ATHENE Cybernation Deutschland

Sicherheit der IT der Universitäten 1/5

Zusammenfassung und resultierende Empfehlungen der Datenerhebung 2023-25 zur externen Angriffsoberfläche der 92 Universitäten in der HRK

Wachsende Angriffsfläche

Unis sind größter Digitalsektor. IT wird vorwiegend selbst betrieben. Wachstum in Diensten seit 2023 ca. 10%. Extern betriebene IT – Dienstleister, Cloud, Hyperscaler – wachsen überprportional, vorwiegend in den USA.

→ Hauptlast des IT-Managements liegt bei den Unis. Abhängigkeit von den USA steigt.

Hosting Modelle

Selbstbetriebene IT	80% +/-
Externe Dienstleister	20% +
Cloud	<0,5% ++

aws, Google Cloud Platform, Azure, ORACLE, OVHcloud

Cloud und Externe sind vorwiegend US-Unternehmen.

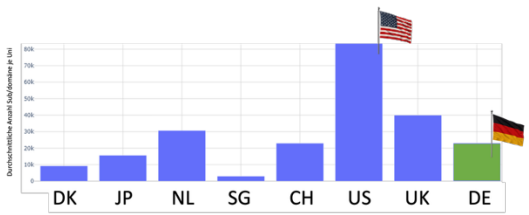
Große Varianz in der Größe

Größe der Unis nach Anzahl der IT-Dienste	Große Unis	Median
9 Groß (≥ 50k)	>1400 Domänen	184 Domänen
52 Mittel (10k - 50k)	>60K Dienste	20K Dienste
31 Klein (< 10k)		

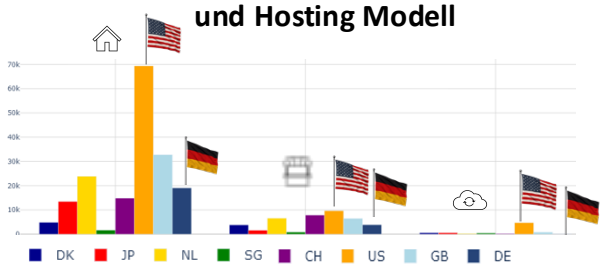
Gewisse Varianz zwischen alten und neuen Bundesländern

West	Ost
236 Domänen	227 Domänen
24K Dienste	18K Dienste
23% Extern	10% Extern
<0,5% Cloud	<0,5% Cloud

Mittlere Anzahl Domänen je Uni



Mittlere Anzahl Domänen je Uni und Hosting Modell



Internationaler Vergleich

- Deutsche Uni-IT ist nicht global die größte.
- DE Uni-IT: mehr Kontrolle über den Standort & weniger international verteilt.
- Weltweit haben Unis sehr große extern sichtbare IT-Landschaften.
- Überall dominiert selbst betriebene IT.
- Cloud noch gering, mit Ausnahme USA.

→ Überall finden sich ähnliche Probleme.

Prof. Dr. Haya Schulmann (haya.schulmann@athene-center.de)

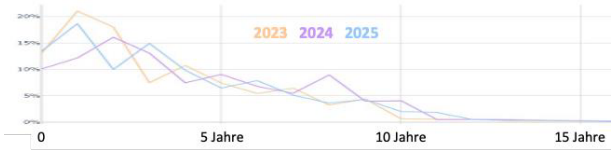
ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Universitäten 2/5

Wie verändert sich die Verwundbarkeit der deutschen Unis?

Wie lange bleiben Schwachstellen offen?



Offene Schwachstellen an Unis (%) nach Alter

Schwachstellen lange ungepatcht

- Ca. 75% aller offenen Schwachstellen sind älter als 1 Jahr.
- Dank ausführbarer Exploits sind diese besonders leicht für Angriffe ausnutzbar.

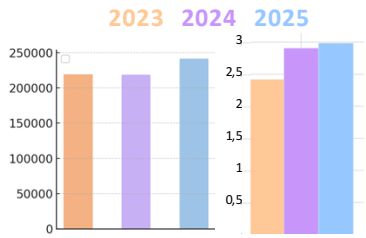
Was läuft, das läuft

- Viel vergessene IT ohne Wartung: Alte Projekte und Labore, selbstentwickelte SW.
- Viele Systeme laufen auf nicht mehr unterstützter Software.
- Anzahl ausnutzbarer Schwachstellen steigt.

→ Angriffsfläche altert, Verwundbarkeit nimmt zu. Modernisierung hält nicht Schritt.

Dienste mit bekannten Schwachstellen

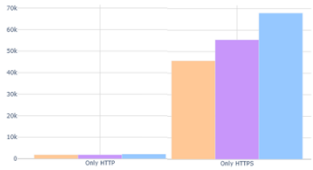
Fortschritte bei einzelnen kritischen CVEs. Insgesamt wächst die Angriffsfläche: Absolute Zahl und End-of-Life (EoL) nehmen zu



#Schwachstellen über alle

% EoL per Dienst

Verschlüsselung nimmt zu



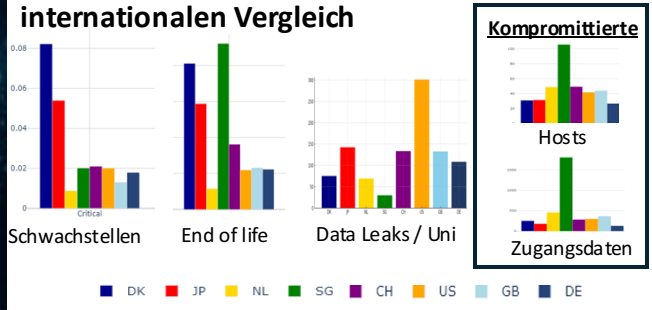
Zahl der Login Seiten ohne (Li) und mit (Re) Verschlüsselung

Anteil der Seiten ohne Verschlüsselung nimmt ab, absolute Zahl sinkt allerdings nicht unbedingt.

Defaults werden sicherer

- Verbesserung resultieren vorwiegend aus Fortschritten und Automatisierung bei Herstellern und Plattformen.
- IT-Standards der Hersteller werden besser, die operative Umsetzung der Uni bleibt aber hinter dem Wachstum und der Komplexität ihrer IT zurück.

Durchschnitt je Universität im internationalen Vergleich



International bewegen sich Deutsche Unis im Mittelfeld

- Überall gibt es Schwachstellen und Kompromittierungen.
- Andere Länder oft deutlich problematischer.
- DE betreibt sehr viel selbst, on-prem, wenig Cloud und große Inlands-IT-Landschaften.

Prof. Dr. Haya Schulmann (haya.schulmann@athene-center.de)

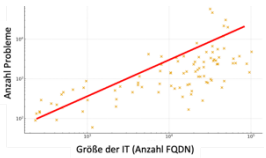
ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

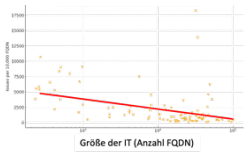
Sicherheit der IT der Universitäten 3/5

Welche Faktoren beeinflussen die (Un-)sicherheit?

Skalierung hilft



Größe Uni X Anzahl Schwachstellen



Größe Uni X Dichte Schwachstellen pro aktivem Dienst

Professionalität:
Geringste Dichte der Verwundbarkeiten
Auswahl: Alle Bundesländer mit mehr als 5 Unis

Angriffsfläche:
Geringste Anzahl an Verwundbarkeiten
Auswahl: Alle Bundesländer mit mehr als 5 Unis

Positive Faktoren: Größe, Zentralisierung, Konsolidierung, Automatisierung

Je größer die gebündelte IT-Einheit, desto mehr Professionalität; je zentraler die Verantwortung, desto weniger Chaos; je konsolidierter die Systemlandschaft, desto kleiner die Angriffsfläche.

- Anzahl Schwachstellen wächst mit Größe, ihre Dichte (Schwachstellen je Dienst) sinkt aber.
- Unis mit größeren zentralen IT-Teams und Unis in Ländern mit Zentraldiensten haben tendenziell bessere Werte: Weniger Heterogenität, Altlasten, Schwachstellen

→ Skaleneffekte erhöhen das Potenzial für Professionalität im IT-Management.

→ Manuelle Prozesse sind fehleranfällig und werden nicht konsequent durchgehalten.

→ Einheitliche Tools, Prozesse, Plattformen reduzieren Fehler, beschleunigen Sicherheits-Updates.

Organisatorische Entscheidungen prägen die IT über Jahrzehnte: Heterogenität und Altlasten erschweren Modernisierung und Sicherheitsarchitektur

- **Beibehalt zweier IT-Landschaften nach Fusionen:** Doppelte Rechenzentren, Identity-Management-Systeme, Mail- und Webinfrastrukturen, usw. Resultierende negative Effekte sind teilweise noch nach 30 Jahren deutlich sichtbar.
- **Kooperationen mit Externen (z.B. Unternehmen), Förderprogramme und Projekte erzeugen zusätzliche Systeme:** Projektfinanzierte Server, Spezialanwendungen, Testumgebungen, externe Zugänge. Ergebnis: heterogene IT, unklare Zuständigkeiten und fehlende Verantwortung, proprietäre Schnittstellen, ungenutzte aber noch erreichbare Dienste (VPNs, Demo-Systeme, Portale), verwaiste IT und nicht mehr unterstützte (EoL) IT.
- **Dezentral Lehrstuhl-IT:** Insellösungen, uneinheitliche Sicherheit, verstreute Zuständigkeiten, schwer konsolidierbare Netze, hohe Dichte an Schwachstellen.
- **Legacy-Laborsysteme & Spezialgeräte:** Messgeräte/Steuerrechner mit alten OS (XP/Win7); nicht patchbar; kaum austauschbar; oft nicht isoliert, sondern im Campusnetz → dauerhaftes Risiko

Prof. Dr. Haya Schulmann (haya.schulmann@athene-center.de)

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Universitäten 4/5

Bekannte Empfehlungen zur Verbesserung der Cybersicherheit in der Forschung greifen meist zu kurz.

Mehr Struktur und Prozesse allein erzeugen nur mehr Overhead. Governance ist wichtig, erzeugt aber keine Sicherheit, sie verwaltet sie nur. Ein Mehr an Sicherheit setzt tiefergreifende und infrastrukturtechnische Verbesserungen voraus.

Lehrbeispiel »Equifax 2017«: Daten von 147,9 Mio. US-Bürger wurden gestohlen, obwohl das Information Security Management System (ISMS) nach ISO 27001 zertifiziert war. Wieso?

- Es gab viele Prozesse, aber die technische Basis war unzureichend.
- Kritische Schwachstelle in Apache blieb offen, obwohl Patch verfügbar war.
- Kryptographisches Zertifikat war seit neun Monaten abgelaufen.
- Netzwerk war unzureichend Segmentiert.

https://www.oxebridge.com/emma/equifax-held-iso-27001-certification-at-time-of-massive-system-hack/

Bekannte Empfehlungen zur Forschungssicherheit[1,2] fordern Compliance, Prozesse, Schulungen:

Awareness, Schulungen, Übungen, Kulturwandel, BCM, ISMS, Gremien, Kommissionen, Risikoanalysen, Listen, Prozesse, IT-Grundschutz, NIS2, …

Es fehlen Empfehlungen zur fundamentalen Neuausrichtung der IT. Resultat: Alles wird auf bestehenden, problematischen Infrastrukturen aufgebaut. Es entsteht Scheinsicherheit.

- Heutige Uni-IT ist historisch gewachsen, dezentral, voller Altlasten, mit verteilten Zuständigkeiten und tausenden Diensten, ohne saubere Segmentierung. Die Verwundbarkeit entsteht vorrangig durch Legacy- und Wildwuchs-Infrastruktur.
- Compliance-orientierte Ansätze alleine machen solch alte und schlecht aufgebaute IT-Organisationen nicht sicherer. IT-Grundschutz und ähnliches setzen kontrollierbare Basissysteme voraus: selbst richtige Sicherheitspläne werden bei falscher Infrastruktur nicht funktionieren. Schulungen und Awareness setzen an der falschen Stelle an: am Verhalten einzelner Menschen, obwohl die größten Risiken strukturell-technisch sind. Awareness ohne effektive Handlungsmöglichkeiten bringt wenig.
- Ohne gleichzeitigen Strukturwandel führen diese Empfehlungen nur zu mehr Bürokratie und Overhead, nicht zu mehr Sicherheit. Die knappen Ressourcen der Unis fließen in Prozessbeschreibungen, Papierpläne, Schulungsprogramme statt in Abschaltung, Konsolidierung, Automation und Modernisierung.

Die Universitäten brauchen eine grundlegende Neuausrichtung der gesamten IT-Landschaft - kein weiteres Optimieren am bestehenden System. Nur so sind Resilienz und Sicherheit realisierbar.

[1] https://www.bundestag.de/dokumente/textarchiv/2025/kw45-pa-forschung-1117822
[2] https://www.hrk.de/positionen/beschluss/detail/handlungsdruck-fuer-hochschulen-laender-und-bund-hrk-empfehlungen-zur-cybersicherheit/

Prof. Dr. Haya Schulmann (haya.schulmann@athene-center.de)

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Universitäten 5/5

Strategie zur Verbesserung der IT-Resilienz und Sicherheit

Schritt 1:
Inventarisierung & Analyse der Angriffsfläche

Schritt 2:
a. Transformation der IT-Infrastruktur
b. Aufbau moderner Sicherheitsarchitektur

2a. Transformation der IT Infrastruktur

- **IT-Infrastruktur festlegen**: Welche Dienste zentral/dezentral/auslagern, welche zwingend on-prem, wohin auslagern (Landes-/Bundesplattformen, SaaS,…)
- Grundlage für professionellen Betrieb ist **Konsolidierung** der Dienste: Zusammenlegung redundanter Services
- **Abschalten:** veraltete IT, ungenutzte Systeme, doppelte Dienste nach Fusionen, Migration dezentraler IT zu zentralen Plattformen
- **Abschaffen** ungeeigneter **On-Prem** Dienste: Nur Kern-IT bleibt lokal, Commodity wandert in Cloud/Landesdienste
- **Modernisierung** & Segmentierung der Labor/Legacy IT: Hochrisiko-Systeme (XP/Win7-Steuerrechner, Messgeräte, Spezialsoftware) isolieren
- **Lifecycle** und Abschaltprozesse definieren: verhindern, dass Systeme 15 Jahre unverändert laufen

Umbau der IT-Infrastruktur nach drei Grundprinzipen:

- Konsolidieren und Zentralisieren
- Modernisieren statt Weitertragen historischer Altlasten
- Strategische Nutzung von Plattformen & Cloud

Top-Level Architektur

2b. Aufbau moderner Sicherheitsarchitektur

- Zero-Trust-Modell: Identität, Autorisierung, Authentifizierung, Kontextprüfung
- Netz- und Zugriffssicherheit – Zero-Trust technisch umsetzen: Netzsegmentierung, Microsegmentierung, minimale Exponierung, sichere Gateways, Reverse Proxies,…
- Automatisiertes und zentrales Patch und Konfigurationsmanagement: Geschwindigkeit und Standardisierung → Voraussetzung für Resilienz
- Logging, Monitoring, SIEM, SOC
- Technische Sicherheitsmaßnahmen: SSL/TLS, Zertifikats-/CT-Monitoring, DNSSEC, SPF/DKIM/DMARC, RPKI, …

Sicherheitsarchitektur verstärkt die Infrastruktur Modernisierung. Sie scheitert aber, wenn die Infrastruktur nicht zuvor modernisiert wird.

- Zero Trust unmöglich, wenn Lehrstühle eigene, unverwaltete LDAP-/Mail-/Webserver betreiben.
- Mikrosegmentierung ist wirkungslos, wenn die Netzlandschaft ungeplant und chaotisch ist.
- Ein SOC bringt wenig, wenn es Tausende verwaiste Systeme gibt, die niemand patcht.

Die Infrastruktur muss zuerst modernisiert, konsolidiert, vereinheitlicht werden. Erst darauf kann eine moderne Sicherheitsarchitektur (ZT, Segmentierung, SOC, Automatisierung) aufbauen.

Prof. Dr. Haya Schulmann (haya.schulmann@athene-center.de)

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Impressum

Kontakt
Goethe-Universität Frankfurt
Fachbereich Informatik und Mathematik
Institut für Informatik
Professur Cybersicherheit
Robert Mayer-Straße 10
60325 Frankfurt am Main

kontakt@cyber.cs.uni-frankfurt.de

Frankfurt am Main, 2025

Hinweise

Dieser Bericht wurde mit Mitteln des Bundesministeriums für Forschung, Technologie und Raumfahrt (BMFTR) und des Hessischen Ministeriums für Wissenschaft und Forschung, Kunst und Kultur (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.