Aktuelle Cybersicherheitslage

Veranstaltung: Cybersecurity, 24.11.2025

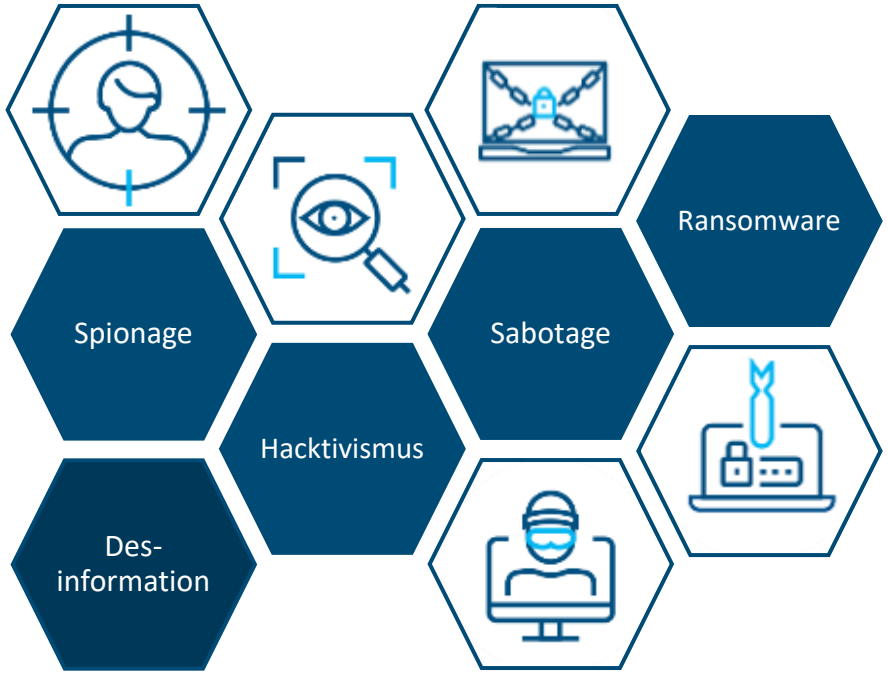
GI Regionalgruppe Köln

Bundesamt
für Sicherheit in der
Informationstechnik

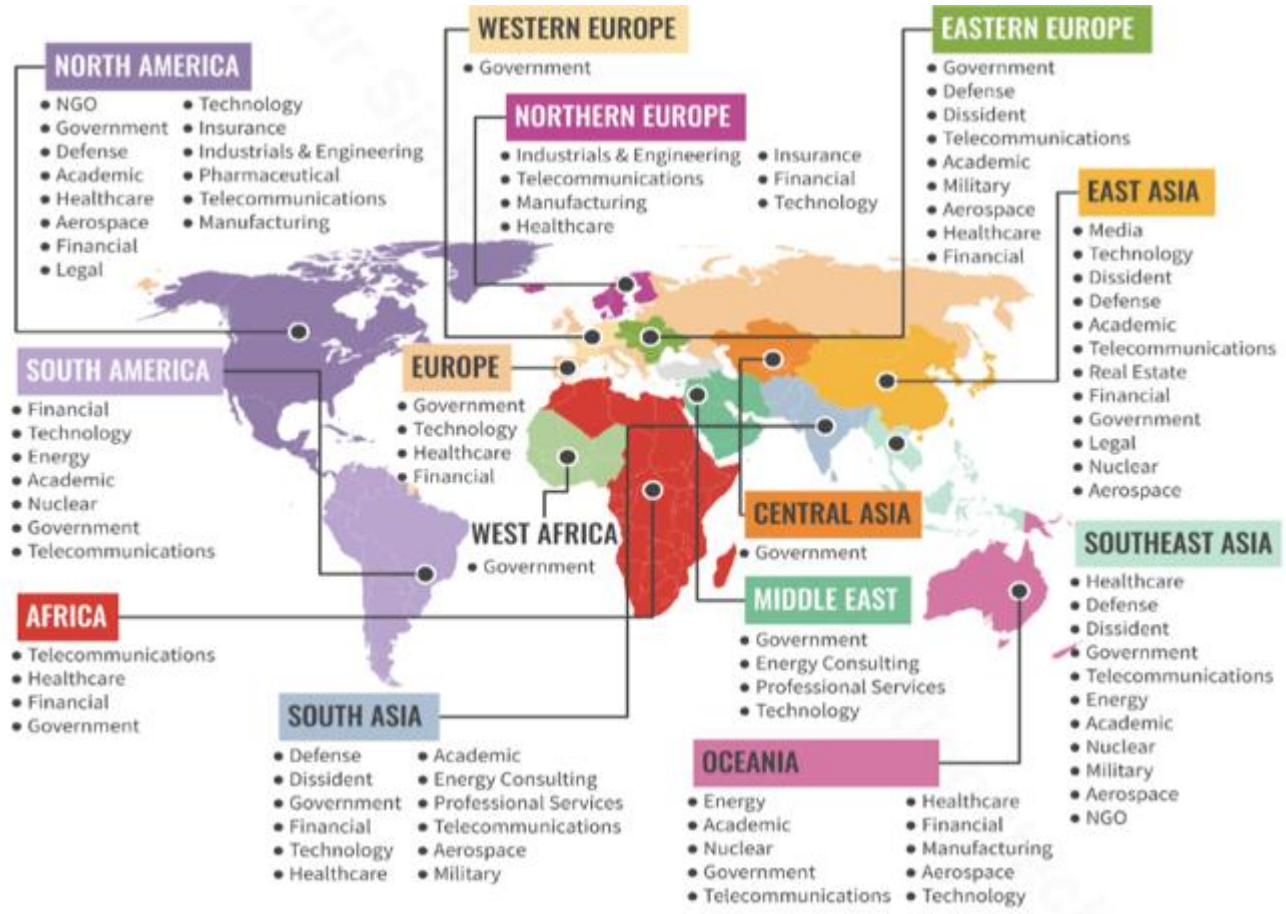
Zeitenwende im digitalen Raum

Bild: © AdobeStock/Azazul

Auswirkungen der aktuellen geopolitischen Verwerfungen



Regions and Sectors Targeted by China-Nexus Activity, 2022



Quelle: CrowdStrike, Annual Threat Report 2022

Unsicherheitsfaktoren:

Russisch-Ukrainischer Krieg, Hegemonialstreben Chinas, Nahostkonflikt, Neupositionierung der USA

BSI

Zahlen, Daten, Fakten

- Standorte: Bonn, Freital, Saarbrücken
- Stellenzahl: **1.785**
- Budget/Haushalt: **237,9** Millionen Euro (2024)
- Präsidentin: Claudia Plattner (seit 2023)

- Operative Cybersicherheit – Lage und CERT
- **Nationales IT-Lagezentrum**: 24/7-Betrieb, Beobachtung & Meldestelle
- Vorfallsbearbeitung: **CERT-Bund**
- **Nationales IT-Krisenreaktionszentrum**
- Kooperation/Kommunikation mit **Cyber-Abwehrzentrum**

- **Geheimschutz**
- BMI/ BMDS: Fachaufsicht, Schnittstelle zur **Politik**

BSI

Lage

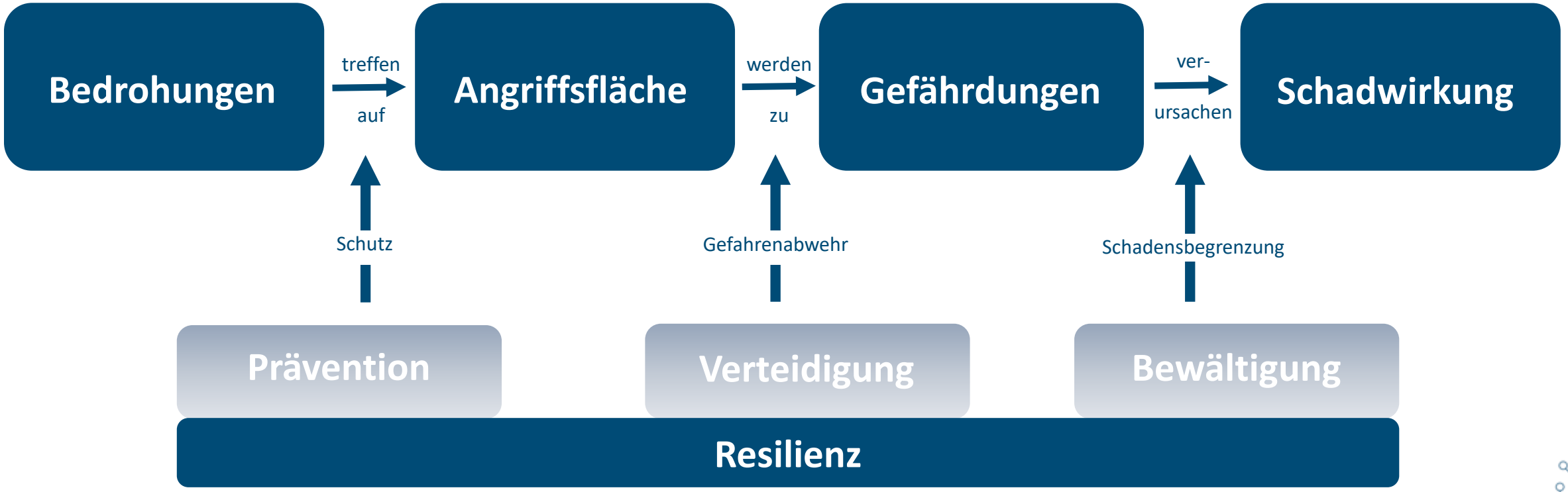
- Situation vs. Lage
- **Lage**: Gesamtschau aller Ereignisse, Vorkommnisse, Entwicklungen
- Beobachtung – Schreibung – Bewertung/Beurteilung - Aktionen

- Nationales IT-Lagezentrum: **Tageslage**
- Tageslage, Wochenlage, **Monatslage, Jahreslage**

- **Auswertungsmethodik:** Kategorisierung**,** Filterung, Verdichtung, Herstellen von Zusammenhängen, Ableitung, Transformation usf.

- **Lage-Produkte:** Lagebilder, Lageberichte, Lage in Zahlen
- Tagesberichte, Wochenberichte, **Monatsberichte**, **Jahresbericht**
- **Struktur der Lageberichte:** Sachverhalt, Bewertung, Maßnahmen

Die Dimensionen der IT-Sicherheit in Deutschland



01 BEDROHUNGEN / THREATS

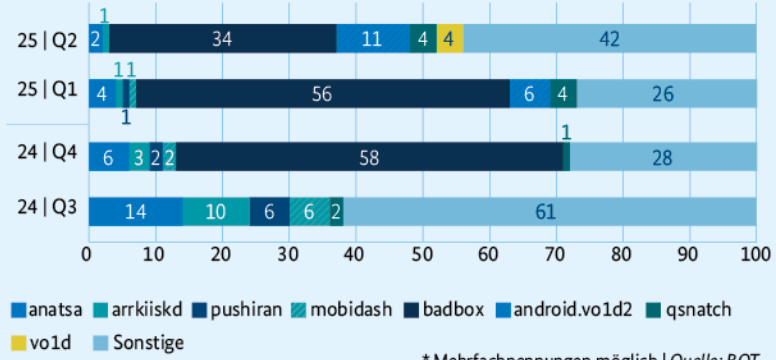
Stabilisierung auf hohem Niveau

75 %

der Advanced-Persistent-Threat-Gruppen, die sich gegen mindestens eines der Top-10-Zielländer richteten, zielten auf die USA.

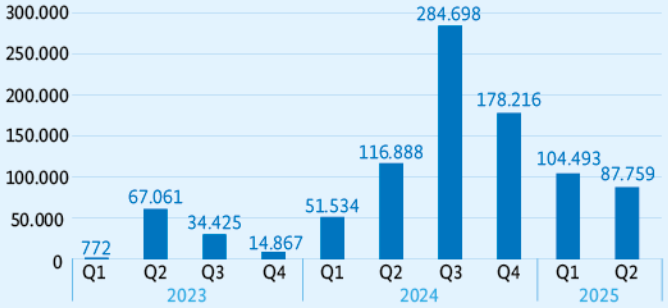
APT-Gruppen (advanced persistent threat) sind sehr gut ausgebildete, oft staatlich gesteuerte Angreifer, die zum Zweck der Sabotage und Spionage gezielt angreifen.

Botnetze nach Unique IP* (Anteile in % an allen Unique IP)



* Mehrfachnennungen möglich | *Quelle: BOT*

Neue malziöse Websiten (Anzahl)



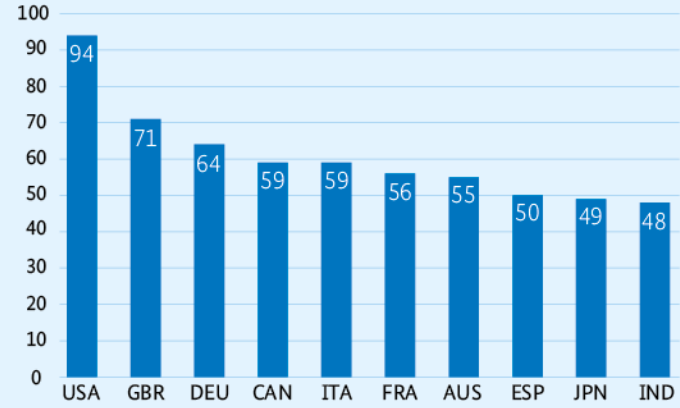
Quelle: MWE

IoT-Geräte kamen mit vorinstallierter Schadsoftware in den Handel.

Im aktuellen Berichtszeitraum wurden mit Badbox und Vo1d zwei neue, große IoT-Botnetze bekannt. Die Malware wurde teilweise bereits während des Produktionsprozesses der IoT-Geräte eingeschleust und konnte vom Nutzenden nicht erkannt werden.

Crime-Gruppen 2025* weltweit nach Zielland

(Top 10, Anteile in %)



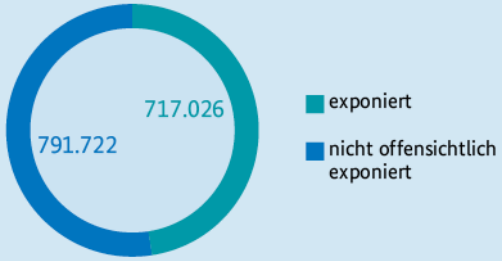
* Mehrfachnennungen möglich | *Quelle: TAS*

02 ANGRIFFSFLÄCHE / ATTACK SURFACE

Web-Angriffsflächen und multiple Kommunikationswege – große Herausforderung

Wie sicher sind deutsche (.de) Websiten?

Erreichbare IP-Adressen* im 2. Quartal 2025 nach Exponiertheit der Metadaten (Anzahl)



* IP-Adressen hinter .de-Domains | *Quelle: WAM*

47,5 %
der erreichbaren IP-Adressen wiesen Sicherheitsmängel auf: teils waren sensible Metadaten oder Schwachstellen einfach einsehbar.

61,3 %
der erreichbaren Domains im deutschen Internet bieten nur den alten weniger sicheren Internet-Protokoll-Standard IPv4.

119 ↗ 24%
durchschnittlich täglich neue bekannt gewordene Schwachstellen

Das waren rund 24 Prozent mehr, als im vergangenen Berichtszeitraum. Ein Teil des Wachstums war auf eine veränderte Melde-Policy der Linux-Kernel-Entwickler zurückzuführen.

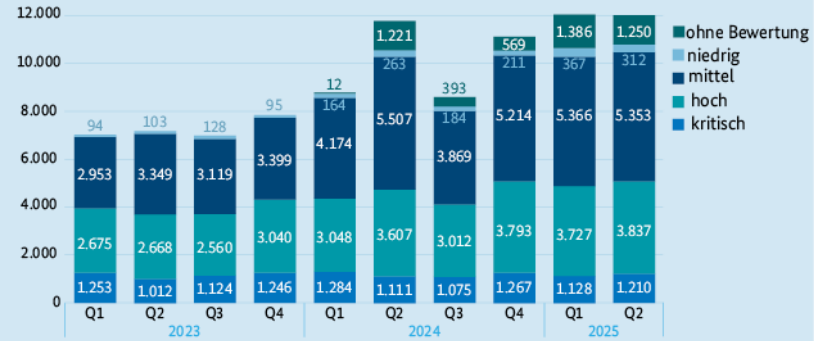
E-Mail- und Social-Media-Angriffsfläche der Bundesverwaltung* (Anzahl)

aktive E-Mail-Adressen in den Netzen des Bundes
Ø täglich 684.000

aktive Social-Media-Accounts der Bundesverwaltung
und 1.480
(hohe Dunkelziffer durch Privat-Accounts von Beschäftigten)

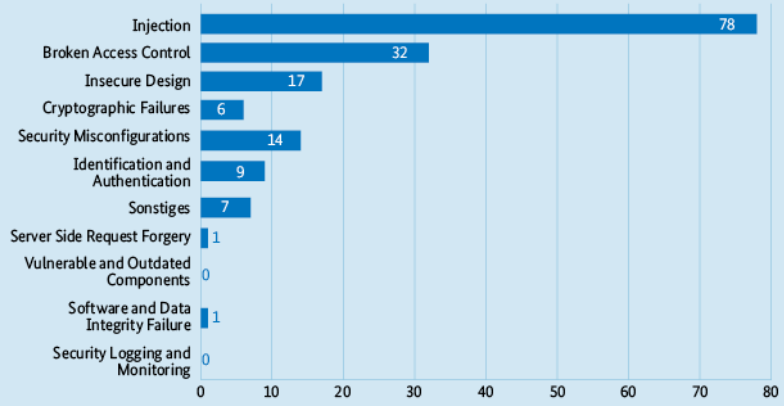
*Ohne Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen. | *Quelle: EBV*

Neu bekannt gewordene Schwachstellen weltweit nach Schweregrad* (Anzahl)



* Revision der Statistik im Februar 2025. Vergleich mit früheren Publikationen nur eingeschränkt möglich. | *Quelle: SSS*

Valide Meldungen schwachstellenbehafteter Produkte* nach Schwäche (Top 10+, Anzahl)



*Mehrfachnennungen möglich, Top 10+ nach OWASP Top 10: 2021 plus Kategorie „Sonstiges“
Quelle: BSI

03 GEFÄHRDUNGEN / ATTACKS

Mehr Exploitation, mehr Datenleaks

Für Deutschland relevante APT-Gruppen 2025 nach Wirtschaftszweig der Geschädigten* (Anzahl)

*Mehrfachnennungen möglich | *Quelle: TAS*

Die meisten Cyberspionage-Gruppen zielten vorwiegend auf die öffentliche Verwaltung.

Insbesondere Institutionen der öffentlichen Verwaltung standen stark im Fokus von Cyberspionen: Fast jede zweite der in Deutschland aktiven APT-Gruppen (13 von 28) hat diesen Sektor ins Visier genommen.

Cybercrime

Rund 80 % der angezeigten Angriffe richteten sich gegen KMU.

950 Anzeigen wegen Ransomware-Angriffen

davon: 72 % mit Datenleaks

Quelle: Bundeskriminalamt

Betroffenheit von Cyberkriminalität

Verbraucherinnen und Verbraucher 2025 nach Betroffenheit von Cyberkriminalität* (Anteile in %)

Betrug	43 %
Betrug beim Online-Shopping	22 %
Datendiebstahl	20 %
Schadsoftware	7 %

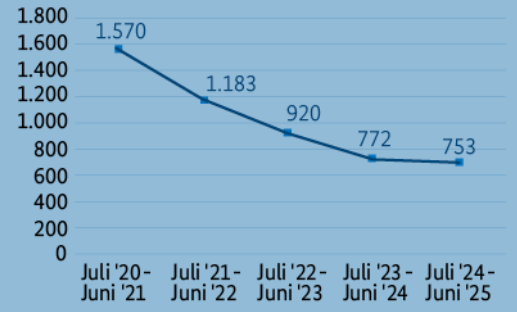
*Mehrfachnennungen möglich | *Quelle: CYM*

950
Anzeigen wegen Ransomware-Angriffen

80 %
davon kleine und mittlere Unternehmen

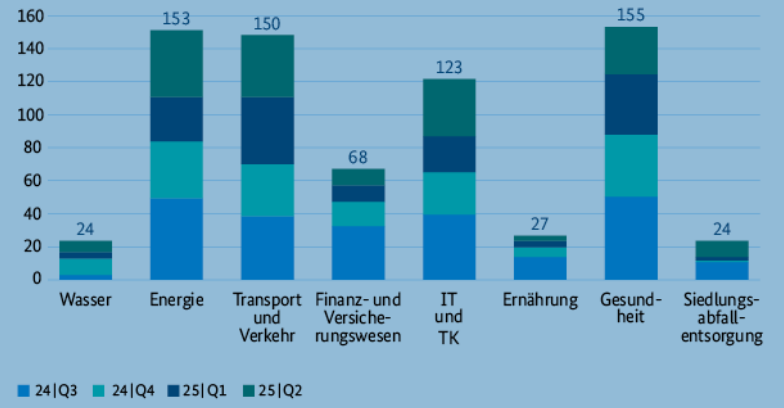
Immer häufiger waren die Angegriffenen nicht nur mit Datenverschlüsselung, sondern auch mit Datenexfiltration und anschließender Erpressung konfrontiert. Kleine und mittlere Unternehmen waren besonders betroffen.

Durchschnittliche tägliche Malware-Angriffe per E-Mail auf die Bundesverwaltung* (Anzahl)



*Ohne Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen. | *Quelle: EBV*

Von Betreibern Kritischer Infrastrukturen gemeldete Störungen* nach Sektor (Anzahl)



*Mehrfachnennungen möglich | *Quelle: KRM*

04 SCHADWIRKUNG / IMPACT

Mehr Datenleaks, mehr Lösegeld

461

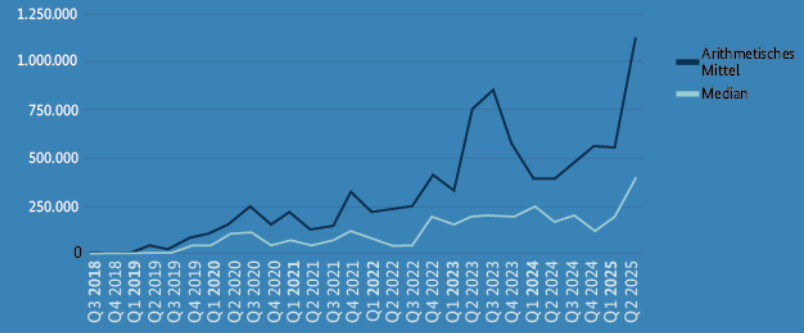
Datenleaks von deutschen Institutionen und Verbrauchenden im Berichtszeitraum

Betroffen waren vor allem Geburtsdaten (92 %), Straßenadressen (72 %) und E-Mail-Adressen (63 %).

Mutmaßlich Geschädigte aus Deutschland auf Leak-Seiten (Anzahl)

Gezählt wird die Nennung einer geschädigten Organisation. | *Quelle: LKG*

Durchschnittliche Lösegeldzahlungen (Dollar)



Quelle: Coveware

Es wurden die durchschnittlich höchsten Lösegelder seit Beginn der Aufzeichnungen beobachtet.

Während die Bereitschaft zur Zahlung von Lösegeldern im aktuellen Berichtszeitraum weiter sank, waren im Zuge von Datenleaks nach Exploitation-Angriffen die durchschnittlich höchsten Lösegelder seit Beginn der Aufzeichnung zu beobachten.

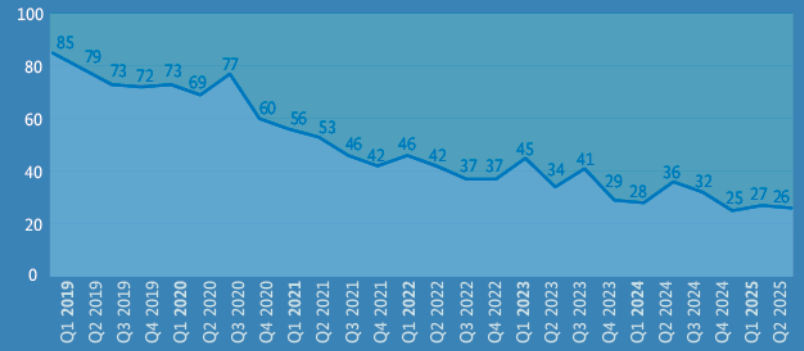
(Quelle: Coveware)

Infizierte Systeme

Die Zahl vernetzter IoT-Geräte verdoppelte sich in den letzten 5 Jahren. IoT-Geräte machen auch in Deutschland einen wachsenden Teil infizierter Systeme aus.

(Quelle: BOT)

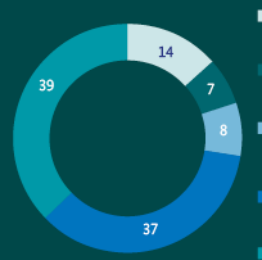
Ransomware-Opfer, die Lösegeld zahlten (Anteile in %)



Quelle: Coveware

05 RESILIENZ

Vom BSI gehaltene CC-Zertifikate nach Themenbereich



- Themenbereich Bankkarten, Pässe, Ausweise u.a.
- Themenbereich Smart Meter Gateways
- Themenbereich Telematikinfrastruktur im Gesundheitswesen
- Themenbereich Standortzertifizierung
- Weitere

6,1
Schutzmaßnahmen kennen die im CyMon befragten Verbrauchenden durchschnittlich

3,8
Schutzmaßnahmen nutzen die im CyMon befragten Verbrauchenden durchschnittlich

Sowohl die Bekanntheit als auch Nutzung von Schutzmaßnahmen waren 2025 weiterhin rückläufig. Neben einem hohen Sicherheitsgefühl gaben auch viele Befragte an, dass sie die Maßnahmen als zu kompliziert empfinden.

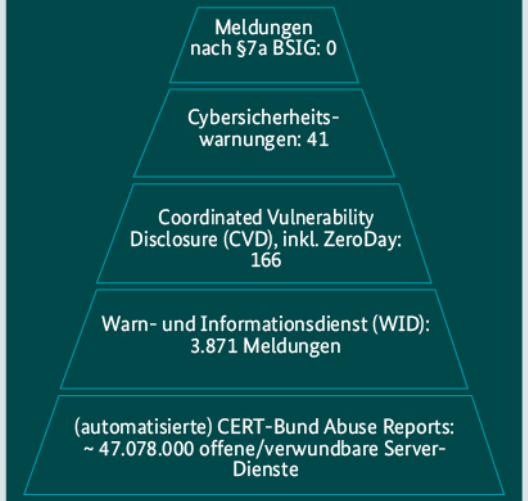
Quelle: CYM

64,1 %

der Betreiber von Kritischen Infrastrukturen haben ein BCMS etabliert und dokumentiert.

Das BSI beaufsichtigt IT-Sicherheitssysteme (ISMS, SzA, BCMS) für Betreiber Kritischer Infrastrukturen (KRITIS).

Prävention für Staat, Wirtschaft und Gesellschaft – Meldesysteme des BSI



Quelle: BSI

78,8 %

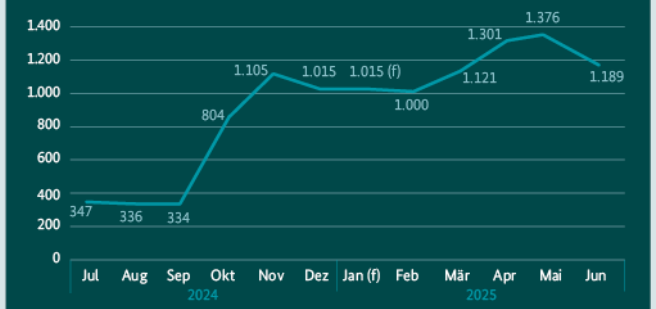
der Betreiber von Kritischen Infrastrukturen haben ein Sicherheitsmanagementsystem etabliert und dokumentiert.

Das BSI beaufsichtigt IT-Sicherheitssysteme (ISMS, SzA, BCMS) für Betreiber Kritischer Infrastrukturen (KRITIS).

Quelle: BSI

Unique-IP-Index (Schadprogramm-Verbreitung)

(Einheit: 2019 = 100)



f: Wert wurde fortgeschrieben | *Quelle: BOT*

BSI-Service-Center

Das Service-Center des BSI ist unter anderem Anlaufstelle für Anfragen von Verbraucherinnen und Verbrauchern zum Thema Cybersicherheit.

Bewältigungsmaßnahmen bei vorinfizierten IoT-Systemen

Mit BadBox vorinfizierte IoT-Systeme, deren Kommunikation mit Kontrollservern blockiert und Gerätebesitzer informiert wurden **ca. 30.000**

Mit Vo1d infizierte IoT-Systeme, deren Gerätebesitzer informiert wurden **ca. 10.000**

Quelle: BSI

49 %

der Betreiber von Kritischen Infrastrukturen haben die MUSS-Anforderungen für ein System zur Angriffserkennung (SzA) erfüllt.

Das BSI beaufsichtigt IT-Sicherheitssysteme (ISMS, SzA, BCMS) für Betreiber Kritischer Infrastrukturen (KRITIS).

Die operative Lage – was uns aktuell bewegt

Bild: © AdobeStock/Azazul

IT-Sicherheitslage in Deutschland auf weiterhin angespanntem Niveau

- Insbesondere unzureichend geschützte Angriffsflächen machen Deutschland im digitalen Raum verwundbar
- Angreifer suchen gezielt nach den verwundbarsten Angriffsflächen.
- Vor allem KMU sowie Institutionen des (vor)politischen Raums betroffen
- Trotz Erfolgen internationaler Strafverfolgungsbehörden gegen Cybercrime-Angreifergruppen:
  - zunehmende Ausnutzung von Schwachstellen (Exploitation)
  - mehr Exfiltration und Veröffentlichung von Daten (Datenleaks)
- Zunahme der APT-Aktivitäten im Kontext geopolitischer Konflikte

IT-Sicherheitslage in Deutschland - Gesamtbewertung

- **Bedrohung**

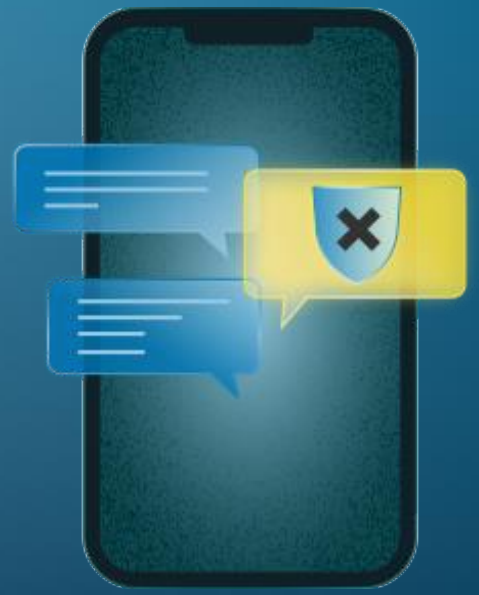
  - Im Cybercrime-Bereich führten internationale Strafverfolgungsmaßnahmen zu einer Stabilisierung auf hohem Niveau

- **Angriffsfläche**

  - Web-Angriffsflächen werden bedeutender.
  - Der Schutz der Angriffsflächen ist entscheidender Hebel

- **Gefährdung**

  - mehr Schwachstellen-Exploits, mehr Daten-Leaks
  - => Die Gefährdungslage ist weiterhin angespannt



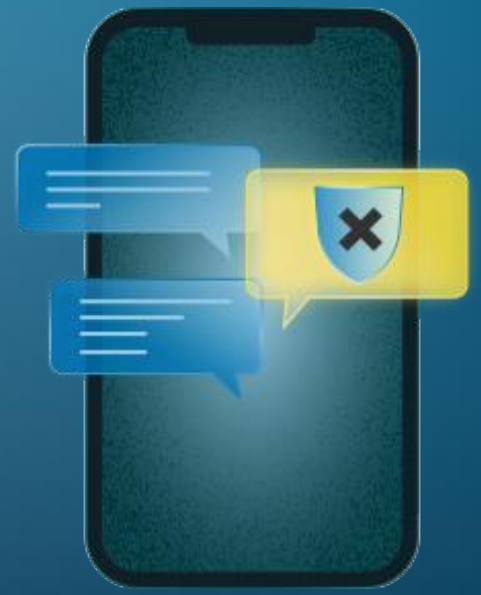
IT-Sicherheitslage in Deutschland - Gesamtbewertung

- **Schadwirkungen**

  - mehr Daten-Leaks, weniger Lösegelder
  - Die größten Schadwirkungen erzielten Angreifer weiterhin mit Ransomware in Verbindung mit Daten-Leaks
  - Bedeutsamer wurden aber auch reine Daten-Leaks.

- **Resilienz**

  - Digitale Sorglosigkeit verbreitet sich bei Verbraucherinnen und Verbraucher.
  - Kleine und mittlere Unternehmen: Alle sind gefährdet – viele, ohne es zu wissen.
  - Die Resilienz der Kritischen Infrastrukturen wächst langsam, aber stetig



Neue Technologien – neue Unsicherheiten

Einfluss von KI auf die Cyberbedrohungslage: Chancen für Angreifer und Verteidiger

KI-assistierte Ransomware-Angriffe

- KI-Programmierassistenten
  - **beschleunigen** Erstellung von Schadcode
  - verringern benötigtes Vorwissen
- KI **beschleunigt** die Analyse und Ausnutzung von Schwachstellen
- KI ermöglicht **skalierbare** Verteilung von Schadsoftware durch hochwertiges & individualisiertes Social Engineering
- KI **beschleunigt** Auswertung exfiltrierter Daten
- KI „unterstützt“ Betroffene bei Bezahlung des Lösegelds in Kryptowährung

Kein Zukunftsthema: Angreifer nutzen KI bereits heute
-> KI ermöglicht **höhere Produktivität** (Geschwindigkeit von Angreifern)
-> KI ermöglicht **skalierbare Angriffe** (über Sprachbarrieren hinweg)

Cybersicherheit muss Top-Priorität sein
KI-Produktivitätsgewinn auch für Verteidigung nutzen

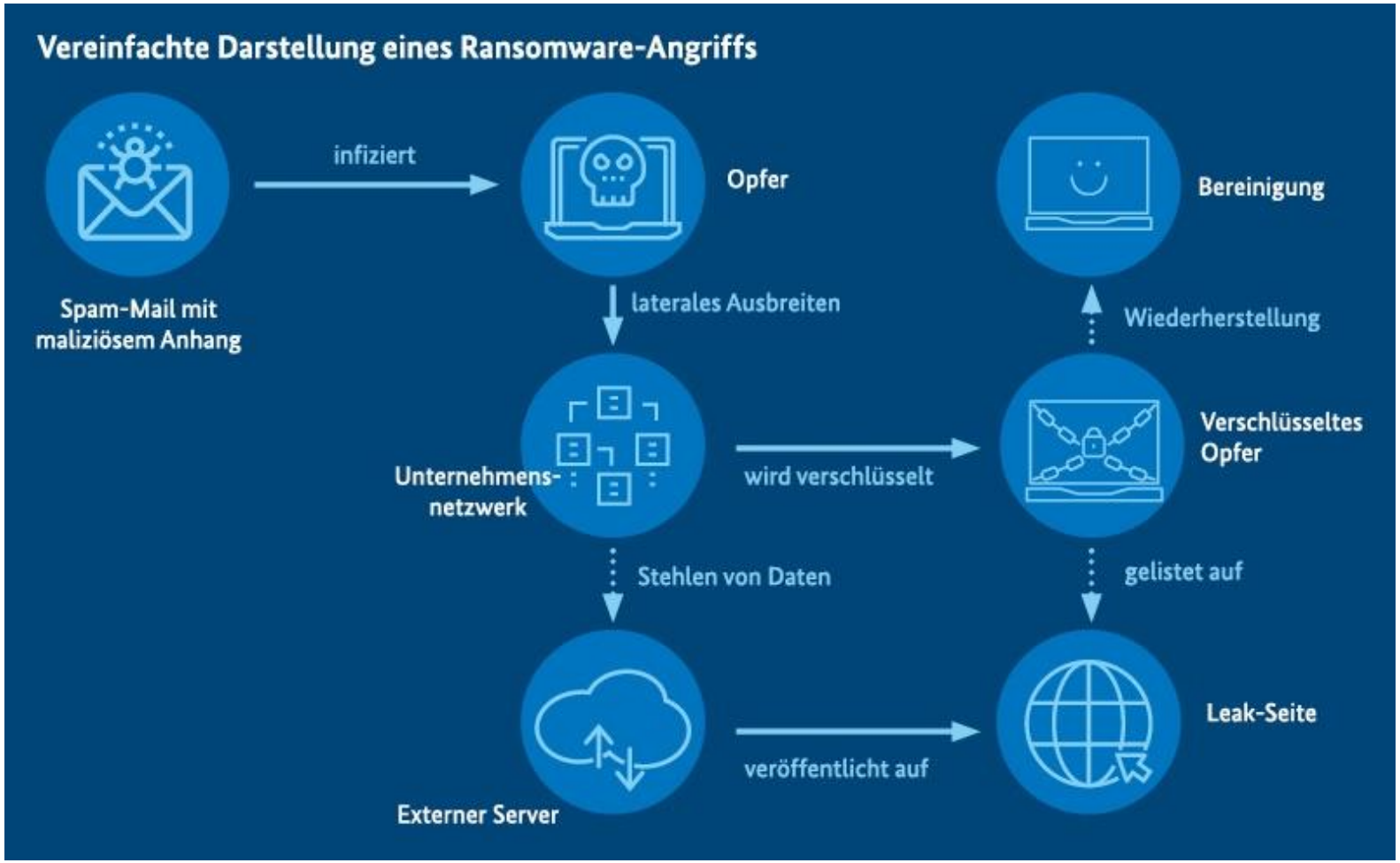
Geschwindigkeit

Skalierung

Lageinformation – Was wir sehen

Ransomware

- **Ransomware-Angriffe → Massengeschäft**
- **Ransomware als Dienstleistung** (RaaS)
- Cyberkriminelle **Schattenwirtschaft**
- Angriffe mit hoher Agilität
- **BSI rät von Zahlungen ab!**
  → Wiederherstellungskosten können sich verdoppeln



BSI-Magazin 2022/02: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2022_02.html

Lageinformation – Was wir sehen

Cloud-Sicherheit: Angriffe nehmen zu

- Ziel ist in der Regel, **Zugriff auf sensible Daten** zu erlangen
- Grundsätzlich können alle Anbieter von Cloud-Diensten von Angriffen betroffen sein – egal ob groß oder klein
- **Mehrere erfolgreiche Ransomware-Angriffe** auf Public-Cloud-Dienste
- **Eingeschränkte Verfügbarkeit** oder verschlüsselt Daten durch Schadsoftware
- **Angriffsvektor oft nicht Cloud-spezifisch**

Lageinformation – Was wir sehen

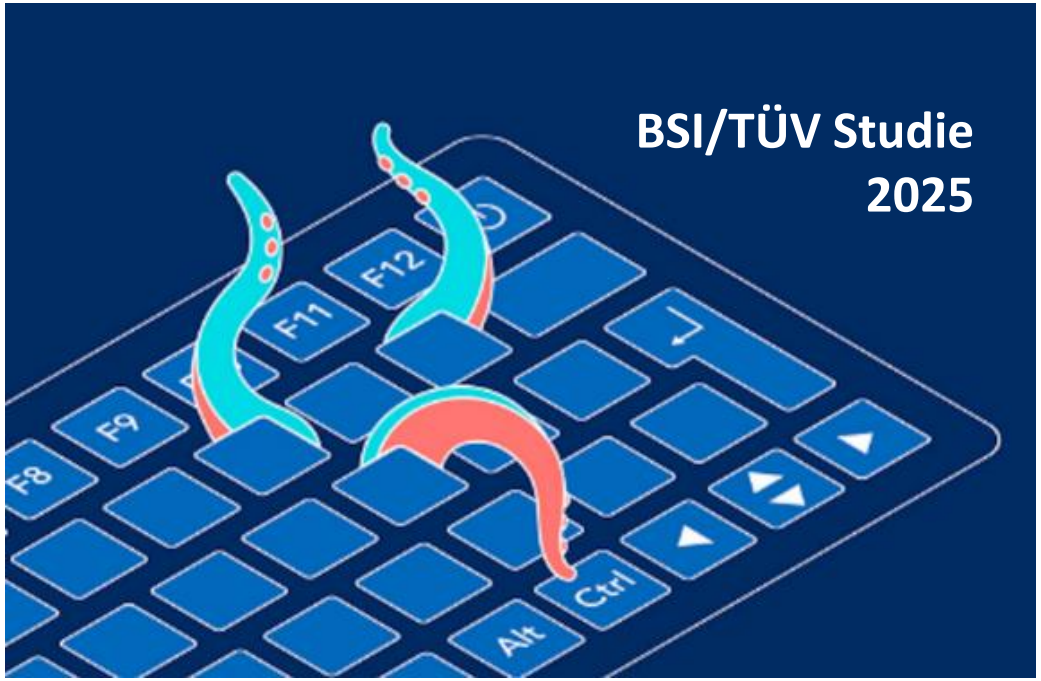
Sicherheit von Dienstleistern/Supply Chain

- **Steigende Abhängigkeit und Vernetzung** der IT-Infrastrukturen
- **Opfer überwiegend KMUs, insbesondere IT-Dienstleister** und Kommunen
- **Zero-Day-Schwachstellen** als neue, alternative Angriffsfläche
- **Erhebliche Schadwirkung** durch breite Wirkung auf Kunden

Cybersicherheit der deutschen Wirtschaft

Unternehmen wiegen sich in trügerischer Sicherheit

- (Hybride) Bedrohungslage steigt
- **KI-gestützte Angriffe** nehmen zu
- Einfallstor IT-Sicherheitsvorfälle - Phishing 84%
- **Aber…**
  - Viele Firmen unterschätzen die Lage
  - Überbewerten die eigene Resilienz
  - **Nur 10% nutzen selbst KI** zur Abwehr
- Zügige Umsetzung **NIS-2-Richtlinie** gefordert



Was können wir tun?
Kooperation
und Gesamtverteidigung

Das BSI als Partner und Taktgeber

Operatives nationales Verbindungswesen

- **Fachliche Vernetzung**
  CERTs, IT-Si Teams, IT-Si Experten
- **BSI Tool Unterstützung**
  Chat, Wiki, MISP, …
- Arbeitstreffen, Fachtreffen, Netzwerktreffen
- **Das BSI (versteht sich) als Partner und Helfer**
- **BSI-Lagezentrum ausgebaut und modernisiert**
- **Behörden im Digital Cluster Bonn**
- **+ Kooperationsvereinbarungen**

VCV VerwaltungsCERT-Verbund	NATIONALES CYBER-ABWEHRZENTRUM	CERT VERBUND	G7
UEFA EURO2024 GERMANY	Nationales Verbindungswesen	DCSO ENGINEERING SECURITY	CSSA Cyber Security Sharing & Analytics
UP KRITIS	Cyber-Sicherheitsnetzwerk	Allianz für Cyber-Sicherheit	**Automotive**
Provider	**Dax40**	**Wahlen**	**BundesCERTs**

Ausblick

Bild: © AdobeStock/Azazul

Ausblick

Bedrohungsszenarien im Cyberraum

- KI-generierte Desinformation und Deepfakes
- Angriffe auf Cloud-Infrastrukturen
- Angriffe auf autonome Systeme
- Angriffe auf KI-Systeme
- Angriffe mit Hilfe von KI
- Angriffe auf Kryptografie mit Quantencomputern

Bild: © AdobeStock/Maryna

Fazit

Schutz der Angriffsflächen ist 2026 der entscheidende Hebel

- Bedrohungslage bleibt angespannt, Dynamik durch KI steigt.
- Resilienz ist möglich: Wir sind der Lage nicht schutzlos ausgeliefert.
- Gemeinsam gestalten wir die **Cybernation Deutschland**: resilient, souverän, handlungsfähig.

Das BSI: Ihr Partner für Cybersicherheit und Krisenresilienz.

- Schnelle Umsetzung der NIS2-Richtlinie ins nationale Recht
- Aufbau einer effektiven Marktaufsicht für den Cyber Resilience Act

Kooperation gewinnt. Gemeinsam sichern wir Deutschlands digitale Zukunft.

Martin Pasbrig

Bundesamt für Sicherheit in der Informationstechnik

Abteilung C "Operative Cybersicherheit – Lage und CERT"

Referat C13 "Statistik und Lagebilder"

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us: