Die aktuelle Lage der Cybersicherheit - Zeitenwende im digitalen Raum –

DuD 2025

Isabel Münch, Fachbereichsleiterin IT-Sicherheitslage, 2. Juni 2025

Bundesamt
für Sicherheit in der
Informationstechnik

Aktuelle Situation – gefühlte Lage in Deutschland

BADBOX WÄCHST, 190.000 ANDROID-GERÄTE INFIZIERT

Pierluigi Paganini 21. Dezember 2024

Sanktionen angekündigt

USA werfen Russland Einmischung in Präsidentenwahl vor

Stand: 04.09.2024 20:41 Uhr

Cyberkriminalität

Immer mehr Lösegeldattacken

Vor allem Mittelständler sind häufig unzureichend gegen Angriffe mit Erpressungssoftware geschützt. Cyberversicherungen werden teuer.

Susanne Schier Frankfurt, Baden-Baden

Der Markt für US-Staatsanleihen ist der größte und wichtigste der Welt. Und doch gelang es Hackern am vergangenen Donnerstag, dieses riesige Geschäft durcheinanderzubringen. Der US-Ableger der chinesischen Großbank ICBC meldete eine sogenannte Ransomware-Attacke: werden die Preise tendenziell weiter steigen, da auch die Schäden aktuell wieder zunehmen", prognostizierte Hasse.

Die Juristin ist bereits seit mehr als 20 Jahren bei Munich Re tätig und seit 2019 unter anderem für das Cybergeschäft in Europa und Lateinamerika verantwortlich. Im deutschen Markt ist ein gutes Dutzend größerer Erstversicherer im Cy-

Verfassungsschutz eingeschaltet

Schwerer Cyberangriff auf die CDU

Stand: 01.06.2024 18:00 Uhr

Eine Woche vor der Europawahl ist die CDU Opfer einer Cyberattacke

MALWARE & DROHUNGEN

Ivanti warnt vor neuen Zero-Day-Angriffen

Ivanti schließt kritische Sicherheitslücken in Connect Secure und Policy Secure

Londoner Kliniken: Cyberkriminelle veröffentlichen Daten

Infolge eines Cyberangriff auf einen Pathologiedienstleister sind Londoner Kliniken im Notbetrieb. Jetzt haben die Cyberkriminellen Daten veröffentlicht.

Updates unmöglich: Niederlande müssen Ampeln wegen Sicherheitslücke austauschen

Per Funk können Angreifer die Ampeln aus der Ferne umschalten und somit den Straßenverkehr stören. Der Austausch wird Jahre in Anspruch nehmen.

Weltweiter IT-Ausfall: Betrieb wird wieder aufgenommen

Das Update eines Programms hat weltweit Windows-Computer zum Absturz gebracht. Crowdstrike hat den Fehler mittlerweie gefunden und behoben.

Cybercrime: KI-generierte Malware in freier Wildbahn gesichtet

Sicherheitsexperten von HP weisen auf einen beunruhigenden Trend hin: Kriminelle nutzen verstärkt generative KI zur Entwicklung von Malware.

Kritische Infrastruktur

Mehr Cyberangriffe auf deutsche Seehäfen

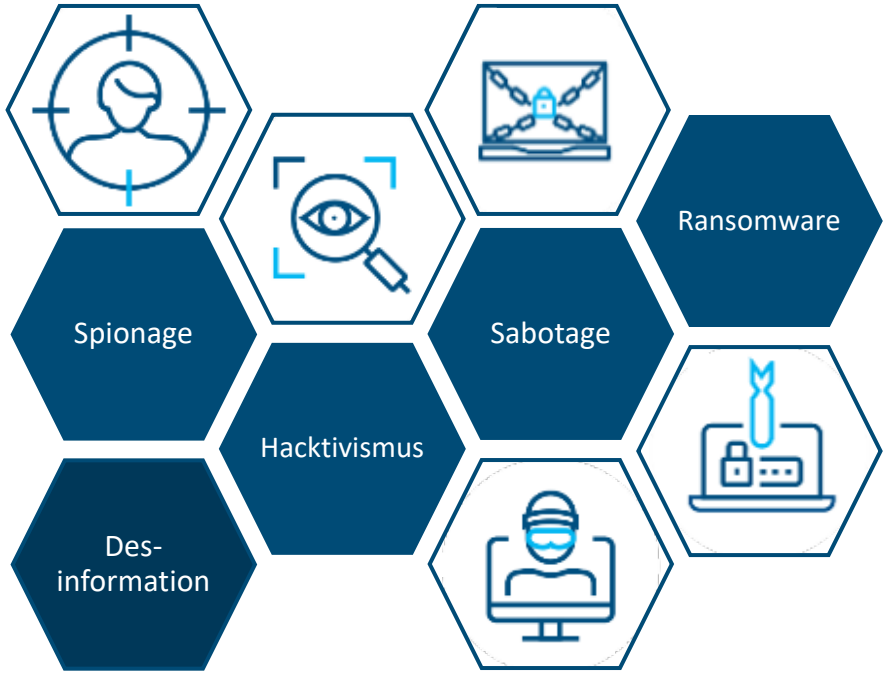
Stand: 05.09.2024 08:56 Uhr

Deutsche Seehäfen waren zuletzt immer häufiger von Cyberangriffen betroffen. Besonders seit Beginn des russischen Angriffskrieges hat die Zahl der Cyberattacken zugenommen.

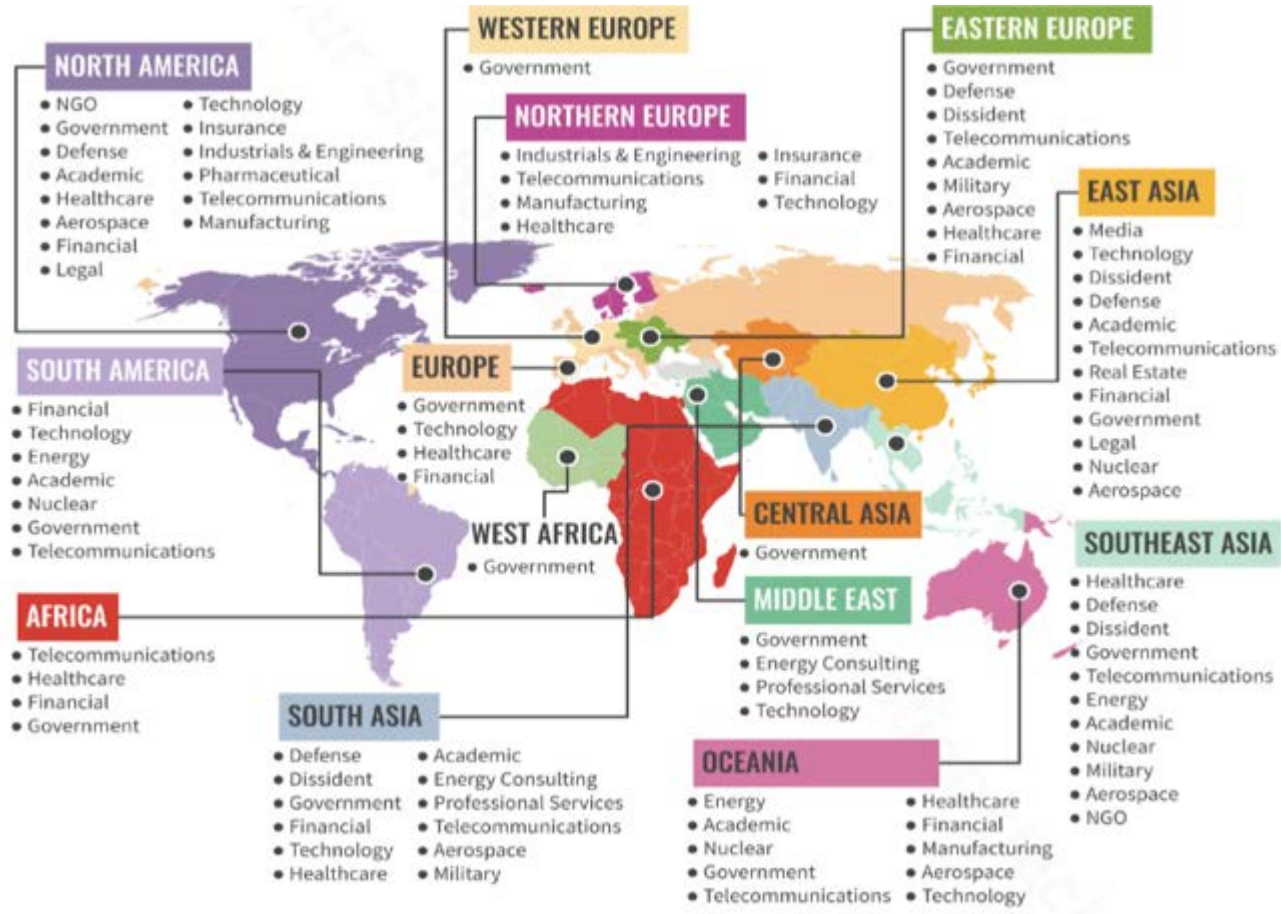
Black Hat 2024 – 15 Ways to Break Your Copilot

Sicherheitsforscher zeigt wie man Copilot missbrauchen kann

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

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

Neue Technologien – neue Unsicherheiten

Post-Quanten-Kryptografie: harvest now, decrypt later

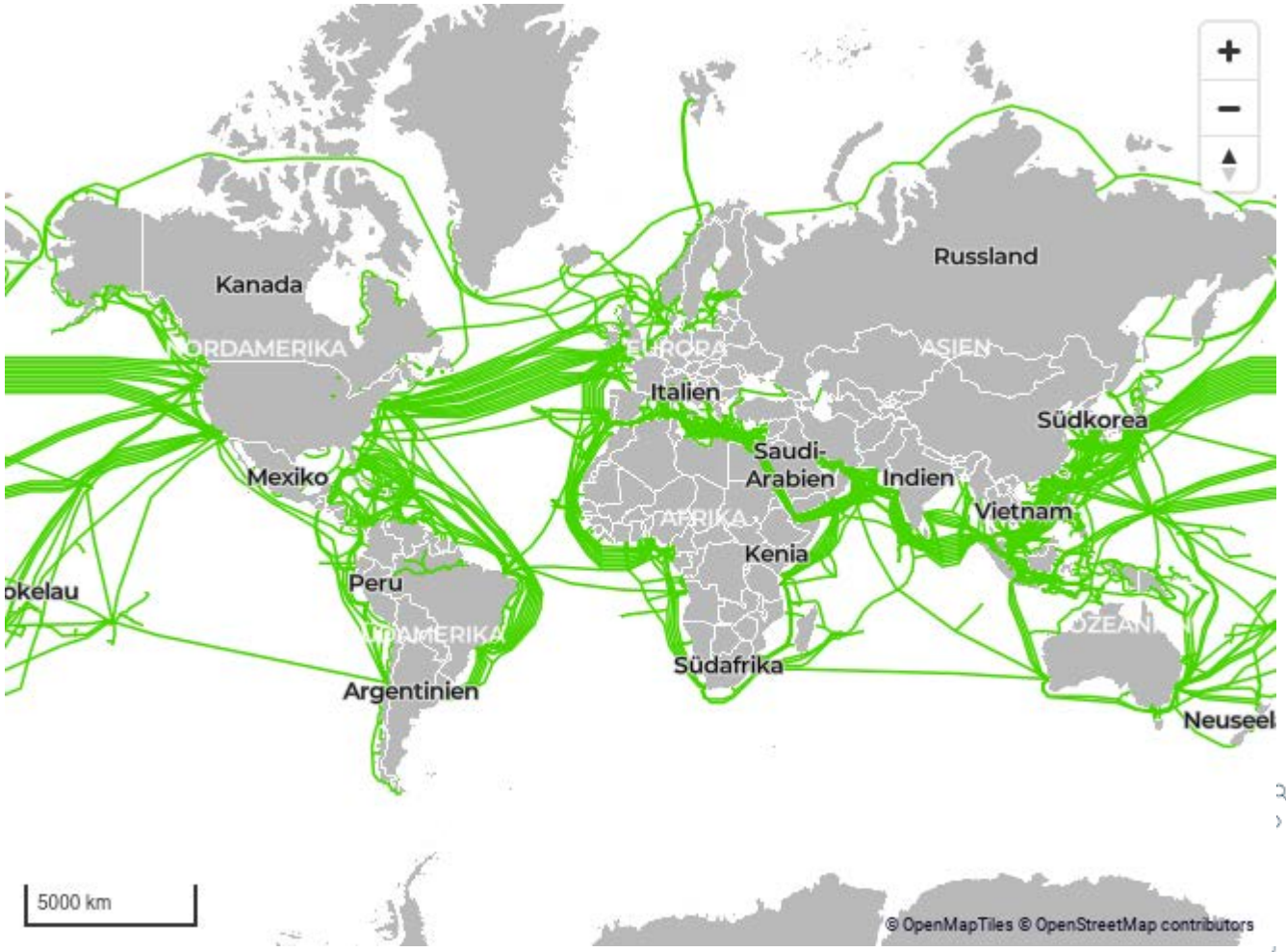
- Heutige asymmetrische Kryptografie (RSA, ECC) kann mit (kryptografisch relevanten) Quantencomputern gebrochen werden (Arbeitshypothese des BSI: Anfang 2030er Jahre).
- Besonders kritische Bedrohungsszenarien:
  - **Store now, decrypt later**: Jetzt verschlüsselte Daten mitschneiden, um sie später zu entschlüsseln.
  - **Lange Migrationszeiten** (z. B. PKI), lange Signaturgültigkeit (z. B. Verträge)
- Die Sicherheit symmetrischer Kryptografie wird „halbiert“.
- Lösungsansätze:
  1. **Quantensichere kryptografische Verfahren**
     - Post-Quanten-Standardisierung: NIST und ISO
     - Anpassung von BSI-Empfehlungen (TR, Leitfäden etc.)
  2. **Sensibilisierung**

Quantencomputer-Studie

Leitfaden PQ-Kryptografie

Unterseekabel und internationale Infrastruktur

- **Mehr als 99 %** des interkontinentalen Datenverkehrs werden über Seekabel abgewickelt
- Mehr als 60 % des internationalen Kommunikationsverkehrs läuft über Seekabel, die nicht den „Betreibern öffentlicher elektronischer Kommunikationsnetze“ gehören
- Große Cloud-Anbieter betreiben ihre eigenen Backbone-Netze und Rechenzentren
- Transitverkehr hauptsächlich über private Netze; weitgehend unreguliert
- **Sabotagevorfälle in Ostsee & Atlantik**



Quelle: TeleGeography, Stand: 5.12.2024 | Grafik: stern/rös

Sabotagevorfälle in Ostsee & Atlantik

- **Durch die deutsche Ausschließliche Wirtschaftszone in der Ostsee verlaufen insgesamt 16 Unterwasserkabel**, davon 9 Hochspannungskabel, 6 dienten der Daten-übertragung; **C-Lion1**: einzige Untersee-Datenkabel, das direkt von Finnland nach Mitteleuropa führt
- **Vorfälle wie die in der Ostsee**, in deren Folge Finnland den Mechanismus des EU-Instrumentariums zur Abwehr **hybrider Bedrohungen** aktivierte, haben jedoch gezeigt, dass Bestandteile der Seekabelinfrastrukturen nach wie vor anfällig sind
- **Reparatur** eines Unterseekabels dauert **üblicherweise zwischen 5 und 15 Tagen**

Schäden an Ostsee-Datenkabeln

Schweden leitet Sabotage-Ermittlungen ein

Stand: 19.11.2024 17:24 Uhr

Ein Unfall oder ein Angriff? Die schwedischen Behörden ermitteln wegen der Beschädigung von Datenkabeln bereits wegen Sabotage. Auch Pistorius und Baerbock vermuten Vorsatz - und schauen in Richtung Russland.

NORDSTREAM UND CO.

Eine Chronik verdächtiger Sabotagefälle in der Ostsee

von **Thomas Krause** 05. Dezember 2024 • 14:58 Uhr • 4 Min

EXKLUSIV Zerstörte Ostsee-Kabel

Chinesisches Schiff unter Verdacht

Stand: 20.11.2024 14:29 Uhr

Ein chinesisches Frachtschiff hat seine Passage durch die Ostsee unterbrochen. Europäische Behörden bringen die "Yi Peng 3" mit der Zerstörung von zwei Unterseekabeln in der Ostsee in Verbindung.

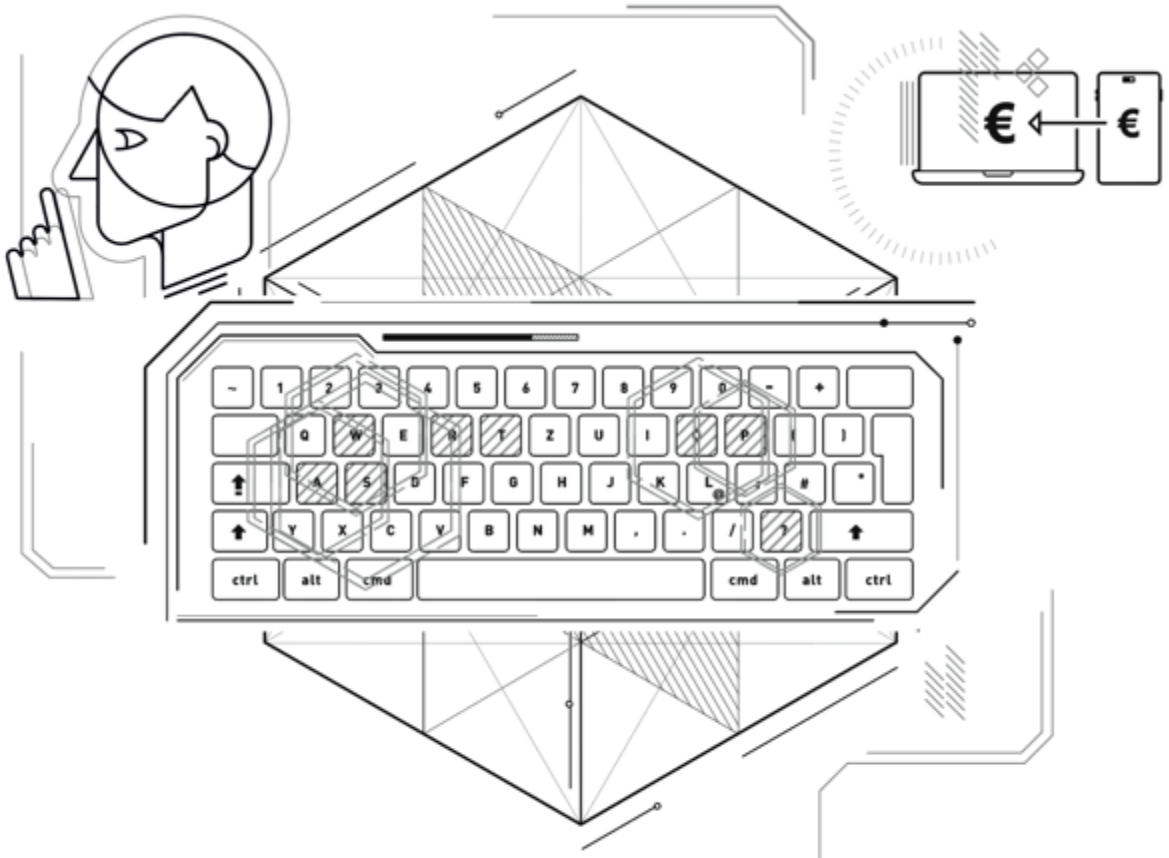
Reparatur kann bis zu zwei Wochen dauern

Die Dimensionen der IT-Sicherheit in Deutschland

Die Lage der IT-Sicherheit in Deutschland 2024

Wie bedroht ist Deutschlands Cyberraum? - Bedrohungen

- Die Lage der IT-Sicherheit in Deutschland **war und ist besorgniserregend.**
- Weiterhin professioneller werdende **arbeitsteilige cyberkriminelle Schattenwirtschaft**
- **APT-Gruppen in Deutschland – darunter die gefährlichsten – bleiben weiterhin aktiv.**
- **Bei Malware gewinnt Android als Zielsystem an Bedeutung**.



Die Lage der IT-Sicherheit in Deutschland 2024

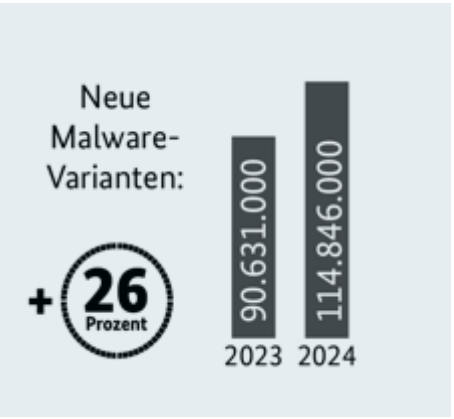
Bedrohungen – Malware & Botnetze

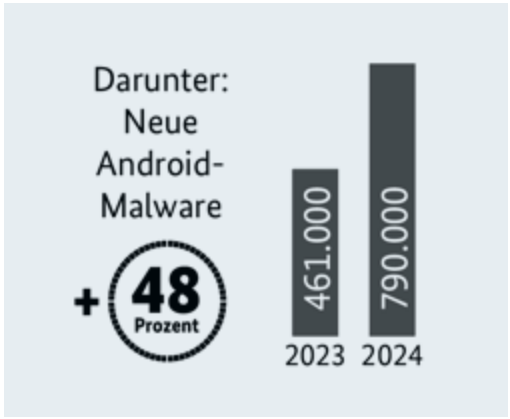
Malware

- Phishing: Einfallstor für Malware
- Weltweit bekannt gewordene Phishing-URLs und -IPs weltweit: ca. 1.000/Tag
- Lebensdauer einer Seite: wenige Tage
- Bei Malware gewinnt Android als Zielsystem an Bedeutung

Botnetze

- In Deutschland regelmäßig aktive Botnetze > 200



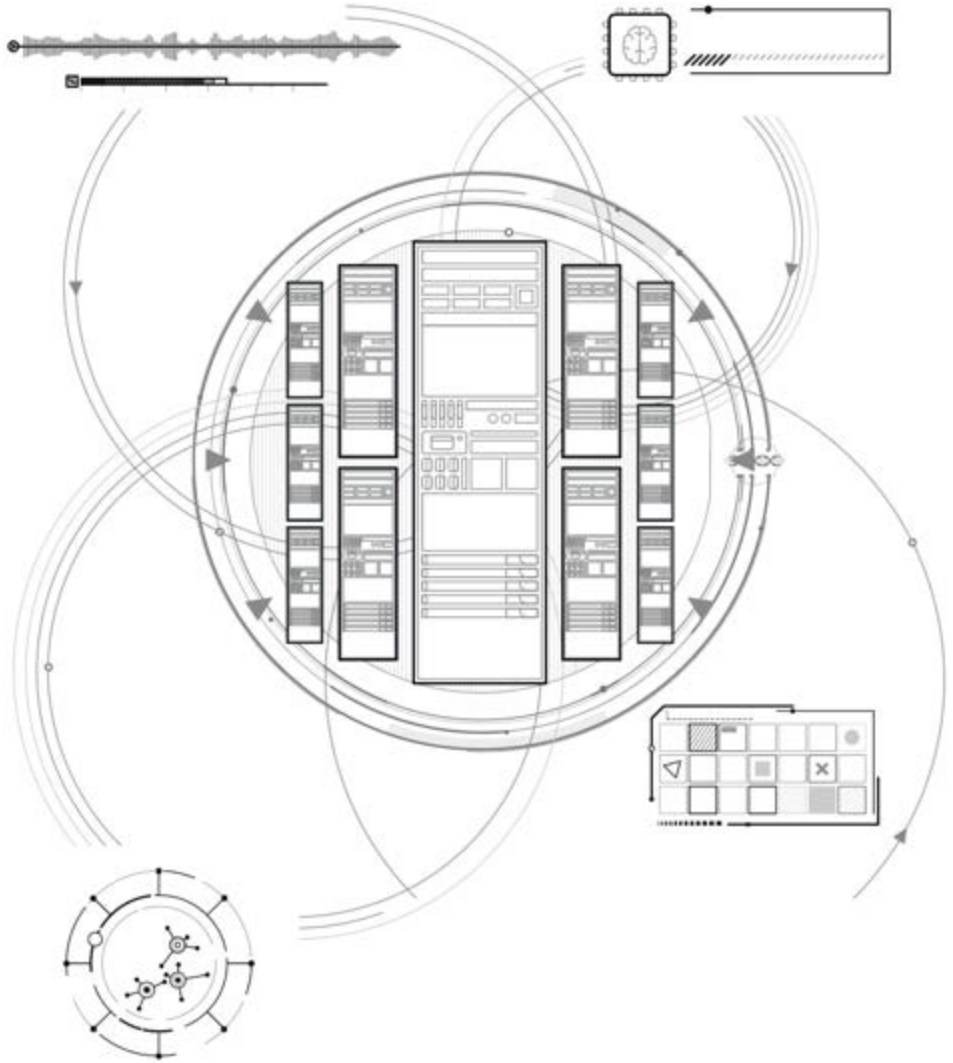


Die Dimensionen der IT-Sicherheit in Deutschland

Die Lage der IT-Sicherheit in Deutschland 2024

Wie bedroht ist Deutschlands Cyberraum? - Angriffsfläche

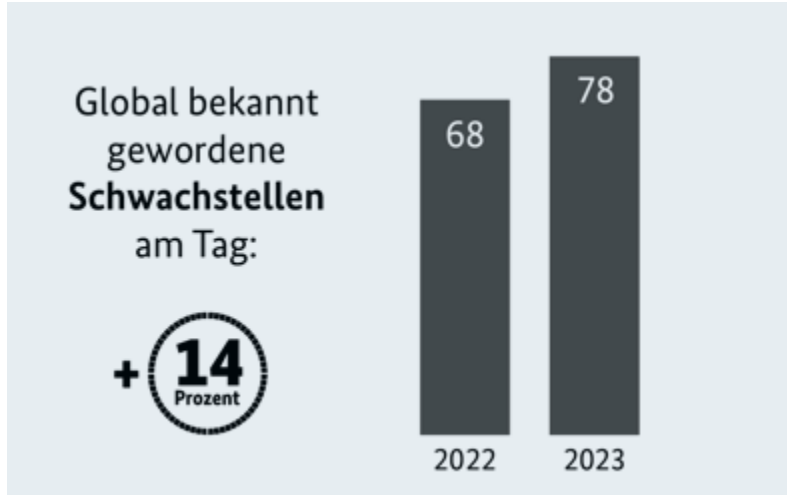
- Pro Tag wurden 78 **neue Schwachstellen in Softwareprodukten** bekannt
- mind. 37 % der 45.000 **Exchange-Server in Deutschland** verwundbar
- 25 % der **Android-Geräte** in Deutschland erhalten **keine Sicherheits-Updates** mehr.
- **Schwachstellen nehmen seit Jahren kontinuierlich zu.**
- **Vielfältige Angriffstechniken treffen auf einen digitalisierten Alltag – alle können angegriffen werden.**



Die Lage der IT-Sicherheit in Deutschland 2024

Angriffsfläche - Schwachstellen in Softwareprodukten

- Oftmals **erstes Einfallstor**
- **78 neue pro Tag** (**+14%** zu 2022)
- Beispiele: Ein System, viele Betroffene: mind. 37 % der 45.000 **Exchange-Server** in Deutschland verwundbar; **Zero-Day** Schwachstellen bei verschiedenen Ivanti-Produkten
- **25% der Android-Geräte** in Deutschland **verwundbar**
- **Angriffsfläche der Bundesverwaltung**:
  - Aus dem Internet erreichbare IP-Adressen: 4.500
  - Aktive E-Mail-Adressen: 639.000

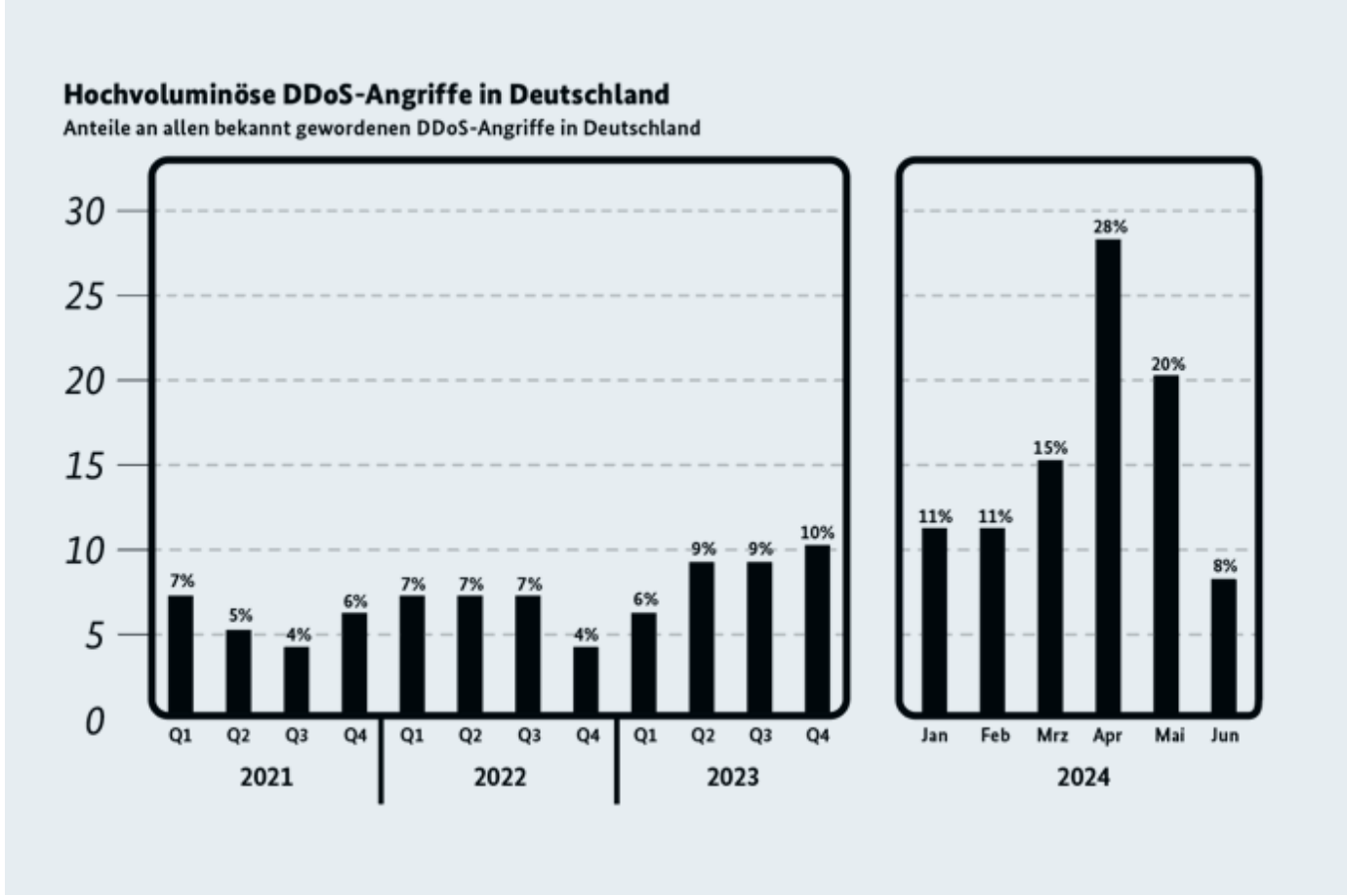


Die Dimensionen der IT-Sicherheit in Deutschland

Die Lage der IT-Sicherheit in Deutschland 2024

Gefährdungen – DDoS Angriffe

- **Anteil bandbreitenstarker DDoS-Angriffe** hat sich gegenüber dem langjährigen Durchschnitt **verdoppelt**

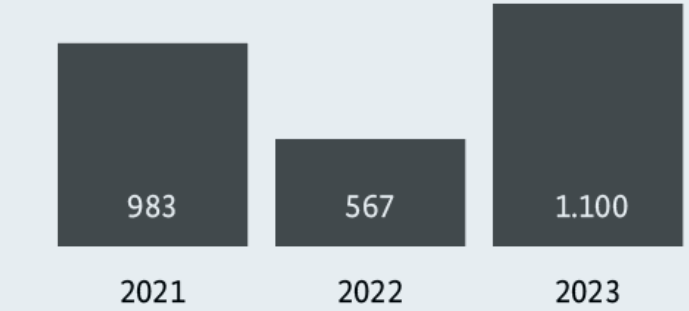


Die Dimensionen der IT-Sicherheit in Deutschland

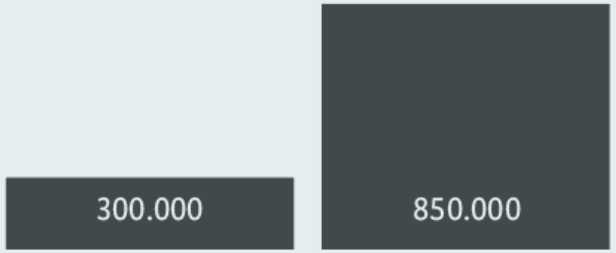
Die Lage der IT-Sicherheit in Deutschland 2024

Schadwirkung

- **Schäden im Milliardenbereich**, unvorhergesehene Ereignisse, menschliches Versagen
- **Ransomware-Angriff auf kommunalen IT-Dienstleister** Oktober 2023, davon betroffen: 72 Kommunen, 20.000 Arbeitsplätze, rund 1,7 Mio. Einwohnerinnen/ Einwohner
- **Geschätzter Schaden durch Systemausfälle** eines fehlerhaften Updates in der Software **Crowdstrike** Falcon: > 8,5 Mio. Geräte > 5 Milliarden Dollar
- **Störungen bei KRITIS-Betreibern: 490**



Von Ransomware-Gruppen erbeutete Lösegelder weltweit (in US-Dollar, Mio.):



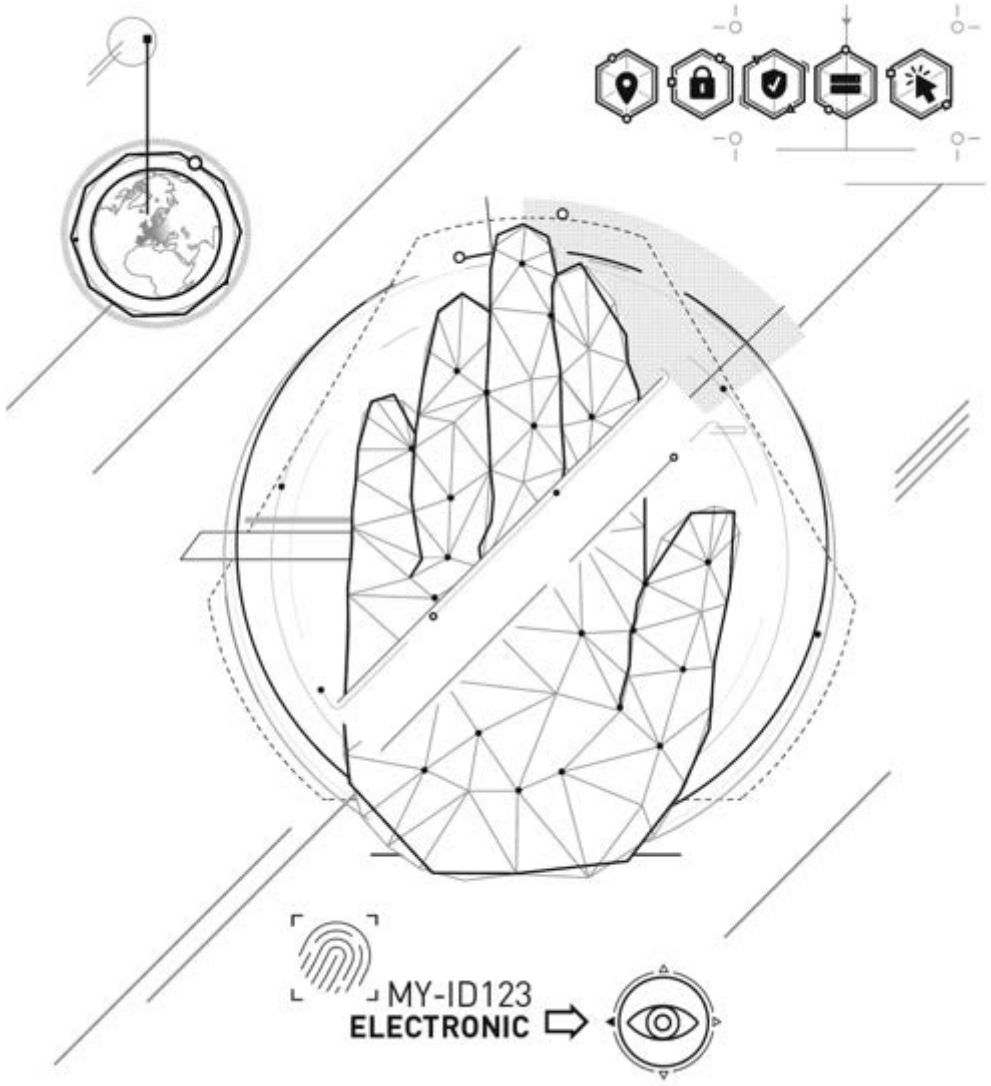
Lösegeld pro Fall (in US-Dollar, ca. Durchschnitt):

Die Dimensionen der IT-Sicherheit in Deutschland

Die Lage der IT-Sicherheit in Deutschland 2024

Wie bedroht ist Deutschlands Cyberraum? – Resilienz

- Deutschland ist den Bedrohungen **nicht schutzlos ausgeliefert**.
- **Warnsysteme des BSI:** von technischen Warnungen über herausgehobene Einzelfälle bis hin zu ernstzunehmenden Gefährdungen
- **Alle Beteiligten** müssen ihren Beitrag zur **Cyberresillienz Deutschlands** leisten.
- **Kooperation gewinnt**.



Die Dimensionen der IT-Sicherheit in Deutschland

Die Lage der IT-Sicherheit in Deutschland 2024

Resilienz – Verteidigung

- **BSI-Schwachstellen-Warnungen** an Betroffene: **Ø 15 pro Tag**
- Nach BSI-Warnung **geschlossene Schwachstellen**: **>500**
- Neue **Sperrungen maliziöser Webseiten**: **Ø 368 pro Tag**
- **Spam-Mails: Ø rund 405.000 pro Tag**

Warnung — Schließung, Sperrungen

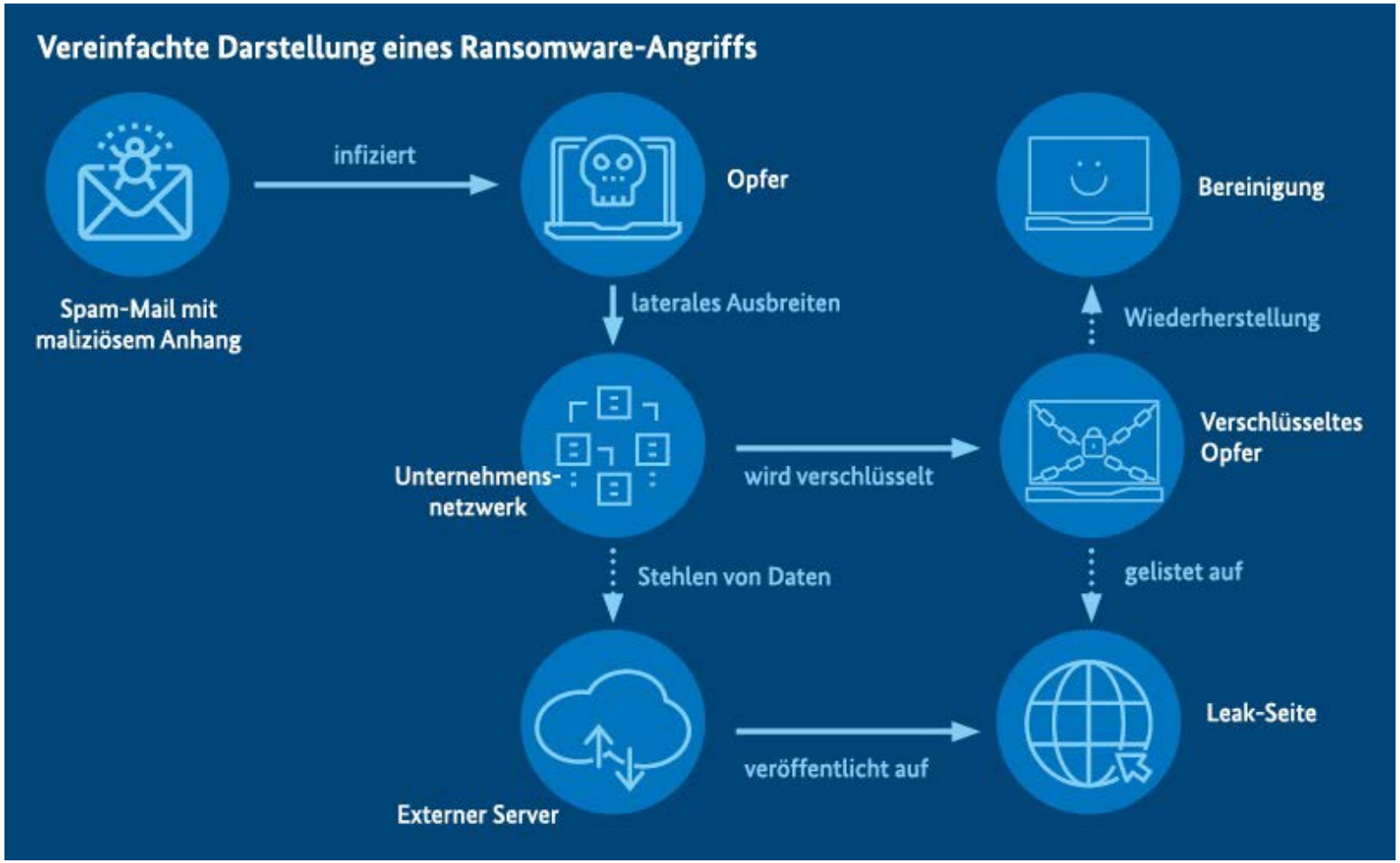
BSI-Schwachstellen-Warnungen an betroffene Behörden	Ø 15 pro Tag
Nach BSI-Warnung geschlossene Schwachstellen im Berichtszeitraum	>500
Neue Sperrungen maliziöser Webseiten	Ø 368 pro Tag
Blockierte Zugriffsversuche auf maliziöse Webseiten	Ø 9212 pro Tag
Geprüfte E-Mails insgesamt Davon: Spam-Mails Spam-Quote Davon: Malware-Mails Malware-Mail-Anteil	Ø rund 753.000 pro Tag Ø rund 405.000 pro Tag Ø 53 % Ø 772 pro Tag 0,1 %

Die Dimensionen der IT-Sicherheit in Deutschland

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 **und** Nutzer 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 und IT-Dienstleister,** beispielsweise Kommunen
- **Erhebliche Schadwirkung** durch breite Wirkung auf Kunden
- **Office-IT-Netze** und **Fernzugriffe** als Einfallstor (Dienstleister, Home Office)
- Auch **Software-Lieferketten** betroffen (vgl. XZ-Utils, Log4j, Kaseya, NotPetya)
- **Zero-Day-Schwachstellen** als Angriffsfläche

Besondere Ereignisse 2025

Bedrohungslage Wahlen

- Bundestagswahl am 23. Februar 2025 in Deutschland und weitere Wahlen 2025
- Grundsätzliches Interesse für Akteure zur möglichen illegitimen Beeinflussung von Wahlen
- Zwei Arten der illegitimen Einflussnahme: direkt auf den Wahlprozess und indirekt auf die Öffentliche Wahrnehmung und damit auf die freie Meinungs- und Willensbildung
- Desinformationskampagnen, Gefahr durch Hack-und-Leak-Operationen
- DDoS-Angriffe sind beliebt bei politisch motivierten Einflussakteuren
- **Das BSI geht davon aus, dass sowohl während der Vorbereitung als auch während der Durchführung die Sicherheit, Integrität oder Verfügbarkeit der Bundestagswahl stets sichergestellt war.**

Bild: © AdobeStock/tinyakov

Besondere Ereignisse 2025

Zero-Day-Schwachstelle in Ivanti Software-Produkten

- **Erneut kritische Schwachstellen in Ivanti Software-Produkten: Endpoint Manager**
- Ivanti warnte am 8. Januar 2025 bereits vor **Schwachstellen in Ivanti Connect Secure, Policy Secure und ZTA Gateway**
- Kritische Zero-Day-Schwachstelle in Ivanti Connect Secure **aktiv ausgenutzt**
- Entsprechende BSI-**Cybersicherheitswarnung** am 9. Januar 2025 versandt
- Es wird dringend empfohlen, alle Ivanti Software-Produkte auf den neuesten Stand zu bringen
- 2023 und 2024 veröffentlichte das BSI bereits fünf Warnungen zu Ivanti-Produkten

Besondere Ereignisse 2025

APT-Gruppe Lazarus wohl für Angriff auf Krypto-Börse Bybit verantwortlich 03/2025

- **Bisher größter Krypto-Währungsdiebstahl** im Zusammenhang mit Sicherheitsvorfall bei der Krypto-Börse-Bybit
- Ethereum im Wert von rund **1,5 Milliarden US-Dollar** gestohlen.
- Komplexe, mehrstufige Kompromittierung der Sicherheitssysteme von Bybit.
- **APT-Gruppe Lazarus** als Angreifer identifiziert.
- FBI nennt Demokratische Volksrepublik Korea (Nordkorea) als Verantwortlichen.

Besondere Ereignisse 2025

Russische Propaganda-Webseiten zielen auf LLMs führender KI-Chatbots 03/2025

- Mehrere Quellen veröffentlichten Berichte über **LLM-Grooming** durch Russland (LLM-Grooming = Manipulation von LLMs, um diese mit erhöhter Wahrscheinlichkeit ein bestimmtes Narrativ oder Weltbild wiedergeben zu lassen)
- **Automatisiert erstellte Desinformation** soll russische Narrative gezielt für LLMs verbreiten
- Durch Millionen manipulierter Berichte können KI-Trainingsdaten beeinflusst werden
- **KI-Chatbots verteilen Desinformation** aufgrund manipulierter Datenbasis
- Phänomen "LLM-Grooming" ist in die Kategorie der "Poisoning-Angriffe" einzuordnen
- **Hersteller der KI-Modelle in der Pflicht**, ihre Lieferketten und die Trainingsdaten genau zu prüfen

Besondere Ereignisse 2025

DDoSia Relevanz in Deutschland 01/2025

- Pro-russische Hacktivisten-Gruppe NoName57(16) führt **weltweit DDoS-Angriffe** durch
- Die Gruppe möchte vor allem Aufmerksamkeit generieren, die **Ziele wechseln** daher
- **DDoS-Angriffe** durch Hacktivisten sind zur Routine geworden, **kosten die Betroffenen jedoch Personal, Zeit und Geld**
- Es existieren **wirksame Mitigationsmaßnahmen** gegen die Angriffe

Ausblick

Bedrohungsszenarien im Cyberraum in den nächsten fünf Jahren?

- 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

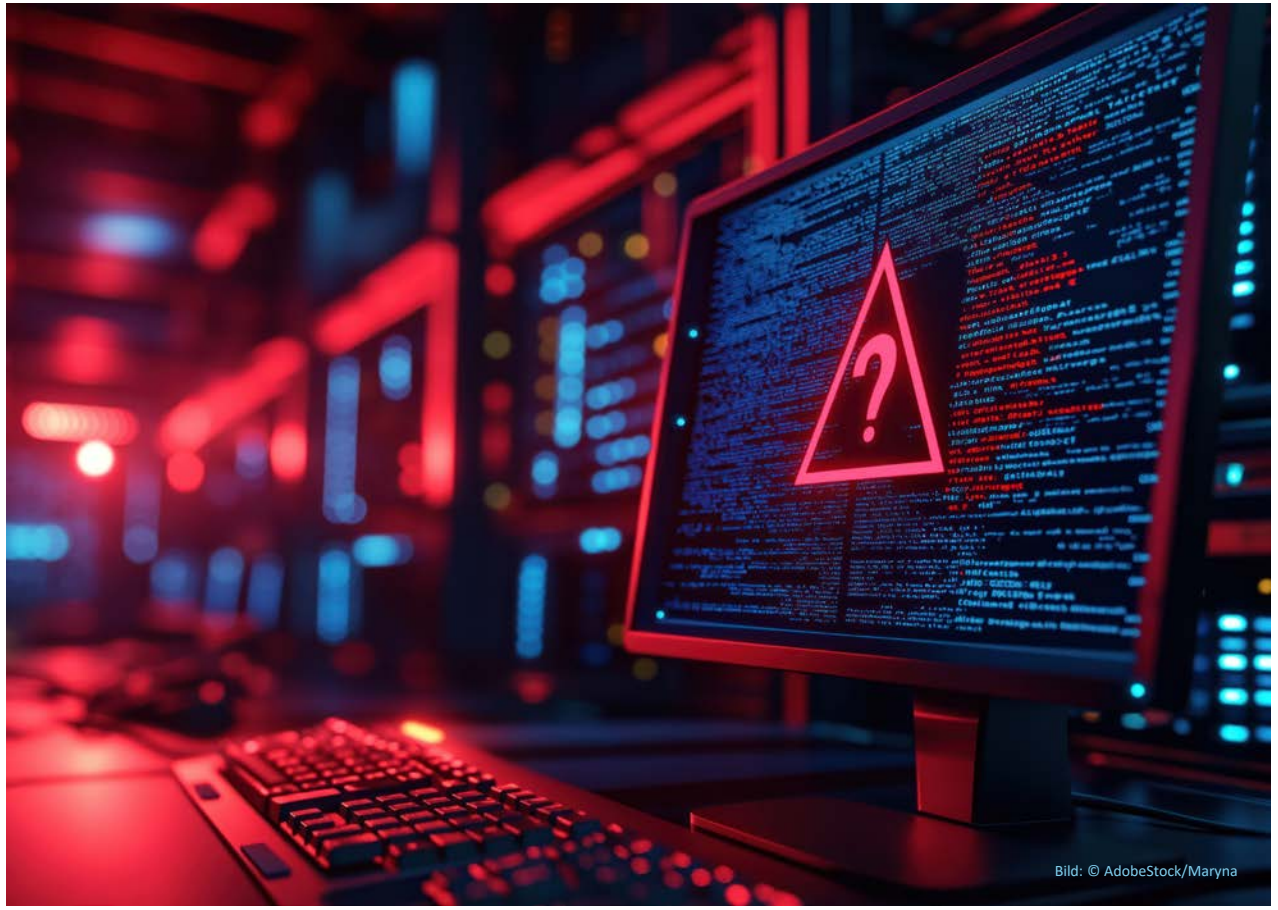


Bild: © AdobeStock/Maryna

Cyber-Sicherheitslage angespannt

Was können Sie tun?

- **Cyber-Sicherheit muss Chefinnen- und Chefsache sein!**
  - Zum Teil des Risiko-Managements machen
  - SBOM bei Zulieferern einfordern
  - Budget für IT-Sicherheit erhöhen
- **Umsetzung IT-Grundschutz**
- **IT-Sicherheitsvorfälle melden!**
- **Werden Sie Teilnehmer der Allianz für Cyber-Sicherheit!**

Onepager: „Management von Cyber-Risiken“

https://www.allianz-fuer-cybersicherheit.de/dok/cyberriskmanagement

Lageinformation – Was wir sehen

Cyber-Sicherheit rechnet sich!

- **Hohe Kosten nach IT-Sicherheitsvorfällen** durch Strafen oder Klagen
- Bußgelder **häufig aufgrund von Verstößen gegen Datenschutzregularien** verhängt, **seltener im direkten Zusammenhang mit Angriffen**
- Strafzahlungen werden **nicht öffentlich bekannt**, oder aufgrund juristischer Verfahren erst mit Zeitverzug
- **Prävention führt zu „Return on Investment“** (ROI)
- Wer Lösegeld zahlt, verdoppelt **Wiederherstellungskosten**!

(siehe https://news.sophos.com/de-de/2023/05/10/state-of-ransomware-2023-ein-ende-der-datenverschluesselung-ist-nicht-in-sicht/)

Vorfälle der letzten Jahre

2021: US T-Mobile – $ 500.000.000

2019: US Capital One – $ 270.000.000

2017: GB/US Equifax – $ 575.510.395

Vielen Dank für die Aufmerksamkeit!

Kontakt:

isabel.Muench@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
D-53175 Bonn
www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us: