Standortübergreifende Sicherheitskonzepte

Gerhard Schneider

direktor@rz.uni-freiburg.de

Albert-Ludwigs-Universität Freiburg

UNI FREIBURG

Definition

- Was heißt hier „Standort“-übergreifend?
  - Übergreifend = mehrere Standorte oder „einen einzigen überspannend“?
  - RZ – eigene Standorte?
  - oder „RZ und Verwaltung“?
  - oder „RZ für die Uni“?
  - oder Kooperationen zwischen Hochschulen (mit/ohne RZ)?
  - Kooperationen zwischen Rechenzentren?
  - Landesinitiativen?
- Wer regelt was?
- Brauchen wir das überhaupt?
- **Schlechte Nachricht: keine Lösungen, nur Ansätze**

Sicherheitskonzepte in der Uni

- Internet kommt aus der Wissenschaft
  - Völlige Freiheit ist notwendig – wir wissen nicht, auf welche Gedanken die Anwender kommen
  - Die Anwender beherrschen ihre Systeme, das RZ ist eher lästig
- Universitätsnetze sind offen – volle Teilnetze des Internet
  - Muss so sein… wirklich??
- Wer entwirft Sicherheitskonzepte?
  - Niemand…
  - Der Admin
  - Mit welcher Berechtigung?
    - Aus bester Absicht, ohne Rückendeckung

Sicherheitskonzepte in der Uni

- Wie sind sie dokumentiert?
  - Nirgendwo ☺
  - Vielleicht im Kopf des Admin…
    - Unauffällig, keine Diskussionen
- Wie werden sie durchgesetzt?
  - Über die Macht des Admin
- Beispiel Freiburg:
  - Bereits 2003 „neues Konzept“ in Hauszeitung beschrieben: Gefährdete Bereiche bekommen ein 10er-Netz
    - Nur auf dem Campus „sichtbar“
  - kritischere Bereiche erhalten nicht geroutetes 10er-Netz
    - selbst für Firewall, etc. zuständig
  - Erfolg: „mittelprächtig“, inzwischen akzeptiert
    - *„hammer scho immer so gmacht“*

Sicherheitskonzepte in der Uni

- Die neuen Benutzer…
  - IT-Amateure, aber IT-Anwender (immer unter Arbeitsdruck)
  - Mit gewissen Vorstellungen
    - Halbwissen, um sich ihre Arbeit zu erleichtern ☹
  - Gestählt beim Einsatz von Ellenbogen
    - Ich will oder ich geh‘ zum *Rektor*
      - Damit ist ein Admin üblicherweise überfordert
  - *Rektor* hat selber Vorstellungen
    - Nicht sonderlich sicherheitskonform – er/sie kommt aus der Wissenschaft
- Sicherheits-Harakiri
  - Admin versucht, die widersprüchlichen Anforderungen abzubilden – unlösbar
  - Im Schadensfall gibt es nur einen Schuldigen

Bedrohungen mit Pressewirkung

- Allgemein bekannt:
  - Verwaltung hat personenbezogene Daten, also Firewall
    - Zurück auf „Los“: wer definiert die Regeln??
  - Neu: Wartungsnetze des technischen Gebäudemanagements
    - Forderungen: möglichst einfach, umfassend, bequem für die Mitarbeiter, Zugriff von zu Hause, bitte mit Privatgerät, usw
    - Bittere Erkenntnis: auch Firmen führen Wartungs- und Konfigurationsaufgaben mit ungesicherten Laptops durch
      - Stuxnet war nur der Anfang
      - Wir hatten bereits Virenbefall durch Firmen
- Szenarien:
  - Angriffe militanter Tierschützer auf die Tierställe
  - Abschalten der Tiefkühltruhen mit echten Viren

Löcher im Käse – aus der Praxis

- Neue Solarpanels sollen zu Management- und Werbezwecken Daten liefern
  - System muss ans Internet
    - Naja, ok – leider hat bei den Planungen niemand bedacht, dass der Aufpunkt hinter massiv Firewall-geschützten Bereichen ist.
    - Das RZ soll das lösen, woanders sei das auch kein Problem
  - Die Probleme von **Industrie 4.0** können wir noch nicht mal erahnen
    - Hacker‘s dream
- Mit Patchwork-Security werden wir nicht zum Ziel kommen!

Erkenntnis

- Man muss sie mit ihren eigenen Waffen schlagen!
- Formalismus nötig !!
  - Admin: ist doch „Schwarzer Peter Spiel“ ☹
- Nur festgezurrte Regeln haben eine Gültigkeit
- Freiburg: 1. Schritt – IT-Richtlinie für die Verwaltung
  - Im Rektorat beschlossen, dabei nette Diskussionen:
    - „ich bekommen doch immer wieder USB-Sticks“
    - „die Cloud-Lösungen auf meinem iPad sind so praktisch – das RZ muss sowas für die Verwaltung anbieten!“
    - Spassfaktor: Juristen die rechtlichen Regeln „erklären“
  - Weitere Dokumente sind in Vorbereitung
    - Nötig: jemand, der schreiben kann ☺

Kooperationen der UBs

- ReDI
  - Kooperation/Konsortium der Bibliotheken in Ba-Wü
  - Wer darf die elektronischen Zeitschriften nutzen?
  - Sicherheit bei Nutzungsfragen – ein IT-Zugangsproblem!
- Zentralisierung des Bibliothekssystems in TÜ
  - Zugriff auf den zentralen Server aus allen Teilen des Landes
  - Wie ist der Gesamtkomplex abgesichert?
    - Datenaustausch, Zugriff, Datensicherheit?
- Zugang zu einer 24x7 Bibliothek
  - Aufgabe der UB – oder eines Gesamtkonzepts

Kooperationen mit und ohne RZ - SAP

- SAP-Server stehen in MA, FR nur Client
  - Gemeinsames Projekt! ☺
  - Sicherheitsfragen von SAP-Consultants nur sehr unzufriedenstellend angegangen
  - RZs nicht befragt
  - Plötzlich Panikanrufe: wir brauchen…
    - Keine Frage: wie passt das ins Sicherheitskonzept

    Die notwendige Infrastruktur schon seit 12 Jahren

    wenn man nachdenkt – und nicht „fordert“
  - Neue Anforderungen: Direktzugriff von TÜ nach FR
    - Wieso? Die Server stehen doch in MA
    - Diskussion sinnlos, Sicherheitskonzept unterminiert

Eigenes IDM

- Campus-übergreifende Sicherheit
  - Wer darf eigentlich an der Uni etwas tun?
    - Die Verwaltung kennt sie alle!
  - RZ-Account mit vielfältiger Nutzung
    - WLAN, UB-Ausleihe, Notenabfrage, usw.
  - Unicard: eine Karte für alle Zwecke – seit 2000 – Mifare☹
    - Mensa, Schließanlage, ÖPNV, Stechuhr
  - Synchronisieren der Nutzer-Datenbanken
  - Plötzlich: wir können Nutzer „zuverlässig“ ausschließen
    - Beim Ausscheiden, etc
- Zentrifugalkräfte nur via Service-Konzept einfangbar
  - Beschlüsse können erst erwirkt werden, wenn etwas akzeptiert ist. RZ muss loslegen; irgendwann kommt der Punkt.

bwIDM

- Eduroam: eigener Account funktioniert überall
- Sowas auch für Landesdienste?
  - Idee: Tübinger Nutzer auf Karlsruher Rechner ohne Verwaltungsaufwand
- Mehr Organisation als Technik
  - Shibboleth, LDAP
  - Abgleich der lokalen Anforderungen gegen die fremde Nutzerverwaltung
  - **Vertrauen** in die fremde Verwaltung (RZ-untypisch)
- Überraschende Erkenntnis: jeder braucht ein IDM
  - keine zentrale Lösung für alle
  - Typisches Beispiel von balanciertem zentral/dezentral

Erkenntnis

- Je mehr eine Nutzerverwaltung leistet, desto besser passen die Nutzer auf ihre Zugangsdaten auf.
  - Deutliche Einsparungen auf Uni-Seite, weil Nutzerverwaltung an vielen Stellen überflüssig wird.
  - RZ erhält dafür leider nichts, hat mehr Arbeit.
- Sicherheit steigt – die lokale Institution weiß meist besser Bescheid
  - Vagabundierende Rechte an anderen Einrichtungen werden zuverlässig eingezogen
  - Lokale Einrichtungen ordnen sich unter
    - Weil sie die Einsparmöglichkeiten erkannt haben

Nutzungskonzepte HPC

- High Performance Computing:
  - Das Land Ba-Wü stellt für die Wissenschaft die entsprechende Infrastruktur bereit
  - Neu: Schwerpunktbildung!
    - UL: Chemie
    - FR: Neuro, Teilchenphysik
    - KIT: Grundversorgung, Rest

    TÜ: Astro, BioInf

    HD/MA: SoWi, Medizin
- Jede Einrichtung schaltet ihre Nutzer für die HPC-Rechner des Landes frei
  - Keine Beantragung beim Ressourcenbetreiben - ungewohnt
  - Heftige Diskussion bei Mitarbeitern, wer denn darf
- Und übernimmt somit die Verantwortung
  - Problem: Schurkenstaaten… Haftungsfragen – noch ungelöst
  - Alternativen? Keine (bzw. Bürokratie, die zu bezahlen ist)

Rechtsstudie

- Was ist eigentlich zu beachten, wenn RZs kooperieren?
  - A betreibt den Server am Standort B
    - Beispiel: HD betreibt TSM in FR
  - A nutzt den Service des Zentrums B
    - Beispiel: KN sichert Daten in TÜ
  - A bietet einen Service für alle
    - Beispiel: KIT betreibt bwSync&Share mit bwIDM
- Fragen: Auftragsdatenverarbeitung, MWSt., Gremienbeteiligungen, Leistungsverrechnung
- Einheitliches Vorgehen für alle RZs als Ziel
  - Vereinfachte Vertragsgestaltung, Rechtssicherheit, Rad nur einmal erfinden, ZENDAS

Landesprojekt AGITSEC

- Wenn wir „treiben“ wollen, müssen wir arbeiten
  - 9 Unis stellen je einen Mitarbeiter in die AG, MWK finanziert je einen zweiten (2Jahre)
    - Nachhaltigkeit über den ersten Mitarbeiter gesichert
  - Erarbeitung von Sicherheitskonzepten
  - Prototypische Installationen mit Berücksichtigung der Erfordernisse der Wissenschaft
    - Diese sind zu beschreiben
    - Dann sind wir abgesichert im Problemfall
      - Denke an den aktuellen Bundestags-Angriff
- Nur bei gemeinsamen Konzepten lässt sich der Schweizer Käse bei den Firewalls vermeiden

Fazit

- Die Zeit der Gurus ist lange vorbei
- Heute regieren andere
  - Und die IT muss sich rechtfertigen
- Formale Prozeduren schützen
  - Wichtig: das RZ muss Triebfeder sein, nicht Spielball der anderen.
- Kooperationen nützen und schützen
  - Nutzen: Synergieeffekte
  - Schutz: wenn andere Standorte von einem abhängen, kann dieser nicht so leicht geschlossen werden
    - Vorteil der „inneren Linie“
- Sicherheitsfragen treiben die strukturelle Entwicklung
  - Sehen wir das doch positiv!