Die Lage der IT-Sicherheit in Deutschland 2026



Impressum:

Herausgeber:	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Bezugsquelle:	Bundesamt für Sicherheit in der Informationstechnik (BSI)
	Godesberger Allee 87, 53175 Bonn
	E-Mail: bsi@bsi.bund.de
	Telefon: +49 (0) 22899 9582 – 0
	Telefax: +49 (0) 22899 9582 – 5400
Stand:	November 2026
Redaktion:	Bundesamt für Sicherheit in der Informationstechnik (BSI)

Inhalt

Inhalt ... **3**
Ausgewählte Vorfälle ... 5
Abbildungsverzeichnis ... 5

Sitemap der digitalen Fassung ... **9**

Vorwort des Bundesministers des Innern ... **10**

Vorwort der Präsidentin des Bundesamts für Sicherheit in der Informationstechnik ... **11**

Zusammenfassung und Lagebewertung ... **13**
Bedrohungslage: Kritische Dynamik ... 14
Angriffsfläche: Wachsende Angriffsflächen, weitläufig angreifbar ... 15
Gefährdungslage: Kleine und mittlere Unternehmen sind besonders gefährdet ... 16
Schadwirkungen: Verdopplung der infizierten Systeme ... 18
Resilienz: Fortschritte, aber zu langsam ... 19
Fazit ... 21

1 Bedrohungslage ... **22**
1.1 Angriffsinfrastrukturen ... 22
1.1.1 Botnetze ... 23
1.1.2 Quantencomputer ... 24
1.1.3 Phishing-Websites ... 25
1.2 Angreiferaktivitäten ... 27
1.2.1 Aufklärungstätigkeiten ... 29
1.2.2 Neue Malware-Varianten ... 31
1.3 Angreifergruppen ... 32
1.3.1 Cybercrime-Gruppen ... 33
1.3.2 APT-Gruppen, Cyberconflict ... 35
1.4 Hybride Bedrohungen ... 37

2 Angriffsfläche ... **41**
2.1 Attack Surface Score ... 41
2.2 Time-to-Exploit ... 42
2.2.1 Neue Schwachstellen ... 43
2.2.2 Hardware-Schwachstellen ... 44
2.2.3 Schwachstellen in KI-Systemen ... 45
2.2.4 Schwachstellen in kryptografischen Verfahren ... 48
2.3 Vernetzte Geräte ... 49
2.3.1 Vernetzte Geräte insgesamt ... 50
2.3.2 Consumer-IoT-Geräte ... 51
2.3.3 Industrial-IoT-Geräte ... 52
2.3.4 Smart-City-Geräte ... 53
2.3.5 Automotive-IoT-Geräte ... 53
2.3.6 Vernetzte Geräte im Gesundheitswesen und der Telematikinfrastruktur ... 56
2.4 Web-Angriffsflächen ... 58
2.4.1 Web-Angriffsflächen unter .de-Domains ... 59
2.4.2 Web-Angriffsflächen der Bundesverwaltung ... 60
2.5 Mail-Angriffsflächen der Bundesverwaltung ... 62

3 Gefährdungslage ... **65**
3.1 Attack Score ... 65
3.2 Gefährdungslage nach Angriffsarten ... 66
3.2.1 Angriffe auf Web-Angriffsflächen ... 66
3.2.2 Angriffe mittels digitaler Kommunikationswege auf die Bundesverwaltung ... 71
3.3 Gefährdungslage nach Angreifermotivation ... 74
3.3.1 Cybercrime ... 75
3.3.2 Cyberconflict, Cyberspionage ... 77
3.4 Gefährdungslage nach Zielgruppen ... 78
3.4.1 Wirtschaft ... 79
3.4.2 Verbraucherinnen und Verbraucher ... 82

4 Schadwirkungen ... 86
4.1 Impact Score ... 86
4.2 Infizierte Systeme ... 87
4.3 Lösegelder ... 88
4.4 Leak-Geschädigte ... 90
4.5 Datenleaks ... 93
4.6 DDoSia-Schadwirkungen ... 94

5 Resilienz ... 97
5.1 Resiliente IT-Produkte und IT-Infrastrukturen ... 97
5.1.1 Cyber Resilience Act ... 97
5.1.2 LLMs als Hochgeschwindigkeits-Schwachstellenscanner ... 99
5.1.3 LLM-Härtung ... 100
5.1.4 5G/6G-Mobilfunkstandard ... 101
5.1.5 Zertifizierung und Kennzeichen ... 102
5.1.6 Cloud-Sicherheit ... 105
5.1.7 Post-Quanten-Kryptografie ... 106
5.1.8 Operational Technology (OT) ... 107
5.1.9 Stand der Technik ... 108
5.2 Resiliente Gesellschaft ... 109
5.3 Resiliente Wirtschaft ... 111
5.3.1 Resilienz Kritischer Infrastrukturen ... 111
5.3.2 Resilienz kleiner und mittlerer Unternehmen ... 113
5.4 Resiliente Bundesverwaltung ... 114
5.4.1 Prävention in der Bundesverwaltung ... 115
5.4.2 Verteidigung der Netze des Bundes ... 116
5.5 Das BSI für die Cybernation Deutschland ... 117
5.5.1 Das BSI für Wirtschaft, Verwaltung und andere Organisationen ... 118
5.5.2 Das BSI für Verbraucherinnen und Verbraucher in Deutschland ... 127

6 Sonderlagen ... 132
6.1 Digitale Souveränität ... 132
6.2 Cyberdome ... 133
6.3 Künstliche Intelligenz ... 134

Anhang ... 138
Methodische Hinweise ... 138
Aktivitätsniveaustatistik (ANS) ... 138
Botnetz-Monitoring (BOT) ... 138
Cybersicherheitsmonitor (CYM) ... 140
DDoS-Statistik (DOS) ... 140
Erhebung über den E-Mail-Verkehr mit der Bundesverwaltung (EBV) ... 140
Erhebung über die Phishing-Websites (PHW) ... 141
Erhebung über Phishing-Mails (PHR) ... 142
Exploitation-Statistik (MCF) ... 142
KRITIS-Meldungen (KRM) ... 143
KRITIS-Nachweise (KRN) ... 144
Leak-Geschädigten-Statistik (LKS) ... 144
Leak-Statistik (DLK) ... 145
Malware-Statistik (MWS) ... 145
Portscan-Statistik (MCS) ... 146
Schwachstellenstatistik (SSS) ... 147
Threat-Actors-Statistik (TAS) ... 148
Web-Angriffsflächenmessung (WAM) ... 148
Abkürzungsverzeichnis ... 149
Glossar ... 152

Ausgewählte Vorfälle

Ausgewählte Vorfälle: Bedrohungslage Schwachstellenscanner Trivy durch Supply-Chain-Angriff kompromittiert.

Ausgewählte Vorfälle: Angriffsfläche Erfolgreiche Angriffe auf Systeme zur Verwaltung mobiler Endgeräte mittels Ausnutzung von Zero-Day-Schwachstellen 63

Ausgewählte Vorfälle: Angriffsfläche Schwachstellen in KI-Agentensystem OpenClaw.

Ausgewählte Vorfälle: Gefährdungslage: Phishing-Angriffe via Messenger 84

Ausgewählte Vorfälle: Gefährdungslage: Cyberspionage-Angriffe auf Ziele im politischen und vorpolitischen Raum 85

Ausgewählte Vorfälle: Schadwirkungen Datenleak bei KI-basierter Bild- und Videobearbeitungs-App .

Ausgewählte Vorfälle: Resilienz - Operation Endgame 130

Abbildungsverzeichnis

Abbildung 1-1: Gefundene Schwachstellen mit hohem Schweregrad pro Woche 22
Abbildung 1-2: Botnetze von Juli 2025 bis Juni 2026 nach Unique IP 23
Abbildung 1-3: Wissenschaftliche Arbeiten nach benötigter Leistung des Quantencomputers 24
Abbildung 1-4: Phishing-Websites weltweit 25
Abbildung 1-5: Ausgewählte Phishing-Hostnames nach nachgeahmter Branche 26
Abbildung 1-6: Portscans am MADCAT-Honeypot des BSI 27
Abbildung 1-7: Portscans am MADCAT-Honeypot des BSI 29
Abbildung 1-8: Portscans am MADCAT-Honeypot von Juli 2025 bis Juni 2026 nach Ports (Top 5) .. 30
Abbildung 1-9: Portscans gegen Port 443 am MADCAT-Honeypot nach geographischer Herkunft 31
Abbildung 1-10: Durchschnittlicher täglicher Zuwachs neuer Malware-Varianten 31
Abbildung 1-11: Aktive Angreifergruppen am 30.06.2026 weltweit nach Motivation 32
Abbildung 1-12: Aktive Leak-Seiten weltweit 33
Abbildung 1-13: Mutmaßlich geschädigte Organisationen weltweit nach Leak-Seite 34
Abbildung 1-14: Aktive APT-Gruppen am 30.06.2026 nach Zielland 35
Abbildung 1-15: APT-Gruppen nach Zielland und Attribution 36
Abbildung 2-1: Attack Surface Score 41
Abbildung 2-2: Time-to-Exploit 42
Abbildung 2-3: Neu bekannt gewordene Schwachstellen weltweit nach Schweregrad 43
Abbildung 2-4: Neu bekannt gewordene Hardware-Schwachstellen 44
Abbildung 2-5: Schwachstellen in KI-Agenten 45
Abbildung 2-6: Neu bekannt gewordene Schwachstellen in KI-Agenten nach Schweregrad 46
Abbildung 2-7: Prompt-Injection-Schwachstellen in KI-Systemen nach Schweregrad 47
Abbildung 2-8: Neu bekannt gewordene Schwachstellen in kryptografischen Verfahren 48
Abbildung 2-9: Prognose von Verbindungen vernetzter Geräte mit dem Internet in Deutschland, Vernetzte Geräte insgesamt 49
Abbildung 2-10: Prognose von Verbindungen vernetzter Geräte mit dem Internet in Deutschland nach Art des Geräts 50
Abbildung 2-11: Prognose von Verbindungen vernetzter Geräte mit dem Internet in Deutschland, Consumer IoT 51
Abbildung 2-12: Prognose von Verbindungen vernetzter Geräte mit dem Internet in Deutschland, Industrial IoT 52
Abbildung 2-13: Prognose von Verbindungen vernetzter Geräte mit dem Internet in Deutschland, Smart City 53
Abbildung 2-14: Prognose von Verbindungen vernetzter Geräte mit dem Internet in Deutschland, Automotive IoT 53

Abbildung 2-15: Schwachstellen mit Bezug zu Fahrzeugen von Juli 2025 bis Juni 2026 nach Ausnutzungsmöglichkeit 54
Abbildung 2-16: Schwachstellen mit Bezug zu Fahrzeugen von Juli 2025 bis Juni 2026 nach möglichem Angriffsweg 55
Abbildung 2-17: Prognose von Verbindungen vernetzter Geräte mit dem Internet in Deutschland, Gesundheitswesen und Telematikinfrastruktur 56
Abbildung 2-18: Kritische Ereignisse in der Telematikinfrastruktur und im Gesundheitswesen 57
Abbildung 2-19: Web-Angriffsfläche von Deutschland 58
Abbildung 2-20: Aus dem Internet erreichbare .de-Domains nach geografischer Lage 59
Abbildung 2-21: .de-Domains nach Hoster 59
Abbildung 2-22: Aus dem Internet erreichbare IP-Adressen der Bundesverwaltung nach Schwachstellenverdacht 60
Abbildung 2-23: Neue Schwachstellenverdachte in der Bundesverwaltung 61
Abbildung 2-24: Erreichbare IP-Adressen der Bundesverwaltung mit Schwachstellenverdacht nach Schweregrad der Schwachstelle 61
Abbildung 2-25: Aktive E-Mail-Adressen der Bundesverwaltung 62
Abbildung 3-1: Attack Score 65
Abbildung 3-2: Exploitation-Angriffe am MADCAT-Honeypot 66
Abbildung 3-3: Exploitation-Angriffe am MADCAT-Honeypot 66
Abbildung 3-4: Exploitation-Angriffe Juli 2025 bis Juni 2026 nach ausgenutztem Protokoll (Top 5) 67
Abbildung 3-5: Durchschnittliche Exploitation-Angriffe auf die React2Shell-Schwachstelle 68
Abbildung 3-6: Bekannt gewordene DDoS-Angriffe in Deutschland 69
Abbildung 3-7: Durchschnittliche Bandbreite aller bekannt gewordenen DDoS-Angriffe in Deutschland 69
Abbildung 3-8: Durchschnittliche tägliche E-Mails und Spam-E-Mails an die Bundesverwaltung .. 71
Abbildung 3-9: Spam-Mail-Index für die Bundesverwaltung 72
Abbildung 3-10: Spam-Mails von Juli 2025 bis Juni 2026 nach Art des Spams 72
Abbildung 3-11: Durchschnittliche tägliche Malware-Angriffe per E-Mail auf die Bundesverwaltung 73
Abbildung 3-12: Durchschnittliche tägliche Zugriffsversuche aus der Bundesverwaltung auf schadcodebehaftete Server 73
Abbildung 3-13: Aktivitätsniveau von Angreifergruppen weltweit 74
Abbildung 3-14: Crime-Aktivitätsniveau 75
Abbildung 3-15: Anzeigen wegen Ransomware-Angriffen insgesamt 75
Abbildung 3-16: APT-Aktivitätsniveau 77
Abbildung 3-17: Störungen Kritischer Infrastrukturen nach Störungsursache 78
Abbildung 3-18: Störungen kritischer Anlagen nach Sektor 79
Abbildung 3-19: Störungen kritischer Anlagen nach ausgewählten Störungsursachen 80
Abbildung 3-20: Störungen in der Luftsicherheit und in der Luftfahrbranche nach Störungsursache 81
Abbildung 3-21: Anzeigen wegen Ransomware-Vorfällen von kleinen und mittleren Unternehmen 81
Abbildung 3-22: Phishing-Mails nach nachgeahmter Branche 82
Abbildung 3-23: Von einer Straftat im Internet betroffene Verbraucherinnen und Verbraucher in Deutschland 83
Abbildung 3-24: Verbraucherinnen und Verbraucher in Deutschland nach Art der Betroffenheit von Cyberkriminalität 84
Abbildung 4-1: Impact Score 86
Abbildung 4-2: Infizierte Systeme 87
Abbildung 4-3: Infizierte Systeme (Unique IP) nach Betriebssystem 87
Abbildung 4-4: Lösegelder insgesamt 88
Abbildung 4-5: Durchschnittliche Lösegeldzahlungen 89
Abbildung 4-6: Betroffene von Ransomware-Angriffen nach Zahlungsbereitschaft 90
Abbildung 4-7: Mutmaßlich geschädigte Organisationen aus Deutschland auf Leak-Seiten 90
Abbildung 4-8: Mutmaßlich Leak-geschädigte Organisationen aus Deutschland und weltweit 91
Abbildung 4-9: Mutmaßlich Leak-geschädigte Organisationen aus Deutschland nach Leak-Seite .. 92
Abbildung 4-10: Datenleaks von Juli 2025 bis Juni 2026 nach Art der geleakten Daten 93

Abbildung 4-11: Von DDoSia angegriffene Server in Deutschland und weltweit nach Erreichbarkeit 94
Abbildung 4-12: Von DDoSia angegriffene Server in Deutschland und weltweit nach Verlangsamung 95
Abbildung 5-1: Fortschritt der CRA-Standardisierungsaktivitäten 97
Abbildung 5-2: Fallstudie: Schwachstellen mit hohem Schweregrad in verbreitetem Internet-Browser 99
Abbildung 5-3: 31 Sprachmodelle nach Robustheit gegen Prompt Injections, 2024 bis 2026 100
Abbildung 5-4: BSI-Beiträge im Standardisierungsgremium 3GPP SA3 101
Abbildung 5-5: das IT-Sicherheitskennzeichen des BSI 102
Abbildung 5-6: Bestand an IT-Sicherheitskennzeichen 102
Abbildung 5-7: Ausgewählte Personenzertifizierungen 103
Abbildung 5-8: Zertifizierte Digitale Gesundheitsanwendungen 104
Abbildung 5-9: Common-Criteria-Zertifizierungen 105
Abbildung 5-10: Cloud Service Provider mit C5-Testat 105
Abbildung 5-11: EU-Roadmap Post-Quanten-Kryptografie 106
Abbildung 5-12: Durchschnittliche tägliche Unique Visitors und Views der Stand-der-Technik-Bibliothek 108
Abbildung 5-13: Von Verbraucherinnen und Verbrauchern genutzte Maßnahmen 110
Abbildung 5-14: Verbraucherinnen und Verbraucher nach Gründen, Maßnahmen nicht zu nutzen 110
Abbildung 5-15: Betreiber Kritischer Infrastrukturen mit Reifegrad/Umsetzungsgrad 3 oder höher von Juli 2025 bis Juni 2026 nach Art des Systems 111
Abbildung 5-16: Betreiber Kritischer Infrastrukturen nach Reifegrad/Umsetzungsgrad ihrer Systeme 112
Abbildung 5-17: KMU nach Selbsteinschätzung sowie nach CyberRisikoCheck 113
Abbildung 5-18: KMU im CyberRisikoCheck von Juli 2025 bis Juni 2026 nach Erfüllungsgrad 114
Abbildung 5-19: IP-Adressen der Bundesverwaltung nach Verschlüsselungsstandard ab TLS 1.2 . 115
Abbildung 5-20: Spezialisierte Meldungen des BSI über akute Verwundbarkeiten an die betroffenen Behörden 116
Abbildung 5-21: Durchschnittliche tägliche neue Sperrungen maliziöser Webseiten 116
Abbildung 5-22: Durchschnittlich täglich erstellte Malware-Detektoren 117
Abbildung 5-23: BITS-Mitteilungen und WID-Meldungen von Juli 2025 bis Juni 2026 Einheit: Anzahl 118
Abbildung 5-24: CVD-Meldungen von IT-Sicherheitsforschenden an das BSI 118
Abbildung 5-25: Meldungen von IT-Sicherheitsforschenden an das BSI nach Art der Meldung 119
Abbildung 5-26: Beratungsanfragen aus Ländern und Kommunen 120
Abbildung 5-27: Beratungen der Bundesverwaltung von Juli 2025 bis Juni 2026 nach Beratungsthema 121
Abbildung 5-28: Beratungen der Justiz im Bund von Juli 2025 bis Juni 2026 nach Beratungsthema 122
Abbildung 5-29: Beratungen der Politik im Bund von Juli 2025 bis Juni 2026 nach Beratungsthema 122
Abbildung 5-30: Bundesbehörden nach Bekanntheit der Beratungsangebote des BSI und Beratungsthema 123
Abbildung 5-31: Auditierte Einrichtungen des Bundes 123
Abbildung 5-32: Resilienzsteigerung durch Standardrevision, Basisdatenerhebung, Umsetzungsberatung sowie Nachhaltung und Begleitung der ergriffenen Maßnahmen 124
Abbildung 5-33: NIS-2-Registrierungen im BSI-Portal am 30. Juni.2026 125
Abbildung 5-34: Akteure der Luftsicherheit in Deutschland 125
Abbildung 5-35: Registrierte Akteure der Luftsicherheit in Deutschland 126
Abbildung 5-36: BSI-Leistungen für Akteure der Luftsicherheit 126
Abbildung 5-37: Unique-IP-Index 127
Abbildung 5-38: Anfragen an das BSI-Service-Center 128
Abbildung 5-39: Anfragen von Verbraucherinnen und Verbrauchern an das Service-Center nach Thema 129
Abbildung 5-40: Newsletter-Abonnements 130
Abbildung 6-1: Cyberdome 133

Sitemap der digitalen Fassung



Abbildung 1 Sitemap der digitalen Fassung

Vorwort des Bundesministers des Innern

Die Sicherheit unseres Landes entscheidet sich zunehmend im digitalen Raum. IT-Sicherheit ist Voraussetzung für unsere Handlungsfähigkeit, unseren Wohlstand und das Vertrauen in unseren demokratischen Rechtsstaat. Auch der diesjährige Bericht zur Lage der IT-Sicherheit in Deutschland zeigt: Deutschland ist Ziel professioneller Cyberangriffe. Und die Bedrohung wächst. Kriminelle stehlen Daten, verschlüsseln Systeme und erpressen Geld. Staatlich gesteuerte Akteure spähen Informationen aus, stören Abläufe und versuchen, Einfluss auszuüben. Sie greifen unser Wissen an, bedrohen unseren Wohlstand und untergraben das Vertrauen in unseren Staat. Betroffen sind Behörden, Betriebe sowie Bürgerinnen und Bürger. Jede unzureichend gesicherte Schnittstelle wird zum möglichen Einfallstor. Aufgewärmte Kühltruhen und Blutbanken sind dabei nur die Spitze des Eisbergs.

Darüber hinaus leiten Künstliche Intelligenz und die Entwicklung von Quantencomputern einen Paradigmenwechsel ein. Quantencomputer, die schon jetzt gängige Verschlüsselungen brechen können, werden bereits absehbar in der Breite verfügbar sein. Das birgt die Gefahr heute bereits gestohlene Daten später zu entschlüsseln.

KI erweitert heute schon die Möglichkeiten von Angreifern. Mit ihrer Hilfe werden Schwachstellen in kürzester Zeit gefunden und ausgenutzt, täuschend echte Nachrichten und Stimmen erzeugt, Menschen gezielter manipuliert und Angriffe schneller vorbereitet. Desinformation und Identitätsbetrug erhalten neue Dimensionen.

KI bietet jedoch auch unseren Sicherheitsbehörden große Chancen. Wenn wir sie uns nutzbar machen, kann sie unsere Fähigkeit zur Gegenwehr stärken: Sie wertet große Datenmengen schneller aus, erkennt ungewöhnliche Aktivitäten, liefert Hinweise auf Schwachstellen und unterstützt die Analyse von Vorfällen. So können Angriffe früher erkannt und Reaktionen beschleunigt, Schäden begrenzt und die digitale Widerstandsfähigkeit Deutschlands weiter ausgebaut werden.

Aktive Cyberabwehr ist eine gemeinsame Aufgabe: Staat, Wirtschaft, Wissenschaft und Bevölkerung müssen Verantwortung übernehmen und ihre Fähigkeiten zur Prävention und Reaktion stärken. Dafür braucht es klare Standards, belastbare Strukturen und solides Fachwissen.

Das Bundesamt für Sicherheit in der Informationstechnik leistet hierzu einen zentralen Beitrag. Der Bericht zur Lage der IT-Sicherheit in Deutschland 2026 schafft Transparenz, ordnet Entwicklungen ein und macht Handlungsbedarf sichtbar.

Alexander Dobrindt

Vorwort der Präsidentin des Bundesamts für Sicherheit in der Informationstechnik

Das Jahr 2026 hat uns – vielleicht mehr als jedes andere zuvor – vor Augen geführt, was eine dynamische Sicherheitslage bedeutet. Die Disruption, die insbesondere von hochperformanter, agentischer KI ausgeht, hat neue Maßstäbe gesetzt: Stellten wir im vergangenen Jahr noch eine leichte Entspannung in der Bedrohungsdimension fest, haben wir es nun mit Werkzeugen zu tun, die Cyberangriffe in bisher unbekannten Mengen und Geschwindigkeiten ermöglichen. So setzen Cyberangreifer mehr und mehr auf die Ausnutzung von Schwachstellen, wobei fortschrittliche KI, die weitgehend automatisiert nach ihnen scannt und passende Schadcodes für Exploitation-Angriffe gleich mitliefert, diese Entwicklung erheblich beschleunigt. In der nächsten Stufe erwarten wir dann zunehmend Angriffe durch autonom agierende KI-Agenten.

Gleichzeitig überschätzen viele Organisationen die Sicherheit ihrer IT-Netzwerke und machen es Angreifern viel zu leicht. Mit Blick auf die Cyberresilienz in Deutschland besorgt uns insgesamt die Gefahr eines Geschwindigkeitsgefälles: Die Angreifer machen sich die neuen Technologien aktuell noch deutlich schneller zunutze als die Verteidiger.

Die Lage der IT-Sicherheit in Deutschland beschreiben wir für den aktuellen Berichtszeitraum daher als angespannt bis kritisch. Dies spiegelt sich auch im erstmals vorgestellten Cyber Index wider, der Verwundbarkeit, Gefährdungen und Schadwirkungen im digitalen Raum in einer Zahl zusammenfasst. Im Vergleich zum vorherigen Berichtszeitraum weist er ein Plus von 50 %aus – kein gutes Zeichen.

Wir wissen spätestens seit der Darwin'schen Evolutionslehre, dass die überlebensfähigste Spezies diejenige ist, die sich am ehesten dem Wandel anpassen kann. Dieses Prinzip gilt uneingeschränkt für die Herausforderungen, vor denen wir stehen, wenn wir den digitalen Raum adäquat schützen wollen. Cyberaggression hat sich verändert – sie ist nicht nur schneller, umfassender und schlagkräftiger, sondern auch um ein Vielfaches komplexer geworden. Und diese Entwicklung steht noch am Anfang. Das bedeutet mitnichten, dass wir ihr schutzlos ausgeliefert sind. Wir müssen uns aber klarmachen, dass Sicherheit im digitalen Raum kein Zustand ist, sondern ein niemals endender Prozess in einem hochdynamischen Umfeld. Hier bestehen zu können erfordert Orientierungs-, Handlungs- und Innovationsfähigkeit.

Konkret bedeutet das zum Ersten, dass wir diese Herausforderungen nicht nur sichtbar, sondern auch messbar machen müssen – denn nur, was wir messen können, lässt sich auch effektiv verändern. Mit Blick auf die Lage der IT-Sicherheit in Deutschland haben wir diesbezüglich nun einen Meilenstein erreicht: Mit unserem diesjährigen Bericht veröffentlichen wir erstmals den BSI Cyber Index. Er ist ab sofort ein wichtiges Werkzeug, das uns schnell und zuverlässig Auskunft über die Cybersicherheitsdynamik in Deutschland gibt und uns zu jedem Zeitpunkt aufzeigt, wo wir ansetzen müssen.

Zum Zweiten müssen wir dem dynamischen Umfeld mit Automatisierung begegnen. Unvorhersehbare Ereignisse erfordern Reaktionen, manchmal sogar in Millisekunden, die manuelle Prozesse nicht leisten können. Um diese Art der Automatisierung zu ermöglichen, bauen wir auf Initiative des Bundesinnenministers mit dem Cyberdome einen Schutzschirm für den digitalen Raum der Bundesrepublik. Als zentral koordiniertes Frühwarn- und Schutzsystem soll er Cyberangriffe nicht nur schneller erkennen und auswerten, sondern auch gezielt abwehren.

Zum Dritten ist es für Deutschland unabdingbar, KI zur Abwehr von Cyberangriffen zu nutzen, statt sie den Angreifern zu überlassen. Die Bundesregierung hat darüber hinaus mit dem AI Safety and Security Institute (AISI) Deutschland eine nationale Kompetenz- und Evaluierungsinstitution für leistungsfähige KI-Systeme geschaffen. Als zentrale Einrichtung bündelt es technische, strategische und sicherheitspolitische Expertise. Zu seinen Kernaufgaben zählt neben der technischen Evaluierung leistungsfähiger KI-Modelle unter anderem die Analyse sicherheitsrelevanter Auswirkungen von KI auf Staat, Wirtschaft und Gesellschaft. Dabei bilden das BSI und die Bundesnetzagentur in einer ersten Phase einen Nukleus des KI-Sicherheitsinstituts und wurden

vom Bundesministerium des Innern (BMI) und dem Bundeministerium für Digitales und Staatsmodernisierung (BMDS) mit den entsprechenden Aufgaben betraut.

Dies sind lediglich drei Beispiele für Maßnahmen, mit denen wir uns den Herausforderungen stellen. Wir sind der festen Überzeugung, dass die Cybernation Deutschland in der Lage ist, dem tiefgreifenden Wandel, in dem sich die digitale Welt befindet, erfolgreich zu begegnen. Unser Bericht zur Lage der IT-Sicherheit zeigt auf, wo wir jetzt am dringendsten anpacken müssen.

Claudia Plattner

Zusammenfassung und Lagebewertung

Die Lage der IT-Sicherheit in Deutschland war im aktuellen Berichtszeitraum angespannt bis kritisch. Damit hat das Bundesamt für Sicherheit in der Informationstechnik eine Verschärfung der IT-Sicherheitslage festgestellt, die im vergangenen Berichtszeitraum noch als angespannt gegolten hatte. Anlass der Neubewertung waren besorgniserregende Entwicklungen rund um die Themen Künstliche Intelligenz (KI) und Exploitation-Angriffe, die Cyberangriffe in bisher ungekannten Mengen und Geschwindigkeiten ermöglichen. Zugleich überschätzten viele Unternehmen, Behörden und andere Organisationen ihre Resilienz gegenüber Cyberangriffen deutlich und machten es Cyberangreifern daher oft zu leicht.

Zur Quantifizierung der IT-Sicherheitslage legt das BSI mit dem aktuellen Bericht zur Lage der IT-Sicherheit in Deutschland erstmals den BSI Cyber Index vor. Mit ihm werden die verschiedenen Dimensionen der Cybersicherheit in einer einzigen normierten Kennzahl zusammengefasst – im aktuellen Berichtszeitraum bereits anhand der normierten Scores über die Entwicklung von Angriffsflächen (Attack Surface Score), Gefährdungslage (Attack Score) und Schadwirkungen (Impact Score). Die prozentualen Veränderungen beziehen sich auf den vergangenen Berichtszeitraum. Steigende Indexwerte zeigen wachsende verwundbare Angriffsflächen, Gefährdungen und Schadwirkungen an.

Gesamtlage:

Angespannt bis kritisch

- **BSI Cyber Index:** durchschnittlich **170 Punkte** im aktuellen Berichtszeitraum (plus 50 % gegenüber dem vergangenen Berichtszeitraum)
- Wachsende, verwundbare **Angriffsflächen**, vor allem durch IoT und KI: **plus 117** %
- Steigende Angriffszahlen, vor allem durch **Exploitation-Angriffe: plus 48 %**
- Hohe Dynamik durch Entwicklungen bei **Künstlicher Intelligenz**
- **Resilienz verbessert sich nur langsam**: Selbst grundlegende Sicherheitsmaßnahmen werden oft nicht oder nur langsam umgesetzt.

BSI Cyber Index:

Einheit: 2024=100 (Messzahl)



Quelle: BSI

Die Dynamik der Entwicklung resultiert im aktuellen Berichtszeitraum aus neuen Verwundbarkeiten und Schwachstellen (plus 35 %), insbesondere in Web-Angriffsflächen, die von leistungsstarken KI-Modellen in kürzester Zeit gefunden und ausgenutzt werden können. Auch deutliche Zuwächse bei Exploitation-Angriffen (plus 48 %) wirkten sich auf den BSI Cyber Index aus. Wer gegen diese nicht gut aufgestellt war und nach einem Cyberangriff Lösegeld zahlte, musste im Einzelfall deutlich mehr zahlen als, im vergangenen Berichtszeitraum. Die je Einzelfall stark gestiegenen Lösegelder schlugen spürbar auf den Gesamtindex durch.

Die Lage im Einzelnen:

Bedrohungslage: Kritische Dynamik

Während im vergangenen Berichtszeitraum eine Stabilisierung der Bedrohungslage auf hohem Niveau festgestellt wurde, nahm die Lage im aktuellen Berichtszeitraum eine kritische Entwicklung. Agentische KI auf der Basis großer Sprachmodelle erwies sich als hochperformanter Teil der Angriffsinfrastruktur, die mehr kann, als Phishing-Mails zu formulieren: Sie findet Schwachstellen und entwickelt zeitgleich Exploits zu deren Ausnutzung (Exploitation). Darüber hinaus kann sie Schwachstellen in bisher unbekanntem Ausmaß zu neuen Angriffsvektoren verketten. Das erleichtert nicht nur die Erstinfektion eines Systems, sondern auch die Ausbreitung innerhalb eines kompromittierten Netzwerks.

Seit einigen Jahren schon setzen Cyberangreifer verstärkt auf Exploitation. Während die Anzahl per E-Mail verbreiteter neuer Malware-Varianten zurückgeht (minus 20 % im aktuellen Berichtszeitraum), verlegen sich die Akteure mehr und mehr auf die Ausnutzung von Schwachstellen in aus dem Internet erreichbaren Systemen. Für die Scans nach solchen Schwachstellen wurde im aktuellen Berichtszeitraum ein Zuwachs von 57 % beobachtet. Fortschrittliche KI, die weitgehend automatisiert nach Schwachstellen scannt und passende Schadcodes für Exploitation-Angriffe erstellt, wird diese Entwicklung erheblich beschleunigen.

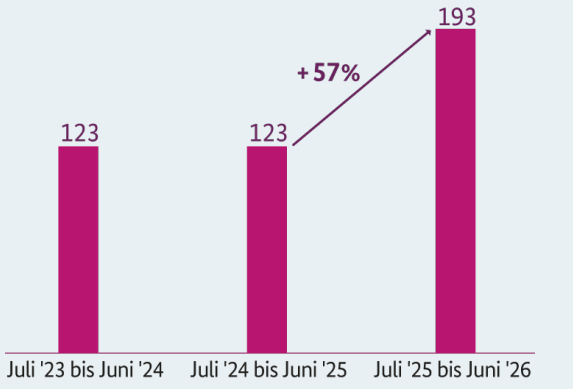
Bedrohungslage:

Kritische Dynamik

- **57 % mehr Schwachstellenscans**
- Zusätzliche Dynamik durch **KI-Agentensysteme als neue Angriffsinfrastrukturen**
- Hohes Bedrohungspotenzial durch automatisiertes Scannen und Erstellung von Schadcode

Portscans am MADCAT-Honeypot

Einheit: 2024=100 (Messzahl)



Quelle: BSI

Cyberkriminelle gehen dabei opportunistisch vor und wählen ihre Ziele hauptsächlich nach Angriffsfläche und Verwundbarkeit aus. Eine häufige Vorgehensweise ist, dass Angreifer die Daten der Geschädigten nicht nur verschlüsseln, sondern sie vorab kopieren, um zusätzlich mit der Veröffentlichung von Geschäftsgeheimnissen zu drohen (Double Extortion).

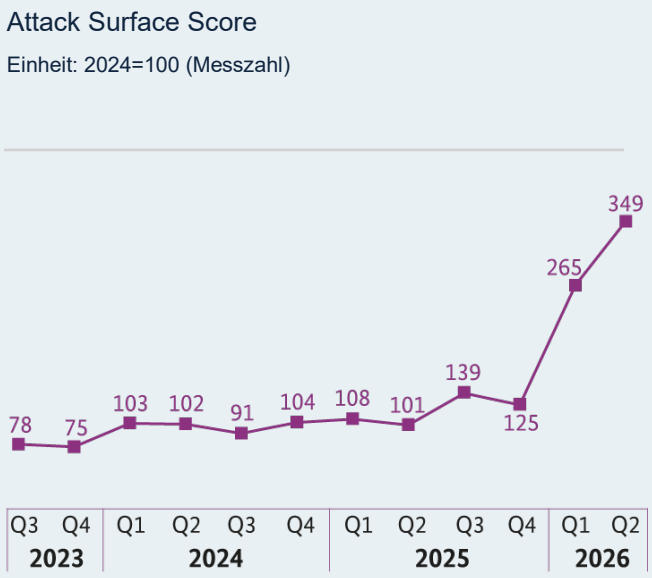
Angriffsfläche: Wachsende Angriffsflächen, weitläufig angreifbar

Die Angriffsflächen in Deutschland wachsen im Zuge der Digitalisierung stetig. Präventive Maßnahmen wachsen nicht ausreichend mit, um sie wirksam zu schützen.

Angriffsfläche:

Attack Surface Score: plus 117 % gegenüber dem vergangenen Berichtszeitraum

- Vor dem Hintergrund **neuer KI-Angriffsinfrastrukturen,** die Schwachstellen in aus dem Internet erreichbaren Systemen in kürzester Zeit finden und ausnutzen, ist die **Verwundbarkeit der Angriffsfläche** auch in Deutschland im aktuellen Berichtszeitraum **signifikant gestiegen.**
- Im 2. Quartal 2026 kletterte der Attack Surface Score auf 349 Punkte und lag damit 3,5-mal so hoch wie im Referenzjahr 2024.



Quelle: BSI

Täglich wurden im Durchschnitt 160 neue Schwachstellen bekannt. Das waren 35 % mehr als im vergangenen Berichtszeitraum. Besonders besorgniserregend ist dabei die immer kürzer werdende Zeitspanne zwischen Bekanntwerden einer Schwachstelle und deren Ausnutzung (Time-to-Exploit). Im vergangenen Berichtszeitraum vergingen bis zur Ausnutzung durchschnittlich 53 Tage, im aktuellen Berichtszeitraum lediglich 25 Tage und im 2. Quartal 2026 nur noch 8 Tage – ein Rückgang um 85 %. Fortschrittliche KI besitzt auch hier das Potential, diese Entwicklung weiter zu beschleunigen. Wie bereits beschrieben, kann sie Schwachstellen identifizieren und automatisiert verketten und ermöglicht so schnellere, und gezieltere Angriffe mit höherem Schadenspotential und geringem Kostenaufwand.

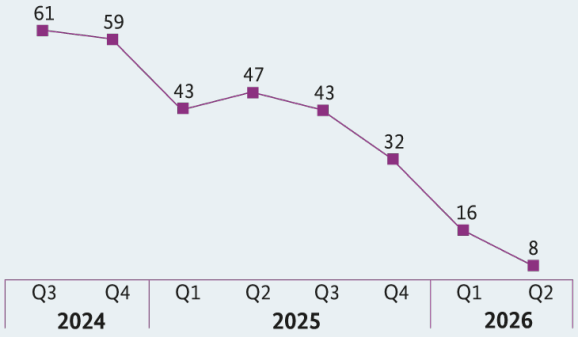
Angriffsfläche:

Wachsende Angriffsflächen, weitläufig angreifbar

- Angriffsflächen wachsen schnell, vor allem durch IoT-Geräte, die oft schlecht abgesichert sind.
- 35 % mehr neue Schwachstellen
- Time-to-Exploit, d. h. der durchschnittliche Zeitraum zwischen Bekanntwerden und Ausnutzung einer Schwachstelle, sank auf nur noch 8 Tage.

Time-to-Exploit

Einheit: Anzahl Tage



Quelle: BSI

Besonders schnell wächst die Angriffsfläche im Bereich vernetzter Geräte. Prognosen zufolge wird es bis Ende 2026 in Deutschland insgesamt rund 620 Millionen Verbindungen von vernetzten Geräten mit dem Internet geben (plus 22 % gegenüber dem Vorjahr), bei rund der Hälfte handelt es sich um Consumer-IoT-Geräte, also internetfähige Alltagsgegenstände.

Gefährdungslage: Kleine und mittlere Unternehmen sind besonders gefährdet

Wenn eine Bedrohung auf eine Angriffsfläche trifft, entsteht eine Gefährdung. Erfolgreiche Cyberangriffe resultieren aus dem Zusammenspiel von Cyberbedrohungen und schlecht geschützten Angriffsflächen.

Über alle Angriffsarten hinweg ist die Gefährdung durch Cyberangriffe im aktuellen Berichtszeitraum gestiegen.

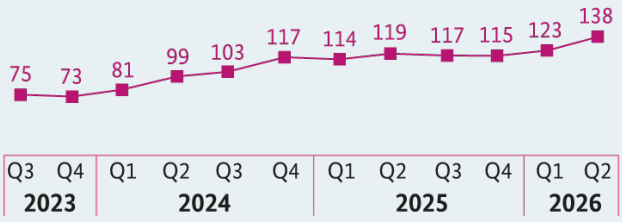
Gefährdungslage:

Attack Score: plus 9 % gegenüber dem vergangenen Berichtszeitraum

- Im aktuellen Berichtszeitraum lag der Attack Score bei durchschnittlich 123 Punkten. Damit lag die Kennzahl 9 % über dem Niveau des vergangenen Berichtszeitraums. Die spürbare Zunahme der Gefährdungen rührte insbesondere von Exploitation-Angriffen her. Hier war im aktuellen Berichtszeitraum ein erheblicher Zuwachs von 48 % zu verzeichnen.

Attack Score

Einheit: 2024=100 (Messzahl)



Quelle: BSI

Ursächlich für das Wachstum des Attack Scores ist insbesondere die starke Zunahme von Exploitation-Angriffen (plus 48 % im aktuellen Berichtszeitraum). Die qualitative Entwicklung der Angriffsinfrastrukturen ist besorgniserregend: Bereits im Herbst 2025 wurde ein automatisierter Angriff mittels KI beobachtet. Im Sommer 2026 gelang es KI-Agenten dann, unkontrolliert aus Testumgebungen auszubrechen und Exploitation-Angriffe gegen unbeteiligte Dritte auszuführen.

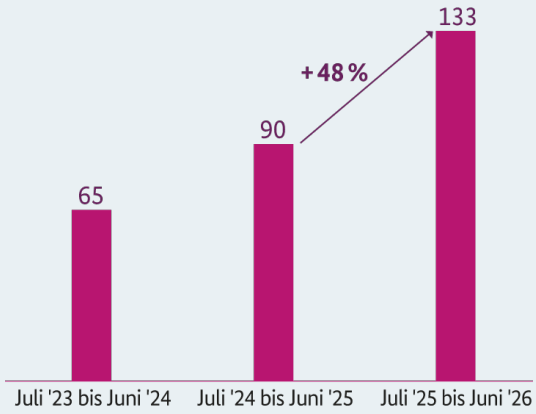
Gefährdungslage:

Starkes Wachstum bei Exploitation, KMU besonders gefährdet

- **48 % mehr Exploitation-Angriffe**, d. h. bei der Ausnutzung von Schwachstellen in aus dem Internet erreichbaren Systemen.
- **90 %** der zur Anzeige gebrachten Ransomware-Vorfälle betrafen KMU.
- **34 % mehr DDoS-Angriffe**, Bandbreite dieser Angriffe ebenfalls gestiegen

Exploitation-Angriffe am MADCAT-Honeypot

Einheit: 2023=100 (Messzahl)



Quelle: BSI

Auch die Zahl von DDoS-Angriffen stieg insbesondere im 2. Quartal 2026 an. Anders als im vergangenen Berichtszeitraum stieg auch die durchschnittliche Bandbreite dieser Angriffe.

Im Bereich Cybercrime wurde im aktuellen Berichtszeitraum ein moderater Anstieg des Aktivitätsniveaus von 8 % beobachtet, ebenfalls stieg die Anzahl der Anzeigen wegen Ransomware-Angriffen (plus 10 %). Besonders betroffen sind hierbei kleine und mittlere Unternehmen (KMU): Im Jahr 2025 trafen 90 % der zur Anzeige gebrachten Ransomware-Vorfälle KMU (2024: 80 %). Dennoch unterschätzen viele KMU ihre eigene Gefährdungslage erheblich und schützen sich nicht ausreichend – so werden sie zu leichten Zielen für opportunistische Angreifer.

Gerade angesichts von Automatisierung und immer schneller verfügbarer Schwachstellen-Exploits ist es daher unerlässlich, dass auch kleinere Unternehmen in IT-Sicherheit investieren. Eine effektive Maßnahme ist beispielsweise, Sicherheitspatches automatisiert einzuspielen, um bekannt gewordene Schwachstellen schnellstmöglich zu schließen.

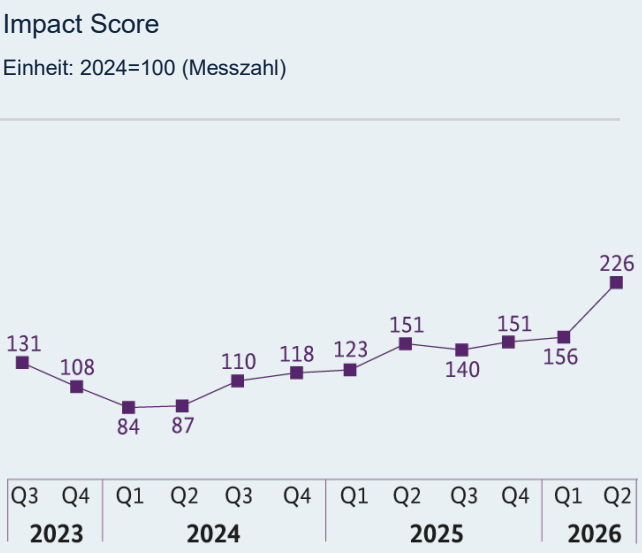
Schadwirkungen: Verdopplung der infizierten Systeme

Während einige der beobachteten Schadwirkungen im Vergleich zum vergangenen Berichtszeitraum auf einem vergleichbaren Niveau blieben oder sogar leicht sanken, stiegen andere Schadwirkungen erheblich.

Schadwirkungen:

Impact Score: plus 33 % gegenüber dem vergangenen Berichtszeitraum

- Der **Impact Score** des BSI, der das Ausmaß der Schadwirkungen durch Cyberangriffe misst, lag im aktuellen Berichtszeitraum bei **durchschnittlich 168 Punkten** und damit erneut deutlich über dem Niveau des vergangenen Berichtszeitraums (plus 33 %), wobei im 2. Quartal 2026 ein neuer Höchststand von 226 Punkten zu verzeichnen war. Während die **Lösegelder je Fall** im aktuellen Berichtszeitraum erheblich **zulegten**, ist die Gesamtsumme der in Blockchains identifizierten Lösegelder leicht gesunken. Dagegen ist die **Zahl der infizierten Systeme in Deutschland erheblich gestiegen**



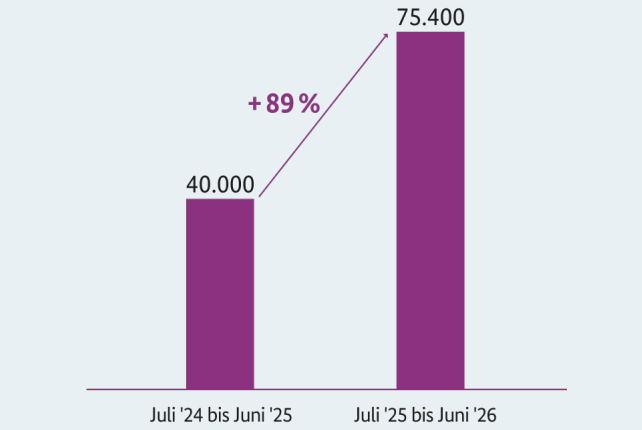
Quelle: BSI

Das Hellfeld infizierter Systeme hat sich im aktuellen Berichtszeitraum nahezu verdoppelt. 88 % der infizierten Systeme waren Android-Geräte – häufig Android-basierte Consumer-IoT-Geräte. Aufgrund „eingesparter“ Sicherheitsmechanismen sind diese vielfach leichte Ziele für Angreifer, die sie beispielsweise zu Botnetzen verknüpfen und für DDoS-Angriffe nutzen.

Schadwirkungen:

Verdopplung der infizierten Systeme

- Hellfeld **infizierter Systeme** in Deutschland hat sich auf durchschnittlich täglich über **75.000** nahezu verdoppelt.
- **88 % davon: Adroid-Geräte**, vor allem Consumer-IoT
  → Aus infizierten Systemen bauen Angreifer neue Angriffsinfrastrukturen wie Botnetze auf, die sie dann zum Beispiel für DDoS-Angriffe einsetzen können.



1) Vom BSI an deutsche Internetprovider und andere Netzbetreiber gemeldete IP-Adressen

Quelle: BSI

Hier wie auch bei Ransomware-Vorfällen zeigt sich, dass es immer teurer wird, an der Sicherheit zu sparen. Umgekehrt zeigt sich aber auch: Immer mehr Organisationen sind gut genug aufgestellt, um sich nicht dem Erpressungsdruck der Angreifer beugen zu müssen: Nur in 20 % der Vorfälle waren die betroffenen Organisationen zur Zahlung eines Lösegeldes bereit. Die von Mitigationsdienstleistern berichteten Lösegeldzahlungen je Fall stiegen allerdings auf

durchschnittlich rund 1,9 Millionen US-Dollar, sodass die Summe der gezahlten Lösegelder lediglich um 8 % zurückging.

Resilienz: Fortschritte, aber zu langsam

Im aktuellen Berichtszeitraum wurde die Resilienz der Cybernation Deutschland an vielen Stellen weiter erhöht. Dennoch wird dieses Ziel noch nicht ausreichend priorisiert und mögliche Verbesserungen werden zu langsam umgesetzt. Angesichts der rasant wachsenden Bedrohungen (zum Beispiel die stark sinkende Time-to-Exploit) besteht die Gefahr eines größer werdenden Geschwindigkeitsgefälles zwischen Angreifern und Verteidigern. Um dies zu verhindern, ist es wichtig, neuartige Technologien wie Large Language Models (LLMs) als Schwachstellenscanner auch gegen Cyberangriffe zu nutzen, statt sie den Angreifern zu überlassen. Die Verteidigerseite hat hier erstmals die Chance, im Wettlauf mit den Angreifern nicht nur zu reagieren, sondern mittels besserer defensiver KI IT-Produkte und -Infrastrukturen sowohl im Herstellungsprozess als auch im Betrieb wirksam zu schützen.

Rechtliche Rahmenbedingungen: Cyberresilienz im Fokus

Regulatorisch macht Cybersicherheit große Fortschritte – auch im aktuellen Berichtszeitraum gab es mehrere umfangreiche Regulierungen, die zur Einhaltung von Mindeststandards verpflichten.

Auf europäischer Ebene schafft der Cyber Resilience Act (CRA) die Verpflichtung, digitale Produkte über ihren gesamten Lebensweg hinweg cybersicher zu gestalten. Darüber hinaus müssen ausgenutzte Schwachstellen in digitalen Produkten künftig gemeldet werden. Zusätzlich wurde die 2022 verabschiedete NIS-2-Richtlinie in nationales Recht umgesetzt. Das Umsetzungsgesetz verpflichtet nun zahlreiche Unternehmen und Organisationen, sich zu registrieren, Cybersicherheitsmaßnahmen umzusetzen und Vorfälle zu melden.

Wirtschaft: Viele Unternehmen erfüllen selbst Mindestanforderungen nicht

Angesichts zu langsamer Verbesserungen der Cyberresilienz in der Wirtschaft kommt die NIS-2-Umsetzung gerade zur richtigen Zeit.

Kleine und mittlere Unternehmen stellen das Rückgrat der deutschen Wirtschaft dar, haben Angriffen aber oft nichts entgegenzusetzen. Obwohl 90 % der befragten Unternehmen ihre Cybersicherheit als „gut“ oder „sehr gut“ einschätzten, erfüllten selbst diejenigen Unternehmen, die sich einem CyberRisikoCheck des BSI unterzogen und deshalb zu den besonders Problembewussten gehören dürften, durchschnittlich lediglich 55 % der Mindestanforderungen, um Angriffsflächen zu schützen und Schadwirkungen im Fall der Fälle begrenzen zu können.

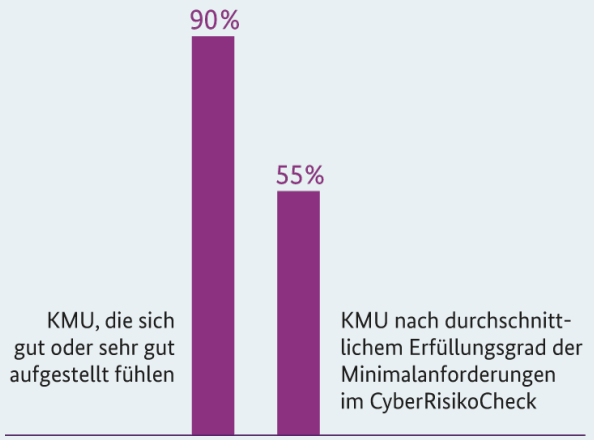
Resilienz:

Fortschritte, aber zu langsam!

- **Schnelle Reaktionsfähigkeit** erforderlich, bspw. durch **Automatisierung und defensive Nutzung von KI**
- **Mindeststandards** werden immer öfter verpflichtend: CRA, NIS-2…
- **Umsetzung oft schleppend**, vor allem in der nicht regulierten Wirtschaft, zugleich oft Selbstüberschätzung potenzieller Angriffsziele
- Weniger als die Hälfte der Verbraucherinnen und Verbraucher nutzt grundlegende Sicherheitsmaßnahmen.
- Notwendigkeit, **Mindeststandards konsequent umzusetzen**

KMU nach Selbsteinschätzung und CyberRisikoCheck

Einheit: Anteile in Prozent



Quelle: BSI

Betreiber Kritischer Infrastrukturen sind hingegen schon länger gesetzlich reguliert – und besser geschützt. Aber auch hier gibt es Verbesserungspotential. Der Anteil der Betreiber Kritischer Infrastrukturen, deren Informationssicherheitsmanagementsysteme und Business-Continuity-Managementsysteme Reifegrad 3 erreichen und somit die rechtlichen Mindestanforderungen erfüllten, blieb mit 78 % bzw. 65 % weitgehend unverändert, der Anteil der Systeme zur Angriffserkennung mit Umsetzungsgrad 3 stieg auf 55 %.

Verbraucherinnen und Verbraucher: Weniger als die Hälfte nutzt grundlegende Sicherheitsmaßnahmen

Im Privaten setzte sich die Sorglosigkeit fort: Obwohl alljährlich jeder Zehnte von Cyberkriminalität betroffen ist, werden selbst die bekanntesten und gängigsten Cybersicherheitsmaßnahmen wie sichere Passwörter von weniger als der Hälfte der befragten Verbraucherinnen und Verbraucher genutzt. Als Grund dafür wurde neben dem Gefühl, sicher zu sein, Überforderung genannt. Dabei könnten selbst einfache Maßnahmen (vgl. „Basistipps zur IT-Sicherheit“) zu mehr Sicherheit beitragen.

Das BSI für die Cybernation Deutschland

Um die Cyber-Resilienz von Staat, Wirtschaft und Gesellschaft zu stärken, leistet das BSI auf vielfältige Arten Unterstützung – vom digitalen Verbraucherschutz über das Erheben und Teilen von Lageinformationen bis hin zur Unterstützung bei der Vorfallsbewältigung und Beteiligung am Takedown von Botnetzen.

Ein wichtiges Element ist die systematische und gezielte Beratung von Organisationen beim Aufbau ihrer Cybersicherheitssysteme – beispielsweise mit dem Programm CyberGovSecure, das initiiert wurde, um die Cyberresilienz der gesamten Bundesverwaltung zügig, wirkungsvoll und messbar zu steigern. Ziel ist es, die Handlungsfähigkeit des Staates in einem zunehmend komplexen Bedrohungsumfeld nachhaltig zu sichern. Das Programm setzt auf umsetzungsorientierte Maßnahmen, eine zentrale Unterstützung bei der Durchführung und eine finanzielle Förderung der teilnehmenden Behörden.

Fazit

Die Lage der IT-Sicherheit in Deutschland war im aktuellen Berichtszeitraum angespannt und zuletzt kritisch. Aufgrund der fortschreitenden Digitalisierung wachsen verwundbare Angriffsflächen konstant und die Anzahl der Angriffe nimmt stetig zu. Die Entwicklung von Künstlicher Intelligenz befeuert diese Dynamik noch weiter. Wo früher die Ausnutzung von Schwachstellen Expertenwissen erforderte und mit einem gewissen Zeitaufwand einherging, werden die Angriffe immer schneller, kostengünstiger und gezielter.

Längst kann man sich nicht mehr hinter der Ausrede verstecken, kein „lohnendes Ziel“ zu sein. Angegriffen wird, wer ein leichtes Ziel ist. Egal ob es sich um veraltete Software kleiner Unternehmen oder schlecht abgesicherte Consumer-IoT handelt, Angreifer gehen grundsätzlich opportunistisch vor.

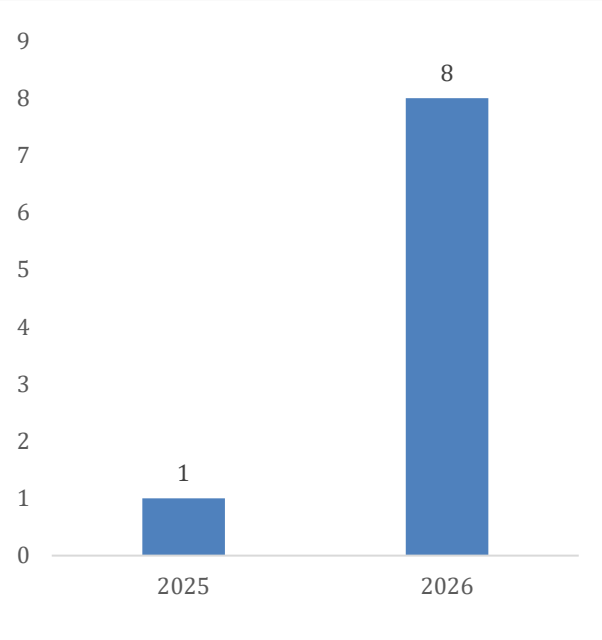
Viele Unternehmen und Verbraucherinnen und Verbraucher wähnen sich aber immer noch in falscher Sicherheit oder vermeiden sogar die Auseinandersetzung mit der eigenen Cybersicherheit, weil das Thema ihnen überfordernd erscheint. Dabei können schon einfache Maßnahmen wie das automatisierte Einspielen von Patches, das Anlegen von Backups und die Verwendung zertifizierter Geräte viel dazu beitragen, sich selbst abzusichern und zu einem weniger leichten Ziel zu machen.

1 Bedrohungslage

Die Bedrohungslage erwies sich im aktuellen Berichtszeitraum als angespannt bis kritisch. Dies war insbesondere auf neue KI-gestützte Angriffsinfrastrukturen zurückzuführen, die es Angreifern ermöglichen, Cyberangriffe in bisher ungekannten Mengen und Geschwindigkeiten durchzuführen (vgl. Angriffsinfrastrukturen). Bereits jetzt haben Angreifer ihre Aufklärungstätigkeiten, mit denen sie potenzielle Ziele im Internet auskundschaften und Cyberangriffe vorbereiten, deutlich erhöht (plus 57 %, vgl. Aufklärungstätigkeiten). Hintergrund waren klassische, aus schlecht geschützten Android-Geräten aufgebaute Residential-Proxy-Botnetze, die im aktuellen Berichtszeitraum neue Größenordnungen erreichten. Diese Dynamik dürfte sich erheblich verstärken.

1.1 Angriffsinfrastrukturen

Abbildung 1-1: Gefundene Schwachstellen mit hohem Schweregrad pro Woche
Einheit: Anzahl



Quelle: Anthropic
Bemerkung: https://red.anthropic.com/2026/exploit/

Die Fähigkeiten von LLM (Large Language Models) zur Identifikation von Schwachstellen in einem weit verbreiteten Internetbrowser haben sich im aktuellen Berichtszeitraum erheblich gesteigert. Unter Einsatz eines LLM wurden durchschnittlich acht Schwachstellen mit hohem Schweregrad innerhalb einer Woche gefunden. Zuvor war es durchschnittlich nur eine Schwachstelle pro Woche gewesen (vgl. Abbildung 1-1). Das entsprach einer Leistungssteigerung des LLM von 700 % innerhalb weniger Monate (vgl. Anthropic) und illustriert die zunehmende Leistungsfähigkeit solcher Systeme.

Das getestete LLM war darüber hinaus auch in der Lage, unmittelbar den passenden Exploit zu einer identifizierten Schwachstelle zu liefern. Es ist daher damit zu rechnen, dass es sehr kurzfristig zum Missbrauch solcher hochperformanten Systeme durch Cyberangreifer kommen wird. Der Missbrauch von Tools, die eigentlich der Prävention von Cyberangriffen dienen, ist ein seit langem bekanntes Phänomen. So werden beispielsweise auch Pentesting-Tools regelmäßig für Cyberangriffe missbraucht.

Mit Blick auf die steigende Performanz von LLM-Schwachstellenscannern, die für Cyberangriffe missbraucht werden können, sollten Hersteller von aus dem Internet erreichbaren IT-Produkten ihre Produkte kurzfristig prüfen und härten. Anwender sollten kurzfristig Maßnahmen ergreifen, um ihre externen, aus dem Internet erreichbaren Angriffsflächen durch wirksames Angriffsflächenmanagement zu schützen. Dazu zählt insbesondere die Automatisierung des Patchmanagements, auch unter Einsatz von KI (vgl. Des Weiteren ist das BSI aktiv in der CRA Expert Group vertreten, um zusammen mit seinen Partnerbehörden und Organisationen der europäischen Wirtschaft, Zivilgesellschaft und ausgewählten Expertinnen und Experten Fragestellungen des CRA zu konkretisieren und den CRA weiterzuentwickeln. Mit der aktiven Teilnahme an der Notifying Authorities Group, dem zentralen Koordinierungsgremium der Notifizierenden Behörden, setzt sich das BSI zudem für eine europäisch harmonisierte und qualitativ angemessene Konformitätsbewertungsinfrastruktur für den CRA ein.

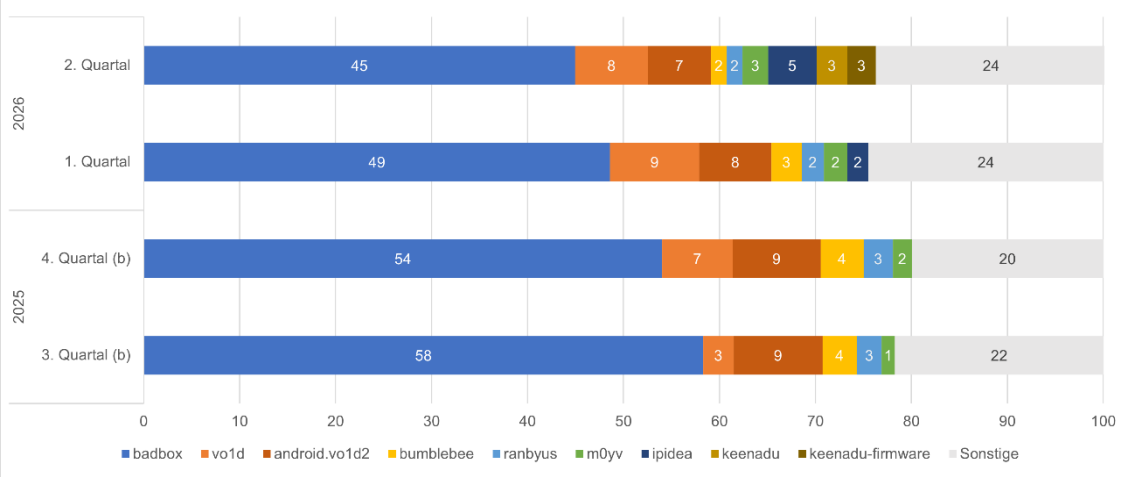
LLMs als Hochgeschwindigkeits-Schwachstellenscanner).

→ Mehr über Angriffsinfrastrukturen

→ Mehr über LLMs zum Schutz externer Angriffsflächen

1.1.1 Botnetze

Abbildung 1-2: Botnetze von Juli 2025 bis Juni 2026 nach Unique IP
Einheit: Anteile in Prozent



Quelle: Botnetz-Monitoring
Bemerkung: Mehrfachnennungen möglich. Wert wurde (b) um Sondereffekte bereinigt.

Mit BadBox und Vo1d führten zwei bekannte IoT-Botnetze die Rangliste der Botnetze an (vgl. auch Infizierte Systeme). Die betroffenen Geräte waren bereits ab Werk mit der Malware infiziert. Mit Aisuru und Kimwolf kamen zwei weitere IoT-Botnetze zum Sinkholing hinzu, die jedoch zahlenmäßig in Deutschland geringer vertreten waren. Mittels Sinkholing leitet das BSI Kontaktversuche infizierter Systeme (Bots) auf sogenannte Sinkhole-Server um, sodass sie von den Command-and-Control-Servern der Angreifer nicht mehr gesteuert werden können (vgl. Sinkholing). Mit dem Cyber Resilience Act hat die EU zudem regulatorische Voraussetzungen für den Schutz jedes digitalen Produkts geschaffen (vgl. Cyber Resilience Act). Das soll der Infizierung von IoT-Geräten vorbeugen.

→ Mehr über Botnetze

Im aktuellen Berichtszeitraum wurden Botnetze insbesondere zur Verbreitung weiterer Schadsoftware, für Betrug im Online-Werbebereich sowie zum Ausspähen sensibler Informationen

eingesetzt. DDoS-Botnetze (Distributed-Denial-of-Service-Botnetze) spielten im Monitoring für Deutschland zwar eine untergeordnete Rolle, dennoch waren Angriffe auf deutsche Ziele zu verzeichnen, etwa durch Netzwerke wie Aisuru oder Kimwolf. Besonders prägend waren die Botnetz-Familien BadBox und Vo1d (im Mittel ca. 5.000 infizierte Systeme), die speziell für IoT-Geräte basierend auf Android – insbesondere TV-Set-Top-Boxen – entwickelt und bereits ab Werk mit der Schadsoftware ausgeliefert wurden.

Die infizierten Geräte bilden dabei sogenannte Proxy-Botnetze. Ähnlich wie bei legitimen Proxy-Diensten wird der Datenverkehr über diese Systeme weitergeleitet, um die eigentliche Herkunft zu verschleiern – allerdings ohne Wissen der Gerätebesitzer. Die Betreiber solcher Botnetze vermieten den Zugriff häufig im Darknet an andere kriminelle Gruppen. Dadurch können unbeteiligte Nutzerinnen und Nutzer mit ihren kompromittierten Geräten unwissentlich in den Fokus von Ermittlungsbehörden geraten.

Das BSI hat auch im aktuellen Berichtszeitraum durch technische Analyse sowie die Umsetzung von Sinkholing-Maßnahmen Takedowns von Botnetzen unterstützt.

BadBox

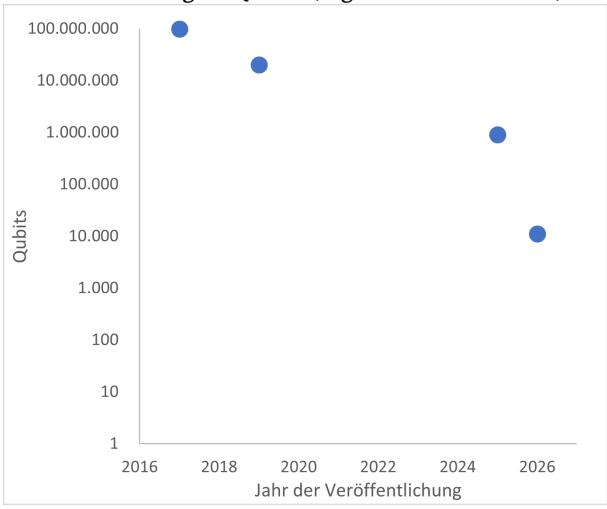
BadBox ist Android-Schadsoftware, die mit der Gerätefirmware ausgeliefert wird. Betroffen sind TV-Boxen, Mediaplayer, digitale Bilderrahmen, Handys und Tablets, die nicht Play-Protect-zertifiziert sind. Infizierte Geräte verbinden sich sofort mit einem Command-and-Control-Server. Damit können Angreifer Einmalcodes für die Zwei-Faktor-Authentisierung abfangen, weitere Schadsoftware nachladen und über das Gerät als Proxy auf das lokale Netzwerk zugreifen.

Vo1d/Android.Vo1d

Die Vo1d-Botnetz-Familie ist Schadsoftware, die Android-TV-Boxen ohne Play-Protect-Zertifizierung betrifft. Sie erlaubt Angreifern, weitere Malware zu installieren. Derzeit werden die infizierten Geräte missbraucht, um ein Proxy-Netzwerk aufzubauen und automatisch Werbung zu klicken (Ad-Fraud). Durch das Proxy-Netzwerk kann sämtliche Netzwerkkommunikation über das befallene Gerät geleitet und kriminelle Aktionen können über die Internetverbindung der Betroffenen durchgeführt werden.

1.1.2 Quantencomputer

Abbildung 1-3: Wissenschaftliche Arbeiten nach benötigter Leistung des Quantencomputers
Einheit: Leistung in Qubits (logarithmische Skala)



Quelle: BSI
Bemerkung: Schätzungen wissenschaftlicher Arbeiten zur benötigten Anzahl an Qubits, um RSA-2048 mittels des Algorithmus von Shor zu brechen

Hinreichend leistungsfähige Quantencomputer können künftig die heute gängigen Verfahren in der Datenverschlüsselung und Authentisierung brechen und stellen daher eine erhebliche Bedrohung für die Vertraulichkeit und Authentizität von Daten dar. Aktuell sind ausreichend leistungsfähige Quantencomputer nicht verfügbar. Jedoch deuten bedeutende Fortschritte auf technischer sowie auf algorithmischer Ebene darauf hin, dass ein solcher Quantencomputer schneller verfügbar sein wird, als man bislang vermutete. (vgl. Abbildung 1-3). Der Umstieg auf quantensichere kryptografische Verfahren ist daher unerlässlich (vgl. Post-Quanten-Kryptografie).

→ Mehr über Quantencomputer

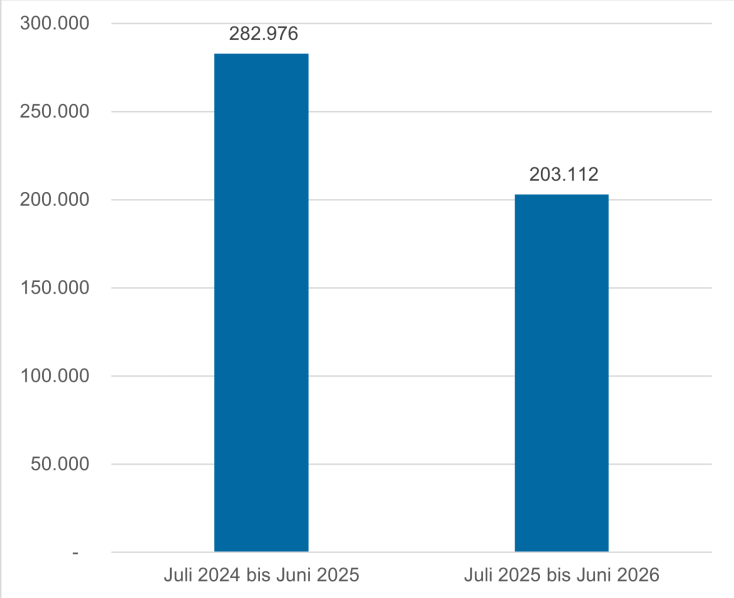
Quantencomputer können künftig die heute verbreitete Public-Key-Kryptografie (zum Beispiel RSA oder Elliptische-Kurven-Kryptografie) brechen und damit zentrale Sicherheitsmechanismen digitaler Infrastrukturen gefährden. Aktuell sind ausreichend leistungsfähige Quantencomputer noch nicht verfügbar. Aufgrund jüngster Fortschritte in der Entwicklung von Quantencomputern sowie auf algorithmischer Seite kommen führende Expertinnen und Experten zu dem Schluss, dass die Bedrohung in den nächsten zehn bis 15 Jahren signifikant steigen wird (siehe hierzu auch die BSI-Studie „Entwicklungsstand Quantencomputer“).

Insbesondere ist in den letzten Jahren die zum Brechen von Kryptografie benötigte Leistungsfähigkeit von Quantencomputern wissenschaftlichen Erkenntnissen zufolge dramatisch gesunken (vgl. Abbildung 1-3). Während 2017 noch rund 100 Millionen physikalische Qubits als erforderlich galten, wurden im aktuellen Berichtszeitraum Berechnungsmodelle vorgestellt, die das Vorhandensein von nur noch rund 11.000 physikalischen Qubits für ausreichend erachten.

Somit ist die Hürde für einen praktisch einsetzbaren Quantenangriff auf aktuell weit verbreitete Verfahren wie RSA-2048 oder ECC-256 heutzutage deutlich niedriger als noch vor wenigen Jahren. Ziele, die lange als „rein theoretisch“ galten, rücken deshalb mehr und mehr in den Bereich des Möglichen. Dadurch steigt die Wahrscheinlichkeit, dass solche Angriffe innerhalb der Lebensdauer von Daten, die heute verschlüsselt und langfristig gespeichert werden, relevant werden könnten. Besonders kritisch ist dies für Daten mit langem Schutzbedarf - „store now, decrypt later“ (SNDL) - sowie für komplexe Systeme wie Public-Key-Infrastrukturen (PKI). So können Angreifer Daten, die sie heute nur verschlüsselt ausleiten können, langfristig speichern und zukünftig mittels Quantencomputer entschlüsseln. Damit könnten sie mit heute verschlüsselten, aber langfristig gespeicherten Daten in Zukunft noch neues Erpressungspotenzial oder Potenzial für weitere Cyberangriffe aufbauen.

1.1.3 Phishing-Websites

Abbildung 1-4: Phishing-Websites weltweit
Einheit: Anzahl



Quelle: Erhebung über die Phishing-Websites

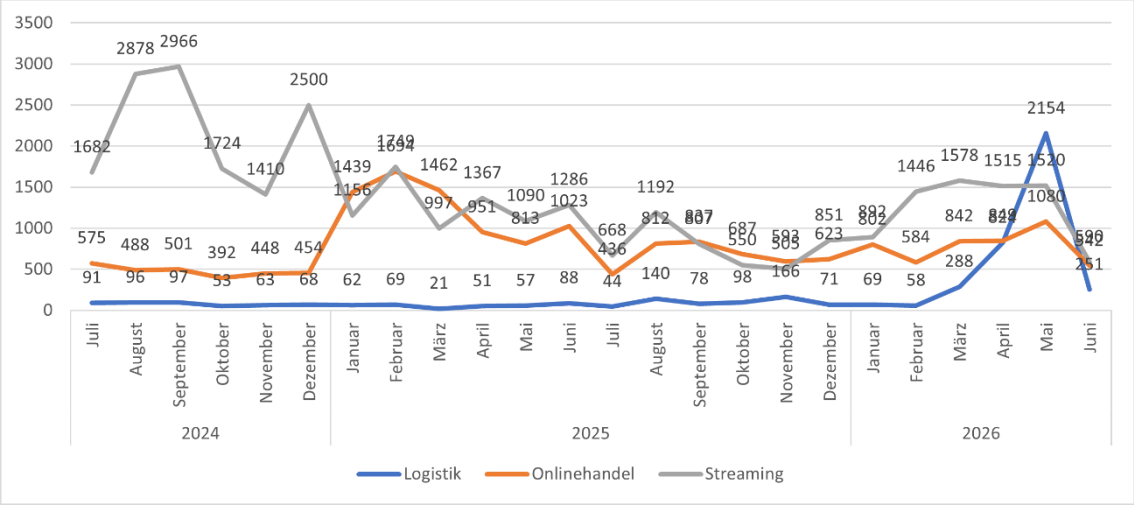
Im aktuellen Berichtszeitraum wurden weltweit 203.112 Phishing-Websites registriert. Das waren 28 % weniger als im vergangenen Berichtszeitraum. Dieser Rückgang kann unter anderem auf erfolgreiche Takedowns (vgl Ausgewählte Vorfälle: Resilienz - Operation Endgame), schnelles und umsichtiges Handeln großer Domain-Provider sowie verbessertes Blacklisting zurückgeführt werden. Darüber hinaus ist auch ein Trend hin zu anderen Phishing-Vektoren zu beobachten, etwa dem „Quishing“ (Einbetten der maliziösen Website in einen QR-Code) oder dem Versand via SMS („Smishing“) oder Messaging-App.

Im Internet verteilte Phishing-Websites ahmen legitime Websites echter Anbieter, etwa aus dem Finanzwesen, nach und dienen dazu, Zugangsdaten und andere personenbezogene Daten abzugreifen. Angreifer platzieren solche Websites und verteilen die Links dazu mit Phishing-Nachrichten mittels E-Mail, Social Media, Instant Messenger und anderer digitaler Kommunikationsformate. Die Phishing-Websites ahmen legitime Websites echter Anbieter, etwa aus dem Finanzwesen nach und dienen dazu, Zugangsdaten und andere personenbezogene Daten abzugreifen. Das BSI unterstützt die Operation Endgame, mit der internationale Strafverfolgungsbehörden unter anderem solche Phishing-Websites vom Netz genommen haben (vgl. Ausgewählte Vorfälle: Resilienz - Operation Endgame)

→ Mehr über Phishing-Hosts

Im Bereich der für Verbraucherinnen und Verbraucher in Deutschland relevanten Phishing-Websites überwogen solche, die Streaming-Dienste nachahmten, mit 12.000 Websites im Berichtszeitraum deutlich vor Onlinehandel-Websites mit 8.700 Phishing-Websites. Verbraucherinnen und Verbrauchern steht eine große Vielfalt an Plattformen und Marken für Onlinestreaming zur Verfügung, welche von namhaften Anbietern bis zu interessengeleiteten Nischenprodukten reicht. Doch durch die wachsende Vielfalt an Produkten, Abo-Modellen und Bezahlmethoden steigt auch die Unübersichtlichkeit für Verbraucherinnen und Verbraucher. Cyberkriminelle nutzen diesen Umstand aus, um täuschend echt wirkende Phishing-Kampagnen unter Missbrauch des Namens der Anbieter umzusetzen.

Abbildung 1-5: Ausgewählte Phishing-Hostnames nach nachgeahmter Branche
Einheit: Anzahl

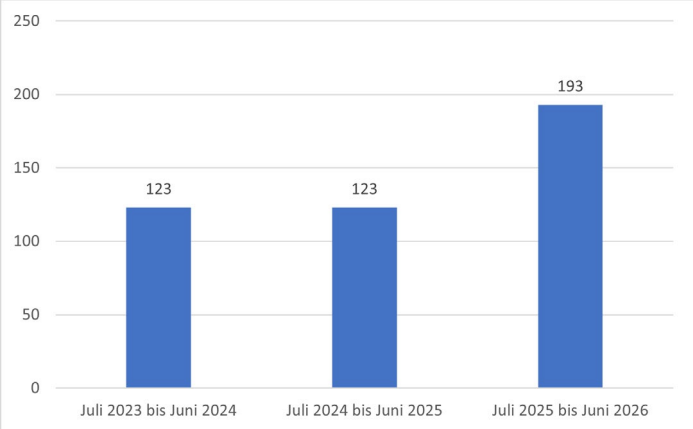


Quelle: Erhebung über die Phishing-Websites

Auffällig war im aktuellen Berichtszeitraum insbesondere die Entwicklung von Phishing-Websites, die Logistik-Dienstleister nachahmten. Innerhalb weniger Monate stieg das Aufkommen solcher Phishing-Websites von durchschnittlich 68 pro Monat auf über 2.100 im Mai 2026. Hintergrund war eine groß angelegte Phishing-Kampagne, mit der Cyberangreifer Websites eines international tätigen Paketdienstleisters imitierten. Verbraucherinnen und Verbraucher erhielten Benachrichtigungen, mit denen sie zur Eingabe von persönlichen Daten aufgefordert wurden, um vermeintliche Sendungen zu erhalten, die bspw. zwischengelagert oder über den Zoll abgewickelt werden sollten. Insgesamt wurden im Berichtszeitraum mehr als 3.000 Phishing-Websites im Rahmen der Kampagne bekannt.

1.2 Angreiferaktivitäten

Abbildung 1-6: Portscans am MADCAT-Honeypot des BSI
Einheit: 2024 = 100 (Messzahl)



Quelle: Portscan-Statistik

Mit Portscans suchen Cyberangreifer nach Schwachstellen in Systemen, die aus dem Internet erreichbar sind. Mit der Ausnutzung von Schwachstellen (Exploitation-Angriffe) haben Angreifer im aktuellen Berichtszeitraum die größte Schadwirkung erzielt (vgl. Lösegelder). Auch wenn Portscans keine Voraussetzung für Exploitation-Angriffe sind, ließen sich gleichwohl auch gesteigerte Portscan-Aktivitäten verzeichnen. Die Messzahl lag mit durchschnittlich 193 Indexpunkten 57 % über dem Vergleichswert des vergangenen Berichtszeitraums (vgl. Abbildung 1-6). Hintergrund des Anstiegs dürften Auswirkungen der allgemeinen Digitalisierung sein, die es Cyberangreifern ermöglicht, Tools, Aufgaben und Prozesse besser zu automatisieren und effizienter zu gestalten.

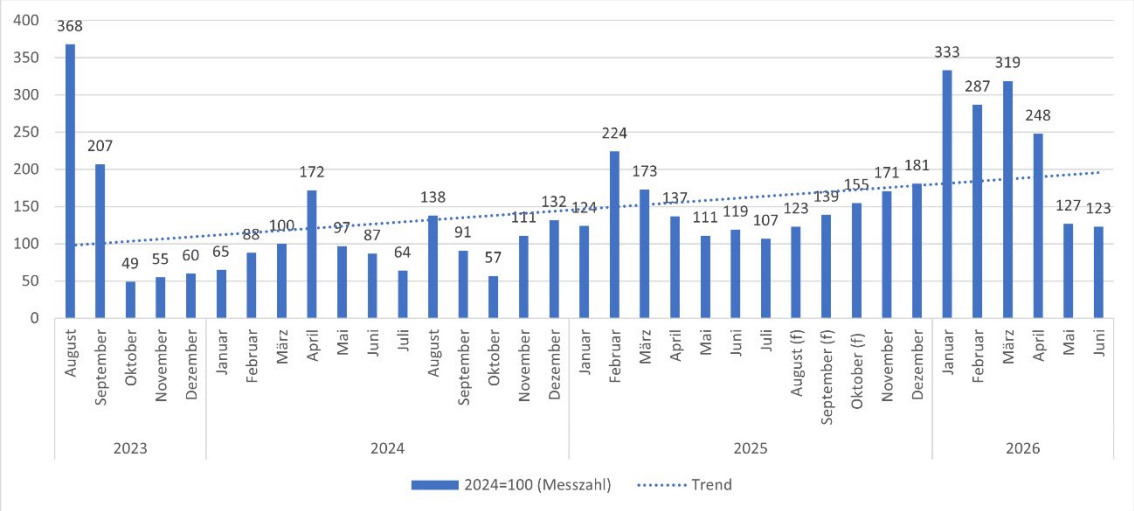
Dazu dürfte auch der Einsatz neuer Angriffsinfrastrukturen wie LLMs bzw. KI-Agentensysteme

das zügige Schließen neuer Schwachstellen beinhaltet. Dabei helfen unter anderem die Informationen, die das BSI mit dem Warn- und Informationsdienst zur Verfügung stellt (vgl. Warn- und Informationsdienst).

→ Mehr über Angreiferaktivitäten

1.2.1 Aufklärungstätigkeiten

Abbildung 1-7: Portscans am MADCAT-Honeypot des BSI
Einheit: 2024 = 100 (Messzahl)



Quelle: Portscan-Statistik
Bemerkung: Sondereffekte im 3. Quartal 2025 bereinigt.

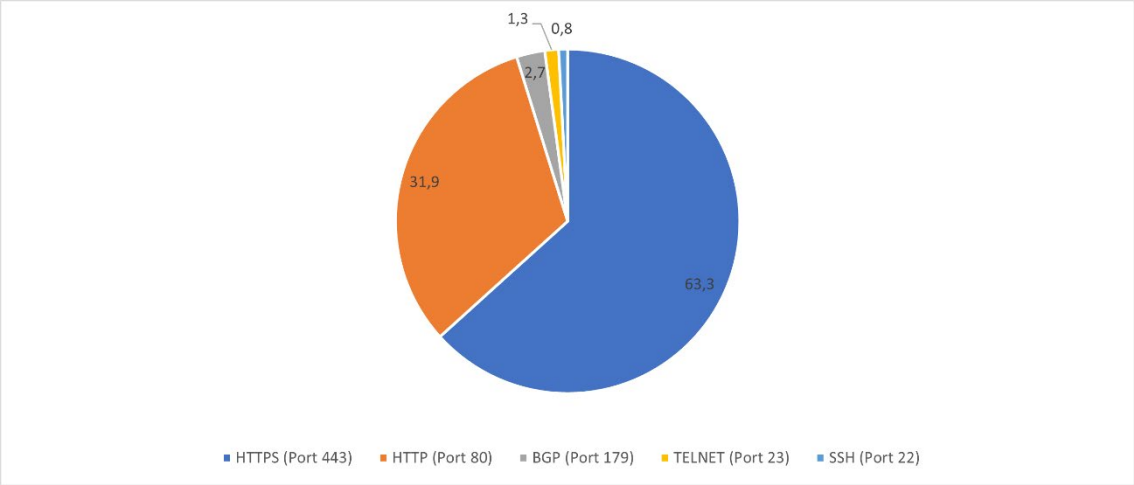
Das Scannen nach offen oder falsch konfigurierten Servern bzw. Schwachstellen in den IT-Systemen der potenziell Betroffenen gehört zu den wesentlichen Aufklärungstätigkeiten, mit denen Angreifer Ziele auskundschaften. Insbesondere nach Bekanntwerden neuer, kritischer Schwachstellen in weitverbreiteten, exponierten Systemen steigen Scans nach Schwachstellen üblicherweise spürbar an (vgl. Time-to-Exploit, Neue Schwachstellen, Exploitation-Angriffe).

Schwachstellen sowie falsch oder mit offenen Ports konfigurierte Server in exponierten, aus dem Internet erreichbaren Systemen stellen eine wesentliche Angriffsfläche dar, die im aktuellen Berichtszeitraum wieder überdurchschnittlich stark bedroht war: die Messzahl über das Aktivitätsniveau der Portscans sprang von durchschnittlich 123 Punkten im vergangenen Berichtszeitraum auf durchschnittlich 193 Punkte. Das war ein Zuwachs um 57 %. Der Warn- und Informationsdienst des BSI informiert über neue Schwachstellen und Advisories zum Schließen von Sicherheitslücken (vgl. Warn- und Informationsdienst). Mit dem CVD-Prozess unterstützt das BSI Hersteller und Entdecker von Schwachstellen bei deren koordinierter Veröffentlichung (vgl. Coordinated Vulnerability Disclosure).

→ Mehr über Aufklärungstätigkeiten

Ports verhalten sich ähnlich wie Postfächer in einem großen Büro, über die je nach Fachgebiet und Zuständigkeit der einzelnen Abteilungen Informationen ausgetauscht werden. Portscans ermöglichen Angreifern zum Beispiel Aufklärung (fachsprachlich: Reconnaissance) darüber, welche Dienste in einem Netzwerk angeboten werden und auf dem Zielsystem zur Verfügung stehen. Dienste sind Aufgaben, die vom IT-System ausgeführt werden, beispielsweise die Dateiübertragung, das Drucken, das Bereitstellen von Websites oder die „Fernsteuerung“ über eine Netzwerkverbindung per Fernzugriff (RDP). Portscans werden daher häufig zum Auskundschaften von IT-Systemen und IT-Netzwerken genutzt.

Abbildung 1-8: Portscans am MADCAT-Honeypot von Juli 2025 bis Juni 2026 nach Ports (Top 5)
Einheit: Anteile in Prozent



Quelle: Portscan-Statistik

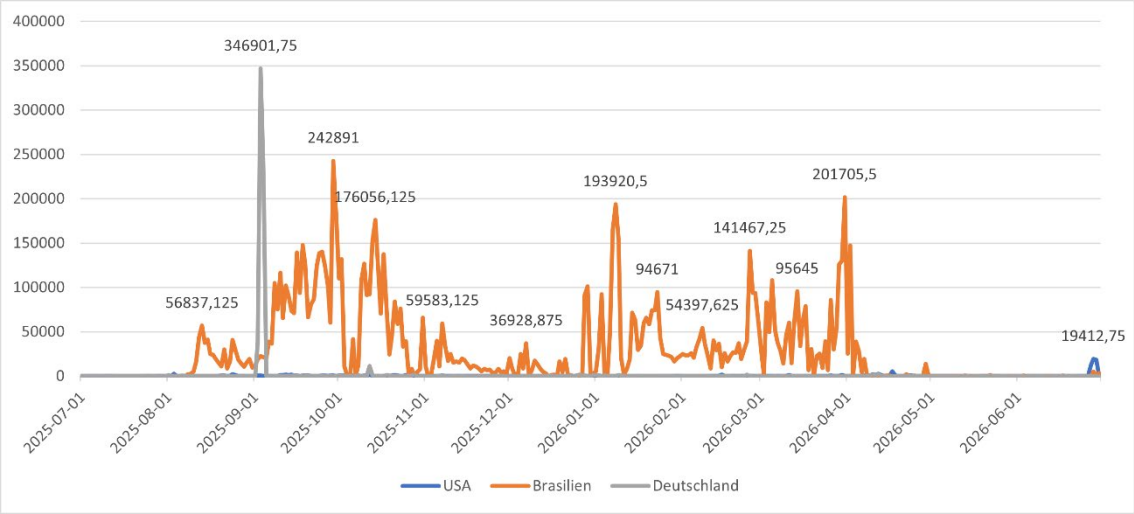
Auf den aktuellen Berichtszeitraum bezogen zeigt sich, wie stark Port 443 (HTTPS) und Port 80 (HTTP) als Ziele von Portscans vertreten sind. Mehr als 60 % der Scans aus den vom BSI aufgezeichneten Top-5-Ports richteten sich gegen Port 443 und nahezu ein weiteres Drittel gegen Port 80 (vgl. Abbildung 1-8). Neben anderen Ports scannen Angreifer diese gleichsam „standardmäßig“ häufig mit, da diese aufgrund ihrer Aufgabe, Websites bereitzustellen, lohnende Ziele darstellen.

Trend an Port 443: Kampagne aus Südamerika

Für den Berichtszeitraum war zeitweise ein sehr starker Anstieg an Scans von Angreifern gegen Port 443 zu beobachten. Port 443 ist der übliche Netzwerk-Port für HTTPS, also für die sichere Datenübertragung zwischen einem Webbrowser und einem Webserver.

Analysten konnten anhand von Informationen wie IP-Adresse, Breiten- und Längengrad sowie ISP (Internetdienstanbieter) die geographische Herkunft ermitteln. Demnach lag der Ursprung der groß angelegten Angriffskampagne mit Schwerpunkt September und Oktober 2025 mit hoher Wahrscheinlichkeit in Brasilien. Die Kampagne hat sich nach einer Pause im November und Dezember und mit Beginn des Jahres 2026 wieder verstärkt, um schließlich Ende des ersten Quartals 2026 abzuflauen. Ursächlich dafür könnten erfolgreiche Mitigationsmaßnahmen seitens der Hersteller und Betreiber der von Angreifern missbrauchten Geräte und von Internetserviceprovidern oder auch ein Ende der Angriffskampagne aufgrund begrenzter Ressourcen auf Angreiferseite gewesen sein.

Abbildung 1-9: Portscans gegen Port 443 am MADCAT-Honeypot nach geographischer Herkunft
Einheit: Anzahl je Sensor



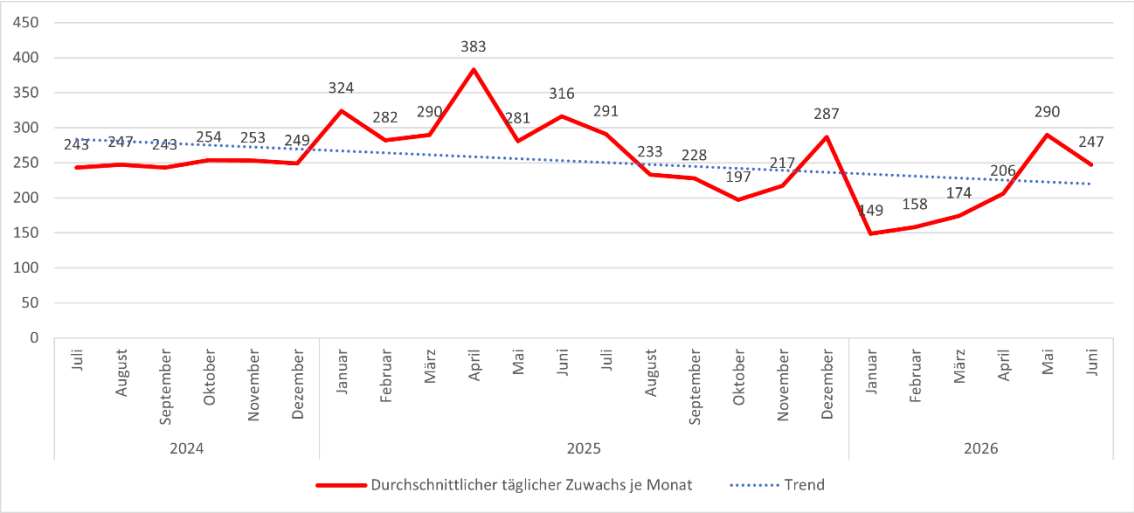
Quelle: Portscan-Statistik
Bemerkung: Auswahl; normiert pro Sensor

Neben den Scans aus Brasilien wurden Anfang Dezember auch kurzzeitig Scans mit Ursprung in Deutschland registriert. Die Quelle der Aktivitäten war hierbei ein in Deutschland registrierter Adressbereich eines Betreibers/Hosters für Gaming-Server mit Sitz in den Niederlanden. Das nur kurze Auftreten von weniger als 48 Stunden spricht für eine schnelle Reaktion und zielgerichtete, verantwortungsbewusste Mitigation (Maßnahmen zur Schadensbegrenzung) des Betreibers selbst.

Die IT-Sicherheitsanalysen der von MADCAT gewonnenen Daten gaben Aufschluss über Verfahren und Angriffsmuster, Angriffstechniken und konkrete Angriffsversuche. Analysen können dabei unterstützen, Massenangriffe im Internet zu detektieren. Ziel ist es, Handlungsbedarf und Handlungsoptionen bei IT-Sicherheitsvorfällen schnell und kompetent einschätzen zu können.

1.2.2 Neue Malware-Varianten

Abbildung 1-10: Durchschnittlicher täglicher Zuwachs neuer Malware-Varianten
Einheit: Anzahl in Tausend



Quelle: Malware-Statistik

Im Berichtszeitraum wurden im Schnitt täglich 223.000 neue Malware-Varianten bekannt. Dies bedeutet einen Rückgang um knapp 20 % gegenüber dem vergangenen Berichtszeitraum, was sich auch in den monatlich aggregierten Zahlen äußert. Ein Grund für den Rückgang dürfte die für

Cyberangreifer zunehmende Attraktivität von Exploitation-Angriffen über Schwachstellen in Web-Angriffsflächen sein. Sie dürften daher weniger Bedarf für neue Malware-Varianten haben. Diese werden zudem vor allem bei Malware-Angriffen per E-Mail verwendet, die an Bedeutung verlieren.

1.3 Angreifergruppen

Abbildung 1-11: Aktive Angreifergruppen am 30.06.2026 weltweit nach Motivation
Einheit: Anzahl



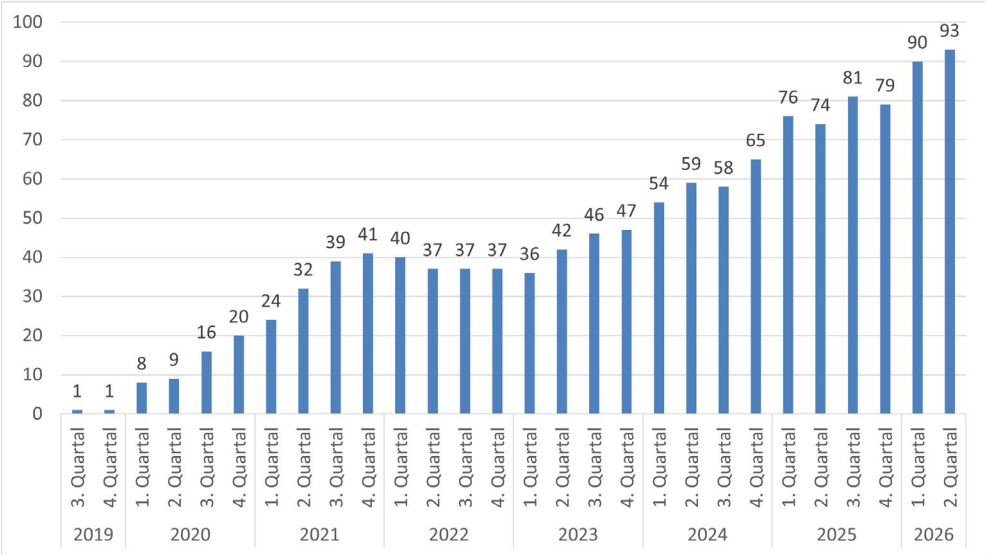
Quelle: Threat-Actors-Statistik

Zum Stichtag 30. Juni 2026 wurden weltweit 86 aktive APT-Gruppen und 68 aktive Cybercrime-Gruppen gezählt (vgl. Abbildung 1-11). APT-Gruppen und Crime-Gruppen verfolgen meist das Ziel, tief in Netzwerke einzudringen und Cyberspionage oder Cybererpressung zu betreiben.

→ Mehr über Angreifergruppen

1.3.1 Cybercrime-Gruppen

Abbildung 1-12: Aktive Leak-Seiten weltweit
Einheit: Anzahl



Quelle: Leak-Geschädigten-Statistik

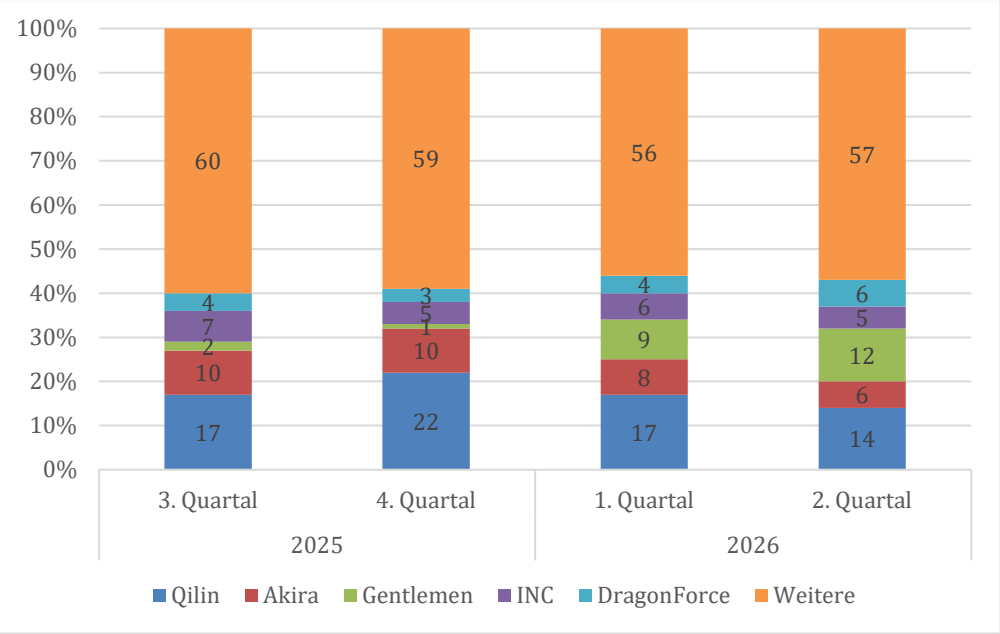
Seit Jahren verlegen sich auch finanziell motivierte, cyberkriminelle Akteure mehr und mehr auf die Ausnutzung von Schwachstellen in Systemen, die aus dem Internet erreichbar sind. Durch Ausnutzung solcher Schwachstellen können Angreifer in interne Netzwerke eindringen, Daten ausleiten und die betroffenen Organisationen unter Androhung der Veröffentlichung von Geschäftsgeheimnissen erpressen. Wer nicht zahlt, dessen Daten werden auf sogenannten Leak-Seiten der Angreifer veröffentlicht. Seit 2019 wurden über 280 verschiedene Leak-Seiten von Cybercrime-Gruppen beobachtet. Im aktuellen Berichtszeitraum erreichte die Zahl der aktiven Leak-Seiten mit weltweit 93 im 2. Quartal 2026 ein neues Allzeithoch (vgl. Abbildung 1-12).

→ Mehr über Cybercrime-Gruppen

Veränderungen in der Cybercrime-Szene

Finanziell motivierte Angreifer gehen weiterhin opportunistisch vor. Die Angriffsfläche und Verwundbarkeit einer Organisation sind dabei maßgeblich für die Zielauswahl. Der Einsatz von Ransomware ist nach wie vor ein bevorzugtes Druckmittel. Mehrere Akteure sind jedoch zu reinen Datendiebstählen mit anschließender Erpressung übergegangen. Im aktuellen Berichtszeitraum waren über 40 % der weltweiten Aktivität auf Leak-Seiten auf die fünf führenden Leak-Seiten Akira, DragonForce, Gentlemen, INC und Qilin zurückzuführen (vgl. Abbildung 1-13).

Abbildung 1-13: Mutmaßlich geschädigte Organisationen weltweit nach Leak-Seite
Einheit: Anteile in Prozent



Quelle: Leak-Geschädigten-Statistik

RaaS INC, Lynx und Sinobi

Die Ransomware-as-a-Services (RaaS) INC, Lynx und Sinobi werden derselben Gruppierung zugeordnet. Diese Gruppe ist seit mindestens 2019 aktiv und veröffentlicht nahezu jährlich eine neue RaaS. Inzwischen betreibt die Gruppe die drei genannten RaaS-Familien parallel.

Im Regelfall betreibt eine Ransomware-Gruppe nur eine einzelne RaaS. In der Vergangenheit war daher mit jeder neuen RaaS-Familie in der Regel ein sofortiger Rückgang an Aktivität bei älteren RaaS zu verzeichnen. Im Gegensatz zu diesem üblichen Vorgehen betreibt die Gruppe seit August 2024 die RaaS INC und Lynx parallel. Zu diesem parallelen Betrieb kam im Juni 2025 Sinobi hinzu. Alle drei RaaS weisen technische Überschneidungen auf.

SafePay

Angriffe mit der Ransomware SafePay fokussieren sich, anders als andere Ransomware-Angriffe, auf Deutschland. (vgl. Leak-Geschädigte). Die mindestens seit November 2024 aktive Betreiber-Gruppe setzt auf Verschlüsselung mit anschließender Erpressung unter Zuhilfenahme zuvor gestohlener Daten. Hierzu kontaktieren die Angreifer Geschädigte auch telefonisch, um psychischen Druck auszuüben.

ClickFix

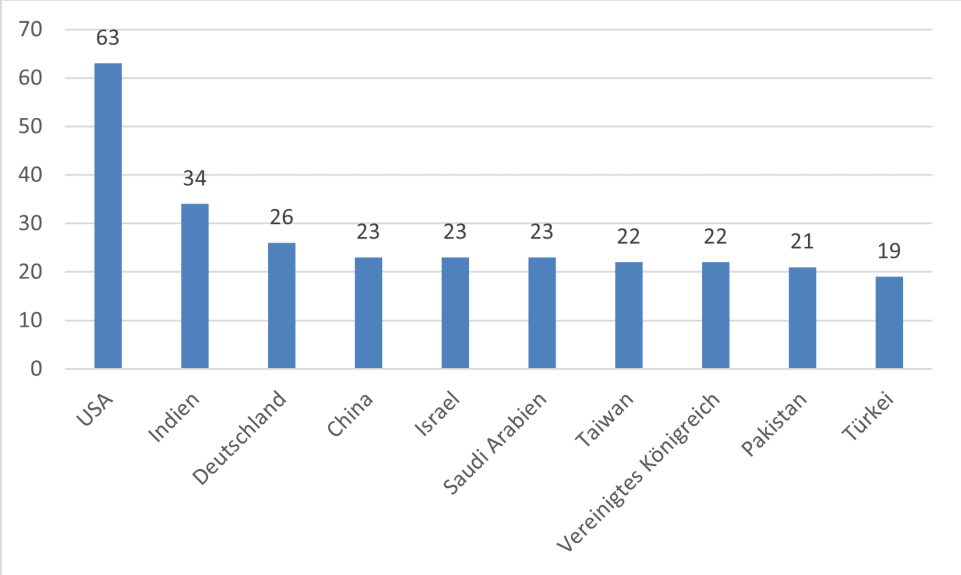
Seit Anfang 2025 erweisen sich maliziöse einzeilige Kommandozeilenbefehle als effektiver Infektionsvektor für Malware wie Infostealer. Hierbei werden Nutzende dazu gebracht, einen maliziösen Befehl eigenhändig auf ihrem System auszuführen. Die Anweisungen zur Selbstinfektion tarnen sich dabei oft als Installationsanleitungen legitimer Software oder als technische Hilfestellungen für allgemeine Computerprobleme. Sie wurden vor allem im Rahmen von Malvertising (d.h. maliziöser Werbung) oder SEO-Poisoning-Kampagnen (d.h. Manipulation von Suchmaschinenergebnissen mit dem Ziel, Nutzende auf maliziöse Websites zu locken) beobachtet. Aufgrund der Ausführung durch die Nutzenden selbst erwies sich die Methode als effektives Mittel zur Umgehung von Detektionssystemen und anderweitigen Sicherheitsvorkehrungen.

Aus dieser allgemeinen Vorgehensweise hat sich eine Variante von Angriffen entwickelt, die sich gefälschte CAPTCHAs zunutze macht. Die Vorgehensweise wurde öffentlich auch als ClickFix und

in einer weiteren Variante als FileFix bekannt. Hierbei werden Betroffene etwa durch manipulierte Suchergebnislisten oder manipulierte Werbeanzeigen auf maliziöse Websites geleitet und dort mit einem CAPTCHA getäuscht. Reagieren Nutzende auf das CAPTCHA und tätigen eine Eingabe, wird ein maliziöser Befehl in die Zwischenablage kopiert. Anschließend werden Nutzende dazu verleitet, den maliziösen Befehl in die Kommandozeile, in den Windows-Dialog „Ausführen" oder bei der Variante FileFix in die Adresszeile des Windows Explorers einzufügen und auszuführen. Varianten dieser Angriffe wurden für alle Betriebssysteme beobachtet, wenngleich der Fokus auf Windows-Systemen liegt.

1.3.2 APT-Gruppen, Cyberconflict

Abbildung 1-14: Aktive APT-Gruppen am 30.06.2026 nach Zielland
Einheit: Anteile in Prozent



Quelle: Threat-Actors-Statistik
Bemerkung: Änderung der Methodik zu dem letzten Berichtszeitraum, Mehrfachnennungen möglich.

APT-Gruppen agieren strategisch und langfristig, sowohl bei der Zielauswahl als auch beim Vorgehen in konkreten Angriffen. Daher ist die Zahl der in den jeweiligen Zielländern aktiven APT-Gruppen im Vergleich zum vergangenen Berichtszeitraum kaum verändert. Grundsätzlich sagt die Zahl der aktiven Gruppen zudem nur wenig über das Ausmaß an Aktivitäten aus. So sind beispielsweise einzelne Gruppen mit nur wenigen Angriffen aufgefallen. Alles in allem ist daher trotz der hohen Gruppenanzahl keine substanzielle Zunahme an APT-Aktivitäten gegen Deutschland zu beobachten. Die USA blieben im aktuellen Berichtszeitraum weiterhin politisch, wirtschaftlich und militärisch ein relevanter Akteur und waren damit ein Spionage-Ziel für 63 % der APT-Gruppen (Abbildung 1-14). Ziele in Deutschland haben im Berichtszeitraum Aktivitäten von 26 % der APT-Gruppen auf sich gezogen. Die Liste der in Deutschland aktiven APT-Gruppen veröffentlicht das BSI auf seiner Website.

→ Mehr über APT-Gruppen

Die Aktivität von APT-Gruppen folgte auch im aktuellen Berichtszeitraum geopolitischen Spannungen. Neben nordkoreanisch und chinesisch attribuierten APT-Gruppen waren in Deutschland wie in den vergangenen Berichtszeiträumen Cyberspionage-Gruppen tätig, die IT-Sicherheitsexperten Russland zuordnen. Diese Gruppen fallen seit Jahren mit Cyberspionage gegen den politischen und vorpolitischen Raum auf (vgl. Ausgewählte Vorfälle: Gefährdungslage: Cyberspionage-Angriffe auf Ziele im politischen und vorpolitischen Raum). Ihr Anteil lag im aktuellen Berichtszeitraum bei 23 % der in Deutschland aktiven APT-Gruppen (vgl. Abbildung 1-15).

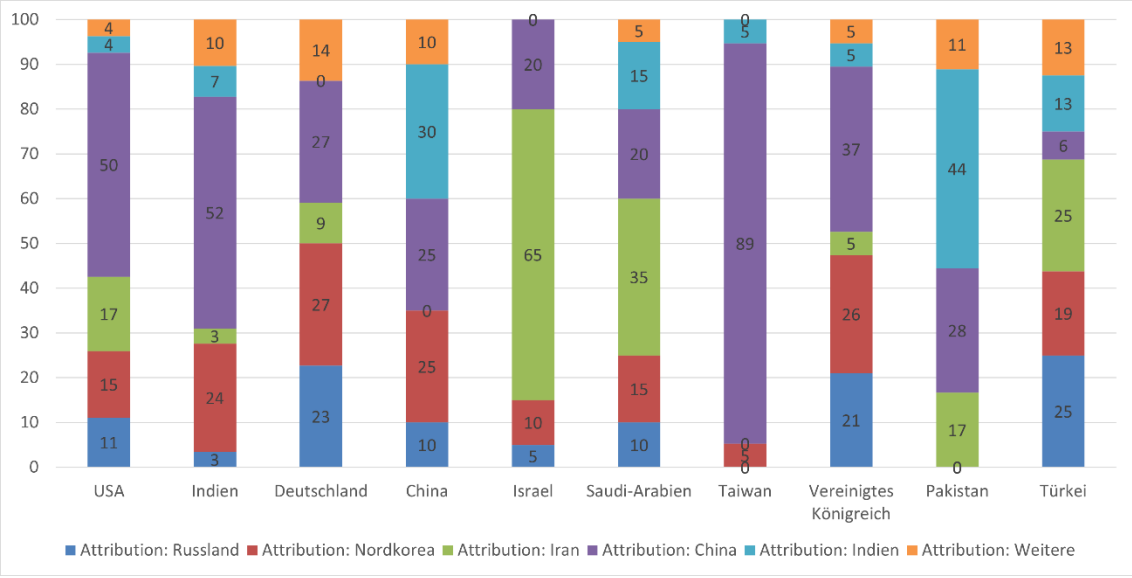
Ähnlich hoch war der Anteil russisch attribuierter Gruppen nur in der Türkei (25 %) und Großbritannien (21 %).

Während es im vergangenen Berichtszeitraum noch Anzeichen für mögliches Prepositioning in Deutschland gab, war die beobachtete Aktivität im aktuellen Berichtszeitraum vor allem auf Cyberspionage zurückzuführen. Prepositioning bezeichnet das vorsorgliche Platzieren von Schadprogrammen in kritischen Netzen, um im Konfliktfall schnell Sabotage betreiben zu können. Cyberspionage dagegen zielt hauptsächlich auf Informationsbeschaffung.

Von den in Deutschland aktiven APT-Gruppen ordneten IT-Sicherheitsexperten 27 % Nordkorea zu. Nordkoreanische Gruppen werden staatlich gesteuert wie Cyberspionage-Gruppen anderer Länder, ihre Angriffe dienen in der Regel jedoch neben der Informationsbeschaffung vor allem auch der Beschaffung von Devisen für das nordkoreanische Regime. Weitere 27 % der APT-Gruppen, die im aktuellen Berichtszeitraum in Deutschland aktiv waren, wurden von IT-Sicherheitsexperten China zugeordnet, wobei ein hohes Dunkelfeld nicht auszuschließen ist. Die chinesische Vorgehensweise, aus Verschleierungsnetzen heraus verwundbare Perimeter-Systeme zu kompromittieren, ist schwer detektierbar und auch schwer einer Gruppe zuzuordnen. Solche Angriffsvektoren sind weltweit zu beobachten (vgl. beispielsweise Exploitation-Angriffe, Die Lage der IT-Sicherheit in Deutschland 2025) und gehören auch für Deutschland seit Jahren zur Bedrohungslage. Trotz der militärischen Eskalation im Nahen und Mittleren Osten in der zweiten Hälfte des aktuellen Berichtszeitraums gab es in Deutschland nur punktuelle Aktivitäten von APT-Gruppen, die von IT-Sicherheitsexperten als mutmaßlich iranisch bewertet werden. Diese haben im Berichtszeitraum Personen in Deutschland ausgespäht, die vom iranischen Regime als Gegner wahrgenommen werden. Im Zielspektrum dieser APT-Gruppen stehen iranischstämmige Oppositionelle, Regimekritiker, Journalisten und Personen aus der Menschenrechtsbewegung sowie Frauenrechtsaktivistinnen. Da sich iranisch attribuierte Cyberoperationen vor allem gegen private Endgeräte und Online-Konten richten, ist von einer hohen Dunkelziffer in Deutschland auszugehen. 9 % der in Deutschland aktiven APT-Gruppen wurden dem Iran zugeordnet.

Außerhalb Deutschlands war der Anteil von APT-Akteuren, die IT-Sicherheitsexperten als mutmaßlich durch den Iran gesteuert bewerten, mit 65 % in Israel am höchsten. Auch in Saudi-Arabien (35 %) war der Anteil dem Iran zugeordneter APT-Gruppen am höchsten. Die gegen Taiwan agierenden Akteure wurden dagegen zu 89 % China zugeordnet. Auch in Indien (52 %) und den USA (50 %) war der Anteil der zu China zugeordneten Cyberspionage-Gruppen vergleichsweise hoch (vgl. APT-Gruppen nach Zielland und Attribution).

Abbildung 1-15: APT-Gruppen nach Zielland und Attribution
Einheit: Anteile in Prozent



Quelle: Threat-Actors-Statistik
Bemerkung: Aktive APT-Gruppen, Mehrfachnennungen möglich.

1.4 Hybride Bedrohungen



Deutschland steht im Fokus hybrider Bedrohungen durch fremde Staaten, die sich durch Cyberoperationen, Desinformationskampagnen sowie Spionage- und Sabotageoperationen insbesondere gegen Regierungseinrichtungen und Kritische Infrastruktur äußern.

Die zunehmende Digitalisierung erhöht die Angriffsfläche Deutschlands im Cyberraum und führt in Kombination mit geopolitischen Spannungen dazu, dass Cyberoperationen fester Bestandteil multidimensionaler geopolitischer Konfliktführung geworden sind.

Die Komplexität hybrider Bedrohungen sowie die zunehmende Digitalisierung der Gesellschaft erfordern ein ganzheitliches und koordiniertes Vorgehen auf nationaler Ebene. Die Bündelung von Cyberschutzaktivitäten als Bausteine des Cyberdome, die Teilnahme im GAZ Hybrid sowie die geplante Übernahme der technischen Analyse für die Zentrale zur Erkennung ausländischer Informationsmanipulation (ZEAM) durch das BSI belegen, dass das BSI ein wichtiger Bestandteil einer souveränen, resilienten und zukunftsorientierten Sicherheitsarchitektur ist (vgl. „Digitale Souveränität“ beschreibt die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können. Im aktuellen Berichtszeitraum sind die politischen und wirtschaftlichen Unsicherheiten in der EU aufgrund geopolitischer und geoökonomischer Spannungen gewachsen. Gleichzeitig ist die digitale Sphäre, die permanent Cyberangriffen ausgesetzt ist, als eigenständige Dimension im Rahmen dieser Spannungen in den Vordergrund getreten. Immer mehr IT-Produkte bilden Angriffsflächen und bergen Risiken. Digitale Abhängigkeiten von außereuropäischen Anbietern, die Deutschland verwundbar machen und seine Handlungsfähigkeit einschränken können, betreffen insbesondere Alltagsthemen wie Mobilfunk, die Energiewende sowie eine Vielzahl digitaler Produkte und Dienste wie Betriebssysteme mobiler Endgeräte oder Social-Media-Angebote. Zudem besteht dringender Bedarf die digitale Souveränität im europäischen Finanzsektor herzustellen.

Um mit digitalen Innovationen Schritt zu halten und dabei digitale Souveränität zu erlangen, ist eine Doppelstrategie zielführend: Zum einen müssen der europäische Markt und die deutsche Digitalindustrie mit dem Ziel technischer und wirtschaftlicher Konkurrenzfähigkeit in ausgewählten Technologiefeldern gestärkt werden. Des Weiteren müssen außereuropäische Produkte mit Hilfe technischer Kontrollschichten so abgesichert werden, dass eine selbstbestimmte Nutzung ohne potentielle Einflussnahme Dritter möglich wird.

Um den Einsatz digitaler Produkte und Services „made in Europe“ zu stärken, setzt das BSI unter anderem auf Public-Private-Partnerships. So haben das BSI und der Hosting- und Cloud-Anbieter IONOS im Januar 2026 eine strategische Kooperation geschlossen. IONOS unterstützt in Abstimmung mit dem BSI die Bundesverwaltung beim Aufbau einer Private-Enterprise-Cloud-Umgebung sowie bei der Fortentwicklung kryptographischer Verfahren. Zudem wurde im Februar

2026 eine Zusammenarbeit zwischen dem BSI und Schwarz Digits (IT-Sparte der Schwarz Gruppe) vereinbart. Ziel ist unter anderem die gemeinsame Entwicklung souveräner Cloud-Lösungen, die auch für den Einsatz in der Bundesverwaltung und in den Landesverwaltungen nutzbar gemacht werden können.

Mit den C3A - Criteria enabling Cloud Computing Autonomy hat das BSI im März 2026 eine richtungsweisende Handreichung vorgelegt, die die Souveränitätseigenschaften von Cloud-Diensten transparent macht. Während die Sicherheitseigenschaften von Cloud-Diensten im Cloud Computing Compliance Criteria Catalogue (C5) des BSI adressiert werden, ermöglicht der Kriterienkatalog C3A eine Bewertung, ob ein Cloud-Angebot im Risikokontext des Anwendungszwecks selbstbestimmt genutzt werden kann. Die C3A dienen dabei als Kriterienkatalog, sie schaffen Transparenz und Orientierung, entfalten jedoch keine regulative Wirkung. Die C3A können sowohl von Cloud-Anbietern als auch von Cloud-Kunden genutzt werden. Cloud-Anbieter können die Einhaltung der Kriterien durch ein Audit nachweisen. Cloud-Kunden können das Framework nutzen, um für das eigene Nutzungsszenario relevante Anforderungen zu identifizieren.

Künstliche Intelligenz (KI) hat sich zu einer strategischen Basistechnologie mit unmittelbaren Auswirkungen auf nationale Sicherheit, staatliche Handlungsfähigkeit, wirtschaftliche Wettbewerbsfähigkeit und gesellschaftliche Stabilität entwickelt: Hochleistungsfähige KI-Modelle verfügen über erhebliche Fähigkeiten in den Bereichen Cyberoperationen, Softwareentwicklung, Automatisierung komplexer Entscheidungsprozesse sowie Wissens- und Informationsverarbeitung. Deutschland benötigt eine dauerhaft leistungsfähige institutionelle Struktur zur technischen Evaluierung und sicherheitspolitischen Einordnung solcher Systeme. Dem trägt die Bundesregierung mit dem neu gegründeten AI Safety and Security Institute Deutschland (AISI Deutschland).

Digitale Souveränität bedeutet, Optionen zu schaffen: Je mehr vertrauenswürdige Produkte verfügbar sind, desto souveräner kann entschieden werden und desto sicherer wird die digitale Zukunft.

Cyberdome sowie Digitale Souveränität).

→ Mehr über hybride Bedrohungen

Unter hybriden Bedrohungen versteht man Aktivitäten fremder Staaten (staatliche oder staatlich gelenkte Akteure), die durch den koordinierten Einsatz verschiedener Instrumente versuchen, illegitimen Einfluss auf die Interessen der Bundesrepublik Deutschland auszuüben. Ein zentrales Mittel hierbei sind Einflussoperationen, deren Ziel es insbesondere ist, deutschen Sicherheitsinteressen zu schaden, die freie Meinungs- und Willensbildung zu beeinträchtigen, Vertrauen in staatliche Institutionen und den gesellschaftlichen Zusammenhalt zu untergraben.

Hierbei können Cyberangriffe, Desinformation, Einflussnahme auf Protestgeschehen oder Spionage und Sabotage zum Einsatz kommen. Die Art der Mittel ist dabei nachrangig, entscheidend ist der schädigende Zweck. Zudem können auch ganz unterschiedliche politische, gesellschaftliche und fachliche Bereiche betroffen sein, die allesamt in hohem und zunehmendem Maße von Informationstechnik abhängen.

Als nationale Cyber- und Informationssicherheitsbehörde setzt das BSI seine Tätigkeitsschwerpunkte im Kontext hybrider Bedrohungen auf die Prävention und Detektion von Angriffen auf die Informationstechnik sowie die Reaktion darauf. Das BSI arbeitet hierbei eng mit nationalen und internationalen Partnern zusammen und ist eng in die Abwehrstrukturen der Bundesregierung eingebunden. So ist das BSI im Gemeinsamen Zentrum zur Abwehr hybrider Bedrohungen (GAZ Hybrid) vertreten, welches am 16. Juni 2026 als operative Informations- und Kooperationsplattform eröffnet wurde. Das GAZ Hybrid dient einem schnellen, effektiven Informationsaustausch und einer intensiven Zusammenarbeit zwischen Bundes- und Landesbehörden im Bereich hybrider Bedrohungen und soll zur Koordinierung der (operativen) Abwehrmaßnahmen beitragen. Ziel ist es, hier Synergien zur Bewältigung hybrider Bedrohungen

bestmöglich zu nutzen und dadurch parallele Zuständigkeiten und Doppelstrukturen zu vermeiden. Dazu fließen über die jeweils teilnehmenden Behörden in das GAZ Hybrid auch Erkenntnisse aus Fachzentren ein, die auf Tatmittel oder Operationsraum spezialisiert sind – etwa das Cyber-AZ und das Gemeinsame Drohnenabwehrzentrum (GDAZ).

Schwerpunkt Cyberoperationen

Staatliche oder staatlich gestützte Cybergruppierungen priorisieren Ziele mit politischem, regierungsnahem oder verteidigungsrelevantem Fokus für langfristig angelegte Cyberspionage. Andere Formen von Cyberoperationen stellen ebenfalls ein hohes Risiko dar. Angriffe auf die Verfügbarkeit von IT-Systemen, beispielsweise Überlastungs- oder Ransomware-Angriffe, werden zu hybriden Zwecken genutzt. In diesem Kontext fand beispielsweise im Februar 2026 ein Überlastungsangriff gegen die Buchungssysteme der Deutschen Bahn statt, welcher zu Ausfällen der Buchungssysteme führte.

Des Weiteren konnten im aktuellen Berichtszeitraum konkrete Cyberoperationen gegen politisch relevante Ziele in Deutschland festgestellt werden. Einige dieser Angriffe, beispielsweise Phishing-Angriffe, eignen sich als Vorbereitungshandlung für nachgelagerte Spionage- oder Informationsoperationen. Andere Angriffe zielten direkt auf die Infiltration sensibler Systeme zu Spionagezwecken ab – etwa mittels Exploitation- oder Supply-Chain-Angriffen. Das BSI unterstützt Betroffene dabei, sich gegen diese Angriffe zu schützen, und hilft darüber hinaus auch bei sicherheitstechnischen Fragestellungen im Nachgang eines Angriffes. Ferner arbeitet das BSI eng mit anderen Sicherheitsbehörden zusammen, beispielsweise im Nationalen Cyber-Abwehrzentrum sowie im neu gegründeten Gemeinsamen Zentrum zur Abwehr hybrider Bedrohungen (GAZ Hybrid), um den Wissens- und Informationsaustausch bestmöglich umzusetzen.

Schwerpunkt Einflussoperationen

Einflussoperationen bezeichnen koordinierte Maßnahmen, um Desinformation oder manipulierte Informationen zu verbreiten. Häufig werden die Fehlinformationen über digitale Kanäle, beispielsweise Social Media, verbreitet und multipliziert. Durch die steigende Verfügbarkeit leistungsfähiger KI-Modelle können manipulierte Informationen ohne besondere Vorkenntnisse erstellt werden. Dies äußert sich insbesondere in der steigenden Anzahl sogenannter Deepfakes und täuschender Kopien seriöser Nachrichten-Websites wie beispielsweise im Rahmen der „Doppelgänger"-Kampagne, einer seit 2022 aktiven russischen Desinformationskampagne, die gefälschte Webseiten, beispielsweise von Spiegel, Stern oder FAZ, aber auch nachgebaute Behördenseiten nutzt.

Das BSI unterstützt die für die Abwehr hybrider Bedrohungen zuständigen Behörden mit technischer Expertise. So hilft das BSI bei der technischen Detektion von Infrastrukturen, Mustern oder anderen relevanten Informationen und teilt diese Erkenntnisse mit nationalen Partnern. Darüber hinaus entwickelt das BSI eigene Methoden, um KI im Rahmen der Softwareprüfung und Cyberabwehr nutzbringend einzusetzen, und setzt sich als Zertifizierungsbehörde für sinnvolle Standards und den sicheren Einsatz neuer Technologien ein.

Ausgewählte Vorfälle: Bedrohungslage
Schwachstellenscanner Trivy durch Supply-Chain-Angriff kompromittiert

Sachverhalt

Der Open-Source-Schwachstellenscanner Trivy von Aqua Security war im März 2026 von einem Supply-Chain-Angriff betroffen, der durch die unvollständige Eindämmung eines früheren Vorfalls ermöglicht wurde. Trivy ist ein Scanner, der unter anderem Container und Programmbibliotheken auf Schwachstellen sowie darin enthaltene Zugangsdaten untersucht. Der Angreifer kompromittierte das Repository des Herstellers, um neue, mit Schadcode erweiterte Trivy-Versionen zu verbreiten. Die Malware in den kompromittierten Trivy-Versionen zielte darauf ab, Zugangsdaten und weitere schützenswerte Informationen von den Nutzenden des Schwachstellenscanners Trivy zu stehlen. Die Schadsoftware versuchte unter anderem, SSH-Schlüssel, Zugangsdaten für Cloud-Dienstleister, Datenbank-, Git- und Docker-Konfigurationen, Kubernetes-Token oder Krypto-Währung-Wallets auszuleiten. Die abgeflossenen Daten könnten zukünftig von den Angreifern genutzt werden, um unter anderem Malware in andere Repositories

bzw. Umgebungen einzuschleusen. Im Zuge des Vorfalls wurde die Schwachstelle mit der Kennung CVE-2026-33634 erfasst, um betroffene Produkte im Rahmen des Supply-Chain-Angriffs verfolgen zu können. Die Verwundbarkeit wurde nach dem Common Vulnerability Scoring System (CVSS), einem international gültigen Industriestandard zur Bewertung des Schweregrads von Schwachstellen, mit 9.4 von 10 als „kritisch" eingeschätzt. Die Kompromittierung von Trivy betraf nach Herstellerangaben nur Open-Source-Komponenten und nicht die kommerziellen Produkte des Herstellers. Der Supply-Chain-Angriff auf Trivy reiht sich in eine monatelange Supply-Chain-Kampagne ein, die Medienberichten zufolge der Gruppe TeamPCP zugeschrieben wird. Von der Kampagne sind inzwischen mehrere Software-Ökosysteme betroffen.

Bewertung

Angriffe auf die Supply-Chain führen regelmäßig zu Gefährdungen bzw. Kompromittierungen verschiedener Anwendungen. Die Möglichkeit für Angreifer, durch die Manipulation von Paketen und Bibliotheken in eine Vielzahl an IT-Systemen einzudringen, macht diese Angriffe zu einer attraktiven Strategie. Gleichzeitig verhindert die häufig vorherrschende Unklarheit bei den Geschädigten darüber, welche Drittanbieter-Komponenten in den eingesetzten IT-Produkten integriert sind, dass die geeigneten Schutzmaßnahmen getroffen werden, sobald Kompromittierungen von Paketen und Bibliotheken bekannt werden.

Die Gruppe TeamPCP (aka White Dev 258, PCP) ist erstmals im Dezember 2025 mit einer Angriffskampagne aufgefallen. Damals behauptete der Akteur, tausende Server mit einem Exploit kompromittiert zu haben. Auch bot der Akteur dabei gestohlene Daten zum Verkauf an. TeamPCP tritt als Angreifergruppe und als Betreibergruppe der RaaS CipherForce auf. Dabei betreibt der Akteur auch einen Telegram-Kanal, über den Affiliates angeworben werden. TeamPCP zeichnete sich bislang durch eine hohe Anpassungsfähigkeit aus. So nutzte der Akteur im Rahmen der Supply-Chain-Angriffe gewonnene Zugangsdaten in kurzer Abfolge aus, um weitere Projekte zu kompromittieren. Dabei dehnte der Akteur die Angriffe auch in wenigen Tagen von Linux- auf Windows-Systeme aus und wies ein tieferes Verständnis von Cloud-Infrastruktur auf.

Supply-Chain-Angriffe von TeamPCP zu Beginn des Jahres 2026 im vergangenen Jahr deuten auf einen Trend hin: Angreifer beschränken sich bei Supply-Chain-Angriffen auf Open-Source-Software nicht mehr auf einzelne Projekte. Gerade bei Open-Source-Software, die in der Softwareentwicklung eingesetzt oder in andere Projekte eingebunden wird, sind häufig zahlreiche Betroffene zu verzeichnen.

Reaktion

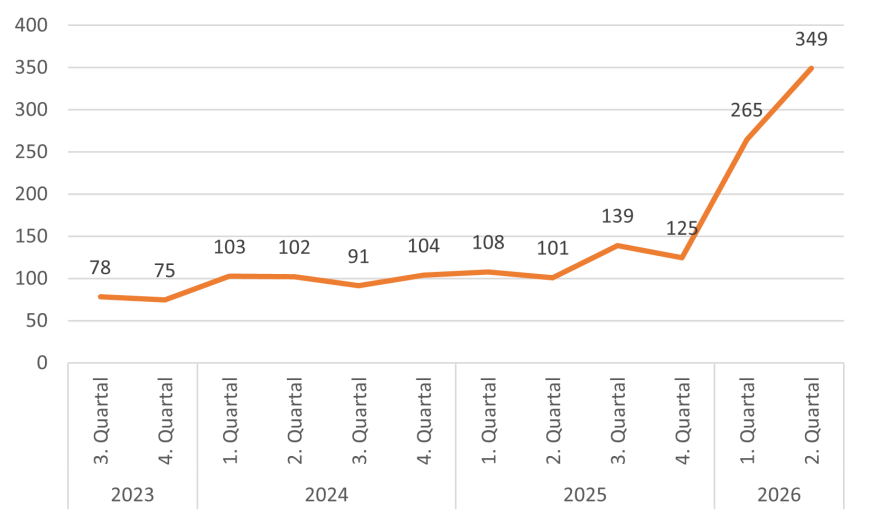
Eine nachhaltige Mitigationsmaßnahme stellte das Aktualisieren auf eine sichere Version dar. Das BSI veröffentlichte eine IT-Sicherheitsinformation zum Vorfall mit weiteren Maßnahmen und Empfehlungen. Demnach war zu prüfen, ob Trivy v0.69.4 oder andere kompromittierte Pakete ausgeführt worden waren. Die damit in Verbindung stehenden Zugangsdaten waren zu wechseln und betroffene Programmdateien zu entfernen. Eine Liste mit IoCs, das heißt Indikatoren, die auf eine Kompromittierung hindeuten, war auf socket.dev verfügbar. Grundsätzliche Maßnahmen zur Absicherung eigener Entwicklungsumgebungen und IT-Systeme waren zudem notwendig.

2 Angriffsfläche

Zur Angriffsfläche zählen alle IT-Systeme, Komponenten und Dienste, die ein Angreifer für einen Cyberangriff ausnutzen oder missbrauchen könnte. Das umfasst zunächst alle IT-Produkte und IT-Infrastrukturen, unabhängig von etwaigen akuten Verwundbarkeiten, aber auch Schwachstellen sowie organisatorische oder menschliche Schwächen. Die größten Angriffsflächen im Cyberraum findet der Angreifer in Form von Domains und URLs (vgl. Angriffe auf Web-Angriffsflächen) sowie von E-Mail-Adressen, Messenger- und Social-Media-Accounts (vgl. Digitale Kommunikationswege) vor. Seit Jahren bieten auch vernetzte Geräte wie Smart-Home-Geräte oder die Telematikinfrastruktur des deutschen Gesundheitswesens immer mehr Angriffsflächen für Cyberangriffe, die Schwachstellen in IP-basierter Kommunikation ausnutzen (vgl. Vernetzte Geräte). Im aktuellen Berichtszeitraum war das Wachstum verwundbarer Angriffsflächen insbesondere auf den starken Anstieg neu bekannt gewordener Schwachstellen (vgl. Neue Schwachstellen), darunter insbesondere neu bekannt gewordener Hardware-Schwachstellen (vgl. Hardware-Schwachstellen) zurückzuführen. KI-Agenten fanden zahlreiche neue Schwachstellen innerhalb kürzester Zeit (vgl. Angriffsinfrastrukturen).

2.1 Attack Surface Score

Abbildung 2-1: Attack Surface Score
Einheit: 2024 = 100 (Messzahl)



Quelle: BSI

Der Attack Surface Score ist eine normierte Kennzahl über verschiedene Angriffsflächen in Deutschland. Neben der allgemeinen Digitalisierung werden insbesondere Schwachstellen, deren Schweregrade und Schadenspotenziale berücksichtigt.

Vor dem Hintergrund neuer KI-Angriffsinfrastrukturen, die Schwachstellen in aus dem Internet erreichbaren Systemen in kürzester Zeit finden (vgl. Angriffsinfrastrukturen), ist die Verwundbarkeit der Angriffsfläche auch in Deutschland im aktuellen Berichtszeitraum signifikant gestiegen. Im 2. Quartal 2026 kletterte der Attack Surface Score auf 349 Punkte und lag damit 3,5-mal so hoch wie im Referenzjahr 2024 (vgl. Abbildung 2-1).

2.2 Time-to-Exploit

Abbildung 2-2: Time-to-Exploit
Einheit: Anzahl Tage



Quelle: Schwachstellenstatistik
Bemerkung: Erstellt am 30. Juni 2026.

Die Time-to-Exploit (TTE) misst, wie viel Zeit Angreifer nach der Veröffentlichung einer Schwachstelle benötigen, um funktionsfähigen Schadcode (Exploit) zu entwickeln und einzusetzen. Dieses Zeitfenster wird kontinuierlich kleiner: Im vergangenen Berichtszeitraum betrug die durchschnittliche TTE noch 53 Tage, im aktuellen Berichtszeitraum durchschnittlich noch 25 Tage mit fallendem Trend: Im 2. Quartal 2026 fiel sie auf nur noch 8 Tage.

Ursprünglich war die Entwicklung verlässlicher Exploits ein langer handwerklicher Prozess von Spezialisten. Inzwischen stellen Angreifer fast augenblicklich Exploits bereit, sobald eine Schwachstelle erfolgreich automatisiert analysiert wurde.

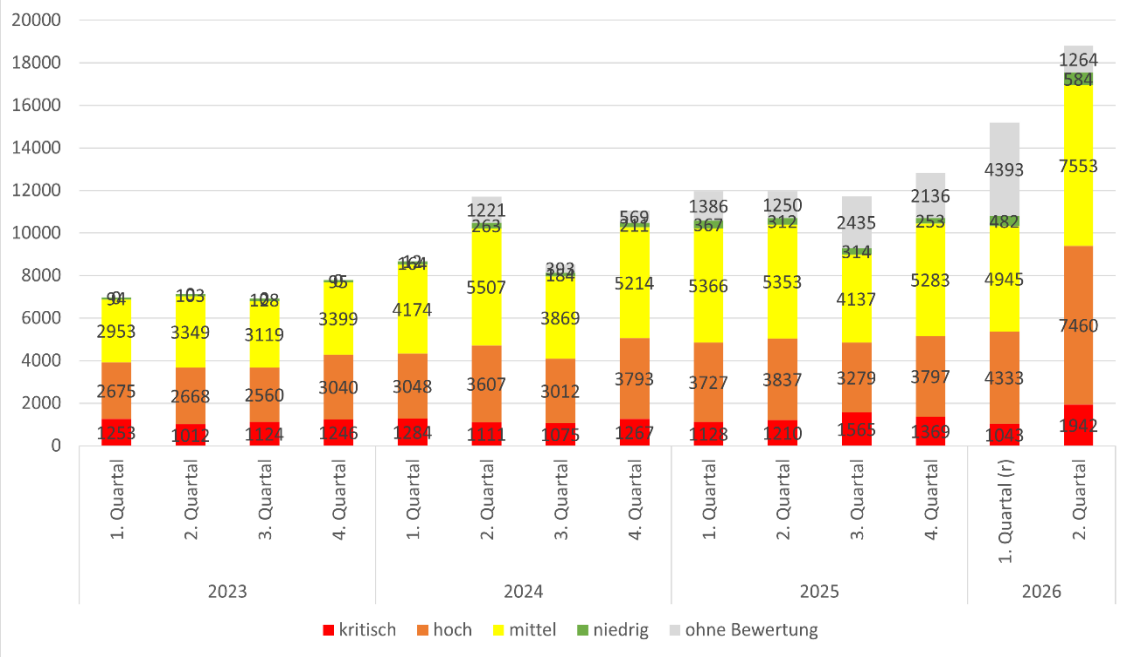
In der TTE bisher nicht berücksichtigt: Mit dem Fortschritt und der Verbreitung von LLMs beschleunigt sich nun nicht nur die Exploit-Generierung, sondern bereits das Identifizieren sowie das automatisierte Verketten von Schwachstellen. Angreifern steht daher nicht mehr nur ein schnelleres Werkzeug, sondern ein autonomes, virtuelles Tool für Cyberangriffe mit sehr hoher Geschwindigkeit zur Verfügung, das rund um die Uhr aktiv ist, in Sekundenbruchteilen dazulernt, vergleichsweise kostengünstig ist und maßgeschneiderte Angriffe produzieren kann (vgl. Angriffsinfrastrukturen). Alle externen Angriffsflächen sollten deshalb engmaschig geprüft und laufend abgesichert werden (vgl. Des Weiteren ist das BSI aktiv in der CRA Expert Group vertreten, um zusammen mit seinen Partnerbehörden und Organisationen der europäischen Wirtschaft, Zivilgesellschaft und ausgewählten Expertinnen und Experten Fragestellungen des CRA zu konkretisieren und den CRA weiterzuentwickeln. Mit der aktiven Teilnahme an der Notifying Authorities Group, dem zentralen Koordinierungsgremium der Notifizierenden Behörden, setzt sich das BSI zudem für eine europäisch harmonisierte und qualitativ angemessene Konformitätsbewertungsinfrastruktur für den CRA ein.

LLMs als Hochgeschwindigkeits-Schwachstellenscanner).

→ Mehr über neue Schwachstellen und Zero-Day-Schwachstellen

2.2.1 Neue Schwachstellen

Abbildung 2-3: Neu bekannt gewordene Schwachstellen weltweit nach Schweregrad
Einheit: Anzahl



Quelle: Schwachstellenstatistik
Bemerkung: Wert wurde (r) korrigiert.

Im aktuellen Berichtszeitraum wurden durchschnittlich täglich 160 neue Schwachstellen bekannt. Das waren 35 % mehr als im vergangenen Berichtszeitraum. Neben einer Vielzahl von Schwachstellen mit niedrigem Schweregrad (plus 52 %) wurden insgesamt knapp 6.000 neue Schwachstellen mit kritischem Schweregrad bekannt (vgl. Abbildung 2-3). Das war ein Anstieg um 26 %. Schwachstellen mit mittlerem oder hohem Schweregrad wurden ebenfalls häufiger entdeckt (plus 11 % bzw. plus 31 %).

In den vergangenen Jahren sind Schwachstellen in aus dem Internet erreichbaren Systemen zur wichtigsten Angriffsfläche für Cyberangriffe geworden. Um sie auszunutzen, verwenden Angreifer sogenannte Exploits, das heißt Schadcode, mit dessen Hilfe Angreifer in IT-Systeme eindringen und dort beispielsweise Daten verschlüsseln oder ausleiten können. Mit Exploitation-Angriffen erzielen Angreifer immer höhere Schadwirkungen (vgl. Lösegelder).

→ Mehr über Zero-Day-Schwachstellen

Die Ausnutzung von Schwachstellen stellte im aktuellen Berichtszeitraum den bedeutsamsten initialen Angriffsvektor dar. Dabei spielen Zero-Days – also Schwachstellen, die zum Zeitpunkt des ersten erfolgreichen Angriffs Herstellern und Entwicklern noch unbekannt sind – eine herausragende Rolle.

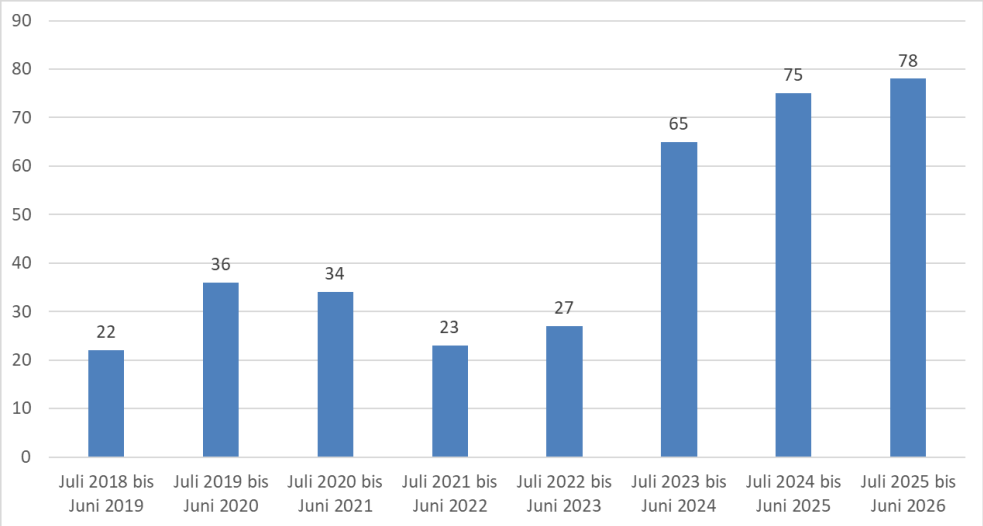
Der immer kürzer werdende Zeitraum zwischen Veröffentlichung der Patches und der Erscheinung öffentlicher Exploits ist besonders besorgniserregend (vgl. Time-to-Exploit, Abbildung 2-2). Mit Hilfe künstlicher Intelligenz (vgl. Künstliche Intelligenz) sowie Reversing der Patches, das heißt gleichsam einer „Rückwärts-Analyse“ des Patchs, die zu der Schwachstelle führt, können Angreifer immer schneller und mit immer weniger Aufwand sowie weniger technischen Know-how Angriffstools entwickeln.

Sind diese einmal öffentlich, folgen in Kürze opportunistische Angriffe weiterer Cyberangreifer. Der Zeitraum ist in vielen Fällen von ehemals Wochen auf inzwischen nur noch wenige Tage bis Stunden geschrumpft. Durch die Weiterentwicklung künstlicher Intelligenz ist davon auszugehen, dass bereits im kommenden Berichtszeitraum die meisten ausgenutzten Schwachstellen Zero-Day-Schwachstellen sein werden.

Diese Entwicklung sowie die stetig steigende Anzahl an Schwachstellen führen zu Handlungsbedarf. Patches für nach dem Common Vulnerability Scoring System (CVSS) als „kritisch“ oder „hoch“ bewertete Schwachstellen sollten insbesondere bei exponierten Systemen nicht aufgeschoben, sondern unverzüglich eingespielt werden. Gleichzeitig sollten die Angriffsflächen minimal gehalten und alle Zugänge und Anwendungen, welche nicht unbedingt einen uneingeschränkten Zugang aus dem Internet benötigen, auf vertrauenswürdige Quellen beschränkt werden. Potenziell Betroffene müssen sich ihrer Angriffsfläche bewusst sein und diese beim Aufkommen neuer Schwachstellen im Blick behalten. Im Falle von Zero-Days oder bei verspätet eingespielten Patches können Systeme bereits mit persistenter Schadsoftware kompromittiert worden sein. Einfaches Patchen ist in diesen Fällen nicht länger ausreichend – die Systeme müssen dann aktiv auf etwaige Kompromittierung untersucht werden.

2.2.2 Hardware-Schwachstellen

Abbildung 2-4: Neu bekannt gewordene Hardware-Schwachstellen
Einheit: Anzahl



Quelle: Schwachstellenstatistik
Bemerkung: Zeitreihe kombiniert unterschiedliche externe Erhebungsstichtage. Der reale Trendverlauf bleibt davon unberührt.

Insgesamt wurden im aktuellen Berichtszeitraum 78 neue Hardware- und Mikroarchitektur-Schwachstellen bekannt (vgl. Abbildung 2-4). Damit erreichte der Wert im aktuellen Berichtszeitraum zum dritten Mal in Folge einen neuen Rekord – 95 % über dem Durchschnitt der vorangegangenen Berichtszeiträume von 40 neuen Hardware-Schwachstellen pro Jahr. Auch die Sicherheit von KI-Systemen wird zunehmend durch Hardware-Schwachstellen bedroht.

→ Mehr über Hardware-Schwachstellen

Hardware-Schwachstellen können schwerwiegende Auswirkungen haben, denn ein flächendeckender Austausch betroffener Produkte ist oft die einzige Möglichkeit zur Behebung, wie das Beispiel RAIN zeigt. Hier konnte der Foreshadow-Angriff auf Intel CPUs von 2018 selbst auf bereits gepatchte Prozessoren erfolgreich durchgeführt werden. Dieselbe Untersuchung zeigt zugleich die Wirksamkeit zusätzlicher Härtungsmaßnahmen: Bei einem großen Cloud-Anbieter scheiterte der Angriff an ergänzenden Schutzmechanismen, die sensible Speicherinhalte dem Zugriff aus virtuellen Maschinen entziehen. Verstärkt im Fokus sind auch Smartphones, die zunehmend dedizierte Sicherheitshardware beinhalten (vgl. SCA_ECDSA).

Schwerpunkte der IT-Sicherheitsforschung liegen außerdem auf Post-Quanten-Kryptografie sowie der Analyse von Angriffen auf deren Hardware-Implementierungen. Diese Algorithmen bieten

Schutz vor Angriffen durch Quantencomputer. Eine gegen Angriffe auf Hardware-Schwachstellen sichere Implementierung von kryptografischen Algorithmen ist jedoch ein relativ junges Forschungsgebiet und deshalb herausfordernd. Seitenkanalangriffe, die nicht auf das kryptografische Verfahren, sondern auf dessen Implementierung gerichtet sind, wie zum Beispiel ML-KEM-SCA, BM, HOCPA, SWOOP), Fault-Angriffe (z. B. DILF, XMSS, Rand) oder Rowhammer Angriffe (SLasH-DSA) nutzen solche Implementierungsschwächen aus.

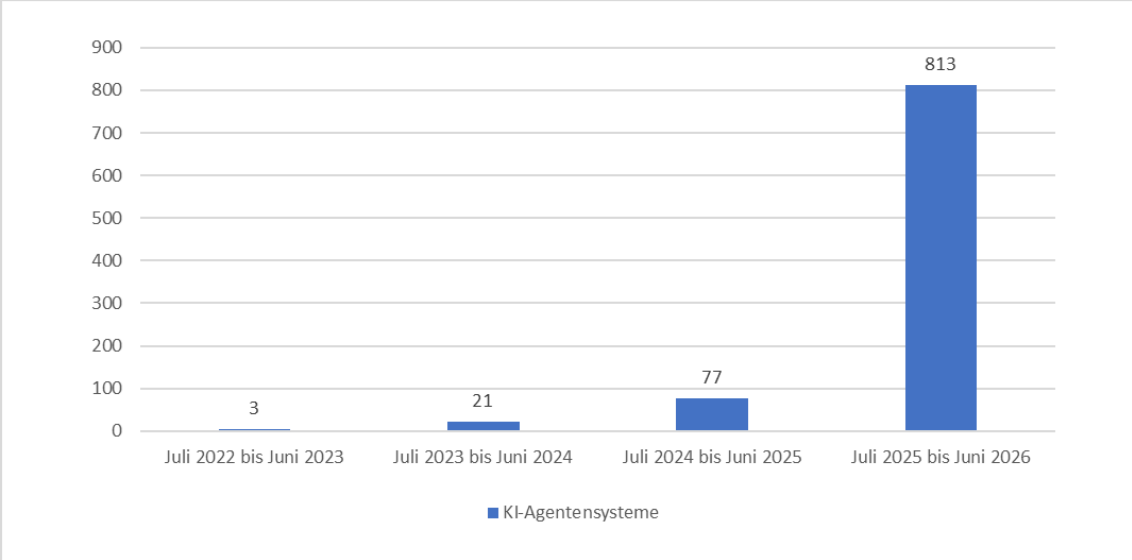
Ein besorgniserregender Trend ist die Vereinfachung der Angriffsmethoden mit maschinellem Lernen. Während in der Vergangenheit vor allem bei Seitenkanalangriffen eine aufwändige und personalintensive manuelle Nachbearbeitung aufgenommener Daten nötig war, können diese Aufgaben nun zunehmend automatisiert werden (z. B. NLM, SnowV). Dies reduziert den Aufwand für Angriffe erheblich und ermöglicht es theoretisch auch Angreifern mit geringeren Ressourcen, solche Angriffe durchzuführen.

Besonders im Umfeld des Cloud-Computings gibt es neue Angriffsvektoren auf etablierte Isolationsmechanismen. Mittels der mikroarchitektonischen Schwachstelle VMScape können Angreifer aus einer regulären, gemieteten virtuellen Maschine heraus die übergeordnete Cloud-Infrastruktur kompromittieren und sensible Daten abschöpfen. Die neue Angriffsmethode TEE.fail zeigt zudem, dass selbst moderne, hardwaregestützte Confidential-Computing-Umgebungen physisch kompromittierbar sind, um so sensible kryptografische Schlüssel zu erlangen.

Ein weiterer Trend sind Angriffe auf neuronale Netze unter Ausnutzung von Hardware-Schwachstellen. Angreifer können KI-Modelle durch Ausnutzung mikroarchitektonischer Schwachstellen beeinflussen. Die Modellarchitektur kann durch Latenzmessungen in SGX-Enklaven (DNN-Latency-Seq) oder durch Analyse von EM-Abstrahlungen von GPUs (ModelSpy) rekonstruiert werden. Geheime Modellparameter und Gewichte werden mittels speicherabhängiger Zugriffsmuster in SGX (AF-Harmfull) oder durch Auswertung von EM-Signalen bei GPU-Berechnungen (BarraCUDA) extrahiert. Sensible Nutzerdaten lassen sich durch Messung von Latenzen beim Power-Gating von KI-Beschleunigern (Gatebleed), EM-Abstrahlung (ScaAR) oder durch Analyse von Seitenkanälen bei Mixture-of-Experts-LLMs (MoEcho) ausspionieren. Neben Informationsdiebstahl ermöglichen hardwarenahe Methoden auch die aktive Störung: Gezielte Bit-Flips im GPU-Speicher (GPUHammer) modifizieren Modelle bösartig und reduzieren die Genauigkeit, während der Missbrauch von Hardware-Mitigationen im Speichermanagement Denial-of-Service ermöglichen kann (Not So Refreshing). Diese Angriffe sind teilweise ohne Hardware-Präparationen aus einem Abstand von mehreren Metern möglich (ModelSpy, ScaAR).

2.2.3 Schwachstellen in KI-Systemen

Abbildung 2-5: Schwachstellen in KI-Agenten
Einheit: Anzahl



Quelle: Schwachstellenstatistik

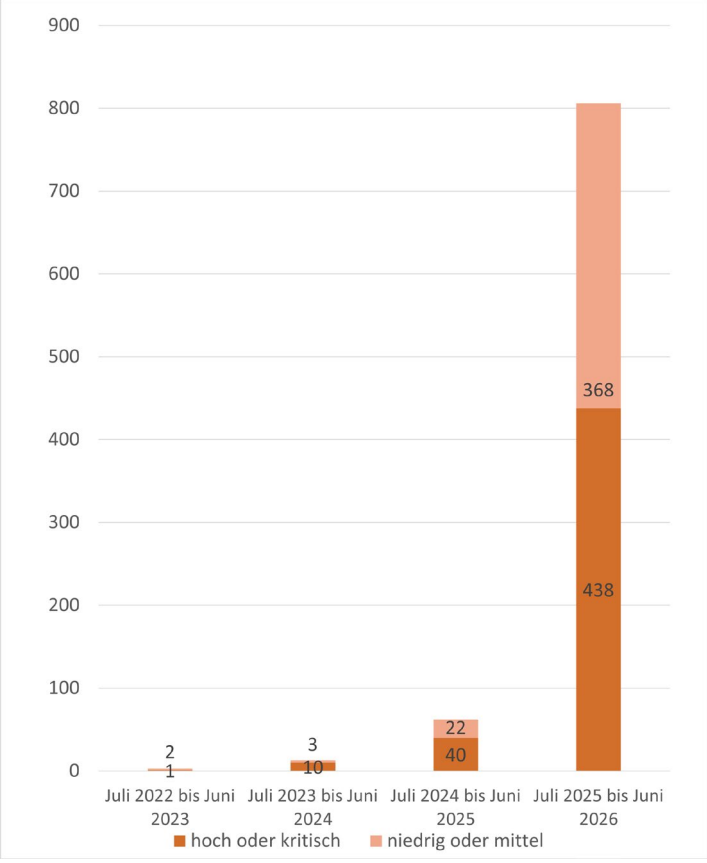
Bemerkung: CVEs von KI-Agentensystemen. KI-Agentensysteme umfassen KI-Coding-Assistenten, allgemeine KI-Agentensysteme und Enterprise-Agentenassistenten. Nicht eingeschlossen sind Agenten-Frameworks, Workflow- und Orchestrierungsplattformen sowie Tool-Gateways. Dieses Produkt nutzt die NVD-API, ist jedoch weder von der NVD empfohlen noch zertifiziert.

KI-Agentensysteme, die eigenständig IT-Werkzeuge nutzen und Arbeitsabläufe steuern, treiben die nächste Welle der Digitalisierung an. Entsprechend ist die Zahl der Schwachstellen in diesen Systemen im aktuellen Berichtszeitraum um 956 % auf 813 gestiegen (vgl. Abbildung 2-5). Die Mehrzahl betraf dabei nicht das KI-Modell selbst, sondern die Schnittstellen zu anderen IT-Werkzeugen. Natürliche Sprache ist nicht nur das Kommunikationsmittel zwischen Mensch und Maschine, sondern ist auch das Mittel für das Finden von Werkzeugen und die Kommunikation verschiedener Agenten untereinander geworden. Dementsprechend ermöglichen Prompt Injections, das heißt Angriffe mittels manipulierter Befehle an ein KI-Agentensystem, die Ausführung vielfältiger Angriffsketten ohne den Einsatz klassischer Schadsoftware, indem sie unerwünschte Aktionen auslösen und bestehende Sicherheitsmechanismen umgehen können. Aus Sicht des BSI werden Sicherheitsaspekte im Wettbewerb um leistungsfähige KI-Agenten nicht ausreichend priorisiert. Möglichkeiten dazu bietet etwa die Härtung von KI-Systemen, mit deren Hilfe sie robuster gegen solche Angriffe werden (vgl. LLM-Härtung).

→ Mehr über Schwachstellen in KI-Systemen

Gut die Hälfte der in agentischen Ökosystemen bekannt gewordenen Schwachstellen hatte einen hohen oder kritischen Schweregrad (vgl. Abbildung 2-6).

Abbildung 2-6: Neu bekannt gewordene Schwachstellen in KI-Agenten nach Schweregrad
Einheit: Anzahl



Quelle: Schwachstellenstatistik
Bemerkung: CVEs von KI-Agentensystemen. KI-Agentensysteme umfassen KI-Coding-Assistenten, allgemeine KI-Agentensysteme und Enterprise-Agentenassistenten. Nicht eingeschlossen sind

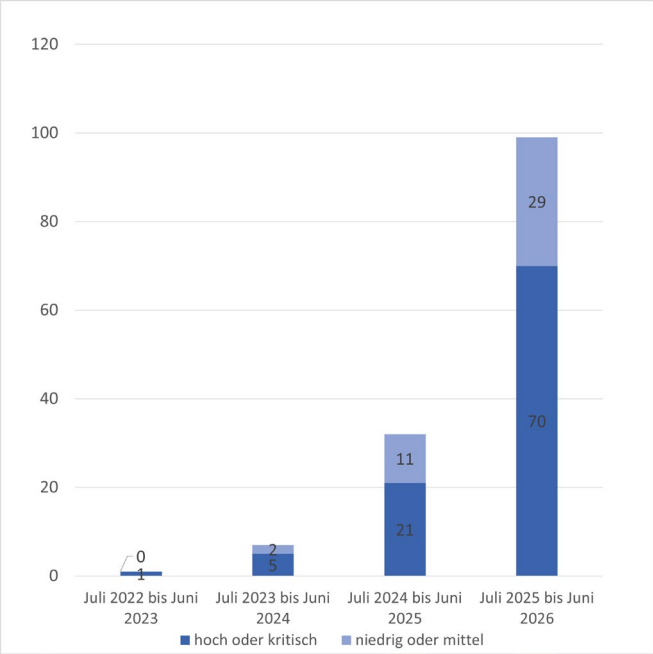
Agenten-Frameworks, Workflow- und Orchestrierungsplattformen sowie Tool-Gateways. Dieses Produkt nutzt die NVD-API, ist jedoch weder von der NVD empfohlen noch zertifiziert.

Die Mehrzahl der Schwachstellen betraf nicht das KI-Modell selbst. Vielmehr waren die Schnittstellen betroffen, über die die Agenten auf andere Werkzeuge zugreifen, Dateien lesen, Code ausführen oder mit APIs und Datenbanken interagieren. Die sichere Gestaltung dieser Schnittstellen – insbesondere die Absicherung von Werkzeugaufrufen, Zugängen zu externen Diensten und Berechtigungskonzepten – ist ein zentraler Stellhebel für die resiliente Ausgestaltung von KI-Ökosystemen.

Welche Auswirkungen einzelne Produkte auf die Statistik haben, zeigt das Agentensystem OpenClaw: Allein für dieses wurden im Berichtszeitraum 539 Schwachstellen erfasst (vgl. **Fehler! Verweisquelle konnte nicht gefunden werden.**).

Darüber hinaus wurden im aktuellen Berichtszeitraum 99 neue Schwachstellen bekannt, die Prompt-Injection-Angriffe ermöglichen (vgl. Abbildung 2-7).

Abbildung 2-7: Prompt-Injection-Schwachstellen in KI-Systemen nach Schweregrad
Einheit: Anzahl



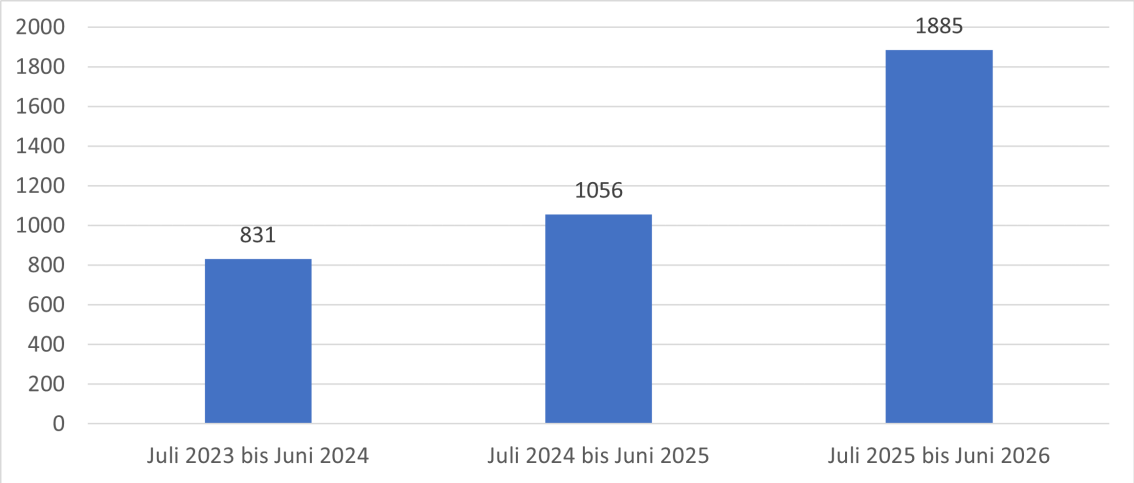
Quelle: SSS
Bemerkung: CVEs, deren Exploit-Kette Prompt Injection als Mechanismus enthält. Ohne Schwachstellen mit unbekanntem Schweregrad. Dieses Produkt nutzt die NVD-API, ist jedoch weder von der NVD empfohlen noch zertifiziert.

Dabei veranlassen Angreifer ein KI-System durch manipulierte Eingaben zu unbeabsichtigtem Verhalten. Rund 60 dieser im aktuellen Berichtszeitraum bekannt gewordenen und analysierten Prompt-Injection-Schwachstellen ermöglichen es Angreifern, das KI-System zur Ausführung von Code – auch Schadcode – zu veranlassen. Die Auswirkungen können damit über bloße Verfälschungen von Ergebnis-Ausgaben deutlich hinausgehen, obgleich Angreifer dafür keine Schadsoftware installieren müssen. Mittels sogenannter indirekter Prompt Injections betten sie schädliche Instruktionen stattdessen direkt in Inhalte ein, die ein KI-System automatisch verarbeitet (etwa E-Mails, Websites oder Dokumente). In der Fachsprache wird die resultierende Angriffskette - von der initialen Prompt Injection über die Ausweitung von Rechten bis zur Einnistung - auch als Promptware bezeichnet.

Es ist davon auszugehen, dass KI-spezifische Schwachstellen, die etwa das Vergiften, also die Manipulation von Trainingsdaten, oder das gezielte Täuschen von KI-Modellen ermöglichen, in der Schwachstellenstatistik noch unterrepräsentiert sind. Die Absicherung multifunktionaler KI-Agentensysteme ist äußerst komplex, und es fehlen derzeit aufgrund der dynamischen Entwicklung noch etablierte Sicherheitsstandards. Klassische IT-Sicherheitsmaßnahmen wie Eingabevalidierung, Ausgabeprüfung und Zugriffsbeschränkung behalten jedoch ihre Relevanz.

2.2.4 Schwachstellen in kryptografischen Verfahren

Abbildung 2-8: Neu bekannt gewordene Schwachstellen in kryptografischen Verfahren
Einheit: Anzahl



Quelle: Schwachstellenstatistik

Kryptografie ist ein wichtiger Baustein für die Sicherheit von IT-Produkten. Das BSI empfiehlt hierzu eine Reihe von Verfahren, die gemeinhin als sicher angesehen werden (vgl. TR-02102). Dennoch können in der Praxis Schwachstellen auftreten, zum Beispiel durch Implementierungsfehler, Seitenkanäle, Schwächen in kryptografischen Mechanismen bzw. Protokollen oder durch schwache Zufallszahlenerzeugung. Im aktuellen Berichtszeitraum wurden 1.885 neue Schwachstellen mit Bezug zur Kryptografie bekannt (plus 79 % gegenüber dem vergangenen Berichtszeitraum).

→ Mehr über Schwachstellen in kryptografischen Verfahren

Im aktuellen Berichtszeitraum hat ein Forscherteam zwei Schwachstellen in der Messaging-App Signal veröffentlicht (https://eprint.iacr.org/2026/484) und auf der Fachtagung RWC 2026 (https://rwc.iacr.org/2026/) vorgestellt. Es handelte sich hierbei um Schwachstellen, die vor Veröffentlichung an Signal gemeldet und innerhalb kurzer Zeit geschlossen wurden. Sie waren nicht ursächlich für die Phishing-Angriffe auf Signal-Konten hochrangiger Politikerinnen und Politiker im Frühjahr 2026 (vgl. Ausgewählte Vorfälle: Gefährdungslage: Phishing-Angriffe via Messenger).

Die beiden bekannt gewordenen Schwachstellen ermöglichten einem Angreifer, unter einer frei wählbaren falschen Identität, beliebige Nachrichten zu senden. Die erste Schwachstelle betraf die Android- und Desktop-Version der Signal-App und basierte darauf, dass die Identität der Nutzenden über eine Telefonnummer oder einen Nutzendennamen gegeben ist. Ein Protokoll verbindet diese beiden Identitäten, sodass aus Sicht der Empfängerinnen und Empfänger alle Nachrichten vom selben Nutzenden kommen, auch wenn für jede Identität der Senderinnen und Sender separate Verbindungen bestehen. Angreifer konnten nun unter bestimmten Bedingungen mit der Telefonnummer der Senderinnen und Sender als Identität beliebige Nachrichten an die Empfängerinnen und Empfänger senden. Verglichen die Empfängerinnen und Empfänger aufgrund der auf ihren Geräten angezeigten Sicherheitswarnungen gemeinsam mit den Senderinnen und

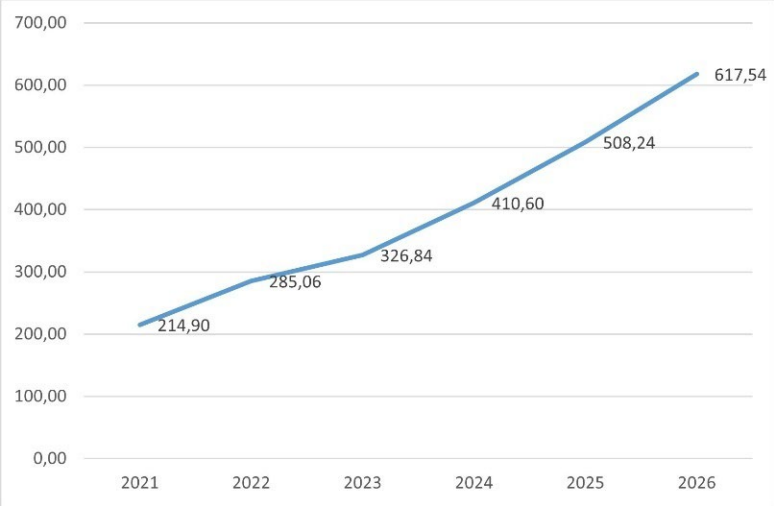
Sendern die Parameter ihrer Verbindung, fielen keine Unregelmäßigkeiten auf, da der Überprüfung lediglich die Verbindung zwischen Senderinnen und Sendern sowie Empfängerinnen und Empfänger basierend auf den Nutzendennamen zugrunde liegt.

Die zweite Schwachstelle betraf die Android-Version der Signal-App. Für einen Angriff mussten weniger Bedingungen als im oben geschilderten Szenario erfüllt sein. Zudem betraf diese Schwachstelle nicht nur Punkt-zu-Punkt-Verbindungen, sondern auch Gruppen-Chats. Der Angriff wurde hier durch die Kombination zweier Eigenschaften erreicht: Werden im Rahmen des SSS-Protokolls von Signal verschlüsselte Nachrichten von Senderinnen und Sendern an Empfängerinnen und Empfänger gesendet, so findet bei den Empfängerinnen und Empfängern keine Überprüfung statt, ob die von den Senderinnen und Sendern verwendeten Schlüssel tatsächlich diejenigen sind, welche jeweils an die Identitäten der Senderinnen und Sender gebunden sind. Die Verbindung zwischen Identität und Schlüssel wird zwar durch ein Zertifikat des Signal-Servers beglaubigt – diesem soll aber im Rahmen einer Ende-zu-Ende-verschlüsselten Verbindung zwischen Senderinnen und Sendern sowie Empfängerinnen und Empfänger nicht vertraut werden müssen. Ein Angreifer, der den Server kontrolliert, war nun dazu in der Lage, unter einer falschen Identität Klartextnachrichten an beliebige Empfängerinnen und Empfänger zu senden – verschlüsselte Nachrichten erfordern Schlüsselmaterial, welches dem Server nicht bekannt ist. Solche Klartextnachrichten dürfen allerdings nur zum Versenden von Fehlermeldungen verwendet werden. In der Android-Implementierung wurden die Nachrichteninhalte allerdings unzureichend geprüft, sodass es dem Angreifer möglich war, über Klartextnachrichten beliebige Inhalte zu versenden.

→ Weitere Informationen: Aktivitäten des BSI zum Thema Kryptografie finden sich unter https://www.bsi.bund.de/dok/Kryptografie

2.3 Vernetzte Geräte

Abbildung 2-9: Prognose von Verbindungen vernetzter Geräte mit dem Internet in Deutschland, Vernetzte Geräte insgesamt
Einheit: Anzahl in Millionen



Quelle: Statista Market Insights
Bemerkung: Dedupliziert, ohne Smartphones, Laptops, Tablets, PCs.

Vernetzte Geräte bieten eine seit Jahren wachsende Angriffsfläche. Prognosen zufolge wird es im Jahr 2026 in Deutschland insgesamt knapp 618 Millionen Verbindungen von vernetzten Geräten mit dem Internet geben (dedupliziert, vgl. Abbildung 2-9) – ein Zuwachs von 22 % gegenüber dem Vorjahr.

Vernetzte Geräte werden von Cyberangreifern gekapert und etwa für DDoS-Angriffe missbraucht oder genutzt, um Angriffsdatenverkehr umzuleiten. Den angegriffenen Systemen wird hierbei suggeriert, der Verkehr käme aus ihrer jeweiligen Region. Eine Anomalieerkennung, die

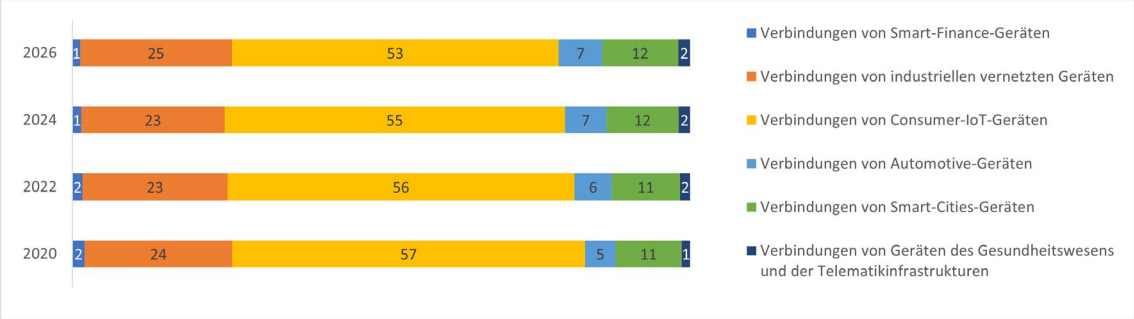
Datenverkehr aus entfernten Regionen gegebenenfalls als unplausibel erkennt und daher abweisen würde, kann so unterlaufen werden. Das macht Infiltrationen wahrscheinlicher.

Mit dem Cyber Resilience Act erhöht die EU die Sicherheit von Produkten mit digitalen Elementen, unter anderem auch von vernetzten Geräten (vgl. Cyber Resilience Act).

→ Mehr über vernetzte Geräte

2.3.1 Vernetzte Geräte insgesamt

Abbildung 2-10: Prognose von Verbindungen vernetzter Geräte mit dem Internet in Deutschland nach Art des Geräts
Einheit: Anteile in Prozent

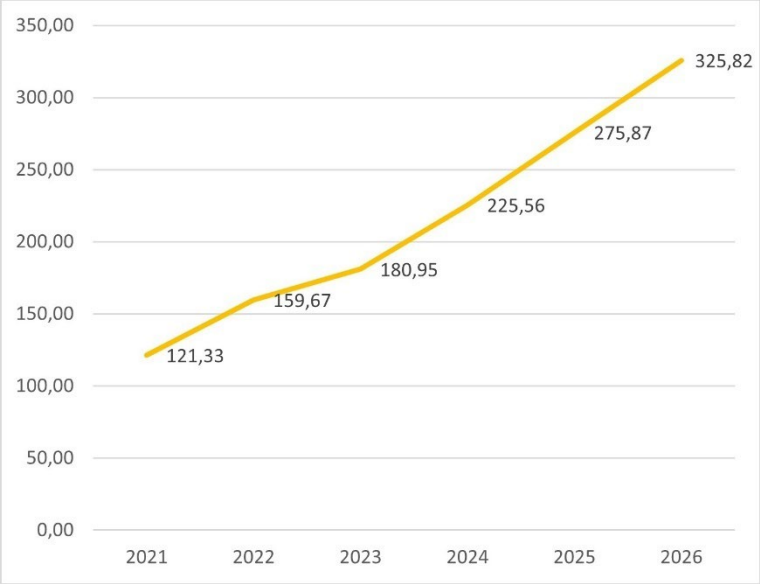


Quelle: Statista Market Insights
Bemerkung: Dedupliziert, ohne Smartphones, Laptops, Tablets, PCs.

Mit 53 % werden bis Ende 2026 laut Prognosen mehr als die Hälfte der Verbindungen vernetzter Geräte mit dem Internet in Deutschland auf Consumer-IoT-Geräte zurückzuführen sein – also auf Geräte für Endverbraucherinnen und -verbraucher wie etwa Smart-Home-Geräte, Smartwatches, Fitness-Tracker und Ähnliches (vgl. Abbildung 2-10). Industrial-IoT-Geräte machen rund ein Viertel der Verbindungen aus. 12 % der Verbindungen entfallen auf Smart-City-Geräte wie etwa Steuerungsinfrastruktur und urbane Datenplattformen.

2.3.2 Consumer-IoT-Geräte

Abbildung 2-11: Prognose von Verbindungen vernetzter Geräte mit dem Internet in Deutschland, Consumer IoT
Einheit: Anzahl in Millionen



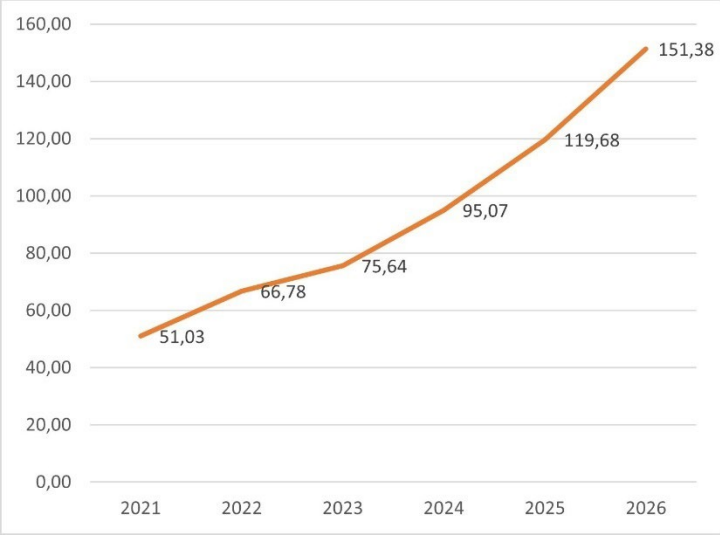
Quelle: Statista Market Insights
Bemerkung: Dedupliziert, ohne Smartphones, Laptops, Tablets, PCs.

Prognosen zufolge dürfte die Angriffsfläche, die durch Consumer-IoT-Geräte entsteht, bis Ende 2026 um 18 % gegenüber 2025 auf 326 Millionen Verbindungen allein in Deutschland wachsen (vgl. Abbildung 2-11). Für Angreifer stellen diese Geräte eine attraktive Angriffsfläche dar: Von allen IoT-Kategorien weisen Consumer-IoT-Geräte die kürzesten Lebenszyklen auf. Hoher Kostendruck der Massenproduktion geht zulasten der Cybersicherheit: Hersteller bieten bislang nur für kurze Zeit oder überhaupt keine Sicherheitsupdates an. Nach Ende des Supports werden neu bekannt gewordene Schwachstellen nicht mehr geschlossen und die Systeme sind leichte Ziele für Cyberangreifer. Um die Endpreise niedrig zu halten, verzichten Hersteller zudem oftmals auf Verschlüsselungsstandards oder setzen nur schwache Verschlüsselung ein, sodass die Geräte unverschlüsselt über lokale Netzwerke oder das Internet kommunizieren und Daten auf Cloud-Servern oder Gateways im Klartext vorliegen. Die stark wachsende und vergleichsweise schlecht geschützte Angriffsfläche des Consumer IoT macht es Angreifern leicht, Angriffsinfrastruktur wie beispielsweise Botnetze mit hoher Leistungsfähigkeit aufzubauen (vgl. Botnetze) oder Daten abzugreifen (vgl. Datenleaks). Mit dem Cyber Resilience Act (vgl. Cyber Resilience Act) hat die EU weitreichende Rahmenbedingungen zur Verbesserung der Cybersicherheit von Produkten mit digitalen Elementen geschaffen.

2.3.3 Industrial-IoT-Geräte

Abbildung 2-12: Prognose von Verbindungen vernetzter Geräte mit dem Internet in Deutschland, Industrial IoT

Einheit: Anzahl in Millionen



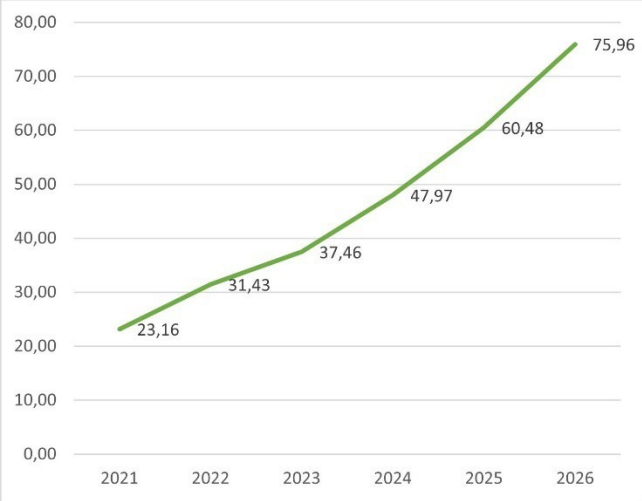
Quelle: Statista Market Insights

Bemerkung: Dedupliziert, ohne Smartphones, Laptops, Tablets, PCs.

Industrial-IoT-Geräte sind IP-basierte, vernetzte Geräte, die isolierte operative Technik (OT) wie etwa industrielle Steuerungssysteme (ICS) mit dem Internet verbinden. Die Angriffsfläche des Industrial-IoT (IIoT) in Deutschland dürfte Prognosen zufolge im Jahr 2026 um 27 % gegenüber dem Vorjahr auf 151 Millionen Verbindungen steigen (vgl. Abbildung 2-12). Hintergrund ist zum einen der tatsächlich zunehmende Einsatz solcher IP-basierter Geräte etwa zu Fernwartungszwecken oder um beispielsweise Daten aus ICS in Clouds abzulegen, zu analysieren und Ergebnisse an das ICS zurückzuspielen. Zum anderen wird aber auch moderne OT stetig digitaler und vernetzter. So bringen solche Systeme inzwischen in der Regel selbst Internet-Schnittstellen mit und entwickeln sich insoweit selbst zu Industrial-IoT-Geräten weiter. Durch die zunehmende Vernetzung von OT und IIoT entstehen neue Angriffsvektoren, die in der Vergangenheit aufgrund getrennter Systeme blockiert waren. Während Cyberangreifer IIoT bisher vor allem für Aufklärungstätigkeiten gegen potenzielle Ziele nutzten, gingen sie im aktuellen Berichtszeitraum dazu über, Steuerungsschleifen von ICS-Systemen besser zu verstehen und industrielle Prozesse gezielt zu manipulieren (vgl. Industrialcyber.co).

2.3.4 Smart-City-Geräte

Abbildung 2-13: Prognose von Verbindungen vernetzter Geräte mit dem Internet in Deutschland, Smart City
Einheit: Anzahl in Millionen

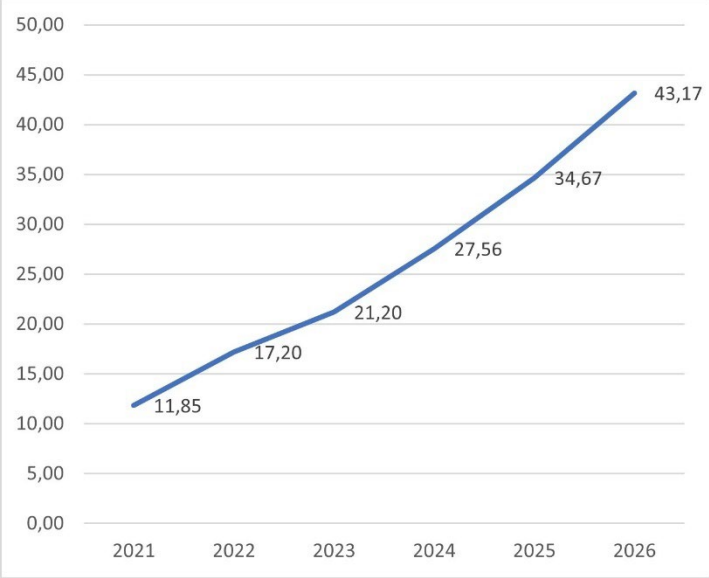


Quelle: Statista Market Insights
Bemerkung: Dedupliziert, ohne Smartphones, Laptops, Tablets, PCs.

Urbane Datenplattformen bilden das Herzstück von Smart-City-Infrastrukturen. Hier laufen die Daten aus unterschiedlichsten Sektoren wie beispielsweise Verkehr, Klima und Wasserständen zusammen und werden zukünftig zur Steuerung der Infrastruktur ausgewertet. Die vernetzten Smart-City-Geräte bilden mit einem Anteil von 12 % aller IoT-Verbindungen (vgl. Abbildung 2-10) nicht nur die drittgrößte, sondern Prognosen zufolge auch eine weiter wachsende Angriffsfläche (plus 26 % bis Ende 2026, vgl. Abbildung 2-13).

2.3.5 Automotive-IoT-Geräte

Abbildung 2-14: Prognose von Verbindungen vernetzter Geräte mit dem Internet in Deutschland, Automotive IoT
Einheit: Anzahl in Millionen



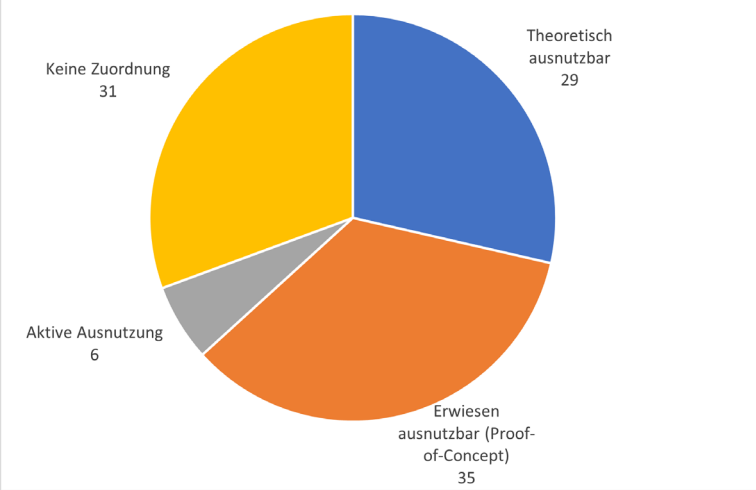
Quelle: Statista Market Insights
Bemerkung: Dedupliziert, ohne Smartphones, Laptops, Tablets, PCs.

Von Steuergeräten über Sensorik bis hin zu Cloud- und Mobilfunkverbindungen: Jede neue Komponente eines modernen PKW oder LKW erweitert die Angriffsfläche und bietet Cyberangreifern neue Möglichkeiten, Schwachstellen auszunutzen. Prognosen deuten auf ein Wachstum der Angriffsflächen im Automotive-Bereich um 25 % bis Ende 2026 hin. Das BSI beobachtet die Entwicklung, nimmt Meldungen von IT-Sicherheitsforschenden entgegen und unterstützt bei der koordinierten Veröffentlichung von Schwachstellen (vgl. Coordinated Vulnerability Disclosure).

→ Mehr über vernetzte Automotive-Geräte

Im aktuellen Berichtszeitraum hat das BSI 49 Meldungen im Kontext Automotive bearbeitet. Ähnlich wie im vorangegangenen Berichtszeitraum beruhte ein Großteil der Meldungen auf Forschungsarbeiten oder Sicherheitsanalysen, die theoretisch ausnutzbare Schwachstellen aufgedeckt haben (29 % der Meldungen, vgl. Abbildung 2-15), sowie auf Schwachstellen, die erwiesen ausnutzbar waren (35 %). 6 % der Schwachstellenmeldungen bezogen sich auf aktiv ausgenutzte Schwachstellen (vgl. Abbildung 2-15).

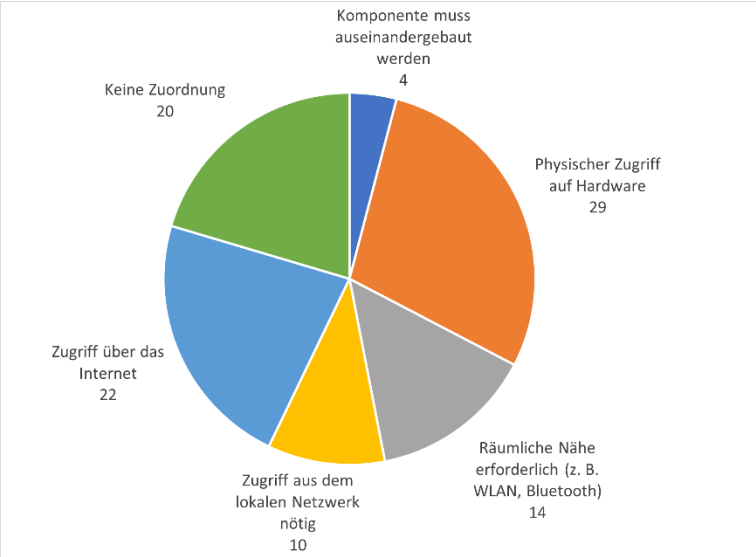
Abbildung 2-15: Schwachstellen mit Bezug zu Fahrzeugen von Juli 2025 bis Juni 2026 nach Ausnutzungsmöglichkeit
Einheit: Anteile in Prozent



Quelle: BSI

Bei etwa 29 % der ausgewerteten Schwachstellen war ein physischer Zugriff auf das Fahrzeug oder die Komponente zur Ausnutzung der Schwachstelle nötig (vgl. Abbildung 2-16) oder die Komponente musste sogar auseinandergebaut werden (4 %). In 14 % der Fälle hätte ein Angriff in räumlicher Nähe (Bluetooth/WLAN) durchgeführt werden können, bei 22 % wäre der Angriff potenziell aus der Entfernung über das Internet möglich gewesen.

Abbildung 2-16: Schwachstellen mit Bezug zu Fahrzeugen von Juli 2025 bis Juni 2026 nach möglichem Angriffsweg
Einheit: Anteile in Prozent



Quelle: BSI

Technische Schwachstellen in der Ladeinfrastruktur

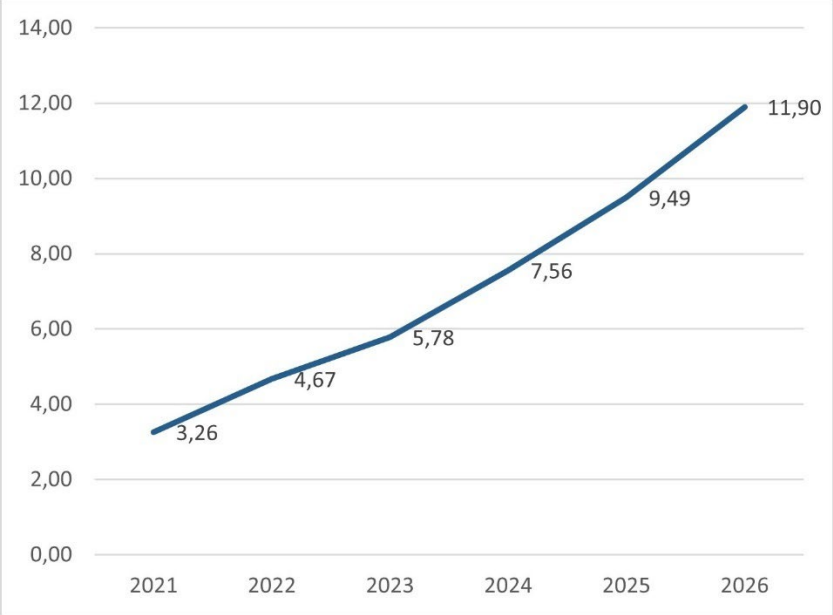
Das BSI hat gemeinsam mit dem Bundesministerium für Verkehr die IT-Sicherheit in der öffentlichen Ladeinfrastruktur im Rahmen einer Studie untersucht. Darin wurden unter anderem einschlägige Schwachstellen und Ergebnisse aus Hacking-Wettbewerben aus den zurückliegenden Jahren ausgewertet. Im Hinblick auf die in der Ladeinfrastruktur relevanten Kommunikationsprotokolle bezogen sich mehr als die Hälfte (21 von 41) der betrachteten CVEs auf Implementierungen des Standards IEC 61850. Weitere 15 CVEs bezogen sich auf das Open Charge Point Protocol (OCPP). Vielen anderen Protokollen konnten keine CVEs zugeordnet werden.

Schwächen in technischen und organisatorischen Normen

Die Anzahl der bekannten Schwachstellen korreliert in der Regel nicht mit dem Sicherheitsniveau der jeweiligen Norm. Normen ohne bekannte Schwachstellen sind also nicht zwangsläufig sicherer. Es ist anzunehmen, dass die beobachteten Unterschiede vor allem daraus resultieren, dass Hacking-Wettbewerbe wie Pwn2Own einem zu testenden Programm erhebliche Aufmerksamkeit verschaffen. Zudem sind solche Programme in der Regel leichter zugänglich. Andere Normen und Systeme dürften bislang schlicht noch nicht so intensiv untersucht worden sein. Die Überprüfung der Protokolle und entsprechender Produkte in ihrer vollen Breite bleibt damit eine fortlaufende Aufgabe.

2.3.6 Vernetzte Geräte im Gesundheitswesen und der Telematikinfrastruktur

Abbildung 2-17: Prognose von Verbindungen vernetzter Geräte mit dem Internet in Deutschland, Gesundheitswesen und Telematikinfrastruktur
Einheit: Anzahl in Millionen



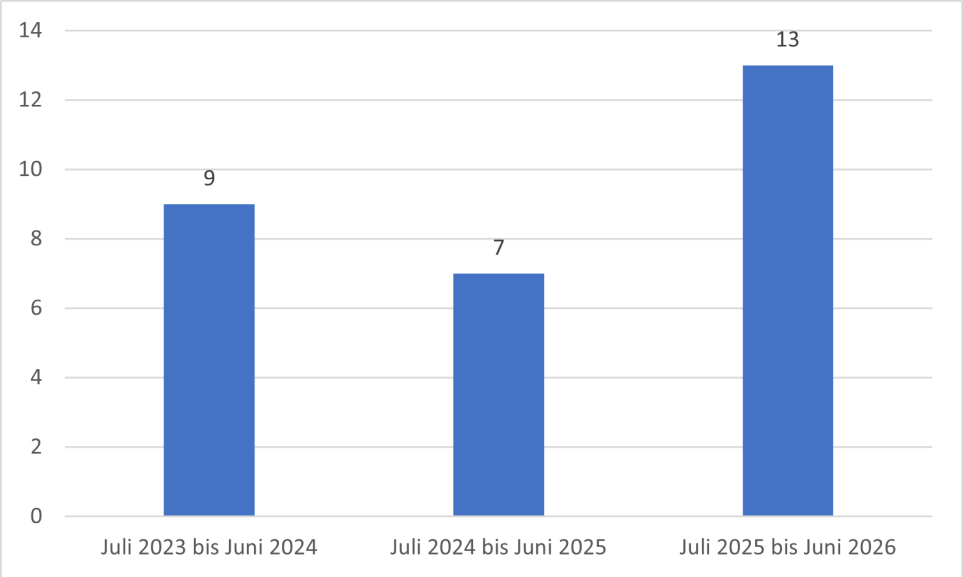
Quelle: Statista Market Insights
Bemerkung: Dedupliziert, ohne Smartphones, Laptops, Tablets, PCs.

Die fortschreitende Digitalisierung des Gesundheitswesens und der Ausbau von Telematikinfrastrukturen führen zu einer zunehmenden Vernetzung von Gesundheitseinrichtungen, medizinischen Geräten und digitalen Patientenakten. Die damit verbundene Angriffsfläche für Cyberangriffe wird laut Prognose bis Ende 2026 um gut 25 % auf knapp 12 Millionen Verbindungen wachsen (vgl. Abbildung 2-17). Ziele im Gesundheitswesen gelten wie die meisten Kritischen Infrastrukturen als besonders attraktiv für Cyberangreifer, da Angreifer mit den dort gestohlenen Daten enormen Erpressungsdruck aufbauen oder etwa im Falle tiefgehender Infiltration sogar lebensgefährliche Sabotageakte durchführen können.

→ Mehr über vernetzte Geräte im Gesundheitswesen und in Telematikinfrastrukturen

Das BSI hat im aktuellen Berichtszeitraum insgesamt 109 Ereignisse im deutschen Gesundheitswesen und der Telematikinfrastruktur erfasst und bearbeitet. Hierin sind Schwachstellen, Ausfälle und Angriffe enthalten. Dabei wurden 14 kritische Ereignisse im Zusammenhang mit Medizinprodukten bewertet. Das entsprach einem Anteil von 13 % (vgl. Abbildung 2-18). Im vergangenen Berichtszeitraum hatte der Wert noch bei 7 % gelegen.

Abbildung 2-18: Kritische Ereignisse in der Telematikinfrastruktur und im Gesundheitswesen
Einheit: Anteile in Prozent

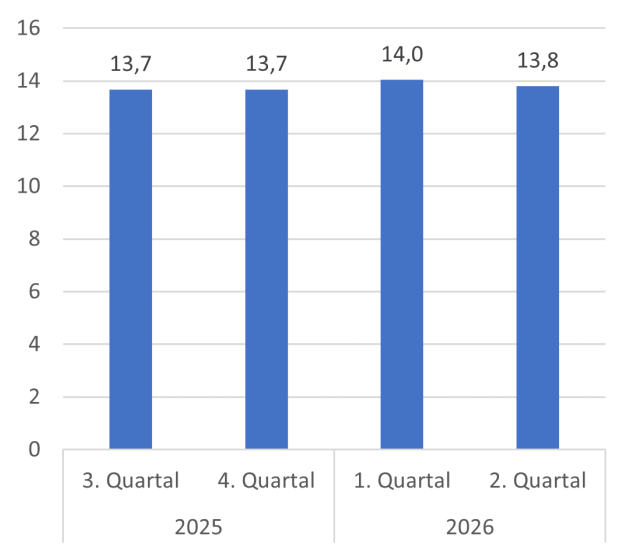


Quelle: BSI
Bemerkung: Ereignis: Schwachstelle, Ausfall oder Angriff

Bei solchen Ereignissen handelt es sich um Schwachstellen, die nicht nur im Rahmen der Cybersicherheit, sondern auch dadurch relevant sind, dass sie zusätzlich ein potenzielles Risiko für Leib und Leben darstellen können, weil sie zum Beispiel Produkte in der medizinischen Versorgung betreffen. Hierbei zeigt sich bereits seit zwei Jahren ein Trend, bei dem kritische Schwachstellen vor allem in Software-Medizinprodukten wie PACS-Systemen (Picture Archiving and Communication System) oder Radiologieinformationssystemen auftreten. Diese Systeme dienen der zentralen Speicherung, Archivierung, Betrachtung und Übermittlung bildgebender Daten in Arztpraxen und Krankenhäusern. Von den 14 als kritisch bewerteten Schwachstellen (13 %, vgl. Abbildung 2-18) betrafen fünf Schwachstellen reine Softwareprodukte. Bei den Schwachstellen handelt es sich insbesondere um unsichere Konfigurationen, schwache Authentifizierungen, die Möglichkeit zur Fernausführung von Programmcode über das Netzwerk sowie SQL-Injections.

2.4 Web-Angriffsflächen

Abbildung 2-19: Web-Angriffsfläche von Deutschland
Einheit: Anzahl .de-Domains in Millionen



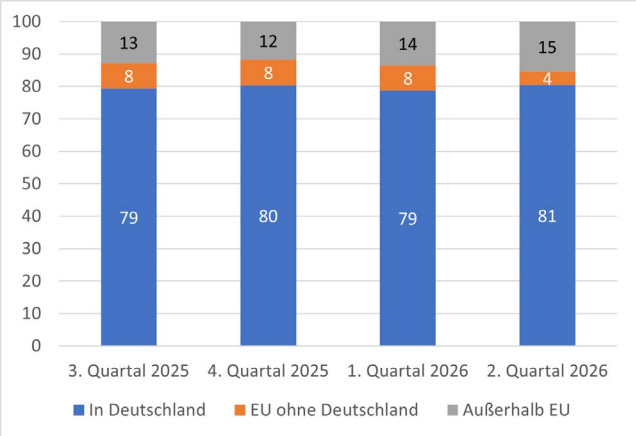
Quelle: Web-Angriffsflächenmessung
Bemerkung: Aus dem Internet erreichbare, erfasste .de-Domains

Die Deutschland zuzuordnende Web-Angriffsfläche umfasst alle .de-Domains. Das waren im aktuellen Berichtszeitraum durchschnittlich 17,7 Millionen Domains. Von diesen waren durchschnittlich 13,8 Millionen Domains, in der Spitze bis zu 14 Millionen Domains aus dem Internet erreichbar und daher potenziell mittels Exploitation angreifbar (vgl. Abbildung 2-19).

→ Mehr über Web-Angriffsflächen

2.4.1 Web-Angriffsflächen unter .de-Domains

Abbildung 2-20: Aus dem Internet erreichbare .de-Domains nach geografischer Lage
Einheit: Anteile in Prozent



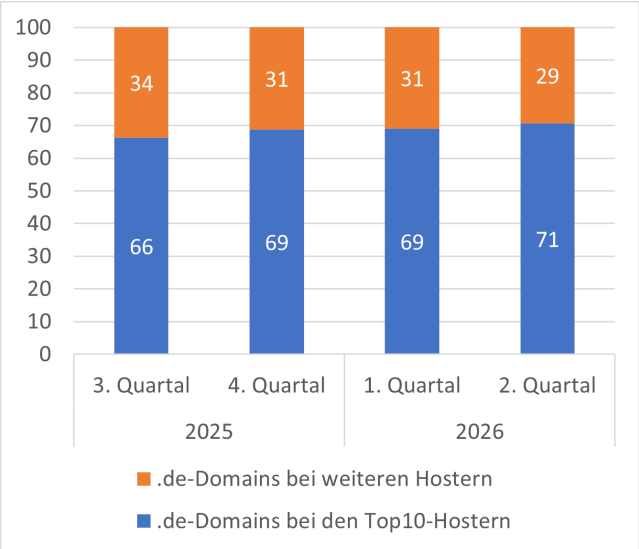
Quelle: Web-Angriffsflächenmessung

Mit durchschnittlich 80 % liegt der weitaus größte Teil der aus dem Internet erreichbaren .de-Domains auch geografisch in Deutschland (vgl. Abbildung 2-20). Sofern sie im Ausland liegen, werden die meisten Domains in den USA gehostet. Viele weitere liegen in anderen europäischen Ländern, aber auch in Kanada.

→ Mehr über Web-Angriffsflächen unter .de

Ein Hoster stellt für seine Kunden Speicherplatz und eine Internetanbindung für deren Websites zur Verfügung. Die Web-Angriffsflächen unter .de-Domains wurden im Berichtszeitraum bei insgesamt rund 6.000 verschiedenen Hostern gehalten. Mit durchschnittlich 69 % lagen die weitaus meisten .de-Domains bei jeweils einem der zehn größten Hoster (vgl. Abbildung 2-21).

Abbildung 2-21: .de-Domains nach Hoster
Einheit: Anteile in Prozent



Quelle: Web-Angriffsflächenmessung
Bemerkung: Aus dem Internet erreichbare, erfasste .de Domains.

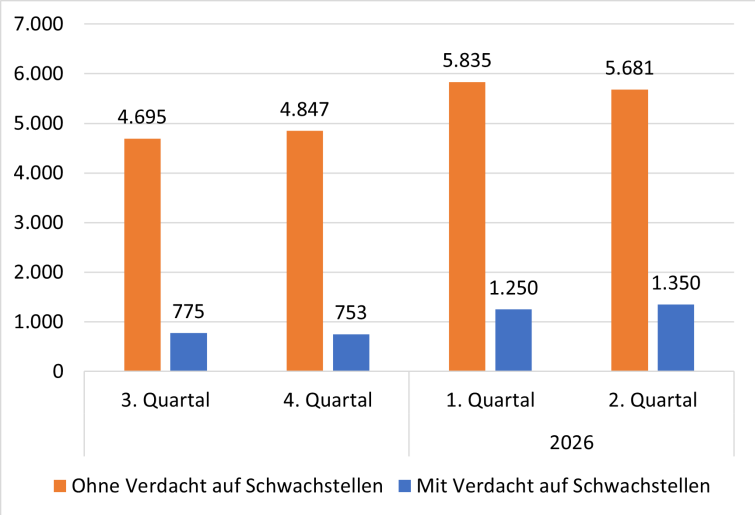
Neben einigen wenigen großen Anbietern gab es sehr viele Klein- und Kleinstanbieter: Durchschnittlich 31 % der .de-Domains wurden hier gehostet.

Wie zu jeder IP-Adresse können auch zu den IP-Adressen hinter .de-Domains über Scan-Dienstleister bei einzelnen Abfragen oft kostenfrei Metadaten abgerufen werden, die zum Beispiel Geoinformationen, Informationen über eingesetzte Software, technische Informationen wie Serverbanner und sogar Informationen über potenzielle Schwachstellen enthalten. Angreifer können sich diese Informationen legal und kostenfrei verschaffen und für Angriffe missbrauchen.

2.4.2 Web-Angriffsflächen der Bundesverwaltung

Abbildung 2-22: Aus dem Internet erreichbare IP-Adressen der Bundesverwaltung nach Schwachstellenverdacht

Einheit: Anzahl



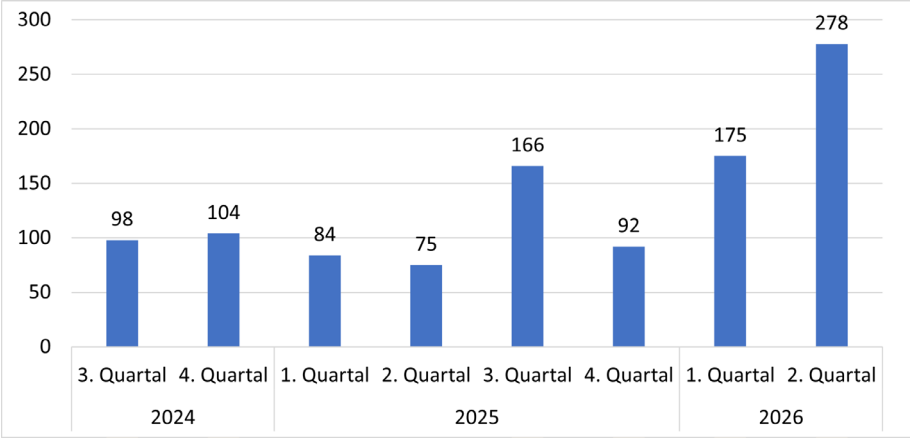
Quelle: BSI

Die Web-Angriffsflächen der Bundesverwaltung umfassen 1,12 Millionen. IP-Adressen und zugehörige Domains, von denen jedoch nur ein geringer Teil tatsächlich aus dem Internet erreichbar ist. Das Schwachstellen-Monitoring des BSI umfasst diesen erreichbaren Teil (Hellfeld) und konnte im aktuellen Berichtszeitraum erheblich ausgeweitet werden, da nunmehr die rechtlichen Voraussetzungen hierfür vorliegen – von durchschnittlich 4.000 IP-Adressen im vergangenen Berichtszeitraum auf aktuell durchschnittlich knapp 6.300 IP-Adressen und zum Ende des Berichtszeitraums auf rund 7.000 IP-Adressen (vgl. Abbildung 2-22). Von der Gesamtmenge der aus dem Internet erreichbaren IP-Adressen der Bundesverwaltung wiesen im aktuellen Berichtszeitraum bis zu 20 % den Verdacht auf mindestens eine Schwachstelle auf, wobei auf einzelnen IP-Adressen aufgrund älterer Serversysteme Schwachstellen gehäuft vorkommen können. Gerade im Kontext von KI, die eine Massenprüfung von Web-Angriffsflächen auf Schwachstellen ermöglicht, muss diesen Systemen erhöhte Aufmerksamkeit geschenkt werden.

→ Mehr über die Web-Angriffsflächen der Bundesverwaltung

Die seit dem 3. Quartal 2025 wachsende Zahl der aus dem Internet erreichbaren IP-Adressen der Bundesverwaltung mit Verdacht auf Schwachstellen liegt sowohl an einer verbesserten Systemerkennung als auch an der Veröffentlichung einzelner Schwachstellen, die weit verbreitete Systeme betreffen (vgl. Abbildung 2-23). Beispiele sind OpenSSH und Apache HTTP Server.

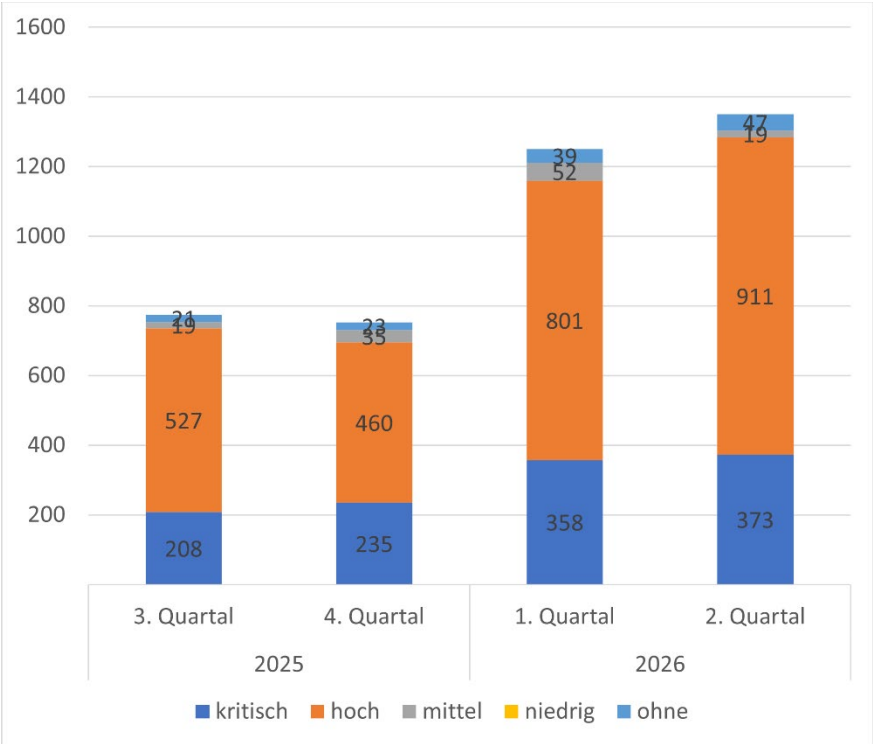
Abbildung 2-23: Neue Schwachstellenverdachte in der Bundesverwaltung
Einheit: Anzahl



Quelle: BSI

Von denjenigen möglichen Schwachstellen, die für die Systeme der Bundesverwaltung erfasst wurden, kamen im 3. Quartal 2025 und im 2. Quartal 2026 schubweise 166 bzw. bis zu 278 Verdachte hinzu. Solche Schwankungen können etwa durch Patchdays großer Hersteller entstehen.

Abbildung 2-24: Erreichbare IP-Adressen der Bundesverwaltung mit Schwachstellenverdacht nach Schweregrad der Schwachstelle
Einheit: Anzahl



Quelle: BSI

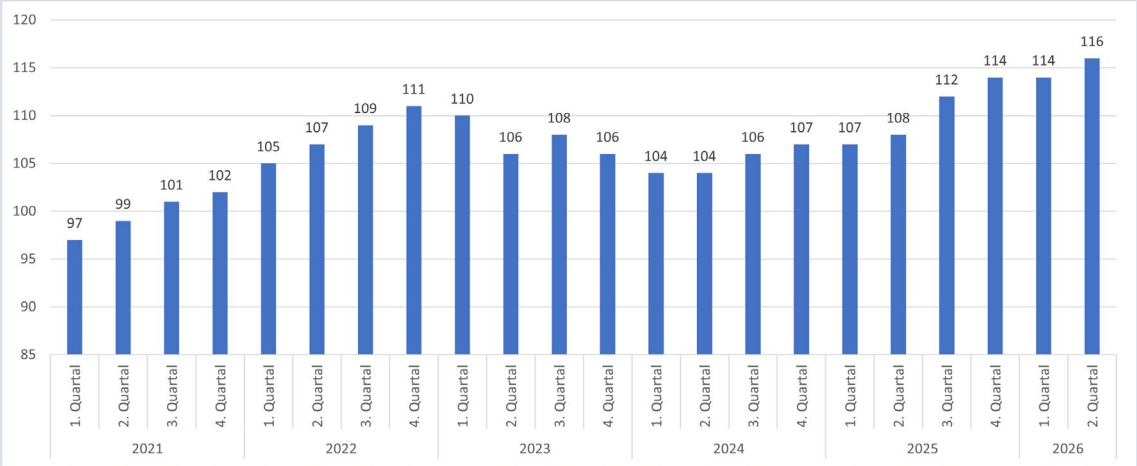
Betrachtet man den einer möglichen Schwachstelle zugeordneten Schweregrad, so ist dieser in den meisten Fällen hoch oder kritisch (vgl. Abbildung 2-24). Dies ist der Tatsache geschuldet, dass die Daten im Monitoring von außen erreichbare Systeme abbilden, deren Angreifbarkeit grundsätzlich ein hoher Schweregrad zugeordnet wird. Die tatsächliche Verwundbarkeit betrifft allerdings nur einen Bruchteil der Systeme, für die ein Verdacht besteht. Wie groß dieser Anteil ist, lässt sich gegenwärtig nicht belastbar feststellen. Nach einer groben Schätzung aus den Meldungen über

tatsächliche Verwundbarkeiten (vgl. Resiliente Bundesverwaltung) bewegt sich die tatsächliche Verwundbarkeit im einstelligen Prozentbereich.

Die Web-Angriffsfläche der Bundesverwaltung ist sowohl durch neu auftretende Schwachstellen als auch durch solche aus veralteten, nicht aktualisierten Systemen gekennzeichnet. Für die Bundesverwaltung ist es also gleichermaßen wichtig, bei Auftreten neuer Schwachstellen die Systeme zeitnah zu härten, die Sicherheitsstandards zu verbessern und anfällige Altsysteme abzubauen. Das BSI bietet hier unterstützend Attack Surface Checks für Behörden an. Der Check unterstützt Behörden pragmatisch bei der Erfassung und Minimierung ihrer Web-Angriffsfläche. Weiterhin werden im Rahmen des Sofortprogramms CyberGovSecure den Behörden der Bundesverwaltung mehrere Maßnahmen angeboten, um ihre Cybersicherheit und -resilienz zu stärken (vgl. Beratung für Bund, Länder, Kommunen, Justiz und Politik).

2.5 Mail-Angriffsflächen der Bundesverwaltung

Abbildung 2-25: Aktive E-Mail-Adressen der Bundesverwaltung
Einheit: 2021=100 (Messzahl)



Quelle: BSI

E-Mail-Adressen sind Angriffsfläche unter anderem für Phishing- und Malware-Angriffe. Sie sind damit eines der Hauptziele für Cyberangriffe. Im Berichtszeitraum umfasste die Angriffsfläche in den Netzen des Bundes für derartige Angriffe durchschnittlich täglich 727.000 E-Mail-Adressen. Die Messzahl über die Mail-Angriffsfläche der Bundesverwaltung lag im Berichtszeitraum bei durchschnittlich 114 Punkten und somit sieben Indexpunkte höher als im vergangenen Berichtszeitraum.

Weitere Angriffsflächen aus dem Bereich digitale Kommunikationswege sind Accounts auf Social Media, bei Messenger-Diensten und Mobilfunknummern. Angreifer nutzten diese Wege ähnlich wie E-Mails: zur Verbreitung ungezielter Massenangriffe mit Schadcode, für Social Engineering oder auch Phishing ebenso wie für gezielte Angriffe wie Spear-Phishing. So umfasste allein die Angriffsfläche offizieller Accounts von Bundesbehörden auf Social-Media-Plattformen rund 1.500 Accounts.

Digitale Kommunikationswege sind zudem nicht an bestimmte Gerätetypen gebunden, sondern können beispielsweise vom PC ebenso wie vom Smartphone, oder vom privaten Gerät ebenso wie vom Dienstlaptop aus genutzt werden. Das Management der Angriffsflächen wird dadurch erheblich verkompliziert und der Schutz komplexer Nutzungsszenarien ist eine Herausforderung.

Ausgewählte Vorfälle: Angriffsfläche
Erfolgreiche Angriffe auf Systeme zur Verwaltung mobiler Endgeräte mittels Ausnutzung von Zero-Day-Schwachstellen

Sachverhalt

Am Abend des 29. Januar 2026 veröffentlichte der Softwarehersteller Ivanti ein Advisory zu zwei kritischen Schwachstellen in seinem Produkt Endpoint Manager Mobile (EPMM). EPMM-Systeme dienen zur zentralen Konfiguration und Administration mobiler Geräte und können sensible Informationen wie z. B. Rufnummern, Gerätenamen oder Sicherheitseinstellungen enthalten. Die Schwachstellen erlaubten einem entfernten, nicht-authentifizierten Angreifer die Ausführung von Code - auch Schadcode. Am 30. Januar 2026 wurde ein Proof-of-Concept zur Ausnutzung der Schwachstellen bekannt.

Das BSI griff das Thema in einer Sicherheitsmitteilung auf und stellte konkrete Empfehlungen zu Detektion und Umgang mit den Schwachstellen zur Verfügung. Zur Unterstützung bei der Detektion von Angriffen entwickelte und veröffentlichte Ivanti in Zusammenarbeit mit dem niederländischen Nationaal Cyber Security Centrum (NCSC-NL) ein Erkennungsskript, mit dem potenziell betroffene Systeme auf Kompromittierung untersucht werden konnten.

Bewertung

Angreifer hatten die Schwachstellen bereits vor Veröffentlichung am Abend des 29. Januar 2026 ausgenutzt waren in verwundbare Systeme auch in Deutschland eingedrungen. Die Angreifer gingen dabei sehr professionell vor. Sie installierten eine sogenannte Reverse Shell zum fortgesetzten Zugriff auf die Systeme und bereinigten Logdateien von den eigenen Angriffsspuren. In einigen untersuchten Fällen konnte das BSI einen Abfluss von Daten aus den betroffenen EPMM-Systemen bestätigen bzw. nicht ausschließen.

Reaktion

Betroffenen Organisationen empfahl das BSI, die kompromittierten EPMM-Systeme entweder über ein sicheres Backup in einen einwandfreien Zustand zurückzusetzen oder eine Neuinstallation durchzuführen. Alle mit der betroffenen Anwendung verbundenen Zugangsdaten sollten ausgetauscht werden. Wichtig war, nach der Wiederherstellung ein Update auszuführen, um die Schwachstellen zu schließen. Aus präventiver Sicht ist es grundsätzlich wichtig, Angriffsflächen (insbesondere von aus dem öffentlichen Internet erreichbaren Systemen) bestmöglich zu schützen und zu minimieren.

Ausgewählte Vorfälle: Angriffsfläche
Schwachstellen in KI-Agentensystem OpenClaw

Sachverhalt

Das Open-Source-Projekt OpenClaw ist ein lokal laufendes KI-Agenten-Framework. Es ermöglicht die Installation eines teilautonom agierenden KI-Agenten, der Anweisungen ausführt und abhängig von Konfiguration und Integration weitreichende Systemrechte sowie Zugriff auf Schlüssel und Passwörter für diverse Dienste, KI-Modelle, Websites, Kreditkarten, soziale Netzwerke usw. erhalten kann.

OpenClaw hat am 31. Januar 2026 ein Advisory zu einer schwerwiegenden Schwachstelle (CVE-2026-25253) veröffentlicht, die Codeausführung aus der Ferne ermöglicht. Betreibern von OpenClaw wird empfohlen, die Software aktuell zu halten, um Schwachstellen schnellstmöglich zu schließen, sowie die Erreichbarkeit aus dem Internet einzuschränken. Am 16. Februar 2026 berichtete das Sicherheitsunternehmen Hudson Rock, dass erstmals Konfigurationsdateien des KI-Agenten OpenClaw durch Infostealer-Schadsoftware entwendet wurden. Dabei handelte es sich nicht um eine gezielte Kompromittierung von OpenClaw selbst, sondern um eine Malware-Infektion auf den betroffenen Systemen. Die Schadsoftware durchsuchte automatisiert kompromittierte Systeme nach Dateien mit Begriffen wie "token" oder "private key" und

entwendete unter anderem die Dateien openclaw.json, device.json sowie persistente Speicherdateien. Auf diese Weise konnten Authentifizierungs-Token und kryptografische Schlüssel abgegriffen werden, was potenziell eine vollständige digitale Identitätsübernahme ermöglicht.

Bewertung

KI-Agenten werden zunehmend zum Angriffsziel, weil sie sensible Zugangsdaten und umfassende Kontextinformationen bündeln. KI-Agenten und -Frameworks sind eine noch relativ neue und unerprobte Technologie, die durch ihre tiefgehende System-Integration und umfangreiche Zugriffsrechte auf lokale Daten ein hohes Sicherheitsrisiko darstellen. Es handelt sich oft um unzureichend getestete, teils fehlerhafte Software.

Reaktion

Aufgrund von Schwachstellen, Konflikten mit Sicherheitsregeln und Sicherheitskonzepten, von potentiellem Datenabfluss und Datenschutzverstößen sollte OpenClaw nur experimentell und nicht auf Produktiv-Systemen und Produktiv-IT-Netzen verwendet werden. Organisationen sollten klare Regeln für das Personal vorgeben und gegebenenfalls die Nutzung von OpenClaw untersagen. Zudem ergeben sich Gefahren bei der Nutzung von OpenClaw als nicht genehmigte „Schatten-IT“.

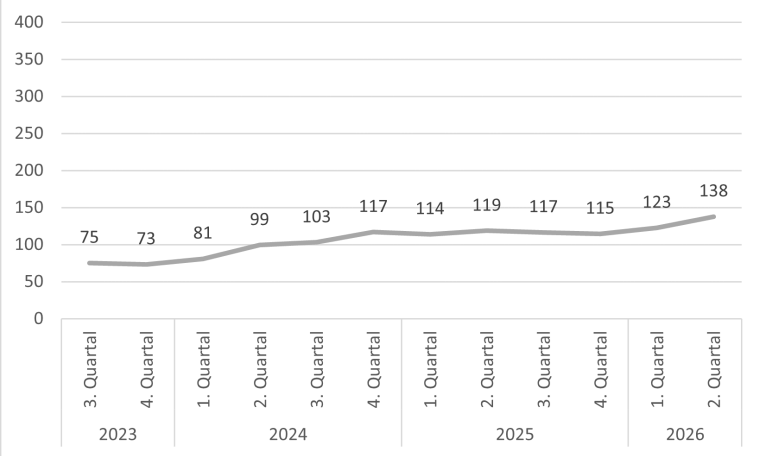
Falls OpenClaw nach Risikoabwägung dennoch verwendet wird, so müssen zumindest aktuelle Updates installiert und die Best Practices des Herstellers befolgt werden. Zusätzlich sollten folgende technische Sicherheitsmaßnahmen berücksichtigt werden: Einsatz von isolierten Umgebungen (z. B. Container, virtuelle Maschinen oder Sandboxes), System- und API-Zugriffe sollten nur im für die Aufgabenstellung erforderlichen Umfang gewährt werden, sichere Verwaltung sensibler Zugangsdaten statt Speicherung im Klartext, Einschränkung von Netzwerkzugriffen und externen API-Aufrufen, Aktivierung von Logging und Monitoring zur Erkennung ungewöhnlicher Agenten-Aktivitäten sowie regelmäßige Sicherheitsüberprüfungen der verwendeten Workflows und Plugins.

3 Gefährdungslage

Über alle Angriffsarten hinweg betrachtet ist die Gefährdung durch Cyberangriffe im aktuellen Berichtszeitraum gestiegen, zuletzt auf 138 Punkte (vgl. Abbildung 3-1). Der Attack-Score über die Gefährdungslage legte damit im Berichtszeitraum insgesamt 9 % zu. Dabei war das Wachstum ganz überwiegend auf Exploitation-Angriffe zurückzuführen. Mit solchen Angriffen nutzen Cyberakteure Schwachstellen in aus dem Internet erreichbaren Systemen aus, um Netzwerke zu infiltrieren und Daten zu verschlüsseln oder auszuleiten. Während andere Arten ungezielter Massenangriffe (vgl. Angriffe mittels digitaler Kommunikationswege auf die Bundesverwaltung) und auch gezielte Cyberspionage- und Cybercrimeangriffe (vgl. Gefährdungslage nach Angreifermotivation) auf weitgehend konstantem Niveau verharrten, sprang die Messzahl für Exploitation-Angriffe sehr deutlich um 48 % auf 133 Punkte (vgl. Angriffe auf Web-Angriffsflächen).

3.1 Attack Score

Abbildung 3-1: Attack Score
Einheit: 2024=100



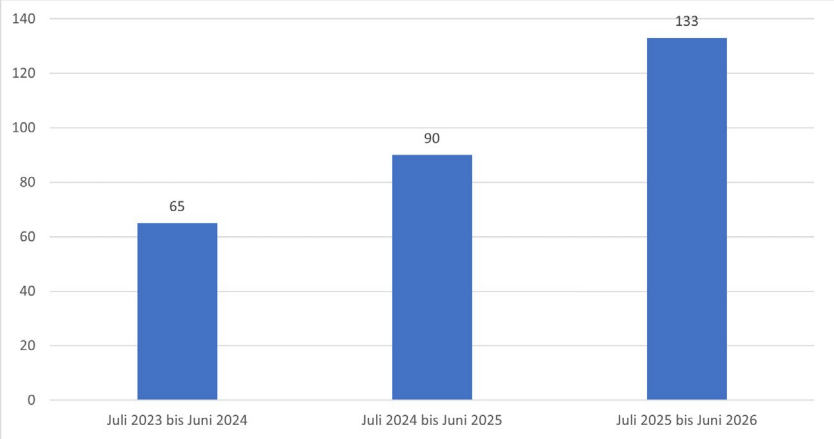
Quelle: BSI

Der Attack Score ist eine normierte Kennzahl über die Gefährdungslage in Deutschland. Es fließen sowohl Daten speziell über Deutschland ein als auch über weltweite Entwicklungen, die für Deutschland Relevanz haben bzw. teilweise sogar direkt auf Deutschland übertragbar sind. Der Attack Score ist Teil des BSI Cyber Index.

Im aktuellen Berichtszeitraum lag der Attack Score bei durchschnittlich 123 Punkten. Damit lag die Kennzahl 9 % über dem Niveau des vergangenen Berichtszeitraums. Die spürbare Zunahme der Gefährdungen rührte insbesondere von Exploitation-Angriffen her (vgl. Exploitation-Angriffe). Hier war im aktuellen Berichtszeitraum ein erheblicher Zuwachs von 48 % zu verzeichnen.

3.2 Gefährdungslage nach Angriffsarten

Abbildung 3-2: Exploitation-Angriffe am MADCAT-Honeypot
Einheit: 2023=100 (Messzahl)



Quelle: Exploitation-Statistik

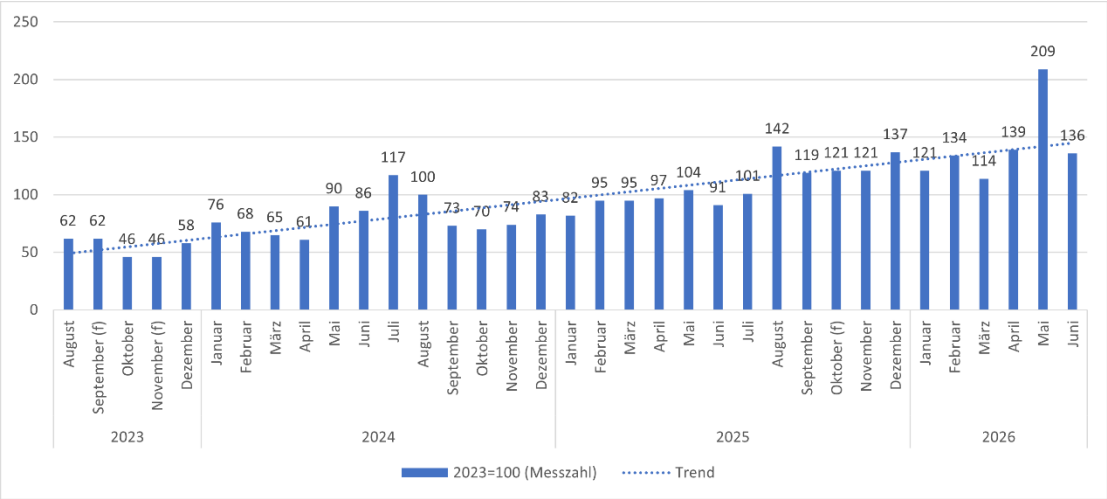
Exploitation, das heißt das Ausnutzen von Schwachstellen in Web-Angriffsflächen, kennt seit Jahren nur eine Richtung: aufwärts. Die Messzahl kletterte im aktuellen Berichtszeitraum auf durchschnittlich 133 Punkte (vgl. Abbildung 3-2). Das war ein Zuwachs von 48 % im Vergleich zum vergangenen Berichtszeitraum. Damals hatte der Indikator bei durchschnittlich 90 Punkten gelegen, was bereits einem Zuwachs um 38 % gegenüber dem vorangegangenen Berichtszeitraum entsprochen hatte. Dabei wurden Sondereffekte durch eine ungewöhnlich ausgeprägte, herausgehobene Angriffskampagne im Oktober 2025 bereits herausgerechnet.

→ Mehr über die Gefährdungslage nach Angriffsarten

3.2.1 Angriffe auf Web-Angriffsflächen

3.2.1.1 Exploitation-Angriffe

Abbildung 3-3: Exploitation-Angriffe am MADCAT-Honeypot
Einheit: 2023=100 (Messzahl)



Quelle: Exploitation-Statistik
Bemerkung: Sondereffekte im September und November 2023 sowie im Oktober 2025 bereinigt.

Exploitation-Angriffe nehmen seit Jahren stetig zu (plus 48 % im aktuellen gegenüber dem vergangenen Berichtszeitraum), denn im Vergleich etwa zu Mail-Angriffsflächen stellen

Schwachstellen in aus dem Internet erreichbaren Systemen eine verbreitet schlecht geschützte Angriffsfläche dar (vgl. dazu beispielsweise Neue Schwachstellen). Darüber hinaus werden Angreifer immer schneller, wenn es um das Identifizieren von offen bzw. falsch konfigurierten Servern oder schwachstellenbehafteten Systemen im Internet geht. Die Time-to-Exploit, ein Indikator, der den durchschnittlichen Zeitraum zwischen dem Bekanntwerden einer Schwachstelle und dem ersten Angriff darauf misst, sank im aktuellen Berichtszeitraum auf durchschnittlich 25 Tage, im 2. Quartal 2026 sogar auf 8 Tage (vgl. Time-to-Exploit). Ein wirksames, möglichst weitgehend automatisiertes Angriffsflächenmanagement (vgl. Des Weiteren ist das BSI aktiv in der CRA Expert Group vertreten, um zusammen mit seinen Partnerbehörden und Organisationen der europäischen Wirtschaft, Zivilgesellschaft und ausgewählten Expertinnen und Experten Fragestellungen des CRA zu konkretisieren und den CRA weiterzuentwickeln. Mit der aktiven Teilnahme an der Notifying Authorities Group, dem zentralen Koordinierungsgremium der Notifizierenden Behörden, setzt sich das BSI zudem für eine europäisch harmonisierte und qualitativ angemessene Konformitätsbewertungsinfrastruktur für den CRA ein.

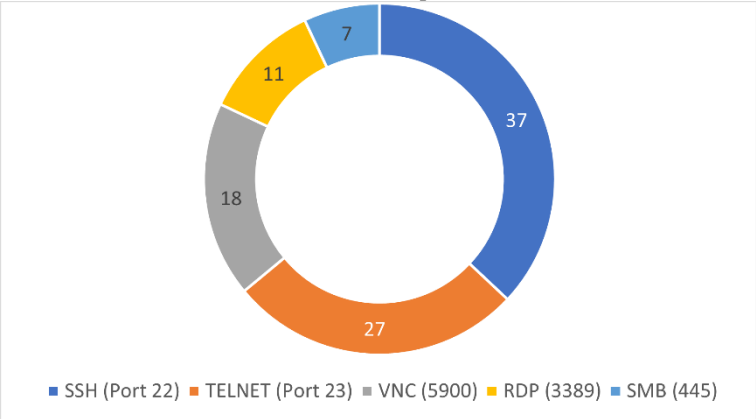
LLMs als Hochgeschwindigkeits-Schwachstellenscanner) ist daher mehr denn je geboten. Das BSI unterstützt mit dem Warn- und Informationsdienst (vgl. Warn- und Informationsdienst).

→ Mehr über Exploitation-Angriffe

Angriffe auf die Vertraulichkeit und Integrität von Internetdiensten werden unter anderem mit Schwachstellen-Exploits durchgeführt. Sie werden von staatlich gesteuerten Cyberspionage-Gruppen (vgl. Angreifergruppen) ebenso eingesetzt wie von Cyberkriminellen, die für andere Gruppen zum Beispiel Ransomware-as-a-Service (vgl. Cybercrime-Gruppen) anbieten.

Im aktuellen Berichtszeitraum deuten die am BSI MADCAT-Honeypot erfassten Angriffsversuche auf eine unverändert angespannte Gefährdungslage durch Angreifer hin, die Schwachstellen in Web-Angriffsflächen ausnutzen. Nicht nur lagen für fast alle Monate des aktuellen Berichtszeitraums die Angriffszahlen über den Monatswerten des vergangenen Berichtszeitraums. Auch der Trend zeigt jenseits monatlicher Schwankungen eine eindeutige Richtung: weitere 48 % Zuwachs im aktuellen Berichtszeitraum (vgl. Abbildung 3-2).

Abbildung 3-4: Exploitation-Angriffe Juli 2025 bis Juni 2026 nach ausgenutztem Protokoll (Top 5)
Einheit: Anteile in Prozent an den Top-5-Protokollen



Quelle: Exploitation-Statistik

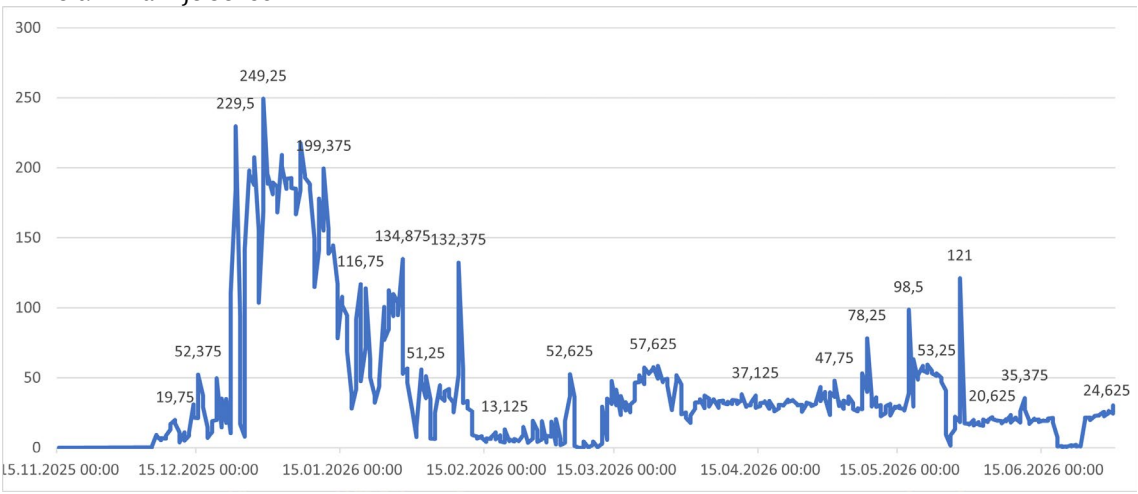
Dabei waren leichte Strukturveränderungen zu beobachten. Unter den Top 5 der ausgenutzten Protokolle stach zwar erneut Port 22 hervor, welcher in der Regel durch das SSH-Protokoll genutzt wird. Mit 37 % der im aktuellen Berichtszeitraum am BSI-Honeypot beobachteten Exploitation-Angriffe (vgl. Abbildung 3-4) war jedoch ein deutlicher Rückgang des Anteils zu verzeichnen (minus 16 Prozentpunkte). SSH dient dazu, sichere Verbindungen in unsicheren Netzwerken wie etwa dem Internet herzustellen, und kommt daher beispielsweise für Account-Logins zum Einsatz. Typisch für Angriffe gegen diesen Port sind etwa

Brute-Force-Angriffe. Hierbei probieren die Angreifer an einem im Internet zufällig gefundenen SSH-Port automatisiert Listen von gängigen, schwachen, weitverbreiteten oder auch errechneten Nutzernamen und Passwörtern aus. Schwach geschützte Accounts oder falsch konfigurierte Server fallen solchen Angriffen leicht zum Opfer, und die steigende Leistungsfähigkeit von KI-Angriffswerkzeugen wird auch Brute-Force-Angriffe beschleunigen und zunehmend erfolgreich machen. Mit RDP und VNC befinden sich auch wieder zwei Protokolle zur Fernwartung in den Top 5, was erneut unterstreicht, dass besondere Vorsicht bei der Exposition von Diensten, welche primär zur Nutzung in geschützten Netzwerkbereichen ausgelegt sind, geboten ist (vgl. Abbildung 3-4).

React2Shell

Exemplarisch für die Durchführung von Exploitation-Angriffen war die Ausnutzung der Schwachstelle React2Shell, auch bekannt als CVE-2025-55182 (ebenfalls bekannt unter CVE-2025-66478), welche mit der höchsten CVSS-Bewertung 10.0 bewertet wurde.

Abbildung 3-5: Durchschnittliche Exploitation-Angriffe auf die React2Shell-Schwachstelle
Einheit: Anzahl je Sensor



Quelle: Exploitation-Statistik

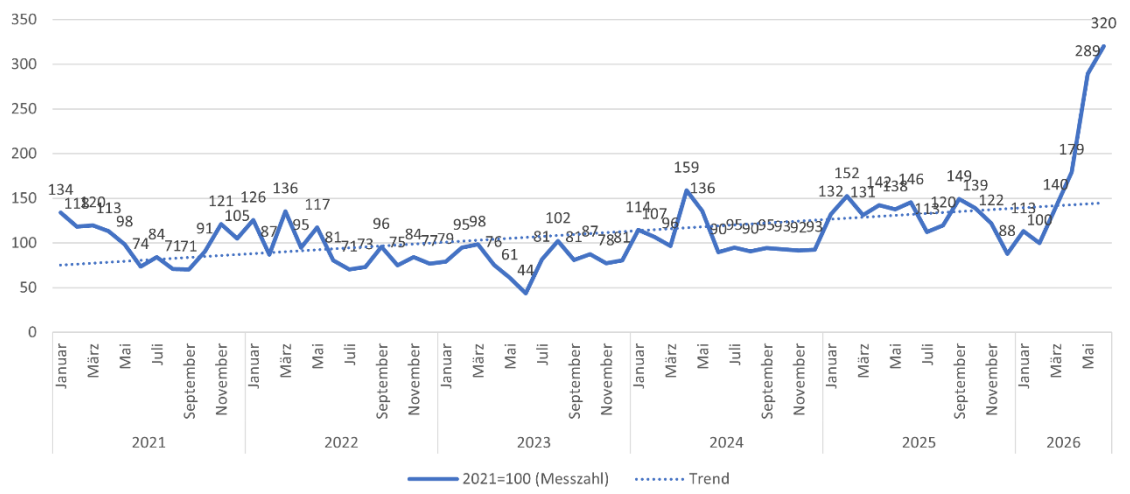
Die Schwachstelle ermöglicht es Angreifern, mit Hilfe von Exploits in den React-Server-Komponenten serverseitige Prozesse zu übernehmen. Somit können manipulierte Daten, die Befehle der Angreifer enthalten, eingeschleust werden, welche dann zur Ausführung gelangen. Angriffswellen begannen nur wenige Stunden nach dem Bekanntwerden eines Proof of Concept am 4. Dezember 2025, der die Ausnutzbarkeit der Schwachstelle bestätigte (vgl. Abbildung 3-5). Anschließend folgte eine Phase verstärkter Ausnutzung. Danach flachte die Kurve zwar ab, die Gefährdung hält jedoch weiterhin an.

Die Sicherheitsrelevanz einer solchen Schwachstelle ist hoch, da diese eine so genannte Remote Code Execution ohne Authentifizierung ermöglicht. In der Folge wirkte das BSI unter anderem durch Warnungen weiter darauf hin, dass Betreiber ihre Systeme prüfen und absichern.

3.2.1.2 DDoS-Angriffe

Abbildung 3-6: Bekannt gewordene DDoS-Angriffe in Deutschland

Einheit: 2021=100 (Messzahl)



Quelle: DDoS-Statistik

Im aktuellen Berichtszeitraum setzte sich der Trend zu mehr DDoS-Angriffen weiter fort (plus 34 % im Vergleich zum vergangenen Berichtszeitraum). Insbesondere im 2. Quartal 2026 kam es zu einem weit überdurchschnittlichen Zuwachs. Die Messzahl über die bekannt gewordenen DDoS-Angriffe in Deutschland erreichte im Juni 320 Punkte und lag damit 208 % über dem langjährigen Durchschnitt (Januar 2021 bis April 2026, vgl. Abbildung 3-6). Auffällig war, dass die zusätzlichen DDoS-Angriffe ausschließlich unter Missbrauch deutscher infizierter Systeme ausgeführt wurden. Hintergrund könnten daher sogenannte Residential Proxy Botnetze sein, mit denen Angreifer ihre Angriffsaktivitäten über regionale infizierte Systeme umleiten, um auf diese Weise GEO-IP-basierte Detektionsmethoden zu unterwandern. Auch die für die Angriffe verwendete durchschnittliche Bandbreite lag teils deutlich über dem langjährigen Durchschnitt (vgl. Abbildung 3-7).

Eine Liste qualifizierter DDoS-Mitigationsdienstleister hält das BSI bereit.

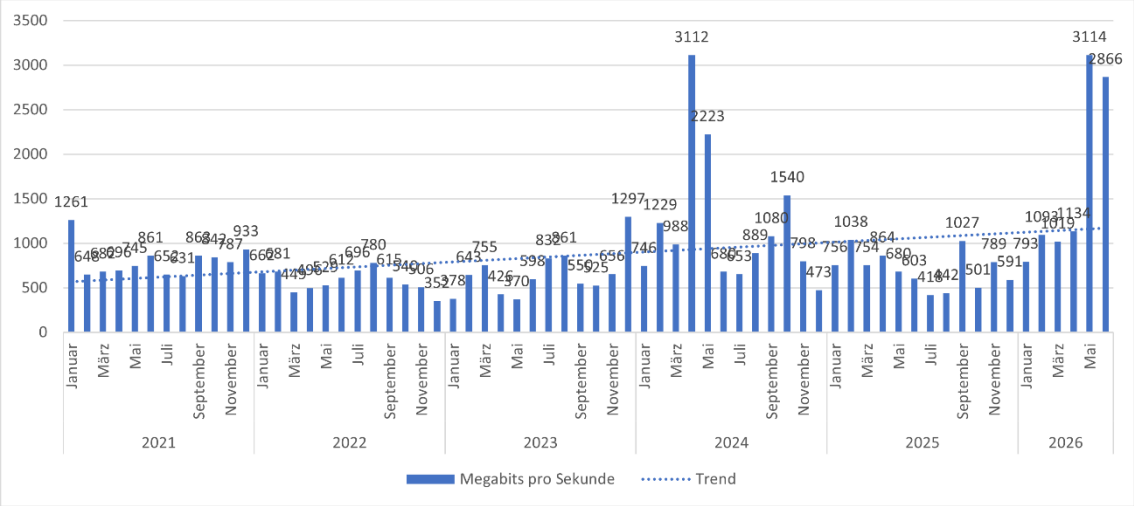
→ Mehr über DDoS-Angriffe

Angriffe auf die Verfügbarkeit von Internetdiensten werden mit darauf spezialisierten Botnetzen durchgeführt (vgl. Botnetze) und als Distributed-Denial-of-Service-Angriff (DDoS-Angriff) bezeichnet. Durch das Überfluten von (Web-)Servern mit Anfragen sind zum Beispiel Websites nicht mehr erreichbar. Das Ziel der Angreifer besteht darin, die angegriffenen Dienste oder Anwendungen so weit zu überlasten, dass diese lahmgelegt werden.

Im aktuellen Berichtszeitraum kam es nach einer zunächst durchschnittlichen DDoS-Gefährdungslage dann im 2. Quartal 2026 zu teils drastischen Anstiegen sowohl der Angriffszahlen (vgl. Abbildung 3-6) wie auch der für die Angriffe verwendeten Bandbreiten. So lagen die durchschnittlichen Bandbreiten insbesondere im Mai und Juni 2026 mit 3.114 Megabits pro Sekunde bzw. 2.866 Megabits pro Sekunde sogar noch über den vormaligen Rekordwerten vom April und Mai 2024 (vgl. Abbildung 3-7). Hintergründe zu diesen ungewöhnlichen Entwicklungen waren zum Redaktionsschluss dieses Berichts noch nicht bekannt, könnten unter anderem. jedoch auf sogenannte Residential-Proxy-Botnetze zurückzuführen sein. Angreifer nutzen sie, um Cyberangriffe über Systeme in regionaler Nähe des Ziels umzuleiten und GEO-IP-basierte Detektion zu erschweren.

Abbildung 3-7: Durchschnittliche Bandbreite aller bekannt gewordenen DDoS-Angriffe in Deutschland

Einheit: Megabits pro Sekunde



Quelle: DDoS-Statistik

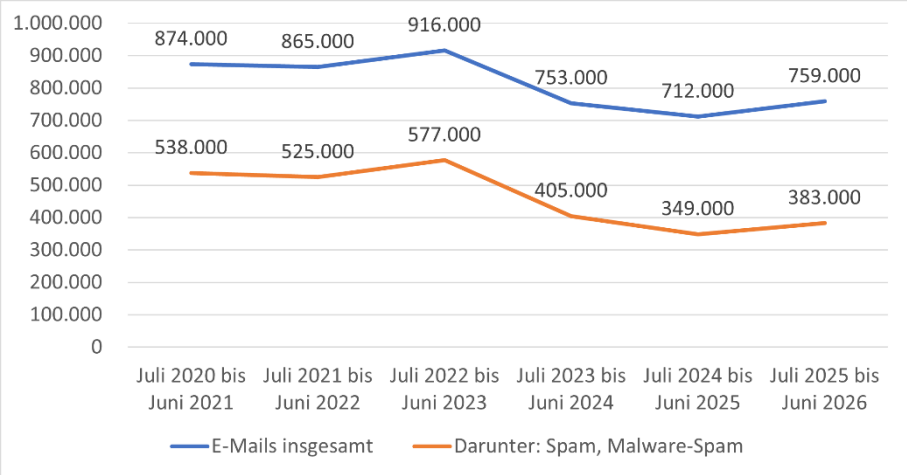
DDoS-Angriff auf die Deutsche Bahn

Am 17. Februar 2026 kam es bei der Deutschen Bahn zu einem groß angelegten DDoS-Angriff mit erheblichem Ausmaß. Nutzerinnen und Nutzer der DB-Navigator-App erhielten beim Suchen und Buchen von Verbindungen wiederholt Fehlermeldungen und konnten in einigen Fällen weder ihre BahnCard-Daten aktualisieren noch bereits gebuchte Tickets einsehen. Die Störung hielt bis in den Vormittag des Folgetages an, bevor Mitigationsmaßnahmen Wirkung zeigten.

3.2.2 Angriffe mittels digitaler Kommunikationswege auf die Bundesverwaltung

3.2.2.1 Spam-E-Mails gegen die Bundesverwaltung

Abbildung 3-8: Durchschnittliche tägliche E-Mails und Spam-E-Mails an die Bundesverwaltung
Einheit: Anzahl



Quelle: Erhebung über den E-Mail-Verkehr mit der Bundesverwaltung
Bemerkung: Ohne Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen.

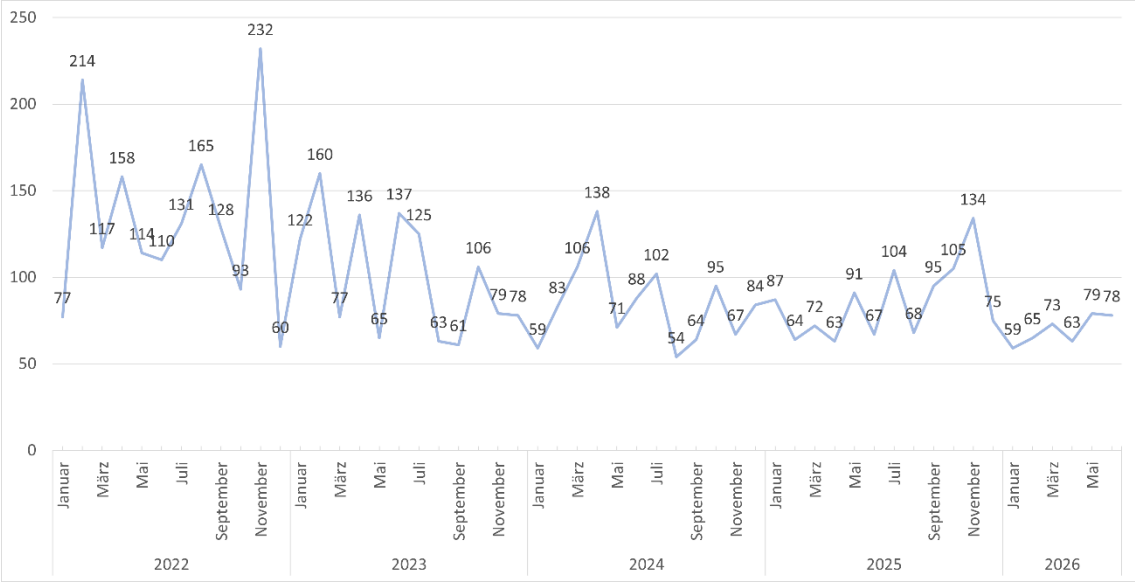
Im Berichtszeitraum gingen durchschnittlich täglich 759.000 E-Mails in den Regierungsnetzen ein, darunter durchschnittlich täglich 383.000 Spam-Mails (vgl. Abbildung 3-8). Die tägliche Spam-Quote lag damit bei durchschnittlich 50 % und damit nahezu unverändert auf dem Niveau des vergangenen Berichtszeitraumes. Die Regierungsnetze sind eines der größten zusammenhängenden Netze in Deutschland und bieten daher ein repräsentatives Beispiel für den E-Mail-Verkehr in Deutschland insgesamt. Trends und Spam-Anteile in den Netzen des Bundes können daher vergleichbar auch im öffentlichen Internet insgesamt auftreten.

→ Mehr über Spam

Spam-Mails

Das Mittel des täglichen Spam-Mail-Index, der das Aufkommen und die Entwicklung von Spam-Mails am zentralen Spam-Filter der Regierungsnetze misst, lag im Durchschnitt bei 83 Punkten und damit 9 % über dem Vergleichswert des vergangenen Berichtszeitraums.

Abbildung 3-9: Spam-Mail-Index für die Bundesverwaltung
Einheit: 2018=100 (Messzahl)

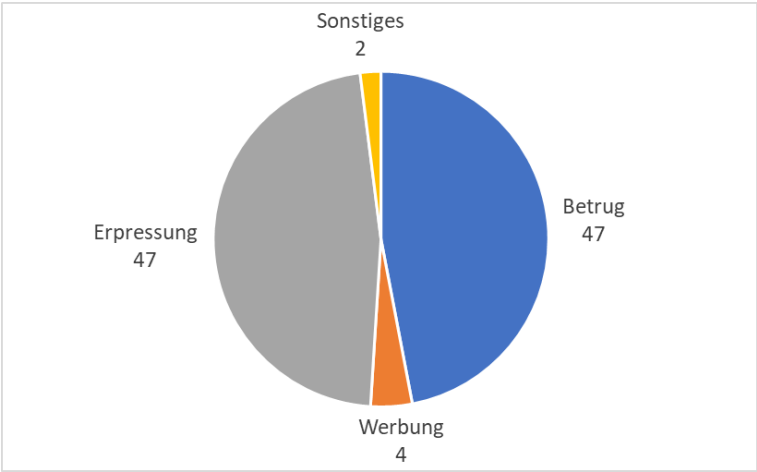


Quelle: Erhebung über den E-Mail-Verkehr mit der Bundesverwaltung
Bemerkung: Ohne Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen.

Ursache hierfür war eine einzelne, ausgeprägte Spam-Kampagne im November 2025, die die Messzahl in diesem Monat auf durchschnittlich 134 Punkte und an einzelnen Tagen sogar auf über 200 Punkte hochschnellen ließ. Ohne diesen Sondereffekt wäre das durchschnittliche Spam-Mailaufkommen insgesamt auf nahezu unverändertem Niveau geblieben.

Rund 94 % der Spam-Mails waren Cyberangriffe wie erpresserische (47 %) oder betrügerische E-Mails (47 %, vgl. Abbildung 3-10). Mit erpresserischen E-Mails drohen Angreifer, vermeintlich kompromittierendes Wissen über das Opfer an dessen Kontakte weiterzugeben, und fordern ein Schweigegeld. Entgegen ihrer Behauptung besitzen die Angreifer aber weder kompromittierende Informationen über die Angegriffenen noch verfügen sie über deren Kontakte, um das vermeintliche Wissen an diese weiterzugeben.

Abbildung 3-10: Spam-Mails von Juli 2025 bis Juni 2026 nach Art des Spams
Einheit: Anteile in Prozent



Quelle: Erhebung über den E-Mail-Verkehr mit der Bundesverwaltung

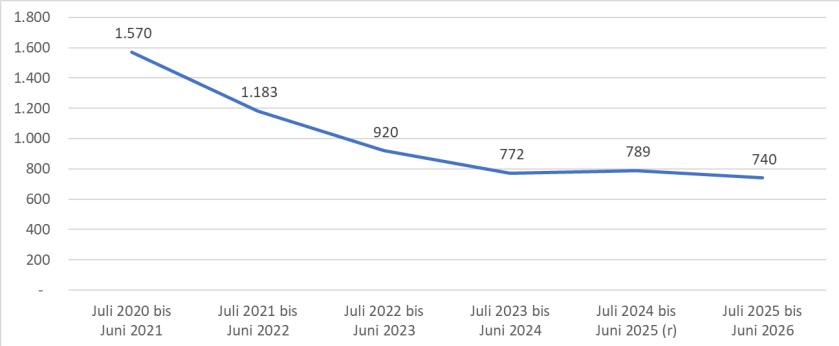
Unter den betrügerischen E-Mails machten Phishing-Mails mit 98 % den größten Anteil aus. Mehrheitlich handelte es sich dabei um sogenanntes Finance Phishing. Dieses täuscht vor, dass die Mail von Banken, Finanzdienstleistern, Online-Shops oder Zahlungsdienstleistern stammt, und

fordert die Angegriffenen etwa zu einer vermeintlich nötigen Kontoverifizierung auf oder zu einer Zahlung vermeintlicher Mahngebühren wegen angeblich nicht bezahlter Rechnungen.

3.2.2.2 Malware-Angriffe per E-Mail auf die Bundesverwaltung

Abbildung 3-11: Durchschnittliche tägliche Malware-Angriffe per E-Mail auf die Bundesverwaltung

Einheit: Anzahl



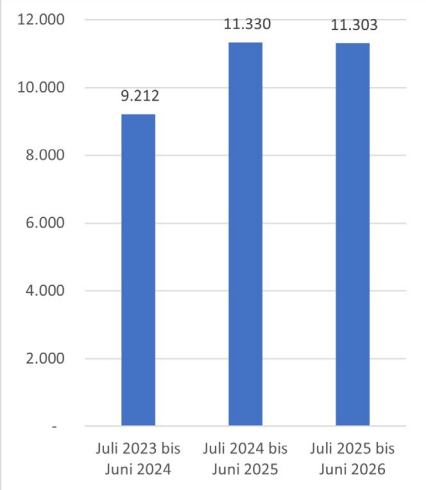
Quelle: Erhebung über den E-Mail-Verkehr mit der Bundesverwaltung
Bemerkung: Ohne Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen. r: Wert berichtigt.

Neben Spam richten Angreifer auch ungezielte Malware-Angriffe gegen die E-Mail-Adressen in den Regierungsnetzen. Solche E-Mails transportieren Malware direkt im Anhang. Ziel der Angreifer ist es, die Empfängerinnen und Empfänger zum Öffnen des Anhangs zu bewegen, um dadurch eine Malware auf dem System der Angegriffenen zu installieren. Im aktuellen Berichtszeitraum erreichten die Regierungsnetze durchschnittlich täglich 740 maliziöse E-Mails (vgl. Abbildung 3-11). Das waren 6 % weniger als im vergangenen Berichtszeitraum.

3.2.2.3 Zugriffsversuche aus der Bundesverwaltung auf schadcodebehaftete Server

Abbildung 3-12: Durchschnittliche tägliche Zugriffsversuche aus der Bundesverwaltung auf schadcodebehaftete Server

Einheit: Anzahl



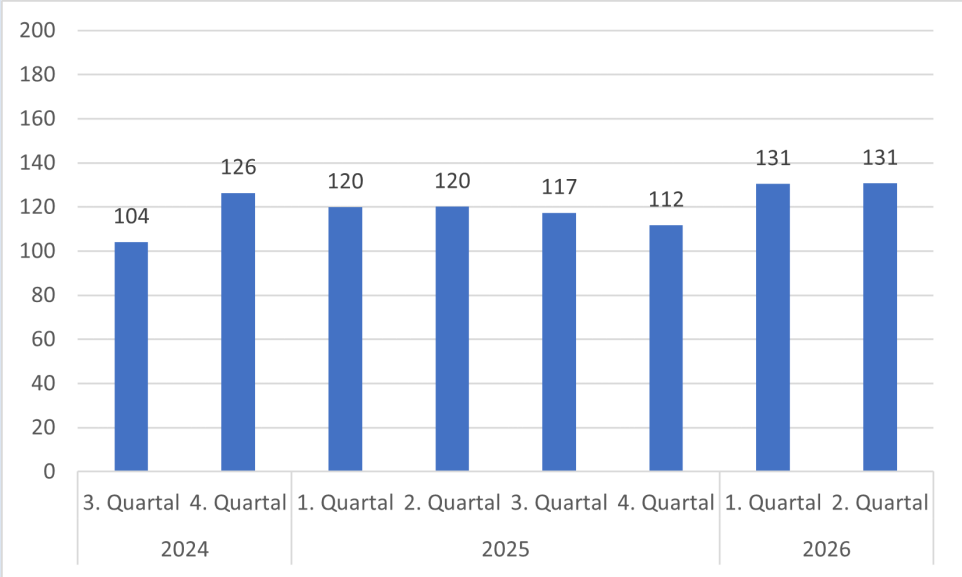
Quelle: BSI

Durchschnittlich täglich 11.303 Zugriffe aus der gesamten Bundesverwaltung auf potenziell maliziöse Websites und Webserver hat das BSI im Rahmen der zentralen Schutzmaßnahmen für die Bundesverwaltung im aktuellen Berichtszeitraum blockiert (vgl. Zugriffsversuche aus der Bundesverwaltung auf schadcodebehaftete Server

Abbildung 3-12). So wird zum Beispiel der Zugriff auf Schadprogramme verhindert, die sich hinter Download-Links verstecken. Diese Links werden von Cyberangreifern im Rahmen von Social-Engineering-Kampagnen über E-Mail, soziale Medien oder Websites verbreitet.

3.3 Gefährdungslage nach Angreifermotivation

Abbildung 3-13: Aktivitätsniveau von Angreifergruppen weltweit
Einheit: 2024=100 (Messzahl)



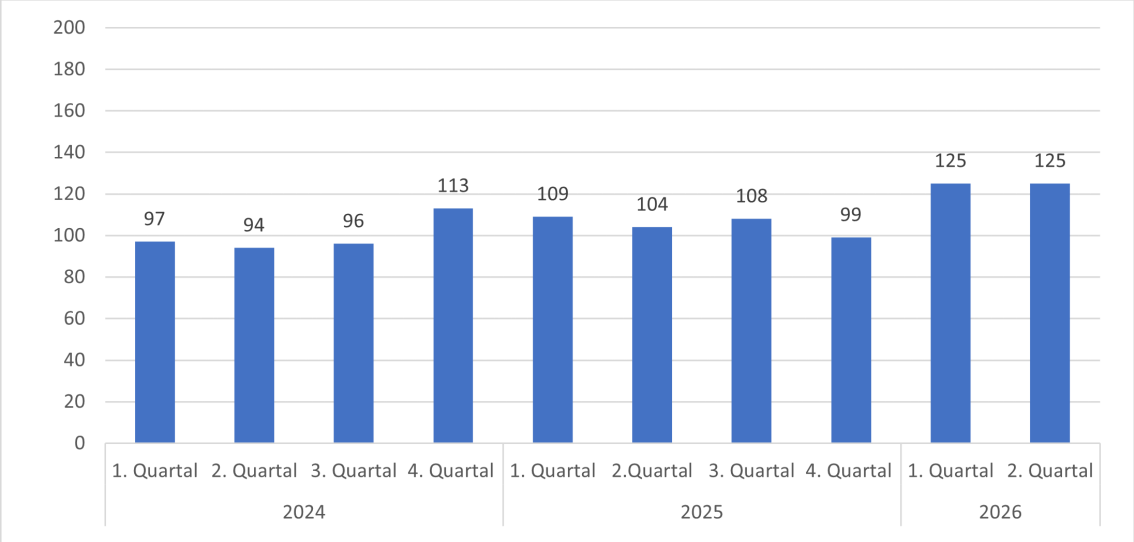
Quelle: Aktivitätsniveaustatistik

Cyberakteure wiesen im aktuellen Berichtszeitraum weltweit eine ähnlich hohe Aktivität auf wie im vergangenen Berichtszeitraum. Der Indikator über das Aktivitätsniveau von Angreifergruppen lag im aktuellen Berichtszeitraum bei durchschnittlich 123 Punkten. Dabei waren leichte Schwankungen zu verzeichnen, die den Indikator im 1. Halbjahr 2026 auf 131 Punkte trieben (vgl. Abbildung 3-13) und insbesondere auf verstärkte Aktivitäten von Cybercrime-Gruppen zurückzuführen waren. In Deutschland fiel im aktuellen Berichtszeitraum insbesondere die Gruppe hinter der Leak-Seite SafePay auf - eine Cybercrime-Gruppe, die sich auffallend auf deutsche Ziele konzentrierte (vgl. Leak-Geschädigte).

→ Mehr über die Gefährdungslage nach Angreifermotivation

3.3.1 Cybercrime

Abbildung 3-14: Crime-Aktivitätsniveau
Einheit: 2024=100 (Messzahl)



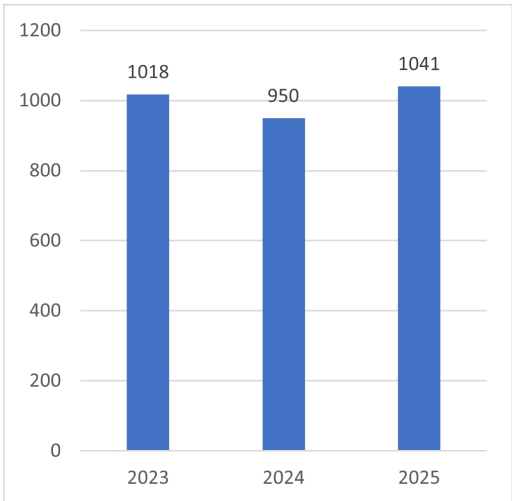
Quelle: Aktivitätsniveaustatistik

Cybercrime-Gruppen waren im aktuellen Berichtszeitraum weltweit deutlich aktiver als im Referenzjahr 2024. Die Aktivitätskennzahl lag bei durchschnittlich 114 Punkten. Im Vergleich zum vergangenen Berichtszeitraum war das ein Zuwachs um 8 %. Auch bei den Polizeien in Deutschland gingen wieder mehr Anzeigen wegen Ransomware-Angriffen ein.

→ Mehr über Cybercrime

Im Jahr 2025 wurden in Deutschland 1.041 Fälle von Ransomware-Angriffen zur Anzeige gebracht (vgl. Bundeslagebild Cybercrime). Dies stellt einen Anstieg um 10 % im Vergleich zum Vorjahr (950 Fälle) dar.

Abbildung 3-15: Anzeigen wegen Ransomware-Angriffen insgesamt
Einheit: Anzahl



Quelle: BKA Bundeslagebild Cybercrime

Das Bundeskriminalamt (BKA) verweist in seinem Bundeslagebild Cybercrime darauf, dass ca. 76 % der Fälle dem Modus Operandi „Double Extortion“ entsprechen, bei dem von dem betroffenen

Unternehmen oder der betroffenen Organisation ein Lösegeld nicht nur für die Entschlüsselung verschlüsselter Daten, sondern zusätzlich dafür verlangt wird, dass exfiltrierte Daten nicht auf sogenannten „Dedicated Leak Sites“ veröffentlicht werden (vgl. Leak-Geschädigte).

Kleine und mittlere Unternehmen (KMU) stehen weiterhin im Fokus der Angreifer. 2025 waren ca. 90 % der betroffenen Unternehmen KMU (2024: ca. 80 %). Der Trend geht somit weiter zu kleineren und potenziell schwächer geschützten Unternehmen und Organisationen. Denn Angreifer gehen den Weg des geringsten Widerstands: Steht der für einen erfolgreichen Angriff erforderliche Aufwand nicht im Verhältnis zum erwarteten Profit (etwa dann, wenn ein potenzielles Ziel gut geschützt und eine Infiltration entsprechend aufwändig wäre), stellt es aus Sicht der Angreifer kein rentables Angriffsziel dar. Angegriffen werden daher nicht etwa bestimmte Branchen oder Umsatzgrößenordnungen von Unternehmen, sondern diejenigen, die es Angreifern am einfachsten machen. Und das waren auch im Jahr 2025 und bis in die Mitte des Jahres 2026 hinein weiterhin die KMU. Somit sollte die Stärkung der Resilienz in den eigenen Systemen- und Softwarelandschaften höchste Priorität haben, um nicht ins Visier der Angreifer zu geraten.

Nachdem 2024 durch Strafverfolgungsmaßnahmen wie „Operation Endgame“ (vgl. Ausgewählte Vorfälle: Resilienz - Operation Endgame) oder „Operation Cronos“ bereits einige Angriffsinfrastrukturen und Cybercrime-Services zerschlagen wurden, konnten hier auch im Jahr 2025 Erfolge verzeichnet werden. So wurden die Ransomware-as-a-service (RaaS) „8Base“ und „BlackSuit“ durch polizeiliche Maßnahmen gezwungen ihre Aktivitäten einzustellen. In Deutschland waren in der Folge die RaaS „Akira“ und „SafePay“ besonders aktiv, um die entstandene Lücke zu schließen (vgl. Cybercrime-Gruppen).

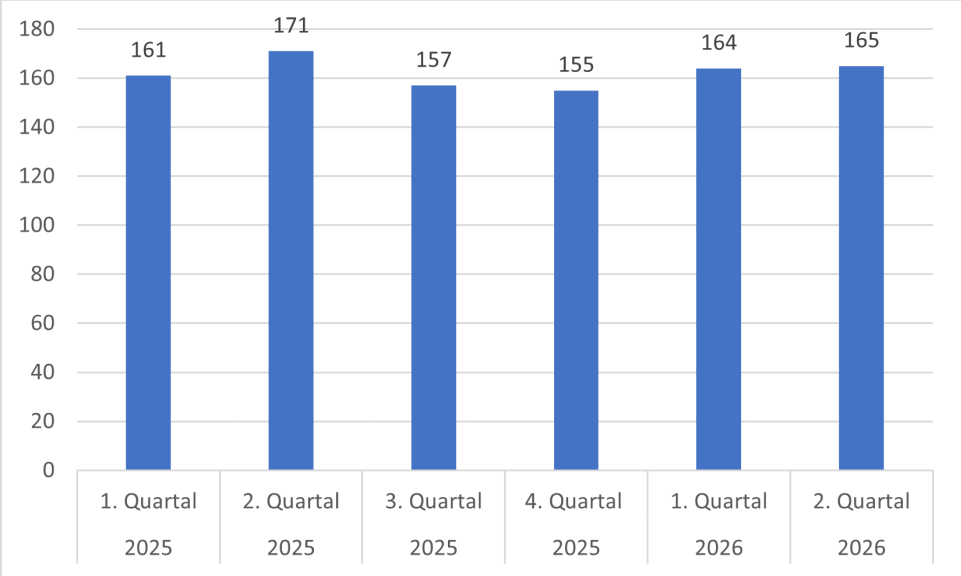
Weiterhin konnten erfolgreiche Maßnahmen gegen die Cybercrime-Handelsplattformen „Nulled“, „Cracked“ und „Archetyp Market“ erzielt werden. Zudem wurden im Zuge von „Operation Endgame 2.0“ und „Operation Endgame 3.0“ über 1.300 täterseitig für kriminelle Aktivitäten genutzte Server abgeschaltet. Die Maßnahmen richteten sich konkret gegen sogenannte Dropper-Schadsoftware, die als Einfallstor für nachfolgende Angriffe dient, sowie gegen Information-Stealer und Fernzugriffstrojaner (Remote Access Trojan, kurz „RAT“).

Zudem konnte in der „Operation Eastwood“ ein aus mehreren hundert Servern bestehendes Botnetz der hacktivistischen Gruppierung „NoName057(16)“ abgeschaltet und internationale Haftbefehle gegen die Verantwortlichen erlassen werden.

Künstliche Intelligenz (KI) bietet Angreifern ein wirksames Werkzeug um ihr Vorgehen zunehmend effizienter zu gestalten. KI bietet viele Möglichkeiten zur Automatisierung und senkt zudem die Einstiegshürden für die Identifizierung von Schwachstellen sowie die Erstellung von Phishing-Texten oder maliziöser Software, wie beispielsweise Exploits für ebensolche Schwachstellen (vgl. LLMs als Hochgeschwindigkeits-Schwachstellenscanner).

3.3.2 Cyberconflict, Cyberspionage

Abbildung 3-16: APT-Aktivitätsniveau
Einheit: 2024=100 (Messzahl)



Quelle: Aktivitätsniveau

Die Angriffsaktivitäten von Cyberspionage-Gruppen bewegten sich im aktuellen Berichtszeitraum weltweit innerhalb üblicher Schwankungen. Die Aktivitätskennzahl für APT-Gruppen lag bei durchschnittlich 160 Punkten und damit nahezu unverändert auf dem Niveau des vergangenen Berichtszeitraums. Neben Angriffen durch Schwachstellenausnutzung kamen auch neue Angriffsvektoren mittels Social Engineering zum Einsatz.

→ Mehr über Cyberspionage

Die Vielfalt der im Berichtszeitraum für Cyberspionage und Cybersabotage verwendeten Angriffsvektoren war hoch. Dagegen spielte ein Vektor, der früher häufig Verwendung fand, inzwischen nahezu keine Rolle mehr: Bis auf wenige Ausnahmen gab es keine client-seitigen Exploits mittels Spearphishing-Anhängen. Das heißt, es wurden kaum Mail-Anhänge verschickt, die Schwachstellen in Bürosoftware ausnutzten. Alle anderen Vektoren wurden von APT-Gruppen bedient:

Social Engineering ist bei E-Mail-basierten Angriffen eine relevante Methode geworden. Ein vergleichsweise neues Phänomen in dieser Kategorie, das sich im aktuellen Berichtszeitraum stark verbreitet hat, ist ClickFix, also das Vorgaukeln von Tests zum Filtern automatisierter Abfragen (Captchas), mit denen Empfängerinnen und Empfänger verleitet werden sollen, Code aus der Zwischenablage auszuführen (vgl. Cybercrime-Gruppen). Daneben bleibt Social Engineering mittels Job- oder Auftragsangeboten über Karriere-Portale oder berufliche soziale Netzwerke weit verbreitet.

Eine weitere Variante von Social-Engineering, die ebenfalls ohne Schwachstellen auskommt, ist die Methode, Archiv-Dateien als Mail-Anhang zu versenden. Diese ZIP- oder RAR-Dateien enthalten Dateitypen, die bei einem Doppelklick unerwünschte Aktionen initiieren. Während Verknüpfungsdateien (mit der Dateiendung .lnk) in diesem Zusammenhang bereits etabliert sind, wurden im aktuellen Berichtszeitraum auch Program Information Files (mit der Dateiendung .pif) und Excel-Web-Query-Dateien (mit der Dateiendung .iqy) gemeinsam mit anderen, legitimen Dateien in Archiven verschickt.

Perimeter-Angriffe (also Angriffe auf Firewalls, VPN-Server und andere Geräte, die direkten Zugang zum Internet haben) gehören inzwischen zum Werkzeugkasten von Cyberspionen, vor allem bei

chinesischen APT-Gruppen. Im Berichtszeitraum galten viele der entdeckten Zero-Day-Exploits (vgl. Neue Schwachstellen) diesen Systemen.

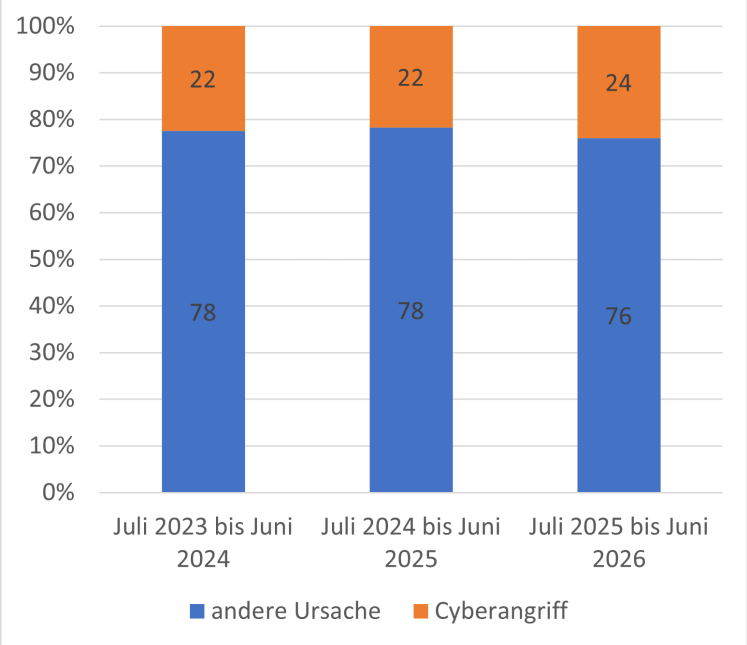
Zudem wurden über E-Mails verstärkt Schwachstellen in Webmailer-Software wie Zimbra, RoundCube und Afterlogic Aurora ausgenutzt. Auch dies ist ein Beispiel für den Trend zu Schwachstellen in Serveranwendungen im Vergleich zu Schwachstellen in Büroanwendungen. Dies war vor allem bei russischen Gruppen wie APT28, GreenCube, GhostWriter und WinterVivern zu beobachten, in geringerem Maße bei asiatischen Gruppen wie SunrisePanda.

Cloudumgebungen wurden häufig über gestohlene Zugangsdaten kompromittiert. Die späteren Angriffsphasen, bei denen unter anderem der langfristige Zugang (Persistenz) gesichert wird, erfolgten dann meist nicht mittels Malware, sondern über legitime Cloudfunktionen bzw. -konfigurationen.

In diesem Zusammenhang ist zu beobachten, dass es sowohl bei russischen und belarussischen als auch bei asiatischen APT-Gruppen spezialisierte Teams gibt, die Zugänge auf Vorrat sammeln. Diese „Access Collection“ genannte Vorgehensweise wird mitunter mit dem Konzept des Prepositioning (vgl. APT-Gruppen, Cyberconflict) vermischt. Vor allem bei Aufdeckung und Veröffentlichung von Zero-Day-Exploits gegen Perimeter-Systeme sind „Compromise first, select later“-Kampagnen zu beobachten. Diese Kompromittierungen werden (ähnlich wie gestohlene Zugangsdaten) über die Zeit gesammelt und bergen ein stetig wachsendes Bedrohungspotenzial.

3.4 Gefährdungslage nach Zielgruppen

Abbildung 3-17: Störungen Kritischer Infrastrukturen nach Störungsursache
Einheit: Anteile in Prozent



Quelle: KRITIS-Meldungen

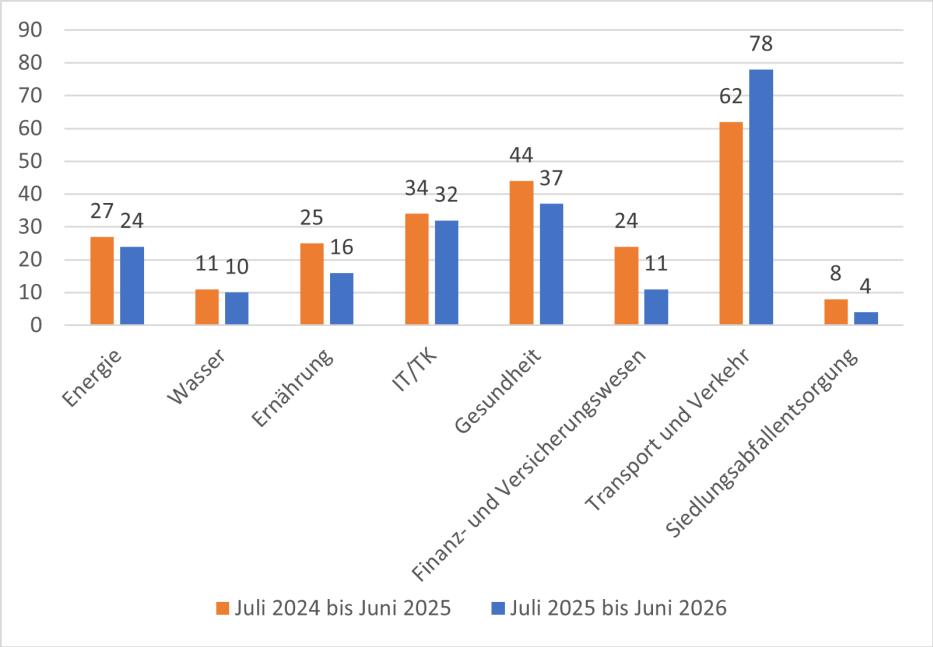
Rund 24 % der Störungen kritischer Anlagen waren im aktuellen Berichtszeitraum auf Cyberangriffe zurückzuführen (vgl. Abbildung 3-17). Im Vergleich zu den vergangenen Berichtszeiträumen ist der Wert damit leicht gestiegen. Andere Ursachen für Störungen waren zum Beispiel elementare Gefährdungen (beispielsweise ein Wassereinbruch) oder Vandalismus (beispielsweise zerstörte oder entwendete Oberleitungen).

→ Mehr über die Gefährdungslage nach Zielgruppen

3.4.1 Wirtschaft

3.4.1.1 Gefährdungslage Kritischer Infrastrukturen

Abbildung 3-18: Störungen kritischer Anlagen nach Sektor
Einheit: Anzahl je 100 Anlagen



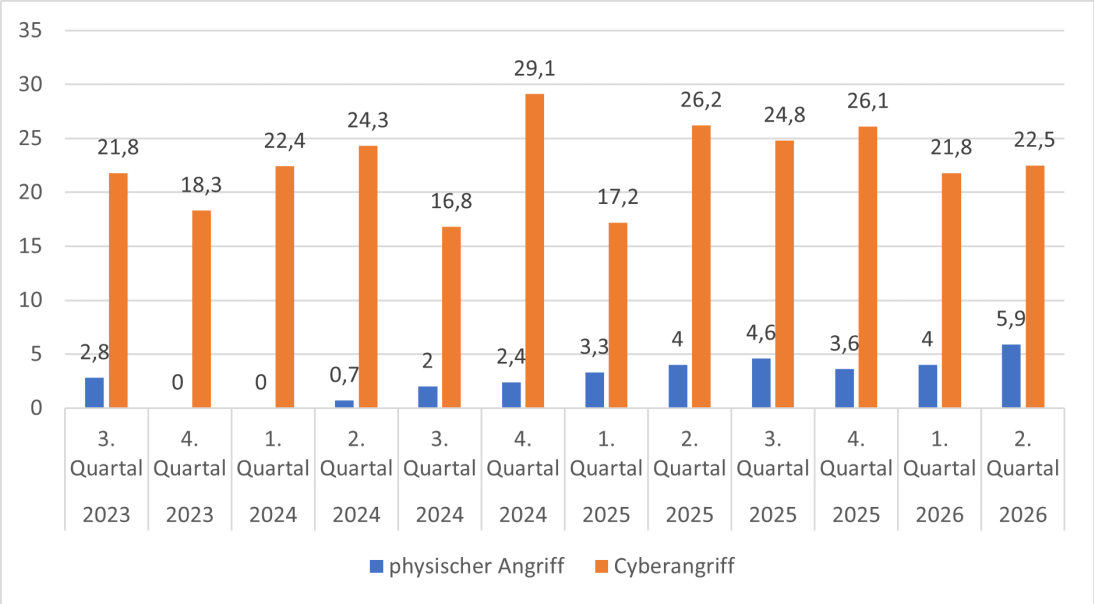
Quelle: KRITIS-Meldungen

Kritische Dienstleistungen wie die Versorgung mit Energie, Wasser und Lebensmitteln, medizinische Versorgung, Transport und Abfallentsorgung sind Grundlage für das Funktionieren unserer Gesellschaft. Der Gesetzgeber sieht deshalb eine spezielle Meldepflicht für Störungen kritischer Anlagen vor. Im aktuellen Berichtszeitraum ist die Anzahl der Störungsmeldungen in fast allen Sektoren gesunken. Im Durchschnitt über alle Sektoren hinweg ist die Zahl der Störungen kritischer Anlagen von 27,6 je 100 Anlagen im vergangenen Berichtszeitraum auf 24,2 Störungen je 100 Anlagen im aktuellen Berichtszeitraum gesunken (minus 12 %). Mit 78 gemeldeten Störungen je 100 Anlagen stach der Sektor Transport und Verkehr hervor (vgl. Abbildung 3-18). Dies war auch der einzige Sektor, der im aktuellen Berichtszeitraum mehr Störungen je 100 Anlagen meldete als im vergangenen Berichtszeitraum (plus 26 %).

→ Mehr über die Gefährdungslage Kritischer Infrastrukturen

Ein Viertel der Störungen Kritischer Infrastrukturen waren im aktuellen Berichtszeitraum auf Cyberangriffe zurückzuführen (vgl. Abbildung 3-17). Seit Anfang 2025 steigt zudem der Anteil der Störungen, die auf physische Angriffe zurückzuführen sind – zuletzt auf knapp 6 % (vgl. Abbildung 3-19).

Abbildung 3-19: Störungen kritischer Anlagen nach ausgewählten Störungsursachen
Einheit: Anteile in Prozent



Quelle: KRITIS-Meldungen

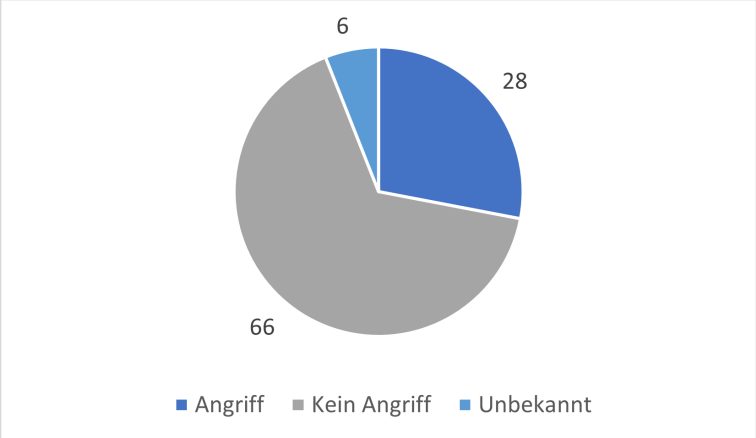
Ein besonderes Risiko stellen Kaskadeneffekte dar. Oft bestehen Abhängigkeiten zwischen verschiedenen Infrastruktur-Sektoren, sodass ein einzelner Vorfall Auswirkungen weit über den ursprünglichen Sektor haben kann. Diese gegenseitigen Abhängigkeiten, auch als Interdependenz bezeichnet, lassen sich in physische (zum Beispiel Stromversorgung von Rechenzentren), geografische (zum Beispiel mehrere Systeme durch dasselbe Naturereignis betroffen), wirtschaftliche (organisatorische bzw. wirtschaftliche Abhängigkeiten) oder auch Cyber-Interdependenzen (zum Beispiel IT-Systeme steuern Stromnetze) unterteilen.

Ein prägnantes Beispiel für Kaskadeneffekte als Folge physischer Angriffe ereignete sich am 3. Januar 2026 in Berlin: Infolge eines Brandanschlags auf eine Kabelbrücke kam es zu einem großflächigen und lang anhaltenden Stromausfall. Aufgrund der Beschädigung an einem Lichtwellenleiter war die Steuerung des Stromnetzes für den Betreiber nicht mehr möglich. Betroffen waren neben 45.000 Haushalten auch vier KRITIS-Betreiber aus dem Sektor Informationstechnik und Telekommunikation und ein KRITIS-Betreiber aus dem Sektor Transport und Verkehr. Da diese von der Stromversorgung abgeschnitten waren, konnten sie ihre kritischen Dienstleistungen nicht oder nur teilweise zur Verfügung stellen.

Es war bereits der zweite flächendeckende Stromausfall in Berlin infolge eines Brandanschlags. Bereits im September 2025 waren mehrere zehntausend Haushalte sowie drei KRITIS-Betreiber aus dem Sektor Informationstechnik und Telekommunikation, zwei KRITIS-Betreiber aus dem Sektor Transport und Verkehr und ein KRITIS-Betreiber aus dem Sektor Gesundheit von der Stromversorgung abgeschnitten.

3.4.1.2 Gefährdungslage in der Luftsicherheit und in der Luftfahrtbranche

Abbildung 3-20: Störungen in der Luftsicherheit und in der Luftfahrbranche nach Störungsursache
Einheit: Anteile in Prozent



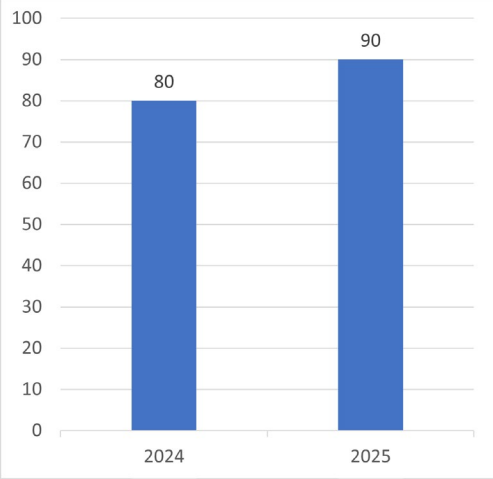
Quelle: BSI

Im gesamten Berichtszeitraum wurden 83 Vorfälle innerhalb der Zielgruppe erfasst, die den Bereichen der nach Luftsicherheitsgesetz regulierten Akteure (Luftsicherheit), der Luftfahrtbranche, die als Kritische Infrastruktur eingestuft ist (KRITIS-Luftfahrt), sowie der durch NIS-2 regulierten Luftfahrtbranche zuzuordnen sind. Rund 28 % der Vorfälle waren auf Cyberangriffe zurückzuführen (vgl. Abbildung 3-20).

Viele Unternehmen müssen die neuen Meldepflichten noch einordnen. In Austauschformaten zeigt sich dies deutlich: Dort berichtete Phishing-Angriffe werden vielfach nicht offiziell gemeldet. Hier besteht weiterer Aufklärungsbedarf, um ein konsistentes Lagebild zu gewährleisten.

3.4.1.3 Gefährdungslage kleiner und mittlerer Unternehmen

Abbildung 3-21: Anzeigen wegen Ransomware-Vorfällen von kleinen und mittleren Unternehmen
Einheit: Anteile in Prozent an allen Anzeigen wegen Ransomware-Vorfällen



Quelle: BKA Bundeslagebild Cybercrime

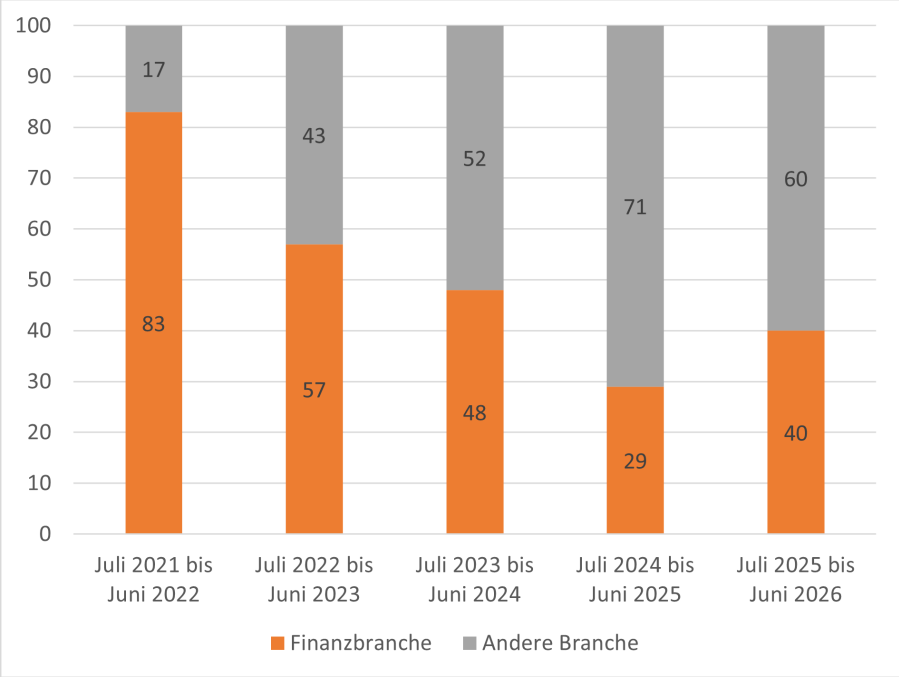
Im aktuellen Berichtszeitraum bestätigte sich ein langjähriger Trend: Kleine und mittlere Unternehmen (KMU), also der weitaus größere Teil der deutschen Wirtschaft, unterschätzen ihre Gefährdungslage deutlich. Sie bieten schon aufgrund ihrer hohen Zahl die größten Angriffsflächen.

Wenn Angreifer im deutschen Internet verwundbare Systeme finden, so betreffen diese mit hoher Wahrscheinlichkeit ein KMU. Schwachstellen in aus dem Internet erreichbaren Systemen stellten im aktuellen Berichtszeitraum wieder die am stärksten gefährdete Angriffsfläche dar (vgl. Time-to-Exploit sowie Neue Schwachstellen), und die meisten dieser Schwachstellen befinden sich in Systemen kleiner und mittlerer Unternehmen. Dementsprechend ist der Anteil kleiner und mittlerer Unternehmen an allen bei den Polizeien angezeigten Ransomware-Angriffen weiter gestiegen: von ca. 80 % im Jahr 2024 auf gut 90 % im Jahr 2025 (vgl. Abbildung 3-21, vgl. Gefährdungslage nach Angreifermotivation).

3.4.2 Verbraucherinnen und Verbraucher

3.4.2.1 Phishing-Mails

Abbildung 3-22: Phishing-Mails nach nachgeahmter Branche
Einheit: Anteile in Prozent



Quelle: Erhebung über Phishing-Mails
Bemerkung: Von Verbraucherinnen und Verbrauchern an das Phishing-Radar der VZ NRW gemeldete Phishing-Mails.

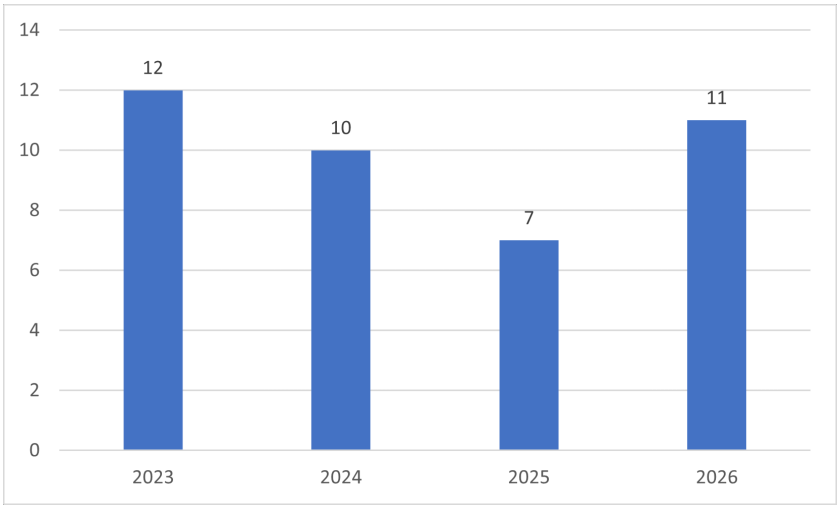
Trendwende bei Finance Phishing: Mit einem Anstieg auf 40 % der von Verbraucherinnen und Verbrauchern gemeldeten Phishing-Mails deutete sich im aktuellen Berichtszeitraum eine Trendwende bei den nachgeahmten Branchen an (vgl. Abbildung 3-22). Bei Finance Phishing war ein Zuwachs von 11 Prozentpunkten zu verzeichnen. In den Jahren zuvor war der Indikator stets rückläufig gewesen.

Neben verdächtigen Nachrichten, die vermeintlich von traditionellen Filialbanken kommen, melden Verbraucherinnen und Verbraucher zunehmend Phishing-Mails im Namen von Neobanken: Direktbanken, welche digital mit ihren Kundinnen und Kunden interagieren und teilweise auf kurzfristige Bankgeschäfte ausgelegt sind, gewinnen in der Bevölkerung an Popularität und werden daher zunehmend von Cyberkriminellen für Phishing-Angriffe nachgeahmt. Verbraucherinnen und Verbraucher werden auf diesem Weg mit gefälschten Nachrichten konfrontiert, welche beispielsweise den digitalen Kundenservice imitieren oder zu kurzfristigen Transaktionen auffordern.

3.4.2.2 Betrug im Online-Raum

Abbildung 3-23: Von einer Straftat im Internet betroffene Verbraucherinnen und Verbraucher in Deutschland

Einheit: Anteile in Prozent



Quelle: Cybersicherheitsmonitor
Bemerkung: Mehrfachnennungen möglich

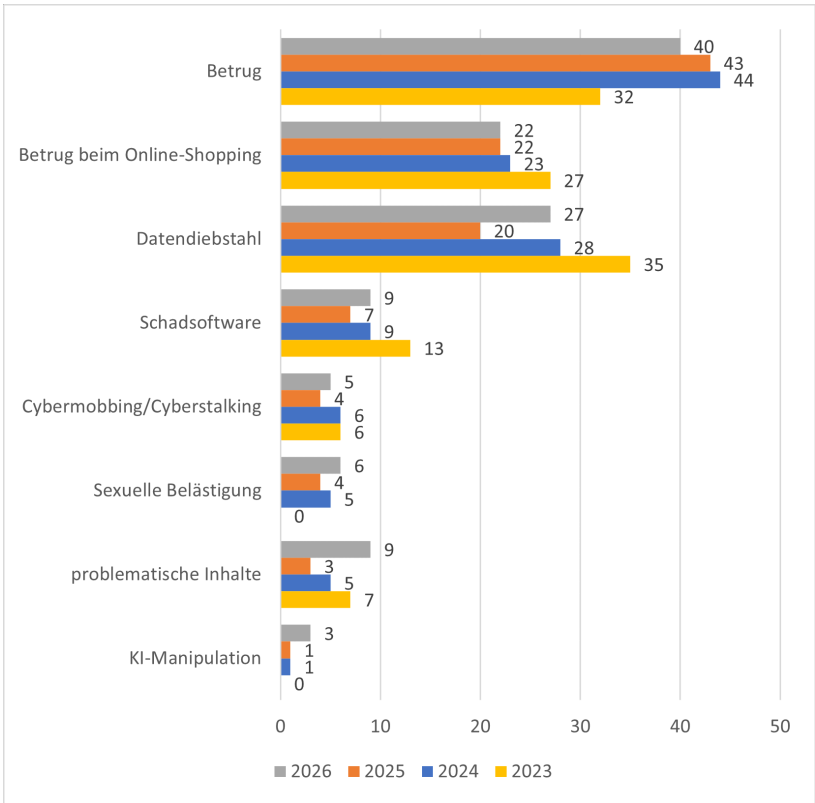
Im langjährigen Durchschnitt sind jährlich 10 % der Verbraucherinnen und Verbraucher in Deutschland von einer Straftat im Internet betroffen. Im Jahr 2026 waren es 11 % (vgl. Abbildung 3-23). Betrug gehörte dabei auch 2026 zu den Top-Cyberstraftaten gegen Verbraucherinnen und Verbraucher.

→ Mehr über Betrug im Online-Raum

Im Rahmen des jährlich vom BSI und der Polizeilichen Kriminalprävention erhobenen Cybersicherheitsmonitors (CyMon) gaben 27 % der Befragten an, schon einmal von Cyberkriminalität betroffen gewesen zu sein (zum Vergleich: 2025: 22 %, 2024: 24 %, 2023: 27 %). Rund 11 % gaben zudem an, in den letzten zwölf Monaten Opfer einer Straftat im Internet geworden zu sein (zum Vergleich: 2025: 7 % 2024: 10 %, 2023: 12 %). Damit ist ein leichter Anstieg bei der Betroffenheit im Vergleich zum Vorjahr zu beobachten.

Gut 22 % der in den vergangenen zwölf Monaten von Cyberkriminalität Betroffenen erlitten Betrug beim Onlineshopping. In Summe 40 %erlebten mindestens eine von mehreren weiteren Betrugsformen (vgl. Abbildung 3-24).

Abbildung 3-24: Verbraucherinnen und Verbraucher in Deutschland nach Art der Betroffenheit von Cyberkriminalität
Einheit: Anteile in Prozent



Quelle: Cybersicherheitsmonitor
Bemerkung: Mehrfachnennungen möglich, „Sexuelle Belästigung“ und „KI-Manipulation“ wurden 2023 nicht abgefragt.

Zudem wurden 27 % Opfer von Datendiebstahl (vgl. Abbildung 3-24). Dazu zählen Fremdzugriffe auf Accounts (14 %) und Phishing (12 %, vgl. Phishing-Mails sowie Datenleaks). 9 % der Betroffenen entdeckten Schadsoftware auf einem ihrer Geräte, etwa Viren, Trojaner oder Ransomware. Neun von zehn der von Cyberkriminalität Betroffenen mussten infolgedessen einen Schaden hinnehmen (88 %). Einen finanziellen Schaden erlitt etwa ein Drittel der Betroffenen (33 %) (vgl. Schadwirkungen).

Der Cybersicherheitsmonitor (CyMon) bietet umfassende Einblicke in das Informations- und Schutzverhalten der deutschen Bevölkerung sowie deren Erfahrungen mit Cyberkriminalität und wird jährlich gemeinsam von BSI und ProPK veröffentlicht.

Ausgewählte Vorfälle: Gefährdungslage:
Phishing-Angriffe via Messenger

Sachverhalt

Am 06. Februar 2026 veröffentlichten BSI und BfV einen gemeinsamen Sicherheitshinweis zum Thema Phishing über Messenger-Dienste, insbesondere bei Signal. Seit Herbst 2025 standen hochrangige Personen aus Politik, Militär und Diplomatie sowie Investigativjournalistinnen und -journalisten in Deutschland und Europa im Fokus derartiger Angriffe. Charakteristisch für diese Angriffskampagne war, dass weder Schadsoftware eingesetzt noch technische Schwachstellen der Messenger-Dienste ausgenutzt wurden. Stattdessen bedienten sich die Angreifer legitimer Sicherheitsfunktionen der Anwendungen und kombinierten diese mit Social Engineering. Ziel war es, unbemerkt Zugriff auf Einzel- und Gruppen-Chats sowie auf Kontaktlisten der betroffenen Personen zu erlangen. Der Schwerpunkt der Angriffe lag auf dem Messengerdienst Signal, wobei vergleichbare Vorgehensweisen aufgrund ähnlicher Funktionsprinzipien auch bei WhatsApp

denkbar sind. Dem BSI und BfV war eine relevante Anzahl Betroffener und kompromittierter Konten bekannt (vgl. Cybersicherheitswarnung).

Am 17. April 2026 lagen Erkenntnisse vor, dass die Kampagne weiterhin aktiv war und an Dynamik gewann. Infolge des zu erwartenden hohen Anfrage- und Meldeaufkommens wurde im BSI das IT-Krisenreaktionszentrum einberufen. Das BSI hat zudem in Zusammenarbeit mit dem BfV einen Leitfaden für Betroffene der Phishing-Angriffe veröffentlicht.

Bewertung

Das BSI hält es angesichts der hochrangingen Zielpersonen für plausibel, dass ein staatlich gestützter Cyberakteur für die Phishing-Angriffe verantwortlich war. Die Niederlande, die USA und Frankreich ordnen die Phishing-Kampagne Russland zu. Aufgrund der geringen technischen Hürden solcher Angriffskampagnen ist das Vorgehen jedoch gleichermaßen von staatlichen Akteuren mit nachrichtendienstlichem Interesse wie auch von Cyberkriminellen anwendbar.

Ein erfolgreicher Zugriff auf Messenger-Konten ermöglicht nicht nur die Einsicht in vertrauliche Einzelkommunikation, sondern potenziell auch die Kompromittierung ganzer Netzwerke über Gruppen-Chats. Darüber hinaus lassen sich sensible Kontaktstrukturen rekonstruieren, die für weitergehende nachrichtendienstliche oder kriminelle Maßnahmen genutzt werden könnten.

Reaktion

Das BSI bearbeitete den Fallkomplex am 17. April 2026 im IT-Krisenreaktionszentrum. In der Folge wurde ein Call-Center für Betroffene eingerichtet, die sich auf diesem Wege direkt an das BSI wenden konnten. Zudem hat das BSI Informationsseiten mit Hilfestellungen für Betroffene erstellt und aktualisierte diese fortlaufend. Betroffene konnten anhand der Hilfestellungen erste Maßnahmen ergreifen. Ihnen wurde empfohlen, ein neues Messenger-Konto zu erstellen und dieses mit einer neuen Mobilfunknummer zu registrieren. Weitere Handlungsempfehlungen konnten dem von BSI und BfV gemeinsam erstellten Leitfaden für Betroffene entnommen werden.

Ausgewählte Vorfälle: Gefährdungslage:
Cyberspionage-Angriffe auf Ziele im politischen und vorpolitischen Raum

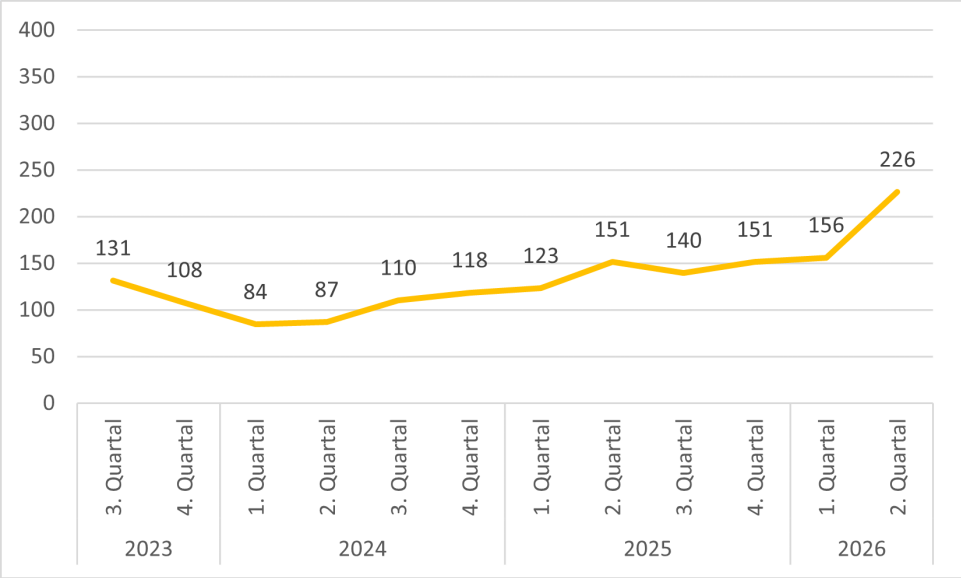
Auch im aktuellen Berichtszeitraum war der politische und vorpolitische Raum wieder Ziel fortgeschrittener Cyberangriffe. Insbesondere für staatlich gesteuerte Angreifer stellen beispielsweise Parteien oder parteinahe Stiftungen attraktive Ziele zum Zweck der Spionage dar. Neben Social-Engineering-Angriffen gegen Personen waren häufig auch Angriffe gegen Perimetersysteme zu beobachten. Diese Systeme sind direkt aus dem Internet erreichbar und können wegen schwacher Passwörter, Fehlkonfigurationen oder Schwachstellen ein Einfallstor in die dahinterliegenden Netzwerke darstellen. Wie auch in den Jahren zuvor wurden solche Systeme erneut mit sogenannten Zero-Day-Schwachstellen angegriffen (Schwachstellen, die zum Zeitpunkt des Angriffs dem Hersteller noch unbekannt waren). Zwei solcher Schwachstellen wurden gegen die Mobilgeräte-Management-Lösung Endpoint Manager Mobile (EPMM) des Herstellers Ivanti ausgenutzt (vgl. **Ausgewählte Vorfälle: Angriffsfläche**
Erfolgreiche Angriffe auf Systeme zur Verwaltung mobiler Endgeräte mittels Ausnutzung von Zero-Day-Schwachstellen). Unter den Betroffenen befanden sich auch mehrere Organisationen aus dem politischen Raum. Die Kompromittierung dieser Systeme hatte zur Folge, dass Angreifer sensible Informationen sowohl über die verwalteten Endgeräte als auch über deren Nutzende entwenden konnten, wie beispielsweise Standort-, Identitäts- oder Kontaktinformationen. Eine große Gefahr besteht darin, dass diese Informationen langfristig für weiterführende Social-Engineering-Angriffe verwendet werden können. Insbesondere bei Personen und Organisationen im politischen und vorpolitischen Raum wird dies regelmäßig bei staatlich gesteuerten Cyberangriffen beobachtet.

4 Schadwirkungen

Zu den durch Cyberangriffe und IT-Sicherheitsvorfälle ausgelösten Schadwirkungen zählen neben direkten finanziellen Schäden, wie etwa Lösegeldzahlungen oder Kosten für die Wiederherstellung von Systemen, auch Schäden wie Systemausfälle, Systeminfektionen oder exfiltrierte Daten. Mit Blick auf den vergangenen Berichtszeitraum blieben die beobachteten Schadwirkungen im aktuellen Berichtszeitraum auf vergleichbarem Niveau oder konnten durch präventive Maßnahmen vereinzelt sogar gesenkt werden (vgl. etwa Lösegelder insgesamt). Durchschnittliche Lösegelder je Einzelfall sind insbesondere im 2. Quartal 2026 allerdings stark gestiegen, wodurch der Impact Score, der die Entwicklung des Gesamtschadens misst, auch im Durchschnitt des Berichtszeitraums gestiegen ist (plus 33 %). Herausgehobene Schadwirkungen waren zudem insbesondere bei infizierten Systemen zu beobachten: Aufgrund zunehmender Exploitation-Angriffe (vgl. Exploitation-Angriffe) hat sich ihre Zahl im aktuellen Berichtszeitraum nahezu verdoppelt (vgl. Infizierte Systeme).

4.1 Impact Score

Abbildung 4-1: Impact Score
Einheit: 2024=100 (Messzahl)

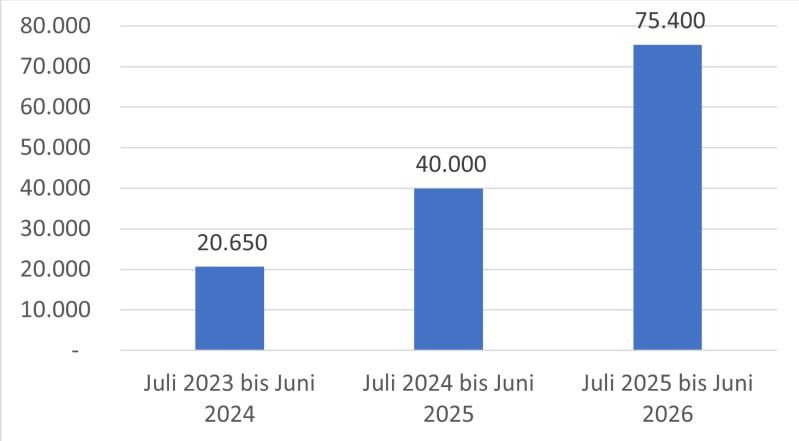


Quelle: BSI

Der Impact Score des BSI, der das Ausmaß der Schadwirkungen durch Cyberangriffe misst, lag im aktuellen Berichtszeitraum bei durchschnittlich 168 Punkten und damit erneut deutlich über dem Niveau des vergangenen Berichtszeitraums (plus 33 %), wobei im 2. Quartal 2026 ein neuer Höchststand von 226 Punkten zu verzeichnen war (vgl. Abbildung 4-1). Während die Lösegelder je Fall im aktuellen Berichtszeitraum erheblich zulegten (vgl. Lösegelder), ist die Gesamtsumme der in Blockchains identifizierten Lösegelder leicht gesunken. Dagegen ist die Zahl der infizierten Systeme in Deutschland erheblich gestiegen (plus 89 %, vgl. Infizierte Systeme).

4.2 Infizierte Systeme

Abbildung 4-2: Infizierte Systeme
Einheit: Anzahl im Tagesdurchschnitt



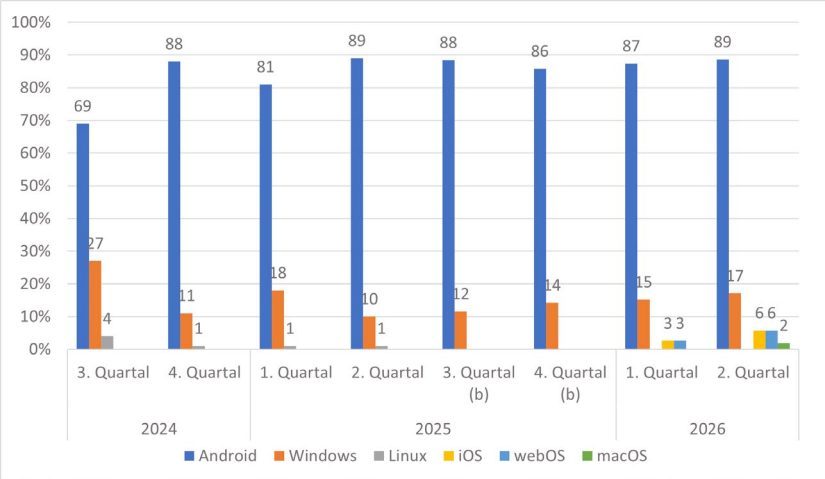
Quelle: BSI
Bemerkung: Vom BSI an deutsche Internetprovider und andere Netzbetreiber gemeldete IP-Adressen

Unzertifizierte Android-Geräte machten im aktuellen Berichtszeitraum mit durchschnittlich 88 % den weitaus größten Teil der vom BSI beobachteten infizierten Systeme aus. In diesem Bereich sind insbesondere IoT-Geräte führend (vgl. Botnetze). Die Zahl der durchschnittlich täglich beobachteten infizierten Systeme in Deutschland stieg im aktuellen Berichtszeitraum auf 75.400 (vgl. Abbildung 4-2). Das war nahezu eine Verdopplung gegenüber dem vergangenen Berichtszeitraum.

→ Mehr über infizierte Systeme

Rund 88 % der infizierten Systeme waren Android-basierte Systeme, häufig Consumer-IoT-Geräte, die aufgrund ihrer häufig schlecht geschützten Angriffsflächen leichte Ziele für Cyberangreifer darstellen (vgl. Vernetzte Geräte, vgl. Consumer-IoT-Geräte). Ebenso wie bei den neu aufgenommenen Familien IPIDEA und Aisuru/Kimwolf verwenden Cyberangreifer infizierte Systeme (Bots) als sogenannte Residential Proxies, die ohne Kenntnis ihrer Benutzerinnen und Benutzer den Datenverkehr Dritter weiterleiteten. Dazu gehört vor allem auch maliziöser Datenverkehr.

Abbildung 4-3: Infizierte Systeme (Unique IP) nach Betriebssystem
Einheit: Anteile in Prozent



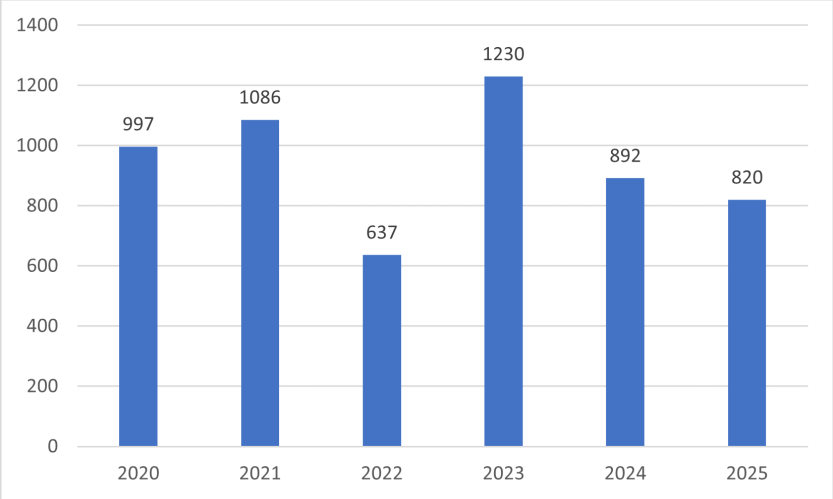
Quelle: Botnetz-Monitoring
Bemerkung: Mehrfachnennungen möglich. Wert wurde (b) um Sondereffekte bereinigt.

Wie in den Vorjahren liegt der Schwerpunkt der vom BSI beobachteten infizierten Systeme weiterhin auf Betriebssystemen mobiler Android-Geräte sowie sonstigen IoT-Geräten (vgl. Abbildung 4-3). Klassische Desktopsysteme etwa mit Microsoft Windows sind nochmals weniger präsent als in den Vorjahren. Wie in anderen Bereichen der Cybersicherheitslage dürfte auch hier die Ursache darin begründet liegen, dass Angreifer ihren Fokus zunehmend auf schlecht geschützte, leicht anzugreifende Systeme legen. So ergreifen aktuelle Desktopbetriebssysteme bereits umfangreiche Schutzmaßnahmen, um Schadsoftwareinfektionen bestmöglich zu verhindern. Darüber hinaus bevorzugen viele Nutzende heutzutage mobile Geräte für ihre Internetaktivitäten, sodass die Angriffsfläche hier überproportional schnell wächst und aufgrund verbreitet veralteter Systeme leichte Ziele bietet. Im IoT-Bereich sowie bei mobilen Endgeräten liegt der Fokus der Hersteller zudem oftmals auf dem Herstellungs- bzw. Verkaufspreis und der Funktionalität der Geräte. So basiert der Großteil der vom BSI beobachteten Systeme auf unzertifizierten Android-Varianten, die nicht mit den üblicherweise enthaltenen Schutzmechanismen des regulären Androidsystems (Play Protect, etc.) ausgestattet sind. Dies verdeutlicht, wie wichtig es ist, beim Kauf neuer Produkte auf eine Zertifizierung sowie die Verfügbarkeit von Herstellersupport, unter anderem in Form von Softwareupdates, zu achten.

Weitere Informationen: Botnetze – Steckbriefe

4.3 Lösegelder

Abbildung 4-4: Lösegelder insgesamt
Einheit: Millionen US-Dollar



Quelle: Chainalysis
Bemerkung: In Blockchains identifizierte Lösegelder.

Obgleich immer weniger Organisationen zur Zahlung von Lösegeldern bereit sind – ein Indiz dafür, dass Organisationen heutzutage besser aufgestellt sind und sich seltener dem Erpressungsdruck von Cyberangreifern beugen müssen (vgl. Abbildung 4-6) – ist die Höhe der Lösegelder mit insgesamt 820 Millionen US-Dollar im Jahr 2025 (vgl. Abbildung 4-4) nur leicht gesunken (minus 8 %). Hintergrund waren deutlich gestiegene Lösegelder je Fall. Anders gesagt: Wer nicht gut aufgestellt war und sich dem Erpressungsdruck der Angreifer beugen musste, musste deutlich höhere Lösegelder aufbringen.

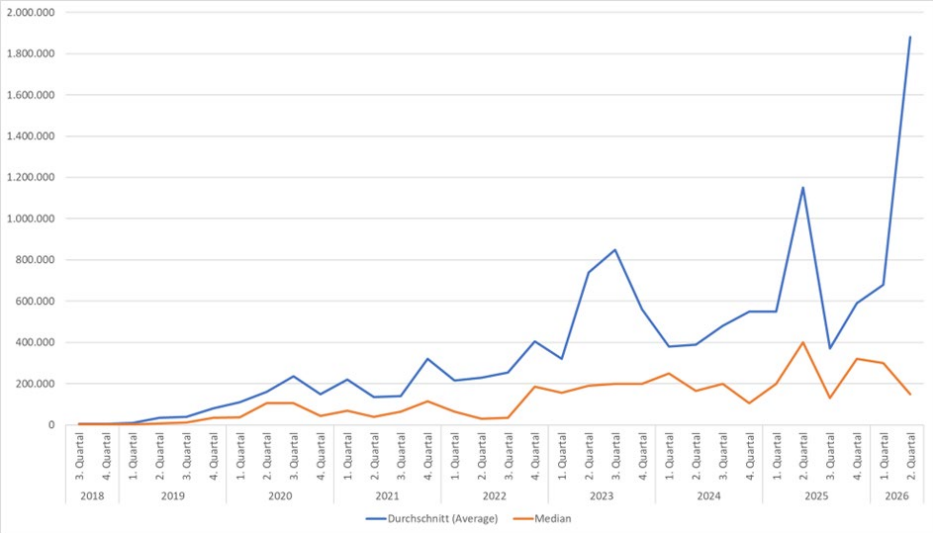
→ Mehr über Lösegelder

Cybercrime-Gruppen gingen auch im aktuellen Berichtszeitraum weiterhin opportunistisch vor. Finanziell motivierte Angriffe richten sich in der Regel nicht gezielt gegen bestimmte Branchen oder Sektoren. Ausschlaggebend ist nach Beobachtungen des BSI vielmehr: wie stark potenzielle

Ziele exponiert sind und über welche Fähigkeiten die dahinterstehenden Organisationen verfügen, Angriffsversuche zu erkennen und abzuwehren. Es kann hier ein fortlaufender Trend zu Angriffen auf kleine und mittlere Unternehmen beobachtet werden.

Der signifikante Anstieg der durchschnittlichen Lösegeldzahlungen je Fall zum Ende des vergangenen Berichtszeitraums setzte sich am Ende des aktuellen Berichtszeitraums noch deutlicher fort (vgl. Abbildung 4-5). Auch der langfristige Trend wies weiter nach oben. Da die Summe der Lösegeldzahlungen insgesamt zurückgegangen ist (vgl. Abbildung 4-4), dürfte dies darauf hindeuten, dass insgesamt weniger Betroffene im Einzelfall jedoch teils deutlich höhere Lösegelder zu zahlen hatten. Zum Ende des Berichtszeitraums zahlten Betroffene im Durchschnitt je Fall 1,9 Millionen US-Dollar (vgl. Abbildung 4-5).

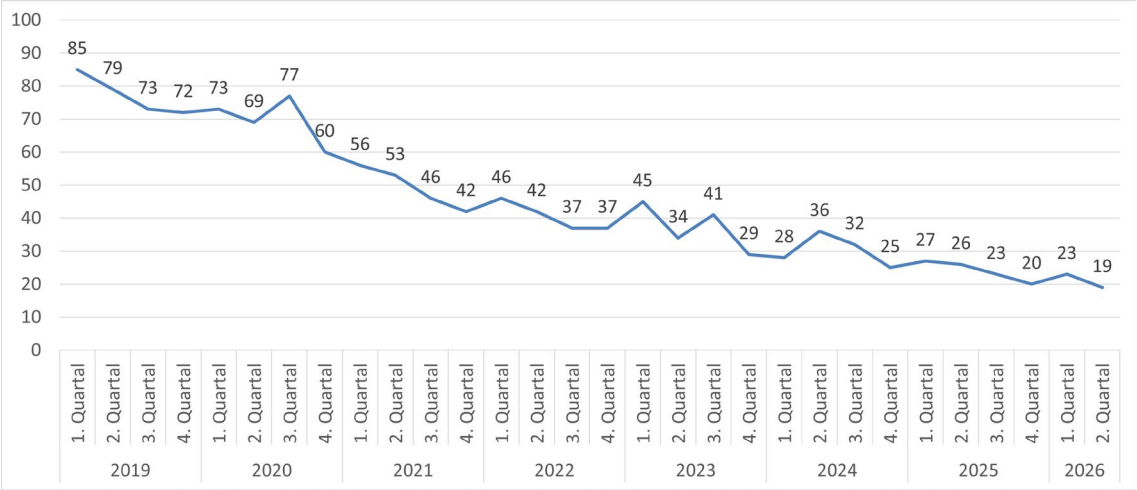
Abbildung 4-5: Durchschnittliche Lösegeldzahlungen
Einheit: US-Dollar



Quelle: Coveware

Der in den vergangenen Jahren beobachtete Trend zu einer abnehmenden Bereitschaft zur Zahlung eines Lösegelds setzt sich fort. Zuletzt waren nur noch 19 % der von einem Ransomware-Vorfall betroffenen Organisationen zur Zahlung eines Lösegelds bereit (vgl. Abbildung 4-6). Hintergrund dürfte die steigende Resilienz potenzieller Betroffener sein. Wer vorgesorgt hat, seine externen Angriffsflächen bereits präventiv gut geschützt hat und im Falle eines trotzdem erfolgreichen Angriffs über aktivierbare Backups verfügt, muss sich in etwaigen Lösegeldverhandlungen nicht jedem Erpressungsdruck von Cyberangreifern beugen.

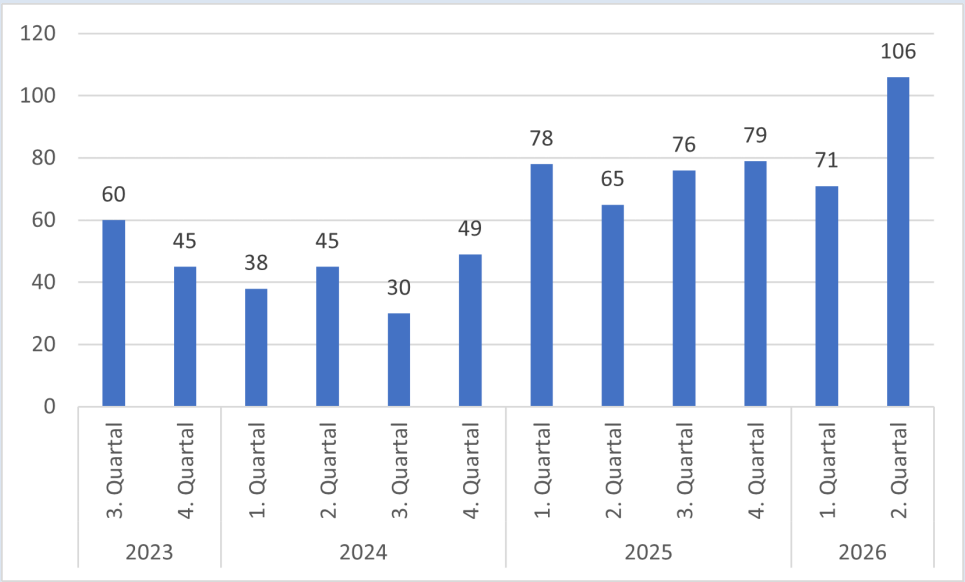
Abbildung 4-6: Betroffene von Ransomware-Angriffen nach Zahlungsbereitschaft
Einheit: Anteile in Prozent



Quelle: Coveware

4.4 Leak-Geschädigte

Abbildung 4-7: Mutmaßlich geschädigte Organisationen aus Deutschland auf Leak-Seiten
Einheit: Anzahl



Quelle: Leak-Geschädigten-Statistik

Insgesamt veröffentlichten Cybercrime-Gruppen im aktuellen Berichtszeitraum die Daten von 332 mutmaßlich geschädigten Organisationen aus Deutschland auf ihren Leak-Seiten. Im 2. Quartal 2026 wurde ein neues Allzeithoch von 106 mutmaßlich geschädigten Organisationen aus Deutschland beobachtet. Hintergrund waren Aktivitäten auf der Leak-Seite SafePay, die sich auf deutsche Unternehmen fokussiert (vgl. Abbildung 4-8)

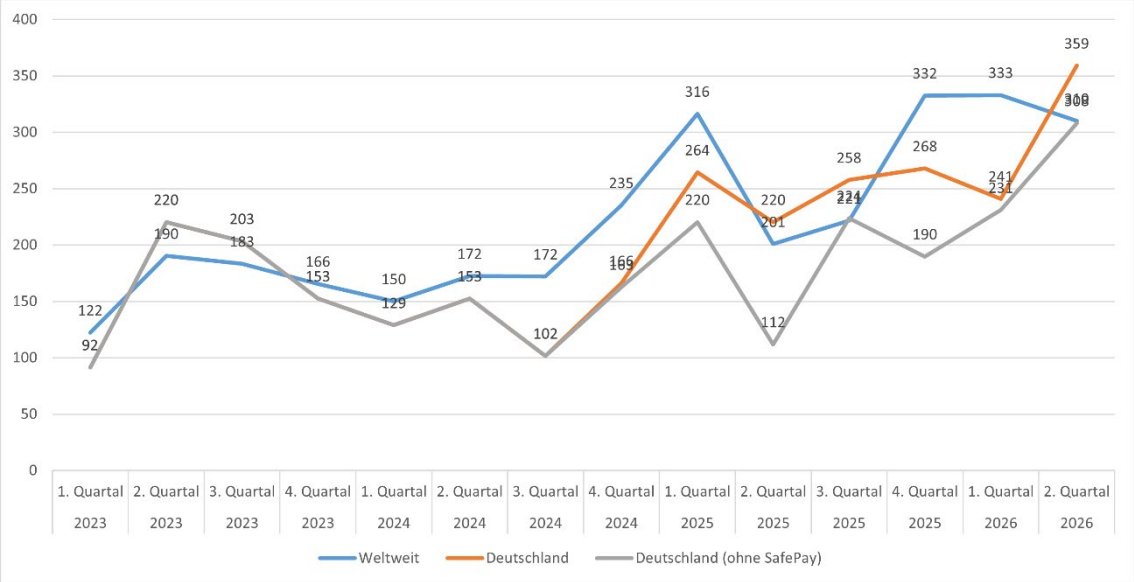
→ Mehr über Leak-geschädigte Organisationen

In der Leak-Geschädigten-Statistik wurden im aktuellen Berichtszeitraum weltweit 8.777 Organisationen erfasst, die mutmaßlich durch Double Extortion im Zuge von Ransomware-Angriffen geschädigt wurden. Dies entsprach einer Steigerung im Vergleich zum vergangenen Berichtszeitraum um 30 %. Die Nennung von mehr mutmaßlich Geschädigten bedeutet dabei nicht

zwangsläufig, dass es tatsächlich auch entsprechend mehr Ransomware-Vorfälle gab. Sie kann vielmehr durch verschiedene Variablen beeinflusst sein, etwa dadurch, dass Unternehmen seltener zur Zahlung von Lösegeld bereit sind (vgl. Lösegelder) und Angreifer daher häufiger nicht (nur) mit der Verschlüsselung erpressen, sondern mit der Veröffentlichung exfiltrierter Daten (Leak) drohen.

Im aktuellen Berichtszeitraum wurden 332 der insgesamt 8.777 mutmaßlich Leak-Geschädigten (4 %) Deutschland zugeordnet (plus 1 Prozentpunkt gegenüber dem vergangenen Berichtszeitraum). Der Index über die mutmaßlich Leak-geschädigten Organisationen in Deutschland lag im aktuellen Berichtszeitraum bei durchschnittlich 281 Punkten, ein Zuwachs von 50 %. Im 2. Quartal 2026 erreichte der Indikator mit 359 Punkten einen neuen Höchststand (vgl. Abbildung 4-8). Dabei stach insbesondere die Leak-Seite SafePay heraus. Die Angreifer hinter SafePay zeigten einen besonderen Fokus auf deutsche Organisationen, der bei anderen Leak-Seiten bislang nicht beobachtet wurde (vgl. Abbildung 4-9). Ohne diesen Sondereffekt hätte die Messzahl im aktuellen Berichtszeitraum bei durchschnittlich 238 Punkten und im 2. Quartal 2026 bei 308 Punkten gelegen (vgl. Abbildung 4-8).

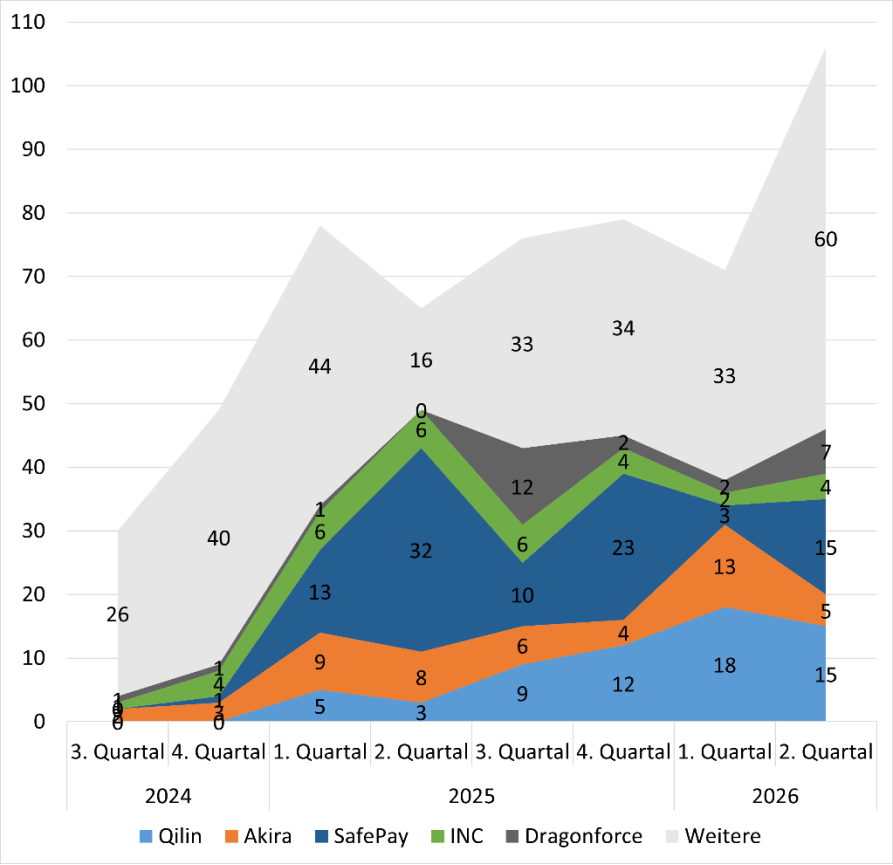
Abbildung 4-8: Mutmaßlich Leak-geschädigte Organisationen aus Deutschland und weltweit
Einheit: 2021 = 100 (Messzahl)



Quelle: Leak-Geschädigten-Statistik

Bislang wurden 19 % aller auf SafePay genannten mutmaßlich Geschädigten Deutschland zugeordnet, ein weit überdurchschnittlicher Wert. Im Vergleich dazu wurden über alle Leak-Seiten hinweg seit Beginn der Aufzeichnung durchschnittlich 4 % der mutmaßlich Geschädigten Deutschland zugeordnet.

Abbildung 4-9: Mutmaßlich Leak-geschädigte Organisationen aus Deutschland nach Leak-Seite
Einheit: Anzahl

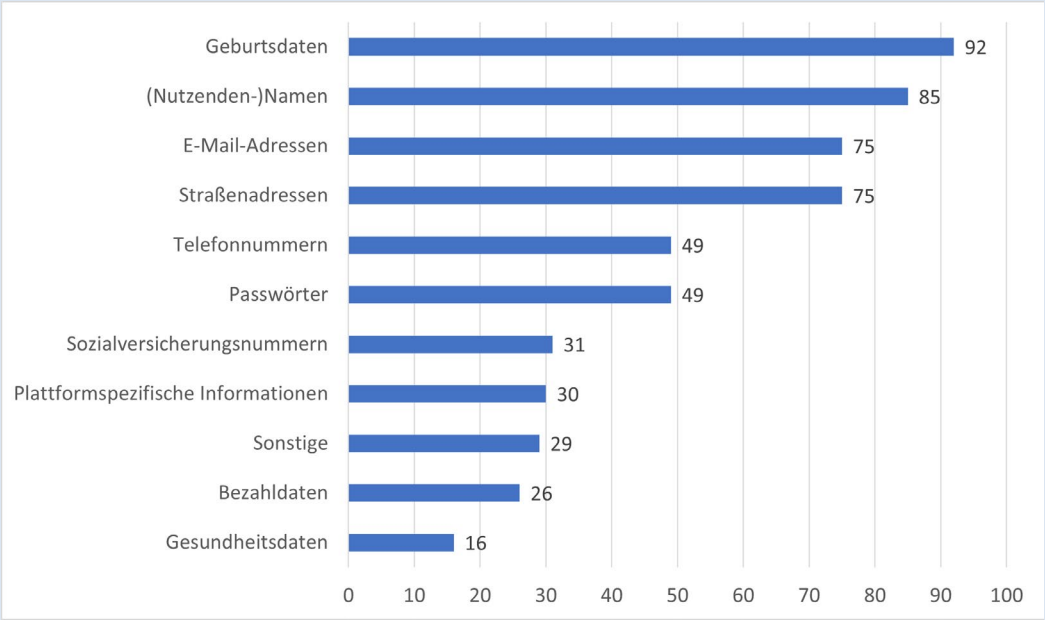


Quelle: Leak-Geschädigten-Statistik

Die Gruppe hinter der zugehörigen Ransomware SafePay wurde im November 2024 erstmals beobachtet. Die Angreifer nutzen Double Extortion (Datenleaks und Verschlüsselung), um Lösegelder zu erpressen. Dabei kontaktiert die Gruppe Betroffene teilweise direkt (zum Beispiel per Telefonanruf), um den Erpressungsdruck zu erhöhen. Die Ransomware hat Ähnlichkeiten mit anderen Ransomware-Familien, ist jedoch wahrscheinlich eine Eigenentwicklung der Gruppe. Auf ihrer Leak-Seite behauptet die Gruppe allerdings, dass sie keine eigene Ransomware-as-a-Service (RaaS) anbietet.

4.5 Datenleaks

Abbildung 4-10: Datenleaks von Juli 2025 bis Juni 2026 nach Art der geleakten Daten
Einheit: Anteile in Prozent



Quelle: Cybersicherheitsmonitor

Im aktuellen Berichtszeitraum wurden 433 Datenleaks bekannt, bei denen Daten von Institutionen sowie von deutschen Verbraucherinnen und Verbrauchern abgeflossen sind. Die Schadwirkung fiel damit im Vergleich zum vergangenen Berichtszeitraum mit insgesamt 461 Fällen etwas moderater aus. Betroffen waren insbesondere Geburtsdaten (92 %), Nutzenden-Namen (85 %), E-Mail- (75 %) und Post-Adressen (75 %), Telefonnummern sowie Passwörter.

→ Mehr über Datenleaks

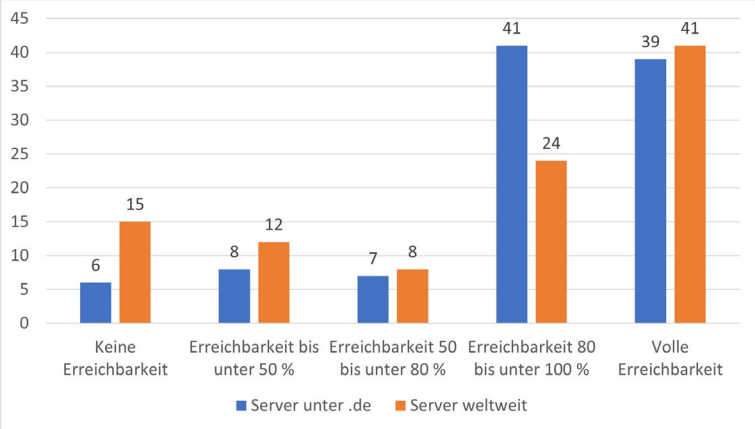
Zu den Hauptursachen für Datenleaks zählen weiterhin unzureichend gesicherte Datenbanken, die aus dem Internet erreichbar sind (vgl. Web-Angriffsflächen) oder Schwachstellen aufweisen (vgl. Neue Schwachstellen) und daher anfällig für Portscans und Exploitation-Angriffe (vgl. Aufklärungstätigkeiten, Exploitation-Angriffe) sind.

Im Berichtszeitraum konnten mehrere Infostealer beobachtet werden, welche sich zum Beispiel als KI-Tools, Browser-Add Ons oder Bildbearbeitungs-Apps getarnt hatten. Nach der Installation der Software durch Verbraucherinnen und Verbraucher wurden bei anschließender Nutzung der Tools persönliche Daten und Zugangsdaten ausgeleitet. Neben persönlichen Informationen wie Namen, Adressen oder Geburtsdaten, konnte so auch Bild- und Videomaterial entwendet werden. Diese Informationen sind für Cyberkriminelle von Mehrwert, um zum Beispiel Identitäten zu stehlen und diese möglichst genau nachzuahmen. Der Missbrauch von Identitäten ist vielfältig und reicht von der Erstellung von Fake-Profilen auf Social Media über das unautorisierte Auslösen von Bestellungen oder Zahlungen bis hin zu Vertragsabschlüssen mit Banken oder Abonnementanbietern.

4.6 DDoSia-Schadwirkungen

Abbildung 4-11: Von DDoSia angegriffene Server in Deutschland und weltweit nach Erreichbarkeit

Einheit: Anteile in Prozent



Quelle: BSI

Die Hacktivisten-Gruppe NoName057(16) ruft seit Jahren pro-russische Akteure auf, ihr DDoSia-Botnetz für DDoS-Angriffe gegen westliche Internetseiten auszuführen. Das Ziel solcher hacktivistischer Angriffe besteht darin, in den westlichen Gesellschaften Vertrauen in staatliche Institutionen zu untergraben, allgemeine Verunsicherung zu schüren und eine vermeintliche Handlungsunfähigkeit des Staates zu demonstrieren.

Die Effektivität von NoName57(16)-DDoS-Angriffen gegen deutsche Ziele war im aktuellen Berichtszeitraum vergleichsweise gering. Nach der Aktion Eastwood, bei der wesentliche Teile der Infrastruktur der Gruppe abgeschaltet wurde, hat sich die Effektivität deutlich verringert. Obwohl die Gruppe ihre Durchschlagskraft seitdem nach und nach wieder erhöhen konnte, liegt sie noch immer deutlich unter den Werten vor Juli 2025. Angriffe gegen deutsche Domains (.de) sind im internationalen Vergleich deutlich seltener erfolgreich (vgl. Abbildung 4-11). Sie erhalten jedoch im vergleichsweise seltenen Erfolgsfall große mediale Aufmerksamkeit.

→ Mehr über Schadwirkungen durch das DDoSia-Botnetz

Im Zuge des russischen Angriffskriegs gegen die Ukraine finden viele feindliche Aktivitäten im Cyberraum statt, die nicht nur gegen die Ukraine gerichtet sind, sondern ebenfalls Staaten in Europa sowie die USA betreffen. So nutzen hacktivistische Bedrohungsakteure, wie die prorussische Gruppe NoName057(16), DDoS-Angriffe und Androhungen von DDoS-Angriffen, um Aufmerksamkeit zu erregen und gesellschaftliche Verunsicherung zu erzeugen. Dabei verursachen diese Angriffe generell nur temporäre Ausfälle oder Erhöhung der Antwortzeiten von Websites und keine dauerhaften Schäden. Handelt es sich allerdings um Webseiten von Regierungseinrichtungen oder Kritischen Infrastrukturen, kann das bereits dazu führen, dass das Vertrauen der Gesellschaft in die Fähigkeit des Staats abnimmt.

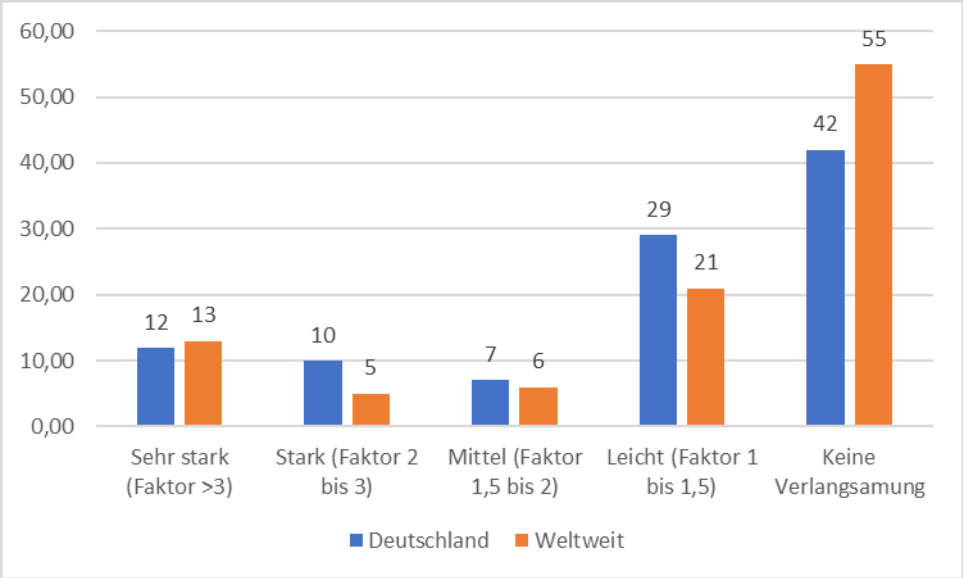
Die Gruppe NoName057(16) betreibt Telegram-Kanäle, um ihren geopolitischen Standpunkt zu verbreiten und Mitglieder zu rekrutieren, die ihre Interessen teilen und sich an Cyberangriffen beteiligen. Für die DDoS-Angriffe wird das eigens zu diesem Zweck entwickelte Tool DDoSia verwendet, dessen Instanzen wie ein Botnetz zusammenarbeiten.

DDoSia nutzt DDoS-Angriffe, das heißt massenhafte Anfragen an Websites, um deren Bandbreite und Ressourcen zu überlasten. Die Überflutung von Webservern und damit verbundenen Internetdienste mit Anfragen kann dazu führen, dass nicht mehr alle Anfragen beantwortet werden können, die Webserver also für andere Anfragen nicht mehr erreichbar sind. Ein Überlastungsangriff führt nicht immer zu Ausfällen, sondern kann stattdessen zu einer Erhöhung der Antwortzeiten der angegriffenen Server führen.

Endet der Angriff, normalisiert sich auch die Erreichbarkeit der Webserver wieder. Die Angriffe haben daher, selbst wenn sie erfolgreich sind, nur eine temporäre technische Wirkung. Ausfallzeiten der Webserver können für einige Unternehmen jedoch gegebenenfalls geschäftskritisch sein und zu einem Reputationsschaden führen. In vielen Fällen besteht der Schaden vor allem in dem häufig großen Medienecho und der verursachten Verunsicherung der Bevölkerung. Es liegt daher im Interesse der Angreifer, die von ihnen ausgehende Bedrohung größer darzustellen, als sie tatsächlich ist.

Sobald eine Seite auf der Zielliste der Hacktivisten genannt wird, warnt das BSI die Betroffenen und beginnt mit dem fortlaufenden Monitoring des Ziel-Webservers, um dessen Erreichbarkeit und damit die Effektivität des angedrohten Angriffs bewerten zu können. Von den Angriffen führten im Berichtszeitraum weltweit 15 % dazu, dass der Webserver während des Angriffs nicht mehr erreichbar war (vgl. Abbildung 4-11). Andere Angriffe waren weniger erfolgreich und führten zu geringeren Einschränkungen. Rund 41 % der Angriffe weltweit hatten keine Auswirkung auf die Erreichbarkeit der angegriffenen Webserver. Vergleicht man diese Werte für .de - Domains mit dem internationalen Durchschnitt wird deutlich, dass sich deutsche Unternehmen und Behörden bereits vergleichsweise gut gegen DDoS-Angriffe schützten (vgl. Abbildung 4-11).

Abbildung 4-12: Von DDoSia angegriffene Server in Deutschland und weltweit nach Verlangsamung
Einheit: Anteile in Prozent



Quelle: BSI

Die Operation Eastwood im Juli 2025 gegen NoName057(16)] führte dazu, dass die Effektivität der Angriffe der Gruppe vorübergehend (Juli und August 2025) abnahm und weltweit in nur knapp 30 % der Angriffe die Erreichbarkeit der angegriffenen Server um mehr als 20 % reduziert wurde (vgl. Abbildung 4-12). Im Laufe des vergangenen Berichtszeitraums wurden die Angriffe nach und nach wieder effektiver (Reduktion der Erreichbarkeit um mehr als 20 % bei mehr als 34 % der angegriffenen Server), blieben aber hinter den Werten vor Juli 2025 zurück (50 % der Server verloren mindestens 20 % Erreichbarkeit). Zudem richtete die Gruppe im Juli und August einen Schwerpunkt auf Angriffe in Deutschland, um Vergeltung für die Operation Eastwood zu üben. Die Angriffe auf .de - Domains nahmen nach dem August 2025 deutlich ab. Der Anteil der Angriffe, die die Erreichbarkeit der in Deutschland angegriffenen Server auf unter 80 % senkte, lag im Berichtszeitraum durchschnittlich bei 22 % (vgl. Abbildung 4-12).

Das Monitoring im Berichtszeitraum zeigt: Ziele in Deutschland sind bereits vergleichsweise gut gegen DDoS-Angriffe geschützt. Trotzdem sind noch immer Angriffe erfolgreich (vgl. etwa den DDoS-Angriff auf die Deutsche Bahn, DDoS-Angriffe). Organisationen, die bisher noch keinen

effektiven DDoS-Schutz haben, sollten ihre Schutzmaßnahmen verbessern. Das BSI hält zudem eine Liste qualifizierter Mitigationsdienstleister bereit.

Ausgewählte Vorfälle: Schadwirkungen
Datenleak bei KI-basierter Bild- und Videobearbeitungs-App

Sachverhalt

Sicherheitsforschende von Cybernews, einem Nachrichtenportal und Forschungsunternehmen für Cybersicherheit, haben eine unzureichend gesicherte Datenbank bei der KI-App „Video AI Art Generator & Maker“ gefunden. Die APP dient der Bild- und Videobearbeitung. Aufgrund eines falsch konfigurierten Google Cloud Storage Buckets waren die Medieninhalte mit einem Gesamtumfang von zwölf Terabyte öffentlich und ohne Authentisierung zugänglich.

Betroffen waren sowohl mehr als 1,5 Millionen von Nutzerinnen und Nutzern hochgeladene Bilder und mehr als 385.000 Videos. Des Weiteren waren auch rund drei Millionen KI-generierte Videos und Bilder und mehr als 386.000 KI-generierte Audiodateien betroffen.

Die betroffene App war mit über 500.000 Downloads und einer durchschnittlichen Bewertung von 4,3 (von 5) im Google Play Store gelistet und wurde zwischenzeitlich entfernt. Der Entwickler mit Sitz in der Türkei fiel laut Sicherheitsforschenden bereits zuvor durch fehlerhaft konfigurierte Backend-Dienste auf.

Bewertung

KI-gestützte Apps und Tools für den privaten Gebrauch gewinnen zunehmend an Popularität. Parallel dazu häufen sich auch Sicherheitsvorfälle, bei denen Bildmaterial, Standortdaten oder weitere sensible Informationen unzureichend geschützt oder offengelegt werden. Insbesondere besteht das Risiko für KI-gestützten Identitätsmissbrauch, zum Beispiel im Rahmen von Social-Engineering-Angriffen oder Deepfake-Szenarien.

Reaktion

Betroffenen wird empfohlen, die App umgehend zu deinstallieren und mögliche verbliebene App-Rückstände auf den Endgeräten zu entfernen. Darüber hinaus ist erhöhte Wachsamkeit im Hinblick auf potenzielle missbräuchliche Verwendung der möglicherweise abgeflossenen Bild- und Videoinhalte geboten. Werden entsprechende Missbrauchsfälle bekannt, sollte unverzüglich Anzeige bei den zuständigen Strafverfolgungsbehörden erstattet werden.

5 Resilienz

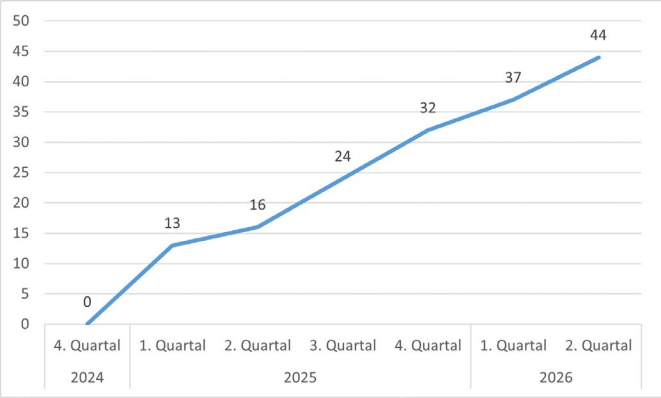
Cyberresilienz ist der Schlüssel einer erfolgreichen Digitalisierung. Dazu gehören widerstandsfähige IT-Produkte und IT-Infrastrukturen ebenso wie problembewusste Organisationen in Staat, Wirtschaft und Gesellschaft und Verbraucherinnen und Verbraucher, die die Resilienz-Maßnahmen für ihre digitalen Angriffsflächen vor dem Hintergrund wachsender Bedrohungen etwa durch automatisierte Angriffe mit KI wirksam vorantreiben. Während der staatlich regulierte Schutz von IT-Produkten und IT-Infrastrukturen im aktuellen Berichtszeitraum etwa mit dem Cyber Resilience Act (CRA) weiter vorangetrieben wurde (vgl. Resiliente IT-Produkte und IT-Infrastrukturen), zeigte sich insbesondere bei nicht regulierten Organisationen in Staat, Wirtschaft und Gesellschaft sowie bei Verbraucherinnen und Verbrauchern verbreitet digitale Sorglosigkeit – ablesbar insbesondere an dem sich hartnäckig haltenden Irrglauben, kein lohnendes Ziel und insgesamt gut aufgestellt zu sein (vgl. Resiliente Gesellschaft, Resiliente Wirtschaft).

5.1 Resiliente IT-Produkte und IT-Infrastrukturen

KI-Modelle, vernetzte Geräte (IoT), 5G/6G- oder Cloud-Infrastrukturen – Resiliente IT-Produkte und IT-Infrastrukturen sind Voraussetzung für die sichere Digitalisierung der Cybernation Deutschland.

5.1.1 Cyber Resilience Act

Abbildung 5-1: Fortschritt der CRA-Standardisierungsaktivitäten
Einheit: Anteile in Prozent



Quelle: BSI

Der Cyber Resilience Act (CRA) legt EU-weit verbindliche Cybersicherheits-Anforderungen für Produkte, mit digitalen Elemente fest. Cybersicherheit ist damit keine freiwillige Zugabe von Herstellern mehr, sondern gehört zu den Grundprinzipien der Digitalisierung und Produktsicherheit in Europa.

Die Standardisierungsaktivitäten im Zusammenhang mit dem CRA sind im aktuellen Berichtszeitraum weiter vorangeschritten. Der Erfüllungsstand umfasste zum 30. Juni 2026 44 % der geplanten Aktivitäten (vgl. Abbildung 5-1).

→ Mehr über den Cyber Resilience Act

Standardisierung

Die im Cyber Resilience Act (CRA) enthaltenen Anforderungen werden in Form harmonisierter Normen durch die europäischen Normungsorganisationen ETSI, CEN und CENELEC spezifiziert.

Die Anforderungen des CRA werden dabei sowohl in produktunabhängigen als auch in produktspezifischen Normen durch Beteiligte aus Wirtschaft, Gesellschaft und Staat umgesetzt. Das BSI bringt hierfür seine umfassende Sicherheitsexpertise ein, ausgerichtet an den zentralen Zielen „hohe Qualität“, „Nutzerfreundlichkeit“ sowie „Security by Design“ und „Security by Default“.

Sobald eine neue Norm eine ausreichende Qualität erreicht und von der Europäischen Kommission im Amtsblatt der Europäischen Union (EU) nach Artikel 27 CRA gelistet wurde, besteht durch die Anwendung dieser harmonisierten Norm die Konformitätsvermutung mit den grundlegenden Anforderungen des CRA.

TR-03183 - eine Anleitung für den CRA

Nur spezielle Produkttypen fallen unter die wichtige oder kritische Produktkategorie, für die die harmonisierten europäischen Normen entwickelt werden. Die meisten Produkte, die unter den CRA fallen, sind Produkte der sogenannten „Default-Kategorie“. Für diese Produkte bietet das BSI mit der TR-03183 eine konkrete Umsetzungshilfe für Hersteller.

Durch ein einfaches und strukturiertes, risikobasiertes Vorgehen, konkrete Produktanforderungen mit Umsetzungshinweisen sowie ausführlichen Informationen zu SBOMs (formalen, maschinenlesbaren Inventarlisten von Softwareprodukten) und Coordinated Vulnerability Disclosure, bietet die TR-03183 kleineren Herstellern die Möglichkeit, sich auf den CRA vorzubereiten. Zusammen mit anpassbaren Workflows und dem Format OSCAL, einem international anerkannten, maschinenlesbaren Standard für Sicherheitsanforderungen, bietet die TR-03183 auch die Möglichkeit, Tooling für den CRA zu entwickeln, um das Thema Cybersicherheits-Compliance gezielt zu digitalisieren.

Die TR-03183 wird aktiv mit aktuell 80 Teilnehmern aus Wirtschaft, Verwaltung und IT-Sicherheitscommunity in GitHub weiterentwickelt. Sie wurde mit Stand 30. Juni 2026 insgesamt mehr als 1.500-mal abgerufen. Die Nachfrage durch die Wirtschaft an Unterstützungsleistungen für den CRA ist hoch, das zeigt die Erfahrung aus Herstellergesprächen und ein hoher Andrang bei entsprechenden Informationsveranstaltungen des BSI.

Aufbau einer Konformitätsbewertungsinfrastruktur (Notifizierung)

Hersteller von im CRA-gelisteten Produkten mit digitalen Elementen müssen in einigen Fällen eine Drittstellenbewertung durchlaufen. Hierfür werden kompetente Konformitätsbewertungsstellen (KBS) benötigt. Das BSI ist für die Notifizierung von KBS unter dem CRA zuständig. Hierbei wird nach erfolgreicher Bewertung den KBS bestätigt, dass sie fähig sind, die Anforderungen aus dem CRA korrekt zu überprüfen. In Deutschland wird für die Notifizierung eine erfolgreiche Akkreditierung im Geltungsbereich CRA vorausgesetzt.

Meldepflicht

Seit dem 11. September 2026 gelten die Meldepflichten des Cyber Resilience Act (CRA). Sie betreffen Hersteller von Produkten mit digitalen Elementen im Sinne des CRA, die ihre Produkte auf dem Binnenmarkt der EU bereitstellen. Meldepflichtig sind aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle mit Auswirkungen auf die Sicherheit von Produkten mit digitalen Elementen. Ab dem 11. Dezember 2027 gilt auch eine Meldepflicht für Open Source Stewards, das heißt diejenigen Organisationen, die die Entwicklung von Open Source Software vorantreiben und verantworten.

Die von der Agentur der Europäischen Union für Cybersicherheit (ENISA) entwickelte und betriebene CRA Single Reporting Platform (CRA-SRP) ist die zentrale, EU-weit einheitliche englischsprachige Meldeplattform. Hersteller übermitteln ihre jeweilige Meldung nur einmal. Die Meldung wird gleichzeitig dem zuständigen, als Koordinator benannten Computer Security Incident Response Team (CSIRT) und der ENISA zugänglich gemacht. Das koordinierende CSIRT kann die Informationen anschließend an weitere betroffene CSIRTs und erforderlichenfalls an die zuständigen Marktüberwachungsbehörden weitergeben. In Deutschland ist das CERT-Bund als koordinierendes CSIRT im BSI ansässig.

Marktüberwachung

Das BSI ist zudem für die Marktüberwachung im Rahmen des CRA zuständig. Dies umfasst seit September 2026 Schwachstellen-Meldeverpflichtungen sowie ab Dezember 2027 verpflichtende

Produktanforderungen für jedes Produkt mit digitalen Elementen, das in Europa in Verkehr gebracht wird. Das BSI stellt die Einhaltung der gesetzlichen Anforderungen sicher, indem es Produkte stichprobenartig proaktiv oder reaktiv untersucht und falls notwendig verhältnismäßige Folgemaßnahmen durchführt. Damit kann das BSI künftig in bestimmten Fällen sogar Produkte mit digitalen Elementen vom Markt zu nehmen, wenn sie den Anforderungen des CRA nicht gerecht werden

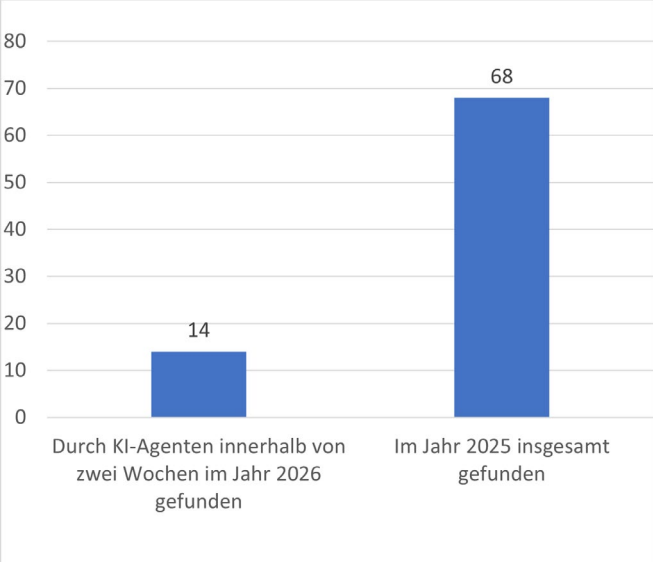
Europäische Koordinierung

Der CRA ist ein europäisches Großvorhaben, das nur gemeinsam und einheitlich mit allen Mitgliedsländern funktionieren kann. Zentrales Koordinierungsgremium ist hierbei die AdCO CRA, die für eine effiziente übergreifende Zusammenarbeit und Kommunikation der europäischen Marktüberwachungsbehörden sorgen und eine einheitliche Auslegung der Marktüberwachungen im europäischen Binnenmarkt gewährleisten soll. Den aktuellen Vorsitz der AdCO hat das BSI inne und leistet damit einen zentralen Beitrag zur europäischen Harmonisierung. Des Weiteren ist das BSI aktiv in der CRA Expert Group vertreten, um zusammen mit seinen Partnerbehörden und Organisationen der europäischen Wirtschaft, Zivilgesellschaft und ausgewählten Expertinnen und Experten Fragestellungen des CRA zu konkretisieren und den CRA weiterzuentwickeln. Mit der aktiven Teilnahme an der Notifying Authorities Group, dem zentralen Koordinierungsgremium der Notifizierenden Behörden, setzt sich das BSI zudem für eine europäisch harmonisierte und qualitativ angemessene Konformitätsbewertungsinfrastruktur für den CRA ein.

5.1.2 LLMs als Hochgeschwindigkeits-Schwachstellenscanner

Abbildung 5-2: Fallstudie: Schwachstellen mit hohem Schweregrad in verbreitetem Internet-Browser

Einheit: Anzahl



Quelle: Anthropic

Bemerkung: In Anthropic Fallstudie durch Frontier-Modelle gefundene Schwachstellen

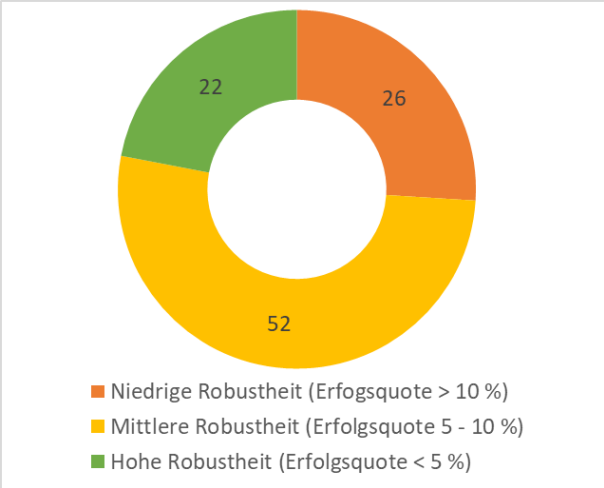
Im Rahmen einer Studie fand ein KI-Agent Anfang des Jahres 2026 innerhalb von zwei Wochen 22 neue Schwachstellen in einem bekannten Browser, davon 14 mit hohem Schweregrad (vgl. Abbildung 5-2). Auf konventionelle Weise wurden im ganzen Jahr 2025 insgesamt 68 neue Schwachstellen mit hohem Schweregrad gefunden. Dies veranschaulicht das enorme Potenzial von KI-Technologie zur Identifizierung neuer Schwachstellen (vgl. auch Angriffsinfrastrukturen).

Verteidigern und Angreifern stehen damit zunehmend wirksame Werkzeuge zur Verfügung, um Schwachstellen in Code zu finden. Es ist noch nicht absehbar, über welche Zeiträume dies zu einer Vergrößerung oder Verkleinerung der Angriffsfläche führt. Entscheidend ist, dass entsprechende Werkzeuge von Verteidigern schnell adaptiert werden, um langfristig einen positiven Effekt zu bewirken.

Mit dem Vorliegen entsprechend performanter Tools ist auf Herstellerseite eine hohe Effizienz und Automatisierung bei der Priorisierung, Mitigation und Behebung von Schwachstellen nötig. Auf Seiten der Anwenderinnen und Anwender gilt das analog für das Patchmanagement. Gleichzeitig sinkt die Einstiegshürde für Angreifer. Security-In-Depth und Zero-Trust-Ansätzen kommt damit eine noch höhere Bedeutung zu.

5.1.3 LLM-Härtung

Abbildung 5-3: 31 Sprachmodelle nach Robustheit gegen Prompt Injections, 2024 bis 2026
Einheit: Anteile in Prozent



Quelle: BSI
Bemerkung: Basiert auf CyberSecEval 2 Prompt Injection Benchmark (Meta AI, 2024). Die Ergebnisse sind als untere Schranke des tatsächlichen Risikos zu sehen.

Unter der Härtung eines Sprachmodells versteht man Maßnahmen, die direkt am Modell ansetzen, um dessen Robustheit und Zuverlässigkeit zu erhöhen. Dazu gehören bereits die sorgfältige Auswahl und Aufbereitung der Trainingsdaten, die Ausrichtung des Modells auf gewünschtes Verhalten durch sogenannte Alignment-Verfahren (zum Beispiel Supervised Fine-Tuning oder Reinforcement Learning from Human/AI Feedback) sowie Trainings- und Evaluationsverfahren, die die Widerstandsfähigkeit gegenüber Manipulationsversuchen erhöhen. Ziel ist es, dass das Modell auch bei ungewöhnlichen oder böswilligen Eingaben zuverlässig und sicher reagiert. Zu solchen Manipulationsversuchen zählen insbesondere Prompt Injections, bei denen Angreifer die Ausgaben von KI-Systemen gezielt beeinflussen, indem sie dem Modell irreführende oder widersprüchliche Anweisungen einschleusen.

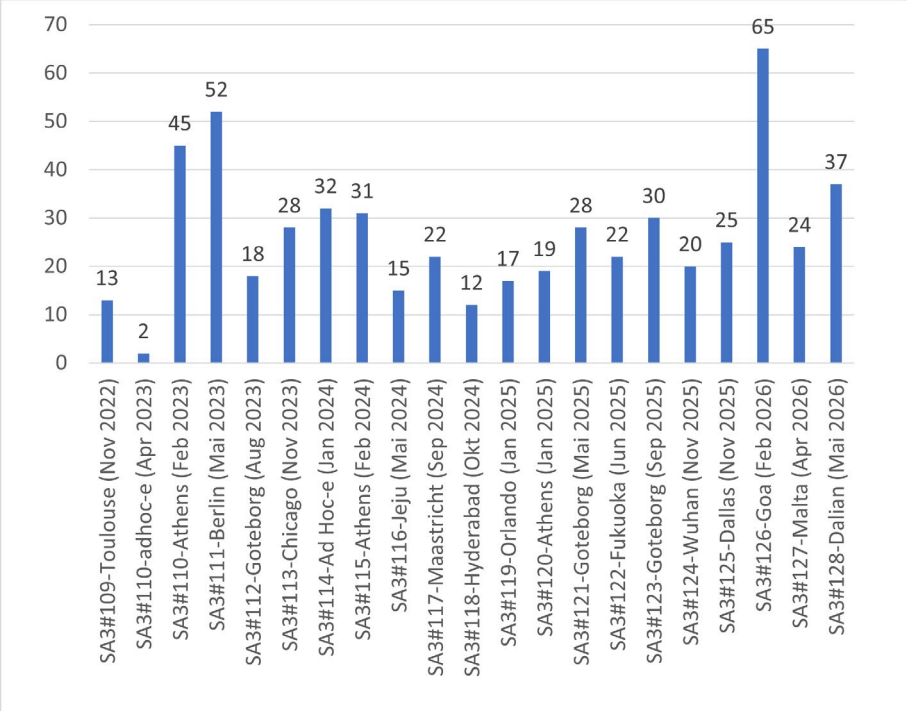
Insgesamt 31 Modelle hat das BSI unter Laborbedingungen auf ihre Härte getestet. Ergebnis: Kein Modell ist immun – selbst das in dieser Hinsicht beste Modell konnte in 2,4 % der Fälle durch den Angriff kompromittiert werden (vgl. Abbildung 5-3). Bei 24 der 31 getesteten Modelle sind es über 5 % und bei acht der Modelle sogar über 10 %.-Unter realen Bedingungen können die Kompromittierungsraten höher ausfallen.

Unabhängiges Benchmarking und eine transparente Veröffentlichung der Ergebnisse sind notwendig, damit Entwicklerinnen und Entwickler sowie Nutzende Modelle fundiert auswählen und Hersteller ihre Härtung gezielt verbessern können. Das BSI setzt sich dafür ein, dass Benchmarks entwickelt und die Ergebnisse veröffentlicht werden.

Gleichzeitig bleibt die Modellhärtung nur eine erste Präventionsmaßnahme. Für den sicheren Einsatz von KI-Agenten sind mehrschichtige Maßnahmen, Transparenz in der Lieferkette sowie anschlussfähige Normen und Standards erforderlich. Das BSI engagiert sich in diesen Bereichen national sowie international, um allen beteiligten Akteuren Orientierung zu bieten.

5.1.4 5G/6G-Mobilfunkstandard

Abbildung 5-4: BSI-Beiträge im Standardisierungsgremium 3GPP SA3
Einheit: Anzahl



Quelle: BSI

5G-Netze und zukünftige 6G-Netze bilden als Schlüsseltechnologien das Rückgrat einer leistungsfähigen digitalen Infrastruktur für die Cybernation Deutschland, die gegenüber Bedrohungen robust und sicher aufgestellt sein muss.

Das BSI hat seine Aktivitäten in dem Gremium 3GPP, dem weltweit wichtigsten Standardisierungsgremium für die Entwicklung von Mobilfunktechnologien, von 120 Beiträgen im vergangenen Berichtszeitraum auf 201 Beiträge im aktuellen Berichtszeitraum erhöht (vgl. Abbildung 5-4). Die vertiefte Arbeit in der Arbeitsgruppe SA3 (Security and Privacy) zur Verbesserung von standardisierten Sicherheitsprüfungen (SCAS-Tests) bei 5G hat zudem zur zunehmenden Beteiligung des BSI bei benachbarten Themen geführt (zum Beispiel Post-Quantum Cryptography, kurz PQC, und Security by Design).

→ Mehr über 5G/6G-Mobilfunkstandard

Im hauseigenen 5G/6G-Security Lab hat das BSI neben der bereits bestehenden Testinfrastruktur von Ericsson auch die Testmöglichkeiten durch ein Nokia-System und ein O-RAN-Campusnetz sowie einem neuen 5G-Roaming-Testszenario ausgebaut. Beim ersten 5G-Hackathon mit externen Expertinnen und Experten wurden ebenfalls diverse Sicherheitstests durchgeführt.

Die 5G-Zertifizierungsprogramme wurden weiterentwickelt. Die Zahl der Zertifizierungsanträge nahm zu und es wurden erste IT-Sicherheitszertifikate erteilt. Praxiserfahrungen wurden in die 3GPP SA3 und die GSMA NESAS Group (Network Equipment Security Assurance Scheme) eingebracht. Das BSI wirkte weiter an der Entwicklung des CSA-Zertifizierungsschemas EU NESAS für RAN- und Kernnetzausrüstung mit.

Als eine der zentralen Maßnahmen stellt die Auditierung der nationalen 5G-Mobilfunknetzbetreiber gemäß §165 Absatz 9 und §166 Absatz 5 TKG sicher, dass die gesetzlich geforderten technischen und organisatorischen Maßnahmen, die unter anderem in den Bereichen Business Continuity Management und Notfallmanagement umgesetzt werden, in solchen Situationen effektiv greifen und kontinuierlich verbessert werden.

5.1.5 Zertifizierung und Kennzeichen

Abbildung 5-5: das IT-Sicherheitskennzeichen des BSI



Quelle: BSI

Der Sicherheitsgrad BSI-zertifizierter IT-Produkte geht über den durch den CRA vorgeschriebenen Sicherheitsstandard hinaus. So können Hersteller beispielsweise ein IT-Sicherheitskennzeichen oder eine Common-Criteria-Zertifizierung beantragen. Für digitale Gesundheitsanwendungen etwa benötigen Hersteller eine Zertifizierung nach Technischer Richtlinie. Zudem zertifiziert das BSI auch Personen, beispielsweise als Grundschutzberater.

→ Mehr über Zertifizierung

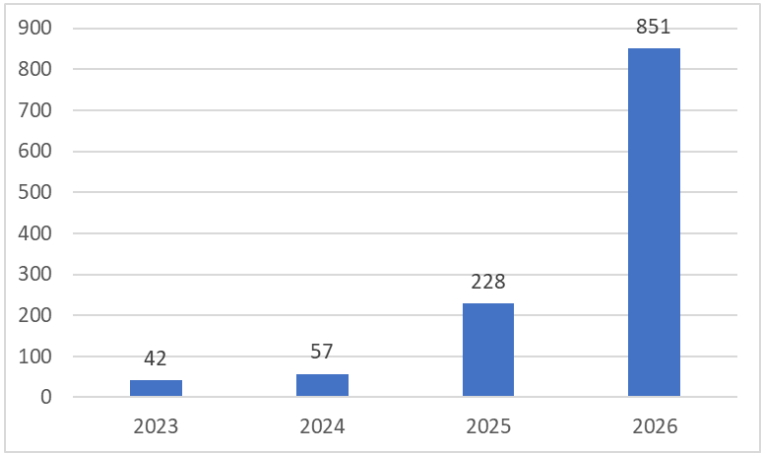
IT-Sicherheitskennzeichen

Das IT-Sicherheitskennzeichen des BSI bietet einen niedrigschwelligen Einstieg in die Kennzeichnung und Zertifizierung von Produkten und Diensten. Hersteller verpflichten sich freiwillig, definierte Sicherheitsanforderungen einzuhalten, bekannte Schwachstellen zu melden und sicherheitsrelevante Updates bereitzustellen. Für Verbraucherinnen und Verbraucher wird das Engagement der Hersteller in Cybersicherheit durch das Kennzeichen sichtbar, es schafft Transparenz über die Sicherheitseigenschaften eines Produkts und erleichtert eine informierte Kaufentscheidung. Gleichzeitig entsteht ein Marktanreiz für Hersteller, IT-Sicherheit stärker schon in die Entwicklung ihrer Produkte zu integrieren („Security by Design“) und ihre Produkte damit präventiv vor möglichen Sicherheitsvorfällen zu schützen.

Seit der Einführung des Kennzeichens im Jahr 2021 wurden sechs Produktkategorien in das Verfahren aufgenommen. Seitdem steigen die Anträge und Erteilungen kontinuierlich. Im aktuellen Berichtszeitraum war ein sprunghafter Anstieg zu verzeichnen, der auf die zunehmende Beteiligung großer Hersteller zurückzuführen ist (vgl. Abbildung 5-6).

Abbildung 5-6: Bestand an IT-Sicherheitskennzeichen

Einheit: Anzahl (kumuliert)



Quelle: BSI

Auch im internationalen Kontext hat sich das deutsche Kennzeichnungsschema als Blaupause für verschiedenartige Labelling-Schemata bewiesen, beispielsweise in der Arbeitsgruppe zum ISO-

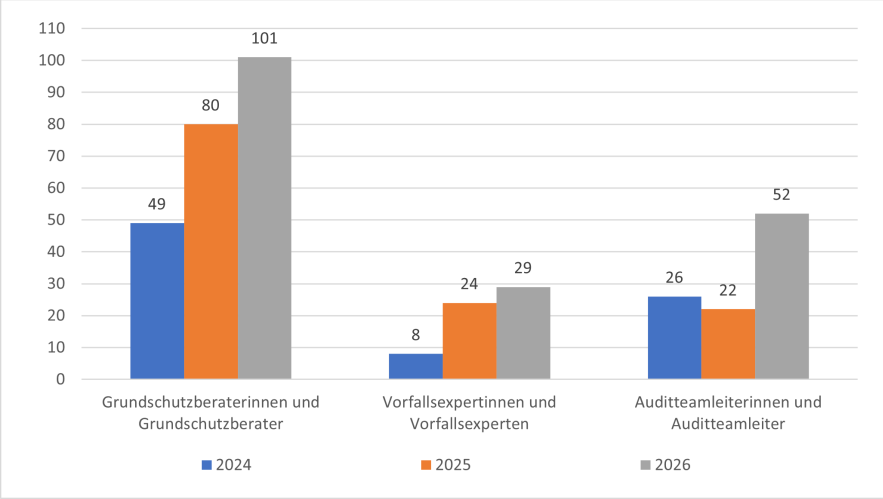
Standard 27404, die das Labelling von IoT-Geräten normiert, sowie im Austausch mit Australien, das die Einführung eines Kennzeichnungsschemas für die Cybersicherheit vernetzter Verbraucherprodukte plant. Durch bereits geschlossene sowie geplante Anerkennungsabkommen gestaltet das BSI die Etablierung und Harmonisierung von Cybersicherheitskennzeichnungen so auch über Landesgrenzen hinweg aktiv mit.

Mehr erfahren unter www.bsi.bund.de/it-sik.

Personenzertifizierung des BSI

Cyberangreifer erzielen aufgrund schlecht geschützter Angriffsflächen erhebliche Schadwirkungen (vgl. Lösegelder). Die steigende Nachfrage nach BSI-Personenzertifizierungen zeigt, dass die Herausforderungen zunehmend erkannt und angegangen werden. Die Personenzertifizierung dient als Fachkundenachweis und erhöht die Reputation der Person bzw. des Unternehmens, bei dem sie tätig ist (vgl. Abbildung 5-7).

Abbildung 5-7: Ausgewählte Personenzertifizierungen
Einheit: Anzahl



Quelle: BSI

- *Zertifizierte Grundschutzberaterinnen und Grundschutzberater* unterstützen Organisationen bei der Einführung eines Informationssicherheitsmanagementsystems (ISMS) und begleiten Institutionen fachkundig bei der Etablierung entsprechender Prozesse. Darüber hinaus können sie bei der Vorbereitung auf Audits beratend tätig werden.
- *Zertifizierte Vorfallexpertinnen und Vorfallsexperten* stehen betroffenen Stellen und Personen im Falle eines IT-Sicherheitsvorfalls unterstützend zur Seite. Zu ihren zentralen Aufgaben zählen die Analyse von Sicherheitsvorfällen, die Begrenzung des entstandenen Schadens, die Untersuchung der zugrunde liegenden Ursachen sowie die Wiederherstellung der betroffenen Systeme.
- *Zertifizierte Auditteamleiterinnen und Auditteamleiter* sind für die Planung und Durchführung von Audits verantwortlich. Diese dienen Organisationen dazu, eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz zu erlangen und dauerhaft aufrechtzuerhalten.

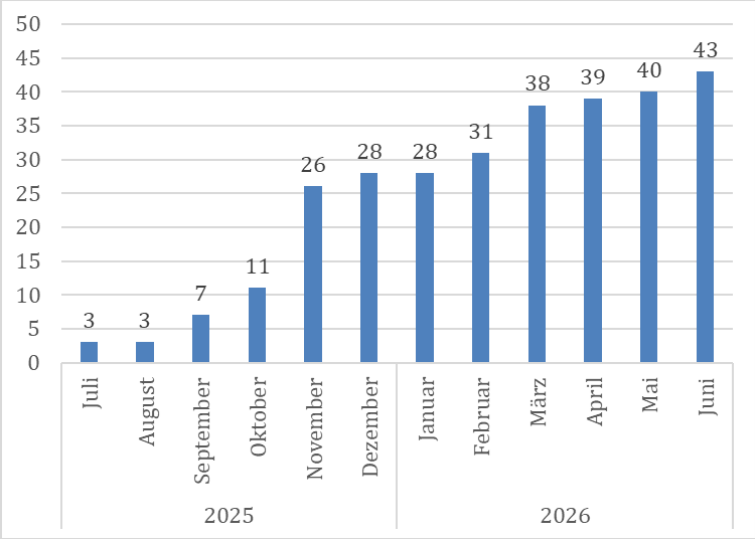
Weitere Informationen hält das BSI im Internet bereit (vgl. www.bsi.bund.de/dok/127736).

Apps auf Rezept: TR-Zertifizierung für Digitale Gesundheitsanwendungen

Mit sogenannten „Apps auf Rezept“ können Ärztinnen und Ärzte in Deutschland Digitale Gesundheitsanwendungen (DiGA) verordnen. Die Apps unterstützen Patientinnen und Patienten und die Behandelnden bei der Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten, wobei die Kosten von den gesetzlichen Krankenkassen übernommen werden.

Damit DiGAs zugelassen werden, müssen sie strenge Anforderungen erfüllen. Neben dem medizinischen Nutzen spielt vor allem die IT-Sicherheit eine zentrale Rolle. Hier setzt die Technische Richtlinie TR-03161 „Anforderungen an Anwendungen im Gesundheitswesen“ des BSI an. Sie legt fest, wie besonders sensible Gesundheitsdaten, deren Verlust oder Manipulation erhebliche Folgen für Patientinnen und Patienten hätte, geschützt werden. Erst wenn die Anforderungen der Richtlinie nachweislich erfüllt sind, können DiGAs dauerhaft als App auf Rezept eingesetzt werden. Die BSI-Zertifizierung nach Technischen Richtlinien bestätigt durch eine unabhängige Prüfung und formale Bescheinigung des BSI, dass die DiGA die Anforderungen erfüllt.

Abbildung 5-8: Zertifizierte Digitale Gesundheitsanwendungen
Einheit: Anzahl (kumuliert)



Quelle: BSI

Um im sensiblen Bereich Digitaler Gesundheitsanwendungen Updates schneller bereitzustellen, hat das BSI Anfang 2026 seine Zertifizierung nach Technischen Richtlinien flexibler gestaltet. Hersteller können sicherheitsrelevante Updates nun zeitnah ausrollen, ohne jeweils eine neue Zertifizierung durchlaufen zu müssen. So bleibt die Aussagekraft des Produktzertifikats erhalten, während gleichzeitig schnellere Entwicklungs- und Update-Zyklen möglich werden (vgl. Abbildung 5-8). Grundlage dafür ist die Technische Richtlinie TR-03185 „Sicherer Software-Lebenszyklus“, die Anforderungen an verlässliche und sichere Entwicklungsprozesse festlegt.

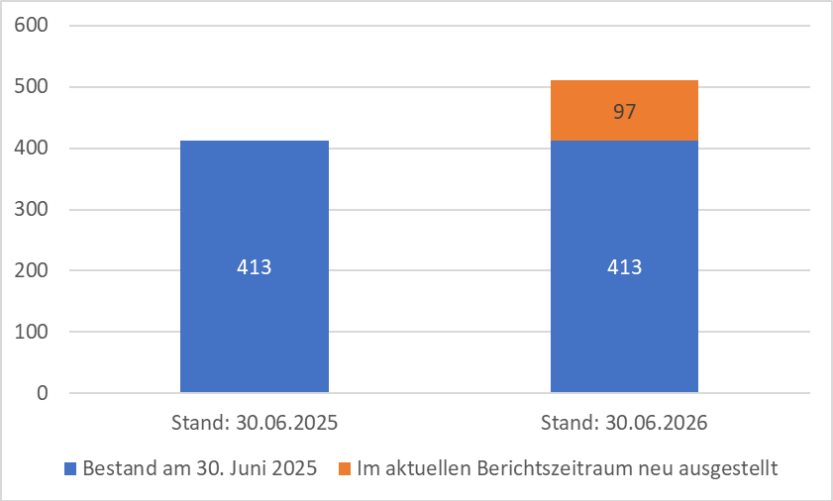
Auf diese Weise schafft die Zertifizierung durch das BSI ein Vertrauen in Produkte für eine sichere Digitalisierung im Gesundheitswesen.

Mehr erfahren: www.bsi.bund.de/dok/TR-03161

Transformation und Umstellung der Common-Criteria-Zertifizierung nach EUCC

Common-Criteria-Zertifizierung (CC-Zertifizierung) ist ein international anerkannter Standard zur Prüfung und Bewertung der Cybersicherheit von Produkten. Im Berichtzeitraum lag für die Common Criteria-Zertifizierung im BSI ein wichtiger Meilenstein: Das CC-Schema des BSI und das europäische Anerkennungsabkommen SOG-IS wurden weitgehend durch das neue EUCC-Schema der EU-Kommission ersetzt. Der Durchführungsrechtsakt 2024/482, basierend auf der EU-Verordnung 2019/881, stellt die neue gesetzliche Grundlage dar. Zertifikate auf Grundlage des EUCC-Schemas sind innerhalb der gesamten EU gültig. Bis Februar 2026 hat das BSI alle Verfahren nach seinem bisherigen CC-Schema beendet. Da die CC-Zertifizierung bei vielen Antragstellern tief in Abläufe integriert ist, erfolgte die Umstellung erst kurz vor Ablauf der Fristen, sodass Anfang 2026 eine besonders hohe Zahl an Zertifikaten ausgestellt wurde. Seither steigt die Zahl der ausgestellten EUCC-Zertifikate kontinuierlich (vgl. Abbildung 5-9).

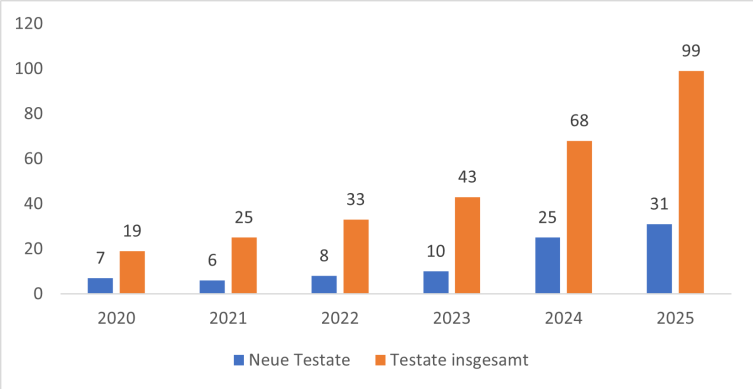
Abbildung 5-9: Common-Criteria-Zertifizierungen
Einheit: Anzahl



Quelle: BSI

5.1.6 Cloud-Sicherheit

Abbildung 5-10: Cloud Service Provider mit C5-Testat
Einheit: Anzahl



Quelle: www.c5-attestations.com

Der Cloud Computing Compliance Criteria Catalogue des BSI (BSI C5) beschreibt das Mindestmaß an Informationssicherheit bei der Erbringung von Cloud-Diensten. Cloud-Dienste für die Bundesverwaltung müssen bereits seit 2017 die Einhaltung der C5-Kriterien nachweisen. Für Cloud-Dienste in der Gesundheitsbranche trat am 1. Juli 2024 der neue § 393 des SGB V in Kraft. In diesem wird unter anderem auch geregelt, dass für Cloud-Dienste im Gesundheitswesen ein C5-Testat oder vergleichbare Testate oder Zertifikate erforderlich sind.

Die Zahl der Cloud-Dienste mit C5-Testat ist im Jahr 2025 signifikant auf 99 Dienste insgesamt und damit um 46 %gegenüber dem Vorjahr gestiegen (vgl. Abbildung 5-10, www.c5-attestations.com). Dadurch steigt für potenzielle Kundinnen und Kunden die Auswahl sicherer Cloud-Dienste.

Zudem wurde im aktuellen Berichtszeitraum der neue C5 veröffentlicht.

→ Mehr über Cloud-Sicherheit

Das BSI unterstützt die öffentliche Verwaltung bei Fragestellungen rund um das Thema sichere Nutzung von Cloud-Infrastrukturen und Cloud-Diensten. Betrachtet wird hierbei der komplette Lifecycle, das heißt Planung, Auswahl und Beschaffung, Implementierung, Nutzung, Einsatz und auch die Beendigung von Cloud-Diensten.

Das BSI berät rund um die sichere Nutzung von Cloud-Diensten. Zur Zielgruppe gehören primär Stellen des Bundes, die bei der Umsetzung des Mindeststandards zur Nutzung externer Cloud-Dienste Unterstützung benötigen. Der Fokus liegt häufig auf essenziellen Schritten vor dem Beginn einer Cloud-Nutzung, zum Beispiel der Erstellung einer Cloud-Nutzungsstrategie, Anforderungen an Cloud-Dienste oder dem korrekten Umgang mit dem Kriterienkatalog C5 und die Auswertung von C5-Testaten. Für die Erstellung einer Cloud-Nutzungsstrategie hat das BSI ein Format für den Strategieprozess erstellt, bei mehreren Behörden bereits durchgeführt und am 6. Oktober 2025 als „Management-Blitzlicht“ veröffentlicht.

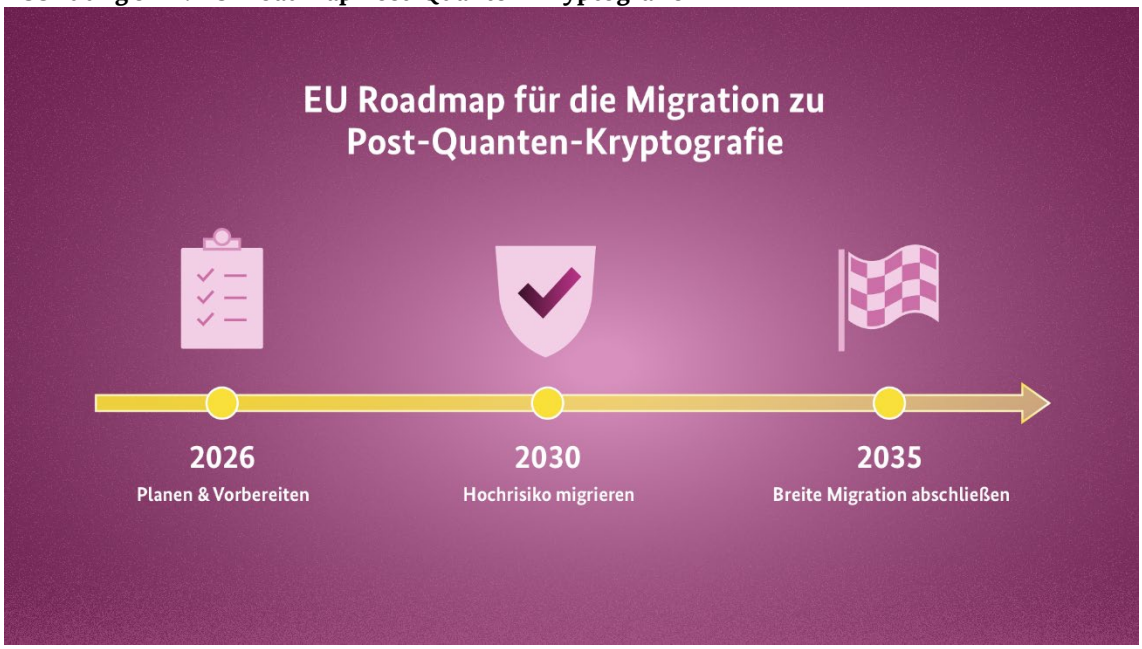
Das BSI ist zudem im Architekturboard der Deutschen Verwaltungscloud vertreten und liefert im Themenkreis zu Informationssicherheit und Datenschutz Impulse zur frühzeitigen Berücksichtigung von Cloud-Sicherheit in wichtigen Planungsprozessen. Ferner ist das BSI am GovTech Deutschland (ehemals GovTech Campus) beteiligt und steht in kontinuierlichem Austausch mit dem Cloud-Reallabor der Deutschen Rentenversicherung Bund um die dortigen Cloud-Projekte (zum Beispiel Anwendung von C5, Verprobung von Wechselfähigkeit) zu begleiten.

Cloud-Lösungen der Hersteller prüft das BSI eingehend und in der notwendigen Sorgfalt im Rahmen von Kooperationsvereinbarungen: Sie bilden einen verbindlichen Rechtsrahmen, um hoch vertrauliche Informationen auszutauschen und technische Analysen und Bewertungen durchführen zu können.

Innerhalb der Kooperationen führt das BSI Risiko- und Bedrohungsanalysen durch, um davon technische und strukturelle Sicherheitsanforderungen und -maßnahmen abzuleiten, die standortunabhängig für alle Cloud Service Provider gelten sollen.

5.1.7 Post-Quanten-Kryptografie

Abbildung 5-11: EU-Roadmap Post-Quanten-Kryptografie



Quelle: BSI

Um der wachsenden Bedrohung durch Quantencomputer zu begegnen, hat die EU eine koordinierte Roadmap für die Umstellung auf Post-Quanten-Kryptografie definiert. Diese sieht vor, dass Mitgliedstaaten bis Ende 2026 nationale Umsetzungspläne entwickeln, kritische Anwendungen bis 2030 umstellen und die Migration bis 2035 weitgehend abschließen.

→Mehr über Post-Quanten-Kryptografie

Aktuell noch sichere Verschlüsselungstechnologien werden durch die Entwicklung von Quantencomputern obsolet.

Während der Übergangsphase zur Post-Quanten-Kryptografie bis 2035 sind Präventionsmaßnahmen in Wirtschaft, Verwaltung, Wissenschaft und anderen Organisationen darauf ausgerichtet, Risiken bei bereits eingesetzten kryptografischen Verfahren zu begrenzen. Eine zentrale Maßnahme ist der Einsatz hybrider Verfahren, bei denen klassische und quantensichere Algorithmen kombiniert werden, sodass ein Bruch eines einzelnen Verfahrens nicht unmittelbar zur Kompromittierung führt.

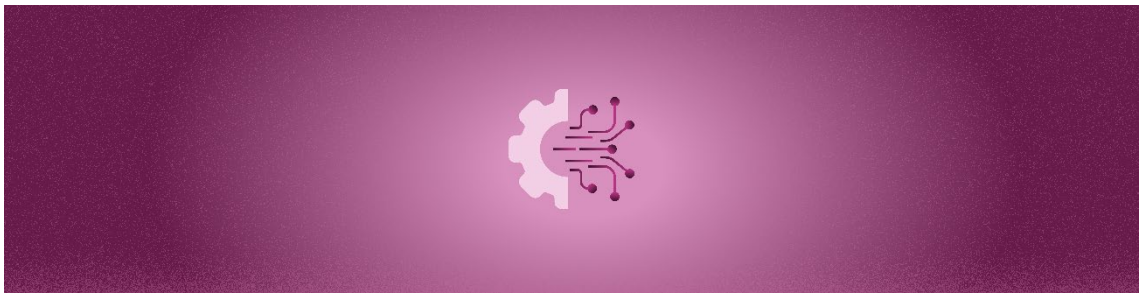
Ergänzend bleiben etablierte Sicherheitsmechanismen relevant, etwa die Prüfung und Sperrung von Zertifikaten sowie die Absicherung von Protokollen (z. B. TLS) gegen Implementierungs- und Downgrade-Angriffe. Bei Implementierungsangriffen nutzt der Angreifer Schwächen in der Implementierung eines Systems anstelle von Schwachstellen in dem System selbst. Downgrade-Angriffe zeichnen sich dadurch aus, dass der Angreifer etwa Abwärtskompatibilitäten ausnutzt, um ein System in einen weniger sicheren Zustand zu versetzen. Eine zentrale Rolle spielt zudem Kryptoagilität, also die Fähigkeit, kryptografische Verfahren flexibel auszutauschen. Dadurch können Systeme bei Bekanntwerden neuer Schwachstellen oder technologischen Entwicklungen zeitnah angepasst werden.

Notfallpläne und vorbereitete Migrationsstrategien sind zentral, um Systeme zeitnah und priorisiert umzustellen. Ebenso ist die Etablierung robuster und quantensicherer Update-Mechanismen entscheidend, um betroffene Komponenten, Konfigurationen und kryptografische Verfahren bei neuen Anforderungen oder Bedrohungen anpassen zu können.

Falls kryptografische Verfahren durch Quantenangriffe kompromittiert werden, zielen Bewältigungsmaßnahmen darauf ab, Schäden zu begrenzen und einen sicheren Betrieb zu gewährleisten. Dazu gehören insbesondere der schnelle Austausch kompromittierter Schlüssel und Zertifikate sowie die Migration betroffener Systeme auf quantensichere Verfahren.

Für bereits abgeflossene oder aufgezeichnete vertrauliche Daten mit langfristigem Schutzbedarf (SNDL) ist eine nachträgliche Sicherung nicht möglich, weshalb präventive Maßnahmen entscheidend sind. Daher ist die vollständige Migration zu Post-Quanten-Kryptografie so schnell wie möglich erforderlich. Deshalb hat das BSI für den Schutz von Verschlusssachen verbindliche Fristen für die Umstellung auf quantensichere Kryptografie festgelegt.

5.1.8 Operational Technology (OT)



Der Bereich Operational Technology (OT), zu dem industrielle Steuerungssysteme gehören, die beispielsweise in Produktionsanlagen verbaut sind, wird zunehmend relevanter für die Resilienz von Unternehmen und Gesellschaft (vgl. Vernetzte Geräte, vgl. Industrial-IoT-Geräte). Der Gesetzgeber hat die gesetzlichen Anforderungen an OT-Produkte sowie deren Entwicklung und Betrieb in den letzten Jahren deutlich erhöht. Während sich der Cyber Resilience Act an die Hersteller von OT und Industrial IoT richtet, stellt die NIS-2-Richtlinie Anforderungen an die Anwender und fordert einen sicheren Betrieb mit einem entsprechenden Informationssicherheitsmanagementsystem (ISMS).

→ Mehr über Operative Technik (OT)

Nicht nur die NIS2-Richtlinie, auch verschiedene andere europäische Gesetzgebungen fordern von Herstellern von Operational-Technology-Komponenten und von Maschinen- und Anlagenbauern

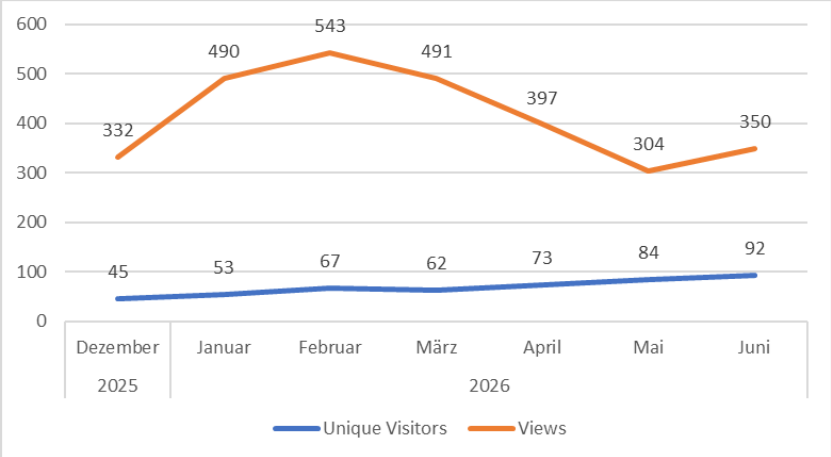
die sichere Entwicklung und Maßnahmen für den sicheren Betrieb von OT; etwa der Cyber Resilience Act (vgl. Cyber Resilience Act). Die neue EU-Maschinenverordnung beispielsweise, die 2027 in Kraft tritt, greift das Thema Cybersicherheit für Maschinen auf. Dabei wird der Fokus auf den Schutz der digitalen Komponenten gelegt, deren Manipulation zu einer Gefahr für Menschen werden kann. Neben diesen Entwicklungen auf europäischer Ebene wurde in Deutschland mit der TRBS 1115 Teil 1 (technische Regel für Betriebssicherheit in Deutschland, die die Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen (MSR) regelt) und dem erweiterten Anhang eine Konkretisierung für Cybersicherheitsmaßnahmen im Kontext des Arbeitsschutzes geschaffen. Das BSI beteiligt sich im Bereich OT in verschiedenen nationalen und internationalen Gremien, um beispielsweise notwendige Implementierungsmaßnahmen, Architektur- und Designentscheidungen oder den Umgang mit Sicherheitslücken in Standards festzuschreiben. Darüber hinaus hat sich die internationale, vertrauensvolle Zusammenarbeit mit Partnerbehörden und die Awareness für die Sicherheit von OT in den letzten Jahren erhöht, was sich auch in verschiedenen, gemeinsamen Veröffentlichungen widerspiegelt.

Um Sicherheitsvorfälle und mögliche Schäden zu vermeiden, ist eine schnelle Reaktion auf neue Schwachstellen und bekannte Vorfälle notwendig. Bei Schwachstelleninformationen und deren Behebungsmaßnahmen setzt das Common Security Advisory Framework (CSAF), ein standardisiertes und quelloffenes Framework zur Kommunikation und automatisierbaren Verteilung von maschinenverarbeitbaren Schwachstellen- und Mitigationsinformationen, an. CSAF ermöglicht es, Sicherheitsinformationen (Security Advisories) automatisiert abzurufen und zu verarbeiten. Mittlerweile stellen über 40 Hersteller von OT-Komponenten ihre Security Advisories neben dem Veröffentlichen auf der eigenen Webseite auch im CSAF-Format bereit. In Verbindung mit gepflegten, also aktuell gehaltenen Assetlisten, ermöglicht die Automatisierung Betreibern sowie Maschinen- und Anlagenbauern die Aufwände ihres Schwachstellenmanagements zu reduzieren. Die eingesparten Ressourcen können dadurch in das Beheben der Schwachstellen oder andere IT-Sicherheitsmaßnahmen fließen und helfen so, Gefährdungen zu minimieren.

5.1.9 Stand der Technik

Abbildung 5-12: Durchschnittliche tägliche Unique Visitors und Views der Stand-der-Technik-Bibliothek

Einheit: Anzahl



Quelle: BSI

Die Stand-der-Technik-Bibliothek wird in einem öffentlich zugänglichen Repository auf der Austauschplattform GitHub verwaltet, die monatlich regelmäßig mehrere Hundert Views erhält (vgl. Abbildung 5-12). Die bisherige Resonanz auf den Wechsel zu dieser Plattform wird positiv bewertet. Zum Berichtszeitpunkt verzeichnet das Repository 308 Stars und 33 Forks. Stars ermöglichen es GitHub-Nutzenden, ihr Interesse an einem Repository zu bekunden und dessen weitere Entwicklung zu verfolgen. Forks sind eigenständige Kopien des Repositorys, die

beispielsweise zur Anpassung oder Weiterentwicklung der Inhalte angelegt werden. Die Kennzahlen zeigen somit, dass die Stand-der-Technik-Bibliothek auf GitHub wahrgenommen, abgerufen und für eine mögliche weitere Nutzung übernommen wird. Da für den Zeitraum vor dem Plattformwechsel keine unmittelbar vergleichbaren Kennzahlen vorliegen, lässt sich daraus jedoch keine belastbare Aussage über eine Zunahme der Nutzung ableiten.

-> Mehr über Stand der Technik

Das BSI zentralisiert Anforderungen an den Stand der Technik und Maßnahmen nach Stand der Technik. Zentrales Verzeichnis für standardisierte, maschinenlesbare Cybersicherheitsanforderungen und die damit verbundenen, empfohlenen oder verbindlichen Sicherheitsmaßnahmen, ist die Stand-der-Technik-Bibliothek. Diese Bibliothek wird durch kontinuierliche Weiterentwicklung stetig verbessert und aktuell gehalten. Sie ist seit September 2025 über GitHub verfügbar.

Von den Inhalten der digitalen Bibliothek im Kontext "Stand der Technik" profitieren alle Stakeholder des BSI, die sich an den Vorgaben und Handreichungen des BSI orientieren. Da die Realisierung und Umsetzung der Cybersicherheit zunehmend digitaler und automatisierter erfolgt, profitieren diese Stakeholder von automatisierbaren Vorgaben, die direkt in den eingesetzten Systemen interpretiert und weiterverarbeitet werden können. Zudem wird es hierdurch möglich, Themenbereiche wie Schwachstellenmeldungen, Risikomanagement und Umsetzungen nach dem Stand der Technik digital miteinander zu verbinden und somit schneller reagieren zu können.

Ein konkretes Beispiel ist die Nutzung der Grundschutz++-JSON-Datei in einem Grundschutztool. Diese könnte dort digital eingelesen werden und mit der Anbindung eines Grundschutztools über eine geeignete Schnittstelle an ein entsprechendes Service Managementtool können manuelle Prozesse digitalisiert und somit zeitlich wesentlich effektiver und reibungsloser umgesetzt werden.

Da der Stand der Technik in einer digitalen Bibliothek zu Laufzeit gegen aktuelle Gefährdungen und Bedrohung geprüft wird, können Aktualisierungen bei einer oben beschrieben Prozessdigitalisierungen automatisch übernommen werden.

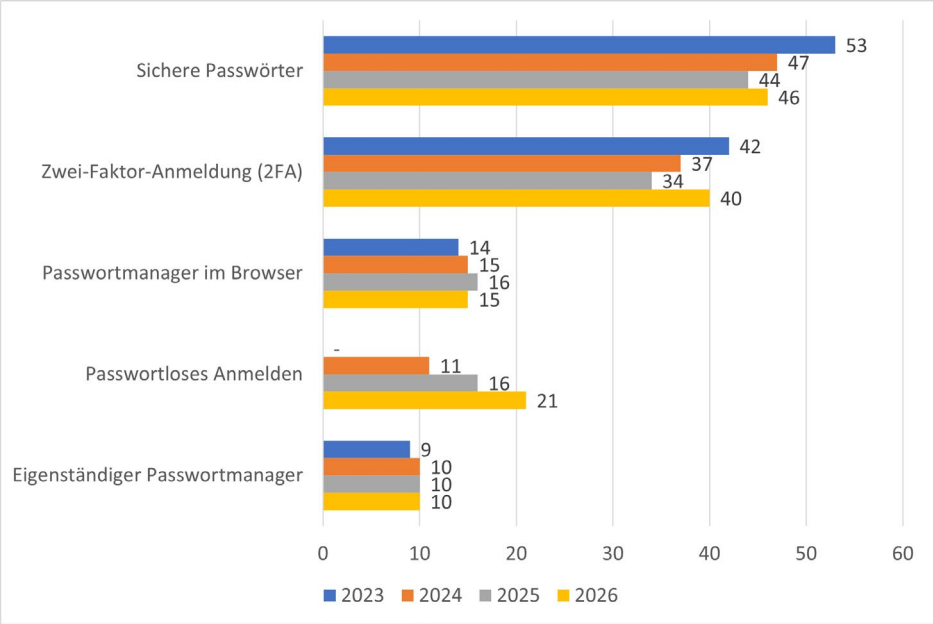
Die Stand-der-Technik-Bibliothek bietet alle Vorgaben, redundanzfrei und maschinenlesbar an einem Ort. Konsolidierte Vorgaben sorgen dafür, dass technische Standards überall einheitlich angewendet werden können. Aktualität und Gültigkeit werden durch einen entsprechenden Lebenszyklus sichergestellt und ein gelebtes digitales Sicherheitskonzept kann entstehen. Der digitale Lebenszyklus sorgt dafür, dass digitale Lösungen von Anfang bis Ende sinnvoll geplant, sicher betrieben und rechtzeitig verbessert oder ersetzt werden. Das BSI und die Cybersicherheitscommunity arbeiten transparent Hand in Hand. Die kooperative Zusammenarbeit sorgt dafür, dass Behörden und Partner-Organisationen in der Wirtschaft besser zusammenarbeiten, Wissen teilen und gemeinsam Lösungen finden.

5.2 Resiliente Gesellschaft

Unter Verbraucherinnen und Verbrauchern in Deutschland herrscht weiter verbreitet digitale Sorglosigkeit. Weniger als die Hälfte von ihnen setzte auch nur einfachste Maßnahmen wie sichere Passwörter ein.

Im Rahmen der jährlich von BSI und Polizeilicher Kriminalprävention (ProPK) durchgeführten Studie „Cybersicherheitsmonitor“ zeigte sich im aktuellen Berichtszeitraum wiederholt eine weit verbreitete digitale Sorglosigkeit unter den Verbraucherinnen und Verbrauchern in Deutschland. Rund 27 %von ihnen wähnten sich sicher, obwohl alljährlich etwa jeder Zehnte von Cyberkriminalität betroffen ist. Viele fühlen sich mit der sicheren Gestaltung ihres digitalen Alltags aber auch überfordert (23 %). Aufgrund digitaler Sorglosigkeit und Überforderung wurden selbst die bekanntesten und einfach zugänglichen Cybersicherheitsmaßnahmen von nicht einmal der Hälfte der Befragten genutzt (vgl. Abbildung 5-13).

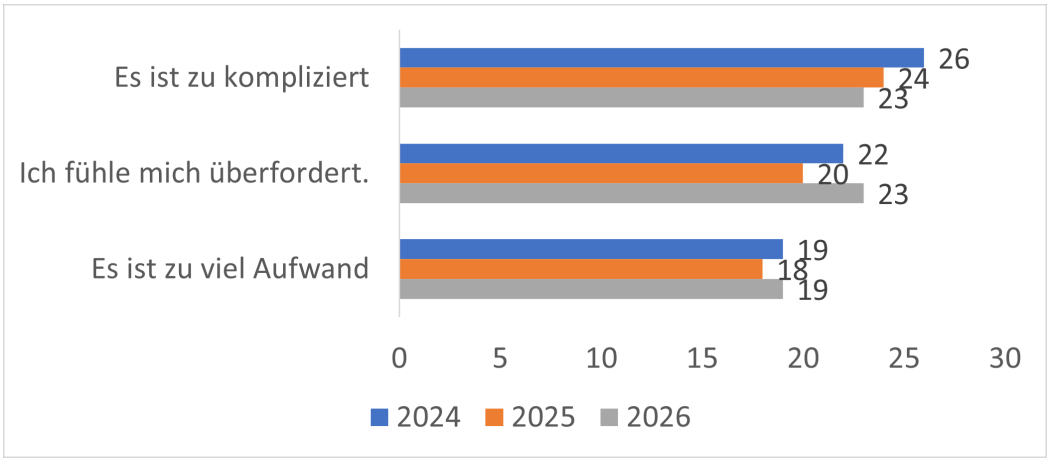
Abbildung 5-13: Von Verbraucherinnen und Verbrauchern genutzte Maßnahmen
Einheit: Anteile in Prozent



Quelle: Cybersicherheitsmonitor
Bemerkung: Mehrfachnennungen möglich, „Passwortloses Anmelden“ 2023 nicht abgefragt.

Durch ein stabiles Informations- und Tooling-Angebot des BSI (vgl. Service-Center) können Verbraucherinnen und Verbraucher ihre digitale Selbstverteidigung stärken. Sichere Login-Methoden tragen zur Resilienz bei: Weiterhin am häufigsten genutzt wurden sichere Passwörter (von 46 % der Befragten, vgl. Abbildung 5-13), dicht gefolgt von der Zwei-Faktor-Authentisierung (40 % der Befragten). Dabei ging der Trend zu sicheren Anmeldemethoden in die richtige Richtung: ein Wachstum von 6 Prozentpunkten bei der Zwei-Faktor-Authentisierung und von 5 Prozentpunkten bei passwortlosem Anmelden. Letzteres umfasst besonders nutzerfreundliche und als besonders sicher geltende Anmeldeverfahren wie etwa biometrische oder kryptografische Verfahren.

Abbildung 5-14: Verbraucherinnen und Verbraucher nach Gründen, Maßnahmen nicht zu nutzen
Einheit: Anteile in Prozent



Quelle: Cybersicherheitsmonitor
Bemerkung: Mehrfachnennungen möglich

Immer noch erscheint vielen Verbraucherinnen und Verbrauchern der Aufwand für Schutzmaßnahmen zu hoch (19 %, vgl. Abbildung 5-14), sie fühlen sich überfordert (23 %) oder

halten Cybersicherheit nach wie vor für zu kompliziert (23 %). Insbesondere der Anteil der Verbraucherinnen und Verbraucher, die sich überfordert fühlen, ist im aktuellen Berichtszeitraum gestiegen (plus 3 Prozentpunkte).

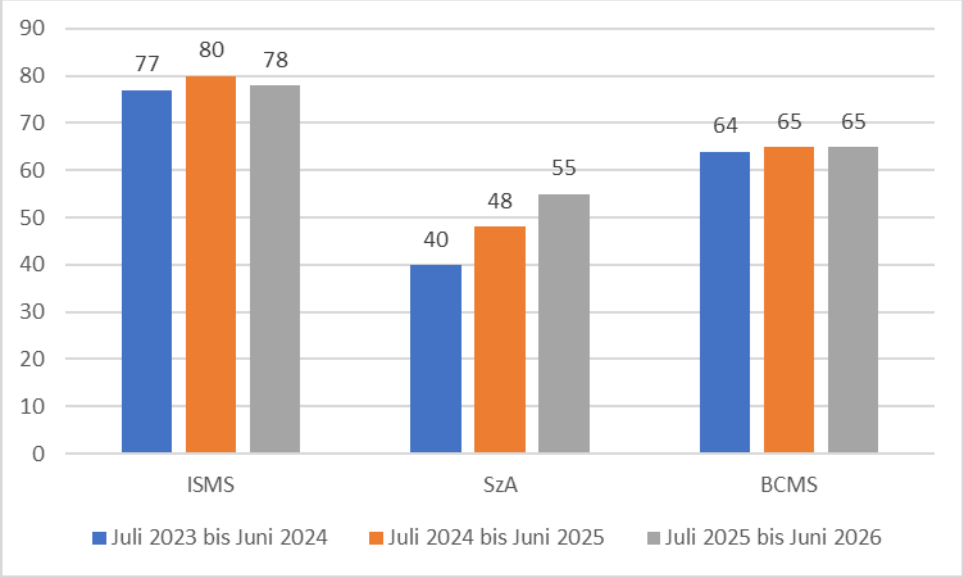
Auch der Trend zu einfachem passwortlosem Anmelden (plus 5 Prozentpunkte) zeigt, dass Hersteller die ihre digitalen Produkte so gestalten, dass Cybersicherheit für Anwenderinnen und Anwender möglichst leicht umzusetzen ist, viel zur resilienten Gesellschaft beitragen.

5.3 Resiliente Wirtschaft

Während sich die Resilienz Kritischer Infrastrukturen langsam weiter verbessert, besteht bei kleinen und mittleren Unternehmen (KMU) noch erheblicher Nachholbedarf. Dabei unterliegen viele einer gleich doppelten Fehleinschätzung: 1. Sie wähnen sich gut aufgestellt, während die Realität eine andere Sprache spricht. 2. Sie glauben verbreitet, kein lohnenswertes Ziel zu sein, während Angreifer hauptsächlich diejenigen angreifen, die am schwächsten geschützt sind.

5.3.1 Resilienz Kritischer Infrastrukturen

Abbildung 5-15: Betreiber Kritischer Infrastrukturen mit Reifegrad/Umsetzungsgrad 3 oder höher von Juli 2025 bis Juni 2026 nach Art des Systems
Einheit: Anteile in Prozent



Quelle: KRITIS-Nachweise

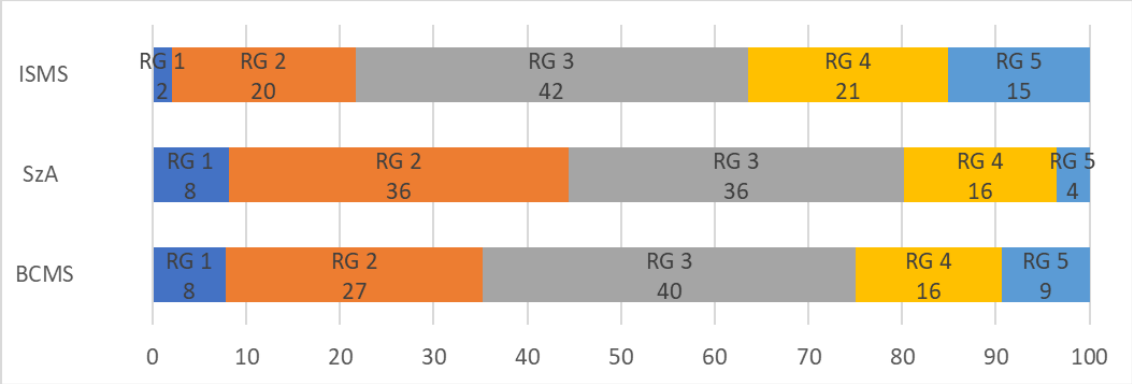
Die Resilienz Kritischer Infrastrukturen wächst weiter – langsam aber stetig – wobei Nachholeffekte bei Systemen zur Angriffserkennung (SzA) zu deutlichen Steigerungen führten. So erfüllten diese Systeme im aktuellen Berichtszeitraum zu 55 % den regulativ mindestens vorgeschriebenen Umsetzungsgrad 3. Das war ein Zuwachs von 7 Prozentpunkten. Der Anteil an Informationssicherheits- und Business-Continuity-Management-Systemen (ISMS- und BCMS-Systeme) mit Reifegrad 3 oder höher blieb dagegen weitgehend unverändert (vgl. Abbildung 5-15). Der im Durchschnitt betrachtet leichte Rückgang bei diesen Systemen war auf den neuen Sektor „Siedlungsabfallentsorgung“ zurückzuführen (auf Bundesebene existieren damit zehn KRITIS-Sektoren), der erst im Jahr 2025 in die Regulierung aufgenommen wurde und daher noch nicht ganz das Niveau der Systeme in den übrigen Sektoren erreicht hat.

→ Mehr über die Resilienz Kritischer Infrastrukturen

Kritische Anlagen haben einen besonderen Schutzbedarf. Diesem wird seit 2008 auch rechtlich Rechnung getragen: Kritische Infrastrukturen unterliegen besonderen Richtlinien und Regularien, die den Zweck haben, ihre Resilienz umfassend zu stärken. Seit 2015 bietet das IT-Sicherheitsgesetz (IT-SiG) einen einheitlichen Rechtsrahmen für die Zusammenarbeit von Staat und Unternehmen für mehr Cybersicherheit bei Kritischen Infrastrukturen. Es sieht vor, dass deren Betreiber sich unter anderem beim BSI registrieren und ihre IT-Sicherheit nach dem „Stand der Technik“ umsetzen. Dies umfasst beispielsweise die Etablierung, Überprüfung und Verbesserung von Systemen zur Stärkung der Resilienz, deren Reifegrade durch Nachweise belegt werden müssen. Reifegrad 3 von insgesamt fünf Reifegraden entspricht dabei den rechtlichen Mindestanforderungen.

Der Reifegrad der Informationssicherheitsmanagementsysteme (ISMS) gibt Aufschluss über die Fähigkeiten der Betreiber Kritischer Infrastrukturen zum Schutz ihrer Angriffsflächen vor Angriffen und anderen Vorfällen. Der Anteil an Betreibern, deren ISMS einen Reifegrad aufweisen, der mindestens den rechtlichen Mindestanforderungen entspricht, lag im aktuellen Berichtszeitraum bei 78 % und blieb damit gegenüber dem vergangenen Berichtszeitraum im Wesentlichen unverändert (vgl. Abbildung 5-15). Allerdings gab es unter den Sektoren zwei Veränderungen: Zum einen gingen aus dem vormaligen Sektor „Finanz- und Versicherungswesen“ die beiden Sektoren „Finanzwesen“ und „Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitsuchende“ hervor. Zum anderen haben die ersten Organisationen des seit 2025 neu regulierten Sektors „Siedlungsabfallentsorgung“ ihre Nachweise im aktuellen Berichtszeitraum eingereicht. Die Systeme in diesem Sektor haben erwartungsgemäß noch nicht die Reife der Systeme in bereits langfristig regulierten Sektoren. Angesichts der Tatsache, dass die Nachweise erstmalig eingereicht werden, hat der Sektor jedoch bereits einen relativ hohen Reifegrad erreicht. Das BSI führt dies auf den aktiven und konstruktiven Austausch des Sektors mit dem BSI zurück.

Abbildung 5-16: Betreiber Kritischer Infrastrukturen nach Reifegrad/Umsetzungsgrad ihrer Systeme
Einheit: Anteile in Prozent



Quelle: KRITIS-Nachweise

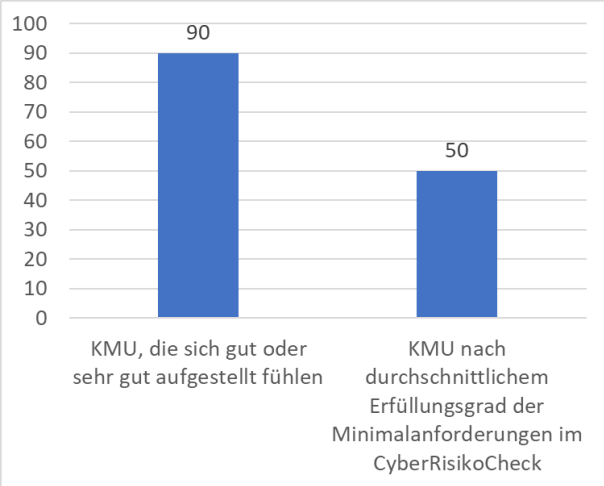
Im Bereich der Reifegrade für das Business Continuity Management System (BCMS) und der Umsetzungsgrade für die Systeme zur Angriffserkennung (SzA) war die Lage im aktuellen Berichtszeitraum deutlich schlechter als in Bezug auf Informationssicherheitsmanagementsysteme. Hier haben große Teile der Organisationen, die Kritische Infrastrukturen betreiben, noch wesentlichen Nachholbedarf, um einen angemessenen Schutz der von ihnen betriebenen Infrastrukturen zu erreichen. Der Anteil der Betreiber, deren BCMS einen Reifegrad von 3 oder höher aufwiesen, lag bei 65 % (vgl. Abbildung 5-16). Bei den SzA lag der Anteil der Betreiber mit Umsetzungsgrad 3 oder höher bei 55 % und mit einem Plus von 7 Prozentpunkten somit deutlich über dem Wert des vergangenen Berichtszeitraums.

Nicht zuletzt mit Blick auf die durch den zunehmenden Einsatz künstlicher Intelligenz überaus dynamische Bedrohungslage, sind verstärkte Anstrengungen im Bereich der Kritischen Infrastrukturen notwendig, damit alle Betreiber und alle Systeme das Mindestmaß an IT-Sicherheit erreichen. Es müssen insbesondere mehr Systeme zur Angriffserkennung in den Unternehmen zum Einsatz kommen, um initial erfolgreiche Angriffe schnell entdecken und eindämmen zu können.

Mit dem KRITIS-Dachgesetz wurde die Regulierung auf den physischen Bereich ausgedehnt – eine dringende Notwendigkeit, wie sich gerade auch im aktuellen Berichtszeitraum in vermehrten physischen Angriffen zeigte (vgl. Gefährdungslage Kritischer Infrastrukturen). Kritische Infrastrukturen werden ebenfalls in der NIS-2-Richtlinie als „besonders wichtige Einrichtungen“ reguliert.

5.3.2 Resilienz kleiner und mittlerer Unternehmen

Abbildung 5-17: KMU nach Selbsteinschätzung sowie nach CyberRisikoCheck
Einheit: Anteile in Prozent



Quelle: BSI, TÜV-Verband

Die Gefährdungslage von kleinen und mittleren Unternehmen (KMU) in Deutschland bleibt vor allem wegen mangelnder Resilienz weiterhin angespannt. Die Cybernation Deutschland bietet damit eine erhebliche, teils schlecht geschützte Angriffsfläche, denn KMU machen gut 99 % der Unternehmen in Deutschland aus.

Während sich die überwiegende Mehrheit von diesen beim Thema Cybersicherheit gut aufgestellt wähnt, erfüllen nur durchschnittlich 55 % der KMU im CyberRisikoCheck des BSI die minimalen Cybersicherheitsanforderungen (vgl. Abbildung 5-17). Dabei dürften diejenigen, die sich einem CyberRisikoCheck unterziehen, bereits ein erhöhtes Problembewusstsein haben.

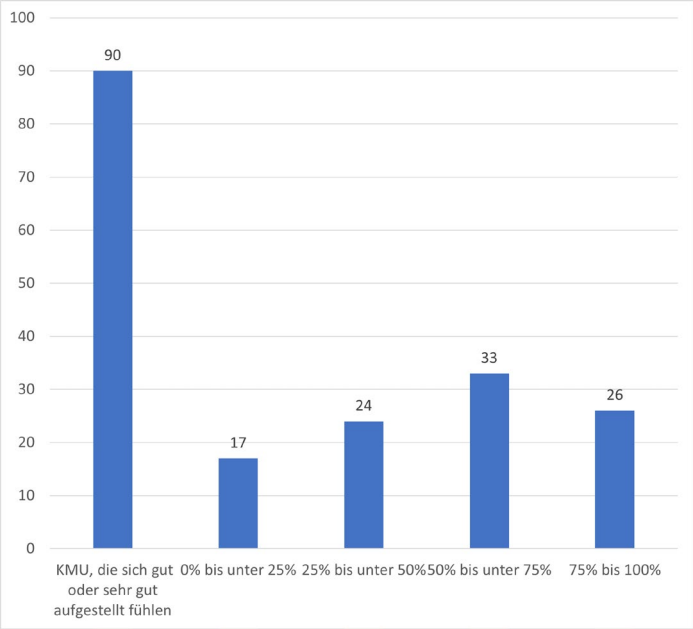
→ Mehr über die Resilienz kleiner und mittlerer Unternehmen

Ein entscheidender Faktor für die niedrige Cyberresilienz der deutschen Wirtschaft scheint – neben finanziellen Aspekten – darin begründet, dass die Geschäftsleitungen deutscher Unternehmen die Cybersicherheit ihrer Organisation systematisch überschätzen – und zwar erheblich. So schätzten 90 % der kleinen, mittleren und großen Unternehmen in Deutschland ihre Cybersicherheit als „eher gut“ oder sogar „sehr gut“ ein (vgl. TÜV-Verband).

Doch die Realität sieht anders aus:

Spätestens seitdem Mitte Oktober 2025 der Hersteller-Support von Microsoft Exchange 2019 endete, verbot sich aus Sicherheitsgründen der Einsatz dieser Version. Ende Oktober 2025 stellte das BSI jedoch fest, dass noch 92 % der bekannten 33.000 on-premise Exchange-Server mit offen aus dem Internet erreichbarem Outlook Web Access auf veralteten Versionen liefen, knapp 50 % sogar mit Version 2016 oder älter.

Abbildung 5-18: KMU im CyberRisikoCheck von Juli 2025 bis Juni 2026 nach Erfüllungsgrad
Einheit: Anteile in Prozent an allen teilnehmenden KMU



Quelle: BSI

Beim CyberRisikoCheck, den vom BSI geschulte IT-Dienstleister als IT-Sicherheitsberatung für kleine und Kleinstunternehmen anbieten, zeigen die Unternehmen darüber hinaus im Durchschnitt einen Erfüllungsgrad von nur knapp 55 % der insgesamt 27 überprüften Anforderungen (vgl. Abbildung 5-17). 41 % von ihnen erfüllten weniger als die Hälfte der Anforderungen (vgl. Abbildung 5-18). Dabei stellen diese lediglich die Minimalanforderungen an Präventiv- und Reaktivmaßnahmen dar, die umgesetzt sein müssen, um wenigstens die exponiertesten Angriffsflächen zu schützen und IT-Systeme im Ernstfall retten zu können.

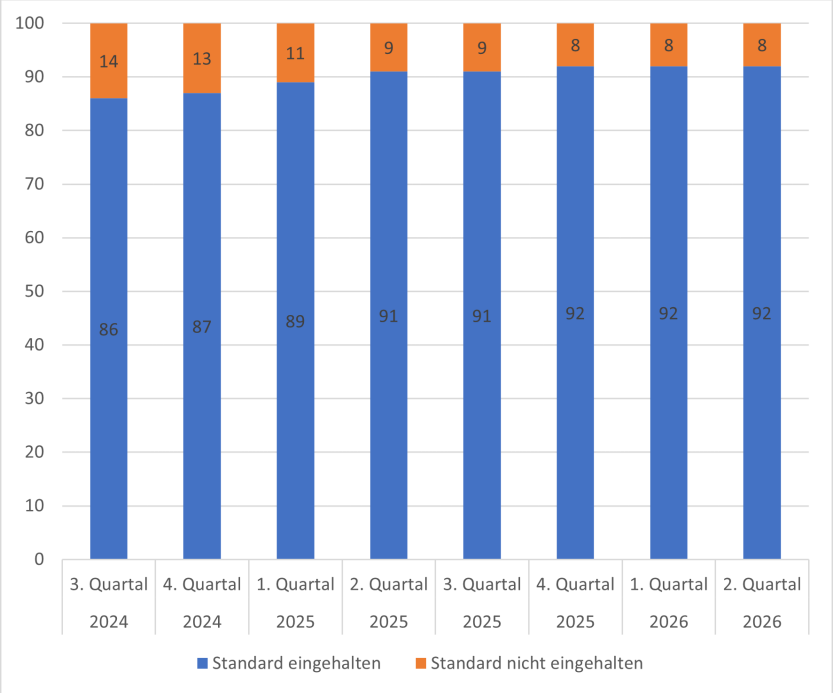
Die Umsetzung der NIS-2-Richtlinie in deutsches Recht kam damit zur richtigen Zeit. Viele der großen und mittleren Unternehmen fallen unmittelbar darunter. Ein nicht unerheblicher Teil der übrigen KMU wird aufgrund der Lieferkettensicherheit, die ihre Kunden erfüllen müssen, künftig dazu verpflichtet werden, deutlich mehr für ihre Cybersicherheit zu tun. Dabei werden kleine Unternehmen, die ganz am Anfang einer Lieferkette stehen, in der Regel weniger Maßnahmen umzusetzen haben als ein direkt nach NIS-2 reguliertes Unternehmen. Unternehmen, die sich zur Bestimmung ihres Cybersicherheitsniveaus bislang auf ihre Intuition verlassen haben, wird dringend angeraten, wenigstens einen CyberRisikoCheck durchzuführen. Bei Bedarf lässt sich auf den Check nahtlos (beispielsweise mit dem Grundschutz++) aufbauen.

5.4 Resiliente Bundesverwaltung

Im aktuellen Berichtszeitraum wurde das Monitoring der Web-Angriffsflächen der Bundesverwaltung aufgrund erweiterter rechtlicher Befugnisse des BSI erheblich ausgebaut. Im Folgenden wird über erste Ergebnisse berichtet.

5.4.1 Prävention in der Bundesverwaltung

Abbildung 5-19: IP-Adressen der Bundesverwaltung nach Verschlüsselungsstandard ab TLS 1.2
Einheit: Anteile in Prozent



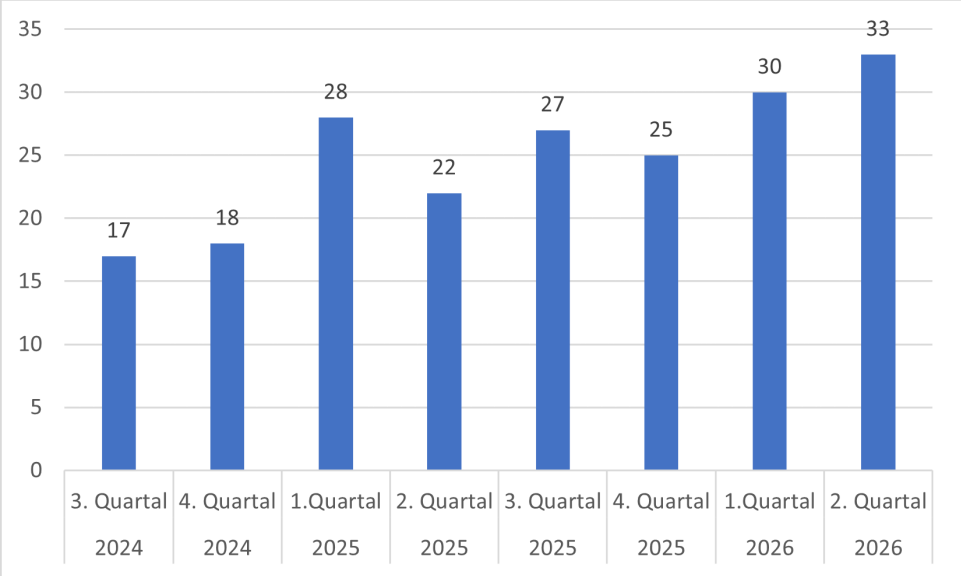
Quelle: BSI

Verschlüsselungsprotokolle dienen der sicheren Übertragung von Daten im Internet. Um Manipulations- und Missbrauchsmöglichkeiten für Angreifer zu minimieren, hat das BSI für den Bund die Verwendung des Verschlüsselungsprotokolls TLS in der Version 1.2 oder höher als Standard festgelegt. Im aktuellen Berichtszeitraum ist der Anteil der IP-Adressen der Bundesverwaltung, die den vorgegebenen Standard erfüllen, weiter gestiegen - von 91 % am Ende des vergangenen Berichtszeitraums auf 92 % zum Ende des aktuellen Berichtszeitraums. Der veraltete Verschlüsselungsstandard SSL ist nicht mehr sicher.

-> Mehr über Prävention in der Bundesverwaltung

Auf der Grundlage des §15 BSIG scannt das BSI die Web-Angriffsflächen der Bundesverwaltung auf akute Verwundbarkeiten. Nach Erfassung eines Schwachstellenverdachts (vgl. Web-Angriffsflächen der Bundesverwaltung) und der Veröffentlichung der ersten Einschätzungen ihres Schweregrads gilt es, die betroffenen Systeme schnellstmöglich zu schützen. Das BSI erfasst in einer täglichen Lageeinschätzung, von welchen Schwachstellen aktuell hohe Gefahren ausgehen. Nach Überprüfung auf das tatsächliche Vorhandensein der Schwachstelle werden betroffene Behörden zeitnah informiert und so aktiv bei der Abwehr akuter Bedrohungen unterstützt (vgl. Angreiferaktivitäten, vgl. Exploitation-Angriffe).

Abbildung 5-20: Spezialisierte Meldungen des BSI über akute Verwundbarkeiten an die betroffenen Behörden
Einheit: Anzahl



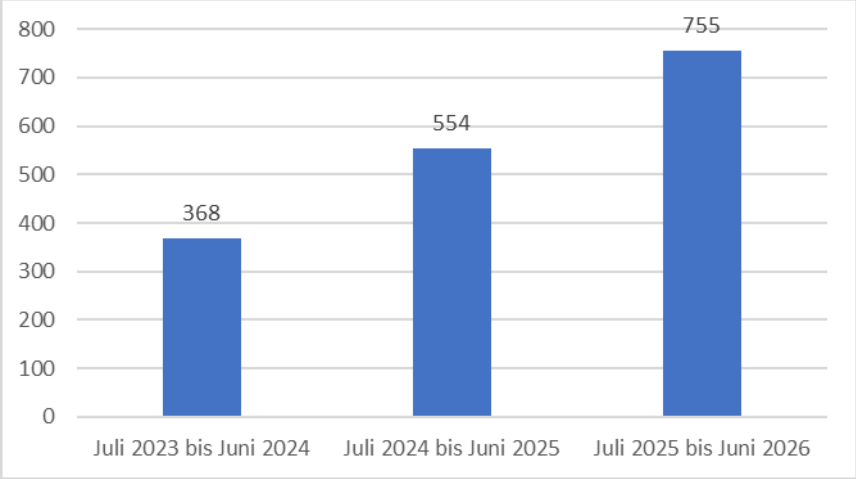
Quelle: BSI

Das BSI hat im aktuellen Berichtszeitraum insgesamt 115 speziell an betroffene Einrichtungen der Bundesverwaltung gerichtete Warnungen über Schwachstellen mit dem Schweregrad hoch oder kritisch versandt (vgl. Abbildung 5-20). Das waren 35 % mehr als im vergangenen Berichtszeitraum. Dabei handelte es sich bei Schwachstellen in spezialisierten Systemen in der Regel um einige wenige, bei Schwachstellen in flächendeckend eingesetzten Systemen wie zum Beispiel Servern, um mehrere betroffene Behörden.

Das BSI baut auch im Bereich der operativen Cybersicherheit sein Informationsangebot für Behörden kontinuierlich aus und bietet für Behörden auch sogenannte Attack Surface Checks an: hierbei wird auf Anfrage die Angriffsfläche einer gesamten Behörde hinsichtlich des Risikos akuter Verwundbarkeit überprüft.

5.4.2 Verteidigung der Netze des Bundes

Abbildung 5-21: Durchschnittliche tägliche neue Sperrungen maliziöser Webseiten
Einheit: Anzahl

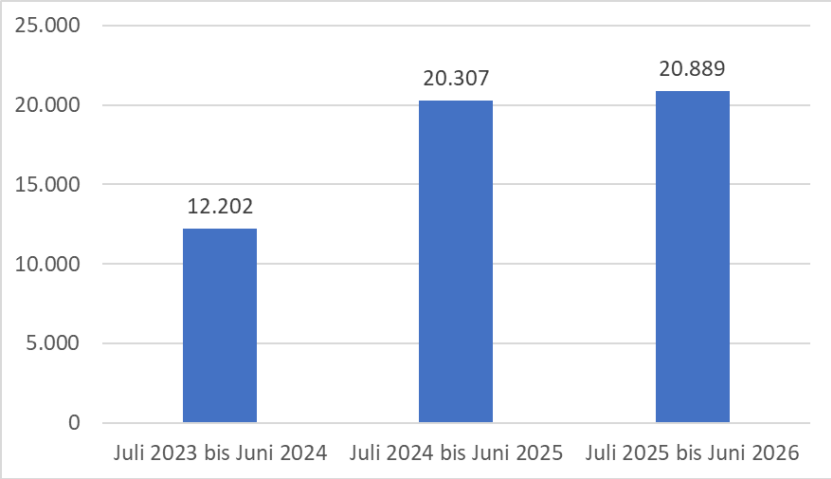


Quelle: BSI

Zur Abwehr von Gefahren für die Regierungsnetze (vgl. Angriffe mittels digitaler Kommunikationswege auf die Bundesverwaltung) setzt das BSI eine Reihe komplementärer Maßnahmen ein. Eine Komponente stellen Webfilter dar, die den Zugriff aus der Bundesverwaltung heraus auf maliziöse Websites und Webserver blockieren. Im aktuellen Berichtszeitraum wurden täglich durchschnittlich 755 maliziöse Websites neu gesperrt. Dabei lässt sich erneut eine Zunahme der eingestellten IOCs (Indicators of Compromise), mit denen die maliziösen Webseiten identifiziert werden, feststellen. Diese Entwicklung resultiert sowohl aus dem kontinuierlichen Anstieg aktiver Cyberbedrohungen als auch aus der wachsenden Anzahl an Quellen, über die IOCs zugeliefert werden. Auch die Kommunikation bereits aktiver Schadsoftware mit Webservern, die unter Kontrolle der Angreifer stehen, wird durch diese Schutzmaßnahme unterbunden. Die Schadsoftware kann danach keine neuen Komponenten und Befehle der Angreifer mehr erhalten. Zudem ist es der Schadsoftware auch nicht mehr möglich, Daten des Geschädigten an diese Webserver zu senden.

-> Mehr über die Verteidigung der Netze des Bundes

Abbildung 5-22: Durchschnittlich täglich erstellte Malware-Detektoren
Einheit: Anzahl



Quelle: BSI

Insbesondere gezielte Angriffe per E-Mail auf die Bundesverwaltung können durch die zentral vom BSI eingesetzten Antivirus-Schutzmaßnahmen nicht mit ausreichender Sicherheit vollständig erkannt und unterbunden werden. Daher betreibt das BSI verschiedene eigene Systeme zur Detektion von Schadprogrammen im E-Mailverkehr der Regierungsnetze. Mit einer Kombination aus automatisierten Testverfahren und manueller Analyse wird der Schutz für die Bundesverwaltung vor hochqualifizierten Angreifern erheblich verbessert. So werden etwa automatisiert und manuell knapp 21.000 Hash-Signaturen täglich generiert (vgl. Abbildung 5-22), mit denen Nachrichten auf Echtheit und Integrität geprüft werden und Schadprogramme in E-Mails an die Bundesverwaltung vor deren Zustellung an die Empfänger-Adresse detektiert werden. Weiterhin werden im Rahmen des Sofortprogramms CyberGovSecure den Behörden der Bundesverwaltung mehrere Maßnahmen angeboten, um ihre Cybersicherheit und -resilienz zu stärken (vgl. Beratung für Bund, Länder, Kommunen, Justiz und Politik).

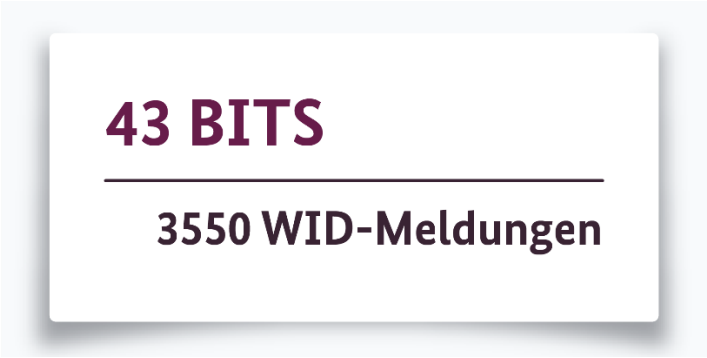
5.5 Das BSI für die Cybernation Deutschland

Um die Resilienz in Staat, Wirtschaft und Gesellschaft weiter aufzubauen, leistet das BSI dauerhaft wirksame Unterstützung – vom Erheben und Teilen von Lageinformationen über systematische und gezielte Beratung von Organisationen beim Aufbau ihrer Cybersicherheitssysteme bis hin zur Unterstützung bei der Vorfallbewältigung. Darüber hinaus leistet das BSI aktive Gefahrenabwehr für die Bundesverwaltung (vgl. Resiliente Bundesverwaltung).

5.5.1 Das BSI für Wirtschaft, Verwaltung und andere Organisationen

5.5.1.1 Warn- und Informationsdienst

Abbildung 5-23: BITS-Mitteilungen und WID-Meldungen von Juli 2025 bis Juni 2026
Einheit: Anzahl



Quelle: BSI

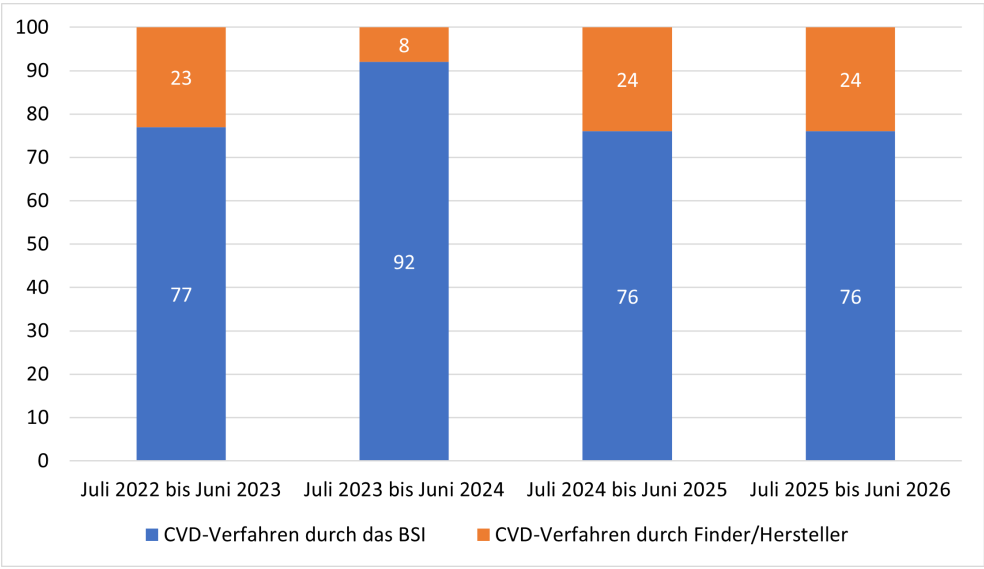
Das BSI bewertet fortlaufend Schwachstellen und weist Betreiber über Sicherheitsmitteilungen, Meldungen im Portal des Warn- und Informationsdienstes sowie über CERTBund Reports regelmäßig auf die Gefahr durch schwerwiegende Schwachstellen sowie fehlkonfigurierte Systeme hin. Trotz aller Bemühungen bleiben Angriffsflächen jedoch bei vielen Organisationen offen und verwundbar.

Im Berichtszeitraum veröffentlichte das BSI 43 BSI-IT-Sicherheitsmitteilungen (BITS) zu (Zero-Day) Schwachstellen in IT-Sicherheitsprodukten und weiteren, oftmals exponierten IT-Produkten (davon 16 Aktualisierungen). Des Weiteren wurden 3.550 neue WID-Meldungen veröffentlicht, um Betreiber beim Patchmanagement zu unterstützen.

→ Zum Warn- und Informationsdienst

5.5.1.2 Coordinated Vulnerability Disclosure

Abbildung 5-24: CVD-Meldungen von IT-Sicherheitsforschenden an das BSI
Einheit: Anteile in Prozent



Quelle: BSI

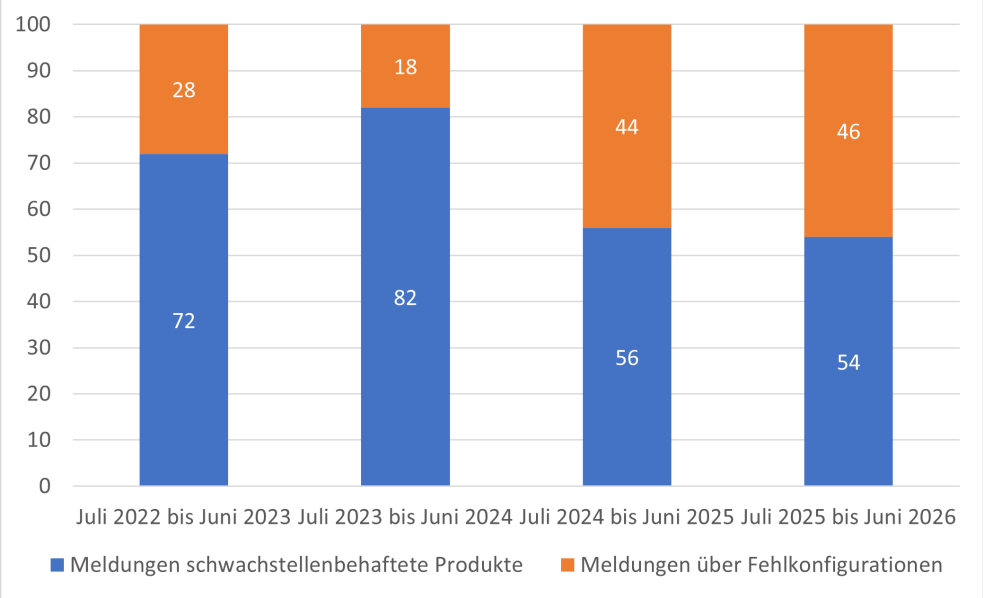
Das Coordinated-Vulnerability-Disclosure-Verfahren (CVD-Verfahren) des BSI ist ein strukturierter Prozess zur sicheren Offenlegung von IT-Schwachstellen. Es ermöglicht Sicherheitsforschenden, entdeckte Schwachstellen vertraulich an das BSI zu melden, welches die Behebung durch den Hersteller koordiniert und eine abgestimmte Veröffentlichung vornimmt.

Die Zahl gemeldeter Schwachstellen steigt kontinuierlich, gleichzeitig wachsen die Anforderungen an deren koordinierte Bearbeitung. Im aktuellen Berichtszeitraum gingen 237 Meldungen von Sicherheitsforschenden im BSI ein, darunter 129 Schwachstellenmeldungen. Für 76 % dieser Meldungen führte das BSI ein CVD-Verfahren durch (vgl. Abbildung 5-24). Die hohe Nachfrage nach Übernahme und Vermittlung der Meldungen verdeutlicht den zunehmenden Bedarf an einer staatlich moderierten Schwachstellenkoordination.

→ Mehr über den CVD-Prozess

Im aktuellen Berichtszeitraum gingen im Rahmen des Coordinated-Vulnerability-Disclosure-Verfahrens (CVD-Verfahren) insgesamt 237 Meldungen von IT-Sicherheitsforschenden an das BSI ein. In 54 % der Fälle handelte es sich um Schwachstellen in Softwareprodukten, 46 % der Meldungen betrafen Fehlkonfigurationen (vgl. Abbildung 5-25). Meldungen über Fehlkonfigurationen steigen sowohl in absoluten Zahlen als auch relativ betrachtet seit Jahren. Dies verdeutlicht eine weitere Herausforderung, vor der Deutschland beim Schutz externer Angriffsflächen steht: Denn Angreifern ist es einerlei, ob eine Infiltration durch eine technische Schwachstelle oder eine Fehlkonfiguration von Systemen ermöglicht wird.

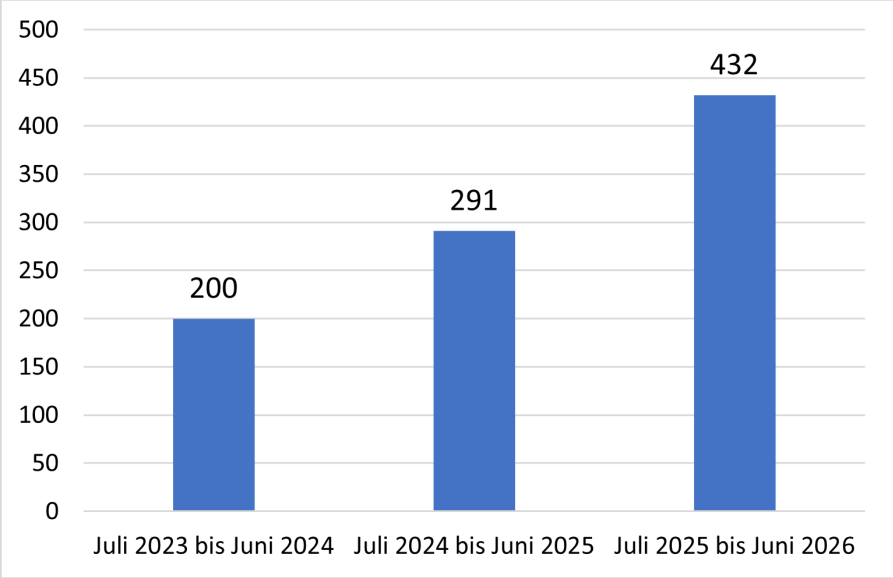
Abbildung 5-25: Meldungen von IT-Sicherheitsforschenden an das BSI nach Art der Meldung
Einheit: Anteile in Prozent



Quelle: BSI

5.5.1.3 Beratung für Bund, Länder, Kommunen, Justiz und Politik

Abbildung 5-26: Beratungsanfragen aus Ländern und Kommunen
Einheit: Anzahl



Quelle: BSI

Die Umsetzungsberatung des BSI ist ein Angebot an die Zielgruppen Bundesverwaltung, Justiz und Politik sowie Länder und Kommunen zur adressatengerechten Stärkung ihrer Cyberresilienz. Die grundsätzliche Bereitschaft zur Nutzung der Angebote der Umsetzungsberatung des BSI ist vorhanden und nimmt zu. So gingen im aktuellen Berichtszeitraum beispielsweise 432 Beratungsanfragen aus Ländern und Kommunen ein (vgl. Abbildung 5-26). Das waren 48 % mehr als im vergangenen Berichtszeitraum.

→ Mehr zur Beratung für Bund, Länder, Kommunen, Justiz und Politik

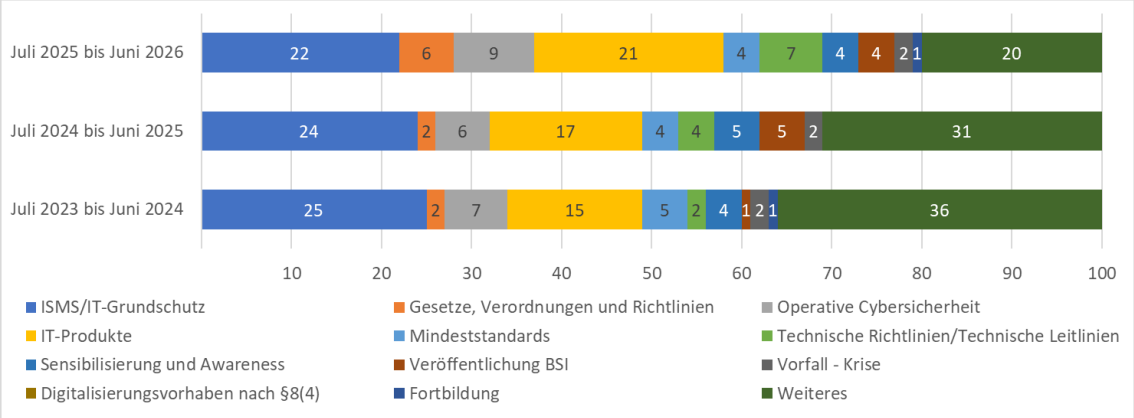
Mit der fortschreitenden Digitalisierung und zunehmenden Cyberbedrohungen steigt auch der Bedarf an resilienten digitalen Prozessen und Strukturen. Die Umsetzungsberatung des BSI ist ein Angebot an die Zielgruppen Bundesverwaltung, Justiz und Politik sowie Länder und Kommunen zur adressatengerechten Stärkung ihrer Cyberresilienz.

Bundesverwaltung

Anhand der durch das BSI durchgeführten Sicherheitsberatungen lassen sich für die Bundesverwaltung wichtige Themenfelder identifizieren, zu denen Maßnahmen für die Prävention ergriffen wurden.

Leicht rückläufig war mit 22 % im aktuellen Berichtszeitraum der Anteil an Beratungen zu den BSI-Standards, IT-Grundschutz inklusive Mindeststandards (minus zwei Prozentpunkte gegenüber dem vergangenen Berichtszeitraum, vgl. Abbildung 5-27). Deutlich zugenommen auf 21 % hat der Anteil an Beratungen zu konkreten IT-Produkten (plus vier Prozentpunkte). Zugelegt hat auch der Anteil der Beratungen zur operativen Cybersicherheit auf 9 % (plus drei Prozentpunkte), wobei rund 60 % dieses Bereichs auf Cloud-Themen entfielen. Beraten wurde darüber hinaus zu Themen wie Risiko-, Notfall- und Business Continuity Management. Zusätzlich wurde die Umsetzungsberatung bei Prüfungen des BSI initiiert (vgl. Auditierung und Umsetzungsberatung bei Sicherheitsmängeln). Insgesamt lässt sich eine Verschiebung der Themen unter anderem zu Gesetzen, Verordnungen und Richtlinien konstatieren. Hintergrund ist eine Priorisierung entlang aktueller Lageentwicklungen.

Abbildung 5-27: Beratungen der Bundesverwaltung von Juli 2025 bis Juni 2026 nach Beratungsthema
Einheit: Anteile in Prozent



Quelle: BSI

Um eine wirkungsvolle und zügig umsetzbare Steigerung der Cyberresilienz im Bereich des Bundes zu gewährleisten, wurde das Programm CyberGovSecure initiiert. Ziel des Programms ist es, die Informationssicherheit der Bundesbehörden schnell, wirksam und messbar zu verbessern und die Handlungsfähigkeit des Staates in einem zunehmend komplexen Bedrohungsumfeld nachhaltig zu sichern. Das Programm liefert umsetzungsorientierte Maßnahmen, eine zentrale Unterstützung bei der Durchführung und eine begrenzte finanzielle Förderung der Behörde.

Landesverwaltung und Kommunen

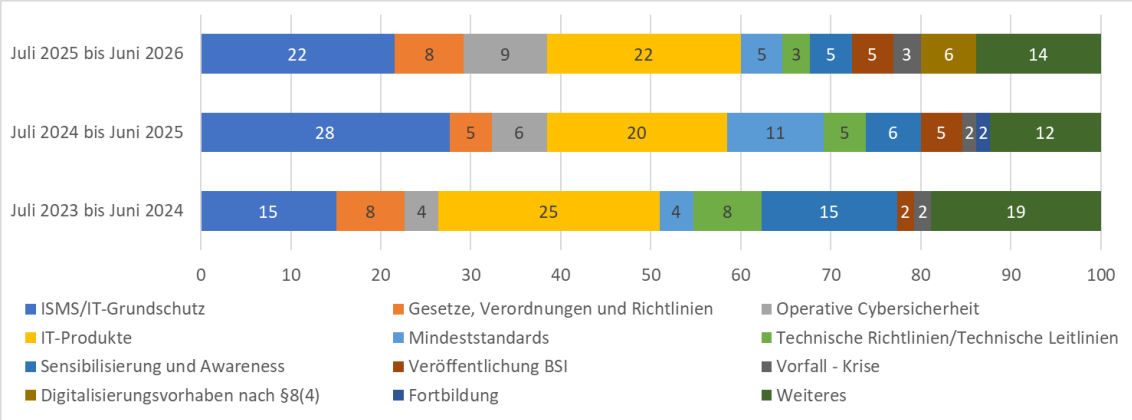
Im Bereich der Länder wurde die Informationssicherheit als Schwerpunktthema im IT-Planungsrat verankert – die zugehörige Themenpatenschaft hat das BSI übernommen. Basierend auf den Erfahrungen, die etwa bei der Durchführung gemeinsamer Übungen zwischen Bund und Ländern im Berichtszeitraum festgestellt wurden, konnten konkrete Projekte im Schwerpunktthema Informationssicherheit initiiert werden, um die Ebenen übergreifende Resilienz zu stärken. Mit diesen Projekten soll unter anderem die Zusammenarbeit zwischen BSI und Ländern im Bereich der Übungen ausgebaut, und der Bereich der Krisen- und Notfallkommunikation verbessert werden.

Bei Ländern und Kommunen nimmt der Beratungsbedarf weiter zu. Dies dürfte auf die fortschreitende Digitalisierung und ein damit verbundenes, wachsendes Problembewusstsein zurückzuführen sein. Ziel ist es deshalb, die Beratungsangebote weiter adressatengerecht und anwenderfreundliche auszubauen.

Justiz und Politik

Wie in der Bundesverwaltung waren auch in der Zielgruppe Justiz Beratungen zu Informationssicherheitsmanagementsystemen sowie zum IT-Grundschutz mit einem Anteil von 22 % im aktuellen Berichtszeitraum rückläufig (minus 6 Prozentpunkte, vgl. Abbildung 5-28), während der Anteil an Beratungen zu IT-Produkten mit 22 % leicht anstieg (plus 2 Prozentpunkte).

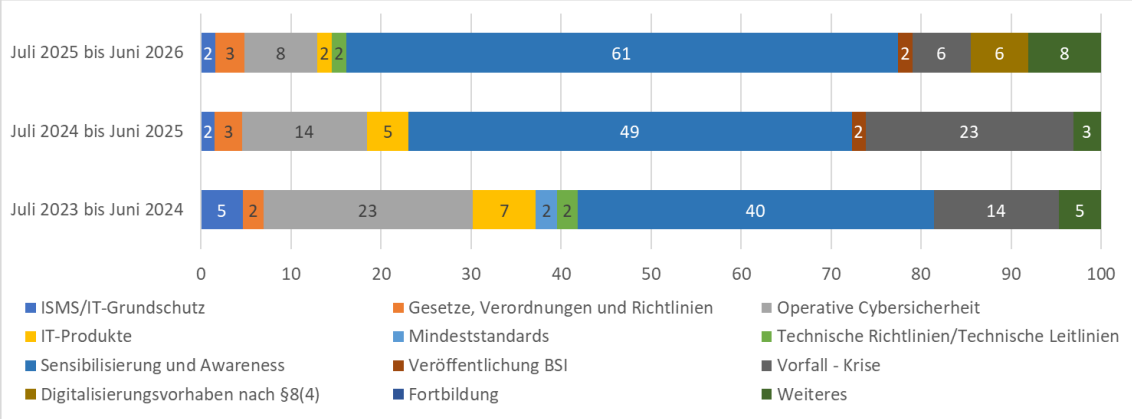
Abbildung 5-28: Beratungen der Justiz im Bund von Juli 2025 bis Juni 2026 nach Beratungsthema
Einheit: Anteile in Prozent



Quelle: BSI

In der Zielgruppe Politik wiesen im aktuellen Berichtszeitraum Beratungen zu Fortbildungen mit 61 % den weitaus größten Anteil auf. Das entsprach einem Zuwachs um 12 Prozentpunkte. Deutlich zurückgegangen ist hingegen der Anteil der Beratungen zur operativen Cybersicherheit auf 8 % (minus sechs Prozentpunkte, vgl. Abbildung 5-29) sowie der Anteil der Beratungen bei Cybersicherheitsvorfällen oder IT-Krisen (6 %, minus 17 Prozentpunkte).

Abbildung 5-29: Beratungen der Politik im Bund von Juli 2025 bis Juni 2026 nach Beratungsthema
Einheit: Anteile in Prozent

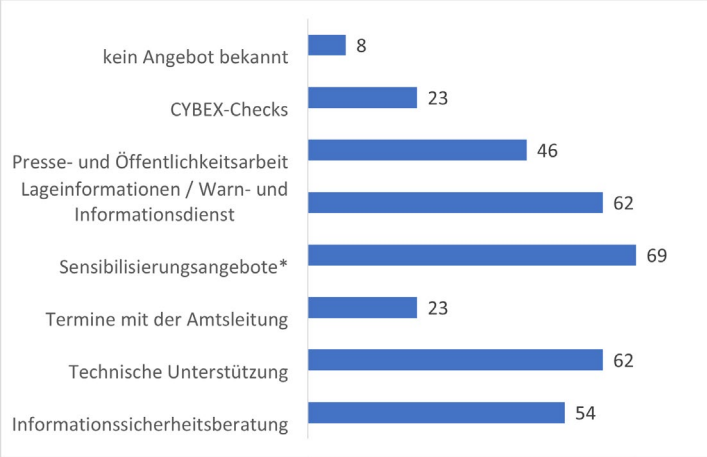


Quelle: BSI

Fazit

Durch Umfragen konnte festgestellt werden, dass die präventiven Angebote des BSI grundsätzlich bekannt sind, der Grad der Bekanntheit jedoch nach Zielgruppe und Angebot variiert. Insbesondere Sensibilisierungsmaßnahmen, Lageinformationen sowie Warn- und Informationsdienste sind einem Großteil der Befragten bekannt. Auch in der Zielgruppe Bundesverwaltung sind die Angebote grundsätzlich bekannt (vgl. Abbildung 5-30).

Abbildung 5-30: Bundesbehörden nach Bekanntheit der Beratungsangebote des BSI und Beratungsthema
Einheit: Anteile in Prozent



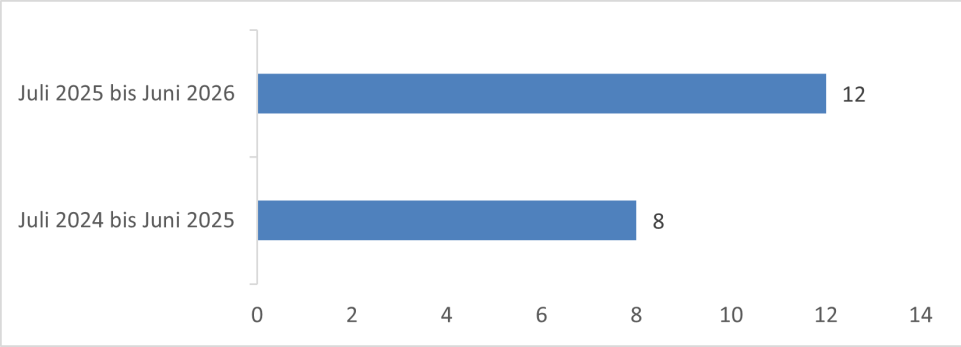
Quelle: BSI

Gleichzeitig wurde ein deutliches Ausbaupotenzial identifiziert. So wurde im Berichtszeitraum in der Zielgruppe Justiz eine Steigerung von knapp 23 % bei Beratungsanfragen festgestellt.

Insgesamt zeigt sich über alle Zielgruppen der Umsetzungsberatung des BSI hinweg, dass eine Schärfung des Problembewusstseins stattgefunden hat. Ursächlich dürfte dies auf die angespannte Cyberbedrohungslage sowie die neuen gesetzlichen Anforderungen zurückzuführen sein. Infolgedessen hat sich auch die Bekanntheit der Angebote der Informationssicherheitsberatung des BSI verbessert.

5.5.1.4 Auditierung und Umsetzungsberatung bei Sicherheitsmängeln

Abbildung 5-31: Auditierte Einrichtungen des Bundes
Einheit: Anzahl



Quelle: BSI
Bemerkung: Auditierte Einrichtungen des Bundes zum Stichtag 30.06.2026

Um das Schutzniveau der Bundesverwaltung weiter zu erhöhen, führt das BSI vorrangig bei den gefährdetsten bzw. priorisierten Behörden eine Standardrevision des Informationsmanagementsystems nach §7 BSIG durch. Damit werden Angemessenheit und Wirksamkeit der Sicherheitsmaßnahmen überprüft sowie potenzielle Schwachstellen identifiziert. Zur Behebung der Mängel bietet das BSI eine gezielte Umsetzungsberatung an. Eine regelmäßige flankierende Basisdatenerhebung erhebt darüber hinaus einen kennzahlenbasierten Datenbestand der Informationssicherheit der gesamten Bundesverwaltung, welcher für Steuerungszwecke und Priorisierung eingesetzt wird.

Zum Stichtag 30.Juni 2026 waren elf Bundesbehörden auditiert.

→ Mehr über Auditierung und Umsetzungsberatung bei Sicherheitsmängeln

Gemäß §7 BSIG unterzieht das BSI die Informationssicherheitsmanagementsysteme (ISMS) besonders priorisierter Bundesbehörden einer Prüfung. Der Prozess dieser Standardrevision (vgl. Abbildung 5-32) beinhaltet zunächst ein umfassendes Interview mit dem entsprechenden Informationssicherheitsbeauftragten (ISB) und den jeweiligen Fachspezialistinnen und Fachspezialisten der Behörde. Im Anschluss werden alle relevanten Dokumente (Richtlinien, Prozessbeschreibungen, Dienstanweisungen, etc.) gesichtet und überprüft. Während Dokumente die Theorie abbilden, zeigen Interviews oft die gelebte Praxis. Zuletzt erfolgt eine Wirksamkeitsprüfung, um die Umsetzung der Informationssicherheitsprozesse zu bewerten.

Abbildung 5-32: Resilienzsteigerung durch Standardrevision, Basisdatenerhebung, Umsetzungsberatung sowie Nachhaltung und Begleitung der ergriffenen Maßnahmen



Quelle: BSI

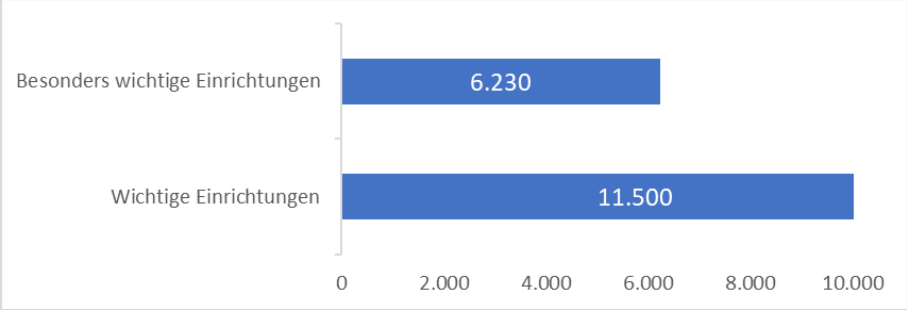
Die festgestellten Sicherheitsmängel und potenzielle Empfehlungen münden in einen umfassenden Prüfbericht. Dieser ist die Grundlage für eine weitere gezielte Umsetzungsberatung der Behörde durch das BSI, um Sicherheitsmängel nachhaltig zu beseitigen. Im Anschluss wird gemeinsam mit der geprüften Behörde ein Maßnahmenumsetzungsplan (MUP) erstellt. Dieser enthält die im Bericht festgestellten Mängel, eine Priorisierung sowie Maßnahmen zur Lösung. Mithilfe des MUP wird ein regelmäßiger Nachhalteprozess etabliert, um die Behörden seitens des BSI bestmöglich lösungsorientiert zu unterstützen.

Die Überprüfung der Sicherheitsmaßnahmen der Behörden und eine darauffolgende Beseitigung von Sicherheitsmängeln trägt somit maßgeblich zu einer resilienten Bundesverwaltung bei.

5.5.1.5 NIS-2-Registrierungen im BSI-Portal

Abbildung 5-33: NIS-2-Registrierungen im BSI-Portal am 30. Juni.2026

Einheit: Anzahl



Quelle: BSI

Am 6. Dezember 2025 ist das Gesetz zur Umsetzung der europäischen NIS-2-Richtlinie in Kraft getreten. Für die vom Gesetz erfassten wichtigen und besonders wichtigen Einrichtungen (wE und bwE) in Wirtschaft und Verwaltung gelten neue gesetzliche Pflichten in der IT-Sicherheit: Sie müssen sich beim BSI registrieren, erhebliche Sicherheitsvorfälle melden sowie technische und organisatorische Risikomanagement-Maßnahmen umsetzen.

Die Registrierung nehmen NIS-2-betroffene Einrichtungen im BSI-Portal vor (https://portal.bsi.bund.de/).

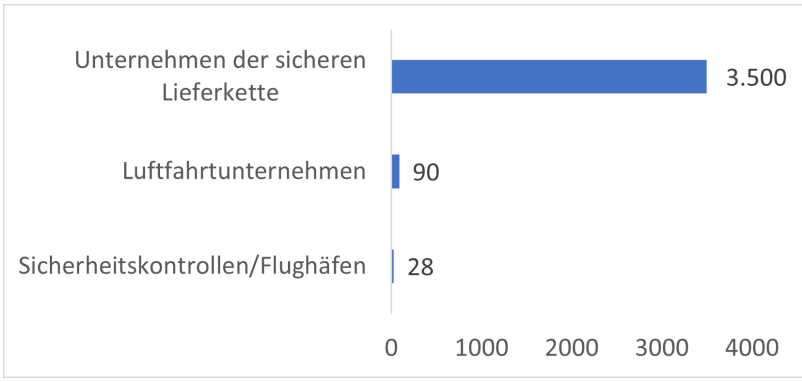
Bis zum 30. Juni 2026 haben sich dort insgesamt 17.730 Einrichtungen registriert. Davon waren 11.500 wichtige Einrichtungen und 6.230 besonders wichtige Einrichtungen (vgl. Abbildung 5-33).

→ für NIS-2-regulierte Unternehmen

5.5.1.6 Registrierungen von Luftsicherheitsakteuren im BSI-Portal

Abbildung 5-34: Akteure der Luftsicherheit in Deutschland

Einheit: Anzahl



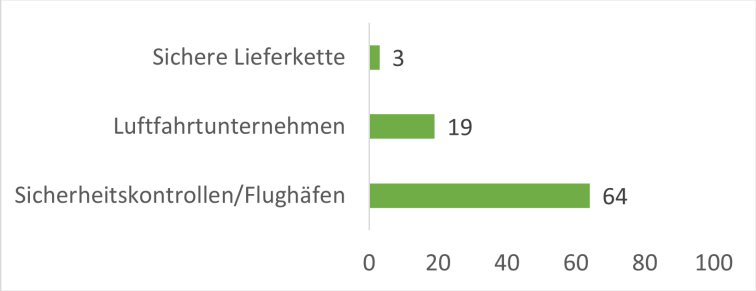
Quelle: BSI

Für die regulierten Akteure der Luftsicherheit gemäß Luftsicherheitsgesetz (LuftSiG, § 5/§ 8 Sicherheitskontrollen/Flugplatzbetreiber, § 9 Luftfahrtunternehmen und § 9a Beteiligte der sicheren Lieferkette) ist eine Registrierung für das Fachverfahren „Luftsicherheit“ im BSI-Portal unerlässlich, um die geltenden Melde- und Informationsvorgaben zu erfüllen und zusätzlich zielgruppenspezifische Informationen zur aktuellen Cybersicherheitslage zu erhalten. Zu den Unternehmen der Luftsicherheit in Deutschland zählen 28 Flughäfen, rund 90 Luftfahrtunternehmen und gut 3.500 Unternehmen der sicheren Lieferkette (vgl. Abbildung 5-34).

→ Mehr über Luftsicherheit

Bis zum 30. Juni 2026 hatten bereits 143 Einrichtungen das BSI-Angebot genutzt und sich im Fachverfahren „Luftsicherheit" registriert. Damit stärkt das BSI-Portal die transparente, praxisgerechte und handlungsorientierte Aufbereitung der Cybersicherheitslage für die zivile Luftfahrt. Dabei unterschied sich die Nutzung des Angebots durch die Unternehmenskategorien stark. Während bereits fast zwei Drittel der Sicherheitskontrollen/Flughäfen im Land registriert sind, traf dies auf nur 19 % der Luftfahrtunternehmen zu (vgl. Abbildung 5-35. Von den rund 3.500 Unternehmen der sicheren Lieferkette waren am 30. Juni2026 3 % registriert.

Abbildung 5-35: Registrierte Akteure der Luftsicherheit in Deutschland
Einheit: Anteile in Prozent

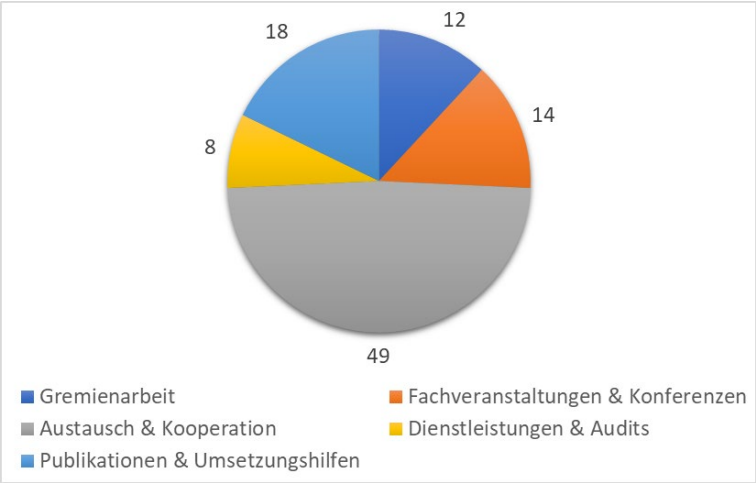


Quelle: BSI

Zur Einordnung der Anteilswerte ist zu berücksichtigen, dass sich die Größen der Zielgruppen deutlich unterscheiden: Es handelt sich um 28 Flughäfen, über 90 Luftfahrtunternehmen und rund 3.500 Beteiligte der sicheren Lieferkette (d. h. unter anderem reglementierte Beauftragte, bekannte Versender und zugelassene Transporteure). Zudem besteht derzeit nur für Flughäfen eine Pflicht zur Registrierung. Vor diesem Hintergrund sind insbesondere die bisher freiwillig erfolgten Registrierungen als guter Ausgangspunkt für eine künftige Ausweitung zu bewerten.

Das Leistungsportfolio des BSI umfasst insbesondere den kontinuierlichen Austausch und die Kooperationen mit der Zielgruppe zur Unterstützung von Cybersicherheitsmaßnahmen sowie die Zusammenarbeit mit dem Bundesministerium für Verkehr (BMV) und dem Luftfahrt-Bundesamt (LBA). Der Erstkontakt erfolgt häufig über das „Luftsicherheitsbüro“, das bei Fragen zur Cybersicherheit in der zivilen Luftfahrt unterstützt.

Abbildung 5-36: BSI-Leistungen für Akteure der Luftsicherheit
Einheit: Anteile in Prozent



Quelle: BSI

Über Fachtagungen, Messen (14 %, vgl. Abbildung 5-36) und Gremienarbeit (12 %) werden Cybersicherheitserkenntnisse direkt vermittelt. Ergänzend bieten zielgerichtete Publikationen und Umsetzungshilfen eine praxisnahe Unterstützung (18 %).

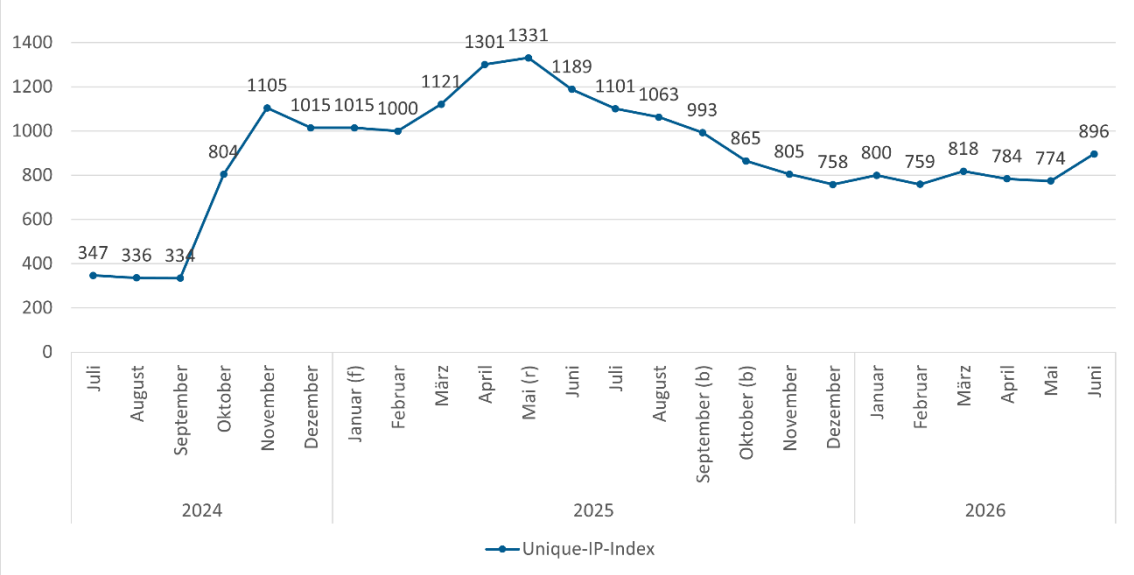
Hervorzuheben sind zudem der ACS-Expertenkreis „Cybersicherheit in der Luftfahrt“ mit über 100 Teilnehmenden, der Support zum BSI-Portal und zur NIS-2-Richtlinie sowie die Unterstützung der Nationalen Qualitätskontrollstelle (NQS) der Bundespolizei bei Luftsicherheitsaudits.

5.5.2 Das BSI für Verbraucherinnen und Verbraucher in Deutschland

5.5.2.1 Sinkholing

Abbildung 5-37: Unique-IP-Index

Einheit: 2019=100 (Messzahl)



Quelle: Botnetz-Monitoring

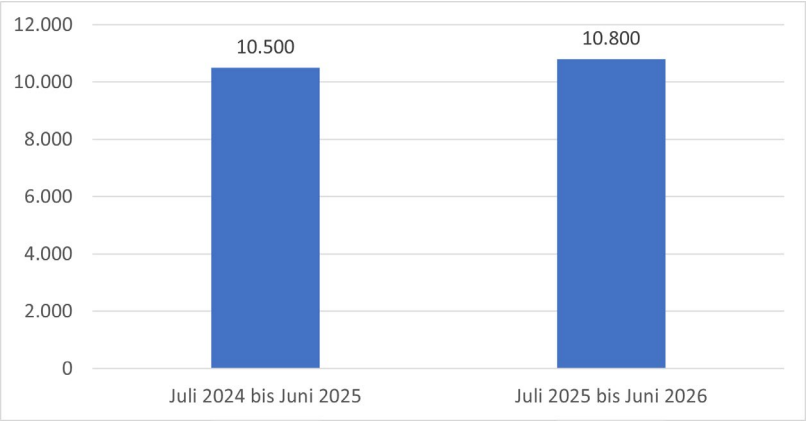
Bemerkung: Wert wurde (b) um Sondereffekte bereinigt, (f) fortgeschrieben, (r) korrigiert.

Im aktuellen Berichtszeitraum handelte es sich bei den weitaus meisten infizierten IT-Systemen in Deutschland um Consumer-IoT-Geräte (vgl. zur Angriffsfläche Vernetzte Geräte, vgl. zu Schadwirkungen Infizierte Systeme). Rund 90 % der infizierten Systeme gehörten zu dieser Kategorie. Das BSI informiert deutsche Netzbetreiber und Internetprovider über infizierte Systeme, damit diese ihre Kundinnen und Kunden warnen und zur Bereinigung der Systeme auffordern können. Der Unique-IP-Index, der das Aufkommen infizierter Systeme im BSI-Sinkholing misst, lag zum Ende des aktuellen Berichtszeitraums im Juni 2026 bei 896 Punkten (vgl. Abbildung 5-37) und damit 25 % unter dem Niveau des Vorjahresmonats. Hintergrund waren Systembereinigungen, insbesondere von Consumer-IoT-Geräten wie Smart-TVs und Heimroutern, welche die Betroffenen nach Hinweis des BSI an die zuständigen Internetprovider und Netzbetreiber vorgenommen haben.

5.5.2.2 Service-Center

Abbildung 5-38: Anfragen an das BSI-Service-Center

Einheit: Anzahl



Quelle: BSI

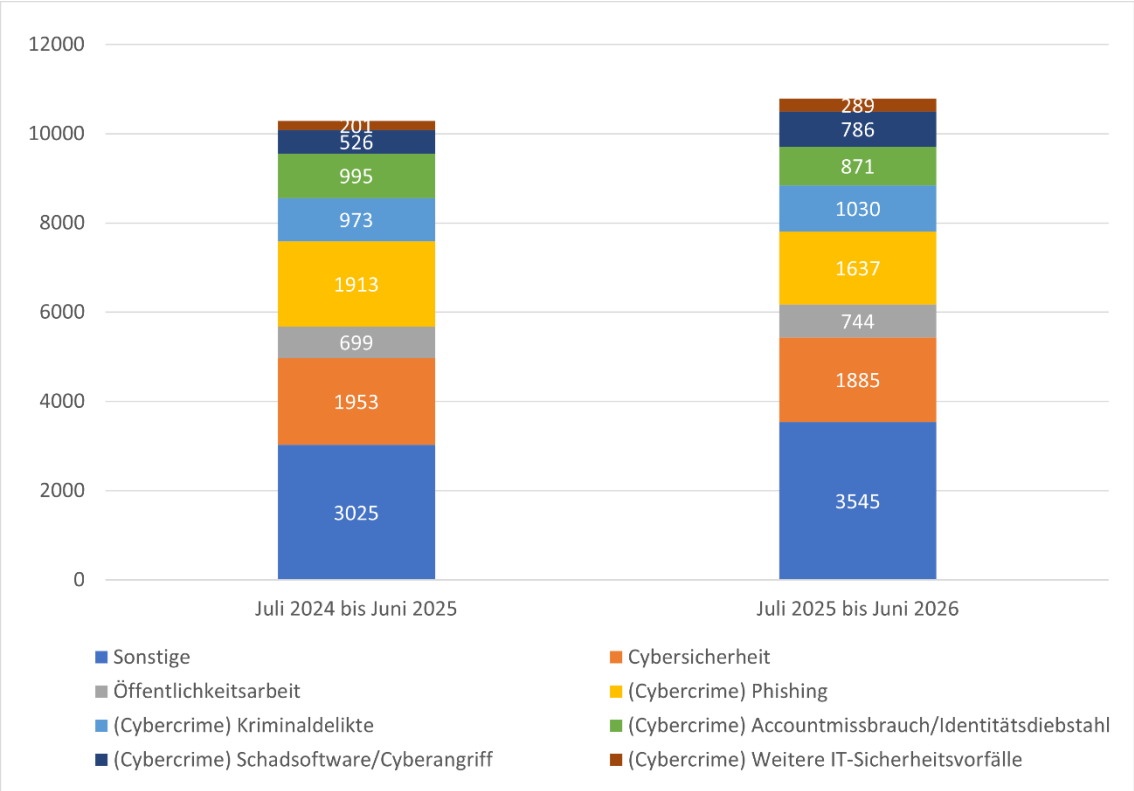
Das Service-Center des BSI ist Ansprechpartner für Verbraucherinnen und Verbraucher bei Cybersicherheitsvorfällen. Durch konkrete Informationen unterstützt es bei der akuten Bewältigung und hilft, zukünftigen Vorfällen vorzubeugen.

Knapp 10.800 Anfragen von Verbraucherinnen und Verbrauchern zum Thema Cybersicherheit erreichten das BSI-Service-Center im aktuellen Berichtszeitraum. Im Vergleich zum vorherigen Berichtszeitraum wurde ein Anstieg des Anfragevolumens um rund 3 % festgestellt (vgl. Abbildung 5-38).

→ Mehr über das Service Center

Das Service-Center des BSI fungiert als zentrale Kontaktstelle für Verbraucherinnen und Verbraucher, um Informationen und Hilfestellungen rund um Cybersicherheit zu erhalten. Die meisten Anfragen von Verbraucherinnen und Verbrauchern an das Service-Center des BSI bezogen sich im aktuellen Berichtszeitraum auf die Kategorie Cybercrime (insgesamt 43 %). Innerhalb der thematischen Kategorie Cybercrime standen insbesondere Anliegen zu Phishing (15 % aller Anfragen, vgl. Phishing-Mails) im Vordergrund. Es folgten Anfragen zu Kriminaldelikten (9 %), Accountmissbrauch und Identitätsdiebstahl (8 %), Schadsoftware-Infektionen (7 %) sowie weiteren IT-Sicherheitsvorfällen (2 %). Unter Sonstiges (32,9 %) wurden unter anderem Anfragen zu digitalen Behördenleistungen wie dem digitalen Personalausweis, sowie allgemeine Auskunftsersuchen nach DSGVO, IFG oder UIG erfasst. Konkrete Fragen zur Cybersicherheit wurden in 18 % der Anfragen gestellt.

Abbildung 5-39: Anfragen von Verbraucherinnen und Verbrauchern an das Service-Center nach Thema
Einheit: Anzahl



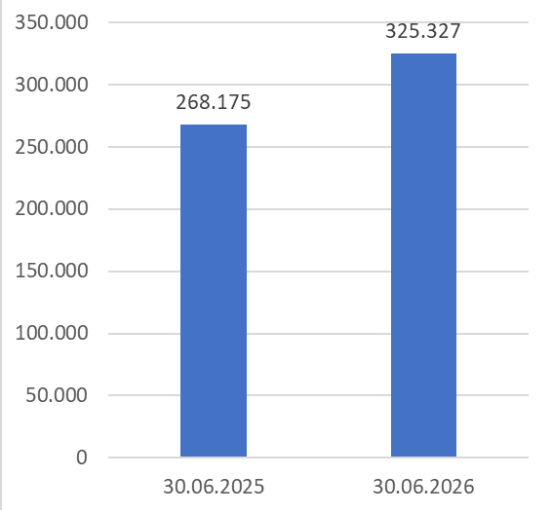
Quelle: BSI

Um Verbraucherinnen und Verbrauchern beim Aufbau ihrer Cyberresilienz zu unterstützten (vgl. Resiliente Gesellschaft) setzt das BSI auf ein breites Informations- und Tooling-Angebot. Dazu gehören leicht verständliche Inhalte, wie Checklisten und Schritt-für-Schritt-Anleitungen, die konkrete Hilfestellungen für den sicheren Umgang mit digitalen Technologien bieten. Ergänzend informiert das BSI regelmäßig über aktuelle Cybersicherheitsthemen, -trends und -vorfälle. Hierzu werden neben dem Podcast „Update verfügbar“ auch der Newsletter „Einfach • Cybersicher“, Social-Media-Beiträge sowie themenspezifische Kampagnen, wie zum Beispiel das E-Mail-Sicherheitsjahr oder das „Cyber 1x1“ mit Lern- und Unterrichtseinheiten zu Cybersicherheit veröffentlicht. Darüber wird die Öffentlichkeit mit dem vorliegenden Bericht über die Lage der IT-Sicherheit in Deutschland unterrichtet.

5.5.2.3 Newsletter

Abbildung 5-40: Newsletter-Abonnements

Einheit: Anzahl



Quelle: BSI

Mit dem Newsletter „**Einfach • Cybersicher**" informiert das BSI Verbraucherinnen und Verbraucher regelmäßig über Vorfälle und aktuelle Trends, damit diese sich besser schützen können. Er richtet sich an alle, die über die wichtigsten Ereignisse rund um die Sicherheit ihres digitalen Alltags mit praktischem Wissen auf dem Laufenden gehalten werden wollen. Der Newsletter erscheint einmal im Monat und ist in leicht verständlicher Sprache geschrieben.

Der Newsletter erfreut sich zunehmender Nachfrage. Die Zahl der Newsletter-Abonnements ist von 268.175 am 30. Juni 2025 auf 325.327 am 30. Juni 2026 angestiegen (vgl. Abbildung 5-40). Das entspricht einem Wachstum von 21 %.

→ Newsletter abonnieren

Ausgewählte Vorfälle: Resilienz - Operation Endgame

Sachverhalt

Die international koordinierteOperation Endgame ging im Zeitraum vom 15. bis zum 19. Juni2026 gegen Schadsoftware drei relevanter Schadsoftware-Familien (SocGholish, StealC und Amadey) vor. Das BSI hatte mit technischen Analysen, Threat Intelligence und Sinkholing zum Gelingen der Operation beigetragen. Beteiligt waren außer dem BSI unter anderem die Generalstaatsanwaltschaft Frankfurt am Main – Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT), das BKA sowie Strafverfolgungsbehörden aus den Niederlanden, Dänemark, Großbritannien, USA und Kanada. Des Weiteren gab es Unterstützung vonseiten Europol, Eurojust, dem US-Softwareunternehmen Microsoft und weiteren internationalen IT-Sicherheitsdienstleistern.

Im Verlauf der Operationen wurden rund 15.000 Websites, über 320 Server – davon 40 in Deutschland – und mehr als 140 betroffene Domains unschädlich gemacht. Es wurden außerdem ca. 33,5 Millionen Zugangsdaten von über 385.000 Betroffenen sichergestellt, wodurch eine Prüfung der individuellen Betroffenheit über öffentlich zugängliche Informationsplattformen ermöglicht wurde. Das BSI stellte mit seiner Threat Intelligence Informationen und Hintergrundwissen zu den Tätergruppierungen, ihrer Motivation und eingesetzten Angriffstechniken zur Verfügung und trug damit wesentlich zur Aufdeckung der Steuerungsserver bei. Durch Sinkholing wurde der Netzwerkverkehr zwischen den von Kriminellen kontrollierten IT-Systemen und der Schadsoftware auf den Opfersystemen umgeleitet, um somit die Kommunikation zwischen den infizierten Computern und den Steuerungsservern der Cyberkriminellen zu stoppen. Zusätzlich unterstützt das BSI bei der Benachrichtigung von Betroffenen in Deutschland. Darüber hinaus

wurde Kryptovermögen im Wert von ca. 47 Millionen US-Dollar identifiziert, gekennzeichnet und dadurch in der Nutzung eingeschränkt.

Im Fokus der Aktion stand insbesondere die Schadsoftware StealC, mit der Kriminelle in den vergangenen Monaten Zugangsdaten und weitere sensible Informationen auf infizierten IT-Geräten ausgespäht hatten. Diese Schadsoftware gehört zur Kategorie der Infostealer (Datendieb), die mittlerweile über Funktionen zum Nachladen weiterer Schadsoftware verfügen. Bisher lag deren Hauptaufgabe ausschließlich in der Infizierung von Opfersystemen, um sensible Daten und Zugangsinformationen zu stehlen. Darüber hinaus ist ein weiteres Ziel der Operation Endgame, die relevantesten Schadsoftware-Varianten der Kategorie Initial Access Malware (sog. Dropper/Loader) unschädlich zu machen. Diese werden häufig zur Erstinfektion genutzt und dienen somit als Türöffner, um unbemerkt Opfersysteme zu infizieren und weitere Schadsoftware nachzuladen. Mit Stand 24. Juni 2026 lagen dem BSI Informationen zu mehr als einer Million betroffener Konten für E-Mail-Zugänge, Messenger-Dienste, Online-Banking, Online-Shops, Gaming-Plattformen und hunderten anderen Online-Diensten vor. Die Passwörter zu den betroffenen Nutzerkonten liegen dem BSI nicht vor.

Bewertung

Die Operation Endgame ist ein in 2022 initiiertes Ermittlungsverfahren internationaler Strafverfolgungsbehörden. Das BSI beteiligt sich seit 2024. Ziel ist es, mit regelmäßigen Aktionen die Angriffskette des Business-Modells Cybercrime-as-a-Service zu durchkreuzen. Die Aktion im Juni 2026 ist bereits die vierte koordinierte Maßnahme gegen die organisierte Cyberkriminalität. Im Zuge vorheriger Aktionen wurden mehrere cyberkriminelle Gruppierungen zerschlagen und Schadsoftware-Familien vom Netz genommen. Im Mai 2024 beispielsweise richtete sich die Aktion gegen finanzielle, personelle und technische Infrastrukturen der Schadsoftware-Familien IcedID, SystemBC, BumbleBee, Smokeloader, Pikabot und Trickbot, deren Aktivitäten erfolgreich beendet wurden. Im September 2024 wiederum wurden Plattformen und Vermögenswerte der kriminellen Kryptowährungsbörsen Cryptex und PM2BTC beschlagnahmt und sichergestellt. Im April 2025 wurden als Maßnahme gegen identifizierte Kundinnen und Kunden des Smokeloader-Akteurs Superstar75737 mehrere Personen vorläufig festgenommen und vernommen sowie Hausdurchsuchungen durchgeführt. Das BSI ist seit dem ersten Schlag im Mai 2024 eingebunden, wertet technische Beweismittel aus, ermöglicht durch Sinkholing die Umleitung des Datenverkehrs auf behördeneigene Server und hilft bei der Bereinigung der Systeme. Damit und mit der aktiven Benachrichtigung Betroffener trägt das BSI maßgeblich zum Opferschutz in Deutschland bei und unterstützt die Ermittlungen und Maßnahmen mit seiner technischen Expertise. Die Benachrichtigung der oben genannten mehr als einer Million Betroffenen war durch die enge Vernetzung des BSI in die Wirtschaft und in den Bereich KRITIS möglich.

Durch das gezielte Vorgehen gegen die Schadsoftware StealC wurden zum zweiten Mal Datensätze eines Infostealers verarbeitet und die vom Datenabfluss betroffenen Personen gewarnt. Der ganzheitliche Ansatz der Abschaltung der Täterinfrastrukturen und Opferwarnungen trägt nachhaltig dazu bei, dass eine zerschlagene Schadsoftware-Familie auch zerschlagen bleibt

Reaktion

Das BSI informiert automatisiert Einrichtungen der öffentlichen Verwaltung, Betreiber Kritischer Infrastrukturen und Unternehmen, welche über NIS-2 oder über die Allianz für Cybersicherheit im BSI registriert sind, zu erkannten Betroffenheiten. Privatpersonen wurden über ihre jeweiligen Internetprovider informiert, denen das BSI bei vorliegender Schadsoftwareinfektion – sofern möglich – die jeweilige IP-Adresse zur Verfügung stellte. Zusätzlich wurde Privatpersonen empfohlen, einen der gängigen Identity-Leak-Checker zu nutzen, in denen gestohlene Zugangsdaten aus bekannten Quellen zur Überprüfung hinterlegt sind. Betreiber von Online-Diensten wurden zudem aufgefordert, ihre betroffenen Nutzerinnen und Nutzer entsprechend zu informieren.

6 Sonderlagen

6.1 Digitale Souveränität

„Digitale Souveränität“ beschreibt die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können. Im aktuellen Berichtszeitraum sind die politischen und wirtschaftlichen Unsicherheiten in der EU aufgrund geopolitischer und geoökonomischer Spannungen gewachsen. Gleichzeitig ist die digitale Sphäre, die permanent Cyberangriffen ausgesetzt ist, als eigenständige Dimension im Rahmen dieser Spannungen in den Vordergrund getreten. Immer mehr IT-Produkte bilden Angriffsflächen und bergen Risiken. Digitale Abhängigkeiten von außereuropäischen Anbietern, die Deutschland verwundbar machen und seine Handlungsfähigkeit einschränken können, betreffen insbesondere Alltagsthemen wie Mobilfunk, die Energiewende sowie eine Vielzahl digitaler Produkte und Dienste wie Betriebssysteme mobiler Endgeräte oder Social-Media-Angebote. Zudem besteht dringender Bedarf die digitale Souveränität im europäischen Finanzsektor herzustellen.

Um mit digitalen Innovationen Schritt zu halten und dabei digitale Souveränität zu erlangen, ist eine Doppelstrategie zielführend: Zum einen müssen der europäische Markt und die deutsche Digitalindustrie mit dem Ziel technischer und wirtschaftlicher Konkurrenzfähigkeit in ausgewählten Technologiefeldern gestärkt werden. Des Weiteren müssen außereuropäische Produkte mit Hilfe technischer Kontrollschichten so abgesichert werden, dass eine selbstbestimmte Nutzung ohne potentielle Einflussnahme Dritter möglich wird.

Um den Einsatz digitaler Produkte und Services „made in Europe“ zu stärken, setzt das BSI unter anderem auf Public-Private-Partnerships. So haben das BSI und der Hosting- und Cloud-Anbieter IONOS im Januar 2026 eine strategische Kooperation geschlossen. IONOS unterstützt in Abstimmung mit dem BSI die Bundesverwaltung beim Aufbau einer Private-Enterprise-Cloud-Umgebung sowie bei der Fortentwicklung kryptographischer Verfahren. Zudem wurde im Februar 2026 eine Zusammenarbeit zwischen dem BSI und Schwarz Digits (IT-Sparte der Schwarz Gruppe) vereinbart. Ziel ist unter anderem die gemeinsame Entwicklung souveräner Cloud-Lösungen, die auch für den Einsatz in der Bundesverwaltung und in den Landesverwaltungen nutzbar gemacht werden können.

Mit den C3A - Criteria enabling Cloud Computing Autonomy hat das BSI im März 2026 eine richtungsweisende Handreichung vorgelegt, die die Souveränitätseigenschaften von Cloud-Diensten transparent macht. Während die Sicherheitseigenschaften von Cloud-Diensten im Cloud Computing Compliance Criteria Catalogue (C5) des BSI adressiert werden, ermöglicht der Kriterienkatalog C3A eine Bewertung, ob ein Cloud-Angebot im Risikokontext des Anwendungszwecks selbstbestimmt genutzt werden kann. Die C3A dienen dabei als Kriterienkatalog, sie schaffen Transparenz und Orientierung, entfalten jedoch keine regulative Wirkung. Die C3A können sowohl von Cloud-Anbietern als auch von Cloud-Kunden genutzt werden. Cloud-Anbieter können die Einhaltung der Kriterien durch ein Audit nachweisen. Cloud-Kunden können das Framework nutzen, um für das eigene Nutzungsszenario relevante Anforderungen zu identifizieren.

Künstliche Intelligenz (KI) hat sich zu einer strategischen Basistechnologie mit unmittelbaren Auswirkungen auf nationale Sicherheit, staatliche Handlungsfähigkeit, wirtschaftliche Wettbewerbsfähigkeit und gesellschaftliche Stabilität entwickelt: Hochleistungsfähige KI-Modelle verfügen über erhebliche Fähigkeiten in den Bereichen Cyberoperationen, Softwareentwicklung, Automatisierung komplexer Entscheidungsprozesse sowie Wissens- und Informationsverarbeitung. Deutschland benötigt eine dauerhaft leistungsfähige institutionelle Struktur zur technischen Evaluierung und sicherheitspolitischen Einordnung solcher Systeme. Dem trägt die Bundesregierung mit dem neu gegründeten AI Safety and Security Institute Deutschland (AISI Deutschland).

Digitale Souveränität bedeutet, Optionen zu schaffen: Je mehr vertrauenswürdige Produkte verfügbar sind, desto souveräner kann entschieden werden und desto sicherer wird die digitale Zukunft.

6.2 Cyberdome

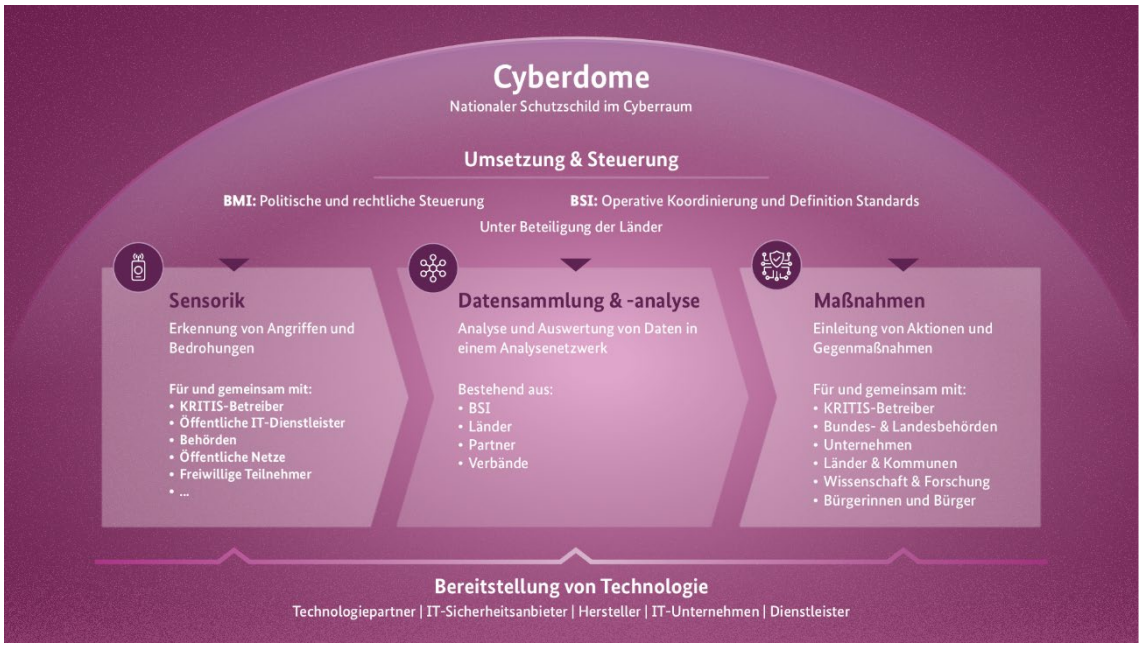
Als führende Wirtschaftsnation und wichtige Drehscheibe der NATO und der EU ist Deutschland ein attraktives Ziel – sowohl für finanziell motivierte als auch staatlich gelenkte Cyberangriffe mit ideologischem, politischem oder militärischem Hintergrund. Hybride Bedrohungen und zum Teil KI-gestützte Angriffe verschärfen die Lage qualitativ und quantitativ.

Daher hat das Bundeskabinett auf Initiative von Bundesminister des Innern, Alexander Dobrindt, im August 2025 beschlossen, dass das Bundesinnenministerium (BMI) ein Realisierungskonzept für einen deutschen Cyberdome erarbeitet. Daran ist das BSI maßgeblich beteiligt.

Was ist der Cyberdome?

Der Cyberdome ist als Schutzschirm für den digitalen Raum der Bundesrepublik geplant. Als zentral koordiniertes Frühwarn- und Schutzsystem soll er Cyberangriffe auf staatliche Institutionen, Kritische Infrastrukturen, Unternehmen sowie die Gesellschaft schneller erkennen, auswerten und die Auswirkungen sowie Schäden der Angriffe minimieren. Dazu werden bereits bestehende Systeme vernetzt oder Sensorik gezielt ergänzt, beispielsweise bei Betreibern Kritischer Infrastruktur oder freiwillig beteiligten Institutionen. Automatisierte Analysen in Echtzeit werten die gewonnenen Informationen systematisch aus und ermöglichen so eine koordinierte Reaktion.

Abbildung 6-1: Cyberdome



Quelle: BSI

Info-Kasten

Der Cyberdome baut auf drei Säulen:

1. Sensorik

Diese umfasst den Aufbau einer Infrastruktur, die dabei hilft Angriffsvektoren und Schwachstellen in öffentlichen Netzen, bei Betreibern Kritischer Infrastrukturen sowie bei freiwillig teilnehmenden Organisationen besser zu erkennen. Dazu werden bereits vorhandene Systeme vernetzt. Wo bestehende Systeme Lücken aufweisen, kann zusätzlich Sensorik gezielt ergänzt werden. So entsteht eine breitere und frühere Sicht auf Bedrohungen, ohne in die geschützten Systeme einzugreifen

2. Analyseverbund

Im Analyseverbund werden die durch Sensorik und weiteren Quellen gewonnenen Informationen zusammengeführt und ausgewertet. Teilnehmende des Analyseverbunds können neben dem BSI

beispielsweise auch Partner aus der öffentlichen Verwaltung, Wirtschaft, Forschung, aus Verbänden und weitere Dienstleister sein. Dabei werden grundlegende Prinzipien wie Datenschutz, Datensparsamkeit und Pseudonymisierung konzeptionell berücksichtigt. So lassen sich einzelne Hinweise verbinden und Bedrohungen besser erkennen und einordnen. Das daraus entstehende gemeinsame Lagebild geht weit über die Sicht einzelner Organisationen hinaus. Dank dieses gemeinsamen Frühwarnsystems können Erkenntnisse zu einem Angriff auch anderen Beteiligten helfen, sich frühzeitig zu schützen.

3. Maßnahmen

Der Cyberdome ist als offenes technisches System ausgelegt, in dem unterschiedliche Anwendungen miteinander kommunizieren können. Dazu werden genormte Schnittstellen und offene Standards genutzt. Über diese können bestehende Technologien eingebunden und neue Sicherheitslösungen ergänzt werden. Durch die Anbindung ist es Unternehmen, KRITIS-Betreibern, Behörden oder auch Forschungseinrichtungen möglich, Informationen des Analyseverbunds automatisiert zu nutzen und in wirksame Schutzmaßnahmen zu überführen. Auf diese Weise entsteht ein Netzwerk, das mit den Anforderungen und Bedrohungen im Cyberraum mitwachsen kann.

Welche Rolle spielt das BSI?

Gemeinsam mit dem BMI befindet sich das BSI derzeit in der Konzeptions- und Planungsphase für den Cyberdome, die bis Jahresende 2026 abgeschlossen sein soll. Der Cyberdome wird als mehrjähriges Programm konzipiert, das bestehende Fähigkeiten neu skaliert, integriert und neue Initiativen bündelt. Das BSI baut dafür bestehende Leistungen und Expertise im Bereich der Informations- und Cybersicherheit zunächst weiter aus, indem schrittweise neue Funktionen zum Einsatz kommen. Dabei spielt auch die Zusammenarbeit mit weiteren Behörden und Einrichtungen des Bundes und der Länder eine zentrale Rolle. Zudem werden Akteure aus Wirtschaft und Zivilgesellschaft aktiv eingebunden, um bestehende Bedarfe direkt adressieren zu können und hinreichende Akzeptanz bei allen Beteiligten zu schaffen.

Bereits in der Konzeptionsphase startete das BSI im aktuellen Berichtszeitraum mit ersten Schutzmaßnahmen und Pilotprojekten, die als Proof of Concept umgesetzt wurden. Die Ergebnisse der Pilotprojekte dienen dem weiteren strukturierten Ausbau des Cyberdome und einer schrittweisen Skalierung.

- Im März 2026 ist ein erstes Pilotprojekt mit den öffentlichen IT-Dienstleistern von Ländern und Kommunen angelaufen. Dabei wird der Einsatz der Datensensorik und Echtzeitanalyse ausgebaut, um so das Frühwarnsystem für Cybersicherheitsvorfälle zu verbessern.

- Zudem ist das Projekt "Deutschland-Scan" bereits in Betrieb. Es handelt sich um eine Art Fitness-Check für die deutsche Internet-Infrastruktur. Hier prüft das BSI, wie gut diese gegen Cyberangriffe geschützt ist: In einem automatisierten Breitenscan werden regelmäßig rund 13 Millionen öffentlich erreichbare Systeme und Webseiten auf Schwachstellen gecheckt. Im anlassbezogenen Tiefenscan, ausgelöst zum Beispiel durch kritische BSI-Sicherheitsmeldungen, werden Erkenntnisse aus dem Breitenscan genutzt, um in einer aufwendigen Detailanalyse unter anderem zu klären, wie die Schwachstelle funktioniert und unter welchen Voraussetzungen sie aus dem Internet ausnutzbar ist. Werden Auffälligkeiten festgestellt, warnt das BSI die Betroffenen.

- Auch mit ersten KRITIS-Betreibern arbeitet das BSI schon intensiv im Bereich der erweiterten Datensensorik am Aufbau einer Infrastruktur zur verstärkten Erkennung von Angriffsvektoren und Schwachstellen.

6.3 Künstliche Intelligenz

KI verändert die Cyberlage und fordert neue Fähigkeiten in Cyberprävention und -verteidigung

Die Entwicklung künstlicher Intelligenz hat in den vergangenen Jahren erheblich an Dynamik gewonnen und dabei Fähigkeiten hervorgebracht, die noch vor kurzer Zeit kaum vorstellbar waren.

Neben Sprache, Bildgenerierung oder Automatisierung, zeigten sich im aktuellen Berichtszeitraum auch fortlaufend neue, komplexe Cyberfähigkeiten – von der Schwachstellenanalyse bis hin zur Unterstützung bei Angriffen, aber auch Verteidigungsmaßnahmen sowie zu deren teilautonomer Durchführung. Die Komplexität von Aufgaben, die KI-Modelle selbstständig bewältigen können, wächst rasant. Damit beeinflusst KI entscheidend die Bedrohungslage und die Geschwindigkeit, mit der Bedrohungen zunehmen.

Cyberfähigkeiten von KI steigen – beim automatisierten Erkennen und Ausnutzen von Schwachstellen bis hin zum selbstständigen Platzieren von Schwachstellen in legitimen Systemen

Ein Faktor für das immer schnellere Ausnutzen von Schwachstellen ist der zunehmende Einsatz von KI. Die aktuell stärksten Modelle sind sogenannte „Frontier"-KI-Modelle. Sie können im Vergleich zu Vorgängermodellen deutlich schneller deutlich mehr Schwachstellen in Software finden und komplexere, funktionsfähige Exploits zur automatisierten Ausnutzung dieser Schwachstellen passend generieren. Selbst vermeintlich weniger kritische Schwachstellen gewinnen durch die neue Bedrohungslage an Bedeutung, da die Modelle in der Lage sind, mehrere Schwachstellen miteinander zu kombinieren und daraus neue, kritische Angriffsvektoren abzuleiten.

KI-Modelle mit Cyberfähigkeiten sind immer leichter zugänglich

Während proprietäre KI-Modelle aktuell nur einem ausgewählten und herstellerseitig verifizierten Nutzerkreis vollumfänglich zur Verfügung stehen, holen auch Open-Source-/Open-Weight-Modelle in Bezug auf komplexe Cyberfähigkeiten auf, wenngleich ihre Fähigkeiten hinter den Spitzenmodellen zurückbleiben. Dabei ist neben einem Modell selbst zunehmend auch der sogenannte Harness entscheidend, also die Umgebung und die Werkzeuge, durch die das Modell seine Fähigkeiten im jeweiligen Einsatzkontext erweitert.

Durch die Entwicklung starker, frei zur Verfügung stehender KI-Modelle sinken die Hardwareanforderungen, sodass – bei anhaltender Entwicklung – der Betrieb sogar auf hochwertiger Consumer-Hardware und mit KI-Agenten inklusive „Harnessing" vorstellbar ist. Demensprechend ist zu erwarten, dass böswillige Akteure in absehbarer Zeit Zugang zu fähigen KI-gestützten Werkzeugen haben und diese mit den sinkenden Hardware-Voraussetzungen intensiver nutzen.

Durch die Nutzung von KI werden Cyberangriffe sowohl in Geschwindigkeit als auch Komplexität zunehmen. In der Vergangenheit wurde KI im Wesentlichen zur Verbesserung existierender Angriffstechniken wie Phishing oder anderen Social-Engineering-Formen genutzt. Auch bei zukünftigen, stärker autonomen Angriffen ist zu erwarten, dass diese bekannten Angriffsmethoden eine wichtige Ausgangsbasis bilden werden. Vor diesem Hintergrund bleiben eine solide Grundabsicherung und gezieltes Mitarbeitertraining wichtig. Trotzdem ist davon auszugehen, dass Anzahl und Erfolgsquote jener Angriffe zunehmen werden, bei denen KI-Systeme direkt mit Zielsystemen interagieren bei denen sie beispielsweise Schwachstellen identifizieren und ausnutzen, um Zugriff auf Systeme aller Art zu erlangen.

KI-Systeme erweitern die Angriffsfläche

Ein zusätzlicher Einfluss auf die Cyberbedrohungslage ergibt sich durch die legale Nutzung von KI: Der Einsatz von KI-Systemen erweitert häufig die Angriffsfläche der IT-Umgebung, da neuartige Angriffsvektoren wie (indirekte) Prompt Injections möglich sind. Deren Auswirkungen werden leicht unterschätzt und oft nicht ausreichend mitigiert. Auf Firmenwebsites bereitgestellte Chatbots oder intern genutzte KI-Sprachmodelle können zum Beispiel durch maliziöse Eingaben manipuliert werden, sodass sie möglicherweise interne Daten preisgeben oder sogar über angeschlossene Werkzeuge fremden Code ausführen. Letzteres stellt die Hauptgefahr bei der Nutzung agentischer KI dar.

KI-Agenten: ein mögliches Risiko für die Betriebssicherheit

Neben dem bewussten Einsatz von KI als Angriffswerkzeug, wurde in den letzten Monaten deutlich, wie sehr uns die Autonomie von KI-Agenten vor Herausforderungen stellt: Seien es Frontier-Modelle, die ungeplant aus ihren Testumgebungen ausbrechen, oder privat genutzte KI-Assistenten, die Infrastrukturen und alltägliche Einrichtungen, beispielsweise Fitnessstudios, hacken. Eine

Studie über den Zeitraum von Oktober 2025 bis März 2026 stellte eine deutliche Steigerung öffentlich diskutierter Vorfälle fest, bei denen autonome KI-Agenten eigenständig Strategien verfolgten, die von den vorgegebenen Zielen oder Sicherheitsvorgaben abwichen oder diese gezielt zu umgehen versuchten. Ob die konkreten Gründe bei Lücken in den Vorgaben, Konflikten zwischen System- und Nutzerprompt, mangelnder Überwachung oder einer zu starken Forcierung des Modells auf die Erreichung eines vorgegebenen Ziels lagen: Immer wieder wird klar, dass die wahrscheinlichkeitsgesteuerte Natur der zugrundeliegenden Neuronalen Netze es verhindert, über die Sprachebene konkrete Sicherheitsschranken nachhaltig durchzusetzen. Die Vorfälle machen deutlich: KI-Modelle sind nicht zuverlässig an menschlichen Zielen und Werten ausgerichtet. Auch bestehende Sicherheitsmechanismen können diese grundlegende Herausforderung nicht vollständig lösen. Hierdurch können sowohl die Angriffssicherheit (Security) als auch die Betriebssicherheit (Safety) betroffen sein: Während Security den Schutz vor absichtlichen Angriffen und Missbrauch bezeichnet, zielt Safety auf die Vermeidung von Schäden durch Fehlverhalten oder unvorhergesehenes Systemverhalten. Bei KI-Agenten können beide Ebenen relevant werden, da ein autonom handelndes System auch ohne böswillige Absicht schädliche Handlungen ausführen und dadurch ein Safety-Risiko darstellen kann.

Prävention und Verteidigung gegen Cyberbedrohungen muss kurzfristig ertüchtigt werden – mit KI

Die hohe Umsetzungsgeschwindigkeit autonom geführter Cyberangriffe erfordert auch auf Seiten der Verteidigung eine entsprechende KI-Unterstützung. Daher ist es essentiell, sich auf Verteidigerseite robuste automatisierte Abläufe (Pipelines) aufzubauen, die KI nutzen, um eigenen Programmcode präventiv auf Schwachstellen zu untersuchen und zu patchen, aber auch, um Angriffe zu detektieren und abzuwehren. Da nicht nur das genutzte KI-Modell eine entscheidende Rolle für den Erfolg eines solchen automatisierten Ablaufs spielt, sondern auch dessen technische Umgebung einen großen Einfluss auf die Qualität hat, sollte man nicht auf die Verfügbarkeit bestimmter Modelle warten, sondern bereits jetzt mit aktuell verfügbaren Modellen arbeiten. Sprachmodelle werden über standardisierte Schnittstellen integriert und können zur Verbesserung der Gesamtqualität je nach Verfügbarkeit gegen leistungsfähigere Modelle ausgetauscht werden. Dies erlaubt den Unternehmen nicht nur, die Fähigkeiten aktueller Modelle zeitnah zu nutzen, sondern auch, interne Prozesse und Datenströme an die neue Anwendung anzupassen und entsprechende Expertise unter den Mitarbeitenden aufzubauen.

Zugang zu starken KI-Modellen – eine Frage der Digitalen Souveränität für Deutschland und Europa

Dennoch wird der notwendige Zugang zu den besten Modellen eine Herausforderung in Europa bleiben. Proprietäre Modelle sind durch verschiedene Leitplanken (sogenannte Guardrails) abgesichert, die missbräuchliche Nutzung verhindern oder erschweren sollen. Dieselben Schutzmechanismen sind jedoch zum Teil auch bei legitimen defensiven Anwendungsfällen aktiv, sodass die Verteidigerseite für bestimmte Aufgaben auf die relevanten Fähigkeiten der Modelle nicht zurückgreifen kann. Offen verfügbare beziehungsweise selbst betriebene KI-Modelle könnten europäischen Stakeholdern eine größere Kontrolle über Modell und Einsatzumgebung ermöglichen, erweisen sich aber noch nicht als gleich leistungsfähig. Auch wenn die offenen Modelle und KI-Agenten aufholen, existiert hier momentan eine kritische Zeitlücke, die die privilegierten Nutzer (vor allem US-amerikanische Firmen) der unlimitierten Frontier-Modelle (ohne Leitplanken) mit Vorteilen für Verteidigung ausstattet, während andere Nutzer sich auf einen Wettlauf mit ähnlichen Mitteln wie die Angreifer einlassen müssen. Dabei stehen sie vor einer zusätzlichen Herausforderung, da Angreifer aufgrund der grundsätzlichen Asymmetrie zwischen Angriff und Verteidigung ohnehin im Vorteil sind.

Darüber hinaus stehen die für den eigenständigen Betrieb und das Hosting erforderliche Infrastruktur sowie das notwendige technische Know-how nicht jedem Unternehmen zur Verfügung. Für die europäische Cyberabwehr stellt sich damit zunehmend die Frage, ob ausreichend leistungsfähige und zugleich kontrollierbare KI-Modelle für eine sichere Verteidigung aller Teilnehmenden verfügbar gemacht werden können. Obwohl der Einsatz von Guardrails ein wichtiger Baustein in der KI-Sicherheit ist, muss sichergestellt werden, dass verteidigende Institutionen Zugang zu leistungsfähigen und restriktionsarmen KI-Modellen erhalten.

Resilienz mit und durch KI

Bei zunehmender Autonomie und Adoption von KI-Systemen darf die Steigerung der Modell-Fähigkeiten nicht die einzige Priorität sein. Sicherheit muss bereits bei der Entwicklung berücksichtigt und transparent umgesetzt werden. Sicherheitsmaßnahmen müssen entwickelt, überprüft und durch kontinuierliche Überwachung auch im laufenden Betrieb nachgewiesen werden.

Um die Chancen und Risiken durch Frontier KI-Modelle für Deutschland zu evaluieren und die Resilienz im Bereich KI nachhaltig zu stärken, wurde Ende August 2026 das neue nationale AI Safety and Security Institute Deutschland (AISI Deutschland) in Berlin gegründet. Der Aufbau erfolgt in mehreren Phasen: Zunächst erfolgt eine Aufgabenteilung entlang der Dimensionen (Cyber-)Security (BSI) und Safety (BNetzA). Im zweiten Schritt wird das Institut zu einer Beratungsinstanz zu KI-Fragen ausgebaut. Zudem ist die Vernetzung mit internationalen Partnern in Frankreich, dem Vereinigten Königreich und dem EU AI Office geplant, um Wissen auszutauschen und gemeinsame Standards zu erarbeiten.

Anhang

Methodische Hinweise

Kennzahlen wie Indizes, Scores, Anteilswerte oder Tagesdurchschnitte werden, soweit nicht anders angegeben, mit spitzen Werten berechnet und in gerundeten Werten ausgewiesen. Es kann daher insbesondere bei Aggregationen zu Rundungsdifferenzen kommen.

Soweit nicht anders angegeben ist der Vergleichszeitraum der Berichtszeitraum des Vorjahresberichts.

Zeichenerklärung

f Wert wurde fortgeschrieben.

. Wert ist unbekannt.

- Wert ist empirisch Null (d.h. nichts vorhanden).

0 Wert ist rechnerisch Null (d.h. empirisch größer als nichts).

X Aussage ist nicht sinnvoll.

r Wert wurde gegenüber früheren Publikationen berichtigt.

/ Wert ist statistisch unsicher und wird daher nicht ausgewiesen.

Aktivitätsniveaustatistik (ANS)

Ziel: Die Aktivitätsniveaustatistik erhebt die bei westlichen Cybersicherheitsexpertinnen und -experten bekannte Gefährdungslage durch Cyberspionage- und Cybercrime-Angriffe. Berichtet wird quartalsweise summarisch über das Aufkommen an Cyberspionage- und Cybercrime-Angriffen, die von für die westliche Welt relevanten Angreifergruppen durchgeführt werden.

Grundgesamtheit: Grundgesamtheit sind alle Cyberspionage- und Cybercrime-Angriffe weltweit im Quartal, die von für die westliche Welt relevanten Angreifergruppen durchgeführt werden.

Stichprobe und Erhebungsdesign: Es fließen alle Cyberspionage- und Cybercrime-Angriffe ein, die das IT-Sicherheitsdienstleistungs-Unternehmen CrowdStrike mittels eigener Sensorik in den Netzen seiner Kunden detektiert und analysiert. Dabei werden einzelne Sensor-Anschläge zu Angriffen aggregiert und diese sodann quartalsweise aufsummiert.

Reichweite: Mit der Aktivitätsniveaustatistik werden summarisch Strukturinformationen über die Gefährdungslage durch Cyberspionage- und Cybercrime-Angriffe für die westliche Welt erfasst. Aussagen über einzelne Angriffe auf einzelne Organisationen sind damit nicht möglich. Ein Rückschluss auf einzelne von CrowdStrike geschützte Netzwerke ist ebenfalls nicht möglich. Zudem werden prioritär Angreifergruppen beobachtet, die für die westliche Welt relevant sind. Angriffe von Angreifergruppen, die ausschließlich gegen andere Teile der Welt aktiv sind, werden daher nicht berücksichtigt.

Qualität: Die Aktivitätsniveaustatistik zeigt die langfristige Entwicklung des Aufkommens an Cyberspionage- und Cybercrime-Angriffen in der westlichen Welt an. Regelmäßige Abgleiche mit summarischen Angaben anderer IT-Sicherheitsdienstleistungs-Unternehmen sowie mit Angaben von Strafverfolgungsbehörden in der westlichen Welt bestätigen, dass das Aufkommen und die Entwicklung dieser Angriffe plausibel abgebildet werden. Die Statistik kann daher repräsentative Aussagen über die Entwicklung, nicht jedoch über die absoluten Größenordnungen dieser Angriffszahlen treffen.

Botnetz-Monitoring (BOT)

Ziel: Das Botnetz-Monitoring des BSI gibt Aufschluss über das Hellfeld bekannter infizierter Systeme (hier: Bots) in Deutschland. Als infiziertes System gilt im Botnetz-Monitoring dabei jedes

IT-System, das mit einer Schadsoftware infiziert ist, die das befallene IT-System in ein Botnetz integriert und fernsteuerbar macht. Als Botnetz gilt ein Zusammenschluss mehrerer infizierter Systeme (Bots), die durch einen oder mehrere Steuerungsserver (Command-and-Control-Server, kurz C2) der Angreifer zentral ferngesteuert werden können und dessen Rechenkapazität für weitere Angriffe zur Verfügung steht. Berichtet wird über Botnetze und über Bots. Botnetze bilden eine zentrale Infrastruktur für Cyberangriffe, da Angreifer die Rechenleistung der kompromittierten Geräte bündeln und für weitere Angriffe missbrauchen. In vielen Fällen werden Botnetzstrukturen auch untervermietet und stellen somit eine niedrige Einstiegshürde für Cyberkriminelle dar, die nicht über eigenes technisches Know-how zum Aufbau und der Verwaltung eines Botnetzes verfügen. Die Infektion der Zielsysteme erfolgt meist unbemerkt. Häufig geschieht sie durch Schadprogramme, die als legitime Anwendungen getarnt sind, oder automatisiert über Netzwerke und das Internet – ohne aktives Zutun der Nutzenden. Moderne Botsoftware ist modular aufgebaut. Dadurch können Angreifer gezielt Funktionen nachladen und anpassen, sodass infizierte Systeme flexibel für unterschiedliche Zwecke eingesetzt werden können. Die schädlichen Aktivitäten richten sich entweder direkt gegen die Betroffenen, beispielsweise durch Datendiebstahl, Identitätsmissbrauch, Verschlüsselung von Daten oder Cryptomining. Alternativ werden die kompromittierten Geräte genutzt, um andere Systeme anzugreifen, etwa durch Netzwerkscans, das Ausnutzen von Schwachstellen, DDoS-Angriffe oder den Versand von Spam. Zusätzlich können weitere Schadprogramme verbreitet, geografische Sperren umgangen oder illegale Inhalte abgerufen werden. In manchen Fällen erzeugen infizierte Geräte auch automatisiert Werbeaufrufe, um unbemerkt weitere Schadmodule nachzuladen oder Werbebetrug (Ad Fraud) zu betreiben, wodurch der Urheber der Schadsoftware kontinuierlich Einnahmen generiert. Berichtszeiträume sind Tage, Monate und Jahre.

Grundgesamtheit: Grundgesamtheit des Botnetz-Monitorings sind alle in Deutschland aktiven Botnetze. Infektionen beschränken sich nicht auf klassische Computersysteme. Vielmehr können grundsätzlich alle internetfähigen Geräte mit eigenem Betriebssystem betroffen sein, wie etwa Smartphones, Tablets, Router oder IoT-Geräte (Smart-TVs, Set-Top-Boxen, Webcams oder digitale Bilderrahmen).

Stichprobe und Erhebungsdesign: Die Stichprobe der Botnetze im Monitoring umfasst eine bewusste Auswahl der im Sinkholing sichtbaren Botnetze in Deutschland anhand des Kriteriums der Größe (Anzahl infizierter Systeme) oder deren Gefährlichkeit. Innerhalb der ausgewählten Botnetze erfolgt eine Hellfeld-Erfassung der im Sinkholing sichtbaren infizierten Systeme (hier: Bots). Sinkholes sind Server, die stellvertretend für die Steuerungsserver der Angreifer die Anfragen der infizierten Systeme entgegennehmen und protokollieren. Dabei werden sowohl eigene Sinkhole-Server als auch externe Sinkholing-Datenquellen genutzt, um infizierte Systeme zu erkennen. BSI-Expertinnen und -Experten bewerten kontinuierlich die Veränderung bekannter sowie das Auftreten neuer Botnetze; neue Erkenntnisse werden unmittelbar in die Stichprobe eingepflegt, indem etwa ein neues Botnetz in das Botnetz-Monitoring aufgenommen wird.

Reichweite: Die Reichweite des Botnetz-Monitorings erstreckt sich auf die zahlenmäßig größten Botnetze in Deutschland bzw. Botnetze mit hoher Schadwirkung. Da diese Botnetze in der Regel Systeme weltweit infizieren, liegen zu den für Deutschland ausgewählten Botnetzen je nach Art und Reichweite der eigenen Sinkholing-Maßnahmen auch Daten über Infektionen weltweit vor. Eine systematische Auswahl der weltweit bedrohlichsten Botnetze erfolgt jedoch nicht. Nicht enthalten sind außerdem Systeme aus zielgerichteten Angriffen auf Einzelinstitutionen und APTs; also Systeme insbesondere finanzstarker Betroffener, die etwa durch einen Ransomware-Angriff direkt geschädigt werden, sowie Ziele von Cyberspionage. Ohne das Vorliegen eines Rückkanals in der Schadsoftware in Form eines per Domainnamen oder IP-Adresse adressierten Systems kann kein Sinkholing erfolgen.

Qualitätsbewertung: Das Botnetz-Monitoring umfasst die zahlenmäßig größten sowie kleinere, aber bedrohliche Botnetze in Deutschland, bei denen mit Sinkholing eine Sichtbarkeit und ein Schutz für Opfersysteme geschaffen werden kann. Es gibt zahlreiche bedrohliche Botnetze, bei denen ein Sinkholing aufgrund der technischen Eigenschaften nicht sinnvoll umsetzbar ist. Dabei kann nur das Hellfeld der im Sinkholing sichtbaren infizierten Systeme erfasst werden. Basierend auf Erfahrungen bei der Abschaltung von Botnetzen ist davon auszugehen, dass die tatsächliche Zahl der infizierten Systeme deutlich höher liegt. Hintergrund dürfte sein, dass ungepflegte IT-Systeme in der Regel nicht nur einzelne Schwachstellen aufweisen, sondern umfassend angreifbar sind und

daher von mehreren Schadprogrammen infiziert werden können. Im Botnetz-Monitoring ist dann nur jene Infektion sichtbar, die durch das beobachtete Botnetz verursacht wurde. Darüber hinaus dürfte eine Untererfassung infizierter Systeme aufgrund der verwendeten Erhebungsmethode vorliegen. Prominente Botnetzfamilien ergreifen beispielsweise Gegenmaßnahmen gegen das Sinkholing, wie etwa die Nutzung fester IP-Adressen, getunnelter DNS-Verbindungen (DNS over HTTPS, DoH) oder Blockchain-Techniken, um die Kommunikation zwischen Steuerungsservern und Bots zu verschleiern. Starke Zeitreihenbrüche können zudem durch sich akut ändernde Bedrohungslagen entstehen. Im Regelfall sind diese jedoch auf Veränderungen an den C2-Infrastrukturen zurückzuführen, also den Wegfall oder die Neuaufnahme von C2-Servern in das Sinkholing, oder auch technische Pannen und Ausfälle. Es kann aber auch eine neue Erkenntnislage zu einer Neuaufnahme eines Botnetzes in das Sinkholing führen. Die Zahl infizierter Systeme steigt dann unter Umständen plötzlich und sprunghaft an.

Cybersicherheitsmonitor (CYM)

Für den Cybersicherheitsmonitor werden jährlich über 3.000 Menschen ab 16 Jahre befragt, die in einem Privathaushalt in Deutschland leben und über einen Internetzugang verfügen. Beim sogenannten Computer Assisted Web Interviewing (CAWI) füllen die Teilnehmenden eine Online-Umfrage in einem Browser aus. Dafür wird eine repräsentative Stichprobe anhand der Merkmale Alter, Geschlecht, Bildung und Bundesland aus dem Bilendi/respondi Online-Access-Panel gezogen. Der Cybersicherheitsmonitor kann damit sowohl Vergleiche zwischen unterschiedlichen Gruppen wie beispielsweise Altersgruppen als auch Entwicklungen über die Zeit darstellen.

DDoS-Statistik (DOS)

Ziel: Die DDoS-Statistik quantifiziert die Gefährdung durch dezentralisierte Diensteverweigerungsangriffe (Distributed Denial of Service, DDoS) über Web-Angriffsflächen und gegen Ziele in Deutschland. Erhoben werden Cyberangriffe, die das Ziel verfolgen, IT-Systeme oder auch IT-Netzwerke durch vom Angreifer herbeigeführte Überlastungssituationen zeitweilig zu verlangsamen oder ganz vom Netz zu nehmen. Die Statistik ist eine monatliche Erhebung. Erfasst werden neben dem Aufkommen an DDoS-Angriffen auch die durchschnittlichen und die maximalen Bandbreiten, die Paketraten und die Dauer der Angriffe.

Grundgesamtheit: alle DDoS-Angriffe gegen Ziele in Deutschland

Stichprobe und Erhebungsdesign: In die Erhebung fließen alle DDoS-Angriffe im AS3320 ein. Bei AS3320 handelt es sich um das autonome System der Deutschen Telekom AG, eines der größten Systeme im deutschen Internet.

Reichweite: Die DDoS-Statistik quantifiziert die Gefährdungslage durch DDoS-Angriffe in Deutschland. Eine Aussage über die weltweite Gefährdungslage wird damit nicht ermöglicht.

Qualitätsbewertung: Die DDoS-Statistik liefert aufgrund der vollständigen Abdeckung des DDoS-Angriffsgeschehens in einem der größten autonomen Systeme Deutschlands vergleichsweise präzise Ergebnisse für die DDoS-Gefährdungslage in Deutschland. Ziele in anderen Ländern sind nur vereinzelt enthalten und haben keinen verzerrenden Effekt.

Erhebung über den E-Mail-Verkehr mit der Bundesverwaltung (EBV)

Ziel: Die Erhebung über den E-Mail-Verkehr mit der Bundesverwaltung bildet die Gefährdungslage durch Mail-Angriffsflächen und eingehenden E-Mail-Verkehr der Bundesverwaltung ab. Berichtet wird über E-Mails, Spam-Mails und Malware-Angriffe per E-Mail auf die Bundesverwaltung sowie über die aktiven E-Mail-Adressen als Angriffsfläche für Spam- und Malware-Mails (ohne Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen). Berichtszeiträume sind Tage, Monate und Jahre.

Aktive E-Mail-Adressen sind formal gültig, existieren, werden genutzt und sind aus dem Internet erreichbar. Darüber hinaus sind sie korrekt konfiguriert, sodass sie E-Mails empfangen und senden können.

Grundgesamtheit: Grundgesamtheit der Erhebung sind alle E-Mails, die von außen an E-Mail-Adressen in der Bundesverwaltung gerichtet sind.

Stichprobe und Erhebungsdesign: Es fließen alle E-Mails in die Erhebung ein, die von außen eine E-Mail-Adresse der an den Schutzmaßnahmen teilnehmenden Behörden in den Netzen des Bundes adressieren, jedoch ohne E-Mail-Adressen von Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen.

Reichweite: Die Erhebung umfasst den eingehenden E-Mail-Verkehr in den Netzen des Bundes. Erhoben werden neben allgemeinen statistischen Merkmalen wie Zeitstempeln und Größen der E-Mails auch der Spam-Status und statistische Informationen über die E-Mail-Anhänge. Die Statistik quantifiziert die Gefährdungslage der Bundesverwaltung durch Spam-E-Mails, Malware-Spam und Malware-Angriffe per E-Mail. Eine qualitative Einschätzung der Gefährdungslage zum Beispiel durch einzelne Malware-Spam-Kampagnen oder Malware-Familien wird dadurch nicht ermöglicht. Eine Einschätzung der Bedrohungslage durch Spam oder Malware-Spam ist ebenfalls nicht möglich.

Qualitätsbewertung: Die Netze des Bundes sind eines der größten zusammenhängenden Netze in Deutschland. Die Ergebnisse statistischer Erhebungen in den Netzen des Bundes können daher regelmäßig als Abbild der Lage in den deutschen Netzen insgesamt betrachtet werden. Inkonsistenzen können gleichwohl durch die sich kontinuierlich verbessernden Detektionsmethoden entstehen. Weiterhin können geringfügige Abweichungen zwischen der Summe der Tagesergebnisse sowie den Monatsergebnissen entstehen. Sie kommen aufgrund technisch bedingt unterschiedlicher Berechnungszeitpunkte des letzten Tages- und des Monatswertes zustande.

Für die Berechnung der Kennzahlen werden Tagesaggregate verwendet. Dabei handelt es sich um die von 00:00 Uhr bis 23:59 Uhr aufsummierten E-Mails. Die Tagesaggregate fließen mit spitzen Werten in die Kennzahlenberechnung ein. Bei der Aufsummierung von Anteilswerten oder Index-Punkten kann es daher zu Rundungsdifferenzen kommen.

Erhebung über die Phishing-Websites (PHW)

Ziel: Mit der Erhebung über die Phishing-Websites im Internet wird ein Teil der Infrastrukturen erhoben, die Angreifer für Cyberangriffe benutzen. Erhoben werden Webseiten, mit denen Angreifer täuschend ähnliche bekannte Webseiten erstellen, um insbesondere Zugangsdaten oder andere Informationen zu sammeln. Erhoben werden die URL, die IP und der Hostname der Phishing-Webseite sowie die Branche, die von der Phishing-Webseite nachgeahmt wird und die Sprache der Phishing-Webseite. Berichtszeiträume sind Monate.

Grundgesamtheit: Grundgesamtheit sind alle im Internet vorhandenen Phishing-Websites.

Stichprobe und Erhebungsdesign: In die Stichprobe fließen alle mutmaßlichen Phishing-Webseiten ein, die die Plattform openphish.com mittels großflächiger Analyse des weltweiten Internets detektieren konnte. Die Daten werden durch openphish.com kontinuierlich erhoben und die Stichprobenelemente teilweise sekundengenau registriert.

Reichweite: Erhoben werden Phishing-Websites weltweit. Nicht berücksichtigt werden die Angriffskampagnen, mit denen Angreifer die Links zu ihren Phishing-Webseiten verteilen.

Qualitätsbewertung: Die Erhebung über Phishing-Websites im Internet kann aufgrund des Umfangs der Stichprobe und der Qualität der Detektoren als vergleichsweise präzise betrachtet werden. Gleichwohl bleibt die Erhebung über die Phishing-Webseiten im Internet eine Hellfeldstatistik; die Größe des Dunkelfelds ist unbekannt. Unschärfen in den Zeitreihen können durch sich stetig verbessernde Detektoren sowie die automatisierte Branchenkategorisierung entstehen. Diese benötigt gewisse Merkmale auf einer Webseite, die nicht immer zwingend genau bestimmbar sind.

Erhebung über Phishing-Mails (PHR)

Ziel: Mit der Erhebung über Phishing-Mails, die deutsche Verbraucherinnen und Verbraucher erhalten, wird die Gefährdungslage von Verbraucherinnen und Verbrauchern durch maliziöse E-Mails ermittelt. Für die Statistik werden Phishing-Mails, die Verbraucherinnen und Verbraucher erreichen und die diese an das Phishing-Radar der Verbraucherzentrale Nordrhein-Westfalen melden, danach kategorisiert, welche Branche nachgeahmt wird. Dabei werden die laufenden Verbrauchermeldungen aggregiert und monatlich berichtet.

Grundgesamtheit: alle Phishing-Mails, die an den Schutzmaßnahmen der Provider vorbei die Postfächer der Verbraucherinnen und Verbraucher erreichen

Stichprobe und Erhebungsdesign: Nicht repräsentative Stichprobe mutmaßlich schädlicher E-Mails insbesondere an deutsche Verbraucherinnen und Verbraucher, die dem Phishing-Radar der Verbraucherzentrale NRW gemeldet werden. Für die Statistik werden die laufenden Verbrauchermeldungen monatlich aggregiert.

Reichweite: Die Erhebung über Phishing-Mails erstreckt sich auf maliziöse E-Mails gegen Verbraucherinnen und Verbraucher in Deutschland. Es sind keine Aussagen über Angreiferverhalten oder Angreiferaktivitäten wie etwa Phishing-Kampagnen möglich. Weiterhin unterliegen private E-Mail-Postfächer den Schutzmaßnahmen der Provider gegen Phishing-Mails. Je besser die seitens der Provider eingesetzten Detektoren, desto weniger Phishing-Mails erreichen die Verbraucherinnen und Verbraucher. Absolute Zahlen und Meldeaufkommen sind daher nicht interpretierbar. Die Erhebung erlaubt aber Aussagen über die aktuellen Phishing-Mails, die Verbraucherinnen und Verbraucher trotz aller Schutzmaßnahmen noch erreichen und daher besonders gefährlich sind.

Qualitätsbewertung: Als Meldestatistik unterliegt die Aussagekraft der Erhebung gewissen Einschränkungen. Insbesondere muss der Meldeweg den betroffenen Verbraucherinnen und Verbrauchern bekannt sein. Die Branchenkategorisierung erfolgt durch Einzelfalleinschätzung von Fachexpertinnen und -experten der Verbraucherzentrale NRW.

Exploitation-Statistik (MCF)

Ziel: Mit der Exploitation-Statistik wird der Datenverkehr erhoben, mit dem Angreifer IP-Adressen massenhaft und ungezielt aufrufen, um Angriffe auf IT-Systeme unter Ausnutzung (Exploitation) von Schwachstellen durchzuführen, um dort beispielsweise Daten zu verschlüsseln oder auszuleiten. Berichtet wird über ausgeführte Exploitation-Angriffe. Berichtszeiträume sind Monate.

Grundgesamtheit: Grundgesamtheit der Exploitation-Statistik ist der Datenverkehr im Internet, den Angreifer zum Zwecke der Durchführung von Exploitation-Angriffen erzeugen.

Stichprobe und Erhebungsdesign: Die Stichprobe der Exploitation-Statistik wird mittels einer Honeypot-ähnlichen Cyber-Threat-Detection-Suite mit geringer Interaktion erhoben.

Reichweite: Die Exploitation-Statistik bildet den Datenverkehr im Internet ab, der IP-Adressen flächendeckend aufruft. Da es sich bei dem Honeypot-System um einzelne Sensoren handelt, können die Ergebnisse zur Einschätzung von Trends, nicht jedoch zur Extrapolation auf Datenvolumina bestimmter Organisationen, Länder, Regionen oder Institutionen verwendet werden.

Qualitätsbewertung: Es fließt sämtlicher Datenverkehr in die Statistik ein, der bei den IP-Adressen des Sensorsystems eingeht. Auch wenn es sich bei den beobachteten Verkehrsdaten mit hoher Wahrscheinlichkeit um Angriffsdatenverkehr handelt, kann dies nicht immer zweifelsfrei festgestellt werden. Beispielsweise können Portscans auch von IT-Sicherheitsfirmen oder IT-Sicherheitsforschenden durchgeführt werden, die sich wie Angreifer verhalten, um Systeme zu testen oder Schwachstellen zu finden. Das Ausmaß der hierdurch gegebenenfalls verursachten Verzerrungen ist unbekannt, dürfte sich jedoch nicht nennenswert auf die statistischen Trends

auswirken, da sie gleichbleibend in der Erhebung berücksichtigt sind und die Erhebungsbedingungen somit konstant bleiben.

KRITIS-Meldungen (KRM)

Ziel: Mit den KRITIS-Meldungen wird die Gefährdungslage der Kritischen Infrastrukturen (KRITIS) in Deutschland gemäß § 8b Absatz 4 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) sowie der Energienetzbetreiber gemäß dem Gesetz über die Elektrizitäts- und Gasversorgung (EnWG) erhoben. Die KRITIS-Meldungen umfassen meldepflichtige Störungen der IT-Sicherheit bei KRITIS-Betreibern. Erhoben werden die Störungsursachen sowie die betroffenen Sektoren, Branchen und Anlagen.

Betreiber Kritischer Infrastrukturen haben folgende Störungen unverzüglich über die Kontaktstelle an das Bundesamt zu melden (Text steht im EnWG analog):

1. Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben,

2. erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können.

Berichtet wird quartalsweise und jährlich.

Grundgesamtheit: Grundgesamtheit sind alle bei KRITIS-Betreibern (gemäß KRITIS-Verordnung) und Energienetzbetreibern gemäß EnWG aufgetretenen Störungen, die zu einem Ausfall der kritischen Dienstleistung geführt haben oder hätten führen können.

Stichprobe und Erhebungsdesign: Auskunftspflichtig sind die Betreiber Kritischer Infrastrukturen in den Sektoren Wasser, Energie, Transport, Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, Ernährung und Siedlungsabfallentsorgung. Einige Betreiber im Finanz- und Versicherungswesen melden nicht direkt an das BSI; ihre Meldungen werden nachrichtlich berücksichtigt. Meldepflichtig sind alle Störungen, die zu einem Ausfall der kritischen Dienstleistung geführt haben oder hätten führen können.

In die Stichprobe fließen alle von KRITIS-Betreibern an das BSI oder andere Behörden übermittelten Meldungen zu aufgetretenen Störungen ein. Es handelt sich um eine Hellfeldstatistik, da es durch gegebenenfalls nicht gemeldete Störungen eine unbekannte Dunkelziffer gibt.

Reichweite: In den Meldungen teilen KRITIS-Betreiber in Deutschland die aufgetretenen Störungen mit. Störungsursachen erstrecken sich nicht nur auf Cyberangriffe, sondern können ein physischer Schaden, technisches Versagen, Fehlhandlung von Mitarbeitenden, Fehlhandlung von Dritten, Versagen der genutzten Infrastruktur, ein physischer Angriff oder verschiedene Arten informationstechnischer Angriffe (Ausnutzung einer Schwachstelle, Hacking und Manipulation, Schadprogramme (Malware), APT-Angriffe, Missbrauch (Innenangriff), Identitätsmissbrauch, Verhinderung von Diensten) sein.

Qualitätsbewertung: Die Datenqualität der im BSI eingehenden Meldungen ist unterschiedlich, da erstens die erhobenen Angaben den KRITIS-Betreibern nicht bei allen Vorfällen bekannt sind und zweitens die KRITIS-Betreiber die zu erteilenden Auskünfte teilweise falsch verstehen und somit gegebenenfalls fehlerhaft ausfüllen. Dies trifft insbesondere bei Freitextfeldern zu. Der KRITIS-Fachbereich plausibilisiert Meldungen im Nachgang und ergänzt fehlende Angaben. Gleichwohl sind im Einzelfall Abweichungen möglich. Darüber hinaus ist von einer unbekannten Dunkelziffer gegebenenfalls nicht gemeldeter Störungen auszugehen.

KRITIS-Nachweise (KRN)

Ziel: Die Statistik stellt die Ergebnisse der unabhängigen Prüfungen von KRITIS-Betreibern nach § 39 Absatz 3 BSIG und somit die Resilienz der Kritischen Infrastrukturen in Deutschland dar. Mit diesen Prüfungen müssen nachweispflichtige KRITIS-Bereiter im zweijährigen Turnus die Reifegrade ihrer Präventions-, Verteidigungs- und Bewältigungssysteme durch unabhängige Prüfer bewerten lassen. Berichtet wird über die Sektoren, die Reifegrade der Informationssicherheitsmanagmentsysteme (ISMS), der Systeme zur Angriffserkennung (SzA) sowie der Business-Continuity-Management-Systeme (BCMS).

Berichtszeiträume sind Quartale.

Grundgesamtheit: alle nachweispflichtigen deutschen KRITIS-Betreiber gemäß KRITIS-Verordnung

Stichprobe und Erhebungsdesign: In die Vollerhebung fließen rund 730 dem BSI gegenüber nachweispflichtige KRITIS-Betreiber in Deutschland ein. Nicht alle KRITIS-Betreiber sind dem BSI gegenüber nachweispflichtig. Einige energiewirtschaftliche Betreiber sind gemäß § 11 Absatz 1f EnWG nachweispflichtig. Diese Nachweise enthalten Umsetzungsgrade der Systeme zur Angriffserkennung, aber keine ISMS/BCMS-Reifegrade. Schließlich müssen kürzlich registrierte Betreiber, zum Beispiel im Sektor Siedlungsabfallentsorgung, erst zwei Jahre nach der Registrierung einen Nachweis einreichen.

Die Prüfungen nehmen externe, dafür geschulte Prüfende vor, die von den KRITIS-Betreibern beauftragt werden. Die Nachweise werden gemäß den Richtlinien des BSI erhoben und quartalsweise stichtagsbezogen ausgewertet.

Reichweite: Die Meldestatistik über die KRTIS-Nachweise erstreckt sich auf die dem BSI gegenüber nachweispflichtigen KRITIS-Betreiber. Aussagen über andere KRITIS-Betreiber sind nicht möglich.

Qualitätsbewertung: Da die Nachweise von geschulten Prüfenden erhoben werden, können diese als vergleichsweise gut betrachtet werden. Der KRITIS-Fachbereich arbeitet kontinuierlich daran, dass die Nachweise die notwendigen hohen Standards erfüllen.

Leak-Geschädigten-Statistik (LKS)

Ziel: Die Leak-Geschädigten-Statistik quantifiziert einen Teil der Schadwirkungen, die Ransomware-Angriffe in Verbindung mit Datenleaks oder Exploitation-Angriffe in Verbindung mit Datenleaks haben. So erbeuten Angreifer Daten bei Geschädigten. Anschließend drohen sie, die erbeuteten Daten auf sogenannten Leak-Seiten zu veröffentlichen, wenn die geschädigte Institution das geforderte Lösegeld nicht zahlt.

Die verschiedenen cyberkriminellen Angreifergruppen richten in der Regel spezifische Leak-Seiten für die Veröffentlichung der Daten derjenigen Geschädigten ein, die kein Lösegeld gezahlt haben. Die Daten können von anderen Cyberkriminellen dort heruntergeladen oder vereinzelt gekauft und für weitere Angriffe missbraucht werden.

Die Leak-Geschädigten-Statistik zählt die Nennungen neuer Geschädigter von Datenleaks auf diesen Leak-Seiten. Berichtet wird nicht über Angriffe, sondern über die Zahl der von den Angreifern auf den von ihnen betriebenen Leak-Seiten genannten Geschädigten, die hierdurch erpresst werden.

Berichtet wird darüber hinaus über die Leak-Seiten und die Aktivität der jeweiligen Angreifergruppen, die die Seiten betreiben. Berichtszeitraum sind Quartale.

Grundgesamtheit: Grundgesamtheit der Leak-Geschädigten-Statistik sind alle geschädigten Unternehmen, Behörden und sonstigen Institutionen von Datenleaks, die aus Cybercrime-Angriffen stammen und die von Angreifern auf dedizierten Leak-Seiten genannt wurden. Leaks, die von Angreifern untereinander abseits von Leak-Seiten gehandelt werden oder auf Untergrundforen und -marktplätzen verteilt werden, sind von dieser Statistik nicht erfasst.

Stichprobe und Erhebungsdesign: In die Erhebung fließen alle neuen Geschädigten ein, die dem BSI aus Detektionen von Datendienstleistern, aus Meldungen von Opfern oder aus öffentlichen Quellen

bekannt geworden sind. Die Leak-Geschädigten-Statistik ist eine Vollerhebung über die bekannt gewordenen Leak-Geschädigten. Die Leak-Geschädigten-Statistik wird quartalsweise erhoben. Gezählt werden alle neuen Geschädigten zu dem Zeitpunkt, zu dem sie durch Nennung auf den Leak-Seiten der Angreifer bekannt werden. Es sind daher keine Doubletten aus früheren Quartalen in einem Berichtszeitraum enthalten.

Reichweite: Die Leak-Geschädigten-Statistik erlaubt keine Aussagen über Ransomware-Angriffe oder Angriffe gegen neue Schwachstellen. Gezählt werden nicht die Angriffe, sondern die Geschädigten. Wenn ein Angriff mehrere Geschädigte betrifft (z. B. infolge eines Angriffs auf einen IT-Dienstleister, der die Erpressung verschiedener weiterer Geschädigter zur Folge hatte), werden alle Geschädigten gezählt, sofern diese auf Leak-Seiten genannt werden. Die Statistik bildet die Menge (mutmaßlich) zahlungsunwilliger Geschädigter weltweit ab, die auf Leak-Seiten genannt wurden. Geschädigte, die gezahlt haben oder aus anderen Gründen nicht genannt wurden, werden nicht berücksichtigt. Als Leak-Geschädigte werden auch solche Geschädigte gezählt, bei denen keine Ransomware zum Einsatz kam, sondern deren Daten nach einem Exploitation-Angriff direkt exfiltriert wurden.

Qualitätsbewertung: Aufgrund der hohen weltweiten Abdeckung durch die Datendienstleister kann die Leak-Geschädigten-Statistik als vergleichsweise genau betrachtet werden. Dies zeigt sich auch an dem erwartungsgemäß hohen Anteil an Doubletten (> 50 %) zwischen den verschiedenen Datenquellen. Doubletten werden bereinigt. Doppelzählungen finden nicht statt. Die Leak-Geschädigten-Statistik ist gleichwohl als Hellfeldstatistik zu betrachten. Erpressungsopfer, die auf Untergrundforen genannt werden, sind nicht enthalten. Es können jedoch Einzelfälle enthalten sein, bei denen Angreifer lediglich behaupteten, einen Angriff durchgeführt zu haben, und eine Erpressung versuchten, ohne dass es tatsächlich zu einem Datenabfluss gekommen wäre.

Leak-Statistik (DLK)

Ziel: Mit der Leak-Statistik erhebt das BSI öffentlich bekannt gewordene Datenleaks mit Verbraucherbetroffenheit.

Grundgesamtheit: alle öffentlich bekannt gewordenen Datenleaks mit Verbraucherbetroffenheit

Stichprobe und Erhebungsdesign: Für die Leak-Statistik wird eine nach betroffenen Branchen stratifizierte Auswahl öffentlich bekannt gewordener Datenleaks mittels kontinuierlichem, automatisiertem Webscraping erhoben.

Qualität: Die Leak-Statistik ist eine Hellfeldstatistik. Die automatisierte Branchenkategorisierung benötigt gewisse Merkmale auf einer bbetroffenen Website, die nicht immer genau bestimmbar sind, wodurch sich eine unbestimmbare Dunkelziffer ergibt.

Malware-Statistik (MWS)

Ziel: Die Malware-Statistik stellt den Stand und die Entwicklung des neu bekannt gewordenen Malware-Aufkommens im Internet dar. Darüber hinaus werden neue Varianten potenziell unerwünschter Anwendungssoftware (PUA) erhoben. Berichtet wird nicht über Angriffe mit Malware, sondern über das bekannt gewordene Malware-Aufkommen insgesamt. Berichtszeiträume sind Monate und Quartale.

Grundgesamtheit: Grundgesamtheit der Malware-Statistik sind alle im Internet verfügbaren Programme, die schädliche Operationen durchführen können, einschließlich solcher Programme, die andere Programme befähigen, schädliche Operationen durchzuführen (z. B. Nachlade-Software). Nicht enthalten sind URLs, über die solche Programme heruntergeladen werden, enthalten sind die herunterzuladenden Programme. Als Variante einer Malware gilt jede auch nur geringfügig veränderte Kopie dieser Malware. Im Gegensatz zu neuer Malware besitzen neue Varianten von bereits bekannter Malware keine neuen Funktionalitäten. Varianten sind aber im Hinblick auf den resultierenden Hashwert einzigartig.

Stichprobe und Erhebungsdesign: Die Malware-Statistik umfasst Programme, die schädliche Operationen ausführen können oder andere Programme dazu befähigen, dies zu tun. Erhoben werden unter anderem die Art der Malware sowie die Plattform und das Format. Darüber hinaus werden neue Varianten potenziell unerwünschter Anwendungssoftware (PUA) erhoben. Da jede neue Malware-Variante eine Bedrohung in dem Sinne darstellt, dass sie für Angriffe verwendet werden kann, quantifiziert die Statistik die Bedrohungslage durch neue Malware.

Reichweite: Die Malware-Statistik umfasst Programme, die schädliche Operationen ausführen können oder andere Programme dazu befähigen, dies zu tun. Erhoben werden unter anderem die Art der Malware sowie die Plattform und das Format. Darüber hinaus werden neue PUA-Varianten erhoben. Da jede neue Malware-Variante eine Bedrohung in dem Sinne darstellt, dass sie für Angriffe verwendet werden kann, quantifiziert die Statistik die Bedrohungslage durch neue Malware. Die errechneten Indikatoren sind Frühwarnindikatoren für Cyberangriffe, da mehr neue Malware-Varianten auch mehr Angriffe mit diesen neuen Varianten nach sich ziehen werden. Die Wahrscheinlichkeit von Malware-Angriffen steigt also mit der Menge neuer Malware-Varianten, wobei aber zwischen dem Auftreten neuer Varianten und Angriffen kein zeitlicher Zusammenhang bestehen muss. Umgekehrt bedeutet ein Rückgang der Indikatoren nicht immer eine Entspannung der Bedrohungslage, da die Produktion neuer Varianten auch deshalb zurückgegangen sein kann, weil die Angreifer mit den bestehenden Varianten ihre Ziele erfolgreich erreichen und die Produktion neuer Varianten insofern nicht erforderlich ist. Eine qualitative Einschätzung der Bedrohung im Sinne einer Gewichtung nach Verbreitungsgrad oder Schadenspotenzial einer Malware wird durch die Malware-Statistik nicht ermöglicht. Aussagen über Angriffe mit Malware sind ebenfalls nicht möglich.

Qualitätsbewertung: Die Ergebnisse der Malware-Statistik können aufgrund des Umfangs und des Aktualisierungskonzepts der zugrunde liegenden Datenbanken als vergleichsweise genau betrachtet werden. Da keine Erkenntnisse über das Dunkelfeld der unbekannten Malware vorliegen, gilt dies allerdings nur für das tatsächlich in der Statistik erfasste Hellfeld der neu bekannt gewordenen Malware. Inkonsistenzen können durch die sich kontinuierlich verbessernden Methoden der Malware-Detektion, insbesondere der Viren-Scanner, entstehen. Diese werden durch standardisierte Revisionen zwar größtenteils aufgefangen. Da die Revisionszyklen jedoch maximal eineinhalb Quartale umfassen, ist davon auszugehen, dass ältere Berichtszeiträume das tatsächliche Malware-Aufkommen tendenziell etwas unterschätzen. Zum März 2023 wurde die Malware-Statistik umfangreich revidiert. Änderungen am Datenbestand, die durch verbesserte Detektionsmethoden bedingt waren, sind rückwirkend berücksichtigt. Ausgewiesene Häufigkeiten für Zeiträume vor März 2023 können sich daher von früheren Berichten über diese Zeiträume unterscheiden.

Portscan-Statistik (MCS)

Ziel: Mit der Portscan-Statistik wird die Bedrohungslage durch Datenverkehr von Angreifern im Internet erhoben. Erfasst wird der Datenverkehr, mit dem Angreifer IP-Adressen massenhaft und ungezielt aufrufen, um Schwachstellen zu finden und Angriffe vorzubereiten. Sogenannte Portscans ermöglichen Angreifern Aufklärung darüber, welche Dienste in einem Netzwerk wie dem Internet angeboten werden und auf dem Zielsystem zur Verfügung stehen. Berichtet wird daher über Portscans zur Angriffsvorbereitung. Berichtszeiträume sind Monate.

Grundgesamtheit: Grundgesamtheit der Portscan-Statistik ist der Datenverkehr im Internet, den Angreifer durch Portscans erzeugen.

Stichprobe und Erhebungsdesign: Die Stichprobe der Portscan-Statistik wird mittels einer Honeypot-ähnlichen Cyber-Threat-Detection-Suite mit geringer Interaktion erhoben.

Reichweite: Die Portscan-Statistik bildet den Datenverkehr im Internet ab, der IP-Adressen flächendeckend aufruft – wie etwa durch Scandienste oder Systeme, die der Vorbereitung von Angriffen dienen. Da es sich bei dem Honeypot-System um einzelne Sensoren handelt, können die Ergebnisse zur Einschätzung von Trends, nicht jedoch zur Extrapolation auf Datenvolumina bestimmter Organisationen, Länder, Regionen oder Institutionen verwendet werden.

Qualitätsbewertung: Es fließt sämtlicher Datenverkehr in die Statistik ein, der bei den IP-Adressen des Sensorsystems eingeht. Auch wenn es sich bei den beobachteten Verkehrsdaten mit hoher Wahrscheinlichkeit um Angreiferaktivitäten handelt, kann dies nicht immer zweifelsfrei festgestellt werden. Beispielsweise können Portscans auch von IT-Sicherheitsfirmen oder IT-Sicherheitsforschenden durchgeführt werden, die sich wie Angreifer verhalten, um Systeme zu testen oder Schwachstellen zu finden. Das Ausmaß der hierdurch gegebenenfalls verursachten Verzerrungen ist unbekannt, dürfte sich jedoch nicht nennenswert auf die statistischen Trends auswirken, da sie gleichbleibend in der Erhebung berücksichtigt sind und die Erhebungsbedingungen somit konstant bleiben.

Schwachstellenstatistik (SSS)

Ziel: Die Schwachstellenstatistik stellt den Stand und die Entwicklung der neu bekannt gewordenen Schwachstellen in IT-Produkten dar. Sie ermöglicht damit Aussagen über die bekannte, verwundbare Angriffsfläche der weltweiten IT-Landschaft für Cyberangriffe. Schwachstellen, die zum Zeitpunkt ihrer ersten Ausnutzung Herstellern und Anwendern noch unbekannt waren (Zero Days), sind nicht enthalten. Neben der Art und Menge der neu bekannt gewordenen Schwachstellen wird deren Schweregrad nach dem CVSS Basescore 3.1 erhoben. Die Auswertung umfasst die Identifikation von Schwachstellen in Systemen der Künstlichen Intelligenz (KI). Berichtszeiträume sind Jahre und Quartale.

Grundgesamtheit: Grundgesamtheit sind alle Schwachstellen in IT-Produkten, die im Berichtszeitraum neu bekannt geworden sind.

Stichprobe und Erhebungsdesign: Die Schwachstellenstatistik ist eine Erhebung auf Grundlage der US-amerikanischen National Vulnerability Database (NVD), des CVE-Program (CVE® Record Information, cvelistV5) der MITRE Corporation (MITRE) sowie der European Vulnerability Database (EUVD) der Agentur der Europäischen Union für Cybersicherheit (ENISA). Schwachstellen, die von der NVD oder der offiziellen CVE-Liste der MITRE aufgrund zu geringer Verbreitung des betroffenen Systems zurückgewiesen wurden, fließen nicht mit in die Statistik ein. Außerdem werden keine Schwachstellen ohne Veröffentlichungsdatum und keine Schwachstellen, die nicht in der NVD eingetragen sind, berücksichtigt. Im Februar 2025 wurde die Statistik einer umfassenden Revision unterzogen. Seitdem werden auch Schwachstellen ohne Bewertung berücksichtigt.

Die Schwachstellenstatistik ist eine Quartalsstatistik, die Erhebung findet jeweils zur Mitte des Folgequartals statt. Später bekannt werdende Schwachstellen werden bei Revisionen berücksichtigt.

Reichweite: Die Schwachstellenstatistik ist eine Meldestatistik auf Basis der Schwachstellen, die weltweit an die NVD gemeldet werden. Nicht enthalten sind Zero-Day-Schwachstellen, die zum Zeitpunkt der ersten Ausnutzung noch unbekannt waren. Weiterhin werden lediglich die neu bekannt gewordenen Schwachstellen erfasst. Aussagen über deren tatsächliche Ausnutzung für Cyberangriffe werden damit nicht ermöglicht. Darüber hinaus sind zwar die IT-Produkte bekannt, in denen die Schwachstellen aufgetreten sind. Informationen über deren Verbreitung in der weltweiten IT-Landschaft liegen jedoch nicht vor. KI-spezifische Angriffsvektoren wie Data Poisoning oder Evasion werden von den Primärquellen nicht systematisch erfasst – die tatsächliche KI-spezifische Angriffsfläche wird daher strukturell unterschätzt.

Schwächen (engl. weaknesses) in einzelnen IT-Produkten sind Zustände in einer Software-, Firmware-, Hardware- oder Dienstkomponente, die unter bestimmten Umständen zur Erzeugung von Schwachstellen beitragen können. Schwächen werden in vielen Fällen von Entwicklerinnen und Entwicklern während der Produktentwicklung generiert. Obwohl Entwickler sehr unterschiedliche Programmierpraktiken anwenden, können sie alle die gleichen Arten von Schwächen erzeugen, die zu Schwachstellen in ihren eigenen Produkten führen. Die CWE-Liste der MITRE sowie die zugehörigen Taxonomien und Klassifizierungsschemata dienen als Sprache zur Identifizierung und Beschreibung dieser Schwächen in Form von CWE-IDs. Die Schwachstellenstatistik ermöglicht daher Aussagen über die zugrunde liegenden Schwächen, die zu der bekannten Angriffsfläche für Cyberangriffe geführt haben.

Qualitätsbewertung: Aufgrund des Umfangs der zugrunde liegenden Rohdatensammlung (NVD) dürfte die Schwachstellenstatistik die bestmögliche Quantifizierung der bekannten, verwundbaren

Angriffsfläche der weltweiten IT-Landschaft darstellen. Die Schwachstellenstatistik ist eine Stichtagserhebung. Insoweit wird der Informationsstand zum Stichtag abgebildet. Später in der NVD eingehende Informationen werden bei Revisionen berücksichtigt. Für die Auswertung von Schwachstellen mit KI-Bezug ist zu berücksichtigen, dass die maschinelle Klassifikation in Einzelfällen fehlerhaft sein kann. Zudem beeinflussen Disclosure-Praktiken und Veröffentlichungswellen einzelner Hersteller die absolute Zahl der Schwachstellen.

Die Schwachstellenstatistik wird in unregelmäßigen Abständen revidiert – etwa dann, wenn sich die Meldepraxis der weltweiten IT-Sicherheitscommunity statistisch relevant verändert hat. Dies war beispielsweise im Jahr 2024 der Fall, als durch veränderte Melde-Policies der Linux-Kernelentwickler Brüche in den Zeitreihen auftraten. Die Statistik wurde daher Mitte Februar 2025, das heißt erstmals für den Berichtszeitraum 4. Quartal 2024, umfangreich revidiert. Vergleiche mit früher publizierten Berichten sind daher nur eingeschränkt möglich.

CVE® ist eine eingetragene Marke der MITRE Corporation; CVE-Inhalte werden gemäß dem CVE Program Terms of Use genutzt.

Threat-Actors-Statistik (TAS)

Ziel: Die Threat-Actors-Statistik erhebt die bei westlichen Cybersicherheitsexpertinnen und -experten bekannten Strukturinformationen über die Bedrohungslage durch Cyberangreifer. Berichtet wird über APT-, Cybercrime- und Hacktivisten-Gruppen. Die Statistik gibt etwa Merkmale wie die Herkunfts-, die Zielländer, die Zielsektoren sowie die verwendete Malware wieder. Berichtet wird halbjährlich.

Grundgesamtheit: Grundgesamtheit sind alle für die westliche Welt relevanten Angreifergruppen.

Stichprobe und Erhebungsdesign: Die Threat-Actors-Statistik ist eine halbjährliche Stichtagserhebung bei den Cybersicherheitsexpertinnen und -experten des IT-Sicherheitsdienstleisters CrowdStrike. Datengrundlage ist die Sensorik von CrowdStrike/Falcon, die durch die Expertinnen und Experten in aufwendigen Analysen mit qualitativen Informationen angereichert wird. Die Threat-Actors-Statistik ist eine Stichtagserhebung, die den Informationsstand zum 30. Juni sowie zum 31. Dezember abbildet.

Reichweite: Mit der Threat-Actors-Statistik werden Strukturinformationen über die Bedrohungslage durch Angreifergruppen für die westliche Welt erfasst. Aussagen über tatsächliche Angriffe sind damit nicht möglich. Zudem werden prioritär Angreifergruppen beobachtet, die für die westliche Welt relevant sind. Angreifergruppen, die ausschließlich andere Teile der Welt bedrohen, werden nicht berücksichtigt.

Qualitätsbewertung: Die mit der Threat-Actors-Statistik erhobenen Strukturinformationen bilden stichtagsbezogen den quantifizierbaren Informationsstand westlicher Cybersicherheitsexpertinnen und -experten über die Bedrohung der westlichen Welt durch Angreifergruppen ab. Aussagen über die weltweite Bedrohungslage sind damit nicht möglich. Qualitative Aussagen über die Gefährdungslage durch Cybercrime, -spionage und -sabotage, die etwa das Ausmaß aktueller Aktivität berücksichtigen würden, sind ebenfalls nicht möglich.

Web-Angriffsflächenmessung (WAM)

Ziel: Die Web-Angriffsflächenmessung quantifiziert die Angriffsfläche Deutschlands für Cyberangriffe im Internet. Erhoben werden stichtagsbezogen die erreichbaren .de-Domains sowie die hierzu im Web verfügbaren. Informationen wie beispielsweise zugehörige IP-Adressen, Hosts, Exponiertheit sowie die Verfügbarkeit sensibler Metadaten, die das Auffinden von Schwachstellen ermöglichen. Ein Anstieg der infrastrukturbezogenen Indikatoren bedeutet dabei ein Wachstum der Angriffsfläche einfach nur aufgrund der Tatsache, dass immer mehr Dienste im Netz bereitgestellt werden. Eine Änderung der risikobezogenen Indikatoren misst dagegen, inwiefern technische Standards im Sinne grundlegender Prinzipien der Cybersicherheit auch erfüllt werden.

Grundgesamtheit: Alle bekannten in Deutschland gemeldeten Second-Level-.de-Domains im Internet mit dem Aufbau „domainname“ + „.de“, wie zum Beispiel „bundesregierung.de“.

Stichprobe und Erhebungsdesign: Im 1. Quartal 2026 befinden sich rund 80 % aller 17,86 Millionen bei der DENIC registrierten .de-Domains in der Stichprobe. Die Stichprobe ist seit ihrer Ersterhebung im 2. Quartal 2025 von 13,2 Millionen auf bis zu 14,04 Millionen Domains gewachsen. Ziel ist eine Vollerhebung. Jede Domain gehört zu einer Organisationseinheit im Netz, einem sogenannten Netzwerkblock, der mit einer Nummer versehen ist (ASN-Nummer). Für die Erhebung werden sowohl frei verfügbare als auch die Daten verschiedener Dienstleister zur Domainerkundung eingesetzt; die Anreicherung der Domains mit Metadaten erfolgt ebenfalls durch den Abruf frei verfügbarer Dienste sowie einschlägiger Datenanbieter von zum Beispiel Geoinformationen – diese geben für einen Netzwerkblock einen ungefähren Aufschluss darüber, wo die IP-Adresse, zu der die Domain gehört, tatsächlich geografisch liegt –, Informationen zu Hostern und Internet-Metadaten. Die für die Web-Angriffsfläche erfassten Informationen sind – abgesehen von der Domainerkundung – für einzelne Domains und IP-Adressen frei, in der Fläche jedoch nicht frei verfügbar.

Das Stichprobendesign setzt sich zusammen aus der kontinuierlichen Domainerkundung, das heißt, es werden fortlaufend bekannte Domains gesammelt. Diese werden regelmäßig auf ihre Erreichbarkeit hin überprüft und entsprechend angereichert. Die Aggregation der Daten erfolgt auf Quartalsebene, das heißt, es werden alle Domains, die im entsprechenden Quartal erreichbar waren, dargestellt.

Reichweite: Die Web-Angriffsflächenmessung umfasst öffentliche, aber flächendeckend nicht frei zugängliche Informationen. Durch die Erfassung des überwiegenden Anteils existierender .de-Domains und die Möglichkeit, gegen die Gesamtmenge der .de-Domains abzugleichen, wird ein großer Teil der Web-Angriffsfläche Deutschlands erfasst. Nicht enthalten sind Domains und IPs, die einer anderslautenden Endung als .de zugewiesen sind, wie zum Beispiel .com oder .org.

Qualitätsbewertung: Aufgrund des Umfangs der Stichprobe erlaubt die Web-Angriffsflächenmessung hochpräzise Aussagen über die .de-Domains im Internet.

Abkürzungsverzeichnis

5G/6G: 5./6. Generation (Mobilfunk)

AMD: Advanced Micro Devices, Inc. (Incorporated)

AMF: Access and Mobility Management Function

API: Application Programming Interface

APT: Advanced Persistent Threat

AS(N): Autonomes System (Nummer)

AWS: Amazon Web Service

BCMS: Business-Continuity-Management-System

BfDI: Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

BITS: BSI-IT-Sicherheitsmitteilung

BNetzA: Bundesnetzagentur

BSI: Bundesamt für Sicherheit in der Informationstechnik

BSIG: BSI-Gesetz

BYOVD: Bring Your Own Vulnerable Driver

C2-Server: Command-and-Control-Server

CC: Common Criteria for Information Technology Security Evaluation

CERT: Computer Emergency Response Team

CISA: Cybersecurity and Infrastructure Security Agency

CSW: Cyber-Sicherheitswarnung

CVD: Coordinated Vulnerability Disclosure

CVE: Common Vulnerabilities and Exposures

CWE: Common Weakness Enumeration

CyMon: Cybersicherheitsmonitor

DDoS: Distributed Denial of Service

DIN: Deutsches Institut für Normung

DIN SPEC: DIN Specification (Standard, Vorstufe zu DIN-Norm)

DSGVO: Datenschutz-Grundverordnung

ECDSA: Elliptic Curve Digital Signature Algorithm

EDR: Endpoint Detection and Response

EEG: Erneuerbare-Energien-Gesetz

EU: Europäische Union

FBI: Federal Bureau of Investigation

FIDO: Fast IDentity Online

GPT: Generative Pre-trained Transformer

GUS: Gemeinschaft Unabhängiger Staaten

HMI: Human-Machine-Interface

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

ICS: Industrial Control System

IDOR: Insecure Direct Object Reference

IEC: International Electrotechnical Commission

IFG: Informationsfreiheitsgesetz

IoT: Internet of Things

IP: Internetprotokoll

ISMS: Informationssicherheitsmanagementsystem

ISO: International Organization for Standardization

ISP: Internetdienstanbieter

IT: Information Technology

KI: Künstliche Intelligenz

KMU: kleine und mittlere Unternehmen

KRITIS: Kritische Infrastrukturen

LLM: Large Language Model

MaaS: Malware-as-a-Service

MADCAT: Mass Attack Detection Connection Acceptance Tools

MD5: Message-Digest Algorithm 5
MFA: Multi-Faktor-Authentifizierung
MIFARE: Mikron Fare Collection System
MSC: Münchner Sicherheitskonferenz
NATO: North Atlantic Treaty Organization
NIS: Network and Information Security
NRW: Nordrhein-Westfalen
PV: Photovoltaik
RaaS: Ransomware-as-a-Service
RADIUS: Remote Authentication Dial-In User Service
RAN: Radio Access Network
RDP: Remote Desktop Protocol
SA: Service and System Aspects
SCAS: Security Assurance Specifications
SDA: Social Design Agency
SEV: Secure Encrypted Virtualization
SNP: Secure Nested Paging
SQL: Structured Query Language
SSH: Secure Shell (Netzwerkprotokoll)
SSL: Secure Sockets Layer
SzA: Systeme zur Angriffserkennung
TDX: Trust Domain Extensions
TK: Telekommunikation
TLS: Transport Layer Security
TPM: Trusted Platform Module
TR: Technische Richtlinie
TS: Technical Specification
UIG: Umweltinformationsgesetz
URL: Uniform Resource Locator
USB: Universal Serial Bus
VNC: Virtual Network Computing
VPN: Virtual Private Network
WID: Warn- und Informationsdienst
ZenDiS: Zentrum für Digitale Souveränität der Öffentlichen Verwaltung

Glossar

Access Broker:	Cyberkriminelle, die sich Zugang zu einem Opfernetzwerk verschaffen und diesen Zugang an andere Kriminelle oder Parteien veräußern.
(KI)-Alignment-Verfahren:	Training und Ausrichtung von KI-Modellen an menschlichen Werten und Zielen, um sie so nützlich, sicher und zuverlässig wie möglich zu machen.
Ad Fraud:	Werbebetrug
AdCO CRA:	Administrative Cooperation Group Cyber Resilience Act. Entwickelt gemeinsame Methoden zur Umsetzung der Anforderungen des CRA und koordiniert Marktüberwachungsmaßnahmen.
Advanced Persistent Threats (APT):	Zielgerichtete Cyberangriffe: Angreifer verschaffen sich persistenten Zugriff auf Netzwerke und weiten ihn aus. Diese Angriffe sind oft schwer zu detektieren.
Affiliates:	Im Cybercrime-as-a-Service (CCaaS) ist der Affiliate der Kriminelle, der einen Service (z. B. Ransomware) nutzt und am Ertrag (z. B. Lösegeld) beteiligt wird.
Agenten, KI-Agenten:	LLM-Agenten wandeln generierte Antworten in aktive Aktionen (z. B. Funktionsaufrufe) um, und handeln nach einer nicht explizit vordefinierten, schwer überprüfbaren Logik.
Agenten, Software-Agenten:	Softwarekomponenten, die autonom Informationen anhand fester Regeln verarbeiten und daraus abgeleitete Aktionen ohne manuelles Zutun ausführen.
Agentische KI:	Künstliche Intelligenz mit Befähigung für eigenständiges Handeln und Entscheiden (z. B. mit Schreibrechten auf einem Dateisystem, Rechten zum Ausführen von Programmen etc.).
Angriffserkennung (SzA):	Systeme zur Angriffserkennung sind nach der Definition aus § 2 Absatz 9b Satz 1 BSIG-Prozesse, die

	durchtechnische Werkzeuge und organisatorische Einbindung unterstützt werden.
Angriffsfläche:	IT-Systeme, Komponenten und Dienste, die ein Angreifer für einen Cyberangriff ausnutzen oder missbrauchen kann.
Angriffsvektor:	Als Angriffsvektor wird die Kombination von Angriffsweg und -technik bezeichnet, mit der sich ein Angreifer Zugang zu IT-Systemen verschafft.
Apache HTTP Server:	Weit verbreiteter, quelloffener Webserver der Apache Software Foundation.
Attack Score:	Normierte Kennzahl über die Gefährdungslage in Deutschland.
Attack Surface Check:	Ein Attack Surface Check ist ein systematischer Prozess zur Identifizierung und Bewertung potenzieller Schwachstellen in einer IT-Umgebung.
Authentifizierung:	Überprüfung der Identität einer Person oder eines Systems anhand eines Merkmals, zum Beispiel per Passwort, Chipkarte oder Biometrie.
Authentizität:	Bezeichnet in der Informationssicherheit, dass Daten nicht unbefugt verändert wurden (z. B. Prüfung durch einen Hashwert) sowie dass ihre Herkunft nachweisbar ist.
Autonome Systemnummer (ASN):	Eine Autonome Systemnummer (ASN) ist eine eindeutige, global vergebene Nummer, die ein autonomes System im Internet identifiziert.
Backdoor:	Versteckt installiertes Programm (oft per Virus, Wurm oder Trojaner), das Dritten unbefugten Zugang zum Computer verschafft und Sicherheitseinrichtungen umgeht.
Backup:	Kopieren von Dateien oder Datenbanken auf einen sekundären Speicherort, um sie bei einem Geräteausfall oder einer Katastrophe wiederherstellen zu können.

BCMS:	Siehe Business Continuity Management System.
Blockchain:	Dezentrale Datenhaltung in einem P2P-Netzwerk: redundant geführte, hashverkettete Datenblöcke, per Konsens aktualisiert; Basis für Kryptowährungen, wie Bitcoin.
Bot/Botnetz:	Als Botnetz wird ein Verbund von Rechnern (Systemen) bezeichnet, die von einem fernsteuerbaren Schadprogramm (Bot) befallen sind.
Brand-Jacking:	Illegale Aneignung bzw. Verwendung einer Markenidentität durch Dritte, meist in betrügerischer Absicht.
Bring Your Own Vulnerable Driver (BYOVD):	Angreifer laden einen anfälligen, signierten Treiber in den Kernel des Zielsystems und führen dort unautorisierte Aktionen aus.
Broken Access Control:	Eine typische Schwäche in Webanwendungen, bei der Benutzer unbefugt auf Ressourcen zugreifen oder Aktionen ausführen können.
Brute-Force-Angriff:	Methode, um Zugang zu einem System oder Konto zu erlangen, indem systematisch zahlreiche Benutzernamen- und Passwortkombinationen ausprobiert werden.
BSI Cyber Index:	Normierte Kennzahl (Index) zur zusammenfassenden Beschreibung der Entwicklungen der Cybersicherheitslage.
BSIG:	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik.
BSI-IT-Sicherheitsmitteilung:	Seit April 2025 fasst das BSI CSW und BSI-Warnung § 7 BSIG zusammen zur „BSI-IT-Sicherheitsmitteilung (BITS)“.
BSI-Portal Warn- und Informationsdienst (WID):	CERT-Bund-Dienst, der neue Schwachstellen und aktuelle Bedrohungen für IT-Systeme publiziert; Zielgruppe ist vor allem die Bundesverwaltung.
Business Continuity Management System (BCMS):	Managementsystem zur Sicherstellung der Fortführung kritischer Geschäftsprozesse bei

	Störungen, zum Beispiel durch Cyberangriffe.
CERT-Bund:	Computer Emergency Response Team (CERT) für Bundesbehörden; zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei IT-Sicherheitsvorfällen.
Command-and-Control-Server:	Von Angreifern betriebener Server zur Steuerung infizierter Systeme (z. B. Botnetze), zum Beispiel zum Datendiebstahl oder für weitere Angriffe.
Common Vulnerabilities and Exposures (CVE):	Verzeichnis bekannter Schwachstellen in Software/Hardware; jede Schwachstelle erhält eine eindeutige CVE-Nummer zum standardisierten Austausch.
Common Weakness Enumeration (CWE):	Standardisierter Katalog, der Arten von Software- und Hardwareschwachstellen kategorisiert und ihnen eindeutige CWE-IDs zuweist.
Computer Security Incident Response Team (CSIRT):	Gruppe von Personen, die in einer formellen Einheit organisiert sind, mit der Aufgabe, schnell und ergebnisorientiert auf Cybersicherheitsvorfälle zu reagieren.
Confidential Computing:	Schützt Vertraulichkeit und Integrität von Daten während der Verarbeitung über attestierte, isolierte Trusted Execution Environments (TEE).
Coordinated Vulnerability Disclosure (CVD):	Koordinierte Veröffentlichung von Schwachstelleninformationen und Patches durch transparente, systematische Prozesse.
Cross-Site-Scripting:	Ausnutzen einer Schwachstelle in Webanwendungen, indem nicht vertrauenswürdiger Code in den Browser des Nutzers eingeschleust wird.
Cyber Resilience Act (CRA):	Erste europäische Verordnung, die ein angemessenes Maß an Cybersicherheit für alle vernetzten Produkte festlegt, die auf dem EU-Markt erhältlich sind.

Cyberakteur:	Einzelperson oder Gruppe, die für Cyberangriffe auf spezifische Ziele verantwortlich ist.
Cybercrime:	Straftaten, die mittels Informationstechnik begangen werden.
CyberGovSecure:	Im Rahmen der EU-NIS-2-Richtlinie werden mit dem Programm CyberGovSecure Maßnahmen zur Stärkung der Cybersicherheit in der Bundesverwaltung umgesetzt.
Cyberresilienz:	Die Fähigkeit, durch Cyberangriffe entstehende Belastungen zu verringern oder zu bewältigen.
Cybersicherheits-Compliance:	Beachtung und Einhaltung der Sicherheitsstandards für Informationssysteme.
Cyber-Sicherheitswarnung:	Informationsprodukt des BSI, das seit April 2025 mit der BSI-Warnung § 7 BSIG zur „BSI-IT-Sicherheitsmitteilung (BITS)“ zusammengefasst wird.
Cyberspionage:	Gezielte Cyberangriffe zum Ausspähen von Daten zur Einflussnahme und Sabotage.
Datenleak:	Ein Datenleak ist ein Sicherheitsvorfall, bei dem Unbefugte Zugriff auf sensible, vertrauliche oder persönliche Informationen erhalten.
Domain:	Eine Domain ist ein eindeutiger Name, der zur Identifizierung einer Website oder eines Servers im Internet verwendet wird.
DoS-/DDoS-Angriffe:	DoS-Angriffe richten sich gegen die Verfügbarkeit von Diensten, Systemen oder Netzen; bei paralleler Ausführung durch viele Systeme spricht man von DDoS.
Double Extortion:	Form der Erpressung über verschlüsselnde Schadsoftware (sog. Ransomware), bei der Opfer mit der Veröffentlichung privater Daten zur Zahlung eines Lösegelds genötigt werden.
ECC-256:	(Elliptic Curve Cryptography) Kryptografisches Verfahren mit einer Schlüssellänge von 256 Bit, das

	Operationen auf elliptischen Kurven über endlichen Körpern verwenden.
ECDSA-Signatur:	Methode zur Erstellung digitaler Signaturen auf Basis elliptischer Kurven; prüft Authentizität und Integrität digitaler Nachrichten.
EDR-Killer:	Malware, mit der Angreifer auf infizierten Systemen IT-Lösungen zur Endpoint Detection and Response (EDR) ausschalten.
EEG-Anlagen:	Anlagen zur Stromerzeugung aus erneuerbaren Energien (z. B. Solar, Wind, Biomasse), die nach dem Erneuerbare-Energien-Gesetz (EEG) gefördert werden.
Elliptische-Kurven-Kryptografie:	Siehe ECC-256.
Exploit:	Methode oder Code, der über eine Schwachstelle in Hard- oder Software nicht vorgesehene Befehle ausführt, zum Beispiel Programmabsturz, Rechteausweitung oder Codeausführung.
Exploitation:	Ausnutzen von Schwachstellen in Software oder Systemen, um unbefugten Zugriff zu erlangen, Daten zu manipulieren oder Schaden anzurichten.
Firewall:	Sicherheitssystem, das den Netzwerkverkehr nach vordefinierten Regeln überwacht und kontrolliert; Barriere zwischen internem Netzwerk und externen Netzen.
Gateway:	Ein Gateway dient als Vermittler zwischen Netzwerken mit unterschiedlichen Protokollen und ermöglicht so die Kommunikation und den Datenaustausch.
Geo-IP:	Siehe Geo-IP-Blocking.
Geo-IP-Blocking:	Einschränkung des Zugriffs auf Inhalte oder Dienste basierend auf dem geografischen Standort eines Nutzers, bestimmt über dessen IP-Adresse.
Google Play Protect:	Schützt vor schädlichen Apps und Malware: scannt Apps vor und nach

	der Installation (Play Store und andere Quellen) und warnt oder entfernt sie bei Bedarf.
GovTech Deutschland:	Eine zentrale Initiative und Plattform zur Modernisierung und Digitalisierung des öffentlichen Sektors in Deutschland.
Guardrails:	Guardrails sind Schutzmaßnahmen, mittels derer man versucht, KI-Systeme sicher, ohne Bias und fehlerfrei zu machen.
Hacktivismus:	Ideologisch motivierte Hacking-Aktivitäten zur Verbreitung politischer oder sozialer Statements; häufig per WebDefacement, DDoS-Angriffen oder Datenmanipulation.
Hash-Signatur:	Kryptografisches Verfahren, um die Identität des Erzeugers und die Integrität eines Dokuments sicherzustellen.
Hashwert:	Zeichenkette aus Ziffern und Buchstaben, resultierend aus einer Hashfunktion; bildet große Datenmengen in ein Datum mit fester Länge ab, eine Rückrechnung ist praktisch unmöglich.
Honeypot:	An ein Netzwerk angeschlossenes System, das als leichtes Ziel bzw. Köder für Angreifer dient, um deren Verhalten zu analysieren.
Host, Hoster:	Ein Hoster stellt für seine Kunden Speicherplatz und eine Internetanbindung für deren Websites zur Verfügung.
Hybride Bedrohungen:	Illegitime Handlungen staatlicher oder staatlich gelenkter Akteure zur Durchsetzung eigener Interessen zum Nachteil anderer Staaten außerhalb konventioneller militärischer Angriffe.
ICS-Panel:	Wesentliches Element eines Industrial Control Systems (ICS); Hauptfunktionen: Überwachung, Regelung und Steuerung industrieller Prozesse.
Indicators of Compromise (IOCs):	Technische Merkmale, die bei der Detektion von Cyberangriffen

	helfen, zum Beispiel IP-Adressen und Hashwerte.
Indirect Prompt Injection:	Angriff, bei dem manipulierte Texte in externe Inhalte eingebettet werden, um ein KI-Modell beim Verarbeiten unbemerkt zu steuern.
Infiltration:	Unautorisierter Zugriff auf ein Websystem mit mutmaßlich böswilliger Intention.
Information Stealer:	Schadprogramme, die es Kriminellen ermöglichen, auf infizierten Geräten unbemerkt persönliche Daten, wie Login-Daten, zu stehlen.
Informationssicherheitsmanagementsystem (ISMS):	Ein ISMS ist ein umfassendes Konzept zur Verwaltung, Steuerung und Verbesserung der Informationssicherheit einer Organisation.
Injection-Angriff, SQL-Injection:	Einschleusen schädlichen Codes zur Manipulation von Anwendungen oder für unautorisierten Zugriff; SQL-Injection betrifft SQL-Datenbanken.
Input-Validierung:	Die Input-Validierung ist ein Prozess, bei dem Eingabedaten einer Anwendung überprüft werden, um sicherzustellen, dass sie den definierten Kriterien entsprechen.
Insecure Direct Object Reference (IDOR):	Schwachstelle, die über Manipulation von Parametern oder IDs unautorisierten Zugriff auf Ressourcen ermöglicht (fehlende Zugriffskontrollen).
Internet der Dinge/Internet of Things (IoT):	Vernetzte, informations- und sensortechnisch aufgerüstete Gegenstände, die Daten erfassen, verarbeiten und speichern.
IP, IP-Adresse:	Das Internetprotokoll (IP) regelt die Adressierung und Weiterleitung von Netzwerkpaketen. IP-Adresse: eindeutige Ziffernfolge, die einem vernetzten Gerät zugeordnet ist.
IP-Adresse (Erklärung):	IP-Adresse steht für Internetprotokoll-Adresse.
IT-Planungsrat	Steuerungsgremium von Bund und Ländern für die Digitalisierung der öffentlichen Verwaltung.

Kernnetz:	Zentrales Element eines Netzes (Mobilfunk) bestehend aus elementaren Steuerungsfunktionen für den Datenverkehr.
KRITIS:	Kritische Infrastrukturen.
Kryptobibliothek:	Kryptografische Bibliothek: Software mit Algorithmen und Protokollen zur Verschlüsselung, die Entwicklern kryptografische Sicherheit erleichtert.
Large Language Model (LLM):	Großes KI-Sprachmodell.
Leak:	Ein Leak bezeichnet die nicht autorisierte Veröffentlichung von Informationen, Daten oder Inhalten, oft über das Internet.
Leak-Seite:	Auf Leak-Seiten veröffentlichen Angreifer Daten mit dem Ziel, die Eigentümer dieser Daten zu erpressen.
LLM-Härtung:	Maßnahmen, um die Robustheit und Zuverlässigkeit eines Sprachmodells zu erhöhen.
Logging:	Als Logging bezeichnet man die automatische Erstellung eines Protokolls (Log) von Softwareprozessen zur Aufzeichnung und Nachvollziehbarkeit von Prozessabläufen und Fehlerzuständen.
Love Scamming:	Love Scamming (Romance Scamming) ist Internetbetrug, bei dem Täter falsche Profile nutzen, um emotionalen Missbrauch zu betreiben und Geld zu erlangen.
Maliziös:	Programme oder Webseiten, die schädliche Operationen ausführen können, werden als maliziös bezeichnet.
Malvertising:	Malvertising kombiniert Malware und Advertising: Schadsoftware wird über Online-Werbung verbreitet.
Malware:	Malware (Malicious Software) bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und schädliche

	Funktionen auszuführen, zum Beispiel Viren, Würmer, Trojaner.
Malware-as-a-Service (MaaS):	Malware-as-a-Service; siehe auch CaaS.
Messzahl:	Zahlen derselben Maßeinheit (z. B. Zeit) zur Darstellung von Indizes oder Anteilen.
Mitigation:	Maßnahmen zur Reduzierung der Auswirkungen oder der Wahrscheinlichkeit von Bedrohungen oder Sicherheitsvorfällen.
Mitigationsdienstleister:	Siehe Mitigation.
Mitigationsmaßnahmen:	Siehe Mitigation.
MITRE:	Die MITRE Corporation ist eine Organisation, die die US-Regierung in technischen Fragen berät.
Multi-Faktor-Authentifizierung (MFA):	Sicherheitsmechanismus, bei dem Benutzer ihre Identität durch zwei oder mehr unabhängige Faktoren nachweisen müssen.
NIS-2-Richtlinie:	Network and Information Security Directive 2. Zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit.
normiert:	Umrechnung von beobachteten Werten auf eine einheitliche Skala, oft zwischen 0 und 1.
Notifying Authority Group:	Gruppe zur Benachrichtigung der Behörden.
OpenSSH:	Quelloffenes Werkzeug für die Steuerung von Rechnersystemen über das SSH-Protokoll.
OpenSSL:	OpenSSL ist eine quelloffene Kryptografische Bibliothek, die TLS/SSL implementiert und häufig verwendet wird, um sichere Verbindungen zu gewährleisten.
Patch:	Ein Patch ist ein Software-Update, das Schwachstellen schließt und Programmfehler behebt.
Patchdays:	Festes, regelmäßiges Datum für Softwareaktualisierungen seitens der Entwickler.
Patchmanagement:	Patchmanagement umfasst Identifizierung, Beschaffung, Testen, Verteilung und Installation von

	Patches auf Systemen zur Sicherstellung der Systemsicherheit.
Perimetersystem:	Perimetersysteme sind Systeme an der Grenze zwischen einem vertrauenswürdigen internen Netzwerk und dem Internet.
Persistenz (Angreifer):	Persistenz bezeichnet die Eigenschaft von Angreifergruppen, Ziele wiederholt anzugehen, bis sie kompromittiert sind (z. B. APTs).
Persistenz (Schadsoftware):	Damit Schadsoftware nach einem Neustart ausgeführt wird, benötigt sie einen Lademechanismus, zum Beispiel Einträge beim Booten.
Persistieren:	Angreifer halten Daten, Zugänge oder Schadprogramme dauerhaft in einem infiltrierten IT-System verfügbar.
Phishing:	Phishing (aus „password“ und „fishing“) ist das Versenden gefälschter Webseiten, E-Mails oder Nachrichten, um persönliche Daten, wie Passwörter, zu erlangen.
Port:	Virtuelle Schnittstelle, über die das Betriebssystem Datenpakete Prozessen zuordnet; mit der IP-Adresse ermöglicht der Port die Adressierung von Servern/Clients.
Prepared Statements:	Prepared Statements sind vorgefertigte SQL-Anweisungen, die mit Parametern befüllt werden, um Sicherheit und Effizienz zu verbessern.
Prompt Injection:	Methode zur Manipulation der Ausgabe von generativen KI-Modellen und Sprachmodellen.
Proof of Concept:	Nachweis, dass ein theoretisches Vorhaben in der Praxis umsetzbar ist.
Protokoll:	Ein Protokoll ist ein standardisierter Satz von Regeln, der die Kommunikation zwischen Kommunikationspartnern (z. B. Computern) regelt.
Provider:	Dienstanbieter mit verschiedenen Schwerpunkten, zum Beispiel Netzwerk-Provider oder Service-Provider.

Proxy-Netzwerk:	Ein Netzwerk, das Proxy-Server einsetzt, um Datenverkehr zwischen Clients und Servern zu vermitteln.
Public-Key-Infrastrukturen (PKI):	Infrastrukturen aus hierarchisch angeordneten Stellen, die digitale Zertifikate ausgeben, um die Vertraulichkeit oder Integrität und Authentizität von Informationen zu sichern.
Public-Key-Kryptografie:	Asymmetrische Verschlüsselung über ein Schlüsselpaar, die anhand eines öffentlichen Schlüssels erfolgt. Nur Empfänger verschlüsselter Daten haben den privaten Schlüssel.
Qubits:	Kleinste Recheneinheit von Quantencomputern, die mehrere Zustände gleichzeitig haben kann. Qubits ermöglichen mehr Speicher, mächtigere Berechnungen und komplexere Kryptografie.
Quellcode:	Der Quellcode ist die in einer Programmiersprache verfasste, für Menschen lesbare Beschreibung des Ablaufs eines Programms.
Quishing:	Quishing bezeichnet Phishing mit QR-Codes, die schwer auf Schadsoftware zu prüfen sind.
RADIUS-Protokoll:	Remote Authentication Dial-In User Service (RADIUS) ist ein Netzwerkprotokoll zur zentralen Authentifizierung, Autorisierung und Abrechnung von Nutzern.
Ransomware:	Ransomware sind Schadprogramme, die Zugriff auf Daten und Systeme einschränken und diese nur gegen Lösegeld freigeben.
Ransomware-as-a-Service (RaaS):	Ransomware-as-a-Service; siehe auch CCaaS.
Reifegrad 3:	Reifegrad des Reifegradmodells zur Einschätzung unternehmenseigener Systeme. Reifegrad 3: Ein ISMS/BCMS ist etabliert und dokumentiert.
Residential-Proxy-Botnetze:	Botnetze, die vorwiegend private Internetanschlüsse verwenden.
Resilienz:	Widerstandsfähigkeit von IT-Systemen gegen Sicherheitsvorfälle oder Angriffe, abhängig von

	organisatorischen und technischen Maßnahmen.
Router:	Ein Router ist ein Gerät, das Datenpakete zwischen Netzwerken weiterleitet und Geräte verbindet.
RSA:	Kürzel der Rivest–Shamir–Adleman-Verschlüsselung.
RSA-2048:	Asymmetrische Verschlüsselung mit einer 2048 Bit Standardschlüssellänge. Ver- und Entschlüsselung erfolgen jeweils über ein Schlüsselpaar aus privatem und öffentlichem Schlüssel.
SBOM:	Software Bill of Materials: umfassende Liste aller Softwarekomponenten, Abhängigkeiten und Metadaten, die mit einer Anwendung verknüpft sind.
Schadprogramm:	Computerprogramme, die entwickelt wurden, um unerwünschte und gegebenenfalls schädliche Funktionen auszuführen.
Schadwirkungen:	Alle Schäden, die ein erfolgreicher Angriff verursacht.
schwerwiegende Sicherheitsvorfälle:	Schwerwiegende Sicherheitsvorfälle heben sich von anderen Vorfällen aufgrund der besonderen Schwere ihrer Auswirkungen ab.
Secure Shell (SSH):	Ein Netzwerkprotokoll zur sicheren Datenübertragung und für den Fernzugriff zwischen Computern.
Secure Sockets Layer (SSL):	Ein veraltetes Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.
Security by Default:	Hersteller liefern Produkte ab Werk so voreingestellt, dass Informationssicherheitsanforderungen erfüllt werden.
Security by Design:	Hersteller berücksichtigen Informationssicherheitsanforderungen bereits bei der Produktentwicklung.
Security-In-Depth:	Cybersecurity-Strategie, die auf allen Ebenen eines Systems mehrere

	unabhängige Schutzschichten einsetzt.
Seitenkanalangriff (Side-Channel-Attack):	Ein Angriff, der physikalische oder logische Nebeneffekte der Programmausführung ausnutzt, um Informationen zu gewinnen.
Server-Side Request Forgery (SSRF):	SSRF ist eine Schwachstelle, bei der ein Angreifer den Server dazu bringt, unerwünschte Anfragen an interne oder externe Ressourcen zu senden.
Sextortion:	Sextortion ist Erpressung, bei der mit der Veröffentlichung von Nacktfotos oder -videos gedroht wird, um Zahlungen oder Handlungen zu erzwingen.
SIM-Swapping:	Beim SIM-Swapping erlangen Kriminelle die Kontrolle über die Mobilfunknummer eines Opfers, um SMS und Anrufe abzufangen.
Sinkhole:	Ein Sinkhole ist ein System, auf das Anfragen von Botnetz-infizierten Systemen umgeleitet werden, um Infektionen aufzuspüren.
Smishing:	Smishing ist Phishing per SMS oder Messenger, oft mit gefälschten Lieferbenachrichtigungen oder Links zu schädlichen Seiten.
Social Engineering:	Angriffe, die menschliche Schwächen, wie Neugier oder Angst, ausnutzen, um Opfer zur Preisgabe von Daten oder zur Ausführung schädlicher Handlungen zu verleiten.
Spam:	Unerwünschte Nachrichten, die massenhaft versendet werden und häufig Werbung oder Schadsoftware enthalten.
Supervised Fine-Tuning /Reinforcement Learning:	Trainingsmethoden von KI-Modellen.
Systeme zur Angriffserkennung (SzA):	Systeme zur frühzeitigen Erkennung von Cyberangriffen.
Takedown:	Takedown ist der Prozess, bei dem rechtswidrige oder schädliche Inhalte von einer Plattform entfernt werden.
Telematikinfrastruktur:	Digitale Infrastruktur für das Gesundheitswesen.

Time-to-Exploit:	Zeitspanne zwischen der Bekanntmachung und der Ausnutzung einer Schwachstelle.
Transport Layer Security (TLS):	Ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.
Ungezielte Massenangriffe:	Ein nicht zielgerichteter Cyberangriff, der nicht auf ein bestimmtes Opfer ausgerichtet ist, sondern auf viele potenzielle Opfer gleichzeitig, wie zum Beispiel bei Spam-Kampagnen.
Unique-IP-Index:	Der Unique-IP-Index bezeichnet die Anzahl eindeutiger IP-Adressen, die mit einem Schadprogramm in Verbindung gebracht werden und dient als Verbreitungsindikator.
Vertraulichkeit:	Schutzziel in der Informatik mit dem Zweck, dass nur berechtigte Personen Zugang zu bestimmten Daten haben.
Vishing:	Vishing (Voice Phishing) ist Telefonbetrug, bei dem Opfer telefonisch zur Preisgabe von Informationen oder Zahlungen verleitet werden.
Webfilter:	Ein Programm, mit dem sich die Internetnutzung einschränken lässt.
Zero Trust:	Prinzip der minimalen Rechte aller Entitäten einer Gesamtinfrastruktur.
Zero-Day-Schwachstelle:	Eine Zero-Day-Schwachstelle ist eine Sicherheitslücke, die Entwicklern zum Zeitpunkt der Entdeckung noch unbekannt ist.