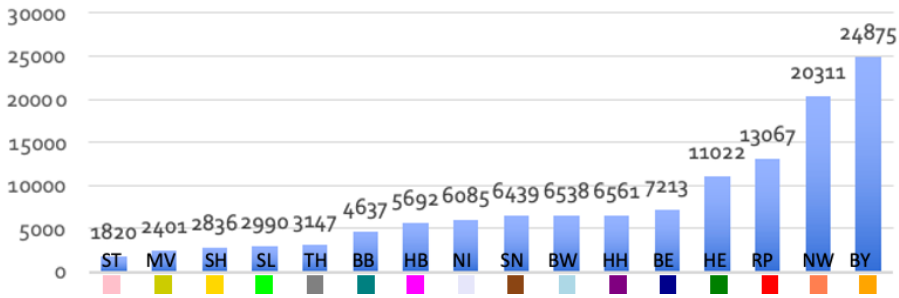
ATHENE Cybernation Deutschland

Sicherheit der IT der Länder 1/9

Studie der externen Angriffsfläche der 16 Bundesländer (2023-2025):
Kernergebnisse und Handlungsempfehlungen

IT-Größe (Anzahl Sub-/Domänen) variiert stark zwischen Ländern und zwischen West/Ost



In Westdeutschland im Durchschnitt mehr Sub-/Domänen als in Ostdeutschland

West	9998
Ost	4276

Wie kann man die Digitalisierung der Länder messen und vergleichen?

Metriken zur Länderdigitalisierung

- **Nutzungsindikator „Service-Dichte“:**
  Wie viele Services pro Domäne?
  Mehr Services = bessere *Domäne* Nutzung
- **Governance-Indikatoren „Zentralisierung“:**
  Wo laufen die Subdomänen (%IT unter Hauptdomain)? und **„Konsolidierung“:**
  Wie viele Subdomains pro Domäne?
  Mehr = bessere Kontrolle & Steuerung
  Treiber sind Sicherheitsorganisationen mit Durchgriffsrechten, Domänen-Policies, zentraler Dienstleister, Verwaltungsreform
- **Strukturindikator „Fragmentierung“:**
  Wie viele Domänen pro Mio. Einwohner?
  Mehr Fragmentierung → mehr Verwaltungsaufwand & Sicherheitsprobleme.
  Treiber sind Regierungsbezirke, fehlende Governance/Policies/Dekommissionierung.
- **Intensität dig. Exposition „IT-Intensität“:**
  Wie viele FQDNs (Fully Qualified Domänen Namen) pro 1,000 Einwohner?

gut | moderat | schwach | schlecht

Land	EW Mio.	Service-Dichte	Zentralisierung	Konsolidierung	Fragmentierung	IT-Intensität
HE	6,3	2,62	69,3%	9,6	166	1,75
BE	3,7	2,72	40,9%	12,2	148	1,90
SL	1,0	1,55	66,7%	9,8	276	2,99
NI	8,0	2,69	44,5%	9,5	72	0,76
ST	2,2	2,32	49,8%	8,0	92	0,83
RP	4,1	3,41	27,1%	11,6	254	3,19
SH	2,9	3,09	27,5%	7,8	111	0,98
BB	2,6	1,63	28,1%	7,9	201	1,78
HH	1,9	1,16	54,4%	6,5	459	3,45
BW	11,1	1,66	3,9%	6,0	85	0,59
TH	2,1	1,22	40,9%	3,9	309	1,50
SN	4,1	0,93	39,5%	3,8	327	1,57
BY	13,2	0,83	27,4%	3,3	442	1,88
HB	0,7	1,62	44,2%	7,1	1004	8,13
MV	1,6	0,87	0,2%	3,0	372	1,50
NW	18,0	0,34	0,2%	1,4	472	1,13

Hier und im Folgenden genutzte Farbkodierung für die 16 Länder

- Berlin
- Bayern
- Saarland
- Nordrhein-Westfahlen
- Rheinland-Pfalz
- Baden-Württemberg
- Bremen
- Schleswig-Holstein
- Sachsen-Anhalt
- Thüringen
- Hessen
- Sachsen
- Mecklenburg-Vorpommern
- Hamburg
- Brandenburg
- Niedersachsen

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

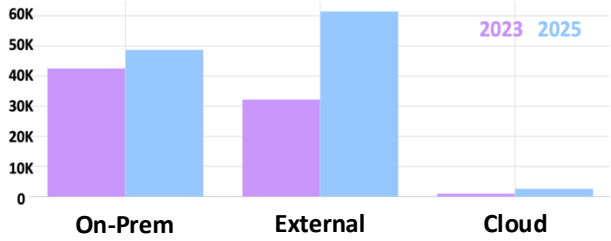
ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Länder 2/9

Bertriebsmodelle (On-Premise, External, Cloud) der Länder-IT:
Wachstum, Externalisierung und Cloud-Abhängigkeiten

Wachstum (FQDNs) der Länder-IT zwischen 2023-2025:

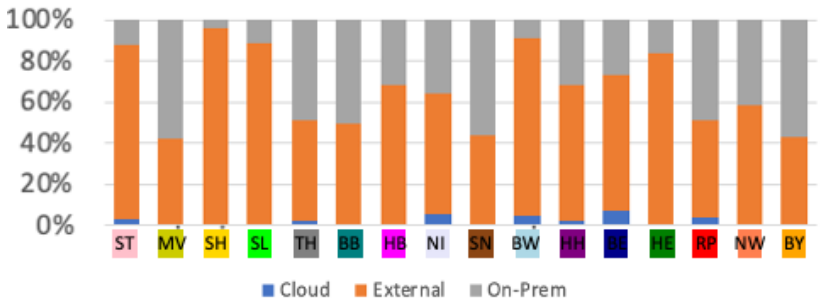


Betriebs-modell	Anteil 2023	Anteil 2025	Wachstum der absoluten Zahlen
On-Prem	ca. 57%	ca. 42%	+14%
External	ca. 43%	ca. 53%	+88%
Cloud	ca. 1%	ca. 5%	Sehr hoch

+53% Gesamtsystemwachstum! Kein Abbau/Abschaltung → Parallelbetrieb alter und neuer IT

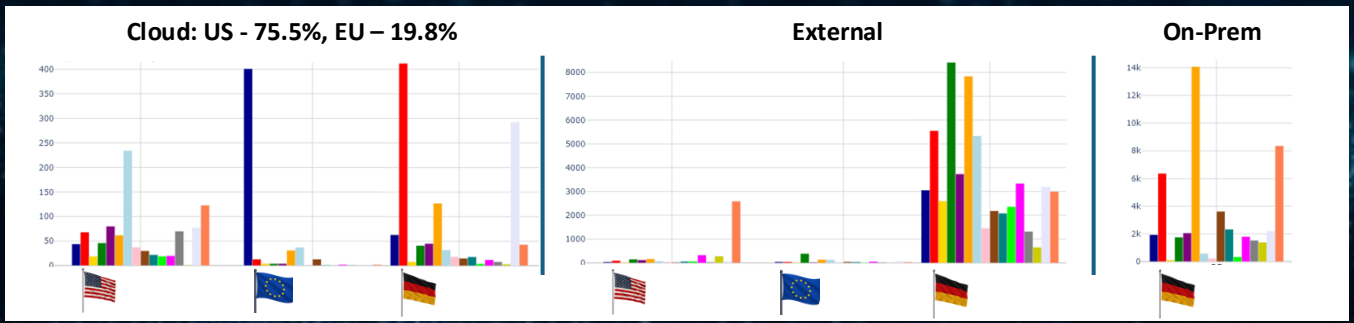
Die Länder-IT wächst, aber nicht durch Modernisierung: „External“ und „Cloud“ expandieren stark, ersetzen „On-Prem“ aber nicht, sondern kommen on top. „Cloud“ war 2023 nahezu unsichtbar, ist jetzt aber operativ relevant. Strukturelle Effekt sind steigende Fragmentierung und größere Angriffsfläche.

IT-Ressourcen (Anteile in %) nach Hosting-Bereich: On-Prem, External, Cloud



	West	Ost
On-Prem	37.7%	43%
External	60.5%	54%
Cloud	1.9%	2.9%

Kein ländereinheitliches Betriebsmodell: Einige Länder sind stärker „On-Prem“ und zentralisiert, andere stärker „External“. „External“ umfasst alles außerhalb des eigenen Netzes (inkl. kommerzielle Hoster, CDNs, andere Institutionen, Dienstleister,...). Länder-IT ist von außen fast komplett über externe Provider sichtbar. Bei klassischem Hosting überwiegen DE/EU Standorte. Bei Cloud eher US.



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

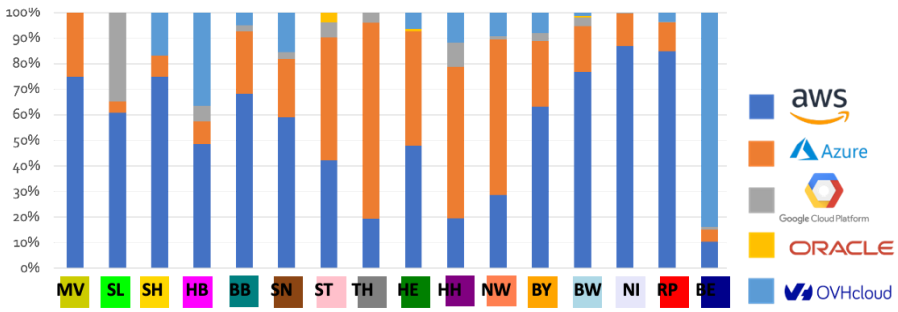
ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Länder 3/9

IT-Lieferketten, Cloud, externe Abhängigkeiten: US Hyperscaler (CDN, Identity, Tracking, CI/CD, SaaS, PaaS, …) dominieren

Welche Cloud-Anbieter verwenden die Länder?



Vielzahl an Cloud Plattformen. Populärste: AWS (52.2%), Azure (21%), OVH (20%)

Relativ mehr Cloud in Ost (2,9 % vs. 1,9 %); absolut mehr in West (1 858 vs. 734). Berlin stark OVH-lastig.

Keine ländereinheitliche Cloud-Strategie. Fragmentierte Verhandlungsmacht – 16 Länder verhandeln einzeln. Cloud-Services verschiedener Länder sind nicht kompatibel; es gibt verschiedene Cloud Security Policies und keine gegenseitige Backup-Strategie. Ohne gemeinsame Cloud-Strategie haben sich die Länder für verschiedene Anbieter entschieden. Die Länder stehen am Scheideweg: Heute sind nur 2,1% der Services in der Cloud, aber der Trend ist eindeutig. In 10 Jahren wird „Cloud" dominant sein. Die Entscheidungen, die *jetzt* getroffen bzw. *jetzt nicht* getroffen werden, bestimmen die digitale Zukunft. Jede Migration wird Millionen kosten und Jahre dauern.

Cloud-Nutzung der Länder tritt in unterschiedlichen Betriebsmodellen auf, z.B. Workloads und Drittanbieter-Dienste. Im „US-lastigen" Land können die eigentlichen Fachverfahren ggf. in DE laufen, oder umgekehrt in den USA betrieben werden.

Cloud-Nutzungstypen

	Typische Dienste	Risiken für Souveränität	Von Außen sichtbar als
IaaS/VMs	Fachverfahren auf AWS EC2	**Hoch** - Daten liegen dort	AWS-IP
PaaS	Datenbank auf Azure SQL	**Hoch** - Daten liegen dort	Azure-IP
CDN/WAF	CloudFront, Cloudflare	**Mittel** - nur Caching/Proxy	AWS-IP
SaaS	Office 365, Salesforce	**Hoch** - Daten beim Anbieter	Azure-IP
Analytics	Google Analytics	**Mittel-Hoch** - Tracking-Daten	GCP-IP
DNS/DDoS	AWS Route53, Shield	**Niedrig** - nur Routing	AWS-IP

Cloud-Diensttypen

	Nutzung	Wo liegen die Daten
CloudFront CDN	Statische Webseiten, Bilder, CSS, JS werden gecached	Edge-Server weltweit, **Originaldaten in DE**
Route53 DNS	DNS-Auflösung für *.land-x.de	Nur Routing-Info, **keine Nutzdaten**
AWS Shield/WAF	DDoS-Schutz, Firewall vor Webservern	Traffic-Filterung, **Daten fließen durch**
S3 Buckets	Dokumenten-Ablage für Fachverfahren	**Dokumente liegen auf AWS**
EC2 VMs	Fachverfahren mit Bürgerdaten	**Personendaten auf AWS-Servern**

Gleiche IP, unterschiedliche Kritikalität. Z.B. AWS-IPs: Nur Routing (Route53 DNS), nur Caching für Webseiten, Bilder, JS (CloudFront CDN), oder echte Daten (auf EC2 Fachverfahren).

Treiber der Anzahl an Dienstleistern: Skalierung und Governance. Aber mehr Assets führt auch zu mehr Abhängigkeiten und viele autonome Einheiten haben mehr Provider.

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

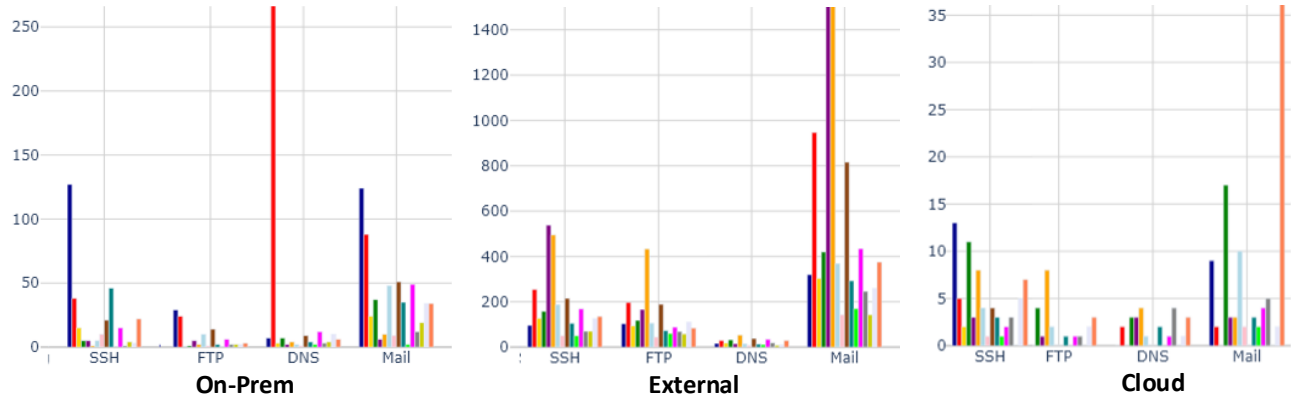
ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Länder 4/9

Outsourcing-Strategien in Länder-IT: Wer lagert was aus?

Aktive Netzdienste (ohne HTTP)



Was wird ausgelagert (Webseiten vs. Infrastruktur)

- **Fast alles ausgelagert** (SH, SL, BW, ST, HE): starkes Hosting-/Dienstleistermodell, häufig „shared/managed"-Stacks.
- **Gemischt / selektives Outsourcing** (BY, MV, SN, RP, NW, BB, HB): Unterschiedliche Strategien je Domäne/Träger: Portale/IdP evtl. intern, Web/Teile der Infra. extern
- **Web eher intern, Infrastruktur stark extern** (BY, MV, SN, RP, NW, BB, HB): zentrale Plattform für Websites, während Mail/FTP/Remote/DB/DNS teilweise extern laufen.

Bei extern betriebenen Services dominieren klassische Internet-Basisdienste (% aller externen Services): Remote connection (26%), Mail (29%), FTP (24%), DB (10%), DNS (10%)
Länder unterscheiden sich stark darin, ob Websites ausgelagert sind (SL/SH extrem vs BY/SN/MV niedrig) und ob DNS/DB „extern dominiert" (HE bei DNS; BY/HB bei DB)

Services bei denen Länder unterschiedlich sind

- **DNS als Outsourcing**: Einige Länder nutzen stark zentrale DNS-/Provider-Strukturen (Telekom/Versatel, spezialisierte DNS-Dienstleister, CDN-Anycast).
→ Implikation für DNS-Governance (Geo-Separation, Delegationsqualität, Ownership)
- **DB-nahe Exposures:** Hohe externe DB-Service-Anzahl (auffällige MySQL-/DB-Exposures)
→ Meist ein Architektur-/Segmentierungsproblem und/oder ein Provider-Security-Problem.
- **Legacy-Dienste** sind überall, aber in unterschiedlicher Kombination. Einige Länder zeigen „Mail"-Profil, andere „FTP-dominant", wieder andere „Remote-dominant". → Das sind oft historische Betriebsmodelle (Webhosting-Pakete, Schul-/Kommunalhosting, alte Transferschnittstellen).

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

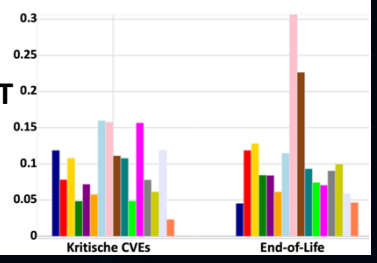
ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Länder 5/9

Verwundbarkeit: Systemischer Patch- und Lifecycle-Backlog

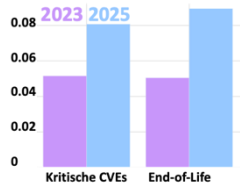
Schwachstellen und End-of-Life (Anteile Systeme) in Länder-IT



Ursachen:
Systemischer Patch- & Lifecycle-Backlog

Angriffsfläche altert, Verwundbarkeit steigt

Mehr kritische CVEs & EoL-Systeme
Aber: Keine Architektur-veränderung und keine Modernisierung der IT



Wo viele autonome Einheiten IT betreiben, fehlen häufiger einheitliche Asset Policies und Lifecycle-Prozesse (z.B. Zertifikatsabläufe).

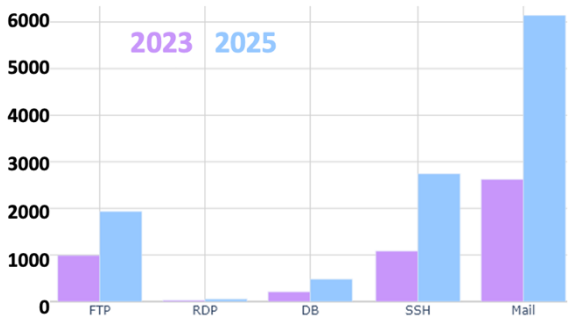
Das ist unabhängig vom Hosting-Modell, da die Dichte nicht mit Anteil External korreliert.

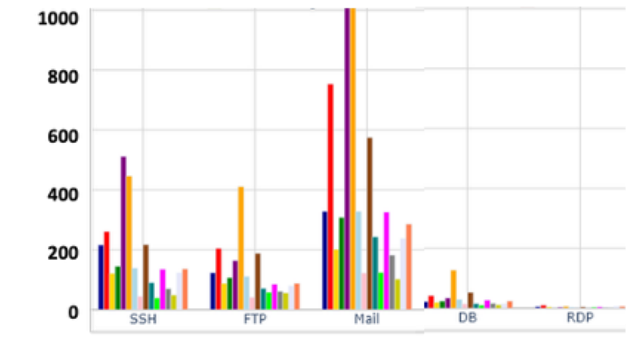
Fragmentierung korreliert mit Lifecycle Schulden und Infrastruktur Problemen
→ Treiber für Hijack-/Takeover-Angriffe

Was läuft, das läuft: Legacy-Dienste bleiben; EoL dominiert und streut am stärksten zwischen den Ländern – Indikator für mangelnde IT-Hygiene & Steuerungsfähigkeit.

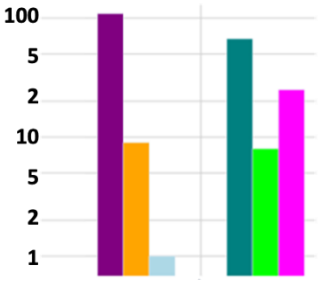
Kritische CVEs bei mehreren Ländern spürbar. Das Hauptproblem sind systemische Betriebs- und Lifecycle-Defizite. Wer EoL nicht konsequent abbaut, wird auch bei CVEs hinterherlaufen.

Basis-Netzdienste (Anzahl), die verwundbar durch Bruteforce sind, wachsen



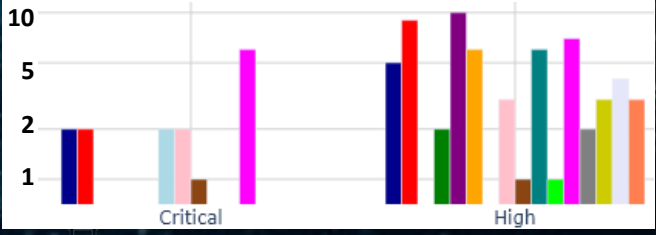


Kompromittierte Mitarbeiterzugangsdaten pro Land zu Produktivsystemen der Länder



Zwischen 2023 und 2025 gibt es keine Verbesserung bei kompromittierten Mitarbeiter-zugangsdaten.

Kritische Datenexponierung: Sensible Daten sind offen zugänglich. Beispiele: Datenbanken, Buckets, Repos mit Zugangsdaten oder Schlüsseln, Backup-Server, Konfig-Dateien, Administrational Web-Portals.



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

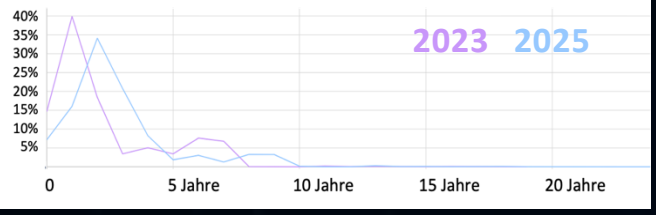
ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Länder 6/9

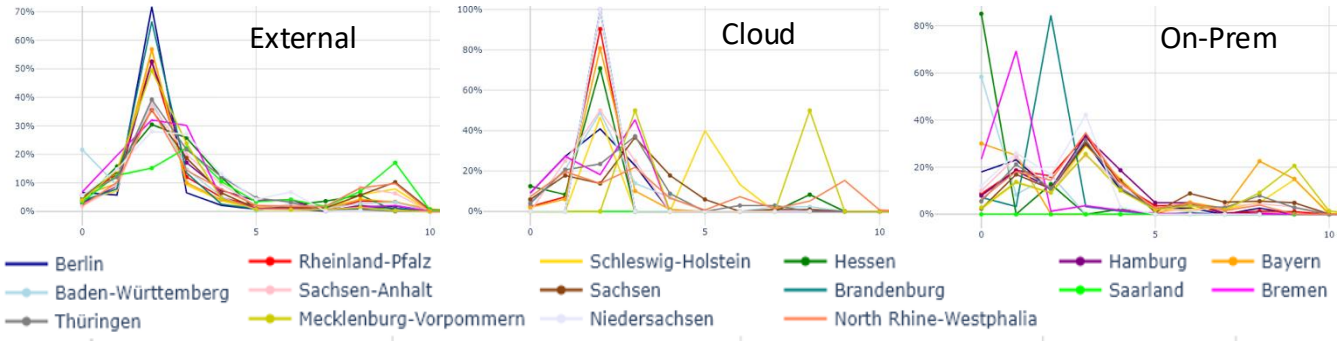
Patchmanagement und Governance

Verteilung des Alters von CVEs für Länder-IT.
Verteilung wandert nach rechts und ist breiter.



2025 zeigt nicht einfach „mehr neue CVEs“, sondern mehrjährige CVEs werden stärker sichtbar – deutliches Signal für strukturelle Ursachen: Fehlende Durchgriff-Governance, zu wenig Automatisierung, Legacy-Inseln und verwundbare zentrale Provider-Plattformen, die viele Systeme gleichzeitig „alt“ halten.

Altersverteilung der kritischen CVEs pro Bundesland-IT nach Betriebsmodell.



Über alle drei Betriebsmodelle ist eindeutig: Der Schwerpunkt liegt nicht bei „ganz frischen“ CVEs, sondern sehr oft bei ~1–3 Jahre alten Schwachstellen, d. h. viele Systeme bleiben monatelang bis jahrelang verwundbar, zusätzlich existiert bei mehreren Ländern ein Altlast-Schwanz bis ~10 Jahre (Legacy/EoL, fehlende Abschaltung/Migration).

- Patchen ist nicht kontinuierlich, sondern „in Wellen“ (Peak bei ~2 Jahren) → zu große Angriffsfenster für Internet-exponierte IT.
- Altlasten werden nicht konsequent abgebaut (Tail bis ~10 Jahre) → fehlende Konsolidierung, fehlende Abschalt-/Migrationspfade, unklare Eigentümerschaft.
- Cloud wird oft falsch betrieben (IaaS ohne Guardrails/Automation) → Cloud verschiebt Verantwortung; ohne Landing-Zone/Policy-as-Code bleiben alte Images/VMs liegen.
- Provider-Plattformen erzeugen Klumpenrisiken: wenige zentrale Stacks „dominieren“ und replizieren Patch-Schulden über viele Portale.
- Starke Konzentration auf wenige Assets/Plattformen, replizierte Technologien dominieren Risiko.

Das Problem ist weniger ein „mehr neue CVEs“, sondern vor allem zu lange Patchlatenzen, Legacy-Schulden und Plattform-/Provider-Konzentrationsrisiken – und damit ein Governance-Problem (Standards/Guardrails/SLAs/Messung), mindestens genauso wie ein rein technisches.

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

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Länder 7/9

Faktoren für IT-Wildwuchs und Sicherheitsprobleme:

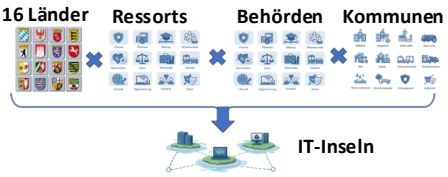
Länder haben fragmentierte, schwach verbindliche und freiwillige Strukturen. IT in Verwaltungen besteht aus bis Hunderten eigenständigen Behörden. Dadurch entstehen Fragmentierung, Legacy-Landschaften, Cloud-Wildwuchs & Sicherheitsprobleme.

- Länder-IT: zeigen extreme Heterogenität, Legacy-Last und fehlende Standards, sind breit exponiert, stark fragmentiert, oft unterreguliert.
- Kein Bundesland hat einen zentral verantwortlichen Akteur für die IT des Landes.
- Kein Bundesland hat eine zentrale Architekturplattform für die gesamte Landesverwaltung.
- Kein Bundesland hat die strukturellen, gesetzlichen, organisatorischen und technische. Voraussetzungen geschaffen, um seine gesamte Behörden-IT zentral zu steuern oder verbindliche technische Baselines und IT-Sicherheitsstandards durchzusetzen.
- Keine organisatorische Durchgriffsmacht: Landes-CERTs, Landes-SOCs oder zentrale IT-Dienstleister dürfen die nachgelagerten Behörden oft nicht verpflichten oder konfigurieren.

Größere IT → Mehr Beteiligte → Mehr Fragmentierung

Ein großes Land hat *mehr* Ressorts, *mehr* Landesbetriebe, *mehr* Kommunen, *mehr* Dienstleister.
IT-Größe erzeugt Komplexität, aber nicht notwendigerweise bessere zentrale Steuerung.

Strukturelle Ursachen



- **Föderale Fragmentierung → viele autonome IT-Einheiten → Hohe Fragmentierung**
  Fragmentierte Zuständigkeiten über Behörden, Landkreise, Kommunen, Eigenbetriebe, Landesrechenzentren, Dienstleister.
- **Ressortprinzip → fehlende Durchgriffsrechte → niedrige Zentralisierung**
  Länder-IT ist verteilt: Verschiedene unabhängige Organisationen mit eigener IT, Anwendungen, Dienstleister, kommunalen- und Landesrechenzentren, externen Hostern, Cloud, Agenturen.
- Föderalismus ohne Koordination führt zu Fragmentierung, inkompatiblen Systemen, fehlenden Synergien, keine gemeinsame Verhandlungskraft, kein vollständiges Register der Landes-IT.

Technische Ursachen

- IT einfach aufzusetzen, schwer abzuschalten
- Fehlende Automatisierung und manuelle Prozesse
- Legacy Lock-in (Fachverfahren von vor 20 Jahren, keine Dokumentation, keine Tests)
- Heterogene Technologiestacks und keine zentralen Vorgaben

Organisatorische Ursachen

- Dezentrale IT-Beschaffung → heterogene IT
- Vergaberecht: Ziel ist nicht der beste, sondern der günstigste Anbieter
- Tarifstrukturen → Fachkräftemangel
- Projektfinanzierung → Insellösungen und Systeme ohne Betriebsbudget
- Politische Zyklen: Legislaturperioden (≤ 5 Jahre) zu kurz für IT-Transformation

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

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Länder 8/9

Faktoren für IT-Wildwuchs und Sicherheitsprobleme

Digitalisierung und IT-Sicherheit der Länder-IT

- Probleme steigen mit Fragmentierung: Mehr Domänen korrelieren mit mehr absoluten Problemen. Länder mit fragmentierter IT haben mehr Exposures für Hijacks.
- Jeder zusätzliche Service auf bestehender Domäne erhöht die Komplexität, aber Konsolidierung senkt Probleme bei *professionellem* IT-Management (d.h. mit zentralen IT-Teams, einheitlichen Tools, Lifecycle-Prozessen, Automatisierung, usw).
- Hohe Dichte mit Governance erhöht Zentralisierung und Konsolidierung. Hohe Dichte ohne Governance erhöht Komplexität und damit Exposures.
- IT-Größe korreliert mit mehr CVEs und Exposures für Hijacks und Injections.

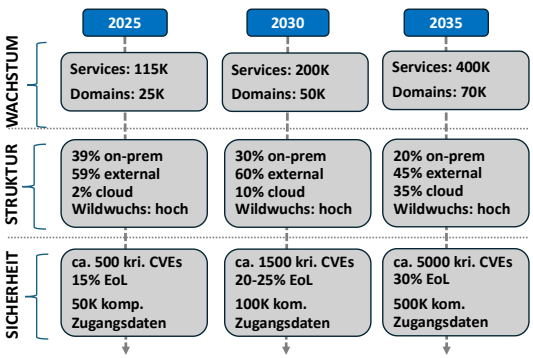
Digitalisierungsqualität vs. Wildwuchs

- Hohe IT-Intensität, niedrige Service-Dichte ➔ viele Services aber wenig pro Domäne ➔ Wildwuchs
- Hohe IT-Intensität, hohe Service-Dichte, Hohe Konsolidierung ➔ viele Services aber effizient genutzt ➔ gesunde Digitalisierung
- Hohe Fragmentierung, niedrige Zentralisierung ➔ viele Domänen nicht unter Kontrolle ➔ Wildwuchs
- Hohe IT-Intensität, niedrige Konsolidierung, hohe Fragmentierung ➔ unkontrolliertes Wachstum
- Niedrige IT-Intensität, niedrige Service-Dichte, hohe Fragmentierung ➔ Wenig IT aber schlecht organisiert

Prognose 2025-2035:
Entwicklung der IT der Bundesländer auf Basis unserer 2023-2025 Messungen

- Die Angriffsfläche wächst weiter schneller als Konsolidierung/Modernisierung:
  Tempo Digitalisierung >> Tempo Modernisierung >> Tempo Sicherheit
- Stand 2025:
  - Wildwuchs (Tausende unkoordinierte Systeme)
  - Schwachstellen (>75% CVEs älter als 1 Jahr)
  - EoL-Systeme (steigend)
  - Fragmentierte Verantwortung und kein Gesamtüberblick
  - Keine Durchsetzungsfähigkeit für Standards

➔ **Ergebnis ist eine wachsende Angriffsfläche bei stagnierender Modernisierung der IT**



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

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Länder 9/9

Lücken im BSI-Lagebericht 2025:
Konsequenzen für Digitalisierungs- und Sicherheitsstrategien

Digitalisierung steht in Deutschland auf „schwachen Füßen“. Aktuelle Digitalisierungsstrategien und -initiativen setzen implizit ausreichend tragfähige, sichere IT-Infrastruktur voraus. Tatsächlich werden aber neue digitale Dienste auf bestehenden, problematischen IT-Infrastrukturen aufgebaut.

Sicherheit soll durch oft teuere Compliance-Programme dargestellt werden. Dadurch werden Angriffsfläche und Wildwuchs aber nicht reduziert. Ohne Strategie zur konsequenten Dekommissionierung wächst die Angriffsfläche mit jedem neuen System.

Digitalisierung braucht nicht nur neue digitale Dienste, sondern auch die Professionalisierung und Modernisierung der vorhandenen IT-Infrastrukturen!

BSI-Bericht 2025 übersieht kritische Aspekte, Empfehlungen greifen daher zu kurz:

- **Der BSI-Lagebericht übersieht das Kernproblem der Länder-IT. ATHENE-Lagebild identifiziert als Kernprobleme:** EoL und veraltete Systeme, fehlender Hersteller-Support, technische Schulden, Modernisierungsrückstände, Lifecycle-Management und Systemalter
- **Laut BSI-Lagebericht sind Angriffsflächen durch besseres Management beherrschbar. ATHENE-Lagebild widerlegt dies**: Altlasten bis 15 Jahre und EoL dominieren Sicherheitsprobleme
  → **Ein großer Teil der Angriffsfläche ist nicht mehr patchbar, völlig unabhängig davon, wie gut das Management ist:** Updates existieren nicht mehr, Hersteller haben Support eingestellt, Anwendungen sind an veraltete Laufzeitumgebungen gebunden
  → **Patching als Sicherheitsmaßnahme stößt an harte Grenzen**: Bei einer wachsenden Anzahl von Systemen (teils älter als 15 Jahre) fehlen Sicherheitsupdates, Fachverfahren sind nicht migrierbar, Abhängigkeiten blockieren Modernisierung
- **Der BSI-Bericht fokussiert auf neue CVEs, aber ATHENE-Lagebild zeigt:** Der Schwerpunkt liegt bei 1-3 Jahre alten Schwachstellen – 75% der CVEs sind älter als 1 Jahr
- **Der BSI-Lagebericht empfiehlt**
  - „Zeitnahe Updates und Patching“ – aber Patching ist wirkungslos bei IT jenseits EoL.
  - ISMS/BCMS-Reifgrade erhöhen – führt zu mehr Compliance-Audits, nicht notwendigerweise zu mehr Sicherheit im technischen Sinne
    - *Compliance und Zertifizierung sind ein Lenkrad ohne Motor - sie verwalten existierende IT-Sicherheit, schaffen sie aber nicht:* Audits prüfen Dokumentation/Prozessnachweise, sind point-in-time und stichprobenartig
    - **ATHENE-Lagebild der Länder-IT findet** keinen messbaren Unterschied in Angriffsfläche/IT-Hygiene zwischen zertifiziert und nicht zertifiziert

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

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.

Die in diesem Bericht enthaltenen Arbeitsergebnisse sind sorgfältig und unter Zugrundelegung des bekannten Standes der Wissenschaft erstellt worden, stellen jedoch Forschungsansätze dar. Eine Haftung oder Garantie dafür, dass die Arbeitsergebnisse bzw. Informationen die Vorgaben der aktuellen Rechtslage erfüllen, wird aus diesem Grund nicht übernommen. Gleiches gilt für die Brauchbarkeit, Vollständigkeit oder Fehlerfreiheit, so dass jede Haftung für Schäden ausgeschlossen wird, die aus der Benutzung dieser Arbeitsergebnisse bzw. Informationen entstehen können. Diese Haftungsbeschränkung gilt nicht in Fällen von Vorsatz.