verbraucherzentrierten Lösungen ein wichtiges Marksegment der IT-Sicherheitsindustrie.

Das wiederum mit *Withfield Diffie, Martin Hellman, Ronald Rivest, Adi Shamir* prominent besetzte und von *Burt Kaliski* moderierte Cryptopanel bewertete in diesem Jahr die allgemeine Situation der Kryptographie eher kritisch. Bezüglich der Angriffe auf den Hash-Algorithmus SHA-1 gäbe es zwar eine Pattsituation, aber in China wachsen in hohem Tempo Ressourcen (Shamir: Crypto-Fabric) mit denen möglicherweise sein Verfall beschleunigt wird. Die globale Ausschreibung des NIST zu neuen Hash-Algorithmen wird nicht vor 2012 konsolidierte Ergebnisse bringen, deshalb sind Überbrückungskonzepte mit SHA256 und SHA384 unvermeidlich. *Diffie* begrüßte in diesem Zusammenhang ausdrücklich die Implementierung der von NSA/NIST im vergangenen Jahr vorgeschlagenen Suite B (AES + ECC + SHA256) in das TSL-Protokoll und in VISTA.

Shamir stellte kritisch fest, dass die Kryptotechnologien keinen wirklich erfolgreichen Beitrag zum ‚Identitätsdiebstahl' geleistet hat. Im Hinblick auf die prinzipiellen Möglichkeiten einer Public-Key-Infrastruktur ist nur Flickwerk ohne eine effektive Revocation-Lösung entstanden. Die langfristige Zukunft der Public Key Cryptography wird sich – so die Experten – mit dem Entwicklungstempo der Quantenkryptographie entscheiden. Der Ansatz von Suite B wird nach ihrer Meinung sichere Signaturen in den nächsten 15 Jahren zulassen.

Shamir's Sicht auf Zukunft der Kryptoanwendungen war zum Schluss pessimistisch:

Weil die Sicherheit der verwendeten Systeme wegen ihrer steigenden Komplexität abnehme, werde man in dreißig Jahren feststellen, dass die Kryptographie zwar viele Schlachten gewonnen, den Krieg für mehr Sicherheit aber verloren habe.

Die diesjährige RSA-Konferenz bot wiederum Gelegenheit den Arbeitsstand und die Realisierungsbedingungen für die USA-Programme im Bereich der IT-Sicherheit und unter den Vorgaben des Departments of Homeland Security kennen zu lernen. Generell wurde dabei deutlich, dass in den großen Projekten erhebliche ‚Reibungsverluste' entstanden sind. Dies hat direkte Auswirkungen für den IT-Sicherheitsmarkt in den USA: So haben sich die Government-Ausgaben für IT-Sicherheit 2006 gegenüber 2005 nahezu halbiert (Forrester). Die wesentliche Ursache für das Abbremsen der Projekte liegt offensichtlich in politischen Differenzen zwischen Washington und den Bundesstaaten. Betroffen ist vor allem die Vorbereitung einer nationalen eID Card (auf Basis der Führerscheine) mit ca. 220 Mio. ID-Cards.

Unter dem Blickwinkel globaler Wirkungen sind folgende auf der RSA 2007 vorgestellten Detailinformationen hervorzuheben:

- Die Suite B mit AES-128, AES-256 für Verschlüsselung; ECDSA with NIST P-256, ECDSA with NIST P-384 für Signaturen; EC DH or EC MQV für Keyy Agreement; und SHA-256, SHA-384 ist in das TLS-Protokoll aufgenommen worden. Sie wird von allen wichtigen Anbietern interoperabel unterstützt. Damit steht erstmals die Elliptic Curve Cryptography für breite Anwendungen zur Verfügung.
- Das Konzept der Extended Validation (EV) für Serverzertifikate und ihre verbraucherfreundliche Darstellung ist anwendungsreif und wird 2007 eingeführt. Beteiligt sind 20 CA's und die Browser-Software-Provider KDE, Microsoft, Opera, Mozilla.
- Dem Aufbau von Vertrauen zwischen PKI-Domänen wird hohe Aufmerksamkeit geschenkt. Zunehmend werden hierfür geschäftprozessnahe ‚Policy-Server' angeboten und konfiguriert.
- Zunehmend werden Trusted Computing und TPM-Anwendungen Realität. In den USA sind bereits Plattformidentität und –Attestation mit TPM 1.2 für Governmentlösungen vorgeschrieben. In MS-VISTA sind Schnittstellen verfügbar, die TPM-Funktionalitäten auch für externe Anbieter verfügbar machen. Utimaco hat hier beispielsweise SafeGuard-Enterprise als Alternative für BitLocker integriert.
- Alternativen zu PKI werden stärker beachtet. Der Kryptoentwicklungschef von RSA, *Bert Kaliski,* hat in diesem Zusammenhang auf die Leistungsfähigkeit von Key-Management-Systemen für symmetrische Schlüssel hingewiesen. Nach seiner Meinung können diese Konzepte den Verfall der asymmetrischen Kryptographie überleben.

Die nächste RSA-Konferenz wird vom 7.-11. April 2008 wiederum in San Francisco stattfinden.

Helmut Reimer

Buchbesprechungen

Meuth, Lotte: Zulässigkeit von Identitätsfeststellungen mittels biometrischer Systeme durch öffentliche Stellen, Beiträge zum Informationsrecht, Band 17, Duncker & Humblot, Berlin 2006, 283 Seiten, 74,- Euro, ISBN 3-428-11953-3

Das Buch von Meuth analysiert die Verwendung biometrischer Systeme aus der Perspektive öffentlicher Stellen insbesondere im Bereich der Strafverfolgung und Gefahrenabwehr. Vor allem die Passagen, welche über die derzeit hauptsächlich diskutierten biometrischen Identifikationspapiere hinausgehen, stellen dabei eine Erweiterung der Debatte dar. Im Spannungsfeld zwischen Sicherheit und Freiheit nimmt die Autorin konsequent die erste Dimension zum Ausgangspunkt: Die Einleitung beginnt mit dem „Bedürfnis des Menschen nach Sicherheit", und die verfassungsrechtliche Analyse untersucht nicht etwa zuerst Art und Intensität der Grundrechtsbeeinträchtigungen durch biometrische Verfahren, sondern die „objektive Schutzpflicht des Staates" im Bereich der inneren Sicherheit.

Nach einer knappen, aber gut strukturierten und verständlichen technischen Einführung behandeln die beiden Hauptteile der Arbeit die geltende Rechtslage hinsichtlich der Identitätsfeststellung mittels biometrischer Systeme einerseits, deren Verfassungsmäßigkeit andererseits. Es folgen ein kurzer Ausblick auf rechtspolitische Änderungsvorhaben und eine Zusammenfassung der Ergebnisse. Auffällig ist leider, dass die Autorin die bisherige juristische Literatur zur Biometrie – mit Ausnahme der einschlägigen Gutachten des ULD Schleswig-Holstein – durchweg nur überaus spärlich berücksichtigt hat.

Der erste Hauptteil beschreibt zunächst die derzeitige Rechtslage bei amtlichen Identitätspapieren, wobei Meuth mehrfach auf die Unzulänglichkeiten der bisherigen Regelungen (vor allem im Bereich der Ausländerausweise) hinweist. Sodann wird das unübersichtliche Geflecht der verschiedenen biometrischen Referenz- und Erkennungsdienstdateien von Deutschen und Ausländern strukturiert und verständlich dargestellt. Von besonderem Interesse ist der Teil über die Identitätsfeststellung im Strafverfolgungs- und Gefahrenabwehrbereich. Hier wird deutlich, welche umfassenden Anwendungsbereiche die Biometrie haben könnte, wenn die bisherigen Ermächtigungsgrundlagen der erkennungsdienstlichen Behandlung, der

polizeilichen Bildaufzeichnung bei Versammlungen und im öffentlichen Raum, insbesondere aber der Rasterfahndung in Zukunft angewendet werden sollten. Gegenüber der ausführlichen Darstellung der Eingriffstatbestände gerät allerdings die Frage etwas in den Hintergrund, inwieweit die Subsumtion biometrischer Verfahren unter diese Tatbestände tatsächlich zulässig ist. Angesichts der Tatsache, dass dem Gesetzgeber diese Verfahren bei der Verabschiedung der jeweiligen Norm unbekannt waren und sie eine besondere Eingriffstiefe aufweisen, dürfte es zumindest zweifelhaft sein, ob etwa der Zugriff auf betriebliche biometrische Referenzdatenbanken auf die sehr weiten polizeirechtlichen Ermächtigungsgrundlagen zur Rasterfahndung gestützt werden könnte.

Der verfassungsrechtliche Teil des Buches beginnt mit der Betrachtung der Gesetzgebungskompetenz. Diese befasst sich nur mit der deutschen Kompetenzordnung, die Zuständigkeiten der Europäischen Union und internationaler Organisationen wie der ICAO fehlen. Das mag im Rahmen einer rein nationalrechtlichen Untersuchung konsequent sein, angesichts der Tatsache, dass die nationale Gesetzgebung zumindest im Bereich der Identitätspapiere entweder wegen des Vorrangs des Europarechts nicht zum Zuge kommt (Pass) oder im Abschreiben der EU-Verordnung zum Pass bestehen wird (Personalausweis), entsteht so aber ein schiefes Bild der tatsächlichen Kompetenzen.

Im Rahmen der staatlichen Schutzpflicht erörtert Meuth die Probleme der Eignung der Biometrie hinsichtlich Merkmalsauswahl, Fehlerraten, Langzeitstabilität, Sicherheitsanforderungen und zentralen Datenbanken und bejaht die Eignung aufgrund des weiten Einschätzungsspielraums des Staates. Ein Verstoß gegen die Menschenwürdegarantie wird für die deutschen Pass- und Personalausweisinhaber bei Verwendung von Templates verneint, hinsichtlich der weiten Nutzungsbefugnis in § 78 Abs. 5 AufenthG angesichts der Eingriffstiefe und dem großen Kreis der Betroffenen bejaht. Leider beschränkt sich Meuth im Folgenden mehrfach auf die Aussage, ein verfassungsrechtliches Urteil könnte erst nach Verabschiedung bereichsspezifischer Ausführungsgesetze gefällt werden. Hier hätte sich der Leser die Benennung verfassungsrechtlicher Kriterien für diese Gesetze gewünscht.

Erfreulich deutlich sind demgegenüber die Forderungen nach Verwendung von Templates, kryptographischen Absicherungen, Verbesserung der Fehlerraten, Rückfallsystemen und dem Verbot einer Beweislastumkehr zulasten der Betroffenen. Das Verlangen, im Rahmen von Polizeikontrollen dürften biometrische Ausweisdaten nur ausgelesen werden, wenn Anhaltspunkte gegen die Besitzberechtigung oder Echtheit sprächen, wird sich allerdings in der Praxis kaum durchsetzen. Wird schließlich der Einsatz von Volldatensätzen bei Identitätspapieren unter allen Umständen für verfassungswidrig erklärt, so wäre die Anwendung dieser Aussage auf die neuen Reisepässe konsequent gewesen, die aus den bekannten Interoperabilitätsgründen Volldatensätze des Gesichtes speichern.

Wie schon im ersten Teil lesen sich auch die verfassungsrechtlichen Erörterungen zu den allgemeinen Identifizierungsbefugnissen der Polizeibehörden sehr interessant, auch wenn der Autorin hier bei der Erörterung allgemeiner Rechtsfragen der polizeirechtlichen Identifizierung, Videoüberwachung und Rasterfahndung bisweilen der Focus auf die Biometrie etwas abhanden kommt. Das Ergebnis, eine „Durchrasterung“ privater und hoheitlicher biometrischer Datenbanken sei auch verfassungsrechtlich unter bestimmten Voraussetzungen nicht zu beanstanden, ist aus Sicht des Rezensenten überaus kritisch zu hinterfragen; das schmälert den Wert der Untersuchung jedoch selbstverständlich nicht. Insgesamt mögen diejenigen, die nach einer umfassenden, grund- und datenschutzrechtlichen Diskussion der Biometrie suchen, an anderer Stelle besser bedient sein. Wer sich jedoch für die polizeirechtliche Perspektive der hoheitlichen Identifizierung – unter Einschluss der Biometrie – interessiert, wird Meuths Buch mit Gewinn lesen.

Gerrit Hornung

Robert, Martine; Giraudy, Erol: Le guide juridique du portail Internet/Intranet, Verlag ESKA, Paris 2005, ISBN 2-7472-0699-8, 512 Seiten, Euro 45,00

Bezüglich der Entwicklung der Aktienkurse von Internet-Unternehmen und der Anzahl der Bücher zum Internetrecht besteht eine gewisse Korrelation: Während zu Zeiten des Internet-Booms eine Vielzahl von Monographien erschienen ist, veröffentlichen die Verlage derzeit nur noch wenige Publikationen. Bei unserem Nachbarn Frankreich ist die Lage auf dem Internet-Buchmarkt noch zugespitzter als bei uns. Wer sich über den letzten Stand des französischen Internetrechts informieren will, hat nur die Wahl zwischen zwei Büchern : Neben dem Werk von Robert/Giraudy gibt es lediglich das Büchlein von Jacques Larrieu, Droit de l´Internet, Verlag ellipses (2005). Das Buch von Robert/Giraudy ist nicht nur wesentlich umfangreicher als das Konkurrenzwerk, es verfolgt auch ein anderes Ziel. Während Larrieu für Juristen schreibt, wenden sich Robert/Giraudy an Praktiker ohne Vorkenntnisse, die für ihr Unternehmen eine Internetpräsenz schaffen wollen.

In der Einführung werden die Grundzüge des französischen Gewerblichen Rechtsschutzes, des Urheberrechts, des Presserechts sowie die wichtigsten Strafrechtsnormen mit Internetbezug skizziert. Daran schließen sich Kapitel über die verschiedenen Domain-Arten, die technischen und rechtlichen Aspekte der Schaffung einer Homepage und über die rechtlichen Besonderheiten bei Fernabsatz- sowie bei Providerverträgen an. Außerdem erörtern die Autoren die arbeitsrechtlichen Rahmenbedingungen, welche die Nutzung des Internets in Betrieben regulieren. Dabei gehen sie auch relativ ausführlich allgemein auf das kollektive Arbeitsrecht ein, wobei hier dem französischen Zielpublikum vieles schon bekannt sein dürfte, dem ausländischen Leser wird das Verständnis der Internetspezifika dadurch aber sehr erleichtert. Ferner werden die Vergabe der „ .fr“-Top-level-Domains durch die AFNIC, das Datenschutzrecht und die Datensicherheit (vor allem unter technischen Aspekten) behandelt. Das Kapitel über das wohl wichtigste Gesetz zum Internetrecht in Frankreich, nämlich die „Loi sur l´économie numérique (LEN) vom 21. Juni 2004“, beschränkt sich im Wesentlichen auf die wörtliche Wiedergabe des Gesetzestextes.

Dieses Verfahren wurde in abgeschwächtem Maße auch bei den anderen Kapiteln angewandt: Wichtige Paragraphen geben die Autoren im Wortlaut wieder. Damit ersparen sie insbesondere dem Leser im Ausland, der im Regelfall nicht über entsprechende Gesetzessammlungen verfügt, die zeitaufwendige Suche nach Gesetzestexten im Internet.

Auf den S. 253 bis 433 findet sich ein Anhang mit diversen Texten (Gesetze und Verordnungen, Regeln zur Vergabe der .fr-Domains u.a.). Dem folgten eine Sammlung wichtiger Internetadressen und ein Glossar. Ein umfangreiches Stichwortverzeichnis beschließt das Buch.

Insgesamt ein Werk, dessen Lektüre (nicht nur) jedem am französischen Internetrecht Interessierten wärmstens empfohlen werden kann. Dieses Buch erschließt dem deutschen Leser auf leicht verständliche Weise die für ihn fremde Rechtsmaterie, ohne dass er auf weitere Literatur oder separate Gesetzestexte zurückgreifen muss.

Joachim Gruber