.1.12.5.

[1214] Siehe dazu Kap. 3.1.8.5.

[1215] *Weichert*, DuD 2010, 680; *Niemann/Paul*, K&R 2009, 447; *Pohle/Ammann*, CR 2009, 273.

[1216] *Schulz/Rosenkranz*, ITRB 2009, 233.

[1217] *Karger/Sarre*, in: Taeger/Wiebe, Inside the Cloud, 432.

[1218] *Söbbing*, in: Leible/Sosnitza, Onlinerecht 2.0: Alte Fragen – neue Antworten? Cloud Computing – Datenschutz – Urheberrecht – Haftung, 45.

trag bereits aus diesem Grund nicht einschlägig sein kann.[1219] Das Dienstvertragsrecht gilt aber für Hilfs- und Zusatzleistungen im Zusammenhang mit der Bereitstellung von Cloudservices. Dies betrifft insbesondere den Support, Hotlines oder Schulungen.[1220]

Wegen der Vermischung und Kombination unterschiedlicher Leistungen handelt es sich oft um typengemischte Verträge. Dabei ist jeder Vertragsteil nach dem Recht des auf ihn zutreffenden Vertragstypus zu beurteilen, soweit dies nicht im Widerspruch zum Gesamtvertrag steht.[1221]

Weil jedoch häufig die Bereitstellung von Hard- oder Software den Kern der vertraglichen Leistungen ausmacht, wird hauptsächlich Mietrecht zur Anwendung kommen.[1222] Damit geht für den Cloudprovider als Vermieter eine verschuldensunabhängige Haftung für anfängliche und bei Vertragsschluss vorhandene Mängel gemäß § 536a BGB einher. Diese Garantiehaftung des Vermieters soll jedoch nach herrschender Meinung und der Rechtsprechung, als für das gesetzliche Haftungssystem atypische Regelung, auch über AGB abdingbar sein.[1223] Für Cloudprovider ist ein solcher Haftungsausschluss wichtig, da etwaige Mängel der Soft- oder Hardware üblicherweise bereits bei Abschluss des Vertrages mit dem Cloudnutzer vorliegen und damit unter § 536a BGB Abs. 1 Alt. 1 BGB fallen würden.[1224]

Im Folgenden sollen nun einzelne Kernleistungen, die für Cloud Computing typisch sind, vertragstypologisch zugeordnet werden.

3.5.1.1 Bereitstellung von Speicherplatz

Die Bereitstellung von Speicherplatz wird vertragstypologisch uneinheitlich eingeordnet. Während die überwiegende Mehrheit in Literatur und Rechtsprechung einen Mietvertrag annimmt, wird für Webhosting die Auffassung vertreten, dass es sich um einen Werkvertrag handele.[1225] Der beim Webhosting wesentliche Aspekt der

---

[1219] *Richardi/Fischinger*, in: Staudinger, BGB, § 611, Rn. 2.

[1220] *Pohle/Ammann*, CR 2009, 275; *Niemann/Paul*, K&R 2009, 447; *Söbbing*, in: Leible/Sosnitza, Onlinerecht 2.0: Alte Fragen – neue Antworten? Cloud Computing – Datenschutz – Urheberrecht – Haftung, 46, 50.

[1221] BGH, NJW 2007, 2394; BGHZ 63, 306, 309 ff.

[1222] *Karger/Sarre*, in: Taeger/Wiebe, Inside the Cloud, 432; *Pohle/Ammann*, CR 2009, 274.

[1223] *Eisenschmid*, in: Schmidt-Futterer, § 536a BGB, Rn. 173; BGH, NJW-RR 1991, 74; BGH, NJW-RR 1993, 519; *Söbbing*, in: Leible/Sosnitza, Onlinerecht 2.0: Alte Fragen – neue Antworten? Cloud Computing – Datenschutz – Urheberrecht – Haftung, 49; *Weidenkaff*, in: Palandt, § 536a BGB, Rn. 7.

[1224] *Söbbing*, in: Leible/Sosnitza, Onlinerecht 2.0: Alte Fragen – neue Antworten? Cloud Computing – Datenschutz – Urheberrecht – Haftung, 49.

[1225] Einen Mietvertrag nehmen beispielsweise an *Niemann/Paul*, K&R 2009, 447; *von dem Bussche/Schelinski*, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, 2011, Teil 1, Rn. 115 und 116; *Leupold/Glossner*, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, 2008, Teil 2, Rn. 20; *Bertermann*, Heise Online-Recht, Kap. II, Rn. 90; AG Charlottenburg MMR 2002, 258; OLG Köln CR 2002, 832; *Redeker*, in: Hoeren/Sieber, Handbuch Mul-

öffentlichen Erreichbarkeit einer Webseite, die dem Vertrag Werkcharakter verleiht,[1226] ist bei den meisten Clouddiensten, also beim bloßen Speichern im Sinne eines Lagerns von Daten, nicht einschlägig. Die Unterscheidung zwischen Webhosting und bloßer Lagerung ergibt sich folglich aus der öffentlichen Zugänglichkeit und Erreichbarkeit der Daten. Während bei Webhosting schwerpunktmäßig Webseiten zur Verfügung gehalten werden, die für die Öffentlichkeit zugänglich sein sollen, also ein Erfolg geschuldet wird, ist bei Cloudspeicherdiensten regelmäßig nur die Nutzung des Speicherplatzes als Datenablage und die begrenzte Erreichbarkeit für den einzelnen Speicherplatznutzer Vertragsinhalt. Clouddienste, für die Werkvertragsrecht einschlägig ist, sind die Image- und Filehoster, soweit der Nutzer einen Werklohn für deren Nutzung entrichten muss.[1227]

Das Speichern von Daten in einer Cloud kann auch als Verwahrung gemäß § 688 BGB angesehen werden können.[1228] Bei einer unentgeltlichen Verwahrung gilt gemäß § 690 BGB ein lediglich eingeschränkter Haftungsmaßstab, nämlich die eigenübliche Sorgfalt.

3.5.1.2 Bereitstellung von Software und Verarbeitung von Daten

Für die Onlinebereitstellung von Software gegen Entgelt ist seit dem ASP-Urteil des BGH[1229] Mietrecht einschlägig. Die im Urteil enthaltenen Wertungen und Argumente sind wegen der Ähnlichkeit der beiden Bereitstellungsmodelle auf Cloud Computing übertragbar.

Nach dem BGH steht „als typische Leistung beim ASP-Vertrag die Gewährung der Onlinenutzung von Software für eine begrenzte Zeit im Mittelpunkt der vertraglichen Pflichten“ und „es liegt deshalb nahe, mit der überwiegenden Meinung im Schrifttum, einen Mietvertrag, der die entgeltliche Gebrauchsüberlassung einer beweglichen oder unbeweglichen Sache zum Gegenstand hat, anzunehmen“.[1230] Außerdem steht laut BGH der Anwendbarkeit von Mietrecht nicht entgegen, dass der Kunde keinen Besitz an den Computerprogrammen erlangt und diese nur über das

timedia-Recht, Teil 12, Rn. 198, 234; *Eckhart*, Information Management und Consulting 4/2010, 56.

[1226] Zum Werkvertragscharakter beim Webhosting wegen der öffentlichen Erreichbarkeit siehe *Redeker*, in: Hoeren/Sieber, Handbuch Multimedia-Recht, Teil 12, Rn. 234.

[1227] Siehe dazu Kap. 2.3.7.1.3. Üblicherweise sind die Basisangebote kostenlos, es gibt aber auch kostenpflichtige Premiumangebote, die eine gewisse Verfügbarkeit und Ladegeschwindigkeit garantieren.

[1228] *Koch*, ITRB 2001, 42; *Söbbing*, in: Leible/Sosnitza, Onlinerecht 2.0: Alte Fragen – neue Antworten? Cloud Computing – Datenschutz – Urheberrecht – Haftung, 45.

[1229] BGH, NJW 2007, 2394.

[1230] BGH, NJW 2007, 2394; ebenso *Koch*, ITRB 2001, 40; *Röhrborn/Sinhart*, CR 2001, 70; *von Westerholt/Berger*, CR 2002, 84; *Klimek*, K&R 2002, 636; *Pohle/Ammann*, K&R 2009, 627, 630.

Internet zugänglich sind. Der Mietvertrag setzt nämlich keine Besitzverschaffung, sondern lediglich die Gebrauchsüberlassung voraus.[1231]

Die unentgeltliche Überlassung und Onlinebereitstellung kann als Leihe gemäß §§ 598 ff. BGB eingeordnet werden. Genauso wie bei der Miete ist auch bei der Leihe eine Besitzverschaffung keine Voraussetzung, sondern es genügt ebenso die Einräumung der bloßen Nutzungsmöglichkeit.[1232] Dies hat insbesondere für die private Nutzung Bedeutung, da sich viele cloudbasierte Dienste an Verbraucher richten und kostenlos angeboten werden.[1233]

Ein Werkvertrag ist hingegen anzunehmen, wenn nicht nur die Nutzung einer Softwareapplikation geleistet wird, sondern der Cloudprovider auch die Verarbeitung der Daten auf seiner Infrastruktur mittels der Software übernimmt. Dies gilt besonders für spezialisierte SaaS-Dienste, wie CRM- oder ERP-Services. Bei solchen verarbeitenden Services ist ein gewisser Erfolg geschuldet, so dass diese erfolgsbezogenen Dienste dem Werkvertragsrecht unterfallen.[1234] Dies hat unter anderem Konsequenzen für die Gewährleistung und die Mängelbeseitigung, die im Werkvertragsrecht viel eher mit dem Kaufrecht, als mit den mietrechtlichen Vorschriften, vergleichbar sind.

3.5.1.3 Bereitstellung von Rechenleistung

Bei der Bereitstellung von Rechenleistung ging der BGH schon im Jahr 1992 davon aus, dass diese als Miete einzuordnen ist.[1235] Im damals entschiedenen Fall ging es um die stundenweise Überlassung eines Großrechners. Im Beschluss führt der BGH aus, dass „das Nutzungsverhältnis über den Rechner, aufgrund dessen der Beklagten die Rechnerkapazität zu bestimmten Tageszeiten für ihren Gebrauch zur Verfügung gestellt wurde, als Mietvertrag (…) zu qualifizieren ist“.[1236]

Diese Rechtsprechung ist auch ohne Bedenken auf Cloud Computing direkt übertragbar, soweit Rechenleistung als Clouddienst bereitgestellt wird. Auch für Rechenkapazität im Rahmen des klassischen IT-Outsourcings oder von Rechenzentrumsverträgen wurde diese Ansicht bereits vertreten.[1237]

[1231] BGH, NJW 2007, 2394.

[1232] BGH, NJW-RR 2004, 1566; *Wunderlich* 2010, 47; *Pohle/Ammann*, K&R 2009, 627.

[1233] *Wunderlich* 2010, 47; zu solchen kostenlosen Diensten siehe auch oben Kap. 2.3.7.1.

[1234] Wohl der gleichen Ansicht *Söbbing*, in: Leible/Sosnitza, Onlinerecht 2.0: Alte Fragen – neue Antworten? Cloud Computing – Datenschutz – Urheberrecht – Haftung, 46.

[1235] BGH, NJW-RR 1993, 178.

[1236] BGH, NJW-RR 1993, 178.

[1237] *Waller*, ITRB 2005, 162; *Kammel*, in: Kilian/Heussen, Computerrechtshandbuch, Teil 17, Rn. 132; *Leupold/Glossner*, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, 2008, Teil 2, Rn. 20.

3.5.2 Back-to-Back-Verträge zwischen Cloudprovidern und Subunternehmen

Da sich die meisten Cloudprovider Subunternehmen als Ressourcenanbieter bedienen, ist es notwendig, dass diese Beziehung vertraglich geregelt ist. Diese Verträge werden als Back-to-Back-Agreements bezeichnet.[1238] Der Cloudanbieter ist bestrebt seine Verpflichtungen und Haftungsrisiken gegenüber dem Cloudnutzer an den Ressourcenanbieter durchzureichen. So ist es für den Fall, dass ein Anbieter mit dem Cloudkunden spezielle Service Levels vereinbart hat, aus dessen Sicht notwendig, dass er sich im Verhältnis zum Ressourcenanbieter durch solche Back-to-Back-Verträge absichert. Dies erfolgt dadurch, dass diese Verträge die Anforderungen der Kunden eins-zu-eins auch im Verhältnis zum Ressourcenanbieter widerspiegeln. Allerdings werden sich nicht alle Ressourcenanbieter auf solche Verträge einlassen.[1239]

3.5.3 Service Level Agreements (SLAs)

In der IT- und TK-Branche ist die Verwendung von Service Level Agreements (SLAs) weit verbreitet. Sie stammen zwar aus dem angloamerikanischen Raum, haben sich aber auch in Deutschland in der Praxis schnell durchgesetzt.[1240] SLAs sind auch im Kontext des Cloud Computing ein anerkanntes Instrument und eine übliche Vertragsform im Sinne des § 311 Abs. 1 BGB zur Festlegung und Beschreibung der regelungsbedürftigen Vertragsinhalte.

Üblicherweise sind SLAs als Anhang zu einem Rahmenvertrag ausgestaltet. Während der Rahmenvertrag die grundsätzlichen Rechte und Pflichten der Parteien regelt, sind die Details in den SLAs festgehalten.[1241] Gegenüber einem einheitlichen Vertrag besteht der Vorteil, dass die SLAs als Anlage den aktuellen Anforderungen angepasst werden können, ohne den Rahmenvertrag ändern zu müssen.[1242]

Rechtlich werfen SLAs, neben der Frage der angebrachten und notwendigen Regelungsinhalte, gewisse spezifische Probleme aus dem AGB-Recht auf.

3.5.3.1 Funktion und Formen

SLAs sind nach der wörtlichen Übersetzung „Leistungsstandardvereinbarungen“ oder „Dienstgütevereinbarungen“ und haben mehrere Funktionen.[1243]

[1238] *Karger/Sarre*, in: Taeger/Wiebe, Inside the Cloud, 433; *Söbbing*, Cloud Computing von der juristischen Seite, http://www.computerwoche.de/management/compliance-recht/1904060/index4.html.

[1239] *Karger/Sarre*, in: Taeger/Wiebe, Inside the Cloud, 433.

[1240] *Schumacher*, MMR 2006, 12.

[1241] *Lütcke/Bähr*, K&R 2001, 83; *Schumacher*, MMR 2006, 13.

[1242] *Lütcke/Bähr*, K&R 2001, 83.

[1243] *Rath*, K&R 2007, 362; *Schumacher*, MMR 2006, 12; *Meyer-Spasche*, HMD – Praxis der Wirtschaftsinformatik, Heft 275, 2010, 71.

Primär dienen sie dazu, wie die Übersetzung andeutet, mit den darin festgeschriebenen Service Levels die Qualität der Leistung zu beschreiben und festzulegen. Hintergrund für die Notwendigkeit einer solchen Festschreibung der Leistung ist die Regelung in § 243 Abs. 1 BGB, wonach Leistungen von „mittlerer Art und Güte" geleistet werden müssen, soweit nichts anderes bestimmt ist.[1244] Dieser gesetzliche Maßstab der „mittleren Art und Güte" ist allerdings im Zusammenhang mit Cloud- und IT-Dienstleistungen in der Praxis untauglich, denn der Kunde benötigt maßgeschneiderte Vereinbarungen, die auf seine individuellen Bedürfnisse zugeschnitten sind.[1245] Ganz besondere Bedeutung haben dabei Festlegungen über die Zeiträume der Leistungsbereitschaft und die Verfügbarkeit der Dienste.[1246]

Die zweite wichtige Funktion ist die individuelle Regelung der Rechtsfolgen, wenn die Vereinbarungen nicht eingehalten wurden, beispielsweise wenn Leistungen schlecht oder überhaupt nicht erbracht werden. Die gesetzlichen Regelungen werden dabei als teilweise dispositives Recht durch die Individualvereinbarungen ersetzt. Die unmodifizierten gesetzlichen Regelungen führen im IT-Bereich nämlich zu unbilligen Ergebnissen, da diese nicht auf IT-Sachverhalte „passen".[1247] Insbesondere sind die Nutzer von den Leistungen der Provider abhängig und daran interessiert, dass eine streitige Situation möglichst schnell behoben wird. Diese Zeitabhängigkeit führt dazu, dass die gesetzlichen Gewährleistungsrechte und Rechtsfolgen mit Gerichtsverfahren und späteren Urteilen dem Nutzer nicht dienlich sind und dieser eine rasche und verbindliche Klärung anstrebt, um die Leistungen der Provider wieder nutzen zu können. Insbesondere die ausschließliche Nutzung von IT-Leistungen aus der Cloud zeigt diese Abhängigkeit und das Bedürfnis nach einer schnellen Einigung und Fortsetzung der Leistung. Die Abhängigkeit kann aber durch Alternativanbieter und offene Standards und die damit einhergehende Flexibilität reduziert werden.

Bei diesen individuell vereinbarten Rechtsfolgen ist jedoch zu beachten, dass durch die Vereinbarungen Minderungsrechte nicht beschränkt werden und dass eventuelle Vereinbarungen über pauschalierten Schadensersatz die Haftung nicht beeinträchtigen.[1248] Die Haftungsregelungen sind zudem auch nur eingeschränkt abdingbar, wie man an § 276 Abs. 3 BGB sehen kann.[1249]

[1244] *von dem Bussche/Schelinski*, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, 2011, Teil 1, Rn. 375; *Schiemann*, in: Staudinger, BGB, § 243, Rn. 46; *Rath*, Die zehn größten rechtlichen Risiken, http://www.computerwoche.de/management/it-services/2364751/index2.html.

[1245] *Schumacher*, MMR 2006, 12.

[1246] Siehe dazu Kap. 3.5.3.2.

[1247] *Schumacher*, MMR 2006, 13; *Rath*, K&R 2007, 362.

[1248] *Redeker* 2007, Rn. 641c.

[1249] *Söbbing*, in: Leible/Sosnitza, Onlinerecht 2.0: Alte Fragen – neue Antworten? Cloud Computing – Datenschutz – Urheberrecht – Haftung, 43.

Weitere Funktionen von SLAs sind solche definierender Art. So kann beispielsweise die Leistungsbeschreibung so konkret sein, dass diese als eine Art Betriebshandbuch fungiert. Zudem können Marketingfunktionen die objektive Vergleichbarkeit der Leistungen mit Mitbewerbern ermöglichen. Auch die Investitionssicherheit ist als Funktion zu beachten, weil durch das detaillierte Festhalten der zu erbringenden Leistungen die entstehenden Kosten bestimmbar und planbar werden.[1250]

3.5.3.2 Vertragsgestaltung und konkrete Regelungsinhalte

Bei der konkreten Ausfertigung von Service Level Agreements zwischen Cloudprovidern und Cloudnutzern ist eine Orientierung an den bereits bekannten Outsourcingverträgen sinnvoll.[1251] Die im Folgenden angedeutete Vertragsgestaltung hat sich im Laufe des langjährigen Praxiseinsatzes von SLAs bewährt.

3.5.3.2.1 Leistungspflichten und Leistungsbeschreibung

Der Leistungsbeschreibung und den Leistungspflichten, als wichtigstem Teil, kann ein Rahmenvertrag vorgehen. Zudem ist es manchmal notwendig, die wichtigsten Begriffe vorab zu definieren.[1252]

Die Leistungspflichten beschreiben, was die Parteien jeweils vertraglich erfüllen müssen. Bei Cloud Computing muss der Provider dem Kunden Zugriff auf die Dienste ermöglichen und die vereinbarten Dienstleistungen in Form von Rechenleistung, Speicherplatz, Plattformdiensten oder Software erbringen. Die Einzelheiten richten sich nach dem Bereitstellungsmodell (IaaS, PaaS, SaaS) und dem konkreten Angebot des Providers. Wegen der homogenen Bereitstellung haben die Kunden selten die Möglichkeit, spezifische Anforderungen und Wünsche umsetzen zu lassen. Ein Merkmal der SLAs im Cloudbereich ist deswegen die faktische Vorgabe der Leistungspflichten durch den Cloudprovider.

Die Hauptleistungspflicht des Kunden liegt in der Bezahlung der in Anspruch genommenen Leistungen. Diese Zahlungspflicht wird in der Regel im Rahmenvertrag, falls ein solcher verwendet wird, festgehalten.

Leistungsbeschreibungen umfassen zudem die Festlegung der Qualität und Quantität der Leistungen. Zur Qualität (QoS) gehört, neben der Verfügbarkeit der Services als wichtigster Regelung, auch die Möglichkeit des Kunden, die Qualität überprüfen zu können (Monitoring und Service Level Management).[1253]

Gerade im Bereich Cloud Computing ist es wichtig, Vereinbarungen über die notwendigen Sicherheitsmaßnahmen zu treffen. Insbesondere sind die Anforderungen des § 9 BDSG samt Anlage stets und die Vorgaben des § 11 BDSG bei einer Auf-

---

[1250] *Schumacher*, MMR 2006, 13.
[1251] *Lütcke/Bähr*, K&R 2001, 83 ff.
[1252] *Lütcke/Bähr*, K&R 2001, 84.
[1253] Zum Service Level Management siehe auch Kap. 3.5.3.2.4.

tragsdatenvereinbarung zu beachten. Die Anforderungen aus § 11 BDSG können in einer schriftlichen Vereinbarung niedergelegt werden. Für manche Anforderungen ist eine solche Schriftlichkeit ohnehin gesetzlich vorgeschrieben.[1254] Für den Fall, dass sonstige Sicherheitsmaßnahmen oder sogar umfassende Sicherheitskonzepte vereinbart werden sollen, sind diese im Vertragstext ausdrücklich zu benennen und ihre Schutzrichtung zu umschreiben. Ab einem gewissen Umfang ist eine Zusammenfassung in gesonderten Security Service Level Agreements (SSLA) sinnvoll.

Neben den Sicherheitsmaßnahmen sind die Weisungsbefugnisse des Nutzers, etwaige Berechtigungen zur Begründung von Unterauftragsverhältnissen, die Art und Weise der Kontrollen oder auch die Datenrückgabe und Löschverpflichtungen bei Beendigung des Vertragsverhältnisses zu beachten. Eine nicht abschließende Orientierung, was geregelt werden muss, bieten die vorbenannten Vorschriften.

3.5.3.2.2 Reaktions- und Mängelbeseitigungsfristen

Neben der Leistungsbeschreibung sind auch die Reaktions- und Mängelbeseitigungsfristen ein wichtiger Teil von SLAs. Diese regeln, wie und in welchem Zeitraum der Provider reagieren muss, wenn die Verfügbarkeit des Clouddienstes nicht mehr gewährleistet ist, also der Dienst an sich oder Teile davon ausgefallen sind oder nicht richtig funktionieren.[1255] Dabei ist zu beachten, dass nur solche Ausfälle dem Provider zurechenbar sind, die providereigene oder angemietete Dienste von Subunternehmen betreffen. Nur diese sind Regelungsinhalt und damit sanktionsbewehrt.

Fällt hingegen der Internetzugang aus, der üblicherweise von einem vom Cloudprovider unabhängigen Telekommunikationsanbieter bereitgestellt wird, so ist dies nicht dem Cloudprovider anzulasten. Soweit TK-Dienste und Clouddienste durch einen Provider als Generalunternehmer aus einer Hand bereit gestellt werden, müsste dieser Umstand bei der Abfassung der Verfügbarkeitsklauseln gesondert berücksichtigt werden.

3.5.3.2.3 Verfügbarkeit und Latenzzeiten

Eher technischer Natur, aber für die Nutzungsfähigkeit von essentieller Bedeutung, sind die Verfügbarkeit der Dienste und die Latenzzeiten. Die Verfügbarkeit wird, wie oben schon für einige Amazon-Dienste beispielhaft erläutert, üblicherweise in Prozent für einen gewissen Zeitraum angegeben. Bei der Vereinbarung der erlaubten Ausfallzeiten ist insbesondere auf den vereinbarten Nutzungszeitraum zu achten. Eine Verfügbarkeit von 99,9 % pro Kalendermonat bedeutet zum Beispiel, dass der Service in jedem einzelnen Monat der Vertragslaufzeit für 43,2 Minuten am Stück ausfallen kann. Die vermeintlich höhere Verfügbarkeit von 99,95 % pro Ka-

---

[1254] Siehe dazu beispielsweise Kap. 3.1.8.5.1.

[1255] *Redeker* 2007, Rn. 641a; zur Verfügbarkeit siehe sogleich Kap. 3.5.3.2.3.

lenderjahr bedeutet hingegen, dass bis zu 4,38 Stunden am Stück ausfallen können, ohne dass dem Kunden Schadensersatzansprüche zustünden.[1256] Der vereinbarte Nutzungszeitraum bestimmt damit indirekt die Länge des, vor allem am Stück möglichen, Ausfallzeitraums.

Während die Verfügbarkeit Dienstausfälle betrifft, sind die Latenzzeiten Indikatoren für das Antwortverhalten der Dienste. Neben überlasteten Internetzugängen kann auch der Cloudservice an sich durch Fehler oder eine Überlastung so langsam reagieren, dass eine Nutzung nur noch erschwert möglich ist. Ab wann eine Nutzung unzumutbar oder unmöglich ist, sollte ebenfalls vorab vertraglich festgelegt werden. Zudem muss nachweisbar sein, dass die Ursache beim Cloudprovider und nicht beim Internetzugangsanbieter liegt. Mögliche Schlechtleistungen Dritter, die die Bereitstellung der Leistung durch den Cloudprovider beeinträchtigen, sind also ebenfalls in den SLAs anzusprechen.[1257]

Darüber hinaus ist eine vertragliche Regelung und Klärung sinnvoll, wie mit notwendigen Wartungen und damit möglicherweise einhergehenden Unterbrechungen oder Störungen umgegangen wird.

3.5.3.2.4 Service Level Management

Um Fehler und Ausfälle ahnden zu können, müssen die Leistungen des Providers durch den Kunden überprüfbar sein. Es ist demnach in den Vertrag aufzunehmen, wie genau dieses sogenannte „Service Level Management“ aussehen und tatsächlich erfolgen soll. Ein solches Management besteht üblicherweise aus zwei Phasen, nämlich aus der Vereinbarung der Leistung, zum Beispiel über die Servicequalität (Quality of Service), und aus der Überwachung dieser Leistung (Service Monitoring) durch den Kunden.

Die gegenwärtigen Cloudangebote legen den Fokus auf die Erfüllung der vereinbarten Leistung nach dem Best-Effort-Prinzip.[1258] Die Angebote sind dabei in der Regel gleichartig und werden als Self-Service angeboten. Individuelle Absprachen und Vereinbarungen sind noch unüblich, da diese für den Cloudanbieter zusätzlichen Aufwand bedeuten.[1259] Die Überwachungsmaßnahmen sind dementsprechend nur in Grundzügen notwendig und zudem für alle Leistungen einheitlich möglich. Mit

---

[1256] Siehe auch *Meyer-Spasche*, HMD – Praxis der Wirtschaftsinformatik, Heft 275, 2010, 72 und obige Fn. 334. Dass solche längeren Ausfälle von Clouddiensten nicht unwahrscheinlich sind, hat der Ausfall der Amazoncloud in Teilen der USA im April 2011 gezeigt; siehe dazu zusammenfassend *Amazon*, Summary of the Amazon EC2 and Amazon RDS Service Disruption in the US East Region, http://aws.amazon.com/message/65648.

[1257] *Pohle/Ammann*, K&R 2009, 628.

[1258] „Best Effort“ steht für den „nach bestem Wissen und Gewissen“-Ansatz, bei dem der Betreiber verspricht „sein Möglichstes zu tun“, ohne jedoch irgendwie geartete Garantien zu geben; *Marnau/Schirmer/Schlehahn/Schunter*, DuD 2011, 335.

[1259] *Baun/Kunze/Nimis/Tai* 2009, 60.

dem Anbieten individueller SLAs müssen die Überwachungs- und Monitoringverfahren allerdings an die speziellen Vereinbarungen angepasst werden.

3.5.3.2.5 Sanktionen

Es ist gerade im Cloudumfeld wichtig, Messverfahren zu vereinbaren, mit denen festgestellt werden kann, ob die vereinbarten Qualitätskriterien eingehalten wurden und Verstöße dagegen zu sanktionieren.[1260] Als Sanktionen sind Vertragsstrafen, die Kürzung der Vergütung, pauschalierter Schadensersatz[1261] oder auch fristlose Kündigungen möglich.[1262]

Vertragsstrafen oder Pönalen sind in den §§ 339 ff. BGB geregelt. Sie dienen als präventives Druckmittel, um den Vertragspartner anzuhalten seine Leistungsverpflichtungen überhaupt (§ 340 Abs. 1 Satz 1 BGB) oder in gehöriger Weise zu erfüllen (§ 341 Abs. 1 Satz 1 BGB). Konkret sind Vertragsstrafen vorab vereinbarte Geldsummen, die bei einem Verstoß gegen die Leistungsverpflichtungen fällig werden. Sie können unabhängig von einem entstandenen Schaden verlangt werden.[1263] Vertragsstrafen können verschuldensabhängig oder verschuldensunabhängig vereinbart werden, wobei in SLAs in der Regel Letzteres der Fall ist.[1264]

Eine zweite Sanktionsmöglichkeit ist der pauschalierte Schadensersatz. Dieser dient der vereinfachten Durchsetzung eines Schadensersatzanspruchs, wobei der Nachweis über die tatsächliche Höhe des Schadens nicht nötig ist. Der Vertragspartner muss nur beweisen, dass ihm überhaupt ein Schaden entstanden ist.[1265]

Bei Fehlverhalten ist zudem die fristlose Kündigung des Vertragsverhältnisses als Sanktionsmöglichkeit in Betracht zu ziehen. Insbesondere die außerordentliche Kündigung sollte in den SLAs geregelt werden, da die gesetzliche Regelung in § 314 Abs. 1 Satz 1 BGB lediglich von einem „wichtigen Grund“ spricht und solche Gründe in Satz 2 nur sehr allgemein umschreibt. Es bietet sich deshalb an, wichtige Gründe vorab vertraglich zu bestimmen. Außerdem ist die Festlegung sinnvoll, ob ein Kunde den ganzen Vertrag oder nur die mangelhaft erbrachte Leistung kündigen darf.[1266]

Auch im Verhältnis des Nutzers zum Provider können Sanktionen eine Rolle spielen. Dieser Fall äußert sich in der Praxis vor allem im Privatkunden- und Verbrau-

---

[1260] *Redeker* 2007, Rn. 641b.

[1261] Auch als „pauschalisierter Schadensersatz“ bezeichnet.

[1262] Näheres hierzu siehe zum Beispiel bei *Meyer-Spasche*, HMD – Praxis der Wirtschaftsinformatik, Heft 275, 2010, 72.

[1263] RGZ 103, 99; BGHZ 63, 260; *Söbbing*, in: Leible/Sosnitza, Onlinerecht 2.0: Alte Fragen – neue Antworten? Cloud Computing – Datenschutz – Urheberrecht – Haftung, 56.

[1264] *Söbbing*, in: Leible/Sosnitza, Onlinerecht 2.0: Alte Fragen – neue Antworten? Cloud Computing – Datenschutz – Urheberrecht – Haftung, 57.

[1265] *Schumacher*, MMR 2006, 16; *Schuster*, CR 2009, 209.

[1266] *Schumacher*, MMR 2006, 17.

cherbereich durch die einseitige Vorgabe des Providers in Form von sanktionsbewehrten Nutzungsbedingungen. Sanktionen ergeben sich dabei unmittelbar aus dieser Vereinbarung zwischen Nutzer und Provider und haben in der Regel Fehlverhalten der Nutzer zum Inhalt. Gravierende Verstöße gegen diese Bedingungen, wie die Begehung von Straftaten, resultieren in der Beendigung des Vertragsverhältnisses bis hin zur Anzeige bei Strafverfolgungsbehörden. Dies ist vor allem dem Umstand geschuldet, dass Cloudservices selbst als neuartige Tatmittel dienen können, um Straftaten zu begehen.[1267]

Nichtabdingbare Nutzungsbedingungen können unter Umständen dazu führen, dass der Provider spezifische Nutzungsabsichten von vornherein nicht toleriert. Neben offensichtlich illegalen Nutzungsabsichten ist auch zum Beispiel die Nutzung der Services für legale, aber kritische Anwendungen, die Gesundheitsschäden oder sogar den Tod von Menschen zur Folge haben können, oft ausgeschlossen.[1268]

3.5.3.2.6 Vertragsbeendigung und weiterer Umgang mit Daten (Exit Management)

Unabhängig davon, wie die Vertragsbeendigung erfolgt, muss gerade in Cloudszenarien der weitere Umgang mit den vorhandenen Daten vertraglich geklärt werden, soweit nicht bereits rechtliche Vorgaben dazu bestehen. Neben einer sicheren Löschung, geht es in der Regel um die Rückübertragung der Daten an den Nutzer. Hinsichtlich einer Löschung personenbezogener Daten ist zum Beispiel § 35 Abs. 2 BDSG als eine solche rechtliche Vorgabe einschlägig.

Für die Rückübertragung sollten spezifische Vereinbarungen getroffen werden, wobei auch die Datensicherheit zu beachten ist.[1269] Beim Provider weiter vorhandene Daten, Datenfragmente oder auch Protokoll- und Metadaten sollten ebenso berücksichtigt werden. Vor allem die Löschung von Daten sollte unwiederbringlich erfolgen und der Erfolg einer solchen Löschung oder Datenzerstörung, soweit technisch machbar, nachgewiesen werden. Vor allem die dezentrale Verteilung der Daten kann sich dabei als problematisch erweisen.

Um die Datenportierung planbar zu gestalten, bietet es sich an Fristen zu vereinbaren, so dass die Daten innerhalb eines festgelegten Zeitraums vollständig auf Infrastrukturen des ehemaligen Kunden oder zum neuen Provider übertragen werden können. Insbesondere wenn (teilweises) Vendor Lock-in eine Rolle spielt, sollte

---

[1267] Beispiele und Einzelheiten hierzu siehe auch in Kap. 3.1.9.10.6.

[1268] *Bradshaw/Millard/Walden* 2010, 20; dass solche Gesundheitsbedenken nicht aus der Luft gegriffen sind, zeigt der mehrtägige Ausfall der Amazoncloud in den USA, wobei ein „Monitoringunternehmen“ als Cloudnutzer den Zustand hunderter Patienten mit Herzbeschwerden nicht mehr überwachen konnte; https://forums.aws.amazon.com/thread.jspa?threadID=65649&tstart=0.

[1269] Zum Beispiel der Transport verschlüsselter Datenträger oder die leitungsgebundene verschlüsselte Übermittlung.

geklärt werden, wie lange der Nutzer die Daten beim Provider vorhalten kann, ohne dass diese gelöscht werden und welche Konditionen in solchen Fällen gelten sollen. Es darf vor allem nicht so weit kommen, dass der Provider die Daten ohne die Abstimmung mit dem ehemaligen Kunden löscht. Gerade die kurzfristig eingegangenen Beziehungen und das Massengeschäft bei Cloud Computing bergen die Gefahr einer übereilten Löschung.

3.5.3.2.7 Urheber- und Nutzungsrechte

Weitere rechtlich klärungsbedürftige Punkte umfassen die Urheber- und Nutzungsrechte an hochgeladenen Daten oder Software. Während mögliche Nutzungsrechte an Daten bei allen Cloudschichten zu regeln sind, betrifft Software im wesentlichen PaaS und die auf der Plattform entwickelten Programme. Manche Anbieter lassen sich sogar Nutzungsrechte an den eingebrachten Daten oder der entwickelten Software einräumen, um dann ihrerseits damit Geschäfte zu betreiben.[1270]

3.5.3.2.8 Datenschutz, Rechtswahl und Gerichtsstand

Durch datenschutzrechtliche Vorgaben aus den §§ 9 und 11 BDSG gibt es erheblichen vertraglichen Regelungsbedarf.[1271] Auch sonstige individuelle Zusicherungen, beispielsweise hinsichtlich der Inanspruchnahme von Subunternehmern oder die territorial begrenzte Speicherung, sind in SLA oder bereits im Rahmenvertrag festzuhalten. Ebenso sind bei einer Grenzüberschreitung die internationalen Rechtsfragen, beispielsweise die Nutzung von EU-Standardvertragsklauseln, abzuklären. Dazu gehören auch, soweit dies wegen Verbraucherschutzvorschriften überhaupt möglich ist, die Vereinbarung des anwendbaren Rechts oder Gerichtsstandsvereinbarungen für den Fall einer künftigen gerichtlichen Auseinandersetzung. Bisweilen kann auch die Vereinbarung eines vorlaufenden Schiedsgerichtsverfahrens angebracht sein. Zu den konkreten rechtlichen Voraussetzungen sei auf die obigen Ausführungen zum Datenschutzrecht und zum internationalen Privatrecht verwiesen.[1272]

3.5.3.3 Einschränkungen durch AGB-Recht

SLAs sind wegen der Vertragsfreiheit individuell vereinbar, unterliegen jedoch bei mehrfacher Verwendung der Inhaltskontrolle gemäß § 307 BGB. Während in Individualverträgen die meisten Vorschriften abbedungen werden können, ist dies bei der Einordnung als AGB gemäß § 305 ff. BGB nur noch unter erschwerten Bedingungen möglich. Gemäß § 307 Abs. 2 Nr. 1 BGB sind die wesentlichen Grundgedanken einer gesetzlichen Regelung in den AGB beizubehalten, da ansonsten unter Umständen eine unangemessene Benachteiligung des Vertragspartners des Verwen-

---

[1270] So wurden bereits die Beispiele Twitpic und Facebook weiter oben in Kap. 3.1.9.10.3 erwähnt; solche umfassenden und fest vorgegebenen Regelungen über Nutzungsrechte sind nach Erkenntnissen von *Bradshaw/Millard/Walden* 2010, 31 aber die Ausnahme.

[1271] Siehe auch Fn. 1254.

[1272] Siehe Kap. 3.1.5.4 und 3.4.

ders, also des Cloudkunden, im Raum steht. Diese Einschränkung kann zu einer Erschwerung der Ausgestaltung der Verträge führen, da die gesetzlichen Regelungen nur eingeschränkt mit modernen Formen des Outsourcings vereinbar sind.[1273] Eine Ausnahme von diesem Grundsatz ist die bereits oben angesprochene Abdingbarkeit der verschuldensunabhängigen Garantiehaftung des Vermieters.[1274]

Eine weitere AGB-Regelung zur Haftung ist das Haftungsfreizeichnungsverbot gemäß § 309 Nr. 7 BGB. Die meisten Anbieter versuchen nämlich ihre Haftung, soweit dies gesetzlich möglich ist, auszuschließen.[1275] Das Haftungsfreizeichnungsverbot findet insbesondere auch auf die Haftung aus unerlaubter Handlung Anwendung, wie nicht zuletzt in § 309 Nr. 7 lit. a) BGB zu sehen ist.[1276]

Für Cloud Computing ist allerdings § 309 Nr. 7 lit. b) BGB einschlägiger, da dieser nicht wie lit. a) Personenschäden, sondern als „sonstige Schäden" Vermögens- und Sachschäden betrifft. Gemäß § 309 Nr. 7 lit. b) BGB ist ein Ausschluss oder eine Begrenzung der Haftung für Schäden, die auf einer grob fahrlässigen Pflichtverletzung des Verwenders, also des Providers, oder auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung eines gesetzlichen Vertreters oder Erfüllungsgehilfen des Verwenders beruhen, unwirksam. Eine ähnliche und allgemeine Regelung findet sich für groben Vorsatz im Übrigen in § 276 Abs. 3 BGB, wonach die Haftung wegen Vorsatzes dem Schuldner nicht im Voraus erlassen werden kann.

Bei der Vorschrift ist zu beachten, dass diese nur die Höchstgrenze aufzeigt, ab der entsprechende Klauseln immer unwirksam sind. Wenn nämlich die Schadensersatzhaftung des Verwenders zur Sicherstellung der ordnungsgemäßen Vertragserfüllung unverzichtbar ist, kann sich dieser deshalb auch nicht für einfache Fahrlässigkeit freizeichnen.[1277] Dabei ist immer nach § 307 BGB ergänzend zu prüfen, ob der Haftungsausschluss oder die Haftungsbeschränkung die Verwendergegenseite unangemessen benachteiligt.[1278] Nach ständiger Rechtsprechung liegt eine unangemessene Benachteiligung bei der Verletzung von vertragswesentlichen Pflichten vor.[1279] Bei der Verletzung solcher sogenannter Kardinalpflichten und der Gefährdung des Ver-

---

[1273] *Söbbing*, in: Leible/Sosnitza, Onlinerecht 2.0: Alte Fragen – neue Antworten? Cloud Computing – Datenschutz – Urheberrecht – Haftung, 43; vergleiche hierzu auch die obige Problematik des Schuldens einer „Sache von mittlerer Art und Güte" gemäß § 243 Abs. 1 BGB.

[1274] Siehe oben Kap. 3.5.1.

[1275] Einzelheiten bei *Bradshaw/Millard/Walden* 2010, 32 ff.; insbesondere nach US-Recht sind laut *Bradshaw/Millard/Walden* 2010, 33 weiträumige Haftungsfreizeichnungen möglich, so dass US-Provider hiervon in der Praxis extensiven Gebrauch machen.

[1276] *Becker*, in: Bamberger/Roth, BeckOK BGB, § 309 Nr. 7, Rn. 4.

[1277] *Becker*, in: Bamberger/Roth, BeckOK BGB, § 309 Nr. 7, Rn. 6.

[1278] *Becker*, in: Bamberger/Roth, BeckOK BGB, § 309 Nr. 7, Rn. 20.

[1279] BGH, NJW 1968, 1567; BGH, NJW 1990, 764; BGH, NJW 2001, 292.

tragszwecks ist demnach lediglich eine Begrenzung auf das vertragstypische vorhersehbare Risiko zulässig.[1280]

Haftungsbeschränkungen auf einen bezifferten oder bezifferbaren Höchstbetrag sind dann unwirksam, wenn dieser Betrag nicht die vertragstypisch vorhersehbaren Schäden abdeckt. Um zulässig zu sein, müssen sie also in einem angemessenen Verhältnis zum vertragstypischen Risiko stehen.[1281]

Die Einordnung als Kardinalpflicht ist vom jeweiligen Einzelfall und von eventuellen Individualvereinbarungen abhängig. Auch das vertragstypisch vorhersehbare Risiko ist nicht nur fallabhängig, sondern gerade bei neuartigen Clouddiensten noch weitestgehend unklar. Mit der absehbaren Durchsetzung von Clouddiensten im Alltag wird sich dazu künftig voraussichtlich eine angepasste Rechtsprechung entwickeln.

Für Privatnutzer sind zudem die Haftungsregeln bei der Inanspruchnahme unentgeltlicher Leistungen und bei Gefälligkeitsverhältnissen zu beachten, da die meisten Clouddienste für diesen Personenkreis unentgeltlicher Art sind. In der Regel besteht zwischen Nutzer und Anbieter ein Vertrag in Form von Nutzungsbedingungen. Bei unentgeltlichen Leistungen gilt ein verminderter Haftungsmaßstab, wie dies beispielsweise für die Leihe gemäß § 599 BGB bereits weiter oben im Rahmen der vertragstypologischen Einordnung festgestellt wurde.

Vollständige Haftungsausschlüsse sind nicht nur bei unentgeltlichen Leistungen, sondern grundsätzlich zulässig, soweit nicht § 276 Abs. 3 BGB oder AGB-Recht mit den soeben erwähnten Konsequenzen eingreifen. Gemäß § 444 BGB lässt auch das arglistige Verschweigen eines Mangels oder die Übernahme einer Garantie einen Haftungsausschluss oder eine Haftungsbeschränkung unwirksam werden.

Soweit die SLAs Leistungsversprechen oder Leistungsbeschreibungen beinhalten, unterliegen diese Teile gemäß § 307 Abs. 3 BGB nicht dem AGB-Recht.[1282]

3.5.4 Bedeutung von DIN SPEC 1041

Der DIN e.V. hat im April 2010 nach vorheriger Zusammenarbeit mit der Universität Hamburg und Vertretern der Industrie die Spezifikation DIN SPEC 1041 für das Outsourcing technologieorientierter wissensintensiver Dienstleistungen[1283] veröf-

---

[1280] *Söbbing*, in: Leible/Sosnitza, Onlinerecht 2.0: Alte Fragen – neue Antworten? Cloud Computing – Datenschutz – Urheberrecht – Haftung, 50; *Becker*, in: Bamberger/Roth, BeckOK BGB, § 309 Nr. 7, Rn. 21.

[1281] BGH, NJW 1984, 1350; BGH, NJW 1985, 3016; *Becker*, in: Bamberger/Roth, BeckOK BGB, § 309 Nr. 7, Rn. 29.

[1282] *von Westerholt/Berger*, CR 2002, 87; *Söbbing*, in: Leible/Sosnitza, Onlinerecht 2.0: Alte Fragen – neue Antworten? Cloud Computing – Datenschutz – Urheberrecht – Haftung, 56; *Rath*, K&R 2007, 365.

[1283] Sogenannte T-KIBS (Technology-Oriented Knowledge-Intensive Business Services).

fentlicht.[1284] Technologieorientierte wissensintensive Dienstleistungen betreffen sowohl das Outsourcing von Geschäftsprozessen (Business Process Outsourcing) als auch das Outsourcing von Informationstechnologie (Information Technology Outsourcing).[1285]

Die Spezifikation dient insbesondere dazu, das Outsourcing von kleinen und mittelständischen Unternehmen nach einem Standardvorgehen zu erleichtern und soll maßgeblich die Vorbereitung von Outsourcing-Projekten unterstützen.[1286] Gerade kleineren Unternehmen mangelt es an Erfahrung mit der Umsetzung von IT-Projekten. DIN SPEC soll es diesen erleichtern, komplexe Projekte in Eigenregie zu bewältigen, ohne dafür teure externe Berater heranziehen zu müssen.[1287]

Das Standardvorgehen gliedert sich in vier Phasen, nämlich Prozessanalyse und Redesign, Entwurf der Organisation der Outsourcingbeziehung, Service-Provider-Auswahl und schließlich Servicemigration und Regelbetrieb. Der Bezug zum Vertragsrecht ergibt sich aus dem Umstand, dass Service Level Agreements und deren Ausgestaltung in der Spezifikation erwähnt werden.[1288] Aus diesen vier Phasen sollen die wesentlichen Ergebnisse Eingang in die SLAs finden. Die in den SLA zu regelnden Inhalte betreffen die Servicebeschreibung und Serviceeigenschaften, Kontroll- und Messinstrumente, Überwachungs- und Berichtswesen, Mitwirkungspflichten, Bonus-Malus-Regelungen, Vergütungsregelungen und Zuständigkeiten und Ansprechpartner.[1289]

Aus rechtlicher Perspektive ist weiterhin erwähnenswert, dass die Spezifikation im Anhang C zwischen typischen rechtlichen Problemstellungen unterscheidet, die im Rahmen von Outsourcingprojekten auftreten können. Die relevanten Rechtsvorschriften sind nach Rechtsbereichen sortiert und umfassen neben arbeits-, steuer- und urheberrechtlichen Vorschriften auch das Datenschutzrecht. Ziel ist es, die Prüfung der Compliance, also der Einhaltung von Gesetzesvorschriften aus den eben genannten Rechtsbereichen, zu ermöglichen.[1290]

DIN SPEC 1041 betrifft zwar nicht speziell Outsourcing in Form des Cloud Computing, jedoch können daraus wichtige Einsichten für eine geplante oder durchzu-

---

[1284] *Nüttgens/Gehrke* 2010, 1 ff.; *Klett/Hilberg*, CR 2010, 417; http://www.dinspec1041.de/index.php?option=com_content&view=article&id=55&Itemid=53.

[1285] *DIN*, Outsourcing von T-KIBS, http://www.dinspec1041.de/index.php?option=com_content&view=article&id=53&Itemid=56.

[1286] *Klett/Hilberg*, CR 2010, 417, 418.

[1287] *Klett/Hilberg*, CR 2010, 418; *Nüttgens/Gehrke* 2010, 12 ff.

[1288] *Nüttgens/Gehrke* 2010, 38 ff.

[1289] *Klett/Hilberg*, CR 2010, 418, 419; *Nüttgens/Gehrke* 2010, 39; siehe dazu auch Kap. 3.5.3.2.

[1290] *Nüttgens/Gehrke* 2010, 63 ff.; *Klett/Hilberg*, CR 2010, 418, 419; zur Compliance siehe die anschließenden Ausführungen.

führende Auslagerung von IT-Services in die Cloud gewonnen werden.[1291] Insbesondere das standardisierte Vorgehen dürfte projektplanungsunerfahrenen Entscheidern in kleinen und mittleren Unternehmen die Migration in die Cloud erleichtern.

3.6 Compliance und Aufbewahrungspflichten

Die sogenannte „Compliance“, zu übersetzen mit „Befolgung“ oder „Rechtsbefolgung“, bedeutet die Einhaltung von Gesetzen, Richtlinien und Verhaltensmaßregeln.[1292] Im Folgenden sollen die einschlägigen Vorschriften dargestellt und ihre Bedeutung für Cloud Computing aufgezeigt werden.

3.6.1 Allgemeine Compliancevorschriften, Haftung und Risikomanagement

Die für die Compliance einschlägigen Regeln richten sich an Unternehmen und deren gesetzliche Vertreter und Verantwortliche. Je nach Unternehmensform sind solche Regeln und Vorschriften direkt oder analog anwendbar. Zentral sind die Vorschriften in den §§ 91 Abs. 2, 93 Abs. 2 Satz 1 AktG und § 43 GmbHG, wobei erstere auf dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) aus dem Jahr 1998 beruhen. Grundlage dieser Vorgaben ist die Verantwortlichkeit der Geschäftsleitung für die ordnungsgemäße Organisation der Gesellschaft. Die Mitglieder der Unternehmensleitung haben bei ihrer Tätigkeit die Sorgfalt ordentlicher Geschäftsleute gemäß § 43 GmbHG oder §§ 93, 116 AktG anzuwenden.[1293] Verstöße gegen die Organisationspflichten führen zur persönlichen und gesamtschuldnerischen Haftung der Geschäftsleitung gegenüber der Gesellschaft gemäß § 93 Abs. 2 Satz 1 AktG und § 43 Abs. 2 GmbHG. Für andere Gesellschaftsformen gelten die Vorschriften analog.

Die Einhaltung gewisser Sorgfaltsmaßstäbe gilt im Übrigen unabhängig davon, ob IT ausgelagert wird und ist nicht allein spezifisch für IT-Problemstellungen.[1294] Sie betrifft alle Tätigkeiten der Geschäftsleitung. Allerdings haben die Organisationspflichten mittelbar Einfluss auf eine Auslagerung von Daten und Geschäftsprozessen in die Cloud und für die IT-Sicherheit allgemein. Wegen der hohen Bedeutung der EDV und IT können Nachlässigkeiten in diesen Bereichen leicht zum Bankrott einer Gesellschaft oder der verantwortlichen Personen führen.

Der Begriff „IT-Compliance“ umfasst als Zielsetzung der Compliance im engeren Sinne die Sicherheit der IT während die Compliance im weiteren Sinne die IT als Mittel zur Unternehmenssicherheit meint.[1295] Cloud Computing kann beides betref-

---

[1291] Ähnlich *Rath*, Die zehn größten rechtlichen Risiken, http://www.computerwoche.de/management/it-services/2364751/index2.html.

[1292] *Lensdorf/Steger*, ITRB 2006, 206; *Schmidt*, in: Horster/Schartner, D-A-CH Security 2009, 26.

[1293] *Roth/Schneider*, ITRB 2005, 19.

[1294] *Niemann/Paul*, K&R 2009, 450.

[1295] *Niemann/Paul*, K&R 2009, 450; zu den jeweiligen Unterschieden siehe *Lensdorf* CR 2007, 413.

fen, so dass es geboten ist Regelungen zwischen einem Cloudanbieter und dem cloudnutzenden Unternehmen zu treffen, die der nicht delegierbaren Verantwortung der Unternehmensleitung Rechnung tragen. Solche Vereinbarungen können Steuerungs-, Weisungs- und Kontrollrechte der Unternehmensleitung, Reportingpflichten des Cloudanbieters und ein für Cloud Computing angemessenes IT-Notfallkonzept beinhalten.[1296] Diesen konkreten Maßnahmen kann ein sogenanntes Compliance-Audit vorausgehen, in dem eine Risikeninventur durchgeführt wird und in der sich die Verantwortlichen einen Überblick über die rechtlichen Anforderungen verschaffen.[1297] Alle diese Schritte und Maßnahmen sollten Teil eines unternehmensweiten angemessenen Risikomanagements und eines funktionierenden Überwachungssystems im Sinne des § 91 Abs. 2 AktG sein, die die gesetzliche Pflicht der Geschäftsleitung zur Risikovorsorge ermöglichen und erleichtern. Zielsetzung eines solchen Überwachungssystems ist das frühzeitige Erkennen von Fehlentwicklungen, die den Fortbestand der Gesellschaft gefährden könnten.[1298]

Die Überwachung der IT-Sicherheit im Unternehmen inklusive der oben erwähnten Maßnahmen bei der Auslagerung in Clouds sind zwingende Teile eines solchen Überwachungssystems.[1299] Die Wahrung der IT-Sicherheit ist demzufolge integraler Bestandteil von unternehmerischen Planungs- und Steuerungsprozessen.[1300] Zu einem angemessenen Risikomanagement in IT-Umgebungen gehört zudem ein taugliches Datensicherheitskonzept.[1301] Gegenüber den Unternehmenskunden kann die fehlende Einhaltung und Wahrung der IT-Sicherheit mit der Konsequenz eines Schadens als Verstoß gegen eine ungeschriebene Schutz- und Rücksichtnahmepflicht im Sinne des § 241 Abs. 2 BGB gewertet werden.[1302]

Gerade die Nutzung von Cloudservices und die mangelnde vertragliche Verpflichtung und spätere Überwachung des Cloudanbieters kann für ein Unternehmen erhebliche Konsequenzen nach sich ziehen. So ist es beispielsweise denkbar, dass der Cloudanbieter personenbezogene Daten oder Geschäftsgeheimnisse nicht sicher aufbewahrt, so dass diese einem Konkurrenten in die Hände fallen oder aus Versehen gelöscht werden.

Da die Steuerungsfähigkeit der Unternehmen als Nutzer in einer Public Cloud reduziert ist, wird es umso wichtiger, die Auswahl des Cloudproviders sorgfältig vorzunehmen und im Betrieb auf regelmäßige externe Audits zu bestehen. Auch der Zugang zu Monitoringtools kann die Steuerungsfähigkeit befördern. Ein weiterer

---

[1296] *Niemann/Paul*, K&R 2009, 450.
[1297] *Schmidt*, in: Horster/Schartner, D-A-CH Security 2009, 27.
[1298] *Roth/Schneider*, ITRB 2005, 19.
[1299] *Roth/Schneider*, ITRB 2005, 19; *Heckmann*, MMR 2006, 282.
[1300] *Heckmann*, MMR 2006, 282.
[1301] *Böken*, iX 04/2011, 115.
[1302] *Eckhart*, DuD 2008, 331.

Aspekt ist die Beschränkung der Verarbeitung auf den EWR, so dass sich möglichst wenige rechtliche Probleme ergeben.

3.6.2 Bereichsspezifische Regelungen (Risikomanagement, territoriale Beschränkungen und nationale Aufbewahrungspflichten)

Neben den allgemeinen Complianceregeln gibt es gebietsspezifische regulatorische Vorgaben. Beispiele finden sich in den §§ 25a und 25c KWG, § 33 WpHG, § 16 InvG für Banken, Kreditinstitute oder Wertpapierdienstleistungsunternehmen und in § 64a VAG für Versicherungen. Für deutsche Banken und Finanzinstitute gilt außerdem das Rundschreiben „Mindestanforderungen an das Risikomanagement (MaRisk)“ der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zur Ausgestaltung des konkreten Risikomanagements. Soweit die genannten Institute Cloud Computing nutzen, müssen sie ihr vorhandenes Risikomanagement an die cloudspezifischen Risiken anpassen.

Auch die Vorschrift in § 146 Abs. 2 AO mit der territorialen Beschränkung der Buchführung auf das Inland oder § 146 Abs. 2a AO, wonach mit Genehmigung der zuständigen Finanzbehörde elektronische Bücher und sonstige erforderliche elektronische Aufzeichnungen in einem Mitgliedstaat der Europäischen Union geführt und aufbewahrt werden dürfen, sind solche bereichsspezifische Vorgaben.[1303] Gerade letztere Vorgabe hat für Cloud Computing erhebliche praktische Bedeutung. Die elektronische Buchführung ist demnach nur in solche Public Clouds und erst nach einer Genehmigung durch die Finanzbehörde auslagerbar, deren Server in der EU belegen sind.

Handelsbücher gemäß § 238 Abs. 1 HGB und Buchungsbelege gemäß § 257 Abs. 1 Nr. 4 HGB müssen laut § 257 Abs. 4 Alt. 1 i.V.m. § 257 Abs. 1 Nr. 1 und 4 HGB zehn Jahre aufbewahrt werden.[1304] Für Handelsbriefe gilt gemäß § 257 Abs. 4 Alt. 1 i.V.m. § 257 Abs. 1 Nr. 2 und 3 HGB eine sechsjährige Aufbewahrungsfrist. Hinsichtlich der Speicherung in einer Cloud ist dies für mögliche Vendor-Lock-In-Szenarien von Bedeutung. Um auch nach oder innerhalb der sechs oder zehn Jahre auf die elektronischen Handelsbücher, Buchungsbelege oder Handelsbriefe vollumfänglich zugreifen zu können, müssen entweder die Kompatibilität zu gewissen Standards durch den Cloudanbieter gewahrt werden oder die handelsrechtlichen Bücher und Briefe parallel auch außerhalb der Cloud gespeichert werden.

Aufbewahrungspflichten ergeben sich auch aus dem US-Recht, beispielsweise dem Sarbanes-Oxley-Act (SOX) und haben auch für deutsche Unternehmen Bedeutung, wenn diese in den USA Tochterunternehmen haben.[1305] Auf europäischer Ebene ist

---

[1303] *Niemann/Paul*, K&R 2009, 450; *Geis* 2009, 2 f.

[1304] Siehe dazu auch *Dorschel*, in: Schartner/Weippl, D-A-CH Security 2010, 177.

[1305] Einzelheiten zu SOX siehe weiter unten im Rahmen der Darstellung der Bezüge zum US-Recht unter 3.9.3.

das sogenannte Basel-II-Paket, das in den Richtlinien 2006/48/EG (Bankenrichtlinie) und 2006/49/EG (Kapitaladäquanzrichtlinie) mündete, mit SOX vergleichbar. Auf nationaler Ebene entsprangen beispielsweise § 25a KWG und dessen Konkretisierung in der MaRisk als Verwaltungsanweisung aus den beiden Richtlinien und damit mittelbar aus Basel-II. Aufbewahrungspflichten ergeben sich dabei aus § 25d Abs. 2 Satz 2 KWG i.V.m. § 8 Geldwäschegesetz.

Vor allem im Medizinbereich besteht eine Vielzahl von Aufbewahrungspflichten.[1306] Nach § 10 Abs. 3 der Ärztlichen Berufsordnung beträgt die Aufbewahrungsfrist für Patientenunterlagen zehn Jahre. Erheblich längere, nämlich mindestens 30-jährige, Fristen gelten nach § 28 Abs. 3 Röntgenverordnung und § 42 Abs. 1 Strahlenschutzverordnung. Auch in Krankenhäusern müssen Krankengeschichten, zum Beispiel nach § 39 Abs. 1 Nr. 2 Berliner Krankenhaus-Verordnung, 30 Jahre lang aufbewahrt werden. Soweit niedergelassene Ärzte oder Krankenhäuser medizinische Daten in Clouds vorhalten wollen, muss die Verfügbarkeit und Vollständigkeit auch nach 30 oder mehr Jahren gegeben sein. Nur am Rande sei noch einmal erwähnt, dass medizinische Daten besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG sind, so dass für diese Daten strengere Anforderungen bei einer Auslagerung in eine (internationale) Cloud gelten.[1307]

Auch das Sozialgeheimnis aus § 35 SGB Abs. 1 i.V.m. § 67 ff SGB X muss als bereichsspezifische Regelung erwähnt werden.

3.7 Urheberrecht

Cloud Computing wirft auch Fragen im Bereich des Urheberrechts auf. Zum einen muss die in Clouds verwendete Software rechtlich einwandfrei lizenziert sein. Dies bedeutet, dass ausreichende urheberrechtliche Nutzungsrechte durch den Hersteller eingeräumt sein müssen. Zum anderen ergeben sich wegen des grenzüberschreitenden Charakters des Cloud Computing diverse Fragen des internationalen Urheberrechts.

3.7.1 Lizenzierung der Software und Wegfall des Lizenzmanagements für die Nutzer

Der SaaS- oder PaaS-Anbieter, mithin der Cloudprovider, hat sicherzustellen, dass die von ihm zur Verfügung gestellten Softwareanwendungen für den konkreten Einsatz, nämlich die Bereitstellung für eine Vielzahl von Kunden, genutzt werden dür-

---

[1306] Eine Übersicht findet sich bei *Wikibooks*, Aufbewahrungsfristen in der Medizin, http://de.wikibooks.org/wiki/Medizinische_Informatik:_Datensicher#Aufbewahrungsfristen_in_der_Medizin; siehe zur Thematik auch *Roßnagel/Schmücker* 2005, 27 ff.

[1307] Siehe dazu oben Kap. 3.1.12.2.

fen.[1308] Urheberrechtlich unproblematisch ist dies nur, wenn die Software vom Anbieter selbst stammt, dieser also gleichzeitig Softwarehersteller ist.[1309]

In den Anfangstagen des Cloud Computing war dies regelmäßig der Fall, da es zum einen nur wenige Cloudprovider im Bereich SaaS gab und zum anderen die Nutzung herkömmlicher Einzelplatzsoftware in Clouds erheblicher Anpassungen bedurfte. Mittlerweile ist es jedoch üblich, bekannte Desktopversionen einer Software cloudtauglich zu portieren.[1310] Früher oder später wird es spezielle Softwaredienstleister geben, die speziell Software für die SaaS-Provider entwickeln. Erste Schritte in diese Richtung zeichnen sich mit den PaaS-Angeboten zur Entwicklung von Cloudsoftware ab. Während diese derzeit eher für die Entwicklung kleinerer (Zusatz)programme und Apps gedacht sind, ist es absehbar, dass auch größere Softwaresuiten dort entwickelt und durch den Provider angeboten werden können. Wegen des modularen Aufbaus der Software ist es wahrscheinlich, dass es mittelfristig im Sinne der SoA zu einer Kombination diverser Programme aus unterschiedlichen Programmierquellen kommen wird.

Die Nutzung fremder Software bedarf, soweit sie nicht explizit vom Entwickler als Open Source oder Public Domain angeboten wird, der Lizenzierung durch den Entwickler als Urheber oder durch das Unternehmen, in dem die Software entwickelt worden ist.[1311]

Das Neuartige an Cloud Computing ist allerdings der Umstand, dass sich der Cloudnutzer nicht mehr in dem Maße um die Klärung der Lizenzfragen kümmern muss, wie dies bisher der Fall war. Vielmehr betrifft diese Verpflichtung weitestgehend den Cloudprovider im Verhältnis zum Softwarehersteller. Folglich verliert die Lizenzierung von Software und damit auch das klassische Softwarelizenzmanagement für den Endnutzer mit Cloud Computing immer weiter an Bedeutung. An die Stelle der Softwarelizenz und eventueller Wartungsverträge tritt der Servicevertrag zwischen Cloudprovider und Cloudnutzer.[1312] Dieses Entfallen des Lizenzmanagements für den Endnutzer ist einer der diversen Vorteile der Nutzung von Software als Service in der Cloud. Für den Nutzer ergibt sich der weitere Vorteil, dass er die Software nicht mehr installieren oder updaten muss.[1313]

Der Nutzer läuft zudem nicht mehr Gefahr, zu wenige oder zu viele Lizenzen zu erwerben. Für die Softwareproduzenten ergibt sich durch Cloud Computing und

---

[1308] Im Gegensatz zu PaaS und SaaS wird bei IaaS im Regelfall keine Software durch den Cloudprovider zur Verfügung gestellt, so dass sich Urheberrechtsfragen nur für diese beiden Servicearten ergeben; siehe auch *Nägele/Jacobs*, ZUM 2010, 285.

[1309] *Karger/Sarre*, in: Taeger/Wiebe, Inside the Cloud, 433.

[1310] Beispielsweise die Microsoft Office Suite als „Office 365“.

[1311] Beispiele für eine solche Entwicklung, wenn auch nur für die Cloudbasissoftware, ist die in Kap. 2.3.7.2.2 erwähnte Cloudsoftware „Eucalyptus“.

[1312] *Diemar*, IP Manager 2010, 52.

[1313] Siehe zu den Vorteilen auch noch einmal die Ausführungen weiter oben in Kap. 2.4.1.1.

SaaS der Vorteil, dass die lizenzwidrige Nutzung der Software, wegen der neuen Art der Softwarebereitstellung, nämlich ohne die bisher notwendige Vervielfältigung installationsbedürftiger Softwarepakete, nicht mehr möglich ist. Der Nutzer erwirbt zwar auch wie bisher nur ein Nutzungsrecht, allerdings ohne auf lokal installierbare Vervielfältigungsstücke der Software angewiesen zu sein.

Wie die Lizenzierung im Innenverhältnis zwischen Softwarehersteller und Cloudprovider erfolgt, ist der jeweiligen vertraglichen Ausgestaltung, also der konkreten Vereinbarung zwischen beiden Parteien, überlassen. In Betracht kommen Volumenlizenzen, die ab gewissen Nutzerkontingenten[1314] teurer werden, oder die nachträgliche konkrete Lizenzierung jedes einzelnen Nutzers. Dies dürfte zum einen von der Größe der Cloud und der Anzahl der Nutzer sowie von der Beliebtheit und Nutzungshäufigkeit der Software abhängen.

3.7.2 Geltende Rechtslage nach dem UrhG

Nach deutschem Urheberrecht findet unter Umständen[1315] eine Vervielfältigung der Software im Sinne des § 16 Abs. 1 UrhG i.V.m. § 69c Satz 1 Nr. 1 UrhG im Browser und damit im Arbeitsspeicher des Nutzers statt. Allerdings wäre eine solche Vervielfältigung regelmäßig gemäß § 44a UrhG als flüchtige oder begleitende Vervielfältigungshandlung und integraler und wesentlicher Teil eines technischen Verfahrens anzusehen und demzufolge zulässig. Aus dem gleichen Grund sind entsprechende Vervielfältigungen auch gemäß § 69d Abs. 1 UrhG als bestimmungsgemäße Benutzung der Software zulässig.[1316] Für eine Anwendbarkeit des § 69d Abs. 1 UrhG müsste sich allerdings die Berechtigung zur Nutzung im Sinne des § 69d Abs. 1 Halbsatz 2 UrhG aus dem Servicevertrag zwischen Cloudprovider und Cloudnutzer ergeben. Eine solche Berechtigung dürfte jedoch regelmäßig vorhanden sein.[1317] In der Regel wird aber Softwarecode gerade nicht im Browser und dem Arbeitsspeicher des Nutzers ausgeführt (Ausnahme: Applets[1318]), sondern beim Cloudprovider, so dass diese providerseitige Verarbeitung lediglich zum Nutzer gestreamt wird oder beim Nutzer über den Browser dargestellt wird.

[1314] Zum Beispiel in Tausenderschritten (0-1000, 1000-2000 Nutzer, usw.).

[1315] So wären beispielsweise in SaaS integrierte Java-Applets im Arbeitsspeicher des Nutzers auszuführen; zur Beschreibung und Funktionsweise von Java-Applets siehe http://java.sun.com/applets; siehe auch *Beilschmidt/Bühr/Götz/Haas/Höfner/Koll/Konowalczyk/Konradi/Marfording/Meents/Schweinoch/Tews* 2010, 50.

[1316] So auch *Söbbing*, in: Leible/Sosnitza, Onlinerecht 2.0: Alte Fragen – neue Antworten? Cloud Computing – Datenschutz – Urheberrecht – Haftung, 43 und *Pohle/Ammann*, CR 2009, 276.

[1317] *Pohle/Ammann*, CR 2009, 276; zur Berechtigung im Sinne des § 69d UrhG siehe auch *Grützmacher*, CR 2011, 489; diesem zufolge können vor allem auch Mitarbeiter oder Dritte, die als Dienstleister fungieren, also der Cloudprovider und seine Beschäftigten, Berechtigte im Sinne der Vorschrift sein. Diese Konstellation betrifft aber nur die Fälle, in denen der Cloudnutzer primär Berechtigter ist und eine bereits vorhandene Lizenz auf den Cloudprovider erstreckt.

[1318] Siehe obige Fn. 1315.

Je nach Ausgestaltung der Cloudservices können für die Bereitstellung zur Nutzung durch den Cloudkunden auch die §§ 19a, 69c Nr. 4 UrhG, also die öffentliche Zugänglichmachung von Werken,[1319] einschlägig sein.[1320] Insbesondere sind Cloudangebote, auch Private Clouds, immer öffentlich im Sinne von § 15 Abs. 3 Satz 2 UrhG, da es praktisch nie eine persönliche Beziehung zwischen Nutzer und Anbieter gibt. Eine öffentliche Zugänglichmachung gemäß §§ 19a, 69c Nr. 4 UrhG dürfte regelmäßig bei Bürosoftware (z. B. Office-Pakete oder CRM-Software) als Cloudservice der Fall sein, da die Software an sich nicht beim Kunden im Arbeitsspeicher vorhanden ist, sondern diese mittelbar über den Browser im Arbeitsspeicher in der virtuellen Umgebung des Cloudproviders gerade nur zugänglich gemacht wird.

Die jeweilige Abgrenzung zwischen Vervielfältigung und bloßer öffentlicher Zugänglichmachung ist indes schwierig und nur anhand der Einzelfallfrage, ob Softwarecode im Arbeitsspeicher des Nutzers verarbeitet wird, zu beurteilen. Eine grobe Einteilung ergibt, dass für SaaS-Angebote daher die Zugänglichmachung von Softwarewerken im Sinne der §§ 19a, 69c Nr. 4 UrhG anzunehmen ist, während bei PaaS-Angeboten und entsprechenden Softwareentwicklungsumgebungen eher die Notwendigkeit besteht, Code des Anbieters auch im Arbeitsspeicher des Nutzers auszuführen, so dass meist eine urheberrechtliche Vervielfältigung gegeben ist.

Die herrschende Auffassung in der Literatur ist der Ansicht, dass Cloudnutzer überhaupt keine urheberrechtlich relevanten Handlungen vornehmen.[1321] Insbesondere kommt es bei einer Nutzung nicht zu einer urheberrechtlich relevanten Vervielfältigung.[1322] Allerdings ist diese Ansicht, wie anhand der unterschiedlichen Cloudnutzungsmodelle geschildert, nicht generalisierbar, sondern einzelfallabhängig.[1323] Die öffentliche Zugänglichmachung im Sinne der §§ 19a, 69c Nr. 4 UrhG ist im Hinblick auf die herrschende Ansicht im Übrigen unschädlich, da die urheberrechtlich relevante Handlung bei einer Zugänglichmachung durch den Anbieter und gerade nicht durch den Nutzer erfolgt.

Nur am Rande ist zu erwähnen, dass bereits vor der Geltung der §§ 19a, 69c Nr. 4 UrhG die Auffassung bestand, dass die Bereitstellung von Software über das Inter-

---

[1319] Das Urheberrecht schützt nach § 1 UrhG Werke im Sinne des § 2 UrhG, wobei § 2 Abs. 1 UrhG nicht abschließend ist. Auch Computerprogramme (Software) gelten als Werke, wenn die Voraussetzungen des § 69a Abs. 3 UrhG erfüllt sind.

[1320] Eine allgemeine Geltung des § 19a UrhG für Cloudservices vertreten *Pohle/Ammann*, CR 2009, 276.

[1321] *Niemann/Paul*, K&R 2009, 448; *Bierekoven*, ITRB 2010, 43; *Söbbing*, in: Leible/Sosnitza, Onlinerecht 2.0: Alte Fragen – neue Antworten? Cloud Computing – Datenschutz – Urheberrecht – Haftung, 52; *Wunderlich* 2010, 53.

[1322] *Söbbing*, in: Leible/Sosnitza, Onlinerecht 2.0: Alte Fragen – neue Antworten? Cloud Computing – Datenschutz – Urheberrecht – Haftung, 52; *Niemann/Paul*, K&R 2009, 448.

[1323] Der gleichen abwägenden Ansicht für das ASP-Bereitstellungsmodell sind *von Westerholt/Berger*, CR 2002, 82; zur Begrenzung auf SaaS- und PaaS-Nutzungsmodelle siehe auch Fn. 1308.

net eine eigenständige Nutzungsart darstellt, für die der Anbieter einer besonderen Lizenz bedarf, auch wenn der Nutzer keine urheberrechtlich relevante Handlung vornimmt.[1324] Die damalige Diskussion im Rahmen des ASP ging dabei insbesondere von der Frage aus, ob ein ASP-Anbieter berechtigt war Software automatisch an seine Kunden zu vermieten und ob die Bereitstellung über das Internet eine Vermietung im Sinne des damals geltenden § 69c Nr. 3 UrhG darstellte.[1325] Mit der Umsetzung des sogenannten „ersten Korbs"[1326] und der Einfügung des § 69c Nr. 4 UrhG, der die Spezialvorschrift zur allgemeinen Norm des § 19a UrhG darstellt, ist die Frage damit dergestalt beantwortet worden, dass es sich um eine öffentliche Zugänglichmachung von Software handelt, die der Erlaubnis durch den Softwarehersteller bedarf.

Im Ergebnis ergibt die Betrachtung der Rechtslage, dass immer mindestens eine öffentliche Zugänglichmachung von fremder Software durch den Cloudprovider erfolgt, soweit er nicht gleichzeitig Softwarehersteller ist. Für die Praxis bedeutet dies, dass Cloudprovider und Softwarehersteller die Nutzungsrechtseinräumung, also die Erlaubnis zur Onlinebereitstellung, vertraglich abklären müssen.[1327] Die Cloudnutzer sind rechtlich abgesichert, wenn sie sich ihrerseits vom Provider vertraglich zusichern lassen, dass dieser die notwendigen Nutzungsrechte besitzt.

Die Cloudnutzer benötigen keine urheberrechtlichen Nutzungsrechte, weil es nicht zu Vervielfältigungshandlungen auf den Nutzersystemen kommt.[1328] Soweit solche Vervielfältigungshandlungen ausnahmsweise, zum Beispiel durch die Nutzung von Applets, in Betracht kommen, sind diese entweder bereits gemäß § 69d Abs. 1 UrhG für die bestimmungsgemäße Benutzung der Software notwendig oder über die Schranke des § 44a UrhG gerechtfertigt.

3.7.3 Internationales Urheberrecht

Rechtliche Fragestellungen des internationalen Urheberrechts ergeben sich aus dem oft grenzüberschreitenden Charakter von Clouds, insbesondere großer Public Clouds. Bei der Anwendung des jeweils einschlägigen Rechts spielen zudem auch Aspekte des Internationalen Privatrechts eine Rolle.

3.7.3.1 Räumlicher Anwendungsbereich

In räumlicher Hinsicht gilt das Territorialitätsprinzip, so dass urheberrechtliche Ausschließlichkeitsrechte in ihrer Geltung räumlich auf das Territorium des Staates

---

[1324] So *von Westerholt/Berger*, CR 2002, 82 für das damalige ASP-Modell.

[1325] Zur Frage der Vermietung siehe *Eckhart*, Information Management und Consulting 4/2010, 55.

[1326] Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft vom 10.9.2003 (BGBl. I, S. 1774-1788).

[1327] *Eckhart*, Information Management und Consulting 4/2010, 56.

[1328] Siehe dazu auch noch einmal obige Fn. 1321.

begrenzt sind, der sie verleiht.[1329] Teilweise wird auch von „Urheberrechtsmosaik“ oder dem „Flickenteppich“ nationaler Urheberrechte gesprochen.[1330] Folge des Territorialitätsprinzips ist, dass sich der Urheber nicht einem einheitlichen weltweit gültigen Urheber- und Leistungsschutzrecht gegenüber sieht, sondern mit einem Bündel nationaler Regelungen mit unterschiedlichem Gehalt konfrontiert wird.[1331] Der Gegenbegriff zum Territorialitätsprinzip ist das Universalitätsprinzip, dessen Anhänger die weltweite Anerkennung eines einheitlichen Urheberrechts annehmen oder einfordern.[1332] Das deutsche Urheberrecht folgt allerdings dem Territorialitätsprinzip. Dieses ist nach der ständigen Rechtsprechung des Bundesgerichtshofs „allgemein anerkannt“ und wird auch in der Literatur ganz überwiegend vertreten.[1333]

3.7.3.2 Völkerrechtliche Verträge

Wegen der Geltung des Territorialitätsprinzips ist es notwendig, völkerrechtliche Verträge abzuschließen. Die bekanntesten Verträge sind die Revidierte Berner Übereinkunft (RBÜ), das Abkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums (Agreement on Trade-Related Aspects of Intellectual Property Rights, TRIPs) und die von der World Intellectual Property Organisation (WIPO) geschlossenen Verträge, nämlich der Urheberrechtsvertrag (WIPO Copyright Treaty, WCT) und der Vertrag über Darbietungen und Tonträger (WIPO Performances and Phonograms Treaty, WPPT).[1334]

3.7.3.3 Persönlicher Anwendungsbereich

Beim persönlichen Anwendungsbereich gilt gemäß § 120 UrhG deutsches Urheberrecht, wenn der Urheber eines Werkes Deutscher im Sinne des Art. 116 GG oder Bürger der EU oder des EWR ist, unabhängig davon, wo das Werk erschienen ist.[1335] Für Ausländer, Staatenlose und Flüchtlinge gelten die umfangreichen Vorschriften der §§ 121 ff. UrhG. Eine Besonderheit des Urheberrechts ist in diesem

---

[1329] *Dreier*, in: Dreier/Schulze 2008, Einleitung, Rn. 42; *Welser*, in: Wandtke/Bullinger, Urheberrecht, Vorbemerkung Vor §§ 120 ff., Rn. 5; *Schack* 2001, Rn. 798; *Nicolini/Ahlberg*, in: Möhring/Nicolini, UrhG, Vorbemerkungen Internationales Urheberrecht, Rn 2; *Nägele/Jacobs*, ZUM 2010, 284; *Schulz/Rosenkranz*, ITRB 2009, 236.

[1330] *Nicolini/Ahlberg*, in: Möhring/Nicolini, UrhG, Vorbemerkungen Internationales Urheberrecht, Rn 2; zur „Mosaikbetrachtung“ siehe insbesondere *Schricker* 2001, Einleitung, Rn. 37.

[1331] Sogenannte „Kegelsche Bündeltheorie“, *Soergel/Kegel* 1996, Anhang nach Art. 12 EGBGB, Rn. 16, 22; *Wandtke*, in: Wandtke/Bullinger, Urheberrecht, Einleitung, Rn. 81; *Nägele/Jacobs*, ZUM 2010, 284.

[1332] Siehe dazu beispielsweise *Schack* 2001, Rn. 806 ff.

[1333] BGHZ 126, 256; BGHZ 136, 385; *Nicolini/Ahlberg*, in: Möhring/Nicolini, UrhG, Vorbemerkungen Internationales Urheberrecht, Rn 2; *Dreier*, in: Dreier/Schulze 2008, Einleitung, Rn. 42; *Welser*, in: Wandtke/Bullinger, Urheberrecht, Vorbemerkung Vor §§ 120 ff., Rn. 5; *Schricker* 2001, Rn. 37; *Walter*, in: Loewenheim, Handbuch des Urheberrechts, § 58, Rn. 9.

[1334] Zu weiteren Einzelheiten siehe die jeweiligen Vertragstexte.

[1335] Mehr dazu bei *Welser*, in: Wandtke/Bullinger, Urheberrecht, § 120 UrhG, Rn. 1 ff.; zum Werkbegriff siehe Fn. 1319.

Zusammenhang zudem das Prinzip der Inländergleichbehandlung, das besagt, dass ausländische Werke im Inland ebenso wie die Werke von Inländern zu behandeln sind.[1336] Dieser Grundsatz bildete sich aus einer Vielzahl bi- und multilateraler völkerrechtlicher Verträge heraus und wurde durch den EuGH in der Phil-Collins-Entscheidung als Verbot der Diskriminierung gemäß Art. 18 AEUV (ex-Art. 12 EGV) für EU-Bürger bestätigt.[1337]

Von diesem sogenannten Fremdenrecht ist das Kollisionsrecht zu unterscheiden. Während das Fremdenrecht bestimmt, ob Ausländer im Inland Rechtsschutz genießen, regelt das Kollisionsrecht, welches Recht auf urheberrechtliche Sachverhalte mit Auslandsbezug Anwendung findet.[1338]

3.7.3.4 Kollisionsrecht und Internationales Privatrecht

Aus dem Territorialitätsprinzip wird kollisionsrechtlich das Schutzlandprinzip (lex loci protectionis) abgeleitet.[1339] Das Schutzlandprinzip besagt, dass die Entstehung des Urheberrechts, die Inhaberschaft, der Inhalt, die Durchsetzbarkeit und die Schranken des Urheberrechts nach dem Recht des Landes zu beantworten sind, für dessen Gebiet sie Geltung beanspruchen.[1340] Das jeweils anwendbare Schutzlandrecht kann nur über die auf seinem Territorium begangenen oder drohenden Verletzungshandlungen befinden (Mosaikbetrachtung).[1341] Eine solche Anknüpfung an das Schutzland findet sich auch in Art. 8 Rom-II-VO.[1342]

3.7.4 Bedeutung für Cloud Computing

3.7.4.1 Verhältnis zwischen Softwarehersteller und Cloudprovider

Mit den vorausgegangenen Ausführungen wird deutlich, dass es kein alleiniges Urheberrecht gibt, das international und einheitlich für Fallkonstellationen des Cloud Computing gilt. Die Erleichterung liegt allerdings darin, dass hinsichtlich der Lizenzvereinbarungen zwischen Softwarehersteller und Provider, soweit es um die Vervielfältigung auf den Servern des Providers geht, nur die Urheberrechtsgesetze dieser beiden Parteien zu beachten sind. Im einfachsten Fall, also dem Fall, dass

---

[1336] *Lewinski*, in: Loewenheim, Handbuch des Urheberrechts, § 57, Rn. 2.

[1337] EuGH GRUR Int. 1994, 53, 56 Rn. 35; *Welser*, in: Wandtke/Bullinger, Urheberrecht, Vorbemerkung Vor §§ 120 ff., Rn. 37.

[1338] *Welser*, in: Wandtke/Bullinger, Urheberrecht, Vorbemerkung Vor §§ 120 ff., Rn. 2; *Wandtke*, in: Wandtke/Bullinger, Urheberrecht, Einleitung, Rn. 80.

[1339] *Nägele/Jacobs*, ZUM 2010, 284; a. A. *Wandtke/Bullinger*, Urheberrecht, Einleitung, Rn. 81.

[1340] *Schulz/Rosenkranz*, ITRB 2009, 236; *Wandtke*, in: Wandtke/Bullinger, Urheberrecht, Einleitung, Rn. 81; BGH, ZUM 2007, 747; BGH, GRUR 2003, 328; GRUR 1999, 153.

[1341] *Nägele/Jacobs*, ZUM 2010, 284.

[1342] *Nägele/Jacobs*, ZUM 2010, 284; *Schulz/Rosenkranz*, ITRB 2009, 236; zu den Konsequenzen siehe die anschließenden Ausführungen.

Hersteller, Anbieter und die Rechencenter sich innerhalb eines Hoheitsgebiets befinden oder ihren Sitz darin haben, gilt das Urheberrecht eines einzigen Staates.

3.7.4.2 Verhältnis zwischen Cloudprovider und Cloudnutzer

Die Rechtslage ist komplizierter, wenn die Lizenzvereinbarungen ungültig sind oder der Provider gänzlich ohne notwendige Lizenzierung Software eines Herstellers verwendet hat, da in diesem Fall auch die Cloudnutzer mangels Legitimationskette[1343] und mangels der Geltung des § 44a UrhG für deutsche Nutzer direkt betroffen sind. Die Schranke des § 44a UrhG gilt nämlich gemäß § 44a Satz 1 Nr. 2 UrhG nur bei einer rechtmäßigen Nutzung des Werkes. Bei einer potentiell weltweiten Nutzung wäre somit eine Vielzahl unterschiedlicher Schutzlandrechte betroffen.[1344]

Der Vollständigkeit halber sei zudem erwähnt, dass der Cloudprovider im Regelfall dem Nutzer den Schaden, den dieser bei der Inanspruchnahme durch den Softwareurheber erlitten hat, ersetzen muss. Vertragliche Hauptleistungspflicht des Providers ist nämlich die Bereitstellung rechtmäßig nutzbarer Software. Der Regressanspruch des Cloudnutzers gegenüber dem Cloudprovider ergibt sich damit regelmäßig unmittelbar aus dem Vertrag zwischen beiden.

In der Regel wird sich der Urheber des Softwarewerkes allerdings direkt an den Provider halten, da dieser primär die unerlaubte Handlung begangen hat oder, wie oben erwähnt, zwischen beiden spezifische vertragliche Absprachen, beispielsweise über den Umfang oder die Zeiträume der Bereitstellung, bestehen. Die gerichtliche Auseinandersetzung mit einer beklagten Partei, die zudem auch noch im gleichen Staat wie der klagende Urheber angesiedelt sein kann oder auf dem Territorium des gleichen Staats unerlaubt gehandelt haben kann, produziert erheblich weniger Aufwand als die mühselige Inanspruchnahme einer Vielzahl international verstreuter Nutzer. Die Komplikationen, die sich aus dem internationalen Urheberrecht ergeben würden, sind damit minimierbar.

Relevanter wird das internationale Urheberrecht und damit das Schutzlandprinzip allerdings im Verhältnis zwischen dem Cloudprovider und dem Cloudnutzer für die Lizenzierung durch den Softwarehersteller in dem Fall, dass sich das Cloudangebot an Nutzer weltweit richtet und damit weltweit rechtmäßige Nutzungs- und insbesondere unrechtmäßige Verletzungshandlungen möglich sind.[1345]

[1343] Für die Einräumung abgeleiteter Nutzungsrechte durch den Provider an die Cloudnutzer bedarf ersterer der Erlaubnis des Softwareherstellers.

[1344] Siehe dazu oben die sogenannte „Mosaikbetrachtung“.

[1345] Erwähnt sei allerdings, dass durch sogenanntes Geotargeting oder Geolocation gewisse IP-Adressbereiche und damit mittelbar gewisse Staaten von der Nutzung ausgeschlossen werden können. Allerdings ist die unrechtmäßige Nutzung und damit eine Verletzungshandlung über Proxyserver oder VPN-Tunnel möglich, so dass die rechtliche Problematik trotzdem weiterbesteht.

3.7.4.2.1 Rechtmäßige Nutzungshandlungen

Der Cloudprovider müsste dann grundsätzlich Nutzungsrechte zugunsten seiner Nutzer für alle Rechtsordnungen weltweit einholen, in denen auch nur theoretisch Nutzungshandlungen auftreten könnten. Neben Nutzungshandlungen, wie der Vervielfältigung von Code in den Caches und Arbeitsspeichern der Nutzer, müsste er mindestens, je nach nationaler Rechtslage und der Ausgestaltung des Cloudangebots, Rechte für die öffentliche Zugänglichmachung nach der Rechtsordnung des jeweiligen Nutzers beim Softwarehersteller einholen.

Diese enge Bindung an das Schutzlandprinzip ist allerdings durch eine freie Rechtswahl gemäß Art. 14 Abs. 1 lit. b) Rom-II-VO im Vertrag zwischen Provider und Nutzer auflösbar, wenn beide Parteien einer kommerziellen Tätigkeit nachgehen. Da ein (Public) Cloudprovider immer kommerziell agieren dürfte, trifft diese Voraussetzung der gewerblichen Tätigkeit den Cloudnutzer.

3.7.4.2.2 Verletzungshandlungen (Unerlaubte Handlungen)

Bei Ansprüchen wegen der Verletzung geistiger Eigentumsrechte ist zu beachten, dass eine solche Rechtswahl, auch eine nachträgliche, gemäß Art. 8 Abs. 3 der Rom-II-VO ausgeschlossen ist.[1346] Gemäß Art. 8 Abs. 1 Rom-II-VO gilt zudem das Schutzlandprinzip, so dass auch die grundsätzliche Erleichterung bei deliktischen Ansprüchen gemäß Art. 4 Abs. 1 Rom-II-VO, nämlich die Geltung des Erfolgsortrechts, bei der Verletzung geistiger Schutzrechte nicht heranziehbar ist.[1347] Erfolgsort im Sinne der Vorschrift ist der Ort, an dem der Schaden eintritt, unabhängig davon, in welchem Staat das schadensbegründende Ereignis oder indirekte Schadensfolgen eingetreten sind.

Allerdings ist das Problem der Verletzung von Urheberrechten wegen der fehlenden Verkörperung und der Ausgestaltung als Dienst weniger akut als bei herkömmlicher Software. Zur Nutzung der Clouddienste und der dahinterstehenden Software muss der Nutzer vom Provider legitimiert sein und vor allem technisch in die Lage versetzt werden, das Angebot tatsächlich zu nutzen. Im Gegensatz zu installationsbedürftiger Software auf Datenträgern ist die unrechtmäßige Nutzung gerade nicht mehr so einfach möglich. Im Prinzip sind nur zwei Konstellationen denkbar, die zu einer unrechtmäßigen Nutzung im Verhältnis zum Provider führen können. Die erste wäre das Einhacken in die SaaS- oder PaaS-Infrastruktur, was allerdings bei ordentlich aufgesetzten und gewarteten Cloudservices wegen des enormen Aufwands eher unwahrscheinlich ist. Die zweite Konstellation betrifft die Weiternutzung nach einer zweitweise erlaubten Nutzungsphase. Diese Konstellation kann allerdings ausgeblendet werden, weil für den Zeitraum der legalen Nutzung Vereinbarungen nach dem Recht des Staates, in dem der Nutzer den Dienst genutzt hat, eingeräumt

---

[1346] *Schulz/Rosenkranz*, ITRB 2009, 236; *Nägele/Jacobs*, ZUM 2010, 284.

[1347] Siehe zum Schutzlandprinzip auch Kap. 3.7.3.4.

worden sind und sich Konsequenzen der Verletzungen dann gemäß Art. 4 Abs. 3 Rom-II-VO aus dem vorherbestehenden Rechtsverhältnis und aus diesem davor einschlägigen Recht ergeben.

Als Ergebnis zur Internationalität lässt sich festhalten, dass durch Ausnahmetatbestände die Fragestellungen des internationalen Urheberrechts überschaubar und weniger kompliziert sind, als man bei Geltung der grundsätzlichen Vorschriften annehmen könnte. Komplizierter ist die Rechtslage allerdings in der Konstellation, dass ein Cloudanbieter weltweit auftritt und die weltweit verstreuten Nutzer nicht gewerblich tätig sind, so dass eine freie Rechtswahl ausscheidet. In solchen Fällen muss sich ein Cloudprovider mit dem Recht der Staaten auseinandersetzen, in denen Schutz beansprucht wird. Der Provider muss sich dann vom Softwarehersteller abgeleitete Nutzungsrechte einräumen lassen, soweit eine solche Einräumung nach dem Recht des jeweiligen Staates der Nutzer und der konkreten Ausgestaltung des Cloudangebots überhaupt notwendig ist.

3.8 Strafrecht, Strafprozessrecht, Strafverfolgung und Cloudforensik

Cloud Computing bringt auch Neuerungen hinsichtlich einer effektiven und gerichtsverwertbaren Strafverfolgung. Im Folgenden sollen deswegen neuartige Probleme bei der Verfolgung von Straftaten und deren Beweisbarkeit vor Gericht thematisiert werden. Anhand des bisher Gesagten ist offensichtlich, dass die herkömmlichen Methoden der Ermittlungsbehörden nur noch eingeschränkt tauglich sind, um die in Cloudsystemen abgelegten und gespeicherten Beweismittel zu erlangen. Neben den bereits bisher akuten Fragen der grenzüberschreitenden strafrechtlichen Verfolgung und Rechtsdurchsetzung durch die Internationalität des Internets, sind einige zusätzliche cloudspezifische Probleme, aber auch neuartige Lösungsmöglichkeiten zu betrachten.

Materiellrechtlich sind die Vorschriften zum Schutz von Geheimnissen darzustellen und zu prüfen, ob sie im Rahmen der Auslagerung von geschützten Geheimnissen in die Cloud einschlägig sein können.

3.8.1 Probleme bei der Strafverfolgung und neue Ermittlungsansätze

Die meisten rechtlichen Befugnisnormen für Strafverfolgungsorgane stammen aus einer Zeit, in der elektronisch gespeicherte Daten noch fremd waren. Die Normen orientierten sich an körperlichen Gegenständen, nämlich an Aktenablagen in Papier, die in Wohnungen oder Geschäftsräumen lagen. Zwar wurden das Strafprozessrecht mit der Zeit so fortentwickelt, dass die auf Papiere bezogenen Vorschriften auch Gegenstände umfassten, die menschliche Gedankenerklärungen und sonstige In-

formationen verkörpern oder speichern, allerdings stellt Cloud Computing auch für diese Erweiterung in praktischer Hinsicht eine Herausforderung dar.[1348]

Während heutzutage die Computerdaten analog zu den älteren Papieren auf Computern und Datenträgern in Wohnungen oder Geschäftsräumen liegen, bringt die Auslagerung der Daten in die Cloud erhebliche Lokalisierungs- und Zugriffsprobleme mit sich. Mit Cloud Computing ist es schwer nachzuvollziehen wo Daten physisch gespeichert sind, so dass eine Durchsuchung, Sicherstellung oder Beschlagnahme von in der Cloud belegenen Daten mit rechtlichen und praktischen Problemen verbunden sein kann.

Die rechtlichen Probleme sind offensichtlich, wenn sich die Server im Ausland befinden und den deutschen Behörden wegen des Territorialitätsprinzips die rechtliche Befugnis zum Zugriff fehlt. Diese sind zwar durch Rechtshilfeabkommen und entsprechende Auskunftsersuchen lösbar, jedoch bestehen zum einen nicht mit allen Staaten der Welt solche Abkommen und zum anderen dauern solche Ermittlungsanfragen und Ersuchen oft sehr lange.[1349] Schon bei herkömmlichen nichtcomputerbezogenen Straftaten ist dies ein Problem. Bei den erheblichen Fluktuationen in einer Cloud sind die Beweismittel oft nicht mehr vorhanden, wenn das Ersuchen erfüllt werden soll. Außerdem gibt es sogar Offshoreplattformen mit Servern in internationalen Gewässern, gegen die streng genommen überhaupt nicht rechtlich vorgegangen werden kann, da kein Staat für diese Plattformen zuständig ist.[1350]

Aber auch bei ausschließlichem Inlandsbezug können sich rechtliche und faktische Probleme bei der Strafverfolgung ergeben. Insbesondere, wenn ein Provider die Kooperation mit den Ermittlungsbehörden verweigert, kann dies zu Problemen führen. Diese betreffen einerseits die Lokalisierung der Daten und andererseits die Sicherstellung oder Beschlagnahme der Daten in der Art und Weise, dass diese vor Gericht als Beweis Bestand haben.

Grundsätzlich ist im deutschen Strafprozessrecht zwischen einer Beschlagnahme nach §§ 94 ff. StPO und der Durchsuchung nach §§ 102 ff. StPO zu unterscheiden. Durchsuchungen dienen unter anderem der Auffindung von Beweismitteln. So aufgefundene Beweismittel können dann nach den §§ 94 ff. StPO sichergestellt oder beschlagnahmt werden. Insbesondere wenn sich ein Provider weigert Daten freiwillig herauszugeben, können diese nach § 94 Abs. 2 StPO beschlagnahmt werden. Dabei sind nach § 95 Abs. 2 StPO auch Ordnungs- oder Zwangsmittel denkbar.

[1348] *Obenhaus*, NJW 2010, 651; BVerfGE 113, 29.

[1349] Im europäischen Raum hat auch die Cybercrime Convention des Europarats bisher kaum Verbesserungen gebracht, da nicht alle Mitgliedsstaaten den Vertrag unterzeichnet oder ratifiziert haben; siehe dazu *Birk/Heinson/Wegener*, DuD 2011, 331.

[1350] Ein vergleichsweise kurioser Fall war die Seeplattform „Sealand“, deren Eigentümer einen souveränen Staat ausrief und auf der Plattform Daten hostete; siehe dazu *Rötzer*, Die künstliche Insel der freien Daten, http://www.heise.de/tp/artikel/12/12769/1.html.

Bei Cloud Computing sind rein rechtlich folglich zunächst nur Durchsuchungen mit dem Zweck der Auffindung von Beweismitteln kritisch. Sobald nämlich klar ist, dass verfahrensrelevante Daten als Beweismittel bei einem inländischen Cloudprovider liegen, kann dieser nach § 95 Abs. 1 StPO verpflichtet sein, diese an die Ermittlungsbehörden herauszugeben.

Um die Ermittlungsarbeit zu erleichtern, hat der deutsche Gesetzgeber mit Wirkung zum 1.1.2008 § 110 StPO um einen dritten Absatz ergänzt. § 110 StPO regelt allgemein die Durchsicht von Papieren. Papiere im Sinne von § 110 Abs. 1 und 2 StPO sind auch solche Unterlagen, die auf einem anderen Material als Papier oder auf einem elektronischen Datenträger gespeichert sind.[1351] In § 110 Abs. 3 StPO sind Speichermedien hingegen ausdrücklich wörtlich erwähnt. Der Vorschrift zufolge dürfen Ermittlungsbehörden die Durchsicht auch auf räumlich getrennte Speichermedien erstrecken, soweit auf sie von dem lokalen Speichermedium aus zugegriffen werden kann. Die Durchsicht ist nach § 110 Abs. 3 Satz 1 letzter Halbsatz StPO nur zulässig, wenn andernfalls der Verlust der gesuchten Daten zu besorgen ist. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gemäß § 110 Abs. 3 Satz 2 StPO gesichert werden. Mithin darf bei einem Beschuldigten von dessen Client-PC auf die Daten in der Cloud zugegriffen werden und die für ein Strafverfahren relevanten Daten gesichert werden. Dies allerdings nur dann, wenn die Gefahr droht, dass die rechtzeitige Sicherstellung des physischen Datenträgers nicht rechtzeitig erfolgen kann. Zudem müssen sich die Daten alle innerhalb Deutschlands befinden. Eine solche Beschränkung auf deutsches Hoheitsgebiet soll sich aus der Gesetzesbegründung und dem Souveränitätsprinzip ergeben.[1352]

Damit realisiert sich aber die Erleichterung nur dann, wenn schon vorher absehbar ist, dass sich die betroffenen Cloudserver ausnahmslos auf deutschem Hoheitsgebiet befinden. In der Praxis sind die Behörden dann jedoch regelmäßig auf die Mithilfe des Cloudproviders angewiesen, da es zum einen kaum rein innerdeutsche Clouds gibt und zum anderen nie auszuschließen ist, dass sich die durchzusehenden Daten im Ausland befinden und es dann zu einer Kompetenzüberschreitung der deutschen Behörden käme. Für die Beantwortung der Frage, ob die Daten rein innerdeutsch belegen sind, ist demzufolge die Mithilfe des Providers notwendig, weil es gerade Charakteristikum aktueller Cloudangebote ist, dass Endnutzer, also auch die ermittelnden Beamten, nicht nachvollziehen können, wo genau die Daten lagern.

Die Onlinedurchsicht nach § 110 Abs. 3 StPO kann aber Tatsachen und Ansätze liefern, um eine physische Ermittlungsdurchsuchung nach § 103 StPO beim Cloudprovider zu rechtfertigen. Rechtlich handelt es sich bei einer solchen Durchsuchung von Daten der Cloudnutzer mangels Beschuldigteneigenschaft des Providers oder seiner Angestellten um eine Durchsuchung bei Dritten gemäß § 103 StPO. Eine sol-

---

[1351] *Hegman*, in: Beck'scher Online-Kommentar StPO, § 110, Rn. 3.

[1352] *Gercke*, CR 2010, 347; BT-Drs. 16/5846, 63.

che ist gemäß Abs. 1 Satz 1 nur dann zulässig, wenn Tatsachen vorliegen, aus denen zu schließen ist, dass sich die gesuchte Spur oder Sache in den zu durchsuchenden Räumen befindet.

Wegen der Einschränkung, dass die Durchsicht nur zulässig ist, wenn ansonsten ein Daten- und Beweismittelverlust zu besorgen ist, wird deutlich, dass die physische Sicherstellung oder die Beschlagnahme von Datenträgern vorrangig sind. Die Beschlagnahme kommt vor allem dann in Betracht, wenn der Provider die freiwillige Herausgabe der angeforderten Daten verweigert, also ein Auskunfts- oder Herausgabeverlangen der Behörden nach § 95 Abs. 1 StPO scheitert.

Bezüglich einer physischen Sicherstellung oder Beschlagnahme besteht bei Cloud Computing, neben den bisher genannten Aspekten der möglichen Unkenntnis des Speicherorts und der hohen Fluktuation, das zusätzliche praktische Problem, dass die zu sichernden Daten in der Regel physisch verteilt gespeichert sind. Wie mehrfach erwähnt, ist es aus Redundanzgründen üblich, dass Teile von Daten über verschiedene Server verteilt gespeichert sind und nur zusammengesetzt für den Nutzer oder die ermittelnden Behörden den ihnen innewohnenden Sinngehalt offenbaren. Da diese Zusammensetzung nur durch die in der Cloud implementierten Algorithmen funktioniert, kann auch eine physische Beschlagnahme aller Server, die die Datenteile beherbergen nur dann zu einem Erfolg beim Zusammensetzen führen, wenn die Auswerter quasi eine Cloudumgebung mit den entsprechenden Algorithmen emulieren. Eine solche Nachbildung ist aber praktisch unmöglich, weil die Zusammensetzungsalgorithmen nur in einer spezifischen Umgebung, nämlich der gesamten Ausgangscloud, funktionieren. Diese „händisch“ zusammenzusetzen verursacht einen nicht mehr verhältnismäßigen Aufwand. Zudem wäre die Beweiseignung bei der Emulation der Algorithmen vor Gericht zweifelhaft. Eine Beschlagnahme der gesamten Cloudinfrastruktur scheidet aus Gründen der Verhältnismäßigkeit und Praktikabilität aus. Eine solche ist allenfalls bei überschaubaren Private Clouds kleinerer Unternehmen denkbar.

Ein letztes Problem betrifft die Aufrechterhaltung des Betriebs einer Cloud. Da die zu beschlagnahmenden Daten innerhalb von virtualisierten Systemen gemeinsam mit vielen anderen Daten unbeteiligter Dritter und nur mittels Hypervisoren getrennt verarbeitet und gespeichert werden, bedeutet die Beschlagnahme eines physischen Datenträgers oder Servers die Unterbrechung des Cloudbetriebs und in den Fällen, in denen die unbeteiligten Daten nicht auf andere Providersysteme transferiert werden, die Verhinderung der Nutzung der Daten durch die unbeteiligten Dritten. Aber auch beim Transfer der Daten Dritter und der nur unzureichenden Löschung durch den Anbieter können Daten oder Datenreste Unbeteiligter bei der forensischen Untersuchung und Auswertung zu Tage treten. Das ist jedoch kein völlig neues Problem, sondern dürfte alltäglich vorkommen, wenn der Beschuldigte Daten Dritter auf der beschlagnahmten Festplatte gespeichert hatte. Allerdings ist

bei Public Cloud Computing zu beachten, dass dabei in der Regel die Drittbetroffenheit erheblicher sein wird als bei einer herkömmlichen Beschlagnahme eines Datenträgers einer Einzelperson.

Allerdings bietet die Virtualisierung in Cloudsystemen auch praktische, wenn auch nicht beweisrechtliche, Vorteile. So können die auszuwertenden Daten durch die Provider oder unmittelbar durch die Ermittlungsbehörden vor Ort unter Mithilfe des Providers als Image oder Snapshot geklont werden.[1353] Daran ist jedoch problematisch, dass die Daten nicht wie bei einer physischen Beschlagnahme unangetastet ausgewertet werden. Während der Imageerstellung durch den Provider können diesem Fehler unterlaufen, zum Beispiel, dass nicht alle relevanten Daten gesichert werden oder es ergibt sich die Situation, dass Daten gezielt manipuliert werden. Die Erstellung des Images oder Snapshots erfolgt dabei üblicherweise von einem aktiven System, so dass die Fehleranfälligkeit steigt und eventuell in Benutzung befindliche Daten nicht vollständig gesichert werden können. Aufgrund dieser Erwägungen dürfte folglich die Beweiskraft der Daten vor Gericht als vergleichsweise gering erscheinen, so dass im Zweifel und soweit dies technisch und faktisch möglich ist, eine echte Sicherstellung oder Beschlagnahme vorzugswürdig erscheint, wobei dann regelmäßig die oben erwähnten Konsequenzen der Störung des Betriebs auftreten.[1354]

3.8.1.1 Telekommunikationsüberwachung gemäß § 100a StPO mittels Deep Packet Inspection

Eine denkbare Lösung für einige der oben genannten Probleme wäre die Möglichkeit für Ermittlungsbehörden, sich während des Datenübertragungsprozesses Kenntnis vom Inhalt der Daten mittels TK-Überwachung gemäß § 100a StPO zu verschaffen.[1355] Wegen der systembedingten Notwendigkeit der Datenübertragung zwischen Cloudprovider und Cloudnutzer ergibt sich dadurch ein neuer Ansatzpunkt für die Ermittlungsbehörden. Die dafür nötige Technologie besteht bereits und nennt sich Deep Packet Inspection (DPI). Diese soll im Folgenden in einem kurzen technischen Exkurs dargestellt werden.[1356]

3.8.1.1.1 Funktionsweise der Deep Packet Inspection

Deep Packet Inspection ermöglicht es Internetzugangsprovidern oder staatlichen Organen in Echtzeit im Internet übertragene Inhalte zu überwachen und mitunter sogar zu manipulieren.

[1353] *Birk/Wegener*, DuD 2010, 645; *Birk/Heinson/Wegener*, DuD 2011, 331.

[1354] Ähnliche Befürchtungen hegen auch *Birk/Wegener*, DuD 2010, 645.

[1355] So auch *Gercke*, CR 2010, 346; *Rath*, in: Schartner/Weippl, D-A-CH Security 2010, 190.

[1356] Die nachfolgenden Ausführungen zur Funktionsweise der DPI wurden bereits in *Bedner*, CR 2010, 339 und *ders.*, Rechtmäßigkeit der „Deep Packet Inspection“, http://kobra.bibliothek.uni-kassel.de/bitstream/urn:nbn:de:hebis:34-2009113031192/5/BednerDeepPacketInspection.pdf vorveröffentlicht.

Die Betonung bei „Deep Packet Inspection“ liegt auf dem Adjektiv „deep“. Daher ist zu klären, was genau daran tiefgehender ist verglichen mit einer nicht tiefgehenden Paketanalyse.

Erster Anknüpfungspunkt ist der Paketbegriff. Über sogenannte „Pakete“ werden Daten im Internet transportiert. Deren Zusammensetzung ist im sogenannten „OSI-Schichtenmodell (Open Systems Interconnection Reference Model)“ definiert. Das Modell beschreibt das Durchlaufen von sieben Schichten (Layern), in denen Funktionen und Protokolle definiert sind und einer bestimmten Aufgabe bei der Kommunikation zwischen zwei Systemen zugeordnet sind. Es basiert auf dem vierschichtigen DoD-Schichtenmodell, das auch als TCP/IP-Referenzmodell bezeichnet wird.

In diesem Zusammenhang ist jedoch nur wichtig, dass ein solches Datenpaket – eben wegen diesen sieben Schichten – aus mehreren Teilen besteht. Dies sind die Nutzdaten, die die eigentlichen Inhaltsdaten darstellen, und die sogenannten Kopfdaten, die auch als Header bezeichnet werden. Jede Schicht fügt den eigentlichen Inhaltsdaten einen eigenen Header hinzu. Die siebte Schicht, die Anwendungsschicht, die oft auch als „Application Layer“ oder „Layer 7“ bezeichnet wird, enthält deswegen nur den (Application) Header und die Nutzdaten. Jede weitere Schicht enthält die Nutzdaten, den eigenen Header und die Header der darunter liegenden Schichten.

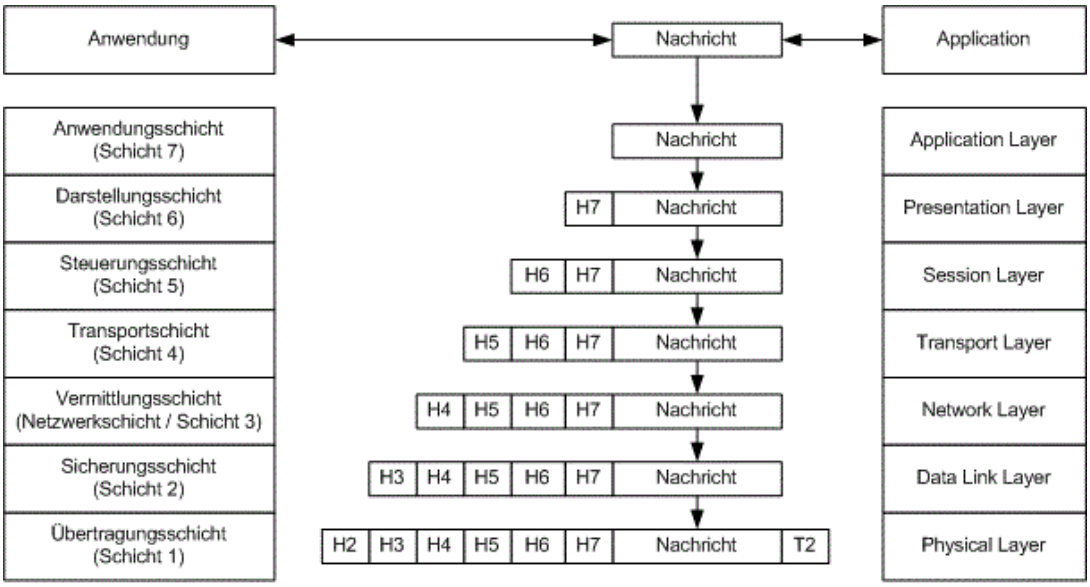

Abbildung 9: OSI-Schichtenmodell[1357]

[1357] *Sieber*, Einführung in das OSI-Referenzmodell, http://www.different-thinking.de/osi.php.

Network- und Accessprovider sollen Daten von einem Ausgangspunkt zu einem Zielpunkt innerhalb des Internets weiterleiten (sogenanntes „Routing“). Unter Accessproviding ist das Gewähren, Aufrechterhalten und nötigenfalls Resynchronisieren des technischen Zugangs zu geschlossenen oder offenen Netzen zu verstehen. Der Accessprovider tritt dabei als Zugangsvermittler auf. Networkprovider vermitteln keine Kundenzugänge zum Internet, sondern betreiben die TK-Infrastruktur, über die die Informationen durchgeleitet werden. Um dies zu ermöglichen, müssen die Router an den jeweiligen Knotenpunkten „wissen“, an welche IP-Adresse die Daten gesendet werden sollen. Diese Information in Form von Quell- und Zieladressen befindet sich im Header auf der dritten Schicht, dem so genannten IP-Header. Im bildlichen Vergleich mit der Briefpost wäre dies der Briefumschlag, auf dem die Absender- und Empfängeradressen stehen.

Damit ein Internetprovider seine Aufgabe erfüllen kann, reicht es demzufolge aus, nur den IP-Header eines Pakets auszuwerten. Daraus kann ein Router die Information entnehmen, woher das Paket kommt und wohin es gesendet werden soll. Vom Inhalt des Pakets muss ein Internetprovider folglich keine Kenntnis nehmen. Dieses Auswerten des Pakets mit dem Ziel, die IP im Header aufzufinden, ist – vereinfacht gesagt – die „Inspection“ aus dem Begriffspaar „Packet Inspection“.

Eine Vorstufe der „Deep Packet Inspection“ ist die „Shallow Packet Inspection“ (SPI). Im Vergleich zur DPI wird bei der SPI nur „oberflächlich“ ausgewertet. Hierunter fällt insbesondere die Auswertung des TCP- und UDP-Headers auf der vierten OSI-Schicht. Dadurch kann der Provider die genutzten Ports ermitteln.

Jede Art der Auswertung, die darüber hinausgeht, ist als „tiefgehend“ anzusehen. Je höher also die Schicht und umso eher Nutzdaten betroffen sind, umso tiefgehender ist die Auswertung. DPI betrifft folglich, in Abgrenzung zur SPI, die höheren Schichten fünf bis sieben des OSI-Modells. Es werden die Header aller Schichten und vor allem die eigentlichen Nutzdaten auf Schicht sieben ausgewertet.

3.8.1.1.2 Deep Packet Inspection und deren Relevanz für die IT-Sicherheit

Neben der Möglichkeit als Ermittlungsinstrument eingesetzt zu werden, ist die DPI-Technologie, wie bereits oben im Teil zur IT-Sicherheit angedeutet, in den falschen Händen, ein potentielles Sicherheitsrisiko für im Internet unverschlüsselt übermittelte Daten.[1358] Es ist daher angebracht die Daten auch auf dem Transportweg zu verschlüsseln. Umgekehrt erschwert eine Verschlüsselung den Zugriff durch die Ermittlungsbehörden oder macht einen solchen Zugriff unmöglich.

[1358] DPI kann aber auch als Sicherheitstechnologie in Firewalls eingesetzt werden, um Malware zu filtern; hierzu und zu weiteren Einsatzbereichen siehe *Bedner*, CR 2010, 339 und *ders.*, Rechtmäßigkeit der „Deep Packet Inspection“, http://kobra.bibliothek.uni-kassel.de/bitstream/urn:nbn:de:hebis:34-2009113031192/5/BednerDeepPacketInspection.pdf.

3.8.1.1.3 Rechtliche Bedeutung

Da die meisten Daten im Internet unverschlüsselt übermittelt werden, ist der Ermittlungsansatz mittels DPI erfolgversprechend. Der Vorteil der TK-Überwachung gemäß § 100a StPO liegt darin, dass sich Daten, die sich zu Beginn und am Ende der Übertragung außerhalb des deutschen Hoheitsgebiets befinden, für die Strafverfolgung nutzen lassen, soweit sie über Infrastruktur, also Providerrechner, Internetknotenpunkte oder Telekommunikationsleitungen, innerhalb Deutschlands übertragen werden.[1359]

Da § 100a Abs. 2 StPO einen Katalog der Straftaten beinhaltet, für den Abs. 1 der Vorschrift anwendbar ist, sind wesentliche Bereiche der (Internet)Kriminalität damit jedoch nicht ausforschbar.[1360] Wegen der prinzipbedingten Flüchtigkeit und der Gefahr der Unvollständigkeit der Daten dürfte zudem deren Beweiswert ebenfalls geringer sein als bei einer klassischen Beschlagnahme von physischen Datenträgern. Auch die mit DPI möglichen Manipulationstechniken von übertragenen Inhalten müssen bei der Beweiswürdigung beachtet werden. So ist es möglich, dass die überwachten Daten auf dem Weg vom Sender zum Empfänger bereits durch Dritte manipuliert wurden.[1361]

Zusammengefasst ist DPI, trotz dieser Einschränkungen, eine neuartige Möglichkeit der Ermittlungsbehörden den faktischen und rechtlichen Problemen in Cloudumgebungen zu begegnen.

3.8.1.2 Strafrechtliche Regelungen zum Geheimnisschutz

Neben strafprozessualen Aspekten sind auch Vorschriften des materiellen Strafrechts im Rahmen von Cloud Computing zu beachten. Dabei geht es im Wesentlichen um den Schutz von Privatgeheimnissen gemäß §§ 203, 204 StGB, Dienstgeheimnissen nach § 353b StGB, dem Steuergeheimnis nach § 355 StGB, in wenigen speziellen Fällen sogar Staatsgeheimnissen gemäß §§ 93, 95 StGB und der im Nebenstrafrecht geregelte Schutz von Geschäfts- und Betriebsgeheimnissen gemäß § 17 UWG.

§ 17 UWG regelt die strafrechtliche Bewehrung des Verrats von Geschäfts- und Betriebsgeheimnissen. Wegen der Begrenzung auf vorsätzliche Handlungen und der Notwendigkeit weiterer strafbarer Absichten (Zwecke des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen)[1362] ist die Vorschrift eher selten im Zusammenhang mit Cloud Computing anwendbar. Gleiches gilt für die Verletzung von Privatgeheimnissen

---

[1359] Siehe auch *Rath*, in: Schartner/Weippl, D-A-CH Security 2010, 190.

[1360] *Gercke*, CR 2010, 346.

[1361] Zum Beispiel mittels eines Man-in-the-Middle-Angriffs.

[1362] Einzelheiten dazu bei *Diemer*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 2011, UWG, § 17, Rn. 29 ff.

gemäß §§ 203 und 204 StGB und sonstige Geheimnisschutzvorschriften, beispielsweise das Steuergeheimnis nach § 355 StGB oder Staatsgeheimnisse gemäß §§ 93 und 95 StGB. Fahrlässigkeitsstrafbarkeit findet sich lediglich im Rahmen der Verletzung von Dienstgeheimnissen, nämlich der fahrlässigen Gefährdung wichtiger öffentliche Interessen gemäß § 353b Abs. 1 Satz 2 StGB.

Da eine aus ökonomischen Gründen motivierte Auslagerung der geschützten Daten im Regelfall nicht einen vorsätzlichen Geheimnisverrat darstellt, sind die meisten Vorschriften, bis eben auf § 353b Abs. 1 Satz 2 StGB, nicht einschlägig, da gemäß § 15 StGB für eine Strafbarkeit fahrlässigen Handelns eine solche ausdrücklich im Gesetz stehen muss. Fahrlässigkeit setzt nach der herrschenden Meinung eine objektive Sorgfaltspflichtverletzung und die objektive Voraussehbarkeit oder Erkennbarkeit der Tatbestandsverwirklichung voraus.[1363] Anknüpfungspunkt und Maßstab der objektiven Beurteilung einer Sorgfaltspflichtverletzung sind Anforderungen, die an einen einsichtigen und besonnenen Menschen in der konkreten Lage des Täters zu stellen sind.[1364]

Im Zusammenhang mit Cloud Computing und § 353b Abs. 1 Satz 2 StGB stellt sich die Frage, ob Personen im Sinne des § 353b Abs. 1 Satz 1 Nr. 1 bis 3 StGB die wesentlichen Gefahren des Cloud Computing bekannt sein müssen, insbesondere, dass Datenauslagerungen ohne starke Verschlüsselung die Gefahr der Kenntnisnahme durch Unbefugte bergen. Während das Herumliegenlassen von Akten die offensichtliche Gefahr der unbefugten Kenntnisnahme birgt, ist dies bei der Inanspruchnahme von Clouddiensten nicht unbedingt der Fall. Zum einen ist den meisten Menschen nicht bewusst, dass die Daten extern verarbeitet oder gespeichert werden und soweit dieses Bewusstsein vorhanden ist, werben die Anbieter oft gerade damit, dass ihre Dienste sicher seien. Angesichts der Neuheit der Technologie ist in der Regel davon auszugehen, dass die Nutzung von Cloudservices als solche nicht objektiv sorgfaltswidrig erfolgt.

Auf der Ebene der Schuld muss zudem eine subjektive Sorgfaltspflichtverletzung des Täters vorliegen. Dabei ist auf die persönlichen Fähigkeiten und das Wissen des Täters abzustellen. Dieser muss anhand seiner Fähigkeiten in der Lage sein, die objektiven Sorgfaltspflichten zu erkennen und zu erfüllen.[1365] Die Beurteilung der objektiven und erst recht der subjektiven Sorgfaltspflichtverletzung ist allerdings eine Frage des jeweiligen Einzelfalls.

Ein weiteres Problemfeld ist die Möglichkeit einer Tatbestandsverwirklichung durch Unterlassen. Ein solches Unterlassen wird insbesondere beim Offenbaren gemäß § 203 Abs. 1 Satz 1 StGB relevant, wenn der Berufsgeheimnisträger eine

---

[1363] *Kühl*, in: Lackner/Kühl, StGB, § 15, Rn. 36 mit weiteren Nachweisen, auch aus der Rechtsprechung des BGH.

[1364] *Kühl*, in: Lackner/Kühl, StGB, § 15, Rn. 37 mit weiteren Nachweisen.

[1365] *Hardtung*, in: Münchner Kommentar zum StGB, Band 3, § 222, Rn. 60.

Garantenstellung gemäß § 13 Abs. 1 StGB inne hat, was in den meisten Fällen der Fall sein wird.

Ob beispielsweise die fehlende Verschlüsselung bei einer Nutzung von Cloud Computing und die damit verbundene Offenbarung eine Tatbegehung durch Unterlassen erfüllt, ist jedoch zweifelhaft. Problematisch ist der dafür notwendige Vorsatz. Zum Unterlassungsvorsatz gehört nämlich das Bewusstsein einer möglichen Erfolgsabwendung.[1366] Der unverschlüsselt Hochladende erkennt jedoch nicht die (auch nur potentielle) Gefahr für die Daten und lädt die Daten auch nicht gezielt und absichtlich unverschlüsselt hoch. Insofern ist eine solche Konstellation allenfalls als straflose Fahrlässigkeit zu werten. Zudem sind einige der Ansicht, dass eine bloße Rechtsgutsgefährdung durch die Möglichkeit der Kenntniserlangung durch Dritte für die Tatbestandsverwirklichung nicht ausreicht.[1367]

Ein weiteres, auch zum Teil datenschutzrechtlich relevantes, Problem in diesem Zusammenhang betrifft den schweigepflichtigen Cloudprovider, wenn sich dieser externer Dienstleister zum Zweck der Vornahme von Wartungs- und Servicearbeiten bedient und nicht ausgeschlossen werden kann, dass ein Zugriff auf personenbezogene Daten notwendig wird. In solchen Fällen genügt der Provider seiner Garantenstellung, wenn er gemäß § 11 Abs. 5 BDSG und über den dortigen Verweis auf § 11 Abs. 1 bis 4 BDSG und die entsprechende Anwendung der Vorschriften, die erwähnten Voraussetzungen und Maßnahmen einhält und ergreift.[1368]

Das Verhältnis zwischen Cloudprovider und Wartungsdienstleister ist mit dem Verhältnis zwischen einem Auftraggeber und Auftragnehmer im Rahmen einer Auftragsdatenverarbeitung vergleichbar. Die entsprechende Anwendung ergibt sich aus dem Umstand, dass die Tätigkeit von Wartungs- und Serviceunternehmen im Sinne des § 11 Abs. 5 BDSG weder als Auftragsdatenverarbeitung noch Funktionsübertragung und auch nicht als Datenübermittlung einzuordnen ist, aber der gleiche Schutzbedarf für die Daten der Betroffenen wie bei einer Auftragsdatenverarbeitung besteht.[1369]

In diesem Zusammenhang eines Verhältnisses zwischen einem Auftraggeber und Auftragnehmer soll der Vollständigkeit halber auch auf die bereits erwähnte strafrechtliche Problematik der möglichen Gehilfeneigenschaft eines Providers im Sinne

---

[1366] *Kühl*, in: Lackner/Kühl, StGB, § 15, Rn. 7.

[1367] *Cierniak*, in: Münchner Kommentar zum StGB, Band 3, § 203, Rn. 52; *Kargl*, in: Kindhäuser/Neumann/Paeffgen, StGB, Band 2, § 203, Rn. 19a; a. A. hinsichtlich des Herumliegenlassens von geschützten Akten und Schriftstücken *Kühl*, in: Lackner/Kühl, StGB, § 15, Rn.17.

[1368] *Cierniak*, in: Münchner Kommentar zum StGB, Band 3, § 203, Rn. 52; *Kargl*, in: Kindhäuser/Neumann/Paeffgen, StGB, Band 2, § 203, Rn. 21; zu diesen Maßnahmen gehören insbesondere diejenigen nach § 9 BDSG samt Anlage, auf die in § 11 Abs. Satz 2 Nr. 3 BDSG verwiesen wird.

[1369] *Gola/Schomerus* 2010, § 11, Rn. 14; siehe hierzu auch Kap. 3.1.8.5.3.

des § 203 Abs. 3 Satz 2 im Verhältnis zu Schweigepflichtigen hingewiesen werden.[1370]

Zusammenfassend wird deutlich, dass der strafrechtliche Geheimnisschutz darauf abzielt, vorsätzlichen Geheimnisverrat zu ahnden. Als ultima ratio ist es schließlich auch nicht Aufgabe des Strafrechts, fahrlässige Versäumnisse von Mitarbeitern beim unreflektierten Umgang mit Geheimnissen, zum Beispiel durch die Nutzung von unsicheren Cloudservices, zu ahnden. Dazu sind innerbetriebliche oder innerbehördliche Richtlinien und Sanktionsmaßnahmen ausreichend. Letztere sind auch nur dann einschlägig, wenn die Mitarbeiter hinsichtlich des Umgangs mit den Daten und den darin gespeicherten Geheimnissen geschult und aufgeklärt wurden. Für Berufsgeheimnisträger ist eine Sanktionierung von fahrlässigem Verhalten auch durch das jeweilige Berufsrecht denkbar.

Effektiver Geheimnisschutz ist damit hauptsächlich eine Frage der internen Organisation und der technischen Gewährleistung des Schutzes. Eine möglichst optimale Umsetzung dieser beiden Aspekte führt zudem dazu, dass auch vorsätzlicher Geheimnisverrat erschwert wird und auch unter diesem Gesichtspunkt das Strafrecht seinen Charakter als ultima ratio bewahrt.

3.9 Bezüge zum Recht der Vereinigten Staaten

Die Darstellung von Aspekten des US-Rechts ergibt sich aus der Tatsache, dass die großen Public-Cloudprovider in den Vereinigten Staaten angesiedelt sind, so dass man bei einer praktischen Nutzung von Public Cloud Computing nicht selten auf diese US-Provider angewiesen ist. Im Folgenden sollen die wichtigsten Probleme, die insbesondere Widersprüche zum deutschen Rechtsverständnis aufwerfen, kurz aufgezeigt werden.

3.9.1 Electronic Discovery

Dem kontinentaleuropäischen Rechtskreis fremd, aber dennoch erwähnenswert, da im praktischen Unternehmensalltag vorkommend und auch mit Bezügen und teilweise Widersprüchen zum deutschen Recht, insbesondere deutschem Datenschutzrecht, ist die sogenannte „Electronic Discovery“ oder „e-Discovery“ nach US-Recht.[1371]

3.9.1.1 Beschreibung und Besonderheiten der e-Discovery

E-Discovery ist Teil eines vorgerichtlichen Verfahrens, der sogenannten „Pre-Trial-Discovery“. Letztere ist die vor der Hauptverhandlung oder dem ersten Termin

---

[1370] Siehe hierzu Kap. 3.1.8.7.

[1371] *Spies/Schröder*, MMR 2008, 275; detailliertere Ausführungen zur e-Discovery siehe bei *Geercken/Holden/Rath/Surguy/Stretton*, CRi 2010, 65; Einzelheiten zum Konflikt zwischen e-Discovery und deutschem Datenschutzrecht siehe bei *Burianski/Reindl*, SchiedsVZ 2010, 187 und *Rath/Klug*, K&R 2008, 596.

stattfindende umfassende und rückhaltlose Aufklärung des Sachverhalts durch die Anwälte der Parteien.[1372] Eine Partei in einem Gerichtsverfahren kann dabei von der Gegenseite die Vorlage umfassender Dokumente zu allen Tatsachen einfordern, die für den behaupteten Klageanspruch oder die Verteidigung relevant sein können.[1373] Am ehesten ist das Verfahren mit § 142 Abs. 1 ZPO vergleichbar, der die Vorlage von gewissen Dokumenten, allerdings auf Anordnung und gegenüber dem Gericht, regelt. *Electronic* Discovery bedeutet, dass elektronisch gespeicherte Informationen herauszugeben sind, wenn diese zur Sachverhaltsaufklärung oder als Beweismittel in Betracht kommen.[1374]

E-Discovery im internationalen Kontext hat die Folge, dass im Fall einer rechtlichen Auseinandersetzung in den Vereinigten Staaten Unternehmen in Deutschland gezwungen sein können, elektronisch gespeicherte Informationen an Dritte in die USA herausgeben oder übermitteln zu müssen.

Mit der flächendeckenden Durchsetzung von EDV und IT-Systemen entwickeln gerade elektronische Informationen immer größere Bedeutung in Pre-Trial-Verfahren. Vorteile sind neben der leichteren Durchsuchbarkeit im Vergleich zu papierförmigen Dokumenten auch der Umstand, dass elektronisch vorhandene Dokumente Metadaten enthalten, die wichtige Rückschlüsse darauf zulassen, wer wann auf ein Dokument zugegriffen hat.[1375]

Der Vollständigkeit halber soll darauf hingewiesen werden, dass auch in anderen „Common Law-Staaten“, namentlich Großbritannien, Discoveryverfahren üblich sind.[1376] Wegen der Einbindung Großbritanniens in die EU sind die potentiellen Datenschutzprobleme allerdings geringer.

3.9.1.2 Probleme im Zusammenhang mit Cloud Computing

Für deutsche Unternehmen die Cloudprovider aus den Vereinigten Staaten nutzen oder die ihren Sitz oder lediglich Zweigstellen in den USA haben, hat e-Discovery somit erhebliche praktische Bedeutung. Gemäß Regel 34 der Federal Rules of Civil Procedure (FRCP) sind Unternehmen, die Daten in der Cloud vorhalten oder anderweitig auslagern, rechtlich immer noch Gewahrsamsinhaber der Daten und damit verpflichtet, diese für potentielle Gerichtsverfahren vorzuhalten und zu sichern. Allerdings kann die Gegenseite direkt den Cloudprovider zur Herausgabe der Daten gerichtlich verpflichten, wobei der eigentlich betroffene Cloudkunde und erst recht

---

[1372] *Spies*, MMR 2007, Heft 7, V; *Rath/Klug*, K&R 2008, 596.

[1373] Zum Beispiel für die USA bei Bundesgerichten (Federal Courts) gemäß Regel 26 Federal Rules of Civil Procedure (FRCP); *Rath/Klug*, K&R 2008, 596; *Geercken/Holden/Rath/Surguy/Stretton*, CRi 2010, 65.

[1374] *Rath/Klug*, K&R 2008, 596.

[1375] *Spies*, MMR 2007, Heft 7, V.

[1376] Siehe dazu insbesondere *Geercken/Holden/Rath/Surguy/Stretton*, CRi 2010, 68.

der datenschutzrechtlich Betroffene unter Umständen von der Herausgabe erst spät oder überhaupt keine Kenntnis erlangen.[1377]

Sollten Cloudprovider mit Hauptsitz in den USA genutzt werden, besteht immer eine solche Unwägbarkeit für die Daten der nutzenden Kunden. Dabei ist es unerheblich, ob der Server des Cloudproviders, der die einschlägigen Daten oder Teile der Daten beinhaltet, auf US-Territorium oder in Europa steht. So ist es denkbar, dass ein US-Provider garantiert, dass die personenbezogenen Daten nur innerhalb Deutschlands gespeichert und verarbeitet werden, jedoch wegen der e-Discovery oder einer Verfügung eines US-Gerichts von diesem in die USA übermittelt werden müssen.

Eine weitere Verschärfung der Lage besteht in dem Umstand, dass die Herausgabe aufgrund einer e-Discovery, wegen des Status eines vorgerichtlichen Verfahrens (Pre-Trial), ohne richterliche Überprüfung des Herausgabebegehrens abläuft. Die Gegenseite muss lediglich darlegen, dass die Daten für den Prozess relevant sein könnten. Ist allerdings nicht der Cloudnutzer, sondern der Cloudprovider als Nichtpartei (Non-Party) Adressat, so bedarf es einer gerichtlichen Verfügung (Subpoena) gemäß den Regeln 34 (c) und 45 FRCP.

Das gleichgelagerte Problem haben Unternehmen mit Tochterunternehmen in den USA, die ihre Daten ausschließlich in Deutschland vorhalten und in den USA verklagt werden. Während diese jedoch zumindest wissen, dass die Daten übermittelt werden müssen, besteht in der obigen Konstellation der Nutzung eines US-Cloudproviders die Verschärfung, dass die betroffenen Unternehmen und vor allem die Betroffenen im Sinne des Datenschutzrechts erst spät oder überhaupt nicht von der Datenübermittlung oder Datenherausgabe erfahren. Direkt betroffene Unternehmen können die Daten hinsichtlich der Beweiseignung zumindest selbst vorauswählen und nicht relevante personenbezogene Daten erst gar nicht übermitteln oder zumindest anonymisieren oder pseudonymisieren, während ein Cloudprovider als Nichtpartei zu einer solchen Auswahl nicht in der Lage und auch nicht befugt ist. Im Zweifel, nicht zuletzt um möglichen Strafen durch das Gericht zu entgehen, übermittelt dieser alle vorhandenen Daten eines Unternehmens, um die Subpoena zu erfüllen, so dass die Situation für fremde personenbezogene oder geheime Daten in der Weise verschärft wird, dass auch vom Herausgabebegehren des Klägers möglicherweise überhaupt nicht umfasste Daten mit übermittelt werden.

Ein weiteres Problem von e-Discovery im Zusammenhang mit Cloud Computing besteht in der Verfügbarkeit der Daten in der Cloud. So ist es möglich, dass ein Cloudprovider während eines Vorverfahrens insolvent wird und der Kunde oder die Gegenseite nicht mehr an die Daten beim Provider gelangen.

[1377] *Curtis/Heckman/Thorp*, Cloud Computing: eDiscovery Issues and Other Risk, http://www.orrick.com/fileupload/2740.pdf.

Außerdem kann sich das technische Problem ergeben, dass sich die Daten wegen fehlender Standards und Inkompatibilitäten nicht portieren lassen, so dass der verpflichtete Cloudkunde die Daten nicht vom Provider an den Gegner übermitteln kann. Er trägt dann das Risiko Strafen vom Gericht aufgebürdet zu bekommen (contempt of court), Schadensersatz wegen Vernichtung von Beweismitteln (spoiliation) zahlen zu müssen oder den späteren Prozess zu verlieren.[1378]

Bei der Abwägung, ob ein Unternehmen seine Daten in die Cloud auslagert, sind diese Aspekte immer mit einzubeziehen. Im Extremfall kann ein durch nicht zugängliche oder nicht portierbare Daten verlorener Prozess ein Unternehmen in die Insolvenz führen.

3.9.1.3 Konflikt zwischen US-Recht und deutschem Datenschutzrecht

Für die elektronische Übermittlung personenbezogener Daten im Sinne des Bundesdatenschutzgesetzes aus Deutschland in die USA im Rahmen einer e-Discovery gelten, wie in den oben geschilderten internationalen Konstellationen, die §§ 4b und 4c BDSG. Für solche Fälle bleibt nach der in Deutschland vertretenen Rechtsauffassung immer das deutsche Datenschutzrecht maßgeblich.[1379]

Ausländisches Recht kann nicht als Rechtsgrundlage herangezogen werden, da ansonsten die mit dem deutschen Recht etablierten Schutzvorkehrungen umgangen werden.[1380] Sogar rechtliche Verpflichtungen, die auf dem Recht eines EU-Mitgliedstaats basieren, sind nicht ausreichend, obwohl das EU-Recht harmonisiert ist und die Datenschutzrichtlinie ein einheitliches Datenschutzniveau garantiert.[1381]

Unterstützung findet die Auffassung durch das Haager Übereinkommen über die Beweisaufnahme im Ausland.[1382] Für Ersuchen im Rahmen einer Pre-Trial-Discovery hat Deutschland gemäß Art. 23 des Übereinkommens einen Vorbehalt erhoben. Die Bundesrepublik behält sich vor, Rechtshilfeersuchen, die ein Pre-Trial-Discovery-Verfahren zum Gegenstand haben, nicht zu erledigen.[1383]

Die US-Gerichte sind allerdings der Auffassung, dass nur die Beweisaufnahme durch ausländische Behörden vom Übereinkommen umfasst ist, jedoch nicht die

---

[1378] Siehe zu den Konsequenzen auch *Spies*, MMR 2007, Heft 7, V f.

[1379] *Gola/Schomerus* 2010, § 4c, Rn. 7.

[1380] *Burianski/Reindl*, SchiedsVZ 2010, 192; *Artikel-29-Datenschutzgruppe*, WP 117 vom 1.2.2006, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_de.pdf, S. 8.

[1381] *Burianski/Reindl*, SchiedsVZ 2010, 192; *Simitis*, in: Simitis, BDSG, § 4b, Rn. 97.

[1382] Haager Übereinkommen vom 18.3.1970 über die Beweisaufnahme im Ausland in Zivil- oder Handelssachen und vom 25.10.1980 über die Erleichterung des internationalen Zugangs zu den Gerichten.

[1383] *Rath/Klug*, K&R 2008, 597 und *Geercken/Holden/Rath/Surguy/Stretton*, CRi 2010, 70 mit weiteren Einzelheiten zum Übereinkommen; *Spies*, MMR 2007, Heft 7, VI.

direkte Inanspruchnahme der ausländischen Unternehmen.[1384] In der Praxis besteht daher das Problem, das sich Unternehmen den Weisungen der US-Gerichte unterwerfen. Dies geschieht aus Kostengründen, zur Vermeidung von Sanktionen durch die US-Gerichte, insbesondere wenn sie Tochterunternehmen in den USA haben, oder aber auch, weil sie selbst Interesse an der Durchführung eines Pre-Trial-Verfahrens haben.[1385]

Rechtsgrundlage für die Übermittlung nach deutschem Datenschutzrecht soll manchen zufolge § 28 Abs. 1 Nr. 2 BDSG, nämlich die Wahrung berechtigter Interessen der verantwortlichen Stelle, sein. Allerdings müsste dabei für jede einzelne E-Discovery-Maßnahme eine Interessenabwägung hinsichtlich der Interessen der Betroffenen erfolgen, so dass das Ergebnis immer einzelfallabhängig ist.[1386] Legt man allerdings obige Ausführungen zugrunde, so käme man schon gar nicht zu einer solchen Abwägung.[1387] Eine solche unterstellt, dürfte es aber regelmäßig so sein, dass die Einzelmaßnahmen isoliert betrachtet zwar zulässig sein können, deren Kombination jedoch zu einer Unverhältnismäßigkeit der Übermittlung führt.[1388] Häufig geht es bei einer e-Discovery aber nicht um vereinzelte Dokumente, sondern gerade um eine Sammlung einer Vielzahl von Daten, so dass eine solche Unverhältnismäßigkeit und ein Verstoß gegen den Erforderlichkeitsgrundsatz und den Grundsatz der Datensparsamkeit das regelmäßige Ergebnis der Abwägung sein dürften.[1389] Lehnt man eine Abwägung der Interessen ab und betrachtet nur die Interessen der Betroffen, sprechen diese Argumente jedoch erst recht dafür die Daten nicht zu übermitteln.

Die Ausnahmen aus § 4c BDSG sind auch nur bezüglich des Datenschutzniveaus relevant, so dass immer noch ein Erlaubnistatbestand notwendig wäre. Aber auch beim Vorliegen eines solchen Erlaubnistatbestands sind die Ausnahmen zur Kompensation des unangemessenen Datenschutzniveaus nur selten einschlägig.

Eine Einwilligung nach § 4c Abs. 1 Nr. 1 BDSG scheitert in der Regel an der praktischen Machbarkeit, da von den angeforderten Daten in der Regel eine Vielzahl von Personen betroffen ist und auch nicht jeder einer solchen Übermittlung zustimmen wird. Im Unternehmensumfeld, also wenn Mitarbeiterdaten betroffen sind, besteht auch das Problem der Freiwilligkeit der Einwilligung. Arbeitnehmer könnten sich aus ihrem Anstellungsverhältnis genötigt fühlen, einer Übermittlung zuzustimmen, so dass diese mangels echter Freiwilligkeit ohnehin nicht rechtsgültig

---

[1384] *Rath/Klug*, K&R 2008, 597; Société Nationale Industrielle Aérospatiale vs. U.S. District Court, JZ 1987, 984.

[1385] *Rath/Klug*, K&R 2008, 597 f; *Spies*, MMR 2007, Heft 7, V, VI.

[1386] So zumindest *Rath/Klug*, K&R 2008, 598.

[1387] Siehe dazu Kap. 3.1.12.1.4.

[1388] Siehe zu einer ähnlichen Problematik auch Kap. 3.1.9.8.1.4.

[1389] Ähnlich *Rath/Klug*, K&R 2008, 598 hinsichtlich der Datensparsamkeit; zur Verhältnismäßigkeit als Kriterium *Burianski/Reindl*, SchiedsVZ 2010, 192.

wäre. Ein weiteres Problem bei der Einwilligung besteht in der Möglichkeit der Betroffenen, diese zurückzuziehen, so dass immer die Gefahr besteht, dass eine Übermittlung oder Verarbeitung ex nunc unzulässig wird.

Allerdings könnte man an § 4c Abs. 1 Nr. 4 BDSG, die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht denken. Diese Vorschrift und der entsprechende Art. 26 Abs. 1 lit. d) der Datenschutzrichtlinie sind allerdings nach Ansicht der Art. 29 Datenschutzgruppe und Stimmen in der Literatur eng auszulegen.[1390] Dabei gilt die bereits oben geäußerte Argumentation der Umgehung der Schutzwirkung der deutschen und europäischen Datenschutzregelungen. Zudem sind laut Artikel-29-Gruppe ausdrücklich die internationalen Übereinkommen, namentlich das Haager Übereinkommen zu beachten und einzuhalten.[1391] Dies hat zur Folge, dass die Ausnahmevorschrift des § 4c Abs. 1 Nr. 4 BDSG, wegen des erwähnten Vorbehalts zum Übereinkommen, nicht zur Anwendung kommt.

Gleiches gilt für Standardvertragsklauseln im Rahmen des § 4c Abs. 2 BDSG, da sich weder die Gegenseite, noch das später entscheidende Gericht auf Beschränkungen im Umgang mit den Dokumenten und den darin enthaltenen Daten festlegen lassen wird.[1392] Ähnliches gilt für das ohnehin kaum Schutz versprechende Safe-Harbor-Abkommen. Ob dieses überhaupt für ein Gericht in analoger Anwendung gelten kann, ist auch zu bezweifeln, da sich dieses an Unternehmen richtet. Allenfalls die Übermittlung zwischen den streitenden Parteien ist in dessen Rahmen möglich, wobei aber auch beim Safe-Harbor-Übereinkommen zusätzlich eine Rechtsgrundlage für die Übermittlung nötig wäre, da dieses, ebenso wie § 4c BDSG, lediglich das unangemessene Datenschutzniveau im Verhältnis zu den Vereinigten Staaten kompensiert.

Im Ergebnis ist also eine Übermittlung personenbezogener Daten im Rahmen einer e-Discovery in die USA nach deutschem und europäischem Recht praktisch nur in der äußerst unwahrscheinlichen Konstellation möglich, dass alle Betroffenen in die Übermittlung einwilligen.

1390 *Artikel-29-Datenschutzgruppe*, WP 114 vom 25.11.2005, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_de.pdf, S. 17; *Artikel-29-Datenschutzgruppe*, WP 117 vom 1.2 2006, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_de.pdf, S. 8; *Burianski/Reindl*, SchiedsVZ 2010, 194; *Däubler*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 4c, Rn. 4.

1391 *Artikel-29-Datenschutzgruppe*, WP 114 vom 25.11.2005, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_de.pdf, S. 18.

1392 So auch *Burianski/Reindl*, SchiedsVZ 2010, 193.

3.9.2 USA PATRIOT Act

Durch Ländergrenzen überschreitende Herausgabe- und Zugriffsbefugnisse von US-Behörden besteht eine Gefahr für den Datenschutz von in der EU belegenen und verarbeiteten Daten und für die IT-Sicherheit von in Europa angebotenen Cloudangeboten.

Die bekannteste US-Regelung dieser Art ist der sogenannte „USA PATRIOT Act".[1393] Der Übersetzung des Gesetzestitels zufolge, ein „Gesetz zur Stärkung und Einigung Amerikas durch Bereitstellung geeigneter Werkzeuge, um Terrorismus aufzuhalten und zu blockieren". Das Gesetz erlaubt dem FBI und der CIA nicht nur auf Daten auf Servern im Hoheitsgebiet der USA, sondern auch auf solche Server einzuwirken, die einem US-Unternehmen gehören und im US-Ausland physisch belegen sind.[1394] Die Unternehmen sind bei einer Behördenanfrage zur Übermittlung der angeforderten Daten verpflichtet. Dafür ist in der Regel auch keine Einschaltung von US-Gerichten notwendig. Durch Erlass eines sogenannten „National Security Letters" werden die Unternehmen unmittelbar durch die Behörden zur Herausgabe verpflichtet.[1395]

Durch den PATRIOT Act wurde zudem der „Foreign Intelligence Surveillance Act" verschärft. Dieser erlaubt die Überwachung von Telekommunikation im Ausland und ermöglicht den Geheimdiensten unmittelbaren Zugriff auf im US-Ausland befindliche Daten. Eine solche TK-Überwachung ist ebenfalls ohne Einschaltung von US-Gerichten möglich.[1396]

Wegen diesen umfassenden Zugriffsbefugnissen der US-Behörden ist es beispielsweise kanadischen und irischen Behörden gesetzlich untersagt, Daten ihrer Bürger

---

[1393] Apronym für „Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001", http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03162:]; Mitte 2011 wurden die verlängerungsbedürftigen Teile des PATRIOT Act um vier weitere Jahre verlängert; siehe dazu *Wilkens*, US-Parlament verlängert Patriot Act um vier Jahre, http://www.heise.de/newsticker/meldung/US-Parlament-verlaengert-Patriot-Act-um-vier-Jahre-1251456.html.

[1394] *Finn*, More On American Owned Data Centres & The Patriot Act, http://www.aidanfinn.com/?p=10380; ähnlich *Rath*, in: Schartner/Weippl, D-A-CH Security 2010, 190; außerdem haben Microsoft und Google die Beantwortung von Auskunftsersuchen der US-Behörden auf Grundlage des PATRIOT Act auch für innerhalb der EU belegene Daten ausdrücklich bestätigt; siehe *Sawall*, Europäische Cloud-Daten nicht vor US-Zugriff sicher, http://www.golem.de/1106/84620.html und *Ihlenfeld*, Google-Server in Europa vor US-Regierung nicht sicher, http://www.golem.de/1108/85533.html.

[1395] Siehe dazu *Böken*, Patriot Act und Cloud Computing, http://www.heise.de/ix/artikel/Zugriff-auf-Zuruf-1394430.html.

[1396] Vergleiche dazu Title 50 U.S.C., § 1802, http://www.law.cornell.edu/uscode/html/uscode50/usc_sec_50_00001802----000-.html.

auf Servern in den USA und auf Servern von US-Unternehmen zu speichern.[1397] Das Verbot gilt somit unabhängig davon, wo die Server physisch stehen.

Für US-Unternehmen, die in Europa agieren, ergeben sich damit unlösbare Rechtsprobleme. Nach US-Recht müssen sie den Übermittlungsbegehren der US-Behörden Folge leisten, nach europäischem Recht dürfen sie aber die Übermittlung nicht ausführen, wenn personenbezogene Daten Inhalt der Übermittlung sind und kein Erlaubnistatbestand eingreift. Einige Unternehmen halten diese Situation zu Recht für untragbar.[1398]

Die EU-Kommission und das EU-Parlament sind sich des Problems bewusst. Europäische Abgeordnete erwarten von der EU-Kommission, dass diese darauf hinwirkt, dass US-Behörden in den Fällen, in denen die Daten auf EU-Territorium belegen sind, die europäischen Regeln und Gesetze beachten.[1399] Allerdings ist anhand der bisherigen Erfahrungen absehbar, dass für US-Behörden EU-Recht und das Territorialitätsprinzip auch künftig keine Rolle spielen wird, wenn diese eine Zugriffsbefugnis nach US-Recht haben.

Darüber hinaus unterminiert der PATRIOT Act auch das Safe-Harbor-Abkommen.[1400] Ein am Abkommen teilnehmendes Unternehmen kann niemals garantieren, dass die ihm anvertrauten personenbezogenen Daten bei ihm sicher sind, wenn es den amerikanischen Ermittlungsbehörden oder Geheimdiensten diese Daten offenbaren muss oder sich die US-Behörden sogar ohne Kenntnis des Unternehmens der Daten bemächtigen können.

3.9.3 Auskunfts- und Aufbewahrungspflichten nach dem Sarbanes-Oxley-Act

Ähnlich zur E-Discovery verhalten sich Auskunfts- und Aufbewahrungspflichten nach dem Sarbanes-Oxley-Act (SOX)[1401] im Finanzbereich.[1402] SOX ist ein US-Bundesgesetz, dessen Einhaltung von der US-Börsenaufsicht SEC überprüft wird. Dem Gesetz zufolge müssen Unternehmen, deren Wertpapiere an US-Börsen ge-

---

[1397] *Greene*, The U.S. Patriot Act has an impact on cloud security, http://www.networkworld.com/newsletters/vpn/2009/092909cloudsec1.html; *Finn*, Irish Government Warns Against Using Microsoft Azure And Others, http://www.aidanfinn.com/?p=10367.

[1398] *Kirsch*, IT-Unternehmen rufen nach Rechtssicherheit für Cloud-Daten, http://www.heise.de/ix/meldung/IT-Unternehmen-rufen-nach-Rechtssicherheit-fuer-Cloud-Daten-1278767.html; *ders.*, US-Behörden dürfen auf europäische Cloud-Daten zugreifen, http://www.heise.de/ix/meldung/US-Behoerden-duerfen-auf-europaeische-Cloud-Daten-zugreifen-1270455.html.

[1399] *Gehring*, EU-Parlamentarier besorgt über US-Zugriff auf Cloud-Daten, http://www.golem.de/1107/84763.html; zu ersten gesetzlichen Regelungen siehe auch sogleich Kap. 3.10.

[1400] Siehe dazu Kap. 3.1.12.5.3.

[1401] http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3763.ENR:.

[1402] *Niemann/Paul*, K&R 2009, 450.

handelt werden, unabhängig von ihrem Hauptsitz (sogenannte „Foreign Private Issuers“), buchhalterische Prüfungs- und Revisionspapiere für einen Zeitraum von mindestens fünf Jahren aufbewahren.[1403] Die Parallele zur E-Discovery ergibt sich dann, wenn solche Papiere Personenbezug aufweisen und aus dem EU-Raum an US-Finanzaufsichtsbehörden übermittelt werden müssen.

Wie bei den nationalen Aufbewahrungsvorschriften müssen die Unternehmen zudem faktisch in der Lage sein, die angefragten oder zur Auskunft verpflichteten Daten in angemessener Zeit herauszugeben. Bei unzureichender Organisation während der Nutzung von Clouddiensten kann es vorkommen, dass die Daten nicht mehr auffindbar sind oder nach einer gewissen Zeit nicht mehr dem Zugriff des Unternehmens unterliegen.[1404]

Auch die Aufbewahrung beim Cloudprovider muss, ebenso wie im Zusammenhang mit nationalen Archivierungsvorschriften, so ausgestaltet sein, dass die Aufbewahrung manipulationssicher erfolgt und gewährleistet ist, dass die Daten während der Aufbewahrungsfrist tatsächlich vorhanden und abrufbar sind.

3.10 Empfehlungen zur Rechtsgestaltung

Im Rahmen der Untersuchung wurden mehrfach gesetzgeberische Defizite und sogar Widersprüche aufgezeigt. Im Folgenden sollen diese Defizite zusammenfassend dargestellt werden. Außerdem sollen rechtspolitische Verbesserungsvorschläge unterbreitet werden, wie diese gesetzgeberischen Mängel beseitigt werden können und dadurch die Rechtslage für den Rechtsanwender verbessert und vereinfacht werden kann. Rechtssicherheit ist nur dann gegeben, wenn die Rechtslage klar und in sich widerspruchsfrei ist. Im Rahmen der Vorschläge soll zudem auf bereits bestehende Gesetzesinitiativen mit Bezügen zu Cloud Computing eingegangen und deren Auswirkungen kurz aufgezeigt und bewertet werden.

Ein essentieller Mangel, der nicht nur speziell Cloud Computing betrifft, findet sich in § 9 BDSG und insbesondere in der Anlage zu Abs. 1 der Vorschrift. Die dort angeführten Maßnahmen sind im 21. Jahrhundert nicht mehr ausreichend, um ein Mindestsicherheitsniveau zu gewährleisten. Wie die Regelungen in einzelnen Bundesländern bereits andeuten, wird es zukünftig notwendig sein, auf IT-Schutzziele abzustellen. Die Klassifizierung und Sammlung der anerkannten IT-Schutzziele zeigte zudem, dass sich das künftige Gesetz nicht auf einige wenige Schutzziele[1405] beschränken darf, weil ansonsten die notwendigen Sicherheitsmaßnahmen auch zukünftig nur unvollständig umgesetzt werden. Außerdem bietet es sich an, flankie-

---

[1403] *Searchsecurity.de*, Sarbanes-Oxley Act, http://www.searchsecurity.de/glossar/SOX/articles/182066.

[1404] Zu nationalen Aufbewahrungspflichten und zum Vendor Lock-in siehe auch Kap. 3.6.2.

[1405] In den Landesdatenschutzgesetzen, die Schutzziele zum Inhalt haben werden unsystematisch sechs Schutzziele genannt; vergleiche Kap. 3.1.9.4.

rende gesetzgeberische Maßnahmen, die zurzeit nur in Spezialgesetzen geregelt sind,[1406] in einem allgemeinen IT-Sicherheitsgesetz[1407] als Rechtsrahmen für die IT-Sicherheit zusammenzufassen und nur abweichende oder ergänzende Regelungen in den jeweiligen Spezialgesetzen aufzuführen. So wäre es, analog zu § 109 TKG für Telekommunikationsunternehmen, sinnvoll ähnlich spezielle Regelungen für Cloudunternehmen aufzustellen. Solche Regelungen sind vor allem bei einer zukünftigen Bedeutung als kritische Infrastruktur angebracht. Insbesondere die Pflicht zur Aufstellung und der aufsichtsbehördlichen Überprüfung eines umfassenden Sicherheitskonzepts kann die IT-Sicherheit bei einem Cloudprovider erheblich erhöhen.

Inhaltlich könnte eine solche Spezialregelung verpflichtende und regelmäßige Audits und Zertifizierungen vorsehen. Mit dem Überschreiten einer gewissen Nutzerzahl könnten diese Pflichten zudem verschärft werden. Zum Beispiel in der Form, dass die Erfüllung gewisser Zertifizierungsstandards für den Weiterbetrieb notwendig ist oder die Häufigkeit der Überprüfungen erhöht wird. Darüber hinaus ist an Transparenzverpflichtungen für die Provider gegenüber den Nutzern zu denken. Insbesondere sind Einzelheiten über genutzte Subunternehmen den Cloudnutzern offenzulegen, falls die Cloudnutzer diese Informationen benötigen, weil sie die Nutzung gewisser Regionen oder von bestimmten Subunternehmen ausschließen wollen. Auch die Einsicht und Übergabe von Protokollen muss den Nutzern ermöglicht werden. Insgesamt sind die Informations- und Kontrollrechte der Nutzer im Vergleich zum Status quo zu stärken. Daneben sind aber auch die Betroffenenrechte nicht zu vernachlässigen, so dass die Transparenz im Verhältnis zwischen dem Provider und den Betroffenen, aber auch zwischen Cloudnutzern und Betroffenen, erhöht werden sollte. Dabei ist an erweiterte Informations- und Widerspruchsrechte zu denken.

Soweit eine Spezialregelung unterbleibt, ist rechtlich darauf hinzuwirken, dass Cloudprovider gewisse Mindestanforderungen an den Datenschutz und die Datensicherheit erfüllen, die zwingend in SLAs vereinbart werden müssen. Inhaltlich kann man sich an den obigen Vorschlägen orientieren.

Ein zweiter Mangel des nationalen Datenschutzrechts betrifft die Auftragsdatenverarbeitung. Das Bundesdatenschutzgesetz kennt keine Verantwortungsverteilung, wie es die Datenschutzrichtlinie mit der Figur der Joint Controllership vorsieht.[1408] Zwar ist nationales Recht richtlinienkonform auszulegen, jedoch wäre eine nationa-

[1406] Zum Beispiel § 109 TKG; siehe dazu Kap. 3.1.9.3.3.

[1407] Zur Idee der Einführung eines allgemeinen IT-Sicherheitsgesetzes siehe auch Kap. 3.1.9.1 und Fn. 723.

[1408] Vergleiche auch die Ausführungen in Kap. 3.1.8.8.

le Kodifizierung für den Rechtsanwender hilfreich.[1409] Mit sogenannten Auslagerungsketten, insbesondere mit Bezug zu außereuropäischen Staaten, muss auch nach nationalem Recht rechtlich widerspruchsfrei und klar umgegangen werden können. Bei einer gesetzlichen Regelung ist aber darauf zu achten, dass es nicht zu einer „Entledigung von Verantwortung“ entlang der Kette kommt. Die jeweiligen Rechte und Pflichten müssen präzise ausgewiesen werden. Soweit eine gesetzliche Regelung zu speziell wäre, sind gewisse Rahmenbedingungen festzulegen, die in den Verträgen zwischen den Beteiligten zwingend zu vereinbaren und auszufüllen sind.

Mit der Regelung von staatenübergreifenden Auslagerungsketten hängt die allgemeine Notwendigkeit differenzierterer Vorschriften zur Übermittlung personenbezogener Daten in Staaten ohne ausreichendes Datenschutzniveau zusammen. Neben der Differenzierung nach Datenschutzniveaus ist auch die unterschiedliche Sensitivität von Daten bei einer künftigen Regelung zu beachten.[1410] Erste gesetzgeberische Initiativen des Bundestags und des Bundesrats zeichneten sich ab, führten jedoch noch nicht zu konkreten gesetzlichen Regelungen.[1411]

Ebenfalls die Internationalität betreffend ist die Notwendigkeit überstaatliche Vereinbarungen und Datenschutzmindeststandards zu vereinbaren. Es ist ein internationaler Rechtsrahmen notwendig, innerhalb dessen Cloud Computing rechtssicher betrieben und genutzt werden kann.[1412] Momentan bestehen beispielsweise Widersprüche zwischen amerikanischem und europäischem Recht, wie man an den Zugriffsbefugnissen im PATRIOT Act sehen kann. Entsprechende völkerrechtliche oder bilaterale Vereinbarungen erfordern dann aber auch die Respektierung der jeweiligen Abmachungen und der fremden Hoheitsgebiete.

Weitere Diskrepanzen betreffen den Umfang von Haftungsausschlüssen der Provider. Während nach US-Recht die Haftung des Providers für Schäden annähernd komplett ausgeschlossen werden kann, ist dies nach deutschem und europäischem Recht nur begrenzt möglich.[1413] Eine Vereinheitlichung der Rechtslage und die Beachtung der Nutzer- und Verbraucherinteressen sind deshalb von Vorteil. Die Akzeptanz der Clouddienste bei den potentiellen Nutzern und insbesondere die Sicherheit und Verfügbarkeit der Dienste wird erhöht, wenn sich ein Provider nicht mehr seiner Verantwortung entledigen kann, weil möglichst weltweit einheitliche und verbindliche Haftungsregeln gelten.

[1409] Wohl anderer Auffassung *Roßnagel/Jandt*, ZD 2011, 161, die, auf die Datenschutzrichtlinie gestützt, eine Verantwortlichkeit mehrerer Stellen auch unmittelbar im nationalen Recht annehmen.

[1410] Siehe hierzu Kap. 3.1.12.6.

[1411] Vergleiche Kap. 3.1.12.6 und insbesondere die Fn. 1170 und 1171.

[1412] Siehe hierzu auch den Vorschlag von Microsoft in Kap. 2.4.1.1.13.

[1413] Siehe dazu Kap. 3.5.3.3.

Insbesondere auf EU-Ebene wurden die wesentlichen rechtlichen und praktischen Probleme des Cloud Computing erkannt und erste gesetzliche Initiativen gestartet, die einige der Probleme durch gesetzliche Regelungen angehen. Mit der sogenannten „Cloud-Strategie“ will die EU-Kommission Kontroll- und Regulierungsmaßnahmen harmonisieren und zumindest in der Europäischen Union verbindliche Haftungsregeln einführen. Darüber hinaus sollen die Defizite des Safe-Harbor-Abkommens durch Überprüfung der Selbstverpflichtungen der US-Unternehmen im Rahmen von Datenschutzaudits minimiert werden.[1414]

Frühe Entwürfe einer Datenschutzverordnung[1415] hatten bereits erste konkrete cloudspezifische Regulierungsansätze zum Inhalt. Beispielsweise soll gemäß Art. 16 Vendor Lock-in durch ein sogenanntes „Recht auf Datenportabilität“ verhindert werden. Um die Probleme mit US-Zugriffsrechten zu minimieren, regelte Art. 42 eines solchen Vorabentwurfs die Notwendigkeit der Zustimmung europäischer Datenschutzbehörden, wenn Gerichte oder Behörden aus Drittstaaten auf europäische Daten zugreifen möchten. In einer späteren Fassung wurde diese Regelung allerdings wieder gestrichen.[1416]

Auch die Problematik von in der EU belegenen Mitteln[1417] als Anknüpfungspunkt für die Anwendbarkeit von EU-Datenschutzrecht ist in den Verordnungsentwürfen erkannt worden. Diese definieren darüber hinausgehende neue und zusätzliche Kriterien, wann europäisches Datenschutzrecht Anwendung finden soll. Zum Beispiel gemäß Art. 2 Nr. 2 bereits dann, wenn sich Angebote an Personen richten, die ihren gewöhnlichen Aufenthalt in der EU haben.[1418]

Auf Europaratsebene wird die Europäische Datenschutzkonvention dahingehend überarbeitet, dass sie bei Cloud Computing und sozialen Netzwerken mehr Gewicht

---

[1414] *Gehring*, EU-Kommission will Cloud-Anbieter untersuchen, http://www.golem.de/1111/88050.html.

[1415] Siehe http://statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf und http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF; siehe dazu auch *Lüke*, EU-Datenschutzverordnung: Gegen den unkontrollierten Datenstrom, http://www.heise.de/ct/artikel/EU-Datenschutzverordnung-Gegen-den-unkontrollierten-Datenstrom-1391778.html; der Erlass der Verordnung würde wegen der unmittelbaren und vorrangigen Geltung die meisten nationalen Datenschutzgesetze obsolet machen.

[1416] Vgl. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF.

[1417] Siehe dazu Kap. 3.1.5.4.

[1418] Siehe hierzu *Moos*, Erster Entwurf einer EU-Datenschutzverordnung, http://www.nortonrose.com/knowledge/publications/60344/erster-entwurf-einer-eu-datenschutzverordnung.

erhält.[1419] Zudem soll darauf hingewirkt werden, die Konvention zum globalen Minimalstandard für Datenschutz zu etablieren.[1420]

Abschließend ist rechtspolitisch zu beachten, dass Cloudtechnologie dazu führen kann, dass die Rechtslage schleichend zu Ungunsten der Bürger geändert wird. So kann die Zentralisierung von Diensten und Daten zu einer Durchbrechung föderaler Strukturen führen, wie das Beispiel des ursprünglich geplanten Bundesmelderegisters zeigte.[1421]

[1419] *Ermert*, Novelle der Europarats-Konvention zum Datenschutz auf dem Weg, http://www.heise.de/newsticker/meldung/Novelle-der-Europarats-Konvention-zum-Datenschutz-auf-dem-Weg-1144430.html; zur Konvention siehe auch Kap. 3.1.2.2.2.

[1420] *Ermert*, Europarat will Datenschutzkonvention zum globalen Minimialstandard machen, http://www.heise.de/newsticker/meldung/Europarat-will-Datenschutzkonvention-zum-globalen-Minimialstandard-machen-1389776.html.

[1421] Siehe dazu Kap. 3.1.7.1 und Fn. 591.

4 Gestaltung rechtsverträglicher Cloudsysteme

4.1 Notwendigkeit und Maßstab der rechtlichen Gestaltung von Technik

Weil Technik nur zu ganz bestimmten Zwecken entwickelt wird, hat diese im praktischen Einsatz nicht nur beabsichtigte, sondern auch unbeabsichtigte soziale Auswirkungen. Die rechtliche Gestaltung von Technik versucht den rechtlich relevanten Teil dieser Auswirkungen durch technische Maßnahmen zu beeinflussen. Auswirkungen, die rechtlich als nachteilig zu bewerten sind, also Risiken, sind zu vermeiden oder zu vermindern, während vorteilhafte Auswirkungen, also die Chancen der Technik, ermöglicht, gefördert oder verstärkt werden sollen. Die so geartete Gestaltung erfolgt im Optimalfall noch vor oder während der Entwicklung einer bestimmten Technik. Rechtliche Gestaltung bedeutet, dass soziale Vorgaben in Form von Rechtsnormen für die Gestaltung maßgeblich sind. Maßstab und Anspruch der rechtlichen Gestaltung ist die Rechtsverträglichkeit. Rechtsverträgliche Gestaltung bedeutet, dass das Zusammenleben der Menschen durch die Technikgestaltung so zu beeinflussen ist, dass es möglichst weitgehend mit den Rechtszielen übereinstimmt.[1422]

4.2 Rechtliche Gestaltung anhand der KORA-Methode

Die konkrete Gestaltung der Cloudsysteme soll anhand der „Methode zur Konkretisierung rechtlicher Anforderungen“ (KORA) erfolgen. KORA ist allgemein eine Vorgehensweise, um rechtliche Anforderungen bei der Informationstechnikgestaltung zu berücksichtigen und wurde im Jahr 1993 im Rahmen einer Untersuchung zur rechtlichen Gestaltung betrieblicher ISDN-Telefonanlagen von der „Projektgruppe verfassungsverträgliche Technikgestaltung“ in Darmstadt entwickelt.[1423]

Seither wurde die Methode mehrfach und erfolgreich zur Gestaltung von unterschiedlichen technischen Systemen angewendet. Beispiele sind die Gestaltung von Sprachspeicherdiensten,[1424] von elektronischen Signaturverfahren in formularorientierten Vorgangssystemen,[1425] von Hypermedia-Systemen bei der Genehmigung von neuen Anlagen nach dem Bundesimmissionsschutzgesetz,[1426] von Systemen zum Interneteinkauf,[1427] von personalisierten Anwendungen in Assistenzsystemen[1428] oder von Workflowsystemen in der öffentlichen Verwaltung.[1429]

[1422] Allgemein zur rechtsverträglichen Technikgestaltung *Roßnagel* 1993, 192 ff., 267 ff. und *Pordesch* 2003, 257 ff.; zum Verhältnis von Recht und Technik siehe auch Kap. 1.5 und zu den cloudspezifischen Chancen und Risiken Kap. 2.4.1.

[1423] *Hammer/Pordesch/Roßnagel* 1993, 43 ff.

[1424] *Pordesch*, DuD 1994, 614.

[1425] *Pordesch/Roßnagel*, DuD 1994, 82.

[1426] *Idecke-Lux* 2000, 205 ff.

[1427] *Scholz* 2003, 341 ff.

[1428] *Schwenke* 2006, 59 ff.

Mit Hilfe der KORA-Methode werden aus rechtlichen Vorgaben an das Zusammenleben in vier Schritten technische Gestaltungsvorschläge abgeleitet. Dabei wird zwischen rechtlichen Anforderungen und rechtlichen Kriterien sowie technischen Gestaltungszielen und technischen Vorschlägen unterschieden. Die rechtlichen Vorgaben und Anforderungen werden demzufolge ab der dritten Stufe technischer und konkretisieren sich schließlich in konkreten technisch umsetzbaren Gestaltungsvorschlägen.[1430] Die Methode erlaubt es die bisherigen, nur lose zusammenhängenden, Ausführungen in ein schlüssiges und grundrechtlich untermauertes Gesamtkonzept zusammenzuführen und die wechselseitigen Abhängigkeiten, insbesondere die Bedeutung der IT-Sicherheit für Cloud Computing, zu verdeutlichen. Erst diese „Konvergenz“ schafft die Voraussetzungen, um rechtlich einwandfreie und sicherheitstechnisch adäquate Gestaltungsvorschläge entwickeln zu können. Die Interdisziplinarität zwischen Recht einerseits und Technik und Informatik andererseits ist demnach ein inhärenter Teil der KORA-Methode. Ökonomische und soziale Umstände werden unter dem Aspekt der Vorteile und Chancen in der Methode ebenfalls interdisziplinär mitberücksichtigt.

4.3 Ableitung von rechtlichen Anforderungen aus grundrechtlichen Vorgaben

Der objektive Schutzbedarf der Grundrechte und das subjektive Schutzbedürfnis des einzelnen Grundrechtsträgers gebieten es, die Entstehung neuer Gefahren durch die technische Entwicklung einzudämmen oder erst gar nicht akut werden zu lassen. Vor dem ersten Ableitungsschritt müssen die einschlägigen Vorgaben in Form von Grundrechten und der Rechtsprechung des Bundesverfassungsgerichts identifiziert werden.[1431] Im Anschluss können daraus die rechtlichen Anforderungen abgeleitet werden.

Die grundrechtlichen Vorgaben sind im Zusammenhang mit Cloud Computing und den damit einhergehenden Gefährdungen von Daten und Rechtsgütern überschaubar. Geschützt werden sollen personenbezogene Daten und Geschäfts- und Betriebsgeheimnisse. Hinzu kommt die Möglichkeit, Daten rechtsgemäß aufbewahren und zu Beweiszwecken nutzen zu können.

Personenbezogene Daten sind durch das Grundrecht auf informationelle Selbstbestimmung und den daraus hergeleiteten Datenschutz (A1) geschützt. Das Grund-

---

[1429] *Laue* 2010, 113 ff.

[1430] *Pordesch* 2003, 262.

[1431] In einigen Urteilen des Bundesverfassungsgerichts finden sich neben rechtlichen Vorgaben und Anforderungen auch manchmal Kriterien, Gestaltungsziele und sogar konkrete technische Gestaltungsvorschläge; ein Beispiel dafür wäre das Urteil zur Vorratsdatenspeicherung; siehe dazu BVerfGE 125, 260.

recht wurde vom Bundesverfassungsgericht aus dem allgemeinen Persönlichkeitsrecht gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG abgeleitet.[1432]

Der Schutz von Geschäfts- und Betriebsgeheimnissen (A2) ist aus Art. 12 Abs. 1 GG und je nach Auffassung auch aus Art. 14 Abs. 1 GG herleitbar.[1433] Sonstige Geheimnisse, die bei der Nutzung von Cloud Computing durch Behörden einschlägig sein können, sind insbesondere das Amts- und Dienstgeheimnis oder das Steuergeheimnis.

Das Amts- und Dienstgeheimnis, das für Beamte beispielsweise in Form der Amtsverschwiegenheit in § 67 Abs. 1 BBG und § 37 Abs. 1 BeamtStG einfachgesetzlich geregelt ist, geht auf die Treuepflicht des Beamten aus den in Art. 33 Abs. 5 GG erwähnten „hergebrachten Grundsätzen des Berufsbeamtentums“ zurück. Eine wichtigere Vorschrift, die den Geheimnisschutz durch Behörden und die Verwaltung betrifft, ist § 30 VwVfG. Demnach haben die am Verwaltungsverfahren Beteiligten einen Anspruch darauf, dass die zum persönlichen Lebensbereich gehörenden Geheimnisse oder Betriebs- und Geschäftsgeheimnisse von der Behörde nicht unbefugt offenbart werden. Dieser Rechtsanspruch auf das sogenannte „Verwaltungsgeheimnis“ stützt sich auf die oben erwähnten Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und Art. 12 Abs. 1 GG sowie Art. 14 Abs. 1 GG.[1434]

Das in § 30 AO geregelte Steuergeheimnis dient, wie das Datenschutzrecht, dem Schutz der informationellen Selbstbestimmung und stützt sich demnach ebenfalls auf Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und zusätzlich gegebenenfalls auf Art. 14 i.V.m. Art. 19 Abs. 3 GG, soweit Unternehmen durch das Steuergeheimnis geschützt werden sollen.[1435] Das Steuergeheimnis wird in § 24 Abs. 2 Satz 1 Nr. 2 BDSG als ein besonderes Amtsgeheimnis bezeichnet.[1436] Mit dem Steuergeheimnis aus § 30 AO hängt das in § 30a AO geregelte Bankgeheimnis zusammen. In diesem Zusammenhang ist auch noch einmal auf das Sozialgeheimnis aus § 35 SGB Abs. 1 i.V.m. mit den §§ 67 ff. SGB X hinzuweisen. Der Transport der Daten über das Internet und sonstige Telekommunikationsleitungen ist durch das Telekommunikationsgeheimnis aus Art. 10 GG geschützt.[1437]

Die Kontrollmöglichkeit (A3) als dritte Anforderung fußt auf dem Rechtsstaatsprinzip gemäß Art. 20 Abs. 2 Satz 2 und Abs. 3 GG sowie Art. 28 Abs. 1 Satz 1 GG und der Rechtsschutzgarantie aus Art. 19 Abs. 4 GG. Hauptziel der Kontrollmöglichkeit ist die Wahrung einer effektiven Rechtsdurchsetzung und damit letztlich die Gewährleistung der rechtsstaatlich begründeten Rechtssicherheit.

[1432] Siehe oben Kap. 3.1.3.1.

[1433] Zum Verhältnis zwischen Art. 12 Abs. 1 GG und Art. 14 Abs. 1 GG siehe auch Kap. 3.1.3.4.

[1434] *Bonk/Kallerhoff*, in: Stelkens/Bonk/Sachs, VwVfG, § 30, Rn. 1, 3; siehe auch Fn. 1433.

[1435] *Rüsken*, in: Klein, Abgabenordnung, § 30, Rn. 1.

[1436] *Rüsken*, in: Klein, Abgabenordnung, § 30, Rn. 3.

[1437] Zur Darstellung der einzelnen Grundrechte siehe oben Kap. 3.1.3.

Kurz zusammengefasst sind die rechtlichen Anforderungen somit der auf natürliche Personen abzielende Datenschutz (A1), der für Unternehmen und den Staat relevante Schutz von Geheimnissen (A2) sowie die Kontrollmöglichkeit (A3).

Die (einfach)gesetzliche Ausgestaltung der beiden wichtigsten Anforderungen entspricht im Wesentlichen dem oben dargestellten Rechtsrahmen. Der Datenschutz (A1) ist durch Datenschutzgesetze, aber auch direkt und indirekt durch vertragliche Abmachungen und Vereinbarungen geschützt, während der Schutz von Geheimnissen (A2) in den soeben dargestellten Vorschriften und zusätzlich in den oben dargestellten Strafvorschriften Anklang findet.[1438]

Datenschutzrechtlich enthält vor allem die Anlage zu § 9 BDSG Anforderungen in Form von Maßnahmen, die bereits zu technischen Gestaltungszielen verdichtet wurden.[1439] Eine Spezialvorschrift für die Beschäftigten und Mitarbeiter findet sich in der Verpflichtung auf das Datengeheimnis gemäß § 5 BDSG.[1440] Dieser Vertraulichkeitsgesichtspunkt ist zwar direkt auf Personen abzielend, allerdings ist die Einhaltung dieser Verpflichtung technisch zu unterstützen, so dass die entsprechende Gestaltung der Technik Verstöße minimieren hilft.[1441] Eine weitere Besonderheit von § 5 BDSG ist der anforderungsübergreifende Charakter als Geheimnisschutz- und Datenschutzvorschrift.

Die Kontrollmöglichkeit (A3) als Anforderung soll primär gewährleisten, dass die Daten auch nach Ablauf von gewissen Jahresfristen noch vorhanden sind und zu Beweiszwecken in möglichen Prozessen oder außergerichtlichen Verfahren herangezogen werden können. Es geht also um die prinzipielle Möglichkeit, eine Kontrolle der gespeicherten Daten durchführen zu können. Die Kontrollmöglichkeit umfasst einfachgesetzlich Aufbewahrungspflichten national nach dem Handelsgesetzbuch oder der Abgabenordnung und mit Bezug zu den Vereinigten Staaten nach dem Sarbanes-Oxley-Act.[1442] Zwar trifft die Verpflichtung zur Aufbewahrung den Cloudnutzer als Vorschriftsadressaten, jedoch muss ein Cloudprovider seine Dienste so ausgestalten, dass eine entsprechende Nutzung möglich ist, falls diese vom Nutzer gewünscht ist. Hierbei spielen auch die Aspekte des Vendor Lock-in und standardisierter und offener Schnittstellen eine Rolle.[1443]

Kontrollmöglichkeit als rechtliche Anforderung ist aber nicht nur im Sinne der Ermöglichung einer nachträglichen gerichtlichen Kontrolle oder Nutzung von Daten zu verstehen, sondern auch als tatsächliche Kontrolle im Sinne einer Prüfbarkeit

---

[1438] Zu den strafrechtlichen Geheimnisschutzvorschriften siehe oben Kap. 3.8.1.2 und 3.1.8.7.

[1439] Details zur Anlage und den entsprechenden Maßnahmen siehe in Kap. 3.1.9.

[1440] Siehe dazu auch Kap. 3.1.11.

[1441] Beispielsweise die technisch unterstützte Umsetzung des Vieraugenprinzips mittels aufgeteilter Credentials.

[1442] Zu Einzelheiten der Regelungen siehe Kap. 3.6 und Kap. 3.9.3.

[1443] Siehe dazu Kap. 2.4.1.2.2.

von Umständen, Systemen und Daten, vergleichbar mit dem IT-Schutzziel der Revisionsfähigkeit.[1444]

4.4 Rechtliche Kriterien

Aus diesen drei rechtlichen Anforderungen werden im zweiten KORA-Schritt rechtliche Kriterien entwickelt. Diese sind nicht nur aus einer Anforderung ableitbar, sondern haben oft zwei oder sogar alle drei Anforderungen als Ursprung. Die meisten Kriterien sind allerdings der informationellen Selbstbestimmung und damit dem Datenschutz geschuldet. Einige sind zudem als Datenschutzprinzipien anerkannt.

Kriterien enthalten sowohl Bezüge zur Technik als auch zu sozialen und rechtlichen Aspekten. Es handelt sich um soziotechnische oder rechtlich-technische Kriterien. Sie beschreiben Problemlösungen für die Anforderungen, jedoch noch ohne Bezug auf einen ganz bestimmten technischen, organisatorischen oder gar rechtlichen Lösungsansatz zu nehmen. Auf dieser Ebene sind alle technischen und auch nichttechnischen Lösungsmöglichkeiten noch denkbar.[1445]

4.4.1 Techniksicherheit (K1)

Ein gemeinsames Kriterium aus den Anforderungen Datenschutz (A1) und Geheimnisschutz (A2) ist die Techniksicherheit (K1) oder Technik(ab)sicherung, also die Herstellung und Gewährleistung von IT-Sicherheit. Ohne die Absicherung der Technik ist weder der Schutz der informationellen Selbstbestimmung noch der Schutz von Geheimnissen in verteilten und informationstechnologischen Systemen möglich. Techniksicherheit in diesem Sinne ist die Erkennung von Bedrohungen, deren Bewertung innerhalb einer Bedrohungsanalyse und die möglichst umfassende Absicherung eines Systems mittels erprobter und neuartiger Gegenmaßnahmen, so wie dies in allen Einzelheiten im Rahmen der Darstellung der IT-Sicherheit geschildert wurde.[1446]

4.4.2 Vertraulichkeit (K2)

Den beiden Anforderungen ist zudem das Element der Vertraulichkeit (K2) gemein. Während dies bei Geheimnissen und deren Schutz offensichtlich ist, gilt dies allerdings auch für die personenbezogenen Daten und die informationelle Selbstbestimmung. Die Daten „gehören“ zunächst dem Betroffenen. Die Aufhebung von Vertraulichkeit ist die höchste und privateste Form der Bestimmung über vertrauliche Daten. Sie sollen also nur mit dem entsprechenden Willen des Betroffenen ver-

---

[1444] Zu Letzterem siehe oben Kap. 3.1.9.5.10.

[1445] *Pordesch* 2003, 265.

[1446] Siehe Kap. 3.1.9.5 bis einschließlich 3.1.9.11.

öffentlicht werden. Dieser Vertraulichkeitsaspekt äußert sich im Datenschutzrecht beispielsweise in § 3 Abs. 9 BDSG.[1447]

Die Ableitung der Vertraulichkeit aus dem Computergrundrecht mittelbar über die Anforderungen Datenschutz und Geheimnisschutz bedeutet die Umformung eines IT-Schutzziels zu einem rechtlichen Kriterium. Die Bedeutung als, aus einer Anforderung abgeleitetes, Kriterium ist, wie der Begriff der Anforderung schon besagt, stärker als bei einem „bloßen“ Schutzziel. Im Gegensatz zu Zielen sind Anforderungen verbindlich.

Wie bei den Schutzzielen bereits erwähnt, bedeutet Vertraulichkeit, dass Informationen nur von Befugten erfasst werden können und vor Ausspähung geschützt sind.[1448] Die Vertraulichkeit als Schutz der Daten vor Ausspähung ergibt sich auch einfachgesetzlich aus der Anlage zu § 9 BDSG, dort insbesondere unter dem Aspekt der fehlenden Befugnis und den entsprechenden Kontrollmaßnahmen zur Abwehr (Satz 2 Nr. 1 bis 4 und Satz 3 der Anlage zu § 9 BDSG). Unbefugten in jenem Sinne bestimmte potentiell schädigende Handlungen zu erschweren oder unmöglich zu machen, ist letztlich Vertraulichkeitsschutz.

4.4.3 Transparenz (K3)

Transparenz als Kriterium (K3) basiert auf dem gleichnamigen IT-Schutzziel und Datenschutzprinzip und damit der Anforderung Datenschutz (A1), aber auch auf der Kontrollmöglichkeit (A3).

Auf den ersten Blick widersprechen sich die Forderungen nach Transparenz einerseits und Vertraulichkeit andererseits. Während die Vertraulichkeit direkt auf die Daten und deren Informationsgehalt abzielt, betrifft die Transparenz den Umgang mit diesen Daten, so dass sich der vermeintliche Widerspruch einfach und schnell auflösen lässt.

Gerade bei Cloud Computing mit potentiell unendlichen Ressourcen, einer Vielzahl von Beteiligten, der wenig durchsichtigen Virtualisierung, der allgemeinen Komplexität des Internets als Vermittlungsmedium und der Gefahr vertraglicher Unklarheiten ist die Forderung nach Transparenz zentral. Transparenz schafft Vertrauen und erleichtert das Treffen von Entscheidungen.

Beim Transparenzkriterium sind jedoch eher die Struktur der Datenverarbeitung und die daran Beteiligten transparent in den Mittelpunkt zu rücken und weniger jeder einzelne Umgang mit den Daten mitsamt Benachrichtigung und Abfrage über denselben. Der Datenumgang sollte allerdings nachträglich immer möglichst vollständig nachvollziehbar sein. Nicht zuletzt aus diesem Nachvollziehbarkeitsaspekt

---

[1447] Siehe dazu Kap. 3.1.12.2.

[1448] *Holznagel* 2003, 13; *Heckmann*, MMR 2006, 281.

wird auch der Zusammenhang zur Kontrollmöglichkeit deutlich. Transparenz fördert und ermöglicht die nachträgliche Kontrolle.

4.4.4 Entscheidungsfreiheit (K4)

Die Transparenz (K3) hängt eng mit der Entscheidungsfreiheit (K4) zusammen. Ohne Transparenz ist Entscheidungsfreiheit nur eingeschränkt oder überhaupt nicht möglich. Entscheidungsfreiheit bedeutet, dass der Betroffene über das Ob und die Art und Weise des Umgangs mit Daten entscheiden können muss. So war die Entscheidungsfreiheit auch ein wesentlicher Gesichtspunkt im Volkszählungsurteil.[1449]

Die Entscheidungsfreiheit hat aber nicht nur im alltäglichen Umgang mit den Daten und Diensten Bedeutung, sondern auch für die Auswahl eines Cloudproviders. Vor allem die Entscheidung über die erstmalige Migration von eigenen lokalen Ressourcen zu Cloudressourcen muss durch transparente Merkmale der Anbieter ermöglicht werden, die als Entscheidungskriterien für Cloudnutzer dienen können. Gerade die akuten Fragen der Wahrung der IT-Sicherheit und des Datenschutzes bei einem bestimmten Cloudanbieter sind für eine solche Entscheidung wichtig. Es ist deswegen vorteilhaft, wenn Cloudprovider die unterschiedlichen Eigenschaften und Merkmale ihrer Dienste den (potentiellen) Kunden offen legen. Bei der Entscheidungsfreiheit in diesem Sinne geht es nicht primär um ein Feedback an den Nutzer, wie die technische Ausgabe eines Zustands oder Vorgangs, sondern hauptsächlich um die Gesamtumstände unter denen der Umgang mit den Daten stattfindet.

Allererster Anknüpfungspunkt und gerade für den rechtlichen Rahmen besonders relevant, ist die Beantwortung der Frage, in welchem Hoheitsgebiet Daten verarbeitet und gespeichert werden und wohin diese übermittelt werden. Dies kommt einer groben Offenlegung der genutzten Rechenzentrumsstandorte gleich. Damit verbunden ist die Offenlegung über bestehende oder geplante Geschäftsbeziehungen mit Subunternehmen und ebenso deren territoriale Zuordnung. Die Informierung über Sicherheitsvorkehrungen und -maßnahmen, Sicherheitsvorfälle oder bestandende und nichtbestandene Audits ist ebenfalls ein zu beachtender Aspekt. Auch die Eigentumsverhältnisse und Entscheidungsbefugnisse sind für die Entscheidung, ob Daten einem Unternehmen anvertraut werden sollen, bedeutsam.[1450]

Wie bereits angedeutet sind Entscheidungsfreiheit und Transparenz jedoch nicht nur vor dem Eingehen der Geschäftsbeziehungen bedeutsam, sondern auch und gerade in der späteren Erfüllung derselben, also in der alltäglichen Praxis. Zu den soeben genannten Umständen kommen in der Alltagspraxis zusätzlich die technisch basierten Aspekte der Aus- und Rückgabe von Zustandsinformationen hinzu.

[1449] BVerfGE 65, 43.

[1450] Siehe hierzu auch die Übersicht bei *Essoh/Doubrava/Münch* 2011, 59.

Ein spezieller Unterrichtungsgrund im Zusammenhang mit Sicherheitsvorfällen ergibt sich unmittelbar aus dem Datenschutzrecht, nämlich die in § 42a BDSG geregelte Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten, die unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind.[1451] Neben der Transparenz ist hierbei auch die Entscheidungsfreiheit tangiert, da unter Umständen ein Sicherheitsvorfall nicht nur gegenüber potentiell Betroffenen kenntlich gemacht werden soll, sondern die Gesamtöffentlichkeit informiert werden muss, wie dies in § 42a Satz 5 BDSG erwähnt ist. Entsprechende Mitteilungen können so informierte, potentielle Nutzer von der Nutzung eines bestimmten Dienstes abhalten und dadurch deren Entscheidungsfreiheit stärken.

Neben dem „Ob“ einer Migration in die Cloud ist allerdings auch das „Wie“ zu beachten. Insbesondere wenn der Nutzer mehrere Provider zur Auswahl hat, ist dies ein zu beachtender Aspekt. Anhand transparenter Bedingungen kann er den für sich besten Anbieter auswählen. Auch die Abdingbarkeit und Verhandelbarkeit von Bedingungen ist ein Aspekt der Entscheidungsfreiheit. Es besteht derzeit die unvorteilhafte Situation, dass die Anbieter kaum oder gar keine Änderungen oder Vereinbarungen der Bedingungen erlauben.[1452] Dies ist nicht zuletzt der Einfachheit und der homogenen Bereitstellung der Dienste geschuldet. Die Möglichkeit sich informiert entscheiden und Änderungs- und Anpassungswünsche vorbringen zu können, ist vorgelagerter Daten- und Geheimnisschutz. Gleiches gilt für die später relevante fortlaufende und aktuelle Informierung des Kunden während einer laufenden Geschäftsbeziehung. Die Einordnung als Kriterium wird insbesondere an einer solchen Informierung ersichtlich, da diese technisch unterstützt erfolgen muss. Auch bei vorlaufenden Aspekten, wie der Entscheidung über die Auslagerung der Daten zu einem Anbieter, ist die Technik relevant. So kann ein Anbieter über Webseiten den technischen Zustand seines Cloudangebots für die Öffentlichkeit dokumentieren.[1453]

4.4.5 Erforderlichkeit (K5)

Wie im Rahmen der Darstellung des gleichnamigen Datenschutzprinzips bereits erwähnt, durchzieht das Erforderlichkeitsprinzip das gesamte Datenschutzrecht.[1454] Erforderlichkeit (K5) basiert demnach auf der Anforderung Datenschutz (A1). Daten, auch personenbezogene, die aufbewahrt werden müssen, unterliegen folglich diesem besonderen Zweck, so dass auch ein Zusammenhang mit der Kontrollmöglichkeit (A3) erkennbar wird.

[1451] International auch als „Security Breach Notification” bekannt.

[1452] Siehe dazu *Bradshaw/Millard/Walden* 2010, 15 ff.

[1453] Siehe dazu weiter unten Kap. 4.6.11 und Fn. 1512.

[1454] Zu weiteren Einzelheiten siehe oben Kap. 3.1.6.4.

Besonders erwähnenswert ist der Umstand, dass die Erforderlichkeit immer im Bezug zum geschützten Rechtsgut und nicht bezüglich technischer Gegebenheiten oder Notwendigkeiten zu bestimmen ist. Der Grundrechtsschutz soll gerade nicht unter den Vorbehalt technischer Möglichkeiten gestellt werden.[1455]

4.4.6 Zweckbindung (K6)

Die Zweckbindung (K6) entspricht ebenfalls überwiegend dem gleichnamigen Datenschutzprinzip und ist damit primär ebenfalls aus A1 abzuleiten. Dem Zweckbindungsgrundsatz zufolge dürfen personenbezogene Daten grundsätzlich nur zu dem Zweck verarbeitet werden, zu dem sie erhoben oder gespeichert worden sind und nicht für andere Zwecke.[1456] Weil die Zweckbindung das Recht auf informationelle Selbstbestimmung wahren soll, folgt daraus außerdem das „strikte Verbot der Sammlung von Daten auf Vorrat“.[1457]

Das Kriterium findet einfachgesetzlich Anklang in Nr. 8 der Anlage zu § 9 BDSG.[1458] Es hat aber auch für den Geheimnisschutz (A2) Bedeutung, da die Zweckbindung auch und gerade für Geheimnisse gilt, wie sich aus § 30 VwVfG, § 30 AO oder § 67 ff. SGB X ergibt.[1459]

Zweckbindung als Kriterium im hier verstandenen Sinne ist allerdings nicht nur daten-, sondern auch funktions- und dienstebezogen und damit weitergehender als der Datenschutzgrundsatz.[1460] Cloudfunktionen dürfen nicht über ihren rechtmäßigen und intendierten Zweck hinaus genutzt werden können. Dies gilt nicht nur für interne Funktionen im Zusammenhang mit der Cloudadministration, sondern auch für die dem Kunden zur Verfügung gestellten Funktionen und Dienste.

Je infrastrukturbezogener der Clouddienst ist, also je eher IaaS oder auch PaaS eine Rolle spielen, umso größer sind die Möglichkeiten des Nutzers das in der Cloud gebuchte System nach den eigenen Vorstellungen und Bedürfnissen anzupassen. Die erlaubten und nicht erlaubten Zwecke sind in den vertraglichen Vereinbarungen möglichst präzise festzuschreiben.[1461]

[1455] *Hammer/Pordesch/Roßnagel* 1993, 74.

[1456] Siehe auch die obigen Ausführungen im Rahmen der Darstellung des Datenschutzprinzips in Kap. 3.1.6.6.

[1457] BVerfGE 65, 47; allerdings aufgeweicht durch das Urteil zur Vorratsdatenspeicherung; siehe dazu BVerfGE 125, 260.

[1458] Siehe dazu auch oben Kap. 3.1.9.3.2.8.

[1459] So auch *Hammer/Pordesch/Roßnagel* 1993, 75.

[1460] *Hammer/Pordesch/Roßnagel* 1993, 75.

[1461] Siehe dazu auch weiter oben Kap. 3.5.3.

4.4.7 Trennbarkeit (K7)

Die Trennbarkeit (K7) oder Abtrennbarkeit von Daten und Systemen, die auch als Kompartimentierbarkeit[1462] oder Zerlegbarkeit bezeichnet werden kann, ist aus allen drei Anforderungen (A1, A2, A3) ableitbar. Personenbezogene, geheimbedürftige und für Beweiszwecke nötige Daten müssen von sonstigen Daten getrennt gespeichert und verarbeitet werden können. Insbesondere müssen die sie speichernden oder verarbeitenden Systeme abgeschottet werden können, so dass ein Bezug zur Techniksicherheit (K1) erkennbar wird. Zielsetzung der Trennbarkeit ist aber nicht nur die Sicherheit der Daten, sondern auch der nur zweckbezogene Umgang damit, so dass auch die Nähe zur Zweckbindung (K6) deutlich wird.

Einfachgesetzlich kann die Trennbarkeit aus der Trennungskontrolle nach Nr. 8 der Anlage zu § 9 BDSG und § 30 BDSG Abs. 1 BDSG hergeleitet werden.

Im Cloudkontext spielt die Trennbarkeit vor allem wegen der Mehrmandantenfähigkeit eine besondere Rolle. Im Grunde genommen ist auch die Verschlüsselung von Daten in einer Cloud als eine Art „Abtrennung“ von offenen Daten zu begreifen. Vertraulichkeit (K2), insbesondere in Cloudsystemen, ist nur durch trennende Maßnahmen zu erreichen.

4.4.8 Beherrschbarkeit und Steuerungsfähigkeit (K8)

Die Beherrschbarkeit und Steuerungsfähigkeit (K8) ist vorwiegend aus der Anforderung Kontrollmöglichkeit (A3), aber auch den Anforderungen Datenschutz (A1) und Geheimnisschutz (A2) ableitbar.

Beherrschbarkeit als Kriterium ist zum einen analog zum gleichnamigen IT-Schutzziel[1463] als Nichtauftreten von Nebenwirkungen und zum anderen im Hinblick auf die späteren Gestaltungsvorschläge als Notwendigkeit der Steuerungsfähigkeit durch die jeweiligen Anwender zu verstehen. Zentral in diesem Zusammenhang ist das Management Interface, mit dem der Cloudprovider die Cloud administriert. Daneben muss allerdings auch der Cloudnutzer jederzeit in der Lage sein, die von ihm gebuchten Cloudleistungen in seinem Sinne steuern zu können. Das Erfordernis der Beherrschbarkeit richtet sich damit sowohl an den Provider, als auch an die einzelnen Nutzer. Kontrolle im Sinne der Anforderung A3 ist nämlich nur möglich, wenn die Systeme und Daten kontrollierbar, sprich beherrschbar und steuerbar, sind. Ein Synonym für Beherrschbarkeit und Steuerungsfähigkeit wäre demnach auch Kontrollierbarkeit.[1464]

Ein weiterer Aspekt des Kriteriums betrifft die Zufälligkeit der Datenverarbeitung in großen Clouds. Zumindest der Provider muss in der Lage sein nachzuvollziehen

---

[1462] Abgeleitet vom englischen Begriff „Compartmentalization“.

[1463] Siehe oben Kap. 3.1.9.5.14.

[1464] Dies kommt auch durch die englische Bezeichnung des IT-Schutzziels der Beherrschbarkeit als „Controllability“ zum Ausdruck; siehe dazu Kap. 3.1.9.5.14.

und in viel geringerem Umfang, nämlich abhängig von der Anzahl der Server und Subunternehmer, vorherzusagen, wo Daten gespeichert werden.[1465] Maximale Beherrschbarkeit erfordert aber, dass der Provider und der Nutzer im Vorhinein festlegen können müssen, wie und wo die Daten gespeichert werden sollen. Dies kann beispielsweise dadurch erfolgen, dass die Zuhilfenahme von Subunternehmen in gewissen Ländern durch den Nutzer unterbunden wird. Falls ein Cloudprovider schon beim Eingehen der Vertragsbeziehungen eine solche Möglichkeit der Vorauswahl anbietet, dann muss er auch technisch gewährleisten, dass die Entscheidung des Kunden in der späteren Praxis eingehalten wird.

Diese Forderung widerspricht zwar der Flexibilität des Cloud Computing, ist jedoch notwendig, wenn der Nutzer als „Herr der Daten“ diese Herrschaft auch effektiv ausüben soll. Es reicht dabei für die Wahrung der Beherrschbarkeit aus, wenn der Provider und Nutzer bestimmte Regionen oder Subunternehmer ausschließen können, so dass Daten dort nicht verarbeitet werden. Beherrschbarkeit in dem Sinne, dass der Nutzer zu jeder Zeit das zu nutzende Rechenzentrum auswählen können muss, ist allerdings nicht notwendig.

4.4.9 Überprüfbarkeit (K9)

Die Überprüfbarkeit als Kriterium (K9) ist zum einen im Sinne des IT-Schutzziels zu verstehen, hat aber vor allem die Kontrollmöglichkeit (A3) und einfachgesetzlich die Eingabekontrolle nach Nr. 5 der Anlage zu § 9 BDSG als Ursprung. Sie erlaubt es, von Personen verursachte oder technische Fehler der Systeme nachträglich zu entdecken und gegebenenfalls abzustellen. Dabei spielt auch die Zurechenbarkeit als Schutzziel mittelbar eine Rolle. Primäres Ziel bei der Technikgestaltung ist jedoch weniger das Ziel der Heranziehung des Verantwortlichen, sondern dass eine solche Überprüfungsmöglichkeit überhaupt in die Technik implementiert wird, zum Beispiel über die Protokollierung der Zugriffe und der Systemzustände. Langfristiges Ziel ist der Schutz der Daten, indem die Fehler der Mitarbeiter und der Systeme reduziert werden.

Das Kriterium der Überprüfbarkeit ist aber auch aus den beiden Anforderungen A1 und A2 ableitbar. Datenschutz ist nicht möglich, wenn Systeme eigentlich geschützte personenbezogene Daten falsch verarbeiten und dadurch Dritten zur Kenntnis bringen. Geheimnisschutz ist vor allem durch die Mitarbeiter des Providers zu gewährleisten, da diese als Insider die größten Schäden anrichten können. Um unautorisierte Weitergaben und den damit verbundenen Verrat von Geheimnissen dokumentieren zu können, müssen die notwendigen technischen Voraussetzungen

[1465] Zur Problematik von Auslagerungsketten siehe Kap. 3.1.8.6.

geschaffen werden. Eine unmittelbare gesetzliche Kodifizierung des Kriteriums der Überprüfbarkeit findet sich, wie angedeutet, in Nr. 5 der Anlage zu § 9 BDSG.[1466]

Auch die Einhaltung des Zweckbindungsgrundsatzes als Kriterium (K6) ist zum Teil durch Überprüfbarkeit besser durchsetzbar. Nachträgliche, technisch implementierte, Überprüfbarkeit hat zudem eine abschreckende Wirkung gegenüber möglichem Fehlverhalten.

Die datenschutzrechtlichen Aufsichtsbehörden sind auf solche technischen Mittel der nachträglichen Kontrolle von Handlungen und Zuständen angewiesen. Überprüfbarkeit ist also auch im Sinne des oben genannten IT-Schutzziels der Revisionsfähigkeit zu verstehen.

Außerdem muss auch in umgekehrter Richtung ein Cloudprovider überprüfen können, ob sich die Nutzer an die vereinbarten Nutzungsbedingungen halten. Mögliches Fehlverhalten oder die Durchführung von Angriffen sind mit Protokollen leichter nachvollziehbar. Die Nutzer sind aber auf diese Dokumentation ihrer Handlungen hinzuweisen. Zum Beispiel mittels eines Hinweises in Form einer vorgeschalteten Seite oder Popups bei der erstmaligen Nutzung.

4.4.10 Beweissicherung (K10)

Die Beweissicherung (K10) ist eng verwandt mit der Überprüfbarkeit (K9). Protokolle können dabei auch für Beweiszwecke herangezogen werden. In Abgrenzung zur Überprüfbarkeit meint Beweissicherung als, aus der Kontrollmöglichkeit (A3) abgeleitetes, Kriterium das Vorhalten von Daten. Diese Daten sind nicht nur im Zusammenhang mit der Tätigkeit des Providers oder der Nutzung durch den Kunden entstanden, sondern die Beweissicherung umfasst vor allem die Inhaltsdaten, die in der Cloud vorgehalten werden. Für gewisse Daten muss sichergestellt sein, dass sie auch nach Jahren vorhanden sind und auch gelesen und ausgewertet werden können. Dieses Erfordernis ergibt sich spezialgesetzlich aus den bereits geschilderten Aufbewahrungsvorschriften.[1467]

Soweit rechtlich vorgegebene territoriale Begrenzungen bei der Speicherung bestehen, wie dies nach § 146 Abs. 2 AO für die elektronische Buchführung der Fall ist, sind auch diese durch entsprechende technische Gestaltung der Cloudservices zu gewährleisten.

4.4.11 Integrität (K11)

Aus dem Computergrundrecht ist mittelbar über die Anforderungen Datenschutz (A1) und Geheimnisschutz (A2) auch das rechtliche Kriterium der Integrität von Daten und Systemen ableitbar. Während sich das Urteil des Bundesverfassungsgerichts zur Onlinedurchsuchung, ebenso wie bei der oben angesprochenen Vertrau-

[1466] Siehe dazu bereits oben Kap. 3.1.9.3.2.5.
[1467] Siehe hierzu insbesondere Kap. 3.6.2 und Kap. 3.9.3.

lichkeit, auf eigengenutzte Systeme beschränkt, ist es geboten, das Kriterium im Sinne des IT-Schutzziels weit zu verstehen und alle Daten und Systeme zu umfassen.[1468]

Integrität ist auch mit der dritten Anforderung begründbar, weil die Kontrollmöglichkeit (A3) nur dann erfolgversprechend ist, wenn gewährleistet ist, dass die Daten unverändert sind und die Systeme wie beabsichtigt funktionieren.

4.4.12 Verfügbarkeit (K12)

Auch die Verfügbarkeit als rechtliches Kriterium kann aus der Kontrollmöglichkeit (A3) abgeleitet werden. Aufbewahrte Daten sind nur dann in diesem Sinne verfügbar, wenn die Daten vorhanden und die Systeme funktionsfähig sind. Im Gleichklang mit dem entsprechenden Schutzziel[1469] bietet es sich an, die Verfügbarkeit allerdings nicht nur für aufbewahrungspflichtige Systeme und deren Daten einzufordern, sondern alle Cloudsysteme so auszugestalten, so dass diese und die darin gespeicherten oder verarbeiteten Daten verfügbar sind. Die Verfügbarkeit als Kriterium ist demnach auch im Sinne von Ausfallsicherheit zu verstehen.

4.5 Technische Gestaltungsziele

Technische Gestaltungsziele sind aus den rechtlichen Kriterien entwickelte abstrakte technische Funktionen, aus denen im letzten Schritt die konkreten technischen Gestaltungsvorschläge abgeleitet werden.[1470] Die Gestaltungsziele sollen eine systematische rechtliche Bewertung und Gestaltung von Merkmalen konkreter Techniksysteme ermöglichen. Hierbei ist zu erwähnen, dass es sich nur selten um „Muss-Anforderungen“, sondern meist um anzustrebende „Soll-Anforderungen“ handelt. Gestaltungsziele können sich auf grundlegende Systemfunktionen, die Architektur oder auch auf Daten beziehen.[1471] Die Ausgestaltung als „Soll-Anforderung“ will den beteiligten Entwicklern einen möglichst breiten Gestaltungs- und Auswahlspielraum und damit Optionen bei der konkreten Entwicklung offen halten. Demgegenüber können sich einzelne konkrete Gestaltungsvorschläge wegen ihrer hohen Bedeutung für die IT-Sicherheit so weit verengen, dass von „Muss-Anforderungen“ auszugehen ist.[1472]

4.5.1 Verschlüsselung von Daten und Datenträgern (Z1)

Aus dem Kriterium Vertraulichkeit (K2) ist die Notwendigkeit der Verschlüsselung der Daten mit sicheren und dem aktuellen Stand der Technik entsprechenden Ver-

---

[1468] Zum Schutzziel siehe Kap. 3.1.9.5.12.
[1469] Zu Einzelheiten hierzu siehe oben Kap. 3.1.9.5.11.
[1470] *Pordesch* 2003, 266, 267.
[1471] *Pordesch* 2003, 266.
[1472] Zu solchen zwingenden Verdichtungen siehe auch weiter unten Kap. 4.6.

schlüsselungsalgorithmen ableitbar (Z1).[1473] Das entsprechende Gestaltungsziel ist auch rechtlich in Satz 3 der Anlage zu § 9 BDSG untermauert.

4.5.2 Etablierung eines umfassenden Management Interfaces (Z2)

Das Kriterium der Beherrschbarkeit (K8) durch den Cloudprovider erfordert, dass er die eigenen, aber auch die angemieteten Cloudressourcen steuern kann. Ein Management Interface für die eigenen Ressourcen ist regelmäßig vorhanden, da der Provider ansonsten die Cloud nicht betreiben und steuern könnte. Wichtiger ist jedoch der Aspekt der Steuerungsfähigkeit (K8) der angemieteten Ressourcen der Subunternehmen. Diese müssen sich in die Infrastruktur des Providers einfügen, beispielsweise indem die gleichen Standards und APIs genutzt werden.[1474] Der Provider muss aber auch in der Lage sein auf diese Ressourcen mindestens mittelbar, noch besser unmittelbar, Einfluss nehmen zu können und vor allem muss er deren Nutzung in bestimmten Fällen unterbinden können. Mit der Anmietung ist zudem sicherzustellen, dass das vermietende Subunternehmen möglichst wenig oder gar keinen Einfluss auf die Datenverarbeitung hat. Dem Providerwillen entgegenstehende Handlungen der Subunternehmen sollten durch technische Vorkehrungen unterbunden werden.

4.5.3 Sicherung des Interfaces durch Zugriffsschutzverfahren (Z3)

Für die Sicherheit der Cloud ist es essentiell, dass nur berechtigte und möglichst wenige Mitarbeiter des Providers auf das Management Interface Zugriff haben. Wegen der damit verbundenen umfassenden Einfluss- und Manipulationsmöglichkeit sind die Zugriffsschutzverfahren auf dem neuesten Stand der Technik zu halten.

Das Gestaltungsziel hat seinen rechtlichen Ursprung nicht nur in den Kriterien Techniksicherheit (K1), Vertraulichkeit (K2) und Beherrschbarkeit und Steuerungsfähigkeit (K8), sondern auch in der Zugriffskontrolle gemäß Nr. 3 der Anlage zu § 9 BDSG. Auch die Zutrittskontrolle gemäß Nr. 1 gewährleistet die Absicherung von Management Interfaces, indem Unbefugten der Zutritt hierzu verwehrt wird. Gleiches gilt für den Zugang im Sinne von Nr. 2 der Anlage.

4.5.4 Etablierung und technische Umsetzung des Vieraugenprinzips (Z4)

Bewährt ist in diesem Zusammenhang das Vieraugen- oder Mehraugenprinzip, um das Missbrauchsrisiko durch interne Angreifer möglichst minimal zu halten. Das kollusive schädigende Verhalten mehrerer Mitarbeiter ist weniger wahrscheinlich als der Missbrauch durch einen Einzelnen. Das Gestaltungsziel ist aus der Beherrschbarkeit und Überprüfbarkeit (K8), jedoch hauptsächlich aus den Kriterien Trennbarkeit (K7) und Vertraulichkeit (K2) ableitbar. Auch Transparenzgesichtspunkte (K3) spielen eine Rolle, da (intern) klar sein muss, wer mit wem interagieren

---

[1473] Zur Erläuterung der Verschlüsselung siehe weiter oben Kap. 3.1.9.9.1.

[1474] Siehe dazu auch weiter unten Kap. 4.5.20.

muss, um Zugriff auf Daten oder Systeme zu erlangen. Auch die Techniksicherheit (K1) soll dadurch ermöglicht und gewahrt werden. Das Vieraugenprinzip kann gemeinsam mit einem Zugriffsmanagementsystem (Z5) eingerichtet werden und in einem solchen technisch-organisatorisch umgesetzt werden.

4.5.5 Nutzung von Identitäts- und Zugriffsmanagementsystemen (Z5)

Administratorenaccounts sind mittels Privileged Identity Management (PIM), das auch als Software Account Password Management oder Privileged Account Management bezeichnet wird, zu kontrollieren.[1475] PIM erlaubt die Kontrolle darüber, wer Änderungen vornehmen darf, beinhaltet die Überwachung der konkreten Änderungen und liefert Protokolle über die Inhalte eines administrativen Vorgangs. Mit PIM sollte die Nutzung eines übergeordneten Identitäts- und Zugriffsmanagementsystems einhergehen, so dass Angriffe durch Insider minimiert werden.[1476] Bei größeren Providern sollten Prozesse innerhalb eines solchen Managementsystems, wie zum Beispiel Freigaben, Rollenzuweisungen oder die Passwortverwaltung teilautomatisiert ablaufen, um das komplexe Mitarbeitergeflecht beherrschen zu können.[1477] Für Kundenaccounts ist die Nutzung von Identitätsmanagementsystemen bereits wegen der Mehrmandantensituation in Clouds zwingend notwendig.

Die Etablierung von Zugriffsmanagementsystemen ist eng mit den bereits erwähnten Zugriffsschutzverfahren für die Interfaces und dem Mehraugenprinzip verbunden, so dass die übergeordneten Kriterien und Ursprünge des Gestaltungsziels die gleichen wie bei Z4 sind.

4.5.6 Sichere Authentisierung (Z6)

Um einen Missbrauch der Clouddienste durch Angreifer zu erschweren, indem die Angreifer identifizierbar werden, sind aus den Kriterien Techniksicherheit (K1), Beweissicherung (K10) und der Beherrschbarkeit und Überprüfbarkeit (K8) sowie dem Schutzziel der Authentizität Methoden und Strukturen zu etablieren, die die Nutzer bei der Anmeldung und ersten Nutzung der Cloudservices zweifelsfrei identifizieren. Die Bestandsdaten müssen korrekt sein.

Vor allem die derzeit übliche Vorgehensweise sich mittels Kreditkarten und den damit verknüpften Bestandsdaten bei Cloudprovidern anzumelden und zu authentisieren ist nicht ausreichend. Es ist nämlich nicht garantiert, dass der Kreditkarteninhaber auch der sich Anmeldende ist. Mit im Internet kursierenden gestohlenen Kreditkartendaten kann sich ein Angreifer als eine andere Person ausgeben und damit effektiv tarnen.[1478] So getätigte Angriffe sind nur noch sehr schwer nachver-

---

[1475] Allgemein dazu auch *Goldmann*, Datenschutz-Berater 11/2010, 18.
[1476] *Koehler*, <kes> Special - Sicheres Cloud Computing, März 2011, 20.
[1477] *Faber*, <kes> Special - Sicheres Cloud Computing, März 2011, 42.
[1478] Siehe auch Kap. 2.4.1.2.5.

folgbar.[1479] Neben direkten Angriffen auf die Cloudinfrastruktur und die gespeicherten Daten wird dadurch insbesondere die anonyme und missbräuchliche Zweckentfremdung von Cloudressourcen ermöglicht.[1480]

4.5.7 Trennung des Nutzertraffic vom administrativen Datenverkehr (Z7)

Weiter oben wurde dieses Gestaltungsziel der Trennung des Nutzerdatenverkehrs vom administrativen Datenverkehr als essentielle Sicherungsmaßnahme bereits im Detail beschrieben.[1481] Es ist unmittelbar aus der Trennbarkeit (K7) abzuleiten und stellt eine der technischen Umsetzungen des rechtlichen Kriteriums dar. Weitere Kriterien, die eine Rolle spielen, sind die Zweckbindung (K6), Beherrschbarkeit und Steuerungsfähigkeit (K8), Integrität (K11) und die Techniksicherheit (K1).

Zur Verwirklichung des Gestaltungsziels ist darauf zu achten, dass weder physisch noch virtuell ein Übergang zwischen Kundensystemen zu den administrativen Systemen besteht. Administratoren sollen nur in besonders begründeten Ausnahmefällen auf Kundensysteme und deren Inhalte zugreifen können. Kunden hingegen dürfen unter keinen Umständen Zugriff auf den administrativen Teil erlangen.

4.5.8 Trennung der virtuellen Nutzersysteme durch sichere Hypervisoren (Z8)

Insbesondere die Sicherung und Gewährleistung der Mehrmandantenfähigkeit durch den Einsatz von möglichst sicheren Hypervisoren ist ein ganz wesentlicher Aspekt der Trennbarkeit.[1482] Die von den einzelnen Cloudkunden genutzten virtuellen Maschinen sollen nicht nur im Verhältnis zum Provider hin abgeschirmt und abgetrennt sein (Z7), sondern auch untereinander. Das Gestaltungsziel stellt somit den zweiten technischen Aspekt des Trennbarkeitskriteriums (K7) dar.

Ebenso wie bei der Trennung des Datenverkehrs spielen demzufolge die rechtlichen Kriterien Trennbarkeit (K7), Zweckbindung (K6), Beherrschbarkeit und Steuerungsfähigkeit (K8), Integrität (K11) und Techniksicherheit (K1) eine Rolle.

4.5.9 Implementierung von Dokumentationsfunktionen (Z9)

Abgeleitet aus den Kriterien Überprüfbarkeit (K9), Beweissicherung (K10) und Transparenz (K3) ist das Gestaltungsziel der Etablierung eines leistungsfähigen Dokumentationssystems (Z9). Handlungen und Systemzustände und vor allem Orte und Zeiten der Datenverarbeitung sollen nachträglich überprüfbar und nachvollziehbar sein. Der Provider sollte möglichst alle Vorgänge dokumentieren können

---

[1479] Siehe dazu auch *Chip Online*, Bericht: Sony-Hacker kamen von Amazon, http://business.chip.de/news/Bericht-Sony-Hacker-kamen-von-Amazon_49035080.html.

[1480] Zu solchen missbräuchlichen Nutzungsmöglichkeiten siehe Kap. 3.1.9.10.6.

[1481] Siehe Kap. 3.1.9.9.2.

[1482] Siehe dazu insbesondere Kap. 3.1.9.10.1.1.

und bei Bedarf die Protokolle und Logdateien der Nutzungshandlungen an die jeweiligen Nutzer übergeben können.

4.5.10 Keine Weitergabe von administrativen Protokollen (Z10)

Administrative Protokolle sind von einer solchen Weitergabe an die Nutzer auszuschließen, weil diese Protokolle Rückschlüsse auf den Aufbau der Cloud, die Mitarbeiter und Berechtigungen und die Sicherheitsmaßnahmen erlauben und demzufolge ein Sicherheitsrisiko darstellen. Soweit Nutzungsprotokolle mit administrativen Inhalten verwoben sind, müssen sie vorher technisch getrennt werden. Zugrundeliegende Kriterien sind folglich die Vertraulichkeit (K2), Trennbarkeit (K7), Zweckbindung (K6), Beherrschbarkeit und Steuerungsfähigkeit (K8) und die Techniksicherheit (K1).

4.5.11 Kein Zugriff des Providers auf Protokollinhalte der Nutzer (Z11)

Umgekehrt dürfen die Protokolle und Dokumentationsinhalte, die die Nutzer anfordern oder selbst veranlasst haben, nicht durch den Provider einsehbar sein, soweit diese Inhaltsdaten betreffen. Der Nutzer kann allerdings dem Provider die Einsicht erlauben. Die Zustimmung hierüber sollte technisch unterstützt möglich sein, beispielsweise durch das Ausfüllen eines Onlineformulars. Das Gestaltungsziel ergibt sich aus den obigen Kriterien, jedoch um die Entscheidungsfreiheit (K4) ergänzt.

4.5.12 Sicherung der Protokolldaten durch Zugriffsschutzverfahren (Z12)

Der Provider muss intern gewährleisten, dass nur befugte Mitarbeiter auf die Protokolle zugreifen können, soweit dies providereigene Protokolldateien betrifft. Kundenseits gespeicherte Protokolle sollten nur durch die jeweiligen Nutzer abrufbar sein.

Die zugrundeliegenden Kriterien sind dabei dieselben, wie bei den Zugriffsschutzverfahren für die administrativen Interfaces (Z3).

4.5.13 Sichere Löschung der Protokolldaten (Z13)

Nicht mehr benötigte Protokolldaten sind sicher zu löschen. Die Löschungsverfahren sind am aktuellen Stand der Technik auszurichten. Insbesondere sind die Verfahren an die verwendeten Datenträger anzupassen. Auch verschlüsselte Daten sind sicher zu löschen, da sich im Laufe der Zeit durch die technische Entwicklung die Gefahr der unbefugten Entschlüsselung erhöht.

4.5.14 Sichere Löschung sonstiger Daten (Z14)

Nicht nur obsolete Protokolldaten, sondern auch alle anderen im Rahmen der administrativen Tätigkeit angefallenen Daten, die nicht mehr benötigt werden, sind sicher zu löschen. Da diese Daten oft Nutzungs- und Bestandsdaten beinhalten, sind sie besonders sensitiv.

Auch von den Nutzern veranlasste Löschungen von Inhaltsdaten, die nicht unmittelbar erfolgen oder beispielsweise nur bloße Verweise zu den Daten löschen, sind unverzüglich sicher und unwiederbringlich mit anerkannten Löschroutinen zu löschen.

Die technischen Gestaltungsziele der sicheren Löschung (Z13, Z14) von nicht mehr benötigten Daten sind aus den Kriterien Erforderlichkeit (K5), Zweckbindung (K6), Entscheidungsfreiheit (K4), Vertraulichkeit (K2) und der Beherrschbarkeit und Steuerungsfähigkeit (K8) hergeleitet.

4.5.15 Bestätigung der Löschung von Daten bei Subunternehmen (Z15)

Um die Beherrschbarkeit zu fördern, sind bei Subunternehmen erfolgte Datenlöschungen zu protokollieren und dem Provider automatisiert zu bestätigen, soweit er nicht selbst die Löschung überprüfen kann. Diese Durchführung und Bestätigung der Löschung muss auch nach einem Auslaufen von rechtlichen Beziehungen möglich sein. Hierfür sind technische Lösungen vorzuhalten, beispielsweise die verschlüsselte Zusendung der Protokolle und Löschungsbestätigungen an die Providersysteme per E-Mail, wenn keine direkte Verbindung mehr zwischen dem Cloudprovider und dem ehemaligen Subunternehmen besteht.

Übergreifende Kriterien sind, neben der erwähnten Beherrschbarkeit und Steuerungsfähigkeit (K8), auch die Transparenz (K3) und die Überprüfbarkeit (K9).

4.5.16 Aufbau von Redundanzen (Z16)

In Clouds ist die Ausnutzung der Vorteile einer redundanten Vorhaltung von Daten und Systemen besonders einfach und effizient möglich.[1483] Virtualisierung und die annähernd unendlichen Ressourcen erlauben bislang ungekannte Integritäts- und Verfügbarkeitsniveaus.[1484] Die Ausfälle von kompletten Rechenzentren oder die Zerstörung von Datenfragmenten haben bei einer redundanten Datenvorhaltung keine oder vergleichsweise geringe Auswirkungen für die Cloudnutzer.

Das Gestaltungsziel der redundanten Datenvorhaltung ergibt sich primär aus den Kriterien Integrität (K11) und Verfügbarkeit (K12), aber auch aus der Techniksicherheit (K1), Beweissicherung (K10) und der Beherrschbarkeit und Steuerungsfähigkeit (K8).

4.5.17 Nutzung von Fehlerkorrekturverfahren, Checksummen und Hashwerten (Z17)

Durch die Fragmentierung und Redundanz besteht die Gefahr, dass durch Fehler bei der Verarbeitung oder Speicherung unterschiedliche Versionen von Daten und Da-

---

[1483] Vergleiche dazu auch die obigen Ausführungen im Rahmen der Sicherheitsmaßnahmen in Kap. 3.1.9.9.6 sowie weiter unten den konkreten Gestaltungsvorschlag in Kap. 4.6.8.

[1484] Siehe dazu auch oben Fn. 893.

teien entstehen. Bei verschlüsselten Daten können diese ungewollten Änderungen außerdem dazu führen, dass Dateien nicht mehr lesbar sind.[1485]

Um solche Folgen zu verhindern, ist es notwendig Fehleranalyse- und Fehlerkorrekturverfahren zu implementieren. Auch Checksummen und Hashwerte und deren regelmäßige Prüfung sind geeignete technische Maßnahmen, um auf solche Speicher- oder Verarbeitungsfehler aufmerksam zu werden.

Rechtlich nicht vorgegeben, aber unter Umständen technisch geboten, ist eine auf den ersten Blick widersinnige oder kontraproduktive Maßnahme, nämlich die absichtliche und zufällige Störung der eigenen Dienste, Teilen derselben und von Arbeitsabläufen. Dieses Vorgehen hat einen ganz einfachen Hintergrund, nämlich die Erfahrungsbildung anhand konkret aufgetretener Sondersituationen und damit die Stärkung der Beherrschbarkeit und Steuerungsfähigkeit (K8) und der Verfügbarkeit (K12).

Die zugrundeliegende Komplexität von Cloudsystemen erlaubt es nicht, jegliches Ausfall- und Schadensszenario zu antizipieren und immer angemessen darauf zu reagieren. Deswegen ist es von Vorteil, in unregelmäßigen Abständen mit unvorhergesehenen Situationen konfrontiert zu werden und diese meistern zu müssen. Zudem erhöht diese künstliche Einstreuung von Fehlern die Aufmerksamkeit und Wachsamkeit der zuständigen Mitarbeiter. Im Ernstfall sind diese dann in der Lage schneller und effektiver zu reagieren. Es entsteht somit einer Art Fehlerkorrekturverfahren durch Erfahrungsbildung. Besonders wichtig ist die stetige Anpassung der Systeme und Failmechanismen an die gewonnenen Erkenntnisse, um damit letztlich die Ernstfälle zu reduzieren. Echte Störungen und Fehler können bis zu einem gewissen Grad sogar automatisiert behoben werden.[1486]

Eine solche Softwarekonstruktion im Cloudkontext ist „Chaos Monkey“, die vom Onlinefilmverleih und Streaminganbieter Netflix[1487] eingesetzt wird. Prominente Bedeutung erlangte die Software nach dem teilweisen Ausfall von Amazons EC2-Clouddienst im April 2011, der auch von Netflix genutzt wird. Während andere Anbieter komplett ausfielen, war Netflix durch die gestärkte Erfahrungsbildung in der Lage seinen Dienst aufrecht zu erhalten.[1488]

[1485] Siehe auch Kap. 3.1.9.7.2.

[1486] *Hicks*, Lessons Netflix Learned from the AWS Outage, http://techblog.netflix.com/2011/04/lessons-netflix-learned-from-aws-outage.html.

[1487] http://www.netflix.com.

[1488] *Hicks*, Lessons Netflix Learned from the AWS Outage, http://techblog.netflix.com/2011/04/lessons-netflix-learned-from-aws-outage.html; *Ernst*, Keine Erklärung für Ausfall von Amazons Cloud-Diensten, http://www.golem.de/1104/83028.html.

Das Gestaltungsziel ist aus den Kriterien Integrität (K11), Verfügbarkeit (K12), Überprüfbarkeit (K9), Beherrschbarkeit und Steuerungsfähigkeit (K8) sowie Beweissicherung (K10) abzuleiten.

4.5.18 Technisch unterstützte Auswahl von Subunternehmen (Z18)

Cloudnutzer müssen besonders bei der Auftragsdatenverarbeitung in der Lage sein, der Nutzung von Subunternehmen zustimmen oder diese abzulehnen zu können.[1489] Weiter oben wurde deshalb eine Kategorisierung der Unternehmen vorgeschlagen.[1490] Denkbar sind mindestens zwei Kategorien, nämlich eine Kategorie mit Subunternehmen, deren Heranziehung durch den Provider ohne Zustimmung des Cloudnutzers möglich ist, weil diese gewisse Mindestvoraussetzungen erfüllen, und eine Kategorie für Unternehmen, die der Zustimmung der Nutzer bedarf, weil im Einzelfall geprüft werden muss, ob diese bestimmte Sicherheitsvoraussetzungen oder sonstige Parameter erfüllen.

Die Nutzer sollten die Möglichkeit haben die vorab festgelegte Kategorie der sicheren Subunternehmen nach Belieben um weitere Subunternehmen erweitern und reduzieren zu können. Der Aufbau und die Nutzung einer Infrastruktur, die obige Kategorienauswahl implementiert, würde die Flexibilität des Providers deutlich erhöhen und dabei gleichzeitig die rechtlichen Vorgaben und Nutzerinteressen wahren.

Das Gestaltungsziel ergibt sich aus dem Kriterium der Beherrschbarkeit und Steuerungsfähigkeit (K8), der Transparenz (K3), eingeschränkt aus der Zweckbindung (K6) und soweit der Nutzer auch Betroffener der Datenverarbeitung ist, auch aus der Entscheidungsfreiheit (K4). Es ist zudem in den Nr. 4 und 6 der Anlage zu § 9 BDSG als Weitergabe- und Auftragskontrolle rechtlich angedeutet.

4.5.19 Regelbasiertes Load Balancing (Z19)

Um bildlich gesprochen die „Wolkenschleier zu lüften“, kann man das, ansonsten auf Zufall beruhende, Load Balancing, also die Serverlastverteilung, in einer Public Cloud so gestalten, dass es nach gewissen vorgegebenen Kriterien funktioniert und diese im Vorhinein festlegbar sind. Dadurch ist dann eher vorherzusagen, wo und wann Daten gespeichert werden. Ein Beispiel für ein solches Kriterium ist die regionale Begrenzung auf ein bestimmtes Rechenzentrum oder ein Hoheitsgebiet inklusive der dort belegenen Rechenzentren und Server.[1491] Die Verteilung und Verarbeitung von Daten erfolgt dann regelbasiert. Dieser regulierende Eingriff stellt

---

[1489] Siehe dazu auch die rechtlichen Ausführungen in Kap. 3.1.8.6.

[1490] Einzelheiten dazu sind in den Kap. 3.1.8.5.1 und 3.1.8.6 zu finden.

[1491] Ein ähnlicher Ansatz ist das regelbasierte „Intelligent Workload Management“ von Novell; siehe dazu *Borchers*, Novell will die Cloud intelligent verwalten, http://www.heise.de/newsticker/meldung/Novell-will-die-Cloud-intelligent-verwalten-880883.html.

einen Kompromiss zwischen optimaler Ausnutzung der verteilt vorhandenen Ressourcen, die nicht vorhersagbar und zufällig erfolgt, und der Einhaltung von gewissen rechtlichen oder sonstigen Vorgaben bei weiterhin größtmöglicher und effektiver Ressourcenausnutzung dar.

Das Gestaltungsziel ist unmittelbar aus der Beherrschbarkeit und Steuerungsfähigkeit (K8) ableitbar. Weitere relevante Kriterien sind die Transparenz (K3) und die Trennbarkeit (K7), wenn Daten nur auf bestimmten Servern vorhanden sein dürfen.

4.5.20 Etablierung und Nutzung standardisierter Schnittstellen und APIs (Z20)

Um das Problem des Vendor Lock-in gar nicht erst entstehen zu lassen, sollten einheitliche Standards für APIs[1492] und Schnittstellen vereinbart und in der Praxis genutzt werden.[1493] Soweit eine solche gemeinsame Übereinkunft nicht erfolgt, können im Laufe der Zeit De-Facto-Standards entstehen. Neue Cloudanbieter können sich an diesen De-Facto-Standards orientieren und ihre Technik den Standards entsprechend gestalten.[1494]

Das Gestaltungsziel ist aus den Kriterien Verfügbarkeit (K12), Beherrschbarkeit und Steuerungsfähigkeit (K8), aber auch der Transparenz (K3) und Entscheidungsfreiheit (K4) abzuleiten.

4.5.21 Fortschreitende Abstraktion und Zusammenfassung zu logischen Geräten (Z21)

Ein an die Grundlagen des Internets und des Cloud Computing gehendes technisches Gestaltungsziel ist die immer stärkere Abstrahierung von Objekten, Ebenen und Schichten. Es ist nicht ersichtlich, wieso es bei der Einfügung lediglich einer zusätzlichen Abstraktionsschicht durch die Virtualisierung bleiben soll. Stattdessen lässt sich durch weitere Abstraktionsschichten die Zahl der logischen Geräte in Clouds und verteilten Systemen immer weiter reduzieren, bis nur noch eine beherrschbare Schicht mit wenigen logischen Geräten vorhanden ist.[1495] Dadurch wird die Übersichtlichkeit gefördert, Komplexität zwischen den Geräten reduziert und

---

[1492] Zum API-Begriff siehe Fn. 336.

[1493] Siehe hierzu unter anderem die Kap. 2.4.1.2.2 und 2.4.1.1.8.

[1494] Als Beispiel für einen solchen De-Facto-Standard siehe das Beispiel des Storagedienstes „Amazon S3“ in Kap. 2.3.8.1.

[1495] Ein vergleichbares Konzept und Produkt, aber als Umsetzung in lokalen Rechenzentren, ist „QFabric“ von *Juniper Networks*. Siehe dazu *Juniper Networks*, Network Fabrics for the modern Data Center, http://www.juniper.net/us/en/local/pdf/whitepapers/2000327-en.pdf, *Juniper Networks*, http://www.youtube.com/watch?v=l5aQPthhoSc und *Pieper*, Auf dem Weg zu einem „neuen“ Netzwerk, http://www.funkschau.de/telekommunikation/know-how/article/80929/2/Eine_Ebene_fuer_exponentielles_Wachstum. Es ist allerdings nur konsequent die darin enthaltene Grundidee der Zusammenfassung zu logischen Geräten in einem größeren Maßstab auf ganze Cloudumgebungen mitsamt den Nutzerclients auszuweiten, so wie dies vorliegend erläutert wird.

die Beherrschbarkeit und Steuerungsfähigkeit (K8) und damit auch die Sicherheit (K1) dieser logischen Geräte gesteigert. Diese Abstraktion lässt eine Anknüpfung an physische Systeme auch nicht mehr zu, da durch die zusätzlichen Abstraktionsschichten nicht mehr feststellbar ist, wie, wann und wo Daten physisch gespeichert werden, so dass herkömmliche (meist untaugliche) Ansatzpunkte und Betrachtungsweisen obsolet werden.

Rechtlicher Anknüpfungspunkt sind nicht mehr physische Systeme, sondern die logischen Geräte, so dass auch die Transparenz (K3) und Überprüfbarkeit (K9) erheblich gesteigert wird. Diese Vorgehensweise ist auch nicht neu, da auch bisher rechtlich, oft willkürlich, auf physische Standorte oder Unternehmenssitze abgestellt wird. Rein technisch ist andererseits auch nicht begründbar, wieso rechtlich an Dateien in Dateisystemen von Betriebssystemen angeknüpft wird. Diese sind ihrerseits nichts anderes, als eine von mehreren Abstraktionsschichten, die auf der tatsächlichen physischen Speicherung auf atomarer Ebene oder der elektrischen Verarbeitung in Nanostrukturen innerhalb von Computerchips aufsetzen.

In künftigen Clouds ist es denkbar die logischen Geräte den jeweiligen Nutzern zuzuordnen. Neben einer Vielzahl von logischen Nutzergeräten, den bisherigen virtualisierten Mandantensystemen, gibt es zusätzlich das dem Provider zugeordnete Steuerungsgerät, bisher als Management Interface bekannt. Physische Hardware und virtuelle Maschinen, nicht nur beim Provider, sondern auch bei den Nutzern in Form von bisherigen Clients, werden damit logisch zu einem einzigen Gerät zusammengefasst. Ähnlich wie bei einem herkömmlichen Computer nicht einzeln an die Tastatur oder sonstige Peripherie angeknüpft wird, sind dann auch Clientsysteme, wie Tablets, Smartphones oder PCs, Teil dieses einzelnen Gesamtsystems.

An ein solches logisches oder virtuelles Gerät ist dann auch rechtlich anzuknüpfen. Beispielsweise durch das Sitzlandprinzip, so dass sich entweder alle Vorgänge in der Cloud nach dem Sitz des Providers richten oder nach dem Sitz des Providers für das zentrale Steuerungsgerät und nach dem jeweiligen Sitz des Nutzers für dessen genutztes logisches System. Alternativ könnte man hinsichtlich der Nutzer an den Standort der Nutzung mittels der Clients abstellen. Dies würde allerdings wieder eine Aufspaltung der Systeme in Server und Clients erfordern und die Protokollierung der Nutzung und des Standorts erfordern.

Mit der Durchsetzung von Ubiquitous Computing wird eine solche Zusammenfassung technischer Systeme, bestehend aus Sensoren, sonstigen Kleinstgeräten und herkömmlichen Clients, zu einzelnen logischen Geräten oder Systemen ohnehin notwendig werden, wenn diese künftig weiterhin beherrscht werden sollen.

Diese Abstrahierung führt zudem dazu, dass auch Rechtsregeln weniger komplex ausgestaltet werden müssen. Bestes Beispiel dafür ist das Datenschutzrecht, dass in seiner Ursprungsform an Großrechenanlagen anknüpfte und für diese Betrach-

tungsweise kohärent und in sich logisch war. Mit der immer tiefgehenderen Differenzierung in kleinere und vernetztere Subsysteme litt auch die rechtliche Anknüpfbarkeit und damit der Geltungsvorrang des Rechts.

4.6 Technische Gestaltungsvorschläge

Basierend auf den technischen Gestaltungszielen sollen im letzten KORA-Schritt technische Merkmale bewertet und schließlich konkrete technische Gestaltungsvorschläge entwickelt und unterbreitet werden.[1496]

Die folgenden Vorschläge, die interdisziplinär entwickelt und in der Sprache der Informatik gehalten sind, stellen in einer rechtswissenschaftlichen Untersuchung lediglich eine beispielhafte Auswahl dar. Diese erheben demzufolge keinen Anspruch auf Vollständigkeit und orientieren sich an der Sicherheits- und Persönlichkeitsrechtsrelevanz der in der Cloud gespeicherten und verarbeiteten Daten. Nicht zuletzt wegen dieser spezifischen Auswahl der wichtigsten Punkte tritt deren Charakter als Gestaltungs*vorschlag* im Folgenden in den Hintergrund, weil gewisse technische Maßnahmen zwingend umzusetzen sind[1497] oder eine solche Umsetzung dringend empfohlen wird.[1498] Es ist deswegen darauf hinzuweisen, dass bei einer umfassenden und möglichst vollständigen Aufstellung von Vorschlägen diese auch tatsächlich mehrheitlich als Vorschläge zu verstehen sind.[1499]

4.6.1 Verschlüsselung der beim Datentransport übermittelten Daten (G1)

Ein wichtiger sicherheitsrelevanter Anknüpfungspunkt in der Beziehung zwischen Cloudprovider und Cloudnutzer ist die wechselseitige Übermittlung von Daten. Wie bereits gesehen, kann der Datentransport leitungsgebunden über das Internet oder physisch mit Hilfe von Datenträgern, insbesondere beim erstmaligen Einbringen der Daten in die Cloud, erfolgen.

Bei der erstmaligen Übermittlung sind sehr große Datenmengen zu transportieren, so dass es billiger und schneller ist, wenn der Kunde die Daten mittels Datenträger, üblicherweise Festplatten, Speicherkarten oder optische Medien, an den Provider übersendet. Gestaltungstechnisch ist es notwendig, dass diese Datenträger vollständig verschlüsselt sind, beispielsweise mittels des AES-Verschlüsselungsverfahrens, und die Schlüssel oder Passwörter von den Datenträgern getrennt verschickt werden.

Werden Daten über das Internet übermittelt, so müssen der Providerserver und der Nutzerclient die SSL/TLS-Verschlüsselungstechnik mit sicheren Zertifikaten unter-

---

[1496] Allgemein dazu *Pordesch* 2003, 267.
[1497] Sogenannte „Muss-Umsetzung“.
[1498] Sogenannte „Soll-Umsetzung“.
[1499] Sogenannte „Kann-Umsetzung“.

stützen und diese auch tatsächlich nutzen.[1500] Insbesondere wegen der Überwachungsmöglichkeiten durch Deep Packet Inspection oder zur Verhinderung von Man-in-the-Middle-Angriffen ist es zwingend notwendig die Transportverschlüsselung als ein wirksames technisches Mittel zum Schutz der übermittelten Inhalte einzusetzen.

4.6.2 Verschlüsselung während der Speicherung (G2)

Für die Speicherung während des Vertragsverhältnisses, aber auch darüber hinaus, gilt das gleiche, wie beim Transport mittels Datenträger. Die in den Cloudrechenzentren befindlichen Datenträger samt Daten müssen ebenfalls mit dem Stand der Technik entsprechenden symmetrischen Algorithmen, zum Beispiel AES, Twofish oder Serpent, verschlüsselt sein. Dabei kann man die Sicherheit erheblich erhöhen, indem man mehrere Algorithmen kombiniert und sogenannte Verschlüsselungskaskaden errichtet. Kombiniert man unterschiedliche Algorithmen, müssten für einen erfolgreichen Angriff auf die Daten alle drei Algorithmen oder der verwendete Schlüssel gebrochen werden. In der Regel wird ein Angreifer deshalb die Schlüssel oder Passwörter als Angriffsziel auswählen. Ein Nachteil der kaskadierenden Verschlüsselung ist der höhere Rechenaufwand. Mit jedem zusätzlich genutzten Algorithmus erhöht sich der zur Ent- und Wiederverschlüsselung notwendige Rechenleistungsbedarf.

Die beiden Gestaltungsvorschläge G1 und G2 ergeben sich unmittelbar aus dem Gestaltungsziel der Verschlüsselung (Z1).

4.6.3 Sichere Schlüssel- und Passwortverwaltung (G3)

Um nicht die hohe Sicherheit der aktuell verwendeten Verschlüsselungsalgorithmen auszuhöhlen, ist es notwendig, ausreichend große Schlüssel(dateien) oder ausreichend lange Passwörter zu verwenden. Zudem sind diese sicher zu verwalten, so dass nur bestimmte Personen die Schlüssel oder Passwörter oder sogar nur Teile davon (Mehraugenprinzip) kennen oder auf solche zugreifen können.

Auch im Betrieb ist technisch durch Abschottungsmaßnahmen (CPU-Ringe[1501], Hypervisoren) und sorgfältige Programmierung sicherzustellen, dass die Schlüssel nicht extrahierbar sind. So bietet es sich an, die Schlüssel allenfalls im CPU-Cache anstatt im Arbeitsspeicher vorzuhalten. Die beste Verschlüsselungstechnologie ist nutzlos, wenn die Schlüssel leicht aus dem laufenden System für Angreifer extra-

---

[1500] Vor allem die Authentizität der Zertifikate muss dabei sichergestellt werden; siehe hierzu auch die Meldungen zur Entwendung von Zertifikaten beim Registrar Comodo Anfang 2011 von *Bachfeld*, Einzelner Hacker übernimmt Verantwortung für Zertifikats-Klau bei Comodo, http://www.heise.de/security/meldung/Einzelner-Hacker-uebernimmt-Verantwortung-fuer-Zertifikats-Klau-bei-Comodo-1216175.html und *Schmidt*, Zwei weitere Comodo-SSL-Registrare gehackt, http://www.heise.de/security/meldung/Zwei-weitere-Comodo-SSL-Registrare-gehackt-1219420.html.

[1501] *Wikipedia*, Ring (CPU), http://de.wikipedia.org/wiki/Ring_%28CPU%29.

hierbar sind. Gerade in virtualisierten Umgebungen ist dies ein wichtiger Aspekt. Ein kompromittiertes Subsystem kann im Extremfall dazu führen, dass alle verschlüsselt gespeicherten Daten lesbar werden. Um ein solches Szenario zu vermeiden, sollten unterschiedliche Daten mit unterschiedlichen Schlüsseln verschlüsselt werden. Während dies für die diversen virtualisierten Mandantensubsysteme selbstverständlich ist, sollten auch unterschiedliche administrative Daten, beispielsweise Protokolle, mit unterschiedlichen Schlüsseln und sogar unterschiedlichen Algorithmen verschlüsselt werden. Außerdem sollten die Schlüssel und Passwörter nur zeitlich befristet gültig sein. Hardwaretoken sollten regelmäßig auf ihre Integrität überprüft werden.[1502]

Der Gestaltungsvorschlag basiert auf den Gestaltungszielen Z1, Z3, Z4 und Z5.

4.6.4 Trennung von Schlüsseln und Daten (G4)

Eine damit zusammenhängende Lösung, die sowohl Verschlüsselung, als auch eine gewisse Trennung zwischen Provider und Nutzer bewirkt, ist die Verwaltung der Schlüssel durch den Nutzer selbst oder durch vertrauenswürdige externe Dritte. Dadurch sind die Daten für den Provider nicht oder allenfalls durch missbräuchliches Abgreifen aus den Computerspeichern oder Caches einsehbar. Zwar müssen die Daten zwecks Verarbeitung immer noch entschlüsselt werden, jedoch hat der Cloudnutzer als Dateninhaber weitgehende Kontrolle über die Daten.[1503] Diese sind Angriffen oder der missbräuchlichen Verwendung durch den Provider nur während der tatsächlichen Verarbeitung ausgesetzt. Die oben angeführten Sicherungsmaßnahmen im Rahmen des Schlüsselmanagements sind bei einer solchen Trennung ebenso gründlich zu beachten.

Einschlägige Gestaltungsziele sind Z1, Z5 und Z8. Wegen der hohen Effektivität und der vergleichsweise einfachen Implementierung von Verschlüsselung, sind G1 bis G4 zwingend umzusetzen.

4.6.5 Nutzung von homomorphen Verschlüsselungsalgorithmen (G5)

Problematischer als die bloße Speicherung verschlüsselter Daten ist der Fall der Verarbeitung von Daten in einer Cloud. Um eine Verarbeitung zu ermöglichen, müssen verschlüsselte Daten entschlüsselt werden.[1504] Eine Ausnahme von diesem Entschlüsselungserfordernis besteht bei der Nutzung von sogenannten voll homo-

---

[1502] Zur Wichtigkeit einer solchen Überprüfung siehe die Meldungen zum Hackerangriff beim betroffenen Sicherheitsdienstleister RSA durch *Coviello*, Open Letter to RSA Customers, http://www.rsa.com/node.aspx?id=3872 und allgemein bei *Sebayang*, RSA-Einbruch gelang durch Zero Day im Flash Player, http://www.golem.de/1104/82525.html.

[1503] Siehe dazu auch *Höfling*, Schlüsselmanagement: wichtiger Sicherheitsbaustein für Cloud-Nutzer, http://www.zdnet.de/magazin/41554679/schluesselmanagement-wichtiger-sicherheitsbaustein-fuer-cloud-nutzer.htm.

[1504] *Heidrich/Wegener*, MMR 2010, 806; *Pankert*, <kes> Special - Sicheres Cloud Computing, März 2011, 24.

morphen Verschlüsselungsmethoden, mit denen jedoch zur Zeit nur rudimentärste Verarbeitungsprozesse, beispielsweise die Anwendung der Grundrechenarten auf die verschlüsselten Daten, möglich sind.[1505]

Wie bei den bisherigen Vorschlägen spielt die Verschlüsselung als Gestaltungsziel (Z1) die wichtigste Rolle. Wegen des frühen Forschungsstadiums und der noch eingeschränkten praktischen Nutzbarkeit, ist homomorphe Verschlüsselung, im Gegensatz zu G1 bis G4 lediglich optional und bei passenden Anwendungsszenarien einzusetzen.

4.6.6 Trennung der verarbeitenden Rechner von der Cloudinfrastruktur während der Verarbeitung (G6)

Bei den herkömmlichen nichthomomorphen Verschlüsselungsmethoden ist es möglich, dass Angreifer die zeitweise unverschlüsselten Daten aus dem Prozessor, Arbeitsspeichern oder Caches abgreifen. Allerdings ist diese Verarbeitung vom Cloudprovider so ausgestaltbar, dass die verarbeitenden Rechner oder virtuellen Maschinen zum Zeitpunkt der Verarbeitung keinerlei Netzwerkanbindung mehr haben. Erst die wiederverschlüsselten Ergebnisse der Rechenoperationen werden dann erneut im Netzwerk und über das Internet dem Nutzer zur Verfügung gestellt. Bei dieser Vorgehensweise wird die technisch-organisatorische Maßnahme der Datentrennung ähnlich zur Nr. 8 der Anlage zu § 9 BDSG umgesetzt. Während die Gesetzesvorschrift an den Zweck der erhobenen Daten anknüpft, wird bei dieser Form der Datentrennung an die Technik und die potentiellen Zugangsmöglichkeiten zu den Daten angeknüpft.

Eine andere Form der Absicherung bietet die Einfügung einer zusätzlichen Abstraktionsschicht durch die Virtualisierung. Dabei wird eine logische Schicht zwischen Anwender und Ressource zwischengeschaltet, um die physischen Gegebenheiten der Hardware zu verstecken. Dies erlaubt auch die Implementierung von zusätzlichen Sicherheitsmechanismen, zum Beispiel die oben thematisierte Trennung zwischen offlinegeschalteten datenverarbeitenden virtuellen Maschinen und solchen, die online angebunden sind. Durch Virtualisierung von Rechnern und Netzwerken kann diese Trennung schnell und automatisiert erfolgen.

Diese Form der Trennung ist am ehesten aus dem Gestaltungsziel der Trennung des administrativen und des Kundendatenverkehrs (Z7) abzuleiten. Die Verschlüsselung (Z1) spielt hingegen nur eine untergeordnete Rolle. Die Umsetzung und Nutzung einer solchen Trennung sollte in der Praxis immer erfolgen, wenn sie möglich ist. Wegen der vorhandenen Virtualisierung und der damit einhergehenden einfachen

---

[1505] Zu Neuerungen bei der Entwicklung homomorpher Verschlüsselungsmethoden, insbesondere für Cloudumgebungen, siehe *Schwan*, Voll homomorphe Verschlüsselung in der Cloud, http://www.heise.de/newsticker/meldung/Voll-homomorphe-Verschluesselung-in-der-Cloud-1021361.html und *Simonite*, Sicheres Computing für die Cloud, http://www.heise.de/tr/artikel/Sicheres-Computing-fuer-die-Cloud-1021071.html.

Umsetzung in Cloudumgebungen, ist die Trennung unter solchen vereinfachten Umständen mindestens geboten.

4.6.7 Einsatz von bewährten und gehärteten Hypervisoren (G7)

Neben dem mehrfach erwähnten Einsatz von Hypervisoren, die auch als Virtual Machine Monitor bezeichnet werden, ist auch an den Einsatz von Sandboxes zu denken.[1506] Bekannte und mit der geläufigen Virtualisierungssoftware eingesetzte Hypervisoren sind der Xen Hypervisor, VMware ESX, IBM z/VM, OpenVZ Hypervisor, der direkt im Linuxkernel integrierte Hypervisor der Kernel-based Virtual Machine (KVM) oder Microsoft Hyper-V.[1507]

Beim Einsatz und der Entwicklung der Hypervisoren und der zugrundeliegenden Virtualisierungssoftware ist nicht nur (zwingend) deren Sicherheit und Fähigkeit zur Segmentierung zu betrachten, sondern auch auf Performancegesichtspunkte zu achten, so dass die Dienste adäquat genutzt werden können und verfügbar sind.

Während Hypervisoren wesentlicher Teil der Virtualisierungssoftware sind, können Sandboxes auch ohne Virtualisierungstechniken eingesetzt werden. Sandboxes werden in der Regel dazu verwendet, um Software oder Softwareteile vom Rest eines Systems abzuschirmen, also in den metaphorischen „Sandkasten“ zu setzen. Neben der Einfügung einer zusätzlichen Sicherheitsschicht, beispielsweise laufen viele Plugins in Browsern in Sandboxes, werden sie auch genutzt, um erkannte Schadsoftware in einer abgesicherten Umgebung analysieren zu können. Letzterer Aspekt kann beispielsweise bei PaaS und der Entwicklung von Sicherheitssoftware relevant werden.

Der Gestaltungsvorschlag ergibt sich unmittelbar aus dem Gestaltungsziel Z8. Wegen der hohen Bedeutung sicherer Hypervisoren ist die Umsetzung zwingend.

4.6.8 Verteilung und Replizierung der Daten auf unterschiedliche physische Server (G8)

Um ein möglichst hohes Datenschutz-, Datenverfügbarkeits- und Datenintegritätsniveau zu gewährleisten, sollten Daten, insbesondere Daten der Cloudnutzer, über mehrere physische Server aufgeteilt werden, so wie dies dem Cloudprinzip folgend bei Public Clouds üblicherweise heute schon gehandhabt wird. Dabei sollte aus Datenschutzgründen darauf geachtet werden, möglichst nur Datenfragmente auf den unterschiedlichen physischen Servern zu lagern, so dass die Information erst durch

---

[1506] Zur Bedeutung der Hypervisoren im Rahmen der Virtualisierung siehe auch oben die Kap. 2.3.4.2.1 und 3.1.9.10.1.1.

[1507] *ITWissen.info*, Hypervisor, http://www.itwissen.info/definition/lexikon/virtual-machine-monitor-VMM.html; zum KVM-Hypervisor siehe auch die Bestrebungen der Open Virtualization Alliance, diesen für Cloudumgebungen weiterzuentwickeln; *Diedrich*, IT-Schwergewichte unterstützen Virtualisierung mit KVM, http://www.heise.de/newsticker/meldung/IT-Schwergewichte-unterstuetzen-Virtualisierung-mit-KVM-1245044.html.

die Zusammensetzung der Fragmente menschlich erfassbar wird.[1508] Für die Backups, beispielsweise über Spiegelrechenzentren, sollte nach dem gleichen Muster verfahren werden.

Angreifer können durch die Aufteilung bei einer Kompromittierung eines einzelnen physischen Servers den Informationsgehalt nicht ersehen, so dass der Angriff im Optimalfall ins Leere geht. Einzelne Fragmente sind bei einer ausreichenden Aufspaltung für einen Angreifer nutzlos.

Dateisysteme in Cloudsystemen sollten außerdem möglichst proprietär sein, so dass bereits deswegen ein Angriff erschwert wird, weil ein Angreifer die Daten nur mit erhöhtem Aufwand lesen und kopieren kann.[1509]

Durch die Verteilung und Replizierung wird außerdem das Risiko eines Datenverlusts minimiert.[1510] Fallen Server aus oder werden Fragmente gelöscht, sind diese im Zweifel auf anderen Servern vorhanden, so dass die Information zur Verfügung steht und damit primär die Datenintegrität erhalten bleibt. Der Gestaltungsvorschlag ergibt sich demnach unmittelbar aus dem Gestaltungsziel des Aufbaus von Redundanzen (Z16).

Die dem Cloudgedanken folgende Verteilung der Daten aus ökonomischen Gründen, nämlich die Idee der optimalen Ausnutzung von Ressourcen, führt somit dazu, dass die eben genannten Vorteile quasi nebenbei auftreten. Soweit Anbieter eine solche spezielle Auftrennung und Verteilung nicht implementiert haben, beispielsweise indem nur komplette Datensätze mehrfach repliziert werden, ist eine Aufteilung im oben vorgeschlagenen Sinn durch eine Anpassung der Cloudsoftware allerdings schnell und einfach umsetzbar. Bei einer Neuentwicklung einer solchen Software sollte daher auf diesen Aspekt verstärkt geachtet werden, da die Vorteile sowohl ökonomischer, als auch datenschutzrechtlicher und sicherheitsrelevanter Natur sind.

Die Verteilung und Replizierung ist als Soll-Umsetzung zu qualifizieren, die sich bei besonders wichtigen Daten im Sinne einer hohen Integrität und Verfügbarkeit auch zu einer Muss-Umsetzung verdichten kann. Ob die Verteilung und Replizierung empfohlen oder zwingend ist, ist damit vom Einzelfall und zum Teil sogar vom konkreten Datum abhängig.

[1508] Siehe hierzu auch die Ausführungen im Rahmen der Redundanz in Kap. 3.1.9.9.6.

[1509] So nutzt beispielsweise Google das proprietäre Dateisystem „Google File System“; siehe dazu *Ghemawat/Gobioff/Leung*, The Google File System, http://labs.google.com/papers/gfs.html.

[1510] Siehe hierzu bereits oben Kap. 3.1.9.10.2 und die Problematik der potentiellen und ungewollten Umgehung von datenschutzrechtlichen Übermittlungsvorschriften in Kap. 3.1.9.7.2.

4.6.9 Identifizierung und Authentisierung mittels tauglicher Identifikationsverfahren (G9)

Um den Missbrauch mittels gefälschter oder entwendeter Bestandsdaten zu unterbinden, müssen die vom Nutzer übermittelten Daten überprüft werden. In Deutschland kämen beispielsweise das Postidentverfahren, die Nutzung des neuen digitalen Personalausweises, De-Mail (De-Ident) oder eine Kombination von SMS und Onlineüberprüfung in Betracht. Schwierig wird dieses Erfordernis im internationalen Kontext, da solche staatenübergreifenden Verfahren und Identitätssicherungsinfrastrukturen, zum Beispiel Public-Key-Infrastrukturen, nicht existieren. Nicht zuletzt deshalb werden oft noch Kreditkartendaten verwendet, da diese international anerkannt und einsetzbar sind und vergleichsweise sicher den echten Kreditkartennutzer ausweisen.

Eine moderne und international umsetzbare Methode wäre das sogenannte „Web of Trust“, das digitale Signaturen und die gegen- und wechselseitige Bestätigung der Echtheit der Signatur und der Zuordnung zum Inhalt hat. In der Praxis wird dieses Verfahren für die Verschlüsselungssoftware PGP und GnuPG verwendet. Der Nachteil ist, ebenso wie bei Public-Key-Verfahren, dass eine Infrastruktur aufgebaut werden muss und zudem ein gewisser Vorlauf an Transaktionen und vor allem ein möglichst großer Pool an Nutzern vorhanden sein muss, damit die gegenseitige, auf Vertrauen gestützte, Bestätigung der Identität möglich ist. Hinzukommt, dass diese Erfahrungsbildung möglichst durch persönliche Treffen oder Telefonanrufe erfolgen sollte, so dass im Prinzip das Problem der sicheren Identifizierung und Authentisierung nur verschoben wird.

Die Identifizierungserfordernisse erschweren zwar die flexible Nutzungsmöglichkeit der Cloudservices, sind aber für eine Verhinderung des Missbrauchs und vor allem die Möglichkeit der Aufklärung und Sanktionierung essentiell. Trotz der Schwierigkeiten der praktischen Umsetzung ist die Identifizierung somit als zwingend anzusehen.

Der Gestaltungsvorschlag ist unmittelbar aus dem Ziel der sicheren Authentisierung (Z6) abzuleiten.

4.6.10 Nutzung von geeigneten und erprobten Zugriffs- und Identitätsmanagementsystemen (G10)

Mindestens genauso wichtig wie der erstmalige Identifikationsprozess ist das Identitätsmanagement im späteren Einsatz, also die Verwaltung von Identitäten. Nur mit einem sicheren Identitätsmanagement ist in einem zweiten Schritt ein sicheres Zugriffsmanagement realisierbar. Vorgefertigte Managementsysteme sind zwingend auf den jeweiligen Einsatzbereich beim Cloudprovider anzupassen.

Vom Identitätsmanagement sollten auch Anonymisierungen und Pseudonymisierungen umfasst sein, soweit solche wünschenswert oder zumutbar ist. Für

Cloudnutzer sollte nach Möglichkeit das Single-Sign-On-Verfahren genutzt werden, wenn mehrere Services genutzt werden.

Dem Gestaltungsvorschlag liegt das Gestaltungsziel der Nutzung von Identitäts- und Zugriffsmanagementsystemen (Z5) zugrunde. Die prinzipielle Nutzung und Umsetzung ist zwingend, während bei der konkreten Ausgestaltung gewisse Spielräume bestehen.

4.6.11 Bereitstellung von Steuerungs- und Monitoringoberflächen und Data Tracking Tools (G11)

Aus den Gestaltungszielen Z2, Z7 und Z8 ergibt sich der, an den Cloudprovider gerichtete, Gestaltungsvorschlag der Bereitstellung von Schnittstellen zur Steuerung der Dienste durch die Kunden. Diese müssen nicht nur auf die gebuchten Dienste Einfluss nehmen können, sondern auch darauf, ob und wie Subunternehmen für die Dienstebereitstellung herangezogen werden dürfen.

Die Steuerung erfolgt in der Regel unmittelbar über den Browser, also über Webinterfaces oder Schnittstellen und APIs, die von den Kunden mittels auf Clients installierter Software oder Smartphoneapps genutzt werden können.[1511] Diese sind faktisch Management Interfaces im Kleinformat und auf die jeweils gebuchten Dienste der Einzelnutzer begrenzt.

Ein besonderer Aspekt der Transparenz und Überprüfbarkeit ist die Bereitstellung von Statusanzeigen und Monitoringmöglichkeiten. Erst die Information der Nutzer über den Zustand der Services erlaubt die gezielte und erfolgversprechende Steuerung durch reaktive Eingriffe, zum Beispiel bei einem Sicherheitsvorfall (sogenanntes Security Incident Management).[1512] Letzteres trifft aber primär den Cloudprovider, da dieser viel effektiver auf Sicherheitsvorfälle reagieren kann. Neben providerseitigen IDS/IPS-Systemen[1513] sollte auch der Nutzer in die Lage versetzt werden, beim Erkennen von unmittelbar ansetzenden Bedrohungen sofort Administratoren oder sonstiges Personal des Providers in Kenntnis zu setzen. Dies kann sowohl über die Steuerungsschnittstelle webbasiert, per E-Mail oder sogar über eine Telefonhotline ermöglicht werden.

[1511] Ähnlich auch *Essoh/Doubrava/Münch* 2011, 41.

[1512] Amazon nennt seine detaillierte Monitoringlösung „CloudWatch“, Microsoft hingegen „Service Health Dashboard“, wobei beide Dienste nur für registrierte Kunden zur Verfügung stehen; siehe dazu *Amazon*, CloudWatch, http://aws.amazon.com/cloudwatch und *Microsoft*, Service Health Dashboard, https://health.emea.microsoftonline.com; Amazons Service Health Dashboard ist dagegen öffentlich verfügbar; siehe *Amazon*, Service Health Dashboard, http://status.aws.amazon.com; zum Security Incident Management siehe auch *Essoh/Doubrava/Münch* 2011, 42 ff.

[1513] Zu den Begriffen siehe auch oben Kap. 3.1.9.3.2.4.

Manche Anbieter stellen bestimmte Statusinformationen, beispielsweise über die Verfügbarkeit der Dienste, für die Allgemeinheit im Netz bereit.[1514] Nicht selten ist diese Form der Information als Werbeargument für den jeweiligen Clouddienst zu verstehen.

Die Monitoringoberflächen haben zudem für die SLAs Bedeutung, da über diese die Einhaltung der vereinbarten Dienstgüte oder Verfügbarkeit ermöglicht wird.[1515] Nicht zuletzt sollten über diese Oberflächen und Steuerungsschnittstellen auch die Protokolle und Logs, beispielsweise über erfolgreiche Löschungen, eingesehen und ausgewertet werden können. Notwendige Software und Hilfsmittel sind durch den Cloudprovider bereitzustellen.

Um dem Nutzer im Sinne von Transparenz und Beherrschbarkeit effektive Mittel an die Hand zu geben, bietet es sich außerdem an, die, zum Teil weltweite, Verschiebung der Daten durch Data Tracking Tools in Echtzeit und nachträglich verfolgbar zu machen.[1516] Da der Provider ohnehin in der Lage ist, die Vorgänge in seiner Cloud nachzuvollziehen und zu steuern, wäre es ein leichtes diese Informationen in Echtzeit an die Kunden weiterzugeben. So können diese steuernd eingreifen und vorher festgelegte Restriktionen, beispielsweise hinsichtlich eines zu nutzenden Territoriums oder Hoheitsgebiets, selbst überprüfen.

Alle diese Möglichkeiten der Einflussnahme sind keine optionalen Serviceleistungen, die auf dem Good-will des Providers basieren, sondern gewissermaßen zwingende Voraussetzung, um gerade bei der Auftragsdatenverarbeitung dem Leitsatz der „Herrschaft über die Datenverarbeitung“ durch den Kunden als verantwortlichem Auftraggeber größtmögliche Geltung zu verschaffen.

4.7 KORA-Methode als disziplinenübergreifende Methode im Cloud-Computing-Kontext

Die Anwendung der KORA-Methode führte nicht nur zur Formulierung von konkreten technischen Gestaltungsvorschlägen, sie ermöglichte auch eine zielführende und schlüssige Zusammenführung der zuvor nur lose zusammenhängenden Inhalte. Bei ihrer Anwendung fiel außerdem auf, dass wichtige IT-Schutzziele aus rechtlichen Anforderungen abgeleitete Kriterien für sicheres Cloud Computing darstellen. Eine vollkommene und vollständige Verbindung der IT-Schutzziele mit der KORA-Methode scheitert allerdings an der jeweils spezifischen Technik, auf die die Methode angewendet wird. Obwohl faktisch alle IT-Schutzziele in Teilbereichen auch

---

[1514] Siehe dazu *Amazon*, Service Health Dashboard, http://status.aws.amazon.com, *Salesforce*, Service Performance History, http://trust.salesforce.com/trust/status und *Google*, Apps Status Dashboard, http://www.google.com/appsstatus.

[1515] Siehe dazu auch die Ausführungen zum Service Monitoring und Service Level Management in Kap. 3.5.3.2.4.

[1516] So auch *Schneider*, IT-Grundschutz 2010, 12.

auf Cloud Computing als IT-System anwendbar sind, sind diese jedoch nicht alle als rechtliche Kriterien ableitbar. Allenfalls kann man diese mittelbar in das Kriterium der Techniksicherheit hineinlesen. Die Herausstellung einiger Schutzziele, zum Beispiel der Vertraulichkeit, ergab sich aus der Hervorhebung der Anforderungen „Datenschutz“ und „Schutz von Geheimnissen“ als zentrale Probleme der Cloudtechnologie.

Eine Verbindung der Disziplinen ist mit der Methode immer nur soweit möglich, wie es die konkret zu bewertende Technik und die rechtlichen Vorgaben zulassen. Die Konkretisierung erfolgt also nicht nur hinsichtlich der Gestaltungsvorschläge, sondern lenkt insbesondere den Blick auf die rechtlich problematischen und damit mittelbar auch auf die sozialen Anforderungen an ein konkretes Techniksystem. Es wird, bildlich gesprochen, „der Finger auf die wunden Punkte“ einer Technik gelegt. Diese Konzentration auf die problematischen Aspekte einer Technik führt letztlich dazu, dass die konkreten Gestaltungsvorschläge eine deutlich verbesserte, rechtlich verträglichere und sozial adäquatere Technik hervorbringen.

5 Schlussbetrachtungen

5.1 Zusammenfassung der Erkenntnisse und Ergebnisse

Die Untersuchung hat eine Vielzahl von neuen Erkenntnissen geliefert. Diese beschränken sich nicht nur auf Erkenntnisse rechtlicher Art, sondern sind, wie die Herangehensweise erwarten lässt, interdisziplinär. Dabei wurden technische und rechtliche Gesichtspunkte nicht nur unabhängig voneinander dargestellt, sondern auch der Zusammenhang zwischen den Disziplinen in Form der KORA-Methode erforscht und aufgezeigt. Diese Forschungen mündeten im Ergebnis in technischen Gestaltungszielen und ausgewählten technischen Gestaltungsvorschlägen.

Den Untersuchungsgegenstand Cloud Computing betreffend wurde festgestellt, dass die Beschreibung und Definition der NIST mit ihren Merkmalen und Eigenschaften mittlerweile als vorzugswürdig angesehen wird, um Cloud Computing zu beschreiben, zu klassifizieren und letztlich zu definieren. Die dargestellten Schichten- und Nutzungsmodelle sind hingegen schon seit längerem anerkannt. Ebenso ist unstreitig, dass Cloud Computing nicht über Nacht entstanden ist, sondern sich aus unterschiedlichen Vorläufermodellen und dem Umstand der Durchsetzung flächendeckender Breitbandinternetzugänge entwickelt hat.

Eine weitere konsensfähige Erkenntnis ist die Einordnung des Cloud Computing als Geschäftsmodell und Technologie. Dessen Dienstleistungscharakter wird die Bereitstellung und Nutzung von IT-Leistungen nachhaltig verändern und zu einem Paradigmenwechsel, vergleichbar mit den Auswirkungen der Elektrifizierung, führen.

Cloud Computing bietet überwiegend Vorteile, insbesondere für den Cloudanbieter und den Cloudnutzer. Die Nachteile äußern sich dagegen meist bei den von der Datenverarbeitung Betroffenen, beispielsweise indem Daten in Staaten ohne angemessenes Datenschutzniveau transferiert werden. Nachteile für den Cloudnutzer sind mögliche Lock-In-Effekte und die damit einhergehende zwangsweise Bindung an einen Anbieter. Eine solche kann allerdings durch offene Standards umgangen werden kann.

Die Sicherheit der Daten und Systeme ist für Cloud Computing ein zentraler Faktor. Ohne Sicherheit und Schutz der Daten kann das Geschäftsmodell nicht funktionieren. Absolute Sicherheit ist allerdings nie erreichbar, jedoch ist in der Regel das Sicherheitsniveau höher, als bei bereits bestehenden In-House-Lösungen. Stichworte in diesem Zusammenhang sind Fragmentierung und Redundanz der vorgehaltenen Daten und ein höheres Sicherheitsknow-how der beim Cloudanbieter Beschäftigten. Insbesondere die Komplexität ist durch geschulte Mitarbeiter besser zu bewältigen. Die Komplexität von IT-Systemen hat aber nicht nur negative Aus-

wirkungen, sondern kann unter Umständen Angriffe erschweren oder gänzlich verhindern.

Im Rahmen der Untersuchung wurden die relevanten Bedrohungen ermittelt und praxistaugliche Sicherheitsmaßnahmen formuliert, die für ein konkretes Sicherheitskonzept bei einem Anbieter berücksichtigt werden können. Eine weitere wesentliche Erkenntnis war die Klassifizierung der IT-Schutzziele, wobei deren Bedeutung für konkrete Sicherheitsmaßnahmen und die technische Gestaltung deutlich wurde.

Es wurde zudem geprüft, ob Cloud Computing bereits als kritische Infrastruktur eingeordnet werden kann. Eine solche Kritikalität ist im Jahr 2012 noch nicht anzunehmen, jedoch wird eine solche beim Eintreffen der Wachstumsprognosen nur eine Frage der Zeit sein.

Die Prüfung und Darstellung der Rechtslage ergab vielfältige Probleme des Cloud Computing mit geltendem Recht, namentlich dem Datenschutzrecht. So sind außereuropäische Clouds nur schwer mit deutschem und europäischem Datenschutzrecht in Einklang zu bringen, so dass als Lösung rein innereuropäische Cloudangebote vorzugswürdig sind. Insbesondere ist Auftragsdatenverarbeitung in außereuropäischen Clouds nicht möglich.

Die Übermittlung in unsichere Drittstaaten ist nur ausnahmsweise erlaubt, wobei die Ausnahmetatbestände nur sehr selten eingreifen. In der Regel ist es auch nicht erforderlich, auf außereuropäische Anbieter zurückzugreifen, so dass es oft schon an der Erforderlichkeit für eine außereuropäische Übermittlung mangelt. Eine solche liegt auch faktisch nie im Interesse des Betroffenen.

Im Hinblick auf EU-Recht bestehen auch gewisse Umsetzungsprobleme, wenn Daten in sichere Drittstaaten übermittelt werden sollen. Hierbei differenziert das nationale Recht nicht ausreichend zwischen solchen Staaten mit und ohne ausreichendem Datenschutzniveau. Ähnliche Umsetzungsprobleme bestehen bei Auslagerungsketten mittels Subunternehmen. Während die Datenschutzrichtlinie die sogenannte „Joint Controllership“ anerkennt, ist eine solche dem deutschen Datenschutzrecht unbekannt.

Nur über die Nutzung der neuen EU-Standardvertragsklauseln sind solche Auslagerungsketten rechtskonform umsetzbar. Allerdings besteht auch in diesem Zusammenhang eine Vielzahl von Auffassungen. Während manche die Klauseln einerseits sogar als Legitimationsgrundlage für eine außereuropäische Auftragsdatenverarbeitung heranziehen möchten, sind andererseits manche Datenschutzaufsichtsbehörden der Meinung, dass auch die Nutzung von Standardvertragsklauseln die Pflichten aus § 11 BDSG auslösen, ohne jedoch die entsprechenden Rechte, namentlich die Privilegierung des Auftragnehmers, vorzusehen.

Nicht zuletzt bei der Darstellung dieser Rechte und Pflichten im Rahmen der Auftragsdatenverarbeitung gemäß § 11 BDSG wurde deutlich, dass die vertraglichen Vereinbarungen zwischen Auftraggeber und Auftragnehmer, also zwischen Cloudnutzer und Cloudanbieter, erhebliche Bedeutung haben. Als weiterer vertragsrechtsrelevanter Aspekt der Forschungsarbeit wurden regelungsbedürftige Punkte bei der vertraglichen Gestaltung mit Hilfe von Service Level Agreements (SLAs) aufgezeigt.

Im Rahmen der Prüfung von § 9 BDSG und der Anlage zu Abs. 1 ergaben sich keine rechtlichen Besonderheiten. Die zu treffenden Sicherheitsmaßnahmen gelten auch im Rahmen von Cloud Computing. Allenfalls die wortgetreue Umsetzung von manchen Maßnahmen erweist sich bei Cloud Computing als problematisch. Allerdings zeigt das Beispiel der Zutrittskontrolle, dass der Gesetzgeber bei der praktischen Umsetzung dieser Maßnahme flexibel ist und Audits und Zertifizierungen als ausreichend ansieht. Insofern war es auch nur konsequent den § 9a ins BDSG aufzunehmen. Die damit zusammenhängenden Zertifizierungsstandards wurden im Rahmen der Arbeit kurz vorgestellt und deren aktuelle und künftige Bedeutung für Cloud Computing hervorgehoben.

Außerdem wurden die wesentlichen Compliancevorschriften und Vorschriften des internationalen Privatrechts dargestellt und im Zusammenhang mit Cloud Computing erläutert. Urheberrechtliche Regelungen sind im Prinzip nur für den Cloudprovider von Bedeutung, so dass klassisches Softwarelizenzmanagement mit Cloud Computing bedeutungslos wird. Hingegen wird Kartellrecht und die Entwicklung von marktbeherrschenden Stellungen von Cloudprovidern immer mehr an Bedeutung gewinnen.

Weitgehend ungelöst sind Rechtsfragen, die sich durch die Kollision von europäischem Recht mit US-Recht, insbesondere dem PATRIOT Act und E-Discovery-Vorschriften, ergeben. Diese führen zu sich widersprechenden Anforderungen an US-Unternehmen, die auch in Europa agieren und mit personenbezogenen Daten umgehen. Diese Widersprüche sind nur auf politischer Ebene lösbar, beispielsweise indem sich die Vereinigten Staaten verpflichten, auf EU-Territorium europäisches Recht zu beachten. In diesem Zusammenhang ist auch auf die unterbreiteten Vorschläge zur rechtlichen Gestaltung und auf die neueren Gesetzesinitiativen, insbesondere die geplante Datenschutzverordnung, hinzuweisen.

Eine weitere wesentliche Erkenntnis, die sich bei der Anwendung der KORA-Methode ergab, ist die, dass die Beherrschbarkeit von Clouds im Vergleich zum Status quo verbessert werden kann. Insbesondere Data Tracking Tools, regelbasiertes und intelligentes Load Balancing und intelligente neue Algorithmen sind bereits heute schon implementierbar. Gleiches gilt für die Auswahl der Subunternehmen nach gewissen Nutzervorgaben.

Andererseits zeigt die Befassung mit Gestaltungszielen und Gestaltungsvorschlägen, dass die Problematik der Verarbeitung und der notwendigen Entschlüsselung zuvor verschlüsselter Daten noch ungelöst ist. Homomorphe Verschlüsselungsmethoden könnten künftig eine Lösung hierfür sein.

Zusammengefasst ist festzuhalten, dass das anfängliche „Chaos“ im Zusammenhang mit der neuen Cloudtechnologie geordnet und durch rechtliche und gestaltungstechnische Eingriffe reguliert werden kann, ohne jedoch dabei das Grundkonzept der Elastizität zu zerstören. Insgesamt ist ein Kompromiss zwischen Flexibilität und Effizienz einerseits und Kontrollierbarkeit andererseits notwendig. Die verbesserte Beherrschbarkeit hat auch unmittelbare Bedeutung für die Sicherheit, da Komplexität und chaotisches Verhalten eingedämmt werden und dadurch Fehler und Sicherheitslücken minimiert werden.

Chaos ist allerdings nicht immer nur negativ zu bewerten, wie das Beispiel „Chaos Monkey“ gezeigt hat. Erfahrungsbildung in chaotischen Situationen und der adäquate Umgang mit unvorhergesehenen Situationen kann geübt werden. Die Technik ist demnach nicht nur rechts- und sozialverträglich zu gestalten, auch der Umgang mit der Technik kann durch technisch unterstützte Maßnahmen verbessert werden.

5.2 Ausblick und künftiger Forschungsbedarf

Angesichts der Neuheit von Cloud Computing bleibt auch künftig noch Raum für weitere Forschungen. Die hier gefundenen Ergebnisse können daher als Einstieg in intensivere Forschungsvorhaben gewertet werden. Während die Arbeit einen generellen Überblick über Cloud Computing und die drängendsten faktischen und rechtlichen Probleme bietet, können künftige Forschungsvorhaben Teile hiervon intensiver und näher beleuchten. Gerade die technische Weiterentwicklung und die kontinuierliche Fortentwicklung des Rechts, insbesondere des Datenschutzrechts, lassen Raum für vielfältige künftige Forschungsprojekte. Vor allem die Bestrebungen eines möglichst weltweiten und einheitlichen Datenschutzniveaus, vergleichbar zum relativ gleichförmigen Schutzniveau im Urheberrecht, werden gerade für Cloud Computing erhebliche Bedeutung erlangen. Es ist zudem absehbar, dass mittelfristig das nationale und europäische Datenschutzrecht, das sich zurzeit am technischen Stand der 70er Jahre des vorigen Jahrhunderts orientiert, nicht zuletzt durch die geplante Datenschutzverordnung auf EU-Ebene, an die aktuellen technischen Gegebenheiten angepasst werden wird. Diese Anpassung ist wissenschaftlich zu begleiten und zu erforschen.

Die Mehrzahl der künftigen Entwicklungen im Bereich „Internet“ werden einen irgendwie gearteten Bezug zu Cloud Computing haben. Auch Ubiquitous Computing ist ohne die Ressourcen aus der Cloud nur eingeschränkt umsetzbar. Speicherung, Berechnung und Aufbereitung der Daten aus den Kleinstgeräten und Sensoren werden künftig extern in Clouds erfolgen und Anwendungen und Applikationen

erlauben, die – wegen den begrenzten Kapazitäten der bisher genutzten Hardware – noch gar nicht vorstellbar sind.

Die weitgehende Durchsetzung von Cloud Computing im Alltag und in immer mehr Lebensbereichen wird eine Vielzahl von neuen technischen, rechtlichen, aber auch sozialen Forschungsansätzen hervorbringen.[1517] Nicht zuletzt die bisher nur vergleichsweise unbefriedigenden Lösungen mittels Verschlüsselung werden die IT-Sicherheitsforschung noch intensiv beschäftigen.

Zur Selbstdurchsetzung des Datenschutzes gehört auch die Idee, dass Daten automatisiert und ohne Zutun des Nutzers nach Ablauf einer vorgegebenen Zeit gelöscht werden („Recht auf Vergessen“).[1518] Gerade die vielfältige Spiegelung und weitläufige Verteilung[1519] von Daten und Datenfragmenten bei Cloud Computing birgt die Gefahr, dass die Daten oftmals nicht richtig gelöscht werden und nach einer gewissen Zeit eine Löschung mangels Überblickbarkeit durch den Cloudprovider oder den Nutzer aufgrund der Volatilität der Geschäftsbeziehungen des Providers mit Subunternehmen, aber auch durch die flexible Inanspruchnahme durch die Cloudnutzer, überhaupt nicht mehr oder nur mit erheblichem Aufwand möglich ist. Effektive Löschkonzepte, aber auch sichere Archivierungsmaßnahmen bis zur Durchführung der Löschung, werden daher künftig immer größere Bedeutung erlangen und dementsprechend den Forschungsbedarf erhöhen.

Neben der Frage der technischen Machbarkeit müsste vorab sozialwissenschaftlich geklärt werden, wie solche Löschfristen festgelegt werden sollten. Nicht jedes Datum ist gleich sensitiv. Auch der Zusammenhang und mögliches Spezialwissen sind für eine solche Bewertung relevant. Zeitliche Änderungen und Veränderungen der Umstände lassen Informationen auch in einem anderen Licht erscheinen. Es müssten also Kriterien für eine solche zeitliche Befristung entwickelt werden. Diese Forschungen hätten auch Bezug zum Recht, da die so gefundenen potentiellen zeitlichen Befristungen auch rechtlich vorgegeben und abgesichert werden könnten.

[1517] Zu Letzteren siehe beispielsweise die Frage der Veränderung des menschlichen Denkens durch Internetdienste, insbesondere Suchmaschinen, und die Externalisierung von Wissen ohne bisherige Limitierungen; siehe dazu *Bohannon*, Searching for the Google Effect on People's Memory, http://www.sciencemag.org/content/333/6040/277 und *Schirrmacher*, Wir brauchen eine europäische Suchmaschine, http://www.faz.net/artikel/C30833/digitales-gedaechtnis-wir-brauchen-eine-europaeische-suchmaschine-30468036.html.

[1518] *Biermann/Mayer-Schönberger*, Das Netz soll auch vergessen, http://www.zeit.de/online/2008/15/datenschutz-mayer-schoenberger; *Polke-Majewski*, Kein Vergeben, kein Vergessen, http://www.zeit.de/2011/15/Internet-Gedaechtnis; ein solches „Recht auf Vergessen (werden)“ ist auch im Entwurf einer Datenschutzverordnung in Art. 15 angedacht.

[1519] Im Jahr 2008 haben Unternehmensserver weltweit 9,57 Zettabyte an Daten verarbeitet, wobei der größte Teil durchlaufende Daten waren; *Graham*, Business Information Consumption: 9,570,000,000,000,000,000,000 Bytes per Year http://ucsdnews.ucsd.edu/newsrel/general/04-05BusinessInformation.asp; *Kremp*, Ein Bücherstapel bis Alpha Centauri, http://www.spiegel.de/netzwelt/web/0,1518,756215,00.html.

Sozialwissenschaftlich ist aber vor allem der Einfluss des Cloud Computing auf die Gesellschaft zu erforschen. Die Technologie hat das Potential, die Gesellschaft nachhaltig zu verändern. Insbesondere in Verbindung mit Ubiquitous und Pervasive Computing ergeben sich erhebliche Folgen für das Zusammenleben der Menschen.

Auch zur immer weitergehenden Abstraktion von physischen Gegebenheiten und die Nutzung von mehreren virtuellen Abstraktionsschichten, mit dem Ziel der Zusammenführung zu wenigen virtuellen und logischen Geräten, sind noch erhebliche Forschungsanstrengungen notwendig. Die bestehende Virtualisierung und die Modellrestrukturierung von Rechenzentren und deren Arbeitsweisen sind dabei ein Anfang. Letztlich wird Cloud Computing gemeinsam mit bereits absehbaren Folge- und Paralleltechnologien, wie Mobile, Ubiquitous und Pervasive Computing die Fundamente und Arbeitsweise des Internets, wie wir es heute kennen, umgestalten und immer tiefer in der Lebenswirklichkeit des Einzelnen integrieren. Die virtuelle Welt des Internet wird mit der realen Welt durch das sogenannte „Internet der Dinge“ kombiniert werden.

Cloud Computing befindet sich als Technologie und Geschäftsmodell noch in einem sehr frühen Entwicklungsstadium, so dass sich, nicht zuletzt durch (betriebs)wirtschaftliche Forschungen und Beobachtungen, sowohl für die Nutzer, als auch die Anbieter mit der Zeit Änderungen ergeben werden. Insbesondere werden sich Angebot und Nachfrage anpassen. Damit ist nicht nur der Markt des Cloud Computing gemeint, sondern auch die konkrete Ausgestaltung der Angebote. Während zurzeit Nutzer kaum auf die Angebote Einfluss nehmen können, wird sich dieses Manko bei einem gesunden Wettbewerb und offenen Standards mit der Zeit ändern. Wettbewerbs- und kartellrechtliche Forschungen und Marktbeobachtungen können dabei frühzeitig verhindern, dass Monopole oder Oligopole entstehen, die eine solche verbraucher- und nutzerfreundliche Entwicklung hemmen könnten.

Letztlich können durch dieses Anpassen an die Kundenwünsche und die entsprechenden Forschungen auch die IT-Sicherheits- und Datenschutzprobleme gelöst oder zumindest reduziert werden. Erste, rechtlich untermauerte, Lösungsansätze wurden mit dieser Forschungsarbeit unterbreitet.

Anlage

Anwendung der KORA-Methode auf Cloud Computing

Anforderungen (A) ergeben sich aus den grundrechtlichen Vorgaben

Datenschutz (A1)	Informationelle Selbstbestimmung
Geheimnisschutz (A2)	Art. 12, 14 GG, „Computergrundrecht“, Art. 10 GG
Kontrollmöglichkeit (A3)	Art. 20 Abs. 2 S. 2, Abs. 3, Art. 28 Abs. 1 S. 1, Art. 19 Abs. 3 GG

Kriterien (K) ergeben sich aus den Anforderungen (A)

Techniksicherheit (K1)	Datenschutz (A1) und Geheimnisschutz (A2)
Vertraulichkeit (K2)	Datenschutz (A1) und Geheimnisschutz (A2)
Transparenz (K3)	Datenschutz (A1) und Kontrollmöglichkeit (A3)
Entscheidungsfreiheit (K4)	Datenschutz (A1)
Erforderlichkeit (K5)	Datenschutz (A1) und Kontrollmöglichkeit (A3)
Zweckbindung (K6)	Datenschutz (A1)
Trennbarkeit (K7)	Datenschutz (A1), Geheimnisschutz (A2) und Kontrollmöglichkeit (A3)
Beherrschbarkeit und Steuerungsfähigkeit (K8)	Kontrollmöglichkeit (A3), Datenschutz (A1) und Geheimnisschutz (A2)
Überprüfbarkeit (K9)	Kontrollmöglichkeit (A3), Datenschutz (A1) und Geheimnisschutz (A2)
Beweissicherung (K10)	Kontrollmöglichkeit (A3)
Integrität (K11)	Datenschutz (A1) und Geheimnisschutz (A2)
Verfügbarkeit (K12)	Kontrollmöglichkeit (A3)

Gestaltungsziele (Z) ergeben sich aus den Kriterien (K)

Verschlüsselung von Daten und Datenträgern (Z1)	K2
Etablierung eines umfassenden Management Interfaces (Z2)	K8
Sicherung des Interfaces durch Zugriffsschutzverfahren (Z3)	K1, K2 und K8
Etablierung und technische Umsetzung des Vieraugenprinzips (Z4)	K7, K2, K8 und K1
Nutzung von Identitäts- und Zugriffsmanagementsystemen (Z5)	K7, K2, K8 und K1
Sichere Authentisierung (Z6)	K1, K10 und K8
Trennung des Nutzertraffics vom administrativen Datenverkehr (Z7)	K7, K6, K8, K11 und K1
Trennung der virtuellen Nutzersysteme durch sichere Hypervisoren (Z8)	K7, K6, K8, K11 und K1
Implementierung von Dokumentationsfunktionen (Z9)	K9, K10 und K3
Keine Weitergabe von administrativen Protokollen (Z10)	K2, K7, K6, K8 und K1
Kein Zugriff des Providers auf Protokollinhalte der Nutzer (Z11)	K2, K7, K6, K8, K1 und K4
Sicherung der Protokolldaten durch Zugriffsschutzverfahren (Z12)	K1, K2 und K8
Sichere Löschung der Protokolldaten (Z13)	K5, K6, K4, K2 und K8
Sichere Löschung sonstiger Daten (Z14)	K5, K6, K4, K2 und K8
Bestätigung der Löschung von Daten bei Subunternehmen (Z15)	K8, K3 und K9
Aufbau von Redundanzen (Z16)	K11, K12, K1, K10 und K8
Nutzung von Fehlerkorrekturverfahren und Hashwerten (Z17)	K11, K12, K9, K8 und K10
Technisch unterstützte Auswahl von Subunternehmen (Z18)	K8, K3, K6 und K4
Regelbasiertes Load Balancing (Z19)	K8, K3 und K7
Etablierung und Nutzung standardisierter Schnittstellen und APIs (Z20)	K12, K8, K3 und K4
Abstraktion und Zusammenfassung zu logischen Geräten (Z21)	K8 und K1

Gestaltungsvorschläge (G) ergeben sich aus den Gestaltungszielen (Z)

Verschlüsselung der beim Datentransport übermittelten Daten (G1)	Z1
Verschlüsselung während der Speicherung (G2)	Z1
Sichere Schlüssel- und Passwortverwaltung (G3)	Z1, Z3, Z4, Z5
Trennung von Schlüsseln und Daten (G4)	Z1, Z5, Z8
Nutzung von homomorphen Verschlüsselungsalgorithmen (G5)	Z1
Trennung der verarbeitenden Rechner während der Verarbeitung (G6)	Z7
Einsatz von bewährten und gehärteten Hypervisoren (G7)	Z8
Verteilung und Replizierung der Daten auf mehrere physische Server (G8)	Z16
Identifizierung und Authentisierung mittels Identifikationsverfahren (G9)	Z6
Nutzung von geeigneten und erprobten Zugriffs- und Identitätsmanagementsystemen (G10)	Z5
Bereitstellung von Monitoringoberflächen und Data Tracking Tools (G11)	Z2, Z7, Z8

Literaturverzeichnis

Abel, R., in: Roßnagel, A., Handbuch Datenschutzrecht – Die Grundlagen für Wirtschaft und Verwaltung, München, 2003.

Ahlberg, H., in: Möhring, P./Nicolini, K., Kommentar zum Urheberrechtsgesetz, München, 2000.

Ambs, F., in: Erbs, G./Kohlhaas, M./Ambs, F., Strafrechtliche Nebengesetze, München 2011.

Armbrust, M./Fox, A./Griffith, R./Joseph, A./Katz, R./Konwinksi, A./Lee, G./Patterson, D./Rabkin, A./Stoica, I./Zaharia, M., Above the Clouds: A Berkeley View of Cloud Computing, 2009, http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

Austinat, R./Fechteler, P./Gieselmann, H., Über den Wolken – Wie Cloud Gaming den Spielemarkt revolutioniert, c't 21/2010, 76.

Baun, C./Kunze, M./Ludwig, T., Servervirtualisierung, Informatik Spektrum, 2009, 197.

Baun, C./Kunze, M., Wolkige Zeiten, iX Special 2/2010, 40.

Baun, C./Kunze, M./Nimis, J./Tai, S., Cloud Computing: Web-basierte dynamische IT-Services (Informatik Im Fokus), Berlin, Heidelberg, 2009.

Becker, J., in: Bamberger, H./Roth, H., Beck'scher Onlinekommentar zum BGB, Edition 18, Stand: 1.2.2007.

Beckereit, F./Frei, A./Koch, F./Meyer, N./Schaupp, D./Stedler, P./Walther, M., BITKOM-Leitfaden Server-Virtualisierung, Teil 2: Design, Deployment und Betrieb, Revision 3, 2009, http://www.bitkom.org/files/documents/virtualisierung_nov_2009_T2.pdf.

Beckereit, F./Harrer, T./Koch, F./Schaupp, D./Skurk, H./Stedler, P./Walther, M./Wilde, H., BITKOM-Leitfaden Server-Virtualisierung, Teil 1: Businessgrundlagen, Revision 3, 2009, http://www.bitkom.org/files/documents/virtualisierung_nov_2009_T1.pdf.

Bedner, M., „Deep Packet Inspection" – Technologie und rechtliche Initiativen, CR 2010, 339.

Bedner, M./Ackermann, T., Schutzziele der IT-Sicherheit, DuD 2010, 323.

Beilschmidt, L./Bühr, O./Götz, D./Haas, P./Höfner, C./Koll, S./Konowalczyk, T./Konradi, J./Marfording, I./Meents, J./Schweinoch, M./Tews, M., BITKOM-Leitfaden Cloud Computing – Was Entscheider wissen müssen, Kapitel „Vertragliche Regelungen", 2010,

http://www.bitkom.org/files/documents/BITKOM_Leitfaden_Cloud_Computing-Was_Entscheider_wissen_muessen.pdf.

Berl, A./Fischer, A./De Meer, H., Virtualisierung im Future Internet, Informatik Spektrum, 2010, 186.

Bertermann, N., in: Heidrich, J./Forgó, N./Feldmann, T., Heise Online-Recht: Der Leitfaden für Praktiker & Juristen, 2. Ergänzungslieferung 2010, Hannover, 2010.

Bierekoven, C., Lizenzierung in der Cloud, ITRB 2010, 42.

Bieresborn, D., in: Von Wulffen, M., Kommentar zum SGB X, München, 2010.

Birk, D./Wegener, C., Über den Wolken; Cloud Computing im Überblick, DuD 2010, 641.

Birk, D./Heinson, D./Wegener, C., Virtuelle Spurensuche – Digitale Forensik in Cloud-Umgebungen, DuD 2011, 329.

Biskup, J., Security in Computing Systems – Challenges, Approaches and Solutions, Berlin, 2009.

Bizer, J., in: Simitis, S., Bundesdatenschutzgesetz, Baden-Baden, 2006.

Bock, M., in: Beck'scher TKG-Kommentar, München, 2006.

Böken, A., Cloud-Strategien entwickeln und erfolgreich umsetzen – Wege in die Wolke, iX 04/2011, 115, http://www.heise.de/ix/artikel/Wege-in-die-Wolke-1209690.html.

Böken, A., Cloud Computing und Auftragsdatenverarbeitung, http://www.linuxtag.org/2010/fileadmin/www.linuxtag.org/slides/Arnd%20B%C3%B6ken%20-%20Cloud-Computing%20und%20Auftragsdatenverarbeitung.pdf.

Bonk, J., in: Stelkens, P./Bonk, J./Sachs, M., Verwaltungsverfahrensgesetz, München, 2008.

Born, A., Get off my Cloud – Software as a Service im Cloud Computing, iX Special 2/2010, 16.

Bradshaw, S./Millard, C./Walden, I., Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, Social Science Research Network 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374.

Brammsen, J., Wirtschaftsgeheimnisse als Verfassungseigentum – Der Schutz der Betriebs- und Geschäftsgeheimnisse gem. Art. 14 GG, DÖV 2007, 10.

Breuer, R., Schutz von Betriebs- und Geschäftsgeheimnissen im Umweltrecht, NVwZ 1986, 171.

Budszus, J./Heibey, H./Hillenbrand-Beck, R./Polenz, S./Seifert, M./Thiermann, M., Orientierungshilfe – Cloud Computing der Arbeitskreise Technik und Medien der

Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 2011, http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf.

Büllesbach, A./Höss-Löw, P., Vertragslösung, Safe Harbor oder Privacy Code of Conduct, DuD 2001, 135.

Burianski, M./Reindl, M., Truth or Dare? The conflict between e-discovery in international arbitration and german data protection rules, SchiedsVZ 2010, 187.

Burkert, H., in: Roßnagel, A., Handbuch Datenschutzrecht – Die Grundlagen für Wirtschaft und Verwaltung, München, 2003.

von dem Bussche, A., in: Leupold, A./Glossner, S., Münchener Anwaltshandbuch IT-Recht, München, 2011.

Buyya, R./Yeo, C./Venugopal, S., Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities, http://arxiv.org/pdf/0808.3558.

Carr, N., The Big Switch – Der große Wandel – Cloud Computing und die Vernetzung der Welt von Edison bis Google, Heidelberg, München, Landsberg, Frechen, Hamburg, 2009.

Catteddu, D., Security & Resilience in Governmental Clouds – Making an informed decision, ENISA, 2010, http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/at_download/fullReport.

Catteddu, D./Hogben, G., Cloud Computing – Benefits, risks and recommendations for information security, ENISA, 2010, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport.

Chaum, D., Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms, Communications of the ACM, 1981, 84.

Christmann, S./Hilpert, H./Thöne, M./Hagenhoff, S., Datensicherheit und Datenschutz im Cloud Computing – Risiken und Kriterien zur Anbieterauswahl, HMD – Praxis der Wirtschaftsinformatik, Heft 275, 2010, 62.

Cierniak, J., in: Münchner Kommentar zum Strafgesetzbuch, Band 3, München, 2003.

Connolly C., The US Safe Harbor – Fact or Fiction?, 2008, http://www.galexia.com/public/research/articles/research_articles-pa08.html.

Curry, S./Darbyshire, J./Fisher, D./Hartman, B./Herrod, S./Kumar, V./Martins, F./Orrin, S./Wolf, D., Infrastructure Security: Getting to the Bottom of Compliance in the Cloud, 2010, http://www.rsa.com/innovation/docs/CCOM_BRF_0310.pdf.

Däubler, W., in: Däubler, W./Klebe, T./Wedde, P./Weichert, T., Bundesdatenschutzgesetz, Kompaktkommentar zum BDSG, Frankfurt am Main, 2010.

Dammann, U., in: Simitis, S., Bundesdatenschutzgesetz, Baden-Baden, 2011.

Danz, U./Federrath, H./Köhntopp, M./Kritzenberger, H./Ruhl, U., Anonymer und unbeobachtbarer Webzugriff für die Praxis, in: IT-Sicherheit ohne Grenzen? Tagungsband 6. Deutscher IT-Sicherheitskongress des BSI, Ingelheim, 1999, 59. http://www.semper.org/sirene/publ/DFKK_99BSI.pdf.

Deussen, P./Strick, L./Peters, J., Cloud-Computing für die öffentliche Verwaltung, ISPRAT-Studie, Fraunhofer-Institut für Offene Kommunikationssysteme, 2010, http://www.fokus.fraunhofer.de/de/elan/_docs/cloud_studie_vorabversion_20101129.pdf.

von Diemar, U., Cloud Computing – Abschied von der Software-Lizenz, IP Manager 2010, 52.

Diemer, H., in: Erbs, G./Kohlhaas, M./Ambs, F., Strafrechtliche Nebengesetze, München 2011.

Dierstein, R., Sicherheit in der Informationstechnik – der Begriff IT-Sicherheit, Informatik Spektrum 2004, 343.

Dietrich, N., ASP – öffentliche Zugänglichmachung oder unbenannte Nutzungsart?, ZUM 2010, 567.

Digmayer, M., Cloud Computing – vom Hype zur etablierten Technologie, IT-Sicherheit 1/2011, 18.

Dikaikos, M./Pallis, G./Katsaros, D./Mehra, P./Vakali, A., Cloud Computing – Distributed Internet Computing for IT and Scientific Research, IEEE Internet Computing, September/October 2009, 10.

Dorschel, J., IT-Sicherheit und Datenschutz in der Vertragsgestaltung, in: Schartner, P./Weippl, E., D-A-CH Security 2010, Klagenfurt, 2010, 175.

Dreier, T., in: Dreier, T./Schulze, G., Kommentar zum Urheberrechtsgesetz, München, 2008.

Dueck, G., Cloud – über die Wolke des IT-Himmels, Informatik Spektrum 2009, 260.

Duisberg, A., in: Picot, A./Hertz, U./Götz, T., Trust in IT – Wann vertrauen Sie Ihr Geschäft der Internet-Cloud an?, Heidelberg, Dordrecht, London, New York, 2011, 49.

Dustar, S./Gall, H./Hauswirth, M., Software-Architekturen für Verteilte Systeme - Prinzipien, Bausteine und Standardarchitekturen für moderne Software, Berlin, 2003.

Eckert, C., IT-Sicherheit, Konzepte, Verfahren, Protokolle, München, 2006.

Eckhart, J., Rechtliche Grundlagen der IT-Sicherheit, DuD 2008, 330.

Eckhart, J., BDSG: Neuregelungen seit 01.09.2009, DuD 2009, 587.

Eckhart, J., Cloud Computing – ein rechtlicher Überblick, Information Management und Consulting 4/2010, 55.

Eckhart, J./Giebichenstein, R./Helbing, T./Hilber, M./Niemann, F./Weiss, A., Eurocloud Leitfaden Cloud Computing – Recht, Datenschutz & Compliance, 2010, http://www.eurocloud.de/dl/EuroCloud_Leitfaden_RDC.pdf.

Ehmann, E., in: Simitis, S., Bundesdatenschutzgesetz, Baden-Baden, 2011.

Eisenschmid, N., in: Schmidt-Futterer, W., Mietrecht – Großkommentar des Wohn- und Gewerberaummietrechts, München, 2011.

Elbel, T., Zur Abgrenzung von Auftragsdatenverarbeitung und Übermittlung, RDV 2010, 203.

Emmerich, V., in: Dauses, M., Handbuch des EU-Wirtschaftsrechts, München, 2010.

Engels, T., Datenschutz in der Cloud – Ist hierbei immer eine Auftragsdatenverarbeitung anzunehmen?, K&R 2011, 548.

Erd, R., Zehn Jahre Safe Harbor Abkommen – kein Grund zum Feiern, K&R 2010, 624.

Erd, R., Auftragsdatenverarbeitung in sicheren Drittstaaten – Plädoyer für eine Reform von § 3 Abs. 8 Satz 3 BDSG, DuD 2011, 275.

Ernestus, W., in: Simitis, S., Bundesdatenschutzgesetz, Baden-Baden, 2011.

Ernst, S., Social Plugins: Der „Like-Button" als datenschutzrechtliches Problem, NJOZ 2010, 1917.

Essoh, D./Doubrava, C./Münch, I., Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter (Mindestsicherheitsanforderungen in der Informationssicherheit), Bonn, 2011, https://www.bsi.bund.de/DE/Themen/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.html.

von Faber, E., Blackbox Cloud Computing, <kes> Special – Sicheres Cloud Computing, März 2011, 40.

Federrath, H./Pfitzmann, A., Anonymität, Authentizität und Identifizierung im Internet, in: Bartsch, M./Lutterbeck, B., Neues Recht für neue Medien, Informationstechnik und Recht 7, Schriftenreihe der DGRI, Köln, 1998, 319.

Federrath, H./Pfitzmann, A., in: Roßnagel, A., Handbuch Datenschutzrecht – Die Grundlagen für Wirtschaft und Verwaltung, München, 2003.

Fickert, T., Entwicklungen des Cloud Computing im Überblick – Aktuelle und künftige rechtliche Probleme, in: Taeger, J./Wiebe, A., Inside the Cloud – Neue Herausforderungen für das Informationsrecht, Tagungsband Herbstakademie 2009, Edewecht, 2009, 419.

Fischer, H., Der Schaden nach dem Bürgerlichen Gesetzbuche, Jena, 1903.

Fischer, T./Steidle, R., Brauchen wir neue EG-Standardvertragsklauseln für das „Global Outsourcing"?, CR 2009, 632.

Fischinger, P., in: von Staudinger, J., Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, München, 2011.

Foster, I./Kesselman, C., The Grid 2: Blueprint for a New Computing Infrastructure, San Francisco, 2003.

Frankl, P./Hamlet, D./Littlewood, B./Strigini, L., Choosing a testing method to deliver reliability; Proceedings of the 19th international Conference on Software Engineering 1997, New York, 68.

Gabel, D., in: Taeger, J./Gabel, D., Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, Frankfurt, 2010.

Gaul, B./Koehler, L., Mitarbeiterdaten in der Computer Cloud: Datenschutzrechtliche Grenzen des Outsourcing, Betriebsberater 2011, 2229.

Gaulke, M., Prüfung der Einhaltung der technischen und organisatorischen Maßnahmen bei Auftragsdatenverarbeitungen, DuD 2011, 417.

Gaycken, S./Karger, M., Entnetzung statt Vernetzung – Paradigmenwechsel bei der IT-Sicherheit, MMR 2011, 3.

Geercken, K./Holden, K./Rath, M./Surguy, M./Stretton, T., Cross Border E-Discovery – How to manage potential evidence in an international environment, CRi 2010, 65.

Geis, I., eDiscovery und Datenschutz, Hamburg 2008, http://www.ivo-geis.de/veroeffentlichungen/eDiscovery_und_Datenschutz.pdf.

Geis, I., Cloud Archiving – Eine archivrechtliche und datenschutzrechtliche Bewertung, Hamburg 2009, http://www.ivo-geis.de/veroeffentlichungen/ArchivierungCloud.pdf.

Gercke, M., Strafrechtliche und strafprozessuale Aspekte von Cloud Computing und Cloud Storage, CR 2010, 345.

Gerhards, J., (Grund-)Recht auf Verschlüsselung?, Baden-Baden, 2010.

Gheri, K., Sicheres Backup trotz Datenflut, <kes> Special – Sicheres Cloud Computing, März 2011, 36.

Giebichenstein, R./Weiss, A., Zertifizierte Cloud durch das EuroCloud Star Audit SaaS, DuD 2011, 338.

Glossner, S., in: Leupold, A./Glossner, S., Münchener Anwaltshandbuch IT-Recht, München, 2008.

Gola, P., in: Gola, P./Schomerus, R., Bundesdatenschutzgesetz Kommentar, München, 2010.

Goldmann, H., Cloud Computing: Sicherheit für Daten auch „in der Wolke“, Datenschutz-Berater 11/2010, 18.

Grapentin, S., Haftung und anwendbares Recht im internationalen Datenverkehr, CR 2011, 102.

Graulich, K., in: Arndt, H./Fetzer, T./Scherer, J., Telekommunikationsgesetz, Berlin, 2008.

Greve, H., Kritische Infrastrukturen, DuD 2009, 756.

Grimm, R./Roßnagel, A., Datenschutz für das Internet in den USA, DuD 2000, 446.

Grobauer, B./Walloschek, T./Stöcker, E., Towards a cloud-specific Risk Analysis Framework, Whitepaper der Siemens IT-Solutions and Services, 2010, http://www.itsolutions.siemens.com/b2b/it/en/global/Documents/Publications/CloudSecurity_Whitepaper_PDF_e.pdf.

Grochla, E./Weber, H./Albers, F./Werhahn, T., Ein betriebliches Informationsschutzsystem, Notwendigkeit und Ansatzpunkt für eine Neuorientierung, Angewandte Informatik 1983, 187.

Grünwald, A./Döpkens, H., Cloud Control? – Regulierung von Cloud Computing-Angeboten, MMR 2011, 287.

Grützmacher, M., Lizenzgestaltung für neue Nutzungsformen im Lichte von § 69d UrhG (Teil 1), CR 2011, 489.

Hammer, V., Die 2. Dimension der IT-Sicherheit – Verletzlichkeitsreduzierende Technikgestaltung am Beispiel von Public Key Infrastrukturen, Braunschweig, Wiesbaden, 1999.

Hammer, V., Risiko, DuD 2000, 167.

Hammer, V./Pordesch, U./Roßnagel, A., Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet, Berlin, 1993.

Hanloser, S., Die BDSG-Novelle II: Neuregelungen zum Kunden- und Arbeitnehmerdatenschutz, MMR 2009, 594.

Hansen, M./Marnau, N./Schlehahn, E/Husmann, E., TClouds – Auf dem Weg zur sicheren und datenschutzkonformen Cloud, <kes> Special – Sicheres Cloud Computing, März 2011, 14.

Harder, B./Maruhn, R., BITKOM-Leitfaden Cloud Computing – Was Entscheider wissen müssen, Kapitel „Cloud Computing und Datenschutz“, 2010, http://www.bitkom.org/files/documents/BITKOM_Leitfaden_Cloud_Computing-Was_Entscheider_wissen_muessen.pdf.

Hardtung, B., in: Münchner Kommentar zum Strafgesetzbuch, Band 3, München, 2003.

Heckmann, D., Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen – Maßstäbe für ein IT-Sicherheitsrecht, MMR 2006, 280.

Hegman, S., in: Beck‘scher Online-Kommentar StPO, Edition 12, Stand: 15.10.2011.

Heibey, H., in: Roßnagel, A., Handbuch Datenschutzrecht – Die Grundlagen für Wirtschaft und Verwaltung, München, 2003.

Heidrich, J./Wegener, C., Sichere Datenwolken – Cloud Computing und Datenschutz, MMR 2010, 803.

Heil, H., Privacy Policies, Binding Corporate Rules (BCR) und verbindliche Unternehmensregelungen, DuD 2009, 228.

Helmbrecht, U., Data Protection and legal compliance in Cloud Computing, DuD 2010, 554.

Helwig, B./Koglin, O., Service Level Agreements für Software as a Service-Dienste, in: Taeger, J./Wiebe, A., Inside the Cloud – Neue Herausforderungen für das Informationsrecht, Tagungsband Herbstakademie 2009, Edewecht, 2009, 175.

Hennrich, T., Compliance in Clouds, CR 2011, 546.

Herold, A./Müller, P., Cloud Computing und SaaS, Herausforderungen, Technologien und Einsatzbereiche, http://knol.google.com/k/cloud-computing-und-saas.

Heselhaus, S., in: Dauses, M., EU-Wirtschaftsrecht, 27. Ergänzungslieferung, München, 2011.

Höhne, F./Pöhls, H., Staatliche Schutzpflichten für die IT-Infrastruktur, in: Schartner, P./Weippl, E., D-A-CH Security 2010, Klagenfurt, 2010, 54.

Hoeren, T., Das neue BDSG und die Auftragsdatenverarbeitung, DuD 2010, 688.

Hoeren, T./Spittka, J., Aktuelle Entwicklungen des IT-Vertragsrechts – ITIL, Third Party Maintainance, Cloud Computing und Open Source Hybrids, MMR 2009, 583.

Holznagel, B., Teilhabe und Recht in der Digitalen Welt – Gutachten für die Enquete-Kommission „Globalisierung der Weltwirtschaft – Herausforderungen und Antworten“, Münster, 2002.

Holznagel, B., Recht der IT-Sicherheit, München, 2003.

Holznagel, B./König, C., Zusammenfassung des Gutachtens zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen, Bonn, 2005, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/Abstract_Regelungsumfang_pdf.pdf?__blob=publicationFile.

Holznagel, B./Schumacher, P., Auswirkungen des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme auf RFID-Chips, MMR 2009, 3.

Holznagel, B., in: Spindler, G./Schuster, F., Recht der elektronischen Medien, München, 2011.

Hornung, G., Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, Baden-Baden, 2005.

Hornung, G., RFID und datenschutzrechtliche Transparenz, MMR 2006, XX.

Hornung, G., Ein neues Grundrecht. Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“, CR 2008, 299.

Hübner, G., Wie wirken Standards und Normen im Recht?, DuD 2011, 56.

Idecke-Lux, S., Der Einsatz von multimedialen Dokumenten bei der Genehmigung von neuen Anlagen nach dem Bundesimmissionsschutz-Gesetz, Baden-Baden, 2000.

Immenga, U./Körber, T., in: Immenga, U./Mestmäcker, E., Wettbewerbsrecht, Band 1 EG/Teil 2, Kommentar zum Europäischen Kartellrecht, München, 2007.

Jandt, S./Wilke, D., Umweltverträgliche Entsorgung von Elektronikgeräten – Unberücksichtigte Folgen für den Datenschutz?, UPR 2010, 433.

Jaster, B./Collier de Mendoca, J./Slamka, C./Radmacher, M., Wer klaut in der Cloud? Chancen und Risiken des Cloud Computings, Opinion Paper Detecon International GmbH, 2010, http://www.detecon.com/media.php/publications/studies/2010/OP_Wer_klaut_in_der_Cloud.pdf?dl=1.

Jonen, A., Semantische Analyse des Risikobegriffs – Strukturierung der betriebswirtschaftlichen Risikodefinitionen und literaturempirische Auswertung, in: Lingnau, V., Beiträge zur Controlling-Forschung, Kaiserslautern, 2006, http://kluedo.ub.uni-kl.de/volltexte/2006/2034.

Jotzo, F., Gilt deutsches Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr?, MMR 2009, 232.

Kaiser, H., Automobil-Branche: Into the Cloud, <kes> Special – Sicheres Cloud Computing, März 2011, 28.

Kallerhoff, D., in: Stelkens, P./Bonk, J./Sachs, M., Verwaltungsverfahrensgesetz, München, 2008.

Kammel, V., in: Kilian, W./Heussen, B., Computerrechtshandbuch – Informationstechnologie in der Rechts- und Wirtschaftspraxis, 29. Ergänzungslieferung, München, 2011.

Kappes, M., Netzwerk- und Datensicherheit, Wiesbaden, 2007.

Karger, M./Sarre, F., Wird Cloud Computing zu neuen juristischen Herausforderungen führen?, in: Taeger, J./Wiebe, A., Inside the Cloud – Neue Herausforderungen für das Informationsrecht, Tagungsband Herbstakademie 2009, Edewecht, 2009, 427.

Kargl, W., in: Kindhäuser, U./Neumann, U./Paeffgen, H., Strafgesetzbuch, Band 2, 2010, Baden-Baden.

Kesdogan, D., Über den Wolken – Wie können Vertraulichkeit und Sicherheit in verteilten Systemen gewährleistet werden, in: Lepper, U., Privatsphäre mit System – Datenschutz in einer vernetzten Welt, Düsseldorf, 2010, 36.

Klatte, M., Neue Herausforderung für die Anti-Malware-Industrie, <kes> Special – Sicheres Cloud Computing, März 2011, 18.

Klett, D./Hilberg, S., Die neue DIN-Spezifikation für das Outsourcing – Inhalt und praktische Anwendung, CR 2010, 417.

Klimek, O., Zugangsbeschränkungen im Rahmen des Application Service Providing – Typische Klauseln und Inhaltskontrolle, K&R 2002, 633.

Koch, F., Application Service Providing als neue IT-Leistung, ITRB 2001, 39.

Koehler, J., Finger weg!, <kes> Special – Sicheres Cloud Computing, März 2011, 20.

Kramer, P./Herrmann, M., Auftragsdatenverarbeitung, Zur Reichweite der Privilegierung durch den Tatbestand des § 11 Bundesdatenschutzgesetz, CR 2003, 938.

Kretschmer, T./Bolliger, K./Koob, C., Life 2 – Vernetztes Arbeiten in Wirtschaft und Gesellschaft, 2010, http://www.telekom.com/static/-/10068/1/life-2-si.

Kühl, K., in: Lackner, K.,/Kühl, K., Kommentar zum Strafgesetzbuch, München, 2011.

Kurz, J., Cloud Computing – IT in der <<Wolke>>, Dossier Cloud Computing in Kooperation mit Microsoft, Netzwoche 17/2008, 34, http://download.microsoft.com/download/8/d/4/8d4396ed-8d89-48f1-8b58-4148d4c9b6d3/Cloud%20Computing_IT%20in%20der%20Wolke.pdf.

Lange, H./Schiemann, G., Handbuch des Schuldrechts in Einzeldarstellungen, Schadensersatz, Tübingen, 2003.

Laue, P., Vorgangsbearbeitungssysteme in der öffentlichen Verwaltung – Rechtliche Rahmenbedingungen und Gestaltungsanforderungen, Kassel, 2010.

Lenckner, T./Eisele, J., in: Schönke, A./Schröder, H., Strafgesetzbuch – Kommentar, München, 2010.

Lensdorf, L., IT-Compliance – Maßnahmen zur Reduzierung von Haftungsrisiken von IT-Verantwortlichen, CR 2007, 413.

Lensdorf, L., Auftragsdatenverarbeitung in der EU/EWR und Unterauftragsdatenverarbeitung in Drittländern, CR 2010, 735.

Lensdorf, L./Mayer-Wegelin, C., Die Bedeutung von Standards und Best Practices beim Schutz personenbezogener Daten, CR 2009, 545.

Lensdorf, L./Steger, U., IT-Compliance im Unternehmen, ITRB 2006, 206.

Leonhard, D., Software as a Service – ein innovatives Geschäftsmodell, München, 2009.

Leupold, A., in: Leupold, A./Glossner, S., Münchener Anwaltshandbuch IT-Recht, München, 2008.

von Lewinski, S., in: Loewenheim, U., Handbuch des Urheberrechts, München, 2010.

Luch, A./Schulz, S., Die E-Daseinsvorsorge als Grundlage der Online-Handlungsfreiheit und „Eintrittskarte“ zur Digitalen Agora, VM 2/2011, 104.

Lütcke, J./Bähr, M., Outsourcing-Verträge und Service Level Agreements in der IT-Branche – Gestaltungsvarianten für die Praxis, K&R 2001, 82.

Mansmann, U., Breitband rasant – Internetanschlüsse werden immer schneller, c’t 25/2010, 92.

Marnau, N./Schirmer, N./Schlehahn, E./Schunter, M., TClouds – Herausforderungen und erste Schritte zur sicheren und datenschutzkonformen Cloud, DuD 2011, 333.

Marnau, N./Schlehahn, E., Cloud Computing und Safe Harbor, DuD 2011, 311.

Martens, B./Teuteberg, F./Gräuler, M., Datenbank und Reifegradmodell für die Auswahl und Bewertung von Cloud-Computing-Services, HMD – Praxis der Wirtschaftsinformatik, Heft 275, 2010, 52.

Mell, P./Grance, T., The NIST Definition of Cloud Computing, Final Version 16, 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdfhttp://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf.

Metzger, C./Reitz, C./Villar, J., Cloud Computing – Chancen und Risiken aus technischer und unternehmerischer Sicht, München, 2011.

Meyer-Spasche, G., Vertragsgestaltung beim Cloud Computing, HMD – Praxis der Wirtschaftsinformatik, Heft 275, 2010, 71.

Möschel, W., in: Immenga, U./Mestmäcker, E., Wettbewerbsrecht, Band 1 EG/Teil 2, Kommentar zum Europäischen Kartellrecht, München, 2007.

Müller, M., Die „Essential Facilities"-Doktrin im Europäischen Kartellrecht, EuZW 1998, 232.

Münch, I./Doubrava, C./Essoh, A., Eine Gefährdungsanalyse von Private Clouds, DuD 2011, 322.

Münch, I./Essoh, A./Doubrava, C., Nicht weniger als …, <kes> Special – Sicheres Cloud Computing, März 2011, 10.

Münzl, G./Przywara, B./Reti, M./Schäfer, G./Sondermann, K./Weber, M./Wilker, A., BITKOM-Leitfaden Cloud Computing – Evolution in der Technik, Revolution im Business, 2009, http://www.bitkom.org/60376.aspx?url=BITKOM-Leitfaden-CloudComputing_Web.pdf.

Müthlein, T., Abgrenzungsprobleme bei der Auftragsdatenverarbeitung, RDV 1993, 165.

Muntermann, J./Roßnagel, H./Rannenberg, K., Potentiale und Sicherheitsanforderungen mobiler Finanzinformationsdienste und deren Systeminfrastrukturen, in: von Knop, J./Haverkamp, W./Jessen, E., E-Science und GRID, Ad-hoc-Netze und Medienintegration; Proceedings der 18. DFN-Arbeitstagung über Kommunikationsnetze; Juni 2004, 361, http://www.is-frankfurt.de/publikationenNeu/PotentialeundSicherheitsanford1057.pdf.

Muschick, E./Müller, P., Entscheidungspraxis: Ziele, Verfahren, Konsequenzen, Berlin, 1987.

Nägele, T./Jacobs, S., Rechtsfragen des Cloud Computing, ZUM 2010, 281.

Nicolini, K., in: Möhring, P./Nicolini, K., Kommentar zum Urheberrechtsgesetz, München, 2000.

Nielen, M./Thum, K., Auftragsdatenverarbeitung durch Unternehmen im Nicht-EU-Ausland, K&R 2006, 171.

Niemann, F./Hennrich, T., Kontrollen in den Wolken? – Auftragsdatenverarbeitung in Zeiten des Cloud Computings, CR 2010, 686.

Niemann, F./Paul, J., Bewölkt oder wolkenlos – Rechtliche Herausforderungen des Cloud Computings, K&R 2009, 444.

Nink, J., in: Spindler, G./Schuster, F., Recht der elektronischen Medien, München, 2011.

Nordmeier, C., Cloud Computing und Internationales Privatrecht – Anwendbares Recht bei der Schädigung von in Datenwolken gespeicherten Daten, MMR 2010, 151.

Nüttgens, M./Gehrke, N., DIN SPEC 1401, Outsourcing technologieorientierter wissensintensiver Dienstleistungen, Berlin, 2010.

Obenhaus, N., Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft, NJW 2010, 651.

Oetker, H., in: Rebmann, K./Säcker, F./Rixecker, R., Münchner Kommentar zum BGB, München, 2006.

Otto, P./Sonntag, P., Wege in die Informationsgesellschaft – Steuerungsprobleme in Wirtschaft und Politik, München, 1985.

Pahlen-Brandt, I., Zur Personenbezogenheit von IP-Adressen, K&R 2008, 288.

Pahlen-Brandt, I., Datenschutz braucht scharfe Instrumente – Beitrag zur Diskussion um „personenbezogene Daten“, DuD 2008, 34.

Pankert, M., Abschließen nicht vergessen, <kes> Special – Sicheres Cloud Computing, März 2011, 24.

Paulus, S., Standards für Trusted Clouds, DuD 2011, 317.

Perrow, C., Normale Katastrophen – Die unvermeidbaren Risiken der Großtechnik, Frankfurt/New York, 1987.

Petri, T., in: Simitis, S., Bundesdatenschutzgesetz, Baden-Baden, 2011.

Podlech, A., Aufgaben und Problematik des Datenschutzes, DVR 1976, 23.

Podlech, A., Gesellschaftstheoretische Grundlage des Datenschutzes, in: Dierstein,

R./Fiedler, H./Schulz, A., Datenschutz und Datensicherung, Köln, 1976, 311.

Podlech, A., Individualdatenschutz – Systemdatenschutz, in: Brückner, K./Dalichau, G., Beiträge zum Sozialrecht – Festgabe für Hans Grüner, Percha, 1982, 451.

Pohl, H., Taxonomie und Modellbildung in der Informationssicherheit, DuD 2004, 678.

Pohle, J./Ammann, T., Über den Wolken ... – Chancen und Risiken des Cloud Computing, CR 2009, 273.

Pohle, J./Ammann, T., Software as a Service – auch rechtlich eine Evolution?, K&R 2009, 625.

Polenz, S., Betriebs- und Geschäftsgeheimnisse der öffentlichen Hand, DÖV 2010, 350.

Polenz, S., in: Kilian, W./Heussen, B., Computerrechtshandbuch – Informationstechnologie in der Rechts- und Wirtschaftspraxis, 29. Ergänzungslieferung, München, 2011.

Pordesch, U., Rechtliche Gestaltungsanforderungen an betriebliche Sprachspeichersysteme, DuD 1994, 614.

Pordesch, U./Roßnagel, A., Elektronische Signaturverfahren rechtsgemäß gestaltet, DuD 1994, 82.

Pordesch, U., Die elektronische Form und das Präsentationsproblem, Baden-Baden, 2003.

Probst, T., Sicherheit durch „Cloud Computing"?, DSB 2009, Heft 7-8, 21.

Räther, P., Datenschutz und Outsourcing, DuD 2005, 461.

Räther, P./Seitz, N., Übermittlung personenbezogener Daten in Drittstaaten – Angemessenheitsklausel, Safe Harbor und die Einwilligung, MMR 2002, 425.

Räther, P./Seitz, N., Ausnahmen bei Datentransfer in Drittstaaten – Die beiden Ausnahmen nach § 4c Abs. 2 BDSG: Vertragslösung und Code of Conduct, MMR 2002, 520.

Rammert, W., Technik. Stichwort für eine Enzyklopädie, Technical University Technology Studies, Berlin, 1999.

Rannenberg, K./Pfitzmann, A./Müller, G., in: Müller, G./Pfitzmann, A., Mehrseitige Sicherheit in der Kommunikationstechnik, Bonn, Reading, Menlo Park, New York, Harlow, Don Mills, Sydney, Mexico City, Madrid, Amsterdam, 1998.

Rath, M., Hinweise zur Ausgestaltung von Service Level Agreements, K&R 2007, 362.

Rath, M., Cloud Computing, IT-Security und der Datenschutz, in: Schartner, P./Weippl, E., D-A-CH Security 2010, Klagenfurt, 2010, 185.

Rath, M./Klug, S., e-Discovery in Germany?, K&R 2008, 596.

Redeker, H., IT-Recht, München, 2007.

Redeker, H., in: Hoeren, T./Sieber, U., Handbuch Multimedia-Recht, 26. Ergänzungslieferung 2010, München 2010.

Reindl, M., Cloud Computing & Datenschutz, in: Taeger, J./Wiebe, A., Inside the Cloud – Neue Herausforderungen für das Informationsrecht, Tagungsband Herbstakademie 2009, Edewecht, 2009, 441.

Renn, O./Zwick, M., Risiko- und Technikakzeptanz, Berlin, 1997.

Repschläger, J./Pannicke, D./Zarnekow, R., Cloud Computing: Definitionen, Geschäftsmodelle und Entwicklungspotenziale, HMD – Praxis der Wirtschaftsinformatik, Heft 275, 2010, 6.

Reti, M./Pauly, M., T-Systems White Paper Cloud Computing, Alternative Sourcing-Strategie für Unternehmens-ICT, 2009, http://download.sczm.t-systems.de/t-systems.ch/de/StaticPage/62/79/00/627900_White-Paper-Cloud-Computing.

Richardi, R., in: von Staudinger, J., Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, München, 2011.

Ricke, T., in: Spindler, G./Schuster, F., Recht der elektronischen Medien, München, 2011.

Rittweger, C./Schmidl, M., Einwirkung von Standardvertragsklauseln auf § 28 BDSG, DuD 2004, 617.

Röhrborn, J./Sinhart, M., Application Service Providing – juristische Einordnung und Vertragsgestaltung, CR 2001, 69.

Roßnagel, A., Die rechtliche Fassung technischer Risiken, UPR 1986, 46.

Roßnagel, A., Rechtswissenschaftliche Technikfolgenforschung: Umrisse einer Forschungsdisziplin, Baden-Baden, 1993.

Roßnagel, A., Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger. Thesen zur Änderung der Staatsaufgaben in einer „civil information society“, ZRP 1997, 26.

Roßnagel, A., Datenschutzaudit – Konzeption, Durchführung, gesetzliche Regelung, Braunschweig, 2000.

Roßnagel, A., Allianz von Medienrecht und Informationstechnik: Hoffnungen und Herausforderungen, in: Roßnagel, A., Allianz von Medienrecht und Informationstechnik?, Baden-Baden, 2001.

Roßnagel, A., 20 Jahre Volkszählungsurteil, MMR 2003, 693.

Roßnagel, A., in: Roßnagel, A., Handbuch Datenschutzrecht – Die Grundlagen für Wirtschaft und Verwaltung, München, 2003.

Roßnagel, A., Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MMR 2005, 71.

Roßnagel, A., Datenschutz in einem informatisierten Alltag – Gutachten im Auftrag der Friedrich-Ebert-Stiftung, Berlin, 2007.

Roßnagel, A., Datenschutzaudit – ein modernes Steuerungsinstrument, in: Hempel, L./Krasmann, S./Bröckling, U., Sichtbarkeitsregime – Überwachung, Sicherheit und Privatheit im 21. Jahrhundert, Leviathan Sonderheft 2010, 263.

Roßnagel, A., Das Gebot der Datenvermeidung und -sparsamkeit als Ansatz wirksamen technikbasierten Persönlichkeitsschutzes? in: Eifert, M./Hoffmann-Riem, W., Innovation, Recht und öffentliche Kommunikation, Berlin, 2011.

Roßnagel, A., in: Koch, H./Pache, E./Scheuing, D., Gemeinschaftskommentar zum Bundes-Immissionsschutzgesetz, Köln, 2011.

Roßnagel, A./Bedner, M./Knopp, M., Rechtliche Anforderungen an die Aufbewahrung von Vorratsdaten, DuD 2009, 536.

Roßnagel, A./Jandt, S., Datenschutz in Social Networks – Kollektive Verantwortlichkeit für die Datenverarbeitung, ZD 2011, 160.

Roßnagel, A./Neuser, U., Die rechtliche Regulierung des Elektrosmogs, UPR 1993, 401.

Roßnagel, A./Pfitzmann, A./Garstka, H., Modernisierung des Datenschutzrechts, Berlin, 2001, http://www.computerundrecht.de/media/gutachten.pdf.

Roßnagel, A./Schmücker, P., Beweiskräftige elektronische Archivierung – Bieten elektronische Signaturen Rechtssicherheit?, Heidelberg, 2005.

Roßnagel, A./Schnabel, C., Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, 3534.

Roßnagel, A./Schneider, M., Anforderungen an die mehrseitige Sicherheit in der Gesundheitsversorgung und ihre Erhebung, it+ti 1996, 15.

Roßnagel, A./Scholz, P., Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721.

Roßnagel, A./Wedde, P./Hammer, V./Pordesch, U., Die Verletzlichkeit der Informationsgesellschaft, Opladen, 1990.

Rost, M./Pfitzmann, A., Datenschutz-Schutzziele – revisited, DuD 2009, 353.

Roth, B., Organisatorische und technische Maßnahmen zum Schutz personenbezogener Daten, ITRB 2010, 60.

Roth, B./Schneider, U., IT-Sicherheit und Haftung, ITRB 2005, 19.

Rüsken, R., in: Klein, F., Abgabenordnung, München, 2009.

Schaar, P., Datenschutz im Internet: Die Grundlagen, München, 2002.

Schack, H., Urheber- und Urhebervertragsrecht, Tübingen, 2001.

Schaffland, H./Wiltfang, N., Bundesdatenschutzgesetz (BDSG) – Ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften, Berlin, 2010.

Schelinski, T., in: Leupold, A./Glossner, S., Münchener Anwaltshandbuch IT-Recht, München, 2011.

Scherer, J., Das Bronner-Urteil des EuGH und die Essential-Facilities-Doktrin im TK-Sektor, MMR 1999, 315.

Scherer, J., in: Dauses, M., EU-Wirtschaftsrecht, 27. Ergänzungslieferung, München, 2011.

Schiedermair, S., in: Dörr, D./Kreile, J./Cole, M., Handbuch Medienrecht – Recht der elektronischen Massenmedien, Frankfurt am Main, 2008.

Schiemann, G., in: von Staudinger, J., Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, München, 2011.

Schmidl, M., Aspekte des Rechts der IT-Sicherheit, NJW 2010, 476.

Schmidl, M./Krone, D., Standardvertragsklauseln als Basis intra-europäischer Auftragsdatenverarbeitung, DuD 2010, 838.

Schmidt, B., Compliance – Die Vorstandspflicht zur Beherrschung von Rechtsrisiken, in: Horster, P./Schartner, P., DACH Security 2009, 25.

Schmidt-Preuß, M., in: Kloepfer, M., Schutz kritischer Infrastrukturen, Baden-Baden, 2010.

Schmitz, P., in: Hoeren, T./Sieber, U., Handbuch Multimedia-Recht, 26. Ergänzungslieferung 2010, München 2010.

Schnabel, C., Datenschutz bei profilbasierten Location Based Services, Kassel, 2009.

Schneider, J., Cloud Computing: Klare Sicht in der Wolke, IT-Grundschutz 2010, 10.

Schneider, J., Die Datensicherheit – eine vergessene Regelungsmaterie?, ZD 2011, 6.

Scholz, M./Lutz, H., Standardvertragsklauseln für Auftragsverarbeiter und § 11 BDSG, CR 2011, 424.

Scholz, P., Datenschutz beim Internet-Einkauf, Baden-Baden, 2003.

Scholz, P., in: Simitis, S., Bundesdatenschutzgesetz, Baden-Baden, 2011.

Schommertz, R., in: Scheurle, K./Mayen, T., Telekommunikationsgesetz, München, 2008.

Schricker, G., Verlagsrecht, München, 2001.

Schröder, C./Haag, N., Neue Anforderungen an Cloud Computing für die Praxis, ZD 2011, 147.

Schubert, C., in: Bamberger, H./Roth, H., Beck'scher Onlinekommentar zum BGB, Edition 18, Stand: 1.8.2010.

Schulz, C., Rechtliche Aspekte des Cloud Computing im Überblick, in: Taeger, J./Wiebe, A., Inside the Cloud – Neue Herausforderungen für das Informationsrecht, Tagungsband Herbstakademie 2009, Edewecht, 2009, 403.

Schulz, C./Rosenkranz, T., Cloud Computing – Bedarfsorientierte Nutzung von IT-Ressourcen, ITRB 2009, 232.

Schulz, S., Cloud Computing in der öffentlichen Verwaltung – Chancen, Risiken, Modelle, MMR 2010, 75.

Schulz, S., Cloud Computing in der öffentlichen Verwaltung?, VM 1/2010, 36.

Schulz, S., Macht Art. 91 c GG E-Government-Gesetze der Länder erforderlich?, DÖV 2010, 225.

Schulze, R., in: Schulze, R., Handkommentar zum BGB, Baden-Baden, 2006.

Schumacher, V., Service Level Agreements: Schwerpunkt bei IT- und Telekommunikationsverträgen, MMR 2006, 12.

Schuster, F., Rechtsnatur der Service Level bei IT-Verträgen, CR 2009, 205.

Schuster, F./Reichl, W., Cloud Computing und SaaS: Was sind die wirklich neuen Fragen?, CR 2010, 38.

Schwarze, L./Müller, P., IT-Outsourcing – Erfahrungen, Status und zukünftige Herausforderungen, HMD – Praxis der Wirtschaftsinformatik, Heft 245, 2005, 6.

Schwenke, M., Individualisierung und Datenschutz – Rechtskonforme Gestaltung der datenschutzrechtlichen Einwilligung im Kontext individualisierter Waren und Dienstleistungen, Wiesbaden, 2006.

Seckelmann, M., „Renaissance" der Gemeinschaftsaufgaben in der Föderalismusreform II?, DÖV 2009, 747.

Siegel, T., IT im Grundgesetz, NVwZ 2009, 1128.

Simitis, S., Datenschutz – Rückschritt oder Neubeginn?, NJW 1998, 2473.

Simitis, S., Auf dem Weg zu einem neuen Datenschutzkonzept, DuD 2000, 714.

Simitis, S., in: Simitis, S., Bundesdatenschutzgesetz, Baden-Baden, 2011.

Singer, O., Aktueller Begriff – Cloud Computing, Ausarbeitung des Wissenschaftlichen Dienstes des Bundestages, Nr. 15/10 vom 12.3.2010, http://www.bundestag.de/dokumente/analysen/2010/cloud_computing.pdf.

Slamka, C./Georg, L., Management-Einschätzungen der Sicherheit im Cloud Computing, in: Schartner, P./Weippl, E., D-A-CH Security 2010, Klagenfurt, 2010, 20.

Söbbing, T., Cloud und Grid Computing, IT-Strategien der Zukunft rechtlich betrachtet, MMR 2008, Heft 5, XII.

Söbbing, T./Wöhlermann, K., Rechtliche Fragen im IT-Outsourcing, HMD – Praxis der Wirtschaftsinformatik, Heft 245, 2005, 48.

Söbbing, T., Cloud Computing und Virtualisierung – Rechtliche Fragen, in: Leible, S./Sosnitza, O., Onlinerecht 2.0: Alte Fragen – neue Antworten? Cloud Computing – Datenschutz – Urheberrecht – Haftung, Stuttgart, 2011.

Soergel, H./Kegel, G., Bürgerliches Gesetzbuch, Band 10, Einführungsgesetz, Stuttgart, 1996.

Sokol, B., in: Simitis, S., Bundesdatenschutzgesetz, Baden-Baden, 2011.

Sokolov, I., Cloud Computing: Overview, Concepts and Business Deployment Scenarios, Wien, 2009,
http://www.ivosokolov.com/papers/Cloud_Computing_Ivo_Sokolov.pdf.

Spies, A., USA: Grenzüberschreitende elektronische Beweiserhebung (Discovery) vs. Datenschutz?, MMR 2007, Heft 7, V.

Spies, A., USA: Cloud Computing – Schwarze Löcher im Datenschutzrecht, MMR 2009, Heft 5, XI.

Spies, A., Cloud Computing: Keine personenbezogenen Daten bei Verschlüsselung, MMR-Aktuell 2011, 313727.

Spies, A./Schröder, C., Auswirkungen der elektronischen Beweiserhebung (eDiscovery) in den USA auf deutsche Unternehmen, MMR 2008, 275.

Spindler, G., IT-Sicherheit – Rechtliche Defizite und rechtspolitische Alternativen, MMR 2008, 7.

Spindler, G., in: Spindler, G./Schuster, F., Recht der elektronischen Medien, München, 2011.

von Sponeck, H., Überlassung von RZ-Kapazität – ein Fall der Auftragsdatenverarbeitung?, CR 1992, 594.

Steinbach, R., Die Umsetzung der EG-Richtlinie Datenschutz im Sozialgesetzbuch, NZS 2002, 15.

Steinmüller, W./Lutterbeck, B./Mallmann, C./Harbort, U./Kolb, G./Schneider, J., Grundfragen des Datenschutzes – Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. 6/3826, 1971.

Stelzer, D., Sicherheitsstrategien in der Informationsverarbeitung – Ein wissensbasiertes, objektorientiertes Beratungssystem für die Risikoanalyse, Wiesbaden, 1993.

Streitberger, W./Ruppel, A., Fraunhofer SIT, Cloud Computing Sicherheit – Schutzziele, Taxonomie, Marktübersicht, München, 2009.

Stritter, B., MozPETs-PeMar. Entwicklung eines Gateways zum anonymen E-Mailversand über Remailer-Netzwerke und Anbindung von Mozilla Mail, Darmstadt, 2006, http://www.ito.tu-darmstadt.de/staff/Lars/Stritter_PeMaR.pdf.

Sutschet, H., Auftragsdatenverarbeitung und Funktionsübertragung, RDV 2004, 97.

Talbot, D., Ein Zaun für die Wolke, Technology Review 03/2010, 36.

Tanenbaum, A./van Steen, M., Verteilte Systeme – Grundlagen und Paradigmen, München, 2007.

Tetzner, T., Sicherheitsanforderungen an das Cloud Computing – Identifikation und Analyse, Saarbrücken, 2010.

Tietz, V./Blichmann, G./Hübsch, G., Cloud-Entwicklungsmethoden – Überblick, Bewertungen und Herausforderungen, Informatik Spektrum 2011, 345.

Tsvihun, I./Stephanow, P./Streitberger, W., Fraunhofer SIT, Vergleich der Sicherheit traditioneller IT-Systeme und Public Cloud Computing Systeme, München, 2010.

Vander, S., Auftragsdatenverarbeitung 2.0, K&R 2010, 292.

Vaquero, L./Rodero-Merino, L./Caceres, J./Lindner, M., A Break in the Clouds: Towards a Cloud Definition, ACM SIGCOMM Computer Communication Review, 2009, 50.

Vec, M., Kurze Geschichte des Technikrechts – Von den Anfängen bis zum ersten Weltkrieg, in: Schulte, M./Schröder, R., Handbuch des Technikrechts, Berlin, Heidelberg, New York, Hongkong, London, Mailand, 2011.

Wächter, M., Rechtliche Grundstrukturen der Datenverarbeitung im Auftrag, CR 1991, 333.

Waller, S., Außervertragliche Gewährleistungsrechte beim IT-Outsourcing, ITRB 2005, 162.

Walter, M., in: Loewenheim, U., Handbuch des Urheberrechts, München, 2010.

Walz, S., in: Simitis, S., Bundesdatenschutzgesetz, Baden-Baden, 2006.

Wandtke, A., in: Wandtke, A./Bullinger, W., Praxiskommentar zum Urheberrecht, München, 2009.

Wank, R., in: Müller-Glöge, R./Preis, U./Schmidt, I., Erfurter Kommentar zum Arbeitsrecht, München, 2011.

Warren, S./Brandeis, L., The right to privacy, Harvard Law Review, Volume 4, 1890, 198.

Weber, M./Voigt, P., Internationale Auftragsdatenverarbeitung – Praxisempfehlungen für die Auslagerung von IT-Systemen in Drittstaaten mittels Standardvertragsklauseln, ZD 2011, 74.

Weichert, T., in: Däubler, W./Klebe, T./Wedde, P./Weichert, T., Bundesdatenschutzgesetz, Kompaktkommentar zum BDSG, Frankfurt am Main, 2010.

Weichert, T., Cloud Computing und Datenschutz, DuD 2010, 679.

Weidenkaff, W., in: Palandt, O., Kommentar zum BGB, München, 2010.

Weiner, N./Renner, T./Kett, H., Geschäftsmodelle im Internet der Dienste – Aktueller Stand in Forschung und Praxis, Studie des Fraunhofer IAO, Stuttgart, 2010.

Weiss, A., Gütesiegel für die Cloud, <kes> Special – Sicheres Cloud Computing, März 2011, 16.

von Welser, M., in: Wandtke, A./Bullinger, W., Praxiskommentar zum Urheberrecht, München, 2009.

von Westerholt, M./Berger, K., Der Application Service Provider und das neue Schuldrecht, CR 2002, 81.

Witt, B., IT-Sicherheit kompakt und verständlich, Wiesbaden, 2006.

Wolff, H., Der verfassungsrechtliche Schutz der Betriebs- und Geschäftsgeheimnisse, NJW 1997, 98.

Wunderlich, M., Rechtliche Aspekte des Cloud Computing, Darmstadt, 2010, http://www.worldwidewundi.de/wordpress/wpcontent/uploads/2010/09/rechtliche_aspekte_des_cloud_computing_diplomarbeit_SS_2010_markus_wunderlich.pdf.

Ziebarth, W., Grundrechtskonforme Gestaltung der Vorratsdatenspeicherung – Überlegungen zu einer europa-, verfassungs- und datenschutzrechtskonformen Umsetzung, DuD 2009, 25.

ISBN 978-3-86219-080-5