ATHENE Cybernation Deutschland

STUDIE DER EXTERNEN ANGRIFFSFLÄCHE

IT der Bundesministerien 2025

Kernergebnisse und Handlungsempfehlungen

Prof. Dr. Haya Schulmann

Juli 2026

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

ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Bundesministerien 1/15

Studie der externen Angriffsfläche der Bundesministerien-IT 2025:
Kernergebnisse und Handlungsempfehlungen – Überblick

1. Man kann nicht schützen, was man nicht sieht

Das BSI-Lagebild für 2025 betrachtet nur einen kleinen Teil der IT Deutschlands und der IT der Bundesverwaltung. Die Angriffsflächen werden daher vom BSI strukturell deutlich unterschätzt.

2. Es gibt nicht die *eine* „Bundes-IT", sondern 16 IT-Realitäten

2.345 Domänen; Faktor über 50 zwischen kleinstem und größtem Ressort; rund 100 Nameserver-Betreiber. Die IT ist historisch gewachsen, nicht geplant. Größe und IT-Entstehung variieren.

3. Die Dienstleister prägen die Architektur

Drei Betriebsmodelle: Eigenbetrieb, Hybrid, Auslagerung. Die IT-Architektur wird faktisch im Vergabeverfahren entschieden – der Gewinner der Ausschreibung entscheidet.

4. Architektur-Archetypen der Bundesministerien

Sieben Archetypen, von Apache-Monokultur bis WAF-Edge-Architektur. Die 16 Ministerien verteilen sich auf sieben grundverschiedene Bauweisen. Die Idee eines DE-Stack trifft auf sieben unvereinbare Ausgangslagen.

5. Heterogenität der IT der Ministerien ist nicht Ineffizienz, sondern fachliche Notwendigkeit

Verteidigung, Diplomatie, Wettervorhersage, Epidemieüberwachung: Verschiedene Aufgaben erzwingen verschiedene IT. Das Problem ist nicht die Vielfalt, sondern die fehlende Steuerung dieser Vielfalt.

6. Technologievielfalt treibt die Schwachstellen

Die Zahl paralleler Technologien korreliert mit der Zahl der Schwachstellen. Jede zusätzliche Schicht bringt eigene Patches, Konfigurationen und CVEs. Vielfalt addiert Risiko. Strategien bauen auf, schalten nie ab. Fusionen erzeugen Parallelbetrieb.

7. Nicht Zero-Days, sondern alte ungepatchte Schwachstellen sind das Hauptproblem

Viele Probleme sind alt und banal: 10 Jahre Patch-Latenz für kritische Lücken gegenüber ca. 5 Tagen bis zum Exploit. 1.050 (48 %) von über 2.182 aktiven kritischen CVEs sind aus 2015-2017, also rund ein Jahrzehnt alt.

8. Kein Ministerium erfüllt die Mindeststandards

32,5 % fehlerhafte Zertifikate, 86 % ohne CSP, 45 % der Mail-Domänen ohne wirksamen Schutz, exponierte Basisdienste (SSH, FTP, MySQL). Governance-Frage, keine Technikfrage.

9. Was die Studie für Sicherheit und Politik bedeutet (Teil 1-3)

Kein Architekturrahmen ersetzt die Grundlagen. Die Sicherheit der Bundes-IT entscheidet sich an Grundhygiene, Betreiberverträgen und der Bereitschaft, Altsysteme abzuschalten.

Lesehinweis zu den Namen der Ministerien

Die Daten wurden Ende 2025 erhoben. Wir verwenden daher die damaligen Kürzel, da die neuen Ministerien damals noch keine eigene benannte IT hatten.

Fazit: Die Sicherheit der IT der Bundesministerien entscheidet sich nicht an neuen Plattformen, sondern an Grundhygiene, Betreiberverträgen und an der Bereitschaft, Altes abzuschalten. Deutschland braucht Baselines für heterogene Fach-IT.

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

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Bundesministerien 2/15

1. Man kann nicht schützen, was man nicht sieht – Teil 1

Deutschland ist größer als nur .de

Wie sieht die Angriffsfläche der Bundesministerien aus?

Top 5 TLD	Anteil	Bemerkung
.de	62 %	Deutsche TLD dominiert
.org	9 %	Forschungs- und Projektdomänen
.eu	7 %	EU-Bezug
.info	6,5 %	Kampagnen und Informationsseiten
.com	6 %	Internationale Präsenz

- Ca. 2/3 unter .de, der Rest unter 15 Top-Level Domains (TLDs), inkl. .org, .info, .com.
- Größe des Domänenportfolios korreliert mit der Anzahl nachgeordneter Behörden.

Angriffsfläche *Deutschlands* wird im Lagebericht des BSI 2025 deutlich unterschätzt:

„Die Web-Angriffsfläche Deutschland umfasste im zweiten Quartal 2025 rund 13,2 Mio aus dem Internet erreichbare .de-Domains.“

Das digitale Deutschland ist jedoch deutlich größer als nur die .de-Domänen. Selbst die Bundesministerien betreiben (s.o.) mindestens 38 % ihrer Domänen außerhalb der .de-Domäne. In den anderen Sektoren dürfte der Anteil außerhalb .de noch deutlich größer sein.

Ein .de-zentriertes Lagebild hat mehrere blinde Flecken

- **Realität:** Einrichtungen in DE verwenden eine Vielzahl an TLDs. Insbesondere ausgelagerte Dienste (Cloud, Dienstleister) nutzen häufig TLDs außerhalb von .de. In der Bundesverwaltung folgt die Nutzung von z. B. .org, .com, .info, .eu, .ru häufig aus den speziellen Fachaufgaben.
- **Folge für die Steuerung:** Eine vollständige Erfassung über alle TLDs hinweg ist Voraussetzung jeder Lagebildbestimmung und Absicherung. Ohne diese Erfassung übersieht man zwangsläufig viele Probleme, z. B. Schwachstellen oder Domänen wie *feministischeaussenpolitikgestalten.org* des AA (Registrierung ausgelaufen) die ein Risiko für Phishing, Übernahme und Impersonation-Angriffe darstellen.

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

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Bundesministerien 3/15

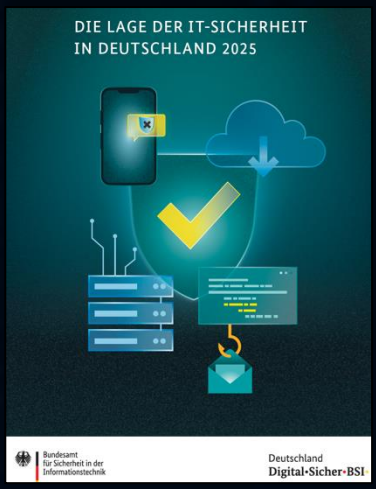
1. Man kann nicht schützen, was man nicht sieht – Teil 2

Deutsche Bundesverwaltung ist größer als nur die eigenen IP-Bereiche

Auch die Angriffsfläche der *Bundesverwaltung* wird im Lagebericht des BSI 2025 deutlich unterschätzt:

*„Im Monitoring befinden sich derzeit ca. **3.800** aktive IP-Adressen, hinter denen ca. 7.400 zugehörige Dienste und ca. 10.000 zugehörige Hosts […] stehen."*

Laut BSI sind dies die aktiven IP-Adressen aus der „Weißen Liste", also der staatseigenen IP-Bereiche. Ein Großteil der Bundesverwaltung läuft aber *außerhalb* dieser Adressbereiche, etwa bei Cloudflare, Hetzner, Strato, AWS, Azure, Google, Akamai, Fastly. All dies liegt außerhalb der BSI-Messungen.



Konkret übersieht die BSI-Messung knapp 90 % aller aktiven IP-Adressen der Bundesverwaltung, und damit die entsprechenden Sicherheitsbefunde

- Das ATHENE-Lagebild ordnet der Bundesverwaltung ca. 36.100 aktive IP-Adressen zu. Davon sind mehr als 21.700, also über 60 %, extern beziehungsweise in der Cloud gehostet. Über 6.400 Cloud-gehostete aktive IP-Adressen und über 5.500 extern/Cloud-gehostete Assets konnten wir konkreten Cloud-Dienstleistern zuordnen.
- In diesen vom BSI nicht erfassten Bereichen fanden wir mehr als **12.100 Sicherheitsbefunde** (Schwachstellen, Fehlkonfigurationen, Lücken).

Grund für diese Diskrepanz sind unterschiedliche technische Ansätze

- Das **BSI-Verfahren** für die Bundesverwaltung geht von der „Weißen Liste" aus, also den staatseigenen IP-Blöcken. Dieses IP-Block-basierte Vorgehen war Anfang der 2000er Jahre üblich, als staatliche IT im Wesentlichen selbst, also „on premise" betrieben wurde. Es ist aber blind für externe/Cloud-gehostete IT-Assets und damit für einen Großteil der IT, die in den letzten 20 Jahren in der Bundesverwaltung entstand. Wer nur den eigenen Adressraum scannt, sieht heute nicht mehr die tatsächliche Angriffsfläche, sondern nur noch ihren historisch gewachsenen Kern.
- Das **ATHENE-Verfahren** folgt hingegen den Domänen und Diensten, unabhängig von der TLD und vom Hoster. Es erfasst deshalb im Gegensatz zum BSI-Verfahren auch verbundene Drittanbieter und misst die Lieferkette der Ministerien. Diese Lieferketten spielen oft eine wichtige Rolle bei gezielten Cyberangriffen und dürfen deshalb in einem Lagebild nicht fehlen.

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

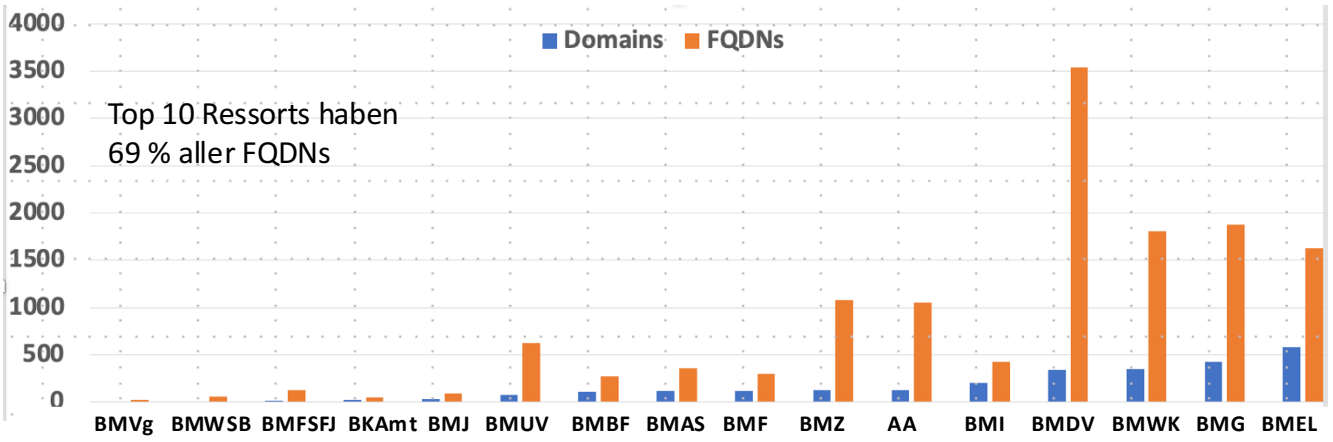
ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Bundesministerien 4/15

2. Es gibt nicht die *eine* „Bundes-IT“, sondern 16 IT-Realitäten

Die IT der Ministerien ist heterogen und historisch gewachsen



16 Ressorts: 15 Bundesministerien im Zuschnitt Ende 2025 + BKAmt

Domänen-Registrierung ist historisch gewachsen

- Domänen von Ministerien und nachgeordneten Behörden, Projekt- und Kampagnendomänen (Fachportale, Initiativen, Förderprogramme), Schutzregistrierungen usw.
- Die älteste nicht .de-Domäne, *giz.com,* stammt von 1993

Zeitraum	Zahl	Bemerkung
1993–1999	5	Pionierphase: Erste Ministeriumsdomänen
2000–2004	132	Aufbau der E-Government-Infrastruktur
2005–2009	136	Stetige Expansion
2010–2014	129	Konsolidierung mit Spitzen
2015–2019	112	Moderate Erweiterung
2020–2025	155	COVID-Digitalisierungsschub

Enthält nur Domänen mit öffentlich verfügbarem Registrierungsdatum (schließt .de-Domänen aus)

- **BMI wirkt „klein“, weil die nachgeordnete IT unsichtbar ist:** BSI, BKA, Bundespolizei, BBK usw. sind extern kaum sichtbar. Sie minimieren gezielt ihre Angriffsfläche (VS-Bereiche, starke Segmentierung). Ihre tatsächliche Größe ist von außen nicht messbar.
- **Zwei Konsequenzen**
  - Für die Sicherheit: Geringe externe Sichtbarkeit ist hier gewollt und gut – sie ist ein Sicherheitsmerkmal.
  - Für den Vergleich: Ministerien lassen sich nicht an Kern-IT messen. Wer nur das Ministerium betrachtet, unterschätzt Ressorts mit großen nachgeordneten Bereichen (BMI, BMDV, BMG).

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

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

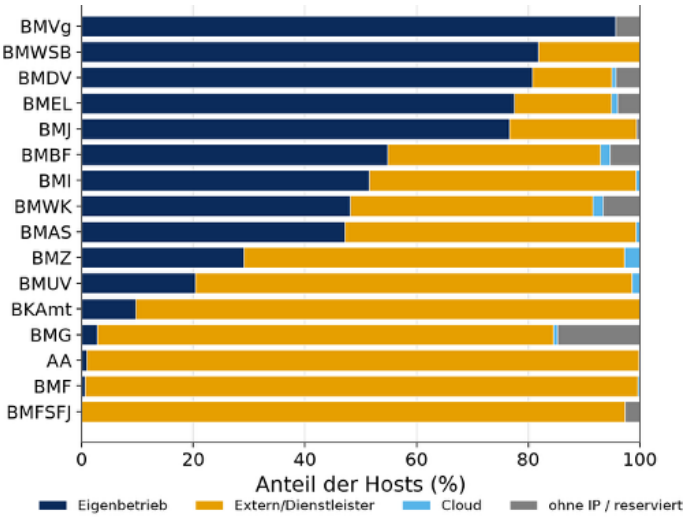
Sicherheit der IT der Bundesministerien 5/15

3. Die Dienstleister prägen die Architektur

BMVg, BMWSB, BMDV, BMEL, BMJ betreiben über 75 % ihrer IT selbst:
Eigene Rechenzentren und IP-Bereiche, dedizierte IT-Dienstleister (z. B. BWI für BMVg). Der Eigenbetrieb entsteht meist aus der historischen Infrastruktur der Fachbehörden.

BMBF, BMI, BMWK, BMAS haben 40-60 % Hybrid / Mischung aus eigenem und externem Betrieb:
Eigene IP-Bereiche lokal, Web-Auftritte extern gehostet, usw.

BMF, AA, BMG, BKAmt, BMUV, BMZ, BMFSFJ haben wenig Eigenbetrieb. Über 70 % sind ausgelagert durch private Dienstleister.



- **Das Betriebsmodell ist eine Sicherheitsentscheidung.** Wer den Dienstleister wählt, wählt die Architektur und das Sicherheitsmodell gleich mit – meist implizit im Vergabeverfahren, nicht aufgrund einer Sicherheitsstrategie. Auslagerung verschiebt die Verantwortung, aber ohne verbindliche Mindeststandards im Vertrag verschwindet sie: Extern betriebene Systeme weisen in den Daten mehr und ältere Schwachstellenfunde auf als der Eigenbetrieb (bei „Medium“ bis zu 3,4-fach).
- **Kein Modell ist per se sicher.** Eigenbetrieb bindet Personal und trägt die größten Altlasten; Auslagerung ist nur so gut wie der Vertrag; Cloud wird genutzt, aber nicht sicher konfiguriert. Der Hebel liegt nicht in der Wahl des Modells, sondern in prüfbaren Sicherheitsauflagen für alle drei, verankert in Beschaffung und Vertrag.

Cloud-Nutzung ist gering, aber US-dominiert: 60 % kommen von US-Anbietern.

Deutsche Hosting-Anbieter (z. B. Hetzner, IONOS, Strato, T-Systems) werden als traditionelle Hoster genutzt. Hosting liefert Infrastruktur – Cloud liefert ein ganzes Betriebsmodell.
ITZBund (der zentrale Bundesdienstleister) spielt extern nur eine Randrolle (ca. 3 %).

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

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Bundesministerien 6/15

4. Architektur-Archetypen der Bundesministerien

16 Ressorts, 7 Bauweisen, und jede Bauweise hat ein anderes Sicherheitsprofil. Ein einheitlicher „Stack“ müsste 7 Ausgangslagen gleichzeitig treffen.

Archetyp	Ministerien	Merkmal (was man sieht)	Sicherheitsfolge (was es bedeutet)
Apache-Monokultur (30-59 %)	BMEL, BMF, BMWSB	Historisch gewachsen Zentrale IT-Vorgaben → homogene, klassische Behörden-IT	Dieselben alten Apache-CVEs bleiben ungepatcht auf Servern; höchster CMS-CVE-Prozentsatz
Apache + TYPO3 Bundes-CMS auf Apache	BMAS, BMUV, BMBF	Inhaltsgetriebene Weblandschaft; Abhängigkeit von CMS-Ökosystem; oft externe Agenturen beteiligt	Hohe Plugin/Extensions-CMS-CVE Anteile, bei BMBF zusätzlich Nginx-Anteil; verteilte Dienstleister = verteilte Verantwortung; Integrationsprobleme; unterschiedliche Sicherheitsmodelle.
Linux/Apache und Windows/IIS + ASP.NET	BMI	Historisch unterschiedliche Projekte; organisatorische Silos; institutionelle Fragmentierung, mehrere IT-Dienstleister / Fachabteilungen	Erhöhte Patch- und Konfigurationskomplexität; mehr Angriffsvektoren
Ungeplanter Multi-Stack Apache + Nginx + PHP + diverse	BMWK, BMZ, BMG, BMDV, BMFSFJ	Heterogene und fragmentierte Technologie; keine architektonische Konsolidierung; schwache Governance; kaum zentrale Steuerung	Historisch gewachsene IT; nachgeordnete Behörden
HAProxy-Reverse-Proxy	AA, BKAmt,	Trennung von Edge und Application; Architektur mit Sicherheitsfokus	Sicherheitsorientiertes Reverse-Proxy-Modell. Security-Bewusstsein und „minimal exposure“-Ansatz: so wenig wie möglich nach außen sichtbar
Security-Only Check Point + OpenSSH	BMVg	Nur Firewall, SSH, Sicherheits-komponenten extern sichtbar; kein Server/App exponiert; stark segmentiert; Apps in internen Netzen	Minimale externe Angriffsfläche; VS-NfD-Sicherheitsarchitektur; BWI betrieben
ADC/WAF-Edge vor Apache (F5 BIG-IP)	BMJ	Kommerzielle Application-Delivery-/WAF-Appliance (F5 BIG-IP) als Sicherheits-Edge; Apache-/Nginx-Origin liegt verdeckt dahinter. Zentral gesteuert. Kleine konsolidierte und einheitliche Angriffsfläche, zentrale Durchsetzung.	Zentrale Durchsetzung, kleine und einheitliche Angriffsfläche — der Edge wird damit aber zum Single Point of Failure. Appliances dieser Klasse (z. B. F5 BIG-IP) waren wiederholt Ziel kritischer, aktiv ausgenutzter Schwachstellen; ein kompromittierter Edge exponiert die verdeckten Origin-Systeme dahinter.

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

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Bundesministerien 7/15

5. Heterogenität der IT der Ministerien ist nicht Ineffizienz, sondern fachliche Notwendigkeit

Warum unterscheidet sich die IT der Ministerien?

- **Ressortprinzip (Art. 65 GG):** Jeder Bundesminister in seinem Geschäftsbereich handelt eigenverantwortlich: Betreibt IT mit eigenen Dienstleistern, Zertifizierungsstellen, Domänen-Strategien und Nameserver-Infrastrukturen. Definiert eigenen Technologie-Stack.
- **Verschiedene Aufgaben:** Die IT der Bundesministerien ist nicht zufällig heterogen. Sie ist heterogen, weil die Ressorts völlig unterschiedliche Aufgaben erfüllen: Verteidigung, Diplomatie, Wettervorhersage, Epidemieüberwachung, Agrarforschung, Messtechnik, Finanzverwaltung, Justiz, Innere Sicherheit.
- **Verschiedene Technologien:** Das BMVg braucht sicherheitsorientierte Infrastrukturen (VS-NfD), das AA globale diplomatische Infrastrukturen, das BMDV/DWD Hochleistungsrechner für Wettermodelle, das BMG/RKI epidemiologische Fachsysteme, das BMWK technische und wirtschaftsbezogene Spezialverfahren, das BMEL Forschungs- und Behörden-IT. Diese Systeme lassen sich nicht sinnvoll in eine einheitliche Architektur und ein Betriebsmodell pressen.
- **Verschiedene Dienstleister:** Wer Babiel wählt, bekommt HAProxy. Wer BWI wählt, bekommt Check Point. Die IT-Architektur-Entscheidung wird implizit beim Vergabeverfahren getroffen, nicht notwendigerweise basierend auf einer bewussten Sicherheitsstrategie.
- **Historische Entscheidungen:** Historische Entscheidungen prägen die IT der Ministerien massiv; sie wirken über die Infrastruktur, Technologie-Stacks, Architekturprinzipien, Organisationsstrukturen und Fusionen.
- **Nachgeordnete Behörden:** Die IT-Komplexität eines Ministeriums korreliert direkt mit der Anzahl und Fachkompetenz seiner nachgeordneten Behörden. Die meisten Ministerien sind selbst kleine IT-Organisationen. Nachgeordnete Behörden (Bundesämter, Bundesanstalten, Forschungsinstitute) mit eigenem Fachauftrag, Budget und Dienstleistern machen zwischen 30 und über 80 % der Infrastruktur aus.

- Ein einheitlicher Bundes-IT-Stack trifft damit auf völlig unterschiedliche Realitäten.
- Die Konsequenz sollte nicht „ein Stack für alle“ sein, sondern gemeinsame Plattformen dort, wo die Aufgaben gleich sind (Massenverfahren, Bürgerdienste, Basis-Bausteine), und verbindliche, prüfbare Mindest-Baselines dort, wo die Aufgaben verschieden bleiben müssen (Fach-IT der Ressorts und ihrer nachgeordneten Behörden). Vereinheitlicht wird die Sicherheitsanforderung, nicht die Technologie.

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

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

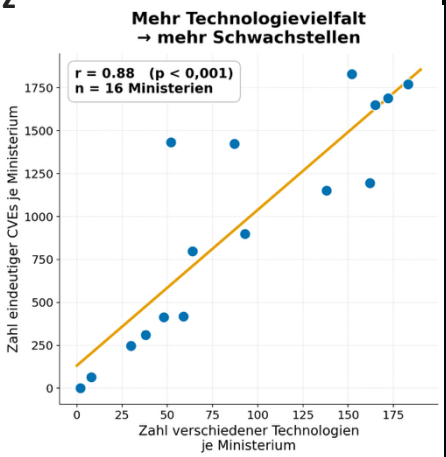
ATHENE Cybernation Deutschland

Sicherheit der IT der Bundesministerien 8/15

6. Technologievielfalt treibt die Schwachstellen

Parallelbetrieb → mehr Schwachstellen, weniger Resilienz

- Zahl der Technologien und Zahl der Schwachstellen laufen eng zusammen (r = 0,88). Absolut wächst beides mit der Größe. Das Risiko steckt in der Zahl der parallelen Schichten.
- Das bedeutet: zusätzliche verschiedene Systeme „addieren" das Risiko. Jede Schicht bringt eigene Patches, Konfigurationen und CVEs.
- Parallele/doppelte Lösungen kosten mehr Geld, binden mehr IT-Personal und reduzieren die Sicherheit.



Jeder Punkt ist ein Ministerium

Staatliche Digitalisierungs- und Modernisierungsprogramme fordern Aufbau und Wiederverwendung, aber praktisch nie Abschaltung mit Termin und Zuständigkeit

- Wir zählen über 10 Initiativen/Strategien (DE-Stack, OZG 2.0, NOOTS, DVC, BMDS-Mod. Agenda, NIS2-Umsetzungsgesetz, KRITIS, …)
- Dadurch entstehen Parallelbetrieb, Technologievielfalt, ungepatchte Systeme, verwaiste Domänen, Zertifikatsfehler und unklare Betreiberverantwortung.
- Die deutsche Digitalpolitik erkennt Fragmentierung, adressiert sie aber meist durch zusätzliche Standards, Plattformen und Nachnutzung. Sie schafft selten eine verbindliche Pflicht, die alte Schicht abzuschalten.
- Das Wiederverwendungs-*Prinzip* steht auf dem Papier, die Wiederverwendungs-*Praxis* findet aber fast nicht statt. Im **DE-Stack** bezieht sich Wiederverwendung auf die Zukunft (neue Komponenten), nicht auf die Ablösung des Altbestands.
- Beispiele: **EfA-Onlinedienste** „Einer für Alle" (BRH 2025: „größtenteils entweder nur in einem Land bzw. einer Kommune einsetzbar oder gar nicht genutzt"). **FIT-Connect** (operativ seit 2022; kein öffentliches Nutzungsmonitoring, laut FITKO weitere 3–5 Jahren bis zur Flächendeckung)

Ressortneuordnungen und Digitalstrategien erhöhen die Technologievielfalt

- Fusionierte Bereiche/Ressorts tragen mehr parallele Technologie-Versionskombinationen (rund 2,35-fach) und vor allem einen älteren Schwachstellenbestand: Rund 23 % der CVEs stammen von vor 2015 gegenüber 15 % bei Einzelressorts; im Schnitt erhöhen Fusionen die Anzahl der CVEs um 21 %.

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

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

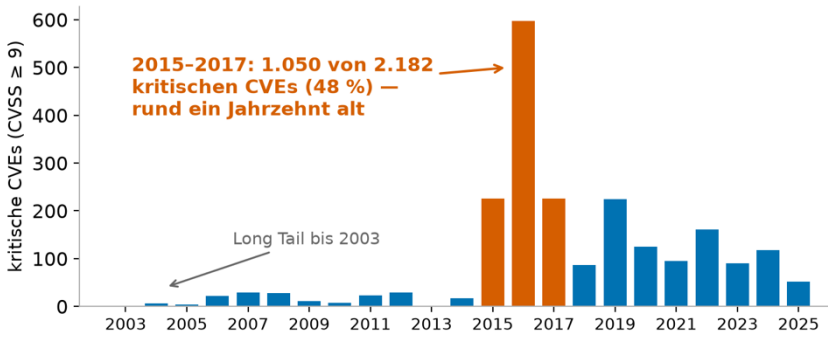
ATHENE Cybernation Deutschland

Sicherheit der IT der Bundesministerien 9/15

7. Nicht Zero-Days, sondern alte ungepatchte Schwachstellen sind das Hauptproblem

Verteilung des Alters von CVEs

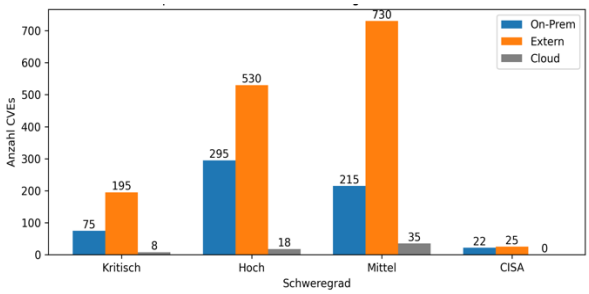
- 15.290 CVEs, über 16 Häuser summiert, mit Durchschnittsalter 7,6 Jahre
- Über **2.182** aktive kritische CVEs (CVSS ≥ 9,0) – häufigstes Alter: Rund **10 Jahre**
- **Ursache:** Patchen zu langsam, alte Systeme werden oft gar nicht mehr gepatcht.
- **Der Schwerpunkt liegt also nicht bei neu entdeckten Zero-Days, sondern bei „alten" Schwachstellen – die für Angreifer besonders interessant sind, da es dafür fertige und mit hoher Wahrscheinlichkeit funktionierende Exploits gibt.**



Kritische CVE-Funde (Host-Ebene) je Ministerium nach Betriebsmodell

Extern gehostete Systeme haben mehr Schwachstellen-Funde als Eigenbetrieb (On-Prem) absolut und je Host: Beide Modelle stellen fast gleich viele Systeme. Ursache: Verantwortung diffundiert.

Auch Eigenbetrieb ist Patch-träge. Fast überall Peak bei 1-2 Jahren. Restanteile bei 4-6 Jahren. Große Anteile kritischer CVEs auch bei 2-4 Jahren, und auch älter als 5.



Kritische CVE-Funde auf Host-Ebene, Durchschnitt je Ministerium, nach Betriebsmodell (absolute Zahlen)

Host-Ebene: ein CVE auf mehreren Hosts zählt mehrfach (≈ 4.046 kritische Funde gesamt). Nicht zu verwechseln mit den 2.182 kritischen CVEs.

End-of-Life (EoL): IT jenseits des Herstellersupports, nie abgelöst

Keine Einzelfälle, sondern systematisches Versagen im Patch-Management.

Nach EoL ist Patchen unmöglich.

Technologie	Betroffene Ministerien	Älteste Version	End-of-Life
PHP 5.x	11	PHP 5.4.16	12.2018
Apache 2.4.6	Mehrere	Juli 2013	-
OpenSSL 1.0.2k	7	Januar 2017	12.2019
jQuery 1.x/2.x	14	jQuery 1.11.1	2016/2017
OpenSSH 6.x/7.x	12	OpenSSH 6.7p1	-

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

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Bundesministerien 10/15

8. Kein Ministerium erfüllt die Mindeststandards

Verschlüsselung

- 6 % der Dienste unterstützen veraltete TLS-Versionen (TLS 1.0/1.1 – seit 2020 unsicher). Bei einzelnen liegt der Anteil bei bis zu 18 %.
- 13 % anfällig für CRIME-Angriff, 4 % ROBOT, 17 % ohne Forward Secrecy.
- Teilweise bis zu 55 % nur über HTTP.
- 26 % aller Zertifikate passen nicht zum Domänennamen → Authentisierungsfehler; Systeme können keine sichere Verbindung aufbauen.
- **32,5 % abgelaufene/fehlerhafte Zertifikate.** Ursache: Kein zentrales Management. Gefahr: Nutzer klicken Browser-Warnungen weg. Folge: Phishing, Man-in-the-Middle-Angriffe
- Legacy-Domänen mit veralteten Ministeriumsnamen.

Web-Sicherheit

- Der Mindeststandard für Websicherheit wird von keinem Ministerium erfüllt.
- Apache 2.4.6 ist in mehreren Ministerien noch aktiv - über 12 Jahre veraltet und Support endete am 30.06.2024, seitdem gibt es keine Sicherheits-Backports mehr
- 86 % ohne CSP: Angreifer können bei einer Lücke beliebigen JS-Code im Kontext einer Ministeriums-Webseite ausführen.

DNS-Lifecycle-Management

- 4 DNS-Einträge verweisen auf nicht mehr existierende Cloud-Ressourcen. Folge: Angreifer können Ministeriums-IT hijacken.
- 14 veraltete interne und 22 externe DNS-Einträge.

E-Mail-Sicherheit

- 45 % aller E-Mail-Domänen haben keinen wirksamen Schutz. Fast die Hälfte aller ministeriellen E-Mail-Domänen können von Angreifern zum Versand gefälschter E-Mails missbraucht werden

Exponierte Netzdienste (SSH 731 · FTP 490 · MySQL 335)

- Ursache: Fehlende Netzsegmentierung; Verwaltungs-/Datenbankdienste aus dem Internet erreichbar.
- Gefahr: Brute-Force, Passwörter (FTP), offene Datenbanken. Folge: Server-Übernahme und Datenabfluss.

Wann betrachten wir ein Ministerium als „konform“?

- Ein Ministerium gilt als nicht konform, sobald mindestens ein extern erreichbarer Dienst gegen den jeweiligen BSI-Mindeststandard (TLS, Web, DNS, Mail) verstößt.
- Unabhängig bestätigt: Der Bundesrechnungshof (2025) stellt fest, dass weniger als 10 % der 100 Rechenzentren des Bundes die BSI-Mindeststandards erfüllen.

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

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Bundesministerien 11/15

9. Was die Studie für Sicherheit und Politik bedeutet – Teil 1:

Governance muss genau dort ansetzen, wo das Risiko liegt

Die Hauptprobleme sind banal

- Alte CVEs, abgelaufene Zertifikate, fehlende E-Mail-Verifizierung, exponierte Basisdienste, kompromittierte Konten. Keine Zero-Days, vermeidbare Grundhygiene
- Kein Betriebsmodell schützt automatisch: Cloud wird genutzt, aber nicht sicher konfiguriert; Auslagerung verschiebt Verantwortung ohne Mindeststandards; Eigenbetrieb trägt die größten Altlasten. Wirkung braucht vertragliche Vorgaben und verbindliche Standards.

Das Spezifische der Ministerien

- Die Angriffsfläche sitzt nicht im Ministerium, sondern im Geschäftsbereich: In den gemessenen Beispielen (BMI, BMAS, BMF) gehören 88-93 % der extern sichtbaren Hosts zu nachgeordneten Behörden und Dienstleistern.
- Vorgaben an die Ministerialverwaltung allein greifen deshalb systematisch daneben. Steuerung muss Behörden und Dienstleister vertraglich erfassen.

Empfehlungen

- Vollständiges Asset-Register über alle TLDs und Betriebsmodelle:
  Man kann nur schützen, was man sieht.
- Verbindliche, prüfbare Sicherheits-Baselines in jedem Beschaffungs-/Betreibervertrag
- Abschaltpflicht mit Termin und Zuständigkeit für alle Altsysteme
- Wirkung extern messen: Angriffsflächen-KPI statt Compliance-Nachweis.

Was folgt daraus für die deutschen Strategien?

- Die Befunde betreffen die beiden Arten von Programmen, die die Bundes-IT derzeit prägen:
  - Digitalisierungsstrategien, insbesondere der DE-Stack als geplante nationale souveräne Technologie-Plattform (→ Teil 2)
  - Cybersicherheitsstrategien, die NIS2-Umsetzung (NIS2-UmsG in Kraft seit 12/2025) und das am 22. Juli 2026 vom Kabinett beschlossene Programm CyberGovSecure (→ Teil 3). Der Kreis regulierter Einrichtungen wächst von rund 4.500 auf etwa 29.500. Konkrete Fristen fehlen weiterhin und die Wirkung bleibt offen.
- Beide bauen auf demselben Bild der Bundes-IT auf – und erben damit dessen Lücken. Wir erklären die Bedeutung und die Folgen der politischen und fachlichen Dimensionen

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

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Bundesministerien 12/15

9. Was die Studie für Sicherheit und Politik bedeutet – Teil 2:

Bedeutung für Digitalisierungsstrategien – DE-Stack droht, Fehler zu wiederholen

Bisherige Strategien waren nur mäßig erfolgreich

Dienstekonsolidierung

Bundesrechnungshof zu 10 Jahre IT-Konsolidierung Bund (und Netze des Bundes

- Laut Berichterstattung rund 836 Mio. € ausgegeben; laut BRH wurde die Kennzahl „Nutzungsgrad“ fallengelassen – wie viele Beschäftigte die zentralen Lösungen tatsächlich nutzen, weiß der Bund selbst nicht. Alte und neue Systeme laufen parallel; der Bund zahlt doppelt.
- Kosten von ITK-Bund von rund 1 Mrd. € auf über 3 Mrd. € gestiegen; die geplante Reduktion auf wenige Rechenzentren wurde aufgegeben.
- IAM Bund (Identitätsmanagement, ca. 23 Mio. €) nach neun Jahren vom BMI an das BMF übergeben; das Programm hat seine Ziele verfehlt.

Aktuelle Deutschland-Stack-Strategie droht, Fehler zu wiederholen

Deutschland-Stack

Kleine Anzahl an Basisdiensten + Versprechen, „die nationale souveräne Technologie-Plattform für die Digitalvorhaben in Deutschland“ bereitzustellen.

- Jenseits Basisdienste fehlen: Betriebene Dienste, Betreibermodell, verbindliche und prüfbare Standards, Migrations- und Abschaltstrategie, gesichertes Budget, Messung und Konformitätsprüfung, Sicherheitsanforderungen und Baseline

- Wiederverwendung wird nur für *künftige* Dienste gefordert. Die Vergangenheit wird nicht betrachtet. Technologiewachstum, Parallelbetrieb und damit Unsicherheit sind vorprogrammiert.
- Die real vorhandene, fachlich begründete Heterogenität wird *ausgeklammert* oder für problematisch erklärt. 16 Ministerien, 7 Technologie-Archetypen, ca. 75,5 verschiedene Technologien pro Ministerium/Fachressorts können nicht mit einem einzigen, einheitlichen Technologiestack bedient werden. Dasselbe gilt für die IT der übrigen Bundes- und Landesverwaltungen.

Quelle: „Vorgehensmodell zur Entwicklung der Deutschland-Architektur“; BMDS, 3.6.2025

Was DE-Stack und Digitalisierungsstrategien allgemein daraus lernen müssen

- Digitalisierung braucht mehr attraktive und breit nutzbare Basisdienste plus digitale, schnelle und nutzbare Angebote für Massenverfahren
- Gemeinsame Plattformen dort, wo Aufgaben gleich sind. Mindest-Baselines dort, wo Fach-IT verschieden bleiben muss. Vereinheitlicht wird die Sicherheitsanforderung, nicht die Technologie.
- Erfolgskriterium ist die gemessene Nutzung, nicht der Rollout.
- Abschaltpflicht für Altsysteme mit Termin und Zuständigkeit.

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

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Bundesministerien 13/15

9. Was die Studie für Sicherheit und Politik bedeutet – Teil 3:

Politische Dimension und Bedeutung für die Cybersicherheitsstrategien

Programm der Bundesregierung zur Steigerung der Cybersicherheit in der Bundesverwaltung (CyberGovSecure)

Was beschlossen wurde

Am 22. Juli 2026 hat das Bundeskabinett das Programm *CyberGovSecure* für die Bundesverwaltung beschlossen. Das BSI hat dafür 9 Handlungsfelder identifiziert. Die strategische Steuerung übernimmt ein Lenkungskreis unter BMDS-Vorsitz, die operative Umsetzung der CISO Bund (BSI-Präsidentin) mit den Sicherheitsbeauftragten der Ressorts.

Zwei Dimensionen, zwei Verantwortungsbereiche

Die Defizite des Programms verteilen sich auf zwei Verantwortungsbereiche:

- Die *fachliche Dimension* verantworten die Organisationen, die die Bundes-IT kennen und steuern müssen: BSI/CISO Bund und die CIO-Organisationen des Bundes und der Ressorts.
- Die *politische Dimension* verantwortet die Politik: Kabinett und Lenkungskreis entscheiden über Fristen, Messgrößen, Budgets und Verbindlichkeit.
- ***Verbindlichkeitslücke* selbst liegt in beiden Bereichen: Ohne fachlich nachgewiesene Wirkung wird den Behörden die Motivation fehlen, ohne politische Fristen und Budgets die Pflicht.**

Bewertung: Politische Dimension

- Formal erfasst sind die Einrichtungen des Bundes gemäß § 29 BSIG, aber die den Ressorts nachgeordneten Behörden sind in der Governance nicht direkt vertreten. Auch die operative Struktur kennt zunächst nur die Sicherheitsbeauftragten der Ressorts.
- Die Umsetzung wird an jede Behörde selbst delegiert. Die Verantwortung verbleibt daher bei der jeweiligen Leitung. Die Koordination erfolgt durch CISO Bund und die „jeweiligen Sicherheitsbeauftragten der Ressorts“ – also in derselben Ressortstruktur, die den Ist-Zustand hervorgebracht hat.
- Keine Fristen; Zielwerte unbeziffert/Ressorts vorbehalten; keine Budgetangaben.
- Erfolgskontrolle ist ein „aufwandsarmes“ Berichtswesen, also voraussichtlich Selbstauskunft.

CyberGovSecure tritt in ein bereits dicht besetztes Feld aus Konsolidierungsprojekten, Cloud- und Infrastrukturvorhaben, Sicherheitsvorgaben und Koordinierungsgremien. Das Programm schafft eine weitere Steuerungsebene, ohne bestehende Vorhaben zusammenzuführen. Damit besteht die Gefahr, dass es die Steuerungs- und Umsetzungslücke, die es schließen soll, zunächst fortschreibt.

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

ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Bundesministerien 14/15

9. Was die Studie für Sicherheit und Politik bedeutet – Teil 3a:

Fachliche Dimension und Bedeutung für die Cybersicherheitsstrategien

Strategien beruhen auf dem Bild, das BSI und CIO-Organisationen dem Lenkungskreis liefern

Bild des BSI ist strukturell unvollständig: Lagebericht des BSI nennt ca. 3.800 IP-Adressen (Weiße Liste) vs. 36.100 von uns gemessene, d.h. knapp 90 % fehlen. Mehr als 12.100 Befunde außerhalb.

ISMS/IT-Grundschutz Assetmanagement verfehlt externes Oberflächenrisiko

- Programm benennt Assetmanagement als Handlungsfeld. Laut BSI-Definition ist Assetmanagement wie IT-Grundschutz-Strukturanalyse (BSI-Standard 200-2), NIS-2-Infopaket und ISO-27001-Tradition: ein Verwaltungsprozess über die Systeme, die die Organisation *selbst* kennt und betreibt. Die externe Entdeckung unbekannter oder vergessener Systeme ist in dieser Definition nicht enthalten. Ohne eine explizit von außen ansetzende Erfassung bleibt genau das Segment unadressiert, in dem sich der Zuwachs verwertbarer Schwachstellen konzentriert:
- Vollständigkeit lässt sich von innen nicht feststellen – und Schwachstellenmanagement schließt diese Lücke nicht, sondern erbt sie, weil es auf der Asset-Liste aufsetzt.
- Ein Inventar verwaltet vorhandene Objekte, aber erfasst externe Befunde nicht, etwa DNS-Einträge auf gelöschte Cloud-Ressourcen (Übernahmerisiko).
- Das Risiko liegt jenseits der „betrieblichen IT-Assets“: Extern betriebene IT (Dienstleister, Agenturen, Projektträger) und angebundene externe Assets bleiben ausgeschlossen.
- Nachgeordnete Behörden sind erfasst aber nicht vertreten: laut ATHENE-Studie für einen großen Teil der gemessenen Angriffsfläche verantwortlich (88-93 % der externen sichtbaren Hosts).
- Das Programm will „Risiken durch undokumentierte und veraltete Assets" identifizieren, doch diese Risiken sind längst bekannt. Es fehlt beides andere: eine Methode, die undokumentierte Assets überhaupt findet (vorgesehen sind nur behördeninterne Scans und Selbstdokumentation, keine externe Erfassung), und für veraltete Assets ein Ziel und ein geregelter Prozess der Abschaltung, mit Termin, Zuständigkeit und definierten Ausnahmen.
- Programme, die auf einem unvollständigen Bild der Bundes-IT beruhen, sind nur beschränkt wirksam. Risiko: Betroffene Behörden betrachten sie als Aufwand ohne Sicherheitsgewinn. Wirkung messbar zu machen ist eine fachliche Aufgabe. Ohne diese Messbarkeit hat die Politik nichts, womit sie die Umsetzung wirkungsvoll steuern und durchsetzen könnte.

Beschaffung und Betreiberverträge fehlen als Handlungsfeld

- Die IT-Architektur eines Ressorts wird maßgeblich im Vergabeverfahren geprägt - wer den Dienstleister wählt, wählt das Sicherheitsmodell mit; extern betriebene Systeme zeigen mehr und ältere Schwachstellenfunde. Nur wer die Rolle der Dienstleister im Bild hat, erkennt den Vertrag als zentralen Sicherheitshebel.

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

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

ATHENE Cybernation Deutschland

Sicherheit der IT der Bundesministerien 15/15

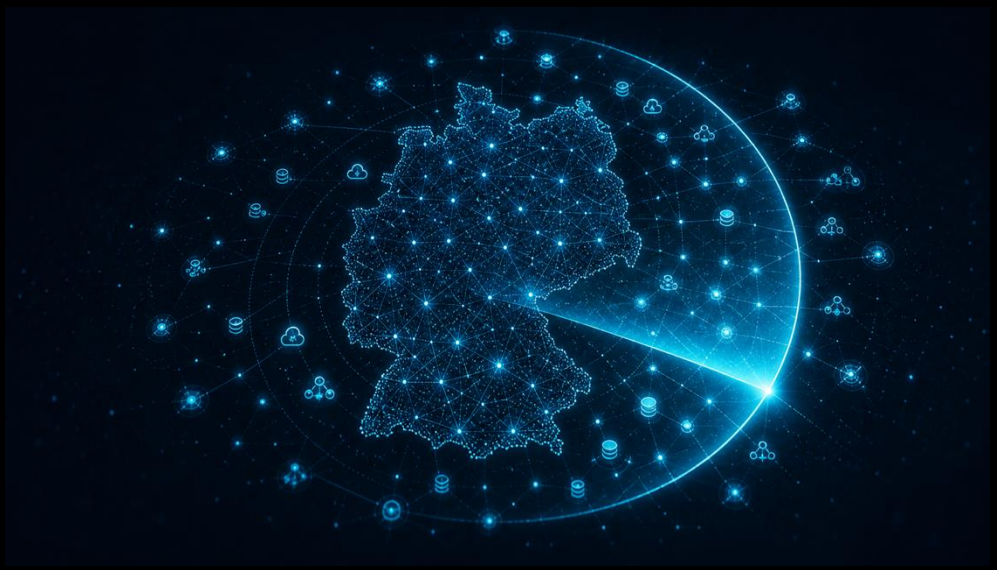
9. Was die Studie für Sicherheit und Politik bedeutet – Teil 3b:

Fachliche Dimension und Bedeutung für die Cybersicherheitsstrategien

Fazit: Was sich ändern muss – Politisch und fachlich

- Programme müssen von der Politik verbindliche, öffentlich kommunizierte Fristen, Messgrößen und Budgets erhalten. Nur so können Ziele erreicht und Wirksamkeit demonstriert werden.
- Programme dürfen keine fachlich unbegründeten Ausnahmen und Beschränkungen enthalten. Der Geltungsbereich wichtiger Programme muss zweifelsfrei alle nachgeordneten Behörden und Dienstleister umfassen. Definierte Baselines müssen in jedem Beschaffungs-/Betreibervertrag verbindlich vorgegeben werden.

- Programme müssen auf einer soliden und vollständigen Wissensbasis aufbauen. Die Bundesverwaltung braucht ein *extern* validiertes Asset-Register über alle TLDs, Betriebsmodelle und Geschäftsbereiche hinweg, einschließlich aller Dienstleister. Der Lagebericht des BSI muss die tatsächliche Angriffsfläche erfassen und bewerten.
- Jede Behörde und jedes Vorhaben benötigt einen verbindlich geregelten Prozess zur Abschaltung von Altsystemen, mit Termin, Zuständigkeit und definierten Ausnahmen.
- Die Behörden der Bundesverwaltung müssen in die Lage versetzt werden, ihre eigene tatsächliche Angriffsfläche zu erfassen und gemessene Angriffsflächen-KPIs zu berichten.
- Sicherheits- und Messanforderungen müssen im Sinne von Baselines vereinheitlicht und vertraglich verbindlich an interne und externe Dienstleister und Betreiber weitergegeben werden.



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, sodass jede Haftung für Schäden ausgeschlossen wird, die aus der Benutzung dieser Arbeitsergebnisse bzw. Informationen entstehen können. Diese Haftungsbeschränkung gilt nicht in Fällen von Vorsatz.

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit