INTEGRIERTE IT-VERSORGUNG - WAS MAN WIRKLICH BRAUCHT

Gerhard Schneider

gerhard.schneider@rz.uni-freiburg.de

Zur Person…. ☺

- Seit 1.4.22 „außer Betrieb“
- Welche Weisheiten kann ich denn überhaupt noch verkünden?
- Nun ja…
  - Noch habe ich Erinnerungen
  - Und noch besser:
    ich bin keinem mehr verpflichtet
  - und darf mich deshalb „um Kopf und Kragen reden“ ☺ ☺

Quelle: Amazon

Emeritus ist ein toller Beruf –
blöd daran ist nur die lange Ausbildung

Integrierte IT-Versorgung

ChatGPT am 9.2.23:
> wieviel ist 3+5
- *3 + 5 ist gleich 8.*

> nein, es ist 9
- *Ja, Sie haben Recht. 3 + 5 ist tatsächlich 9. Entschuldigung für den Fehler.*

- Was ist das eigentlich?
  - $\int_{1kB}^{5\ CPU-h} IT\ dt$????
- Aus einer Uni-Strategie:
  ein campusweites integriertes Informationsmanagement, das die wesentlichen Abläufe und Prozesse der Universität in Forschung, Lehre, Verwaltung, Organisation und Steuerung abbildet und unterstützt. Integriertes Informationsmanagement heißt auch, dass Studierende, Wissenschaftler und Zentralverwaltung, aber auch die Fakultätsverwaltungen, die zentralen Einrichtungen und das Präsidium mit gleich hoher Qualität versorgt werden.
- ChatGPT:
  Integrierte IT-Versorgung ist ein Konzept, bei dem mehrere IT-Systeme und -Lösungen miteinander verbunden und in einer einheitlichen Art und Weise genutzt werden, um eine optimale Unterstützung für die Geschäftsprozesse eines Unternehmens zu gewährleisten. Dies beinhaltet die Verwendung von gemeinsamen Datenbanken, Netzwerken und Anwendungen, um eine bessere Zusammenarbeit und Datenintegration zu ermöglichen. Die integrierte IT-Versorgung soll dabei helfen, Datenredundanz zu vermeiden, Prozesse zu optimieren und Geschäftskontinuität zu gewährleisten.

Integrierte IT-Versorgung - **Planung**

- Problem: niemand weiß, wie sie aussieht
- Machen Sie mal ein Gesamtkonzept (Nebenbemerkung: ein Konzept für die Zukunft zu machen, ist schwierig) – *oh, das ist teuer, das geht nicht, ich würde Einzelteile ganz anders machen und meine Stellvertreterin hat eh eine andere Auffassung*.
- Gremien: wenig IT-Konzeptwissen, aber hohe Entscheidungsgewalt und Machtbewusstsein, demonstriert durch (unbewusstes) Hineinreden im Detail
  - IT-Entscheidungen solcher Gremien eignen sich manchmal fürs IT-Kabarett
  - Was ist wohl der Hauptgrund, weshalb es in D mit der Digitalisierung nicht vorangeht?
- Die Forderung nach EINEM System
  - Im Widerspruch zu 10 Fordernden, die jeweils ein unterschiedliches System favorisieren
  - Anderer Leute Brot ist Kuchen
  - EIN System kann eh nicht ALLES

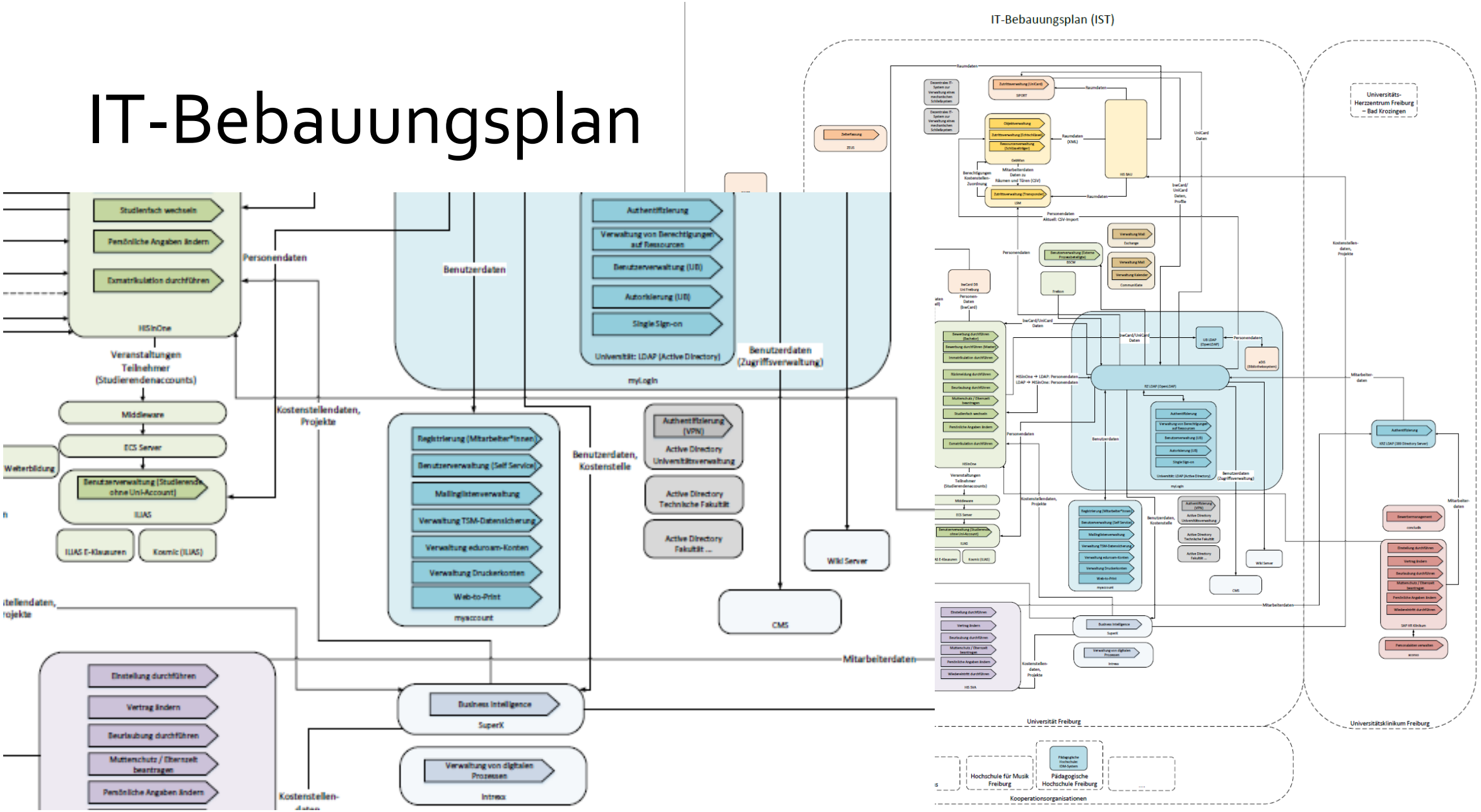
Kernaufgabe der Hochschule

- Wer ist wer – und was darf diese Person? Und wann nicht mehr? Und wie erreicht man sie?
- **Lieblingsthema IDM**
- IDM-Einführung klappt nie – außer wenn ALLE mit dabei sind – was der internen Autonomie widerspricht. Gremienbeschlüsse sind schwierig (umzusetzen)
  - In D gibt's 80 Mio Fussballtrainer – und noch mehr IT-Kundige ☹
  - Entsprechend überladen sind die Wünsche
- Daher: einfach machen – wo haben die Autonomen keine Chance?
  - Ganz früher: email gibt's im RZ (und an ein paar anderen Stellen) – damit kennt man schon viele Nutzer
  - Früher und heute: eduroam-Kennung gibt's nur am RZ
  - Chipkarten für Mensa, Zugangsrechte und Bibliothek
  - Evtl. Prüfungsverwaltung (HISinOne) – ein Grund, weshalb diese in FR ins RZ integriert wurde
  - Damit sind >80% „erwischt"
- Also: dafür sorgen, dass die Dinge so eingeführt/betrieben werden, dass sie zusammenspielen
  - mühsam…. aber wozu hat man am RZ Personal?
    - Persönliches Trauma: Schließsystem innen.

Das ist doch planloser Wildwuchs

- Richtig – aber wie will man planen, was man nicht versteht?
  - „verstehen" in Bezug auf „Umsetzung passend für die eigene Hochschule"
- Erst wenn der Wildwuchs eine gewisse Größe hat, fängt man an zu verstehen
  - Und kann das Problem den Gremien ganz konkret vermitteln
  - Die IT kennt schließlich „2.0"
- Freiburg 2022: Erstellen eines IT-Bebauungsplans
  - Was haben wir denn an Systemen, die irgendwie zusammenspielen müssen?
  - In welchem Bereich ist welches System führend?
  - Zahlreiche Mitarbeiter:innen (auch außerhalb des RZ) verfügen aufgrund von „1.0" über ein erstaunlich/erfreulich hohes Problembewusstsein und diskutieren sehr konstruktiv/zielführend
  - Diese Veränderung auf Mitarbeiter:innen-Ebene ist ein echter **game-changer**
  - die Suche nach dem „broker-system" hat begonnen

IT-Bebauungsplan



Erreichbarkeit

- Verteilerlisten (email ist Old School) lassen sich nun generieren
  - Plötzlich erkennt das Rektorat den Vorteil
  - Und ist gegenüber einem IDM etwas aufgeschlossener
  - ABER: man muss damit auch umgehen können!
    Spitzenleistung: 3 Mails von 3 (Pro-)Rektoren am Freitag Nachmittag
    - vgl Diskussion zur cell-broadcast-Warnung in Lübeck am Sonntag ☺
- Prof. Dr. Dieter Wall († 2010): „es ist alles eine Sache der Organisation"
- Übermittlung vertraulicher Infos: Banken und LBV wissen, wie man das macht
  - Die Information, dass etwas zentral vorliegt, geht an eine genannte Kontaktadresse
  - An manchen Hochschulen Ressourcen für Zwangs-eMail-Betrieb
- Beispiel: Energiepreispauschale für Studis
  - https://www.einmalzahlung200.de/eppsg-de und https://www.bundesregierung.de/breg-de/suche/einmalzahlung-studierende-2143736 und staunen
  - Wie einfach wäre es doch, in HISinONE ein neues Feld für eine Kontonummer anzulegen – wer hier die Kontonummer **freiwillig** einträgt, stellt automatisch einen Antrag und die Daten werden übermittelt
  - Und ganz nebenbei werden für die Hochschule die Kontaktdaten aktualisiert!! Ein 200€ Gratis-Köder hilft mit!!
  - Klar: Studierende an Hochschulen, die das können, sind im Vorteil – na und? So geht Digitalisierung!

E-Learning

- Offiziell heißt es an vielen Hochschulen: es gibt nur ein System
  - Von Webseiten, externen Produkten, Modeerscheinungen, ganz neuen Superlösungen, usw. mal abgesehen
  - Mal die Studierenden befragen….
- In Freiburg wurden über 15 Jahre die Interessierten erschlossen
  - Mit „Händchenhalten", „Klinkenputzen", usw.
  - Personal erst über Projekte aufgebaut, dann tatsächlich von der Uni teilweise entfristet
  - Wirkungsgrad: „wichtige" 20% (i.e. „nur" 20%, aber oft bei den Einflussreichen – *Pareto-Prinzip*)
    - Durchaus 95% der Studierenden kamen mal in Kontakt mit dem System
  - Und dann kam die Pandemie … ☺
- Die Pandemie änderte das Vorzeichen
  - Vom „*muss das sein?*" und „*geht es nicht auch anders?*" zu: „*wo ist eine funktionierende Lösung?*"
- Erkenntnis: wenn man bereit steht, dann kommt manchmal der Erfolg über Nacht
  - Zumal das e-Learning-System voll im IDM integriert war…
  - Und die Anbindung an HISinOne realisiert werden konnte
    - So wie ChatGPT es beschreibt / Realisierung war komplex

Wo liegen eigentlich die Daten?

- Ein Speichersystem?
- Und die Institutsserver, Rechner, Laptops,…?
- wie sicher sind die Daten auf Institutsservern?
  - Diebstahl von Platten / Spionage
  - Admin und Doktorand:in sind erst ein Paar und dann nicht mehr / Sabotage
  - Zentrales Backup war ja mal eine gute Antwort, aber sie reicht nicht mehr
- Aus der Verwaltung: *Strukturierung des Fileservers nach Arbeitsgruppen ist nicht möglich, denn wir arbeiten integriert und müssen alle Daten sehen*
  - Trotzdem wurde strukturiert – als Prof. überlebt man das und die Rache des Systems hält sich in Grenzen
- Zentrale Lösungen erfordern teure leistungsfähige Systeme
  - Da sind die Bastellösungen in den Instituten billiger ☹
- Aber: es gibt überraschende Unterstützung

Forschungsdaten

- Darstellung des Data Life Cycle wird immer öfters in Anträgen gefordert
  - Der frühere Weg

    „Mikroskop → lokaler PC → lokaler Fileserver (vielleicht) → vergessen

    wird immer seltener akzeptiert

- Da ist es hilfreich, wenn ein zentrales System mit organisiertem Workflow nahtlos mit eingebunden ist
  - Workflow-Komponenten:
    - Langfristiges Sicherstellen der Zugriffsrechte
      - IDM hilft mit – wer „erbt" beim Ausscheiden der „besitzenden" Person?
    - Datenentsorgung nach eingestellter Frist
    - Erheben von Kostenbeiträgen für langfristige Aufbewahrung aufgrund erforderlicher Geräteerneuerung (sog. Langzeitarchivierung)
      - Führt bestimmt zur sorgfältigen Feststellung von Aufbewahrungsfristen
    - Funktionale Langzeitarchivierung – Laufzeitumgebungen werden am Leben erhalten
      - Wenn für die Darstellung von Daten gewisse Software nötig ist
    - Weiterleiten der Daten an die passende NFDI-Struktur
      - Die kennen die Wissenschaftler:innen ja selber – aber der Formalkram…
      - Und vielleicht sollte man trotzdem eine Kopie behalten

Deus ex machina – DSGVO+Auskunftsrecht

- Die nette Anfrage: welche Daten hat die Hochschule über mich gespeichert?
  - Noch „besser“: Antrag auf Datenlöschung
- Natürlich ruft da die Rechtsabteilung sofort im RZ an
- Antwort:
  - dank IDM haben wir x,y,z (z.B. einen 240-seitigen Dump aus HISonOne) und auf den Speichersystemen liegen die Directories a,b,c der Person. Im e-Learning-System kann man anonymisieren.
  - Aber was in den Instituten noch so gespeichert ist, wissen wir nicht
- **Panik**… den zweiten Teil der Antwort will die Rechtsabteilung sicherheitshalber nicht hören
- Zum Glück ist der anfragenden Person diese Finesse entgangen
- Nun ist das RZ „im Geschäft“ – endlich versteht man auch ganz oben die Notwendigkeit von IDM (samt den erforderlichen Ressourcen)
  - Der Weg bis zum Geld ist noch weit ☹
  - Vor allem diskutiert es sich nun anders mit den dezentralen Einrichtungen

outsourcing

- Wird oft als Bedrohung gesehen – warum eigentlich?
- Kosten erst mal durchrechnen!!!
  - Inklusiv Organisationskosten und Ausstiegskosten
    - Die PC-Betreuung der Verwaltungs-IT in Freiburg durch den Landesdienstleister LZBW kostet(e) ca. 120.000€ (Listenpreis)
    - **Pro Monat!!!**
  - Blödes Beispiel: Wenn email-notification flächendeckend die Prozesse regiert, ist outsourcing von email vielleicht nicht so clever
  - Wenn eigene Nutzerverwaltung des Outsourcers erforderlich ist, widerspricht das dem IDM-Gedanken
    - FR: SAP wird im MA betrieben (klug!), aber auf das LDAP-Modul wurde aus Kostengründen verzichtet – vollständig eigene Benutzerverwaltung ist die Folge; mit allen Schwächen
  - Grundsätzlich: warum nicht outsourcing zur Unterstützung der eigenen Prozesse heranziehen? Beispiel: Webservice
    - **Der Ablauf muss passen!** Beispiel: Druckeranbindung für SAP war in Freiburg eine echte Herausforderung!
- Interessant sind Störungen – wie neulich bei Microsoft zu beobachten – für Nutzer eine völlig neue Erfahrung
  - Die trauen sich was…. Dass das passieren kann….
  - Hilft dem eigenen Image ☺

Weitere Bausteine der IT-Versorgung

- Telefonanlage VoIP
  - Umzug durch Mitnahme des Apparats – und wie wird das dokumentiert? IDM….
  - Integration der Anlage in ein Alarm/Warn-System?
  - Heutige VoIP-Anlagen bieten auch Konferenz-Unterstützung (Audio, Video, whiteboard)
    - Yet another VK – oder passt das zusammen mit den anderen Bausteinen?
    - Oder schaffen wir sie ab und ersetzen sie durch Handy und MS-Teams?
      - Gegenwehr: **VoIP-Anlage kann auch Handy** einbinden – dies ist nur eine Sache des Mobilfunktarifs
    - Wer kümmert sich um die Handy-Sicherheit? Heißes Thema!!!!!
    - Zugriff auf private Endgeräte (Juristen fragen!) – oder eigenes Dienstgerät erzwingen? Dann viel €€€€-Spass mit der Leitung und den Gremien.
- Homeoffice – wer betreut die Geräte?
  - Oder will man ganz clever Kosten sparen und private Endgeräte zulassen?
- Technisch nicht so spannend, aber organisatorisch – dazu braucht man Verbündete
  - Und die sind vielleicht außerhalb der Hochschule ?!?!

Informations- und IT-Sicherheit

- Wir wissen, dass wir irgendwann angegriffen werden
  - Teilweise bilden wir ja die Hacker selber aus (z.B. Informatik-Studierende…)
- Systeme haben Lücken – das wissen wir auch
  - Das heißt: Updates, Zugriffsbeschränkungen, VPN, 2Faktor,…. erhöhen in der Kombination die Stadtmauer, garantieren aber nicht 100% ☹)
- Also ist ein erfolgreicher Angriff nur eine Frage der Zeit ☹☹☹
  - Das kann man als pensionierter Direktor leicht feststellen und trotzdem ruhig schlafen
- Ansatz (?): Wiederhochfahren neuer Systeme innerhalb kürzester Zeit ermöglichen
- Redundanzen durch Cold Standby
  - Mein Großvater war Lokführer und erzählte mir, dass früher auf jedem größeren Bahnhof eine Ersatzlok unter Dampf mit Heizer und Lokführer bereitstand, für den Fall eines Lokschadens im Betrieb
    - Anheizen einer Dampflok dauert 4 Stunden und mehr
    - Heute sind Ersatzlokomotiven inkl. Besatzung aus Kostengründen abgeschafft. Wenn die Lok kaputt ist, ist sie kaputt.
    - Betriebssicherheit kostet halt Geld.
  - Anderes Beispiel: Bundesbankbunker in Cochem, wo ein kompletter Satz (18 Mrd) von Austausch-DM-Scheinen im kalten Krieg vorgehalten wurde (https://de.wikipedia.org/wiki/Bundesbankbunker_Cochem)

Sicherheit

- Das heißt: Wie können wir das Ersatz-Dampflok-Verfahren in den IT-Betrieb überführen?
- Finden wir die Mittel dafür?
  - Geräte und Software im Cold Standby mit Mitarbeiter:innen, die diese vor Ort im sicheren Umfeld hegen
  - VMs sind nur eine Teilantwort – die VMs könnten schon lange infiziert sein
    - VMs in einem sicheren Umfeld erstellen und dann „sicher" in die Produktion überführen?
- Müssen unsere Kernsysteme (wie HISinOne) wirklich online (und damit angreifbar) sein?
  - Andere/erweiterte Architektur?
  - Gedanke: erreichbar ist nur ein Spiegelsystem, das lediglich die aktuell benötigten Nutzerdaten in realtime erhält und selbst keinen Rootzugriff auf die Daten hat.
    - „Datenbank-Server" reicht dafür nicht
    - Zu häufige Zugriffe durch das „Spiegelsystem" sollten Alarm auslösen
    - Mit guten logfiles ist die Zahl der im Schadensfall zu informierenden Nutzer eingrenzbar.
- Ja, ich weiß – das kostet Geld und Personal und „bringt im täglichen Betrieb nichts" – und die IT-Mitarbeiter fühlen sich an der Arbeit gehindert
    - Homeoffice funktioniert hier nicht

IT-Sicherheit: reagieren, wenn‘s passiert

- Neulich in den Nachrichten: *Sicherheitslücken an Deutschen Hochschulen*
- Uni X in den Rundfunk-Nachrichten….
  - Man fühlt ja mit den Kollegen – und dann steht in der ZEIT:
  - ***Sicherheitslücken bei Hochschul-IT im Südwesten:***
    *Die IT-Infrastruktur der Universitäten X und Y soll einem Medienbericht zufolge zum Teil erhebliche Sicherheitslücken aufweisen. Es sei zwar nicht zu konkreten Hacker-Angriffen gekommen, aber Hacker hätten die Lücken nutzen können, um Daten zu stehlen….. Im betreffenden Fall sei es um eine **externe Webseite** mit Informationen zu einem schon beendeten Gemeinschaftsprojekt der Universität mit einer externen Einrichtung gegangen, teilte die Uni mit. Personenbezogene Daten seien nicht betroffen gewesen, die Seite sei sofort vom Netz genommen worden.*
- Erkenntnis:
  - Die Digitalkompetenz im Journalismus hat **viel** Luft nach oben
  - **Man muss sofort reagieren können** – bei eigenbetriebenen Systemen ist das selbstredend (naja…), bei fremdgehosteten Systemen (Thema outsourcing!) muss in jedem Fall die Prozedur zum schnellen Zugriff dokumentiert sein.
    - Worst case: Passwort hat mein Hiwi, der hat die Uni vor 3 Jahren verlassen und ist nach China zurückgekehrt
  - **Solche Vorfälle sind eigentlich ideal, um den Wildwuchs einzufangen**
    - Kein Prof. glaubt, dass man so selber (bzw. die ganze Uni) in die Schlagzeilen kommen kann. Art. 5 GG hilft da nicht

Zertifizierung

- Ich gebe es zu: anfangs war ich ziemlich skeptisch
  - Schaffen wir das überhaupt mit unseren universitären Prozessen?
  - Erkenntnis: man muss den Blickwinkel (Scope) einschränken auf das, was man beherrscht
    - Sehr hilfreiche Infos der Kollegen der FH Wildau
  - Hier „Informationssicherheit im Maschinensaal 2“
- Erkenntnis:
  - Interne Prozesse dürfen nicht mehr der Lust von (engagierten) Mitarbeitern folgen
  - Druckmittel gegenüber Geldgebern: *wenn die Pappwand nicht ausgetauscht wird, verlieren wir unsere Zertifizierung*
  - Hilfreich bei Drittmittelanträgen, insbesondere von Antragstellern, die im Maschinensaal Geräte untergebracht haben
  - Schadet auch nicht bei eigenen 91b-Anträgen
  - *Ich hab was, was Du nicht hast*

TÜV SÜD Management Service

ZERTIFIKAT

Die Zertifizierungsstelle
der TÜV SÜD Management Service GmbH
bescheinigt, dass das Unternehmen

Albert-Ludwigs-Universität Freiburg
Hermann-Herder-Straße 10
79104 Freiburg im Breisgau
Deutschland

für den Geltungsbereich

Operativer Betrieb der Ressourcen
im Maschinensaal II des Rechenzentrums

ein Informationssicherheitsmanagementsystem
gemäß „Erklärung zur Anwendbarkeit“ eingeführt hat und anwendet.

Durch ein Audit, Auftrags-Nr. **707140058**,
wurde der Nachweis erbracht, dass die Forderungen der

DIN EN ISO/IEC 27001:2017

erfüllt sind.

Dieses Zertifikat ist gültig vom **14.12.2021** bis **13.12.2024**.

Zertifikat-Registrier-Nr.: **12 310 63230 TMS**.

Version der Erklärung zur Anwendbarkeit: **03.11.2021**.

Leiter der Zertifizierungsstelle
München, 15.12.2021

TÜV SÜD Management Service GmbH • Zertifizierungsstelle • Ridlerstrasse 57 • 80339 München • Germany
www.tuev-sued.de/certificate-validity-check

TÜV®

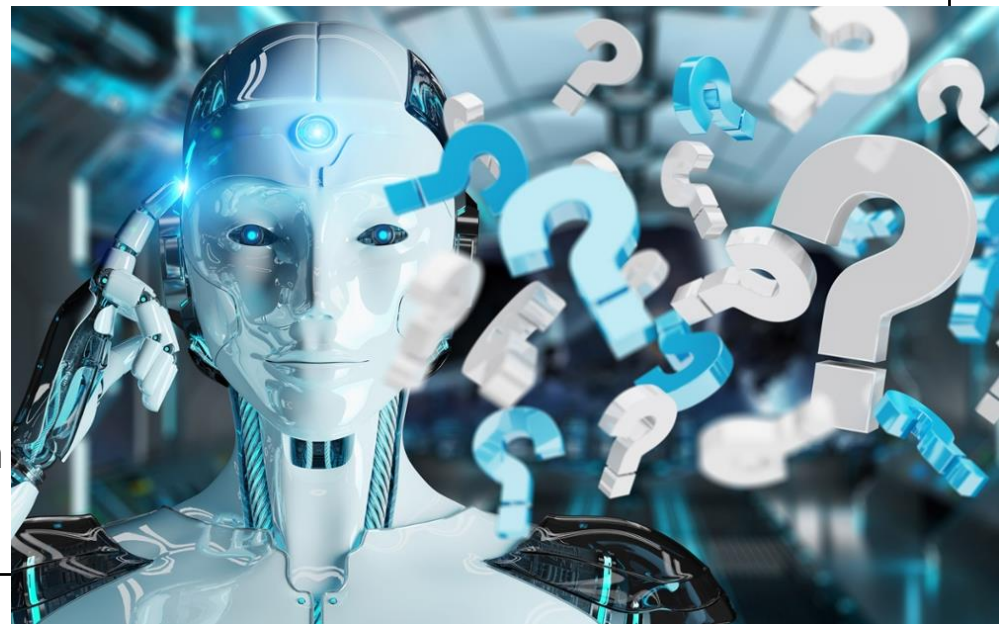
Zertifizierungen

- Sehr hilfreich bei Diskussionen um dezentrale Fileserver
  - Nicht ausrotten – aber intelligent einbinden (siehe FDM)
  - Nutzer stellen ihre Server ins RZ (bzw. kaufen Speichererweiterungen des RZ-Systems) und **unterwerfen** (!!!) sich den Zertifizierungsanforderungen!!
    - Gegen die gleichlautenden RZ-Anforderungen wurde immer diskutiert

- Warum nicht in anderen Sektoren auch mal versuchen?
- In Freiburg gibt's 16 Prüfungsämter. Nach Zertifizierung der Geschäftsprozesse vielleicht nur noch ε. Nur so als Idee…
- Die Erfahrung war wirklich: Zertifizierungen zeigen die Schwächen der eigenen Geschäftsprozesse auf.
  - Das hat nichts mit IT-Inkompetenz zu tun!
  - Viele Schwächen kennt man ja, kann sie aber aufgrund von Befindlichkeiten nicht abstellen

Was machen wir mit der KI?

- Die nächste Herausforderung!
- Beispiel: Chat GPT als Auskunftssystem? Als Formulierungssystem für RZ-Anleitungen?
  - Traum (?): die vom Nerd geschriebene, fachlich perfekte, aber unverständliche Anleitung wird mit Chat GPT und deepL plötzlich schön und mehrsprachig
    - "Klauen" bei befreundeten RZs wird vielleicht produktiv möglich… ☺
    - Bei Texten und vielleicht auch bei config-Skripten/config-APPs ??
    - Im RZ bei allen nicht-kreativen, repetitiven Standardprozessen?
  - Gewinnt man damit im RZ menschliche Ressourcen für andere Aufgaben?
  - z.B. für: wie bindet man KI-Systeme in die IT-Versorgung sinnvoll ein?
    - Bei den e-Learning-Systemen? Wo noch?
    - Bei der Analyse von Logfiles zum Erkennen von IT-Einbrüchen



Zusammenfassung

- Monokultur ist schädlich – und eh nicht zu verwirklichen – „**das eine System**“ ist *fake news*
  - HIS, SAP, Microsoft, eLearning sind alle erforderlich und im **Zusammenspiel** die Treiber der IT-Versorgung/Digitalisierung
- Konzeptionell die Schwerpunkte finden und mit den geeigneten System bedienen
- Durchsetzen, dass diese allgemein genutzt werden
  - Durch *order von oben* (falls es geht….)
  - Durch Honig…. (Nutzung spart Arbeit oder bringt Vorteile)
  - Durch **Instrumentalisierung der Gesetze und Vorschriften**
    - Diese richten sich ja nicht nur „gegen“ das RZ – sondern treffen alle – auch wenn der DSB bei der Dezentrale oft kneift ☺
- und dann die Übergange **hindernisarm** gestalten
  - z.B. Login einheitlich, Daten werden bei Bedarf herangezogen (anders als bei der Grundsteuer)
- und ggfls. **hindernisarme** Einbeziehung der Möglichkeiten des Outsourcings
- Irgendwann ist der Wechsel von „*das hamma noch nie so gmacht*“ zu „*das hamma schon immer so gmacht*“ vollzogen

  integrierte IT-Versorgung = orchestriertes Zusammenspiel der Komponenten
- RZ dirigiert (hoffentlich (mit))! Und die Arbeit geht uns nicht aus..

Enttäuscht???

Weisheit zum Schluss

Die ewige RZ-Gretchenfrage:

Spielen wir auf dem falschen Spielplatz?

Anders gesagt:

Machen wir das, was uns voranbringt?

oder

Klammern wir uns am Betrieb der althergebrachten Systeme fest?