DIE LAGE DER IT-SICHERHEIT IN DEUTSCHLAND 2025

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

EINLEITUNG

Als die Cybersicherheitsbehörde des Bundes beobachtet das Bundesamt für Sicherheit in der Informationstechnik (BSI) kontinuierlich die Lage der IT-Sicherheit in Deutschland. Dabei stehen einerseits die Entwicklungen der Bedrohungs- und Gefährdungslagen sowie das Wachstum der Angriffsflächen für Cyberangriffe im Fokus des BSI. Andererseits beobachtet das BSI die Entwicklung der gesamtgesellschaftlichen Resilienz gegen Cyberbedrohungen und -gefährdungen und treibt Maßnahmen zur Steigerung von Präventions-, Verteidigungs- und Bewältigungsfähigkeiten aktiv voran.

Der BSI-Bericht zur Lage der IT-Sicherheit in Deutschland 2025 stellt die wichtigsten Entwicklungen für den Berichtszeitraum 1. Juli 2024 bis 30. Juni 2025 vor.

Die Cybersicherheitslage ist messbarer geworden. Unser Lagebericht stellt erstmals konsequent statistische Indikatoren in den Vordergrund. Wahr ist aber auch: Wir alle gemeinsam – Staat, Wirtschaft, Wissenschaft und Gesellschaft – haben noch ein großes Stück Arbeit vor uns. Wenn wir es nicht kurzfristig schaffen, uns und unsere Angriffsflächen zu verteidigen, werden wir verwundbar bleiben.

Claudia Plattner, Präsidentin des Bundesamtes für Sicherheit in der Informationstechnik

Den vollständigen Bericht finden Sie unter:
https://bsi.bund.de/lagebericht

Im gleichen Maß, in dem wir Digitalisierung vorantreiben, müssen wir im BMI IT-Sicherheit fordern und fördern. Cybersicherheit macht den Weg zum digitalen Staat erst gangbar. Auch deshalb ist dieser Bericht so wichtig: Indem er die ganze Bandbreite möglicher Angriffs- und Schutzpunkte aufzeigt, schärft er das Bewusstsein dafür, wie wichtig Cybersicherheit für jede und jeden Einzelnen von uns und für die Cybernation Deutschland ist. Unsere Gesellschaft, unsere Wirtschaft und letztlich unsere Demokratie als solche sind darauf angewiesen.

Alexander Dobrindt, Bundesminister des Innern

FAZIT DES BSI-LAGEBERICHTS 2025

Für die Lage der IT-Sicherheit in Deutschland besteht im Jahr 2025 kein Grund zur Entwarnung: Sie bleibt weiterhin auf angespanntem Niveau. Zwar sind wiederholt Erfolge gegen Cyberkriminalität zu verzeichnen, die sich weiter zuspitzende geopolitische Lage führt aber zu einer unverändert angespannten IT-Sicherheitslage. Ein wesentlicher Faktor dafür sind weiterhin die unzureichend geschützten Angriffsflächen.

Die Lageentwicklung wird in diesem ersten Online-Bericht des BSI noch deutlicher als in den Vorjahren durch quantitative Messungen dargestellt. Die Anzahl der Diagramme und Tabellen hat sich mit über 70 mehr als verdoppelt, während die Texte prägnanter gehalten sind und sich auf die statistischen Aussagen fokussieren. Dafür führen mehr Links als in den Vorjahren zu vertiefenden Informationen und zahlreiche Verweise stellen Querverbindungen her.

Wie schon im vorangegangenen Jahr hat das BSI auch in diesem Berichtszeitraum die Lage der Cybernation Deutschland in den fünf Dimensionen Bedrohungen, Angriffsfläche, Gefährdungen, Schadwirkungen und Resilienz beobachtet. Die noch konsequentere Darstellung der Lage in statistischen Messzahlen erleichtert Schlussfolgerungen: So werden einerseits Handlungsbedarfe, zum Beispiel im Bereich der Datenleaks oder der maliziösen Webseiten, direkt belegbar. Andererseits sind aber auch Erfolge messbar, etwa beim Botnetz-Monitoring im Rahmen des BSI-Sinkholing. Damit hat das BSI einen wichtigen Meilenstein auf dem Weg hin zu einem vollständigen Wirksamkeitsmonitoring und einem umfassenden, quantitativ messbaren Cyberlagebild für Deutschland erreicht.

Die Entwicklung der Cybersicherheit im Berichtszeitraum
In der Dimension Bedrohungen sind in diesem Jahr durchaus positive Trends zu beobachten. Im Cybercrime-Bereich führten internationale Strafverfolgungsmaßnahmen zu einer Stabilisierung. Namentlich mit LockBit und Alphv konnten zwei vormals sehr aktive Angreifergruppen nahezu ausgeschaltet werden. Bei den Angriffsinfrastrukturen stachen im Berichtszeitraum insbesondere die Botnetze Badbox und Vo1d als die größten und aktivsten hervor. An der Bekämpfung von Botnetzen in Deutschland war das BSI mit Sinkholing-Maßnahmen beteiligt.

Die Angriffsflächen in Deutschland – insbesondere Web-Angriffsflächen – zeigen dagegen nach wie vor einen besorgniserregenden Zustand. Web-Angriffsflächen müssen mehr professionelle Aufmerksamkeit durch wirksames Angriffsflächenmanagement erhalten. So werden beispielsweise viel zu oft bekannte Schwachstellen in Perimetersystemen zu spät oder gar nicht gepatcht. Im aktuellen Berichtszeitraum wurden darüber hinaus durchschnittlich täglich 119 neue Schwachstellen in IT-Systemen bekannt, ein Wachstum von rund 24 Prozent im Vergleich zum vergangenen Berichtszeitraum. Angriffsflächenmanagement für Web-Angriffsflächen muss ab sofort genauso selbstverständlich werden, wie es zum Beispiel Antiviren-Software für Mail-Angriffsflächen heute schon ist.

Die im Berichtszeitraum beobachteten Gefährdungen, das heißt die Zahl der tatsächlichen Angriffe, Vorfälle und Störungen, gingen damit auch in diesem Jahr nicht zurück. Erfolge im Bereich der Bedrohungen führen wegen zu vieler zu schlecht geschützter Angriffsflächen noch nicht zu einer Abnahme der Gefährdungen. Dabei setzte sich konkret der Trend weg von großen, aufwendigen Angriffen hin zu vielen kleinen, einfach durchzuführenden fort: rund 80 Prozent der angezeigten Angriffe, zum Beispiel mit Ransomware, richteten sich gegen kleine und mittlere Unternehmen (KMU), denen häufig die Mittel und das Wissen fehlen, um sich selbstständig zu schützen.

In der Dimension Schadwirkung beobachtete das BSI ebenso weiterhin hohe Werte. Die Anzahl der Leak-Geschädigten nahm zu, ebenso wie Zugangsdatendiebstähle. Während die Bereitschaft zur Zahlung von Lösegeldern im aktuellen Berichtszeitraum weiter sank, wurden im Zuge von Datenleaks nach Exploitation-Angriffen die durchschnittlich höchsten Lösegelder seit Beginn der Aufzeichnungen registriert. Hinzu kommen die Kosten durch entgangene Einnahmen bei angriffsbedingten Systemausfällen sowie Kosten für IT-forensische Untersuchungen oder für die Wiederherstellung von IT-Systemen.

Die dargestellten Gefährdungen und Schadwirkungen im BSI-Lagebericht 2025 zeigen, dass in der Dimension Resilienz noch großer Handlungsbedarf besteht. Vor allen Dingen die eigenen Angriffsflächen müssen verstärkt in den Fokus genommen werden. Während hier beispielsweise die meldepflichtigen KRITIS-Betreiber stetig Fortschritte bei ihren ISMS- und BCMS-Reifegraden erzielen, stehen wirksame Maßnahmen, insbesondere bei vulnerablen Gruppen wie beispielsweise KMU, politiknahen Institutionen oder Verbraucherinnen und Verbrauchern überwiegend noch aus.

Die Schlussfolgerung des BSI: Angriffsflächen schützen!
Der Schutz der Angriffsflächen ist 2026 der entscheidende Hebel, um die Cybersicherheit zu verbessern. Wie der diesjährige Bericht zeigt, suchen Angreifer verstärkt einfach anzugreifende Ziele mit schlechter Resilienz aus. Alle Institutionen müssen ihre Risikobewertung entsprechend anpassen: Je schlechter eine Angriffsfläche geschützt wird, desto wahrscheinlicher wird ein erfolgreicher Angriff. Dagegen senkt jedes konsequente Angriffsflächenmanagement – etwa ein restriktives Zugangsmanagement, zeitnahe Updates oder die Minimierung öffentlich erreichbarer Systeme – das Risiko erfolgreicher Angriffe unmittelbar. Dies trifft nicht nur auf große und umsatzstarke Unternehmen zu, sondern genau so auf KMU, Behörden, Wissenschaft sowie Bürgerinnen und Bürger. Und nur, wer sich aktiv schützt, erhöht die Chancen, Gefährdungen zu entgehen oder Schadwirkungen zu minimieren.

Die Analyse und das Management der eigenen Angriffsflächen müssen daher in jedem Unternehmen und jeder Institution – ob klein oder groß – als unverzichtbarer Teil eines effektiven Risikomanagements verstanden werden. Zudem müssen Hersteller, Diensteanbieter und staatliche Stellen gemeinsam an sicheren Produkten arbeiten und für Unternehmen und Verbrauchende einen besseren Schutz bieten. Aber auch die Bürgerinnen und Bürger müssen ihr Bewusstsein für Cybersicherheit erhöhen und resilienter werden.

Alle gesellschaftlichen Akteure, Wirtschaft, Staat, Forschung, Verbraucherschutz und auch die Verbrauchenden selbst sind gefordert, künftig noch stärker wirksame Maßnahmen zum Schutz ihrer Angriffsflächen zu ergreifen.

SYSTEMATIK DER BSI-LAGEBEOBACHTUNG

Das BSI beobachtet die Lage der Cybernation Deutschland in den Dimensionen **(1) Bedrohungen, (2) Angriffsfläche, (3) Gefährdungen, (4) Schadwirkung und (5) Resilienz.** Trifft eine Bedrohung, beispielsweise ein Schadprogramm, auf eine Angriffsfläche, zum Beispiel einen Webserver, entsteht eine Gefährdung. Eine Gefährdung ist also beispielsweise ein Cyberangriff, der je nach Resilienz (etwa dem Stand der Sicherheitsupdates) Schadwirkungen (zum Beispiel einen Datenabfluss) zur Folge haben kann. Oder anders ausgedrückt: Eine Schwäche (Angriffsfläche) wird ausgenutzt von einem Akteur (Bedrohung), der damit in einer Aktion (Gefährdung) einen Schaden (Schadwirkung) anrichtet.

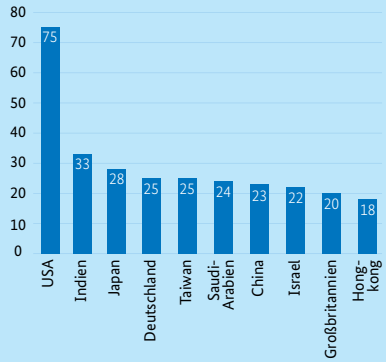
01 BEDROHUNGEN / THREATS

Stabilisierung auf hohem Niveau

ANGREIFERGRUPPEN

APT-Gruppen

APT-Gruppen 2025* weltweit nach Zielland (Top 10, Anteile in %)

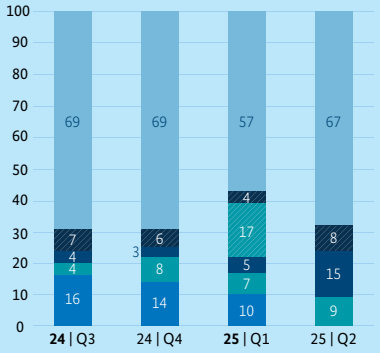


75 % der APT-Gruppen, die sich gegen mindestens eines der Top-10-Zielländer richteten, zielten auf die USA. Deutschland lag mit 25 % dieser APT-Gruppen auf Platz 4.

*Mehrfachnennungen möglich | *Quelle: TAS*

Cybercrime-Gruppen

Mutmaßlich Geschädigte weltweit nach Leak-Seite (Anteile in %)

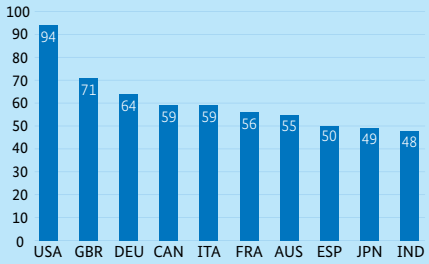


Cybercrime-as-a-Service, speziell Ransomware-as-a-Service, blieb im aktuellen Berichtszeitraum hoch. Ziele waren vermehrt mit Datenverschlüsselung und Datenexfiltration mit anschließender Erpressung konfrontiert. Zu den Hauptbetroffenen zählten KMU.

RansomHub, Akira, Qilin, Clop, Play, Weitere

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

Crime-Gruppen 2025* weltweit nach Zielland (Top 10, Anteile in %)



94 % der Crime-Gruppen, die sich gegen mindestens eins der Top-10-Zielländer richteten, zielten auf die USA, Deutschland lag auf Platz 3 (64 %). Seit 2019 wurden über 200 Leak-Seiten von Cybercrime-Gruppen beobachtet. Einzelne Cybercrime-Gruppen mussten ihre Aktivitäten jedoch nahezu vollständig einstellen.

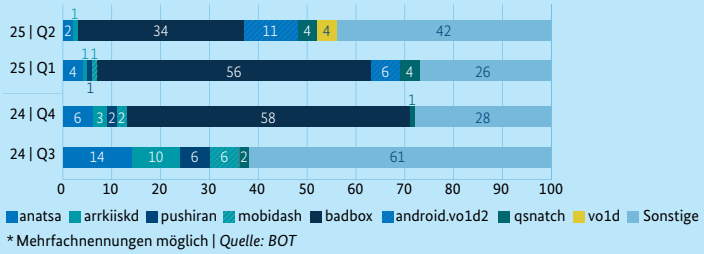
*Mehrfachnennungen möglich | *Quelle: TAS*

ANGRIFFSINFRASTRUKTUR

Botnetze

Zwei neue und für Nutzende schwierig erkennbare IoT-Botnetze wurden bekannt, darunter mit Badbox das größte in Deutschland aktive Botnetz (bis zu 58 % der infizierten Systeme). Die Geräte wurden bereits in der Produktionsphase infiziert.

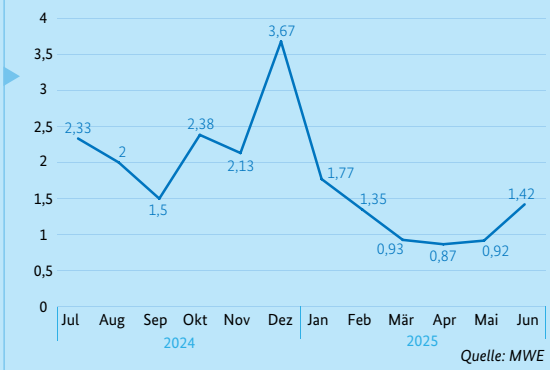
Botnetze nach Unique IP* (Anteile in % an allen Unique IP)



*Mehrfachnennungen möglich | *Quelle: BOT*

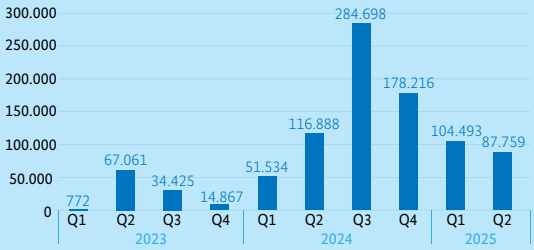
Maliziöse Webseiten

Durchschnittliche Lebensdauer maliziöser Webseiten (in Stunden)



Quelle: MWE

Neue maliziöse Webseiten (Anzahl)



Quelle: MWE

Phishing-Seiten

Weltweit bekannt gewordene Hostnames: über **800/Tag**

05 RESILIENZ

PRÄVENTION

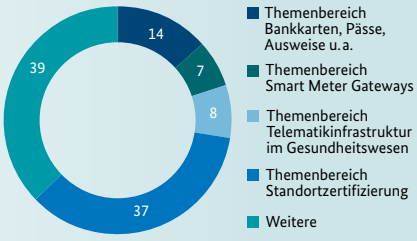
ZERTIFIZIERUNG

Common Criteria

Vom BSI gehaltene CC-Zertifikate gesamt und nach Themenbereichen (Anzahl)

413 vom BSI gehaltene CC-Zertifikate (Stand 30.6.2025)

105 davon im Berichtszeitraum neu ausgestellte Zertifikate:



Quelle: BSI

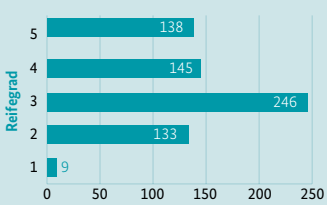
WIRTSCHAFT

Allianz für Cyber-Sicherheit

8.622 Unternehmen und Institutionen gehören der Allianz für Cyber-Sicherheit an, davon **212 Partner** und **117 Multiplikatoren**

(Stand: Anfang Sep. 2025) Quelle: BSI

KRITIS: ISMS-Reifegrade (Anzahl)



Reifegrade: System ist
5 – regelmäßig überprüft und verbessert
4 – regelmäßig überprüft
3 – etabliert und dokumentiert
2 – weitestgehend etabliert
1 – geplant, nicht etabliert

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

Quelle: KRN

Den vollständigen Bericht finden Sie unter:
https://bsi.bund.de/lagebericht

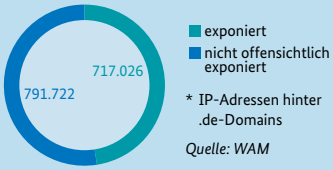
02 ANGRIFFSFLÄCHE / ATTACK SURFACE

Web-Angriffsflächen und multiple Kommunikationswege – große Herausforderung

WEB-ANGRIFFSFLÄCHE

Web-Angriffsflächen unter .de-Domains

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

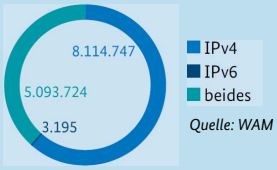


* IP-Adressen hinter .de-Domains

Quelle: WAM

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

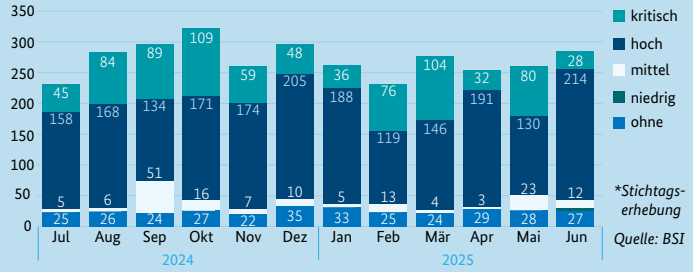
Erreichbare .de-Domains im 2. Quartal 2025 nach bereitgestelltem Internetprotokoll (Anzahl)



Quelle: WAM

Web-Angriffe auf die Bundesverwaltung

Täglich erreichbare IP-Adressen der Bundesverwaltung mit Schwachstellenverdacht nach Schweregrad der Schwachstelle* (Anzahl)



*Stichtagserhebung

Quelle: BSI

DIGITALE KOMMUNIKATIONSWEGE

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

rund 1.480

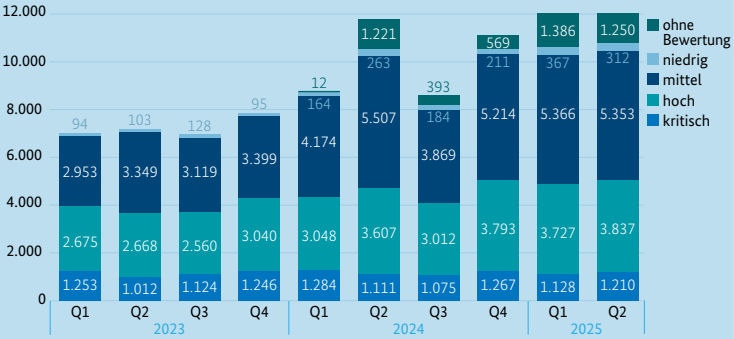
(hohe Dunkelziffer durch Privat-Accounts von Beschäftigten)

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

SCHWACHSTELLEN

Neue Schwachstellen

Neu bekannt gewordene Schwachstellen weltweit nach Schweregrad* (Anzahl)



* Revision der Statistik im Februar 2025. Vergleich mit früheren Publikationen nur eingeschränkt möglich.

Quelle: SSS

Bekannt gewordene Schwachstellen weltweit

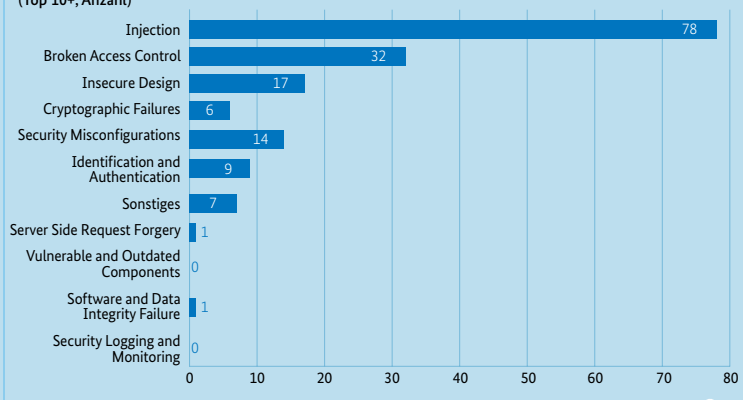
Durchschnittlich täglich

119 (+24 %, teils durch geänderte Melde-Policy)

Quelle: SSS

Valide Meldungen schwachstellenbehafteter Produkte* nach Schwäche

(Top 10+, Anzahl)



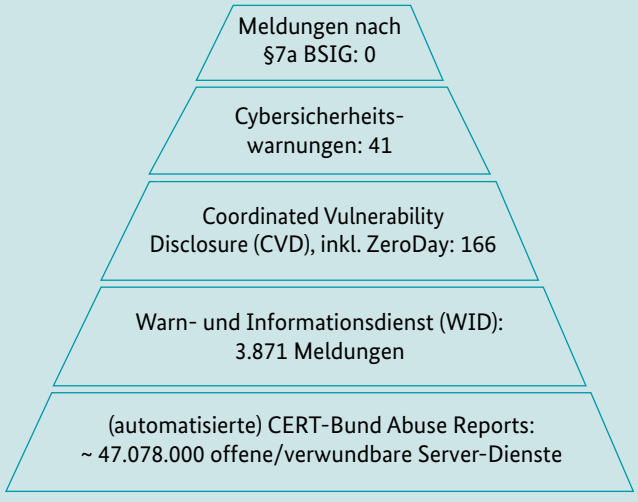
*Mehrfachnennungen möglich, Top 10+ nach OWASP Top 10: 2021 plus Kategorie „Sonstiges" | *Quelle: BSI*

05 RESILIENZ

VERTEIDIGUNG

MELDESYSTEME DES BSI

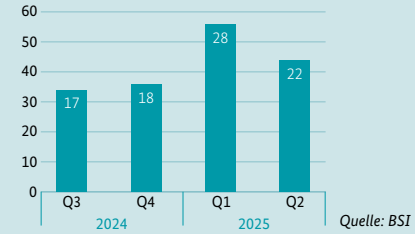
Prävention für Staat, Wirtschaft und Gesellschaft – Meldesysteme des BSI



Quelle: BSI

BUNDESVERWALTUNG

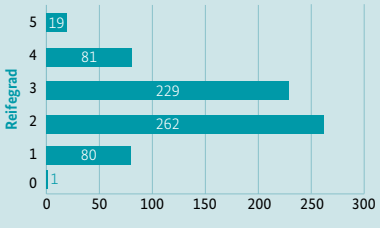
Spezialisierte Meldungen des BSI über akute Verwundbarkeiten an die betroffenen Behörden (Anzahl)



Quelle: BSI

WIRTSCHAFT

KRITIS: SzA-Reifegrade (Anzahl)



Umsetzungsgrad: Maßnahmen
5 – MUSS, SOLLTE, KANN erfüllt
4 – MUSS und SOLLTE erfüllt
3 – MUSS erfüllt
2 – Umsetzung begonnen
1 – in Planung
0 – nicht vorhanden

Quelle: KRN

03 GEFÄHRDUNGEN / ATTACKS

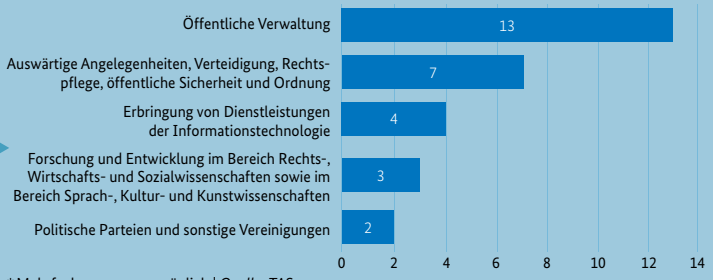
Mehr Exploitation, mehr Datenleaks

ANGREIFERMOTIVATION

Cyberspionage

Die öffentliche Verwaltung war ein Hauptziel von Cyberspionage: Die mit Abstand meisten der für Deutschland relevanten APT-Gruppen haben diesen Sektor ins Visier genommen.

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



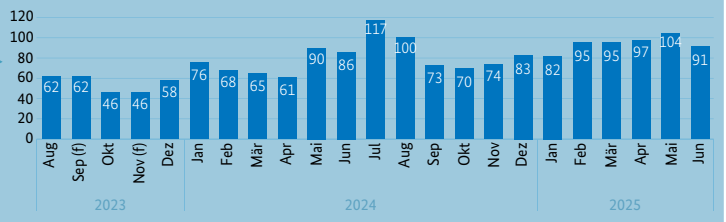
*Mehrfachnennungen möglich | *Quelle: TAS*

WEB-ANGRIFFSFLÄCHE

Web: Exploitation, Infiltration, Brute-Force

Exploitation hat im Berichtszeitraum deutlich zugenommen: +38 % im Vergleich zum vergangenen Berichtszeitraum.

Exploitation-Angriffe (Messzahl) am MADCAT-Honeypot



Sondereffekte im September und November 2023 bereinigt. (f): Werte fortgeschrieben. | *Quelle: MAD*

Rund 80 % der angezeigten Angriffe richteten sich gegen KMU.

950 Anzeigen wegen Ransomware-Angriffen

davon: 72 % mit Datenleaks

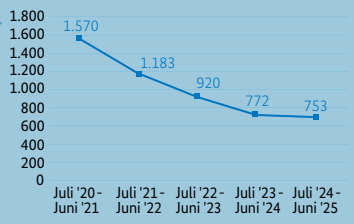
Quelle: Bundeskriminalamt

BUNDESVERWALTUNG

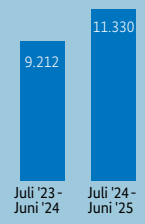
Angriffe über digitale Kommunikationswege

Trotz mehr potenzieller Ziele gingen in der Bundesverwaltung weniger E-Mails ein – hier sank die Zahl der Angriffe. Die Zahl blockierter Zugriffe auf schädliche Webseiten stieg jedoch um 23 %.

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



Durchschnittliche tägliche Zugriffsversuche aus der Bundesverwaltung auf schadcodebehaftete Server (Anzahl)



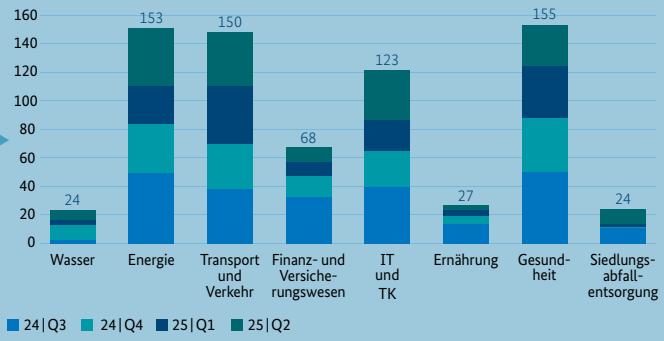
*Ohne Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen. | *Quelle: EBV*

Quelle: BSI

WIRTSCHAFT

Kritische Infrastrukturen

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



*Mehrfachnennungen möglich | *Quelle: KRM*

VERBRAUCHERINNEN UND VERBRAUCHER

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*

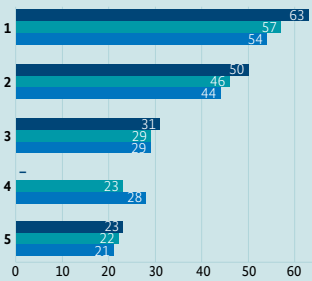
05 RESILIENZ

BEWÄLTIGUNG

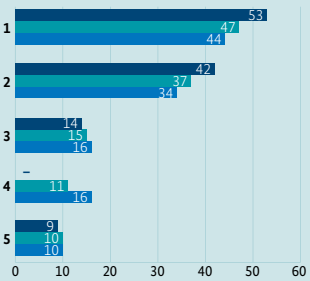
VERBRAUCHERINNEN UND VERBRAUCHER

Schutzmaßnahmen

Verbraucherinnen und Verbraucher nach Art der ihnen bekannten Schutzmaßnahmen (Anteile in %)



Verbraucherinnen und Verbraucher nach Art der von ihnen tatsächlich genutzten Schutzmaßnahmen (Anteile in %)



1 Sichere Passwörter **2** Zwei-Faktor-Anmeldung (2FA) **3** Passwortmanager im Browser **4** Passwortloses Anmelden **5** eigenständiger Passwortmanager

Mehrfachnennungen möglich; Zeichenerklärung: – keine Daten vorhanden | *Quelle: CYM*

Ø Anzahl bekannter Maßnahmen: 6,1

Ø Anzahl genutzter Maßnahmen: 3,8

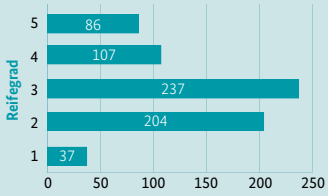
Sowohl die Bekanntheit als auch Nutzung von Schutzmaßnahmen waren 2025 weiterhin rückläufig.

Neben einem hohen Sicherheitsgefühl gaben auch viele Befragte an, dass sie die Maßnahmen als zu kompliziert empfinden.

Quelle: CYM

WIRTSCHAFT

KRITIS: BCMS-Reifegrade (Anzahl)

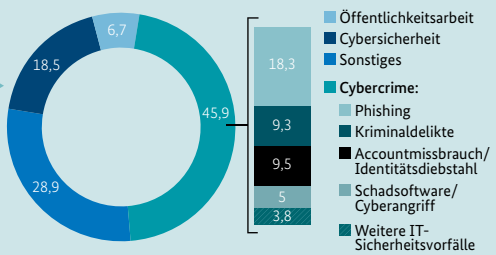


Reifegrade: System ist
5 – regelmäßig überprüft und verbessert
4 – regelmäßig überprüft
3 – etabliert und dokumentiert
2 – weitestgehend etabliert
1 – geplant, nicht etabliert

Quelle: KRN

VERBRAUCHERINNEN UND VERBRAUCHER

Anfragen von Verbraucherinnen und Verbrauchern an das Service-Center des BSI nach Thema (Anteile in %)



Quelle: BSI

Knapp 10.500 Anfragen von Verbrauchenden zum Thema Cybersicherheit erreichten das BSI-Service-Center im aktuellen Berichtszeitraum. Das BSI-Service-Center nimmt somit eine wichtige Rolle als Beratungsstelle ein.

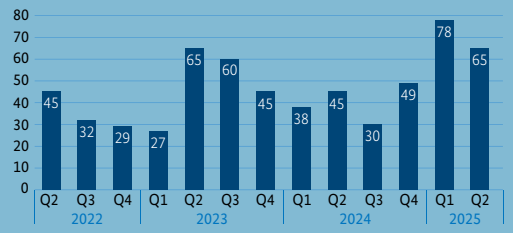
04 SCHADWIRKUNG / IMPACT

Mehr Datenleaks, mehr Lösegeld

DATENLEAKS

Leak-Geschädigte

Mutmaßlich Geschädigte aus Deutschland auf Leak-Seiten (Anzahl)



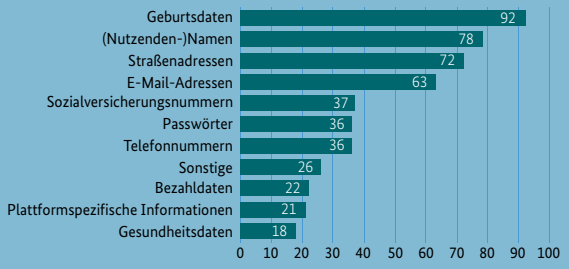
Neues Allzeithoch an Leak-Geschädigten war teilweise auf Mehrfach-Leaks derselben Geschädigten zurückzuführen.

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

Datenleaks

Im Berichtszeitraum gab es 461 Datenleaks mit Daten von deutschen Institutionen und Verbrauchenden. Betroffen waren Geburtsdaten (92 %), physische (72 %) und E-Mail-Adressen (63 %), plus z. B. Gesundheits- und Finanzdaten sowie Passwörter.

Datenleaks nach Art der geleakten Information* (Anteile in %)



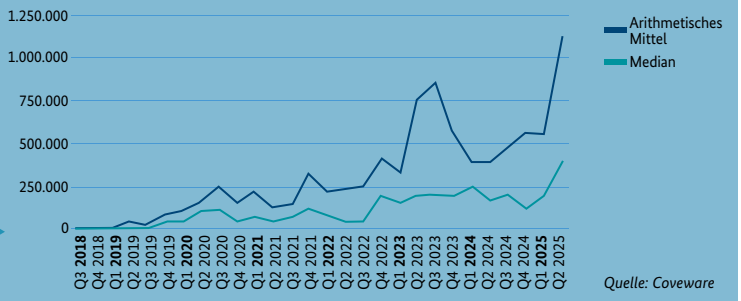
* Mehrfachnennungen möglich | *Quelle: DLK*

LÖSEGELDER

Lösegelder

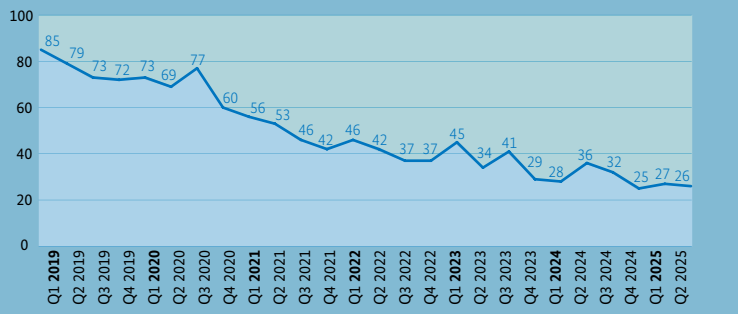
Während die Bereitschaft zur Zahlung von Lösegeldern im aktuellen Berichtszeitraum weiter sank, waren im Zuge von Datenleaks nach Exploitation-Angriffen die durchschnittlich höchsten Lösegelder seit Beginn der Aufzeichnungen zu beobachten.

Durchschnittliche Lösegeldzahlungen (Dollar)



Quelle: Coveware

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

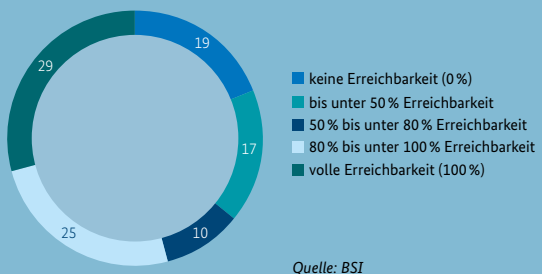


Quelle: Coveware

DDOS-AUSFÄLLE

DDoS-Hacktivismus

Erreichbarkeit der von DDoSia angegriffen Server (Anteile in %)

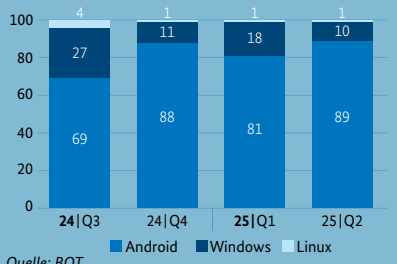


Quelle: BSI

INFIZIERTE SYSTEME

Infizierte Systeme

Infizierte Systeme (Unique IP) nach Betriebssystem (Anteile in %)



Das Wachstum des Internet of Things (IoT) treibt die Digitalisierung an. IoT-Geräte machen auch in Deutschland einen wachsenden Teil infizierter Systeme aus. Internetprovider nutzen Meldungen des BSI an sie, um Betroffenen zu helfen.

Quelle: BOT

05 RESILIENZ

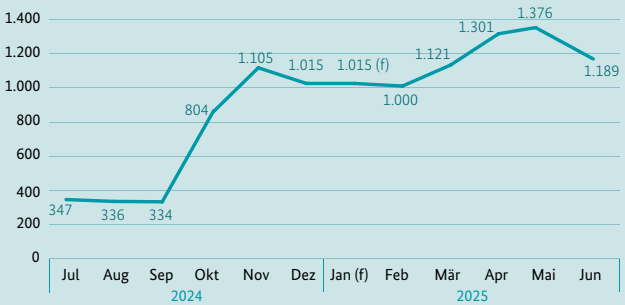
UNTERSTÜTZUNG DURCH DAS BSI

Bereinigung infizierter Systeme

Der Unique-IP-Index misst die Menge infizierter Systeme in den Botnetzen, die im BSI-Sinkholing sind. Durch sogenanntes Sinkholing werden die Kommunikationsversuche infizierter Systeme (Bots) mit den Command-and-Control-Servern der Angreifer auf Server des BSI umgeleitet. Die Bots können dadurch nicht mehr für weitere Angriffe missbraucht werden.

Darüber hinaus unterrichtet das BSI die Provider infizierter Systeme, damit diese ihrerseits wiederum ihre Kunden informieren können.

Unique-IP-Index (Einheit: 2019 = 100)



f: Wert wurde fortgeschrieben | *Quelle: BOT*

Bewältigungsmaßnahmen bei vorinfizierten IoT-Systemen

Mittlerweile werden häufig auch IoT-Systeme (Internet of Things) Opfer von Botnetzen. Im Fall von BadBox gelangen die günstigen Android-Geräte oft bereits infiziert in den Handel. Mit dem Internet verbunden, werden sie Teil eines Botnetzes und können von Angreifern ausgenutzt werden – oft, ohne dass dies für die Besitzer der infizierten Geräte erkennbar ist. Das BSI betreibt Maßnahmen, um betroffene Geräte zu identifizieren und die Besitzer zu benachrichtigen.

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87, 53175 Bonn
E-Mail bsi@bsi.bund.de
Telefon +49 (0) 22899 9582-0

Stand: Oktober 2025

Druck
Appel & Klinger Druck und Medien GmbH, Schneckenlohe

Texte, Redaktion und Layout
Bundesamt für Sicherheit in der Informationstechnik

Bildnachweise
Titel: Bettina Gericke | Kompaktmedien, Agentur für Kommunikation GmbH; S. 2, Portraits: A. Dobrindt und C. Plattner: © BMI/Henning Schacht

Artikelnummer: BSI-LB25/514