FAU

CISO Sprechstunde

05.11.2025

Aktuelles aus der FAU

Aktuelles

News

1. CIO Gremium beschließt flächendeckende Einführung von 2FA
   EUL trägt Entscheidung mit

   To Do:
   - Technikgestaltung (VPN, SSO, Mail)
   - GPR einbinden
   - Kommunikations- und Zeitplan erstellen
   - Kosten- und Aufwandsschätzung
   - EV für UL

IT Krisenstabsübung

Am 20.11.2025 findet die nächste IT-Krisenstabsübung statt

– Diesmal als Blaupause mit HITS IS entwickelt und für alle Bay. Hochschulen

– Erstmalig mit externen Incident-Managern (EY)

Informationssicherheitsmanagementsystem (ISMS)

Audit durch HITS IS

HITS IS: „Sicherste Uni in Bayern“

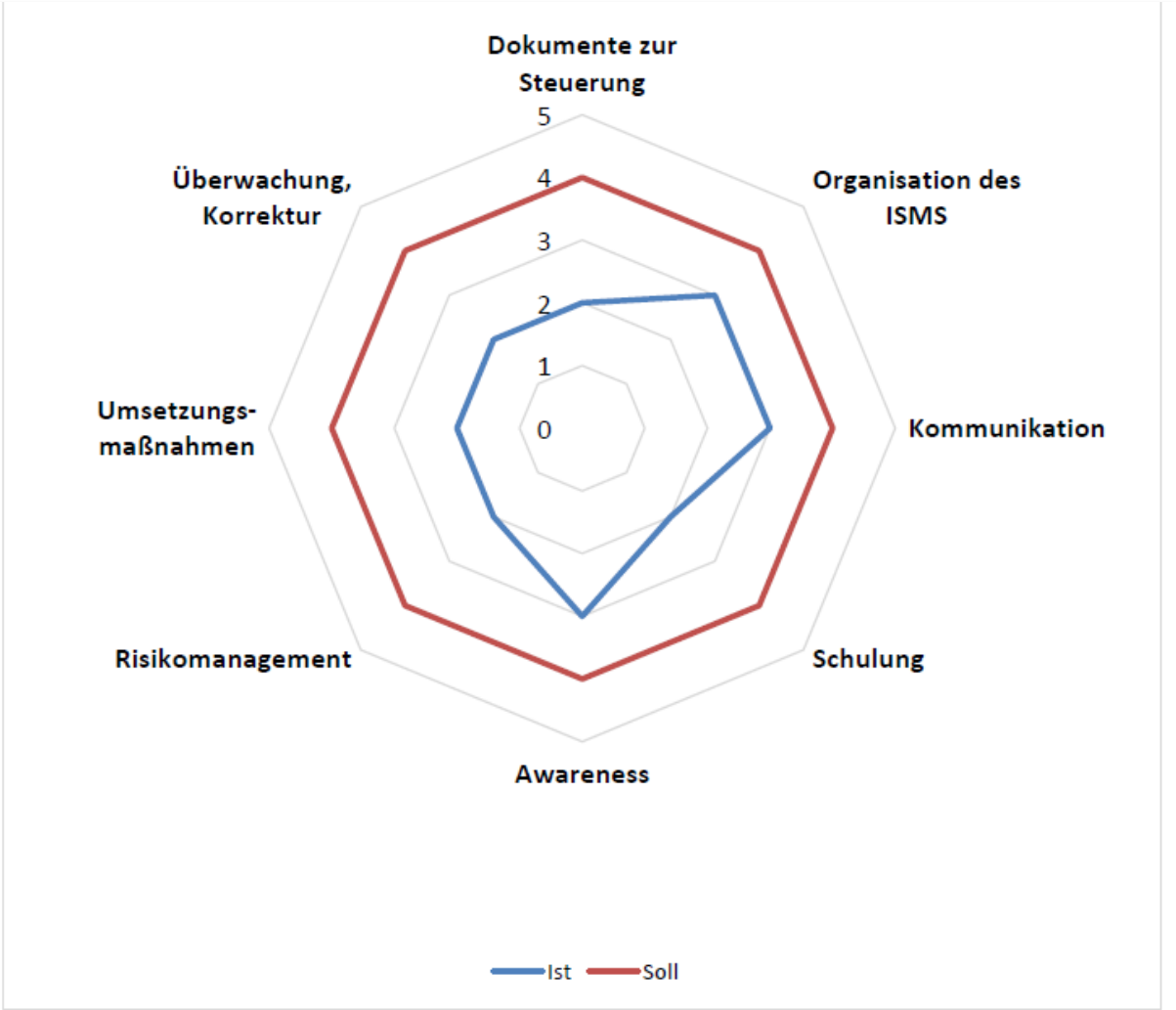


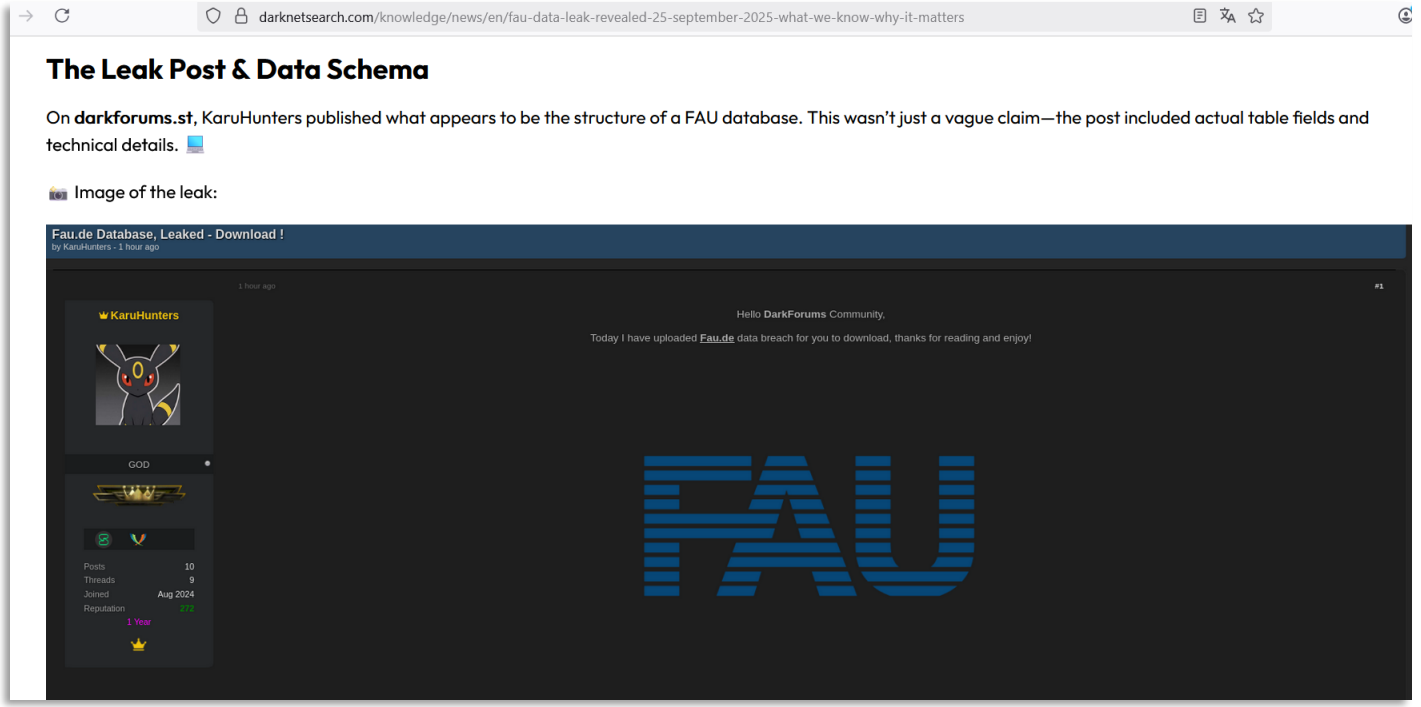
Abbildung 2: Reifegrad des HISP

Herausforderung

Datenleck auf „Eckpfeiler für den wissenschaftlichen Erfolg“

- Internetsystem mit alter Software (Betriebssystem EOL, Middleware & Apps veraltet: CMS, PHP)
- Inadequate Systemarchitektur: Webserver, Datenbanken, Fileserver, externe Anmeldungen usw. alles auf einem einzigen Server im Internet
- Verstößt gegen FAU-Regelungen und DSGVO

Leider kein Einzelfall!



Internetsysteme ohne Pflege!

- **WICHTIG:** Halten Sie bitte Ihre SW aktuell!
- End of Life (EoL) SW/Betriebssysteme liefern gravierende Schwachstellen

- BSI meldet aktuell:
  80 neue CVS-Schwachstellen pro Tag
  davon
  10% Zero Day mit CVSS 9 pro Tag

Der **CVSS-Score** bewertet, **wie gefährlich** eine Sicherheitslücke ist:

CVSS-Bereich	Schweregrad	Bedeutung
0.0 – 3.9	Niedrig	Geringes Risiko
4.0 – 6.9	Mittel	Eingeschränkt ausnutzbar
7.0 – 8.9	Hoch	Gefährlich
9.0 – 10.0	**Kritisch**	**Sehr gefährlich – oft Remote Code Execution, Privilege Escalation oder keine Authentifizierung nötig**

CVS: Common Vulnerabilities and Exposures
CVSS: Common Vulnerability Scoring System

Trennung der Systeme

1. Frontend (Webserver), Applikationsserver und DB-Server sollten physisch oder logisch getrennt sein

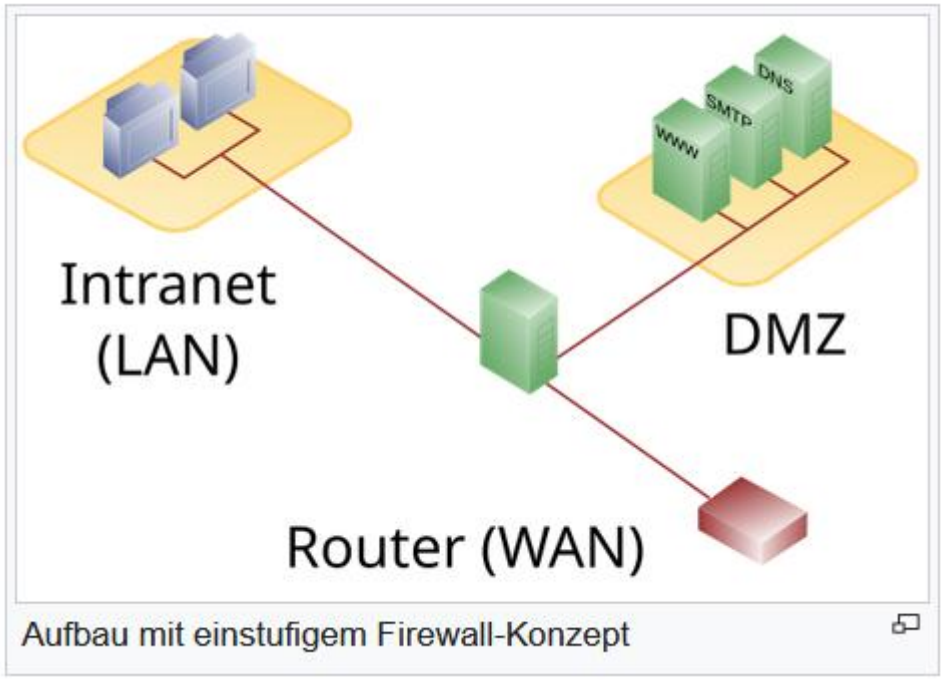
2. Nutze DMZ (Demilitarized Zone)-Konzepte:
   - Öffentlicher Webserver steht in einer DMZ
   - Applikations- und Datenbankserver stehen im internen Netz
   - Nur notwendige Ports werden zwischen den Zonen geöffnet (z. B. 443 für HTTPS, 3306 für MySQL-Verbindung nur intern)

⚖️ Vergleich: DMZ vs. NAT

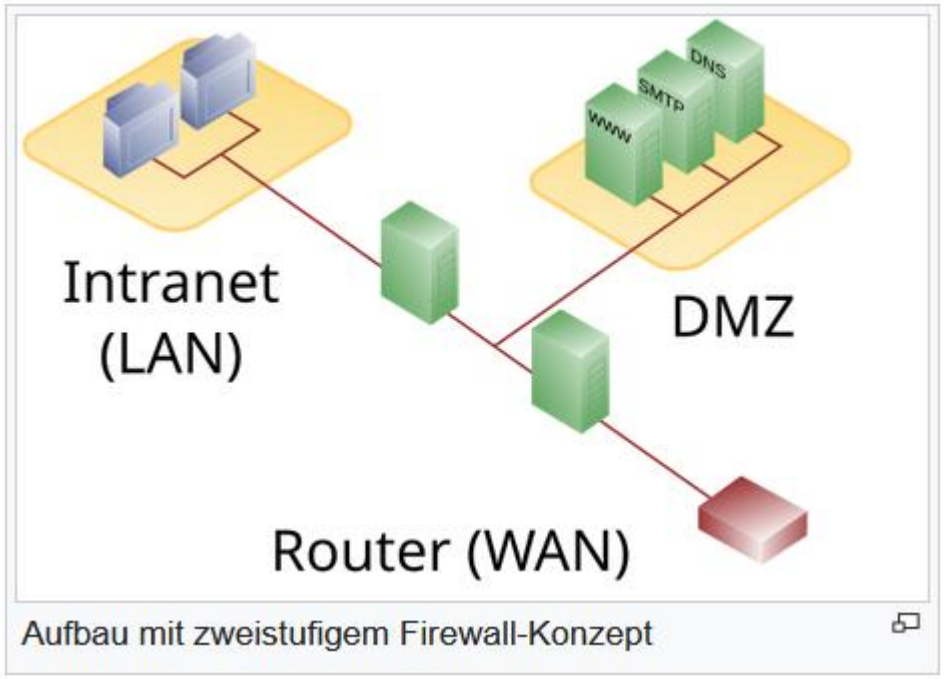
Merkmal	NAT	DMZ
Hauptzweck	Adressübersetzung	Sicherheitssegmentierung
Schützt interne IPs	✅ Ja	✅ Ja (durch Segmentierung)
Filtert oder kontrolliert Datenverkehr	❌ Nein	✅ Ja (über Firewalls)
Schutz bei kompromittiertem Server	❌ Kaum	✅ Hoch
Komplexität	Einfach	Mittel–hoch
Bestandteil eines sicheren Netzwerks	Basisfunktion	Sicherheitsarchitektur

3. Setze einen Reverse Proxy (z. B. NGINX, HAProxy) oder eine Web Application Firewall (WAF) davor, um Angriffe (z. B. SQL-Injection, XSS) abzufangen, SSL/TLS zu terminieren, Zugriffe zu protokollieren

DMZ - Demilitarisierte Zone



Aufbau mit einstufigem Firewall-Konzept



Aufbau mit zweistufigem Firewall-Konzept

Quelle: Wikipedia

RRZE Services

RRZE-Services **zur Verbesserung der Informationssicherheit Ihres Lehrstuhls**

https://www.services.rrze.fau.de

https://www.rrze.fau.de/infocenter/preise-kosten/

https://www.rrze.fau.de/infocenter/preise-kosten/kostengruppen/

FAUAD

FAU Active Directory

Zentrale Verzeichnisse und Rechtemanagement

Aufgabe	Beschreibung
Benutzerverwaltung	Erstellen, löschen und verwalten von Benutzerkonten (z. B. Mitarbeiter, Administratoren)
Rechteverwaltung	Festlegen, wer auf welche Ressourcen (Ordner, Drucker, Anwendungen) zugreifen darf
Zentrale Authentifizierung (Single Sign-On)	Benutzer melden sich **einmal** an (z. B. am PC) und erhalten Zugriff auf alle freigegebenen Dienste
Gruppenrichtlinien (GPOs)	Automatische Konfigurationen für Computer und Benutzer (z. B. Passwortregeln, Desktop-Einstellungen).
Computer- und Serververwaltung	Jeder Computer im Unternehmen kann im AD registriert und zentral gesteuert werden.
Ressourcenverwaltung	Drucker, Laufwerke, Server usw. können zentral im Verzeichnis gefunden und genutzt werden.

Soft- und Hardware

Netzwerk und Softwaretechnik

Netzwerktechnik

Windows-Softwareverteilung

Netzwerktechnik
Support bei ihrer Netzanbindung

Zum Beispiel:
- Einrichtung und Betreuung von LAN-Anschlüssen im Institut
- WLAN-Versorgung für Lehrstuhl und Veranstaltungen
- VPN-Zugänge für Homeoffice und Reisen
- Beratung bei der Netzwerkintegration neuer Labore
- Unterstützung bei Störungen

Windows-Softwareverteilung
WinSV installiert und aktualisiert lehrstuhlübergreifend Windows-Rechner automatisiert und konsistent.

Sonderprojekte nach Aufwand

Daten

Speicherplatz und Archiv

https://www.rrze.fau.de/infocenter/preise-kosten/kostengruppen/

Speicher mit Datensicherung

Speicher und Datensicherung

Speicherplatz im BasisStorage mit täglichem Backup, DSGVO konform
Kosten: 150 GB pro Person frei;
danach kostenpflichtig (ab ca. 1,50€/TB/Monat, je nach Kostengruppe)

- Z.B für zentrale Datenablage für Forschungsprojekte (ermöglicht gemeinsame Nutzung von Messdaten, Skripten und Auswertungen), automatisches Backup und Wiederherstellung bei Datenverlust.
  Skalierbar von 100 GB bis mehrere TB

Backup und Archivierung – Kosten Backup: ab 0,01€/GB/Monat;
Archiv: ab 1€/TB/Monat

- Tägliches Backup und Archivierung für Langzeitspeicherung von Servern und PCs, Wiederherstellung (inclusive versehentlich gelöschter Dateien), langfristige Archivierung von Projektdaten nach Projektende, mit revisionssicherer E-Mail-Archivierung

➔ verlässlicher Schutz vor Datenverlust, einfache Wiederherstellung auf Datei- und Systemebene, rechtssichere und langfristige Datenaufbewahrung

Schulungen, Beratung, Unterstützung

Client Support

Teilweise kostenfrei

IT-Schulungszentrum:

- Praxisnahe IT-Kurse und Admin-Trainings für Beschäftigte und Studierende), Weiterbildung für wissenschaftliche Mitarbeitende (z. B. Datenanalyse, Git), Kurse für sichere Arbeit mit sensiblen Daten, Trainings für Tools (z. B. Word, Excel, Citavi)
- **Kosten** ab ca. 35€/Kurs für Beschäftigte (meist kostenlos für Studierende)

IT-Betreuungszentren: Client-Betreuung

- Vollständige Betreuung von Arbeitsplatzgeräten inkl. Hotline, Pflege und Lifecycle-Management.

IT-Betreuungszentrum Süd (IZS) befindet sich direkt am FAU Campus Erlangen Süd

- Verwaltung und Pflege von Büro-PCs, Notebooks und Druckern. Vertretung des Lehrstuhl-Admins, standardisierte Einrichtung neuer Geräte, regelmäßige Updates und Sicherheitsprüfungen. Entlastung des Lehrstuhls von Routineaufgaben, schneller Support durch feste Ansprechpartner, einheitliche Geräte- und Softwarestände
- **Kosten** 21€/Gerät/Monat; optionale Pakete (z. B. Ausstattungspauschale für 30€/Gerät/Monat)

RRZE-Helpdesk

- Die zentrale Anlaufstelle für alle IT-Fragen, Störungen und Serviceanfragen an das Rechenzentrum. Er bietet Erste Hilfe bei allen IT-Problemen am Arbeitsplatz, Anlaufstelle für Fragen zu RRZE-Diensten, Unterstützung bei der Bestellung von Services, Koordination und Weiterleitung an Spezialisten innerhalb des RRZ. Er fungiert als zentraler Kontaktpunkt statt verstreuter Ansprechpartner, schnelle Reaktionszeiten und klare Prozesse, kompetente Auskünfte zu allen RRZE-Services
- **Kosten** kostenfrei für alle FAU-Angehörigen

Was können wir für Sie tun?

Ihre Fragen?

Ihre Wünsche?