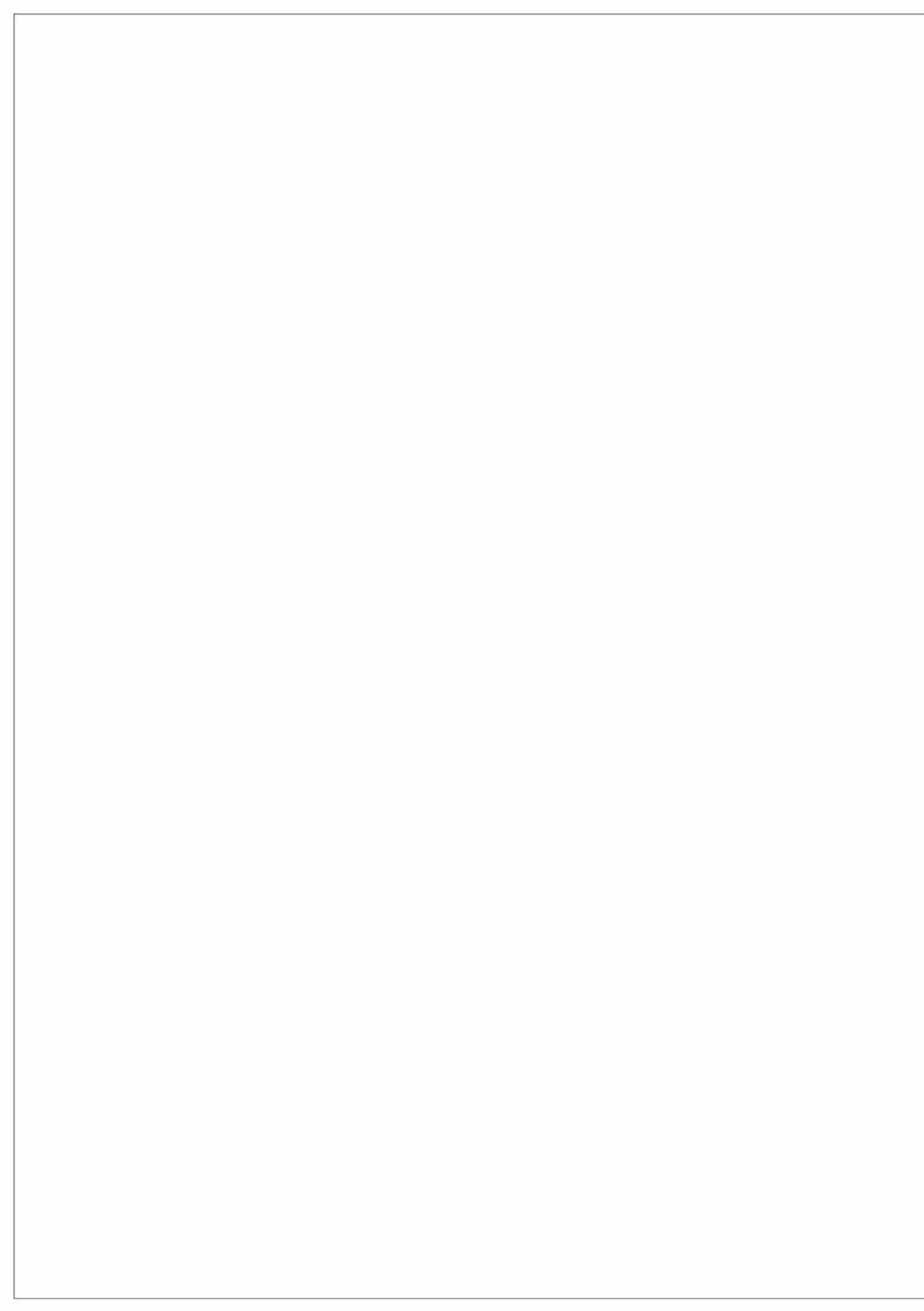


# **DIE LAGE DER IT-SICHERHEIT IN DEUTSCHLAND 2024**



Bundesamt  
für Sicherheit in der  
Informationstechnik

Deutschland  
**Digital•Sicher•BSI•**



# INHALT

---

<b>Verzeichnis ausgewählter Vorfälle .....</b>	<b>3</b>
<b>Abbildungsverzeichnis .....</b>	<b>3</b>
<b>Vorwort .....</b>	<b>4</b>
<b>1 Einleitung .....</b>	<b>8</b>
1.1 Zusammenfassung und Lagebewertung	8
1.2 Systematik der BSI- Lagebeobachtung	12
<b>A BEDROHUNGSLAGE .....</b>	<b>14</b>
<b>2 Schadprogramme .....</b>	<b>15</b>
2.1 Neue Schadprogramme	15
2.2 Botnetze	15
<b>3 Ransomware-Gruppen .....</b>	<b>19</b>
3.1 Cyberkriminelle Schattenwirtschaft	19
3.2 Für Deutschland relevante Ransomware-Gruppen	20
<b>4 APT-Gruppen .....</b>	<b>22</b>
4.1 Cyberaktivitäten im Rahmen geopolitischer Spannungen und Konflikte	22
4.2 Informationsoperationen	23
4.3 Technische Trends	23
4.4 Diplomatische, juristische und politische Maßnahmen	24
4.5 Für Deutschland relevante APT-Gruppen	25
<b>5 Phishing .....</b>	<b>28</b>
<b>B ANGRIFFSFLÄCHE .....</b>	<b>30</b>
<b>6 Schwachstellen .....</b>	<b>31</b>
6.1 Schwachstellen in Softwarereprodukten	31
6.2 Schwachstellen in Hardware	34
6.3 Pfadbezogene Schwachstellen	34
6.4 Schwachstellen in vernetzten Geräten	35
6.5 Schwachstellen in Perimetersystemen	36
6.6 Schwachstellen in kryptografischen Verfahren	36
<b>7 Große KI-Sprachmodelle .....</b>	<b>39</b>
7.1 Schwachstellen von Sprachmodellen und ihre Ursachen	39
7.2 Missbräuchliche Verwendung von Sprachmodellen	41
7.3 Entwicklungen	42
7.4 Fazit	42

<b>C GEFÄHRDUNGSLAGE .....</b>	<b>44</b>
<b>8 Ausgewählte allgemeine Angriffsarten .....</b>	<b>45</b>
8.1 Distributed Denial of Service	45
8.2 Leak-Opfer	47
8.3 Angriffe auf die Cloud	53
<b>9 Erkenntnisse zur Gefährdungslage in der Gesellschaft .....</b>	<b>55</b>
9.1 Gefährdungslage am digitalen Verbrauchermarkt	55
9.2 Gefährdungslage in sozialen Netzwerken	58
<b>10 Erkenntnisse zur Gefährdungslage in der Wirtschaft .....</b>	<b>61</b>
10.1 Gefährdungslage Kritischer Infrastrukturen	62
10.2 Gefährdungslage der KMU in Deutschland	68
<b>11 Erkenntnisse zur Gefährdungslage in der Bundesverwaltung .....</b>	<b>73</b>
<b>D RESILIENZ .....</b>	<b>76</b>
<b>12 Cyberresilienz gesellschaftlicher und politischer Großveranstaltungen .....</b>	<b>77</b>
12.1 Cybersicherheit von Wahlen im Superwahljahr 2024	77
12.2 Cybersicherheit im Rahmen von Sportereignissen	78
<b>13 Resilienz in der Cloud .....</b>	<b>79</b>
<b>14 Elektronische Identitäten .....</b>	<b>81</b>
14.1 Für die Zukunft: EUDI-Wallet	81
14.2 Anerkennung von eIDs in Europa	82
14.3 AusweisApp	82
<b>15 Europäisierung der Cybersicherheit .....</b>	<b>83</b>
15.1 Cyber Resilience Act (CRA)	83
15.2 NIS-2-Richtlinie	84
15.3 Cybersecurity Act (CSA)	85
15.4 Lagebericht europäische Standardisierung	86
<b>16 Zulassung von VS-Produkten .....</b>	<b>87</b>
<b>17 Fazit .....</b>	<b>90</b>
<b>18 Glossar .....</b>	<b>94</b>
<b>19 Quellenverzeichnis .....</b>	<b>102</b>
<b>20 Abkürzungsverzeichnis .....</b>	<b>104</b>
<b>12 Monate Cybersicherheit im Überblick .....</b>	<b>anhängend</b>

## Verzeichnis ausgewählter Vorfälle

Ausnutzung von Zero-Day-Schwachstellen bei IT-Dienstleistern in Deutschland	33
Takedowns	52
Kompromittierung der Microsoft-Cloud-Infrastruktur	54
CrowdStrike Falcon verursacht weltweit IT-Ausfälle	72
Cybersicherheitsvorfall bei einem Remote-Screensharing-Anbieter	73
Angriffe auf E-Mail-Postfächer verschiedener Einrichtungen	75
Ransomware-Angriff auf einen kommunalen IT-Dienstleister	76

## Abbildungsverzeichnis

Abbildung 1: Systematik der BSI-Lagebeobachtung	14
Abbildung 2: Durchschnittlicher täglicher Zuwachs neuer Schadprogramm-Varianten	18
Abbildung 3: Durchschnittlicher täglicher Zuwachs neuer Android-Schadprogramm-Varianten	18
Abbildung 4: Infizierte Systeme (Unique IP) Juli 2023 bis Juli 2024 nach den Top-10-Botnetzen	20
Abbildung 5: Top-5-Leak-Seiten Juli 2023 bis Juni 2024 nach Zahl der Leak-Opfer	23
Abbildung 6: Für Deutschland relevante APT-Gruppen	28
Abbildung 7: Ausgewählte Phishing-URLs und Phishing-IPs weltweit nach nachgeahmter Branche	30
Abbildung 8: Von Verbraucherinnen und Verbrauchern gemeldete Phishing-E-Mails nach Art der nachgeahmten Branche	31
Abbildung 9: Meldungen über schwachstellenbehaftete Produkte Juli 2023 bis Juni 2024 nach möglicher Schadwirkung	34
Abbildung 10: Bekannt gewordene DDoS-Angriffe in Deutschland	48
Abbildung 11: Anteil hochvoluminöser Angriffe an allen bekannt gewordenen DDoS-Angriffen in Deutschland	48
Abbildung 12: Durchschnittliche Lösegeldzahlungen nach Quartal	49
Abbildung 13: Ransomware-Opfer nach Zahlungsverhalten	50
Abbildung 14: Mutmaßliche Opfer auf Leak-Seiten aus Deutschland und weltweit im Vergleich	51
Abbildung 15: Mutmaßliche Opfer aus Deutschland auf Leak-Seiten	51
Abbildung 16: Mutmaßliche Opfer aus Deutschland auf Leak-Seiten	52
Abbildung 17: Mutmaßliche Opfer weltweit nach Leak-Seiten	53
Abbildung 18: Anteile betroffener Verbraucherinnen und Verbraucher	58
Abbildung 19: Anfragen von Verbraucherinnen und Verbrauchern an das Service Center des BSI	73
Abbildung 20: Art der geleakten Informationen nach Häufigkeit (Fälle mit Verbraucherbetroffenheit)	60
Abbildung 21: Betroffenheit von Verbraucherinnen und Verbrauchern aus Deutschland an registrierten Datenleaks	60
Abbildung 22: Über welche der folgenden Kanäle suchen Sie Informationen über Cybersicherheit?	61
Abbildung 23: Genutzte Informationsquellen Cybersicherheit – Informationsquellen nach Alter	62
Abbildung 24: Meldungen nach KRITIS-Sektoren im Berichtszeitraum	65
Abbildung 25: ISMS-Reifegrade und BCMS-Reifegrade nach Sektoren laut jeweils letztem vorliegenden Nachweis	66
Abbildung 26: Umsetzungsgrade SzA gemäß dem jeweils letzten vorliegenden Nachweis	67
Abbildung 27: Aufteilung Unternehmen in Deutschland im Jahr 2019	71
Abbildung 28: Index über die neuen Sperrungen maliziöser Webseiten	76
Abbildung 29: Spam-Mail-Index für die Bundesverwaltung	77
Abbildung 30 : Zulassungsverfahren des BSI für VS-Produkte gemäß Verschluss Sachen Anweisung (VSA)	88
Abbildung 31: Nationale und internationale Zulassungen des BSI für VS-Produkte	88
Abbildung 32: Gesamtzahlen der VS-Anforderungsprofile des BSI	88

# VORWORT

---

Die Chancen, die sich durch die zunehmende Digitalisierung fast aller Bereiche unseres Zusammenlebens eröffnen, sind vielfältig. Vielfältig sind aber auch die Möglichkeiten, diese digitalen Räume für hybride Angriffe und kriminelle Machenschaften zu nutzen. Wir erleben durch den russischen Angriffskrieg gegen die Ukraine und seine Folgen auch eine Zeitenwende für die innere Sicherheit. Die Bedrohungslage im Bereich der Cybersicherheit ist unvermindert hoch. Deshalb handelt die Bundesregierung entschlossen, um die Widerstandskraft Deutschlands gegenüber Cybergefahren weiter zu steigern.

Im Jahr 2024 wurde das deutsche IT-Sicherheitsrecht umfassend modernisiert und neu strukturiert: Mit der Umsetzung der zweiten EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2) in deutsches Recht sind

nun mehr Unternehmen in mehr Sektoren dazu verpflichtet, Cybersicherheitsmaßnahmen vorzunehmen und Cyberangriffe zu melden. Darüber hinaus stärken wir die Cybersicherheit der Bundesverwaltung. Mit dem Cyber Resilience Act (CRA) wird die Cybersicherheit in zusätzlichen Sektoren implementiert: Hersteller oder Importeure von vernetzbaren Produkten müssen künftig nicht nur Betriebssicherheit sicherstellen, sondern auch Informationssicherheit.

All diese neuen Regeln schaffen mehr Sicherheit. Sie stellen jedoch auch eine Herausforderung dar – für die betroffenen Unternehmen ebenso wie für das Bundesamt für Sicherheit in der Informationstechnik (BSI), dem mit neuen Aufsichtsinstrumenten künftig eine Schlüsselrolle zukommt. Das Bundesamt für Sicherheit in der Informationstechnik

unterstützt die Unternehmen aktiv – und seine Angebote werden bereits rege genutzt. Das ist eine gute Nachricht, denn die Schäden, die durch Cyberangriffe Jahr für Jahr entstehen, sind immens – für Wirtschaft, Verwaltung und Gesellschaft.

Die Resilienz gegen Cyberangriffe ist in einer digitalisierten Welt wichtig für die Wehrhaftigkeit unserer freiheitlichen Demokratie als Ganzes. Es lohnt sich also, diese Herausforderung anzunehmen. Der vorliegende Bericht zur Lage der IT-Sicherheit in Deutschland ist dazu ein wichtiger Beitrag zu mehr Widerstandsfähigkeit, denn er hilft beim Verstehen, Vorbeugen, Erkennen von Gefahren im Cyberraum. Ich danke allen, die daran mitgewirkt haben und wünsche Ihnen eine interessante Lektüre mit vielen spannenden Informationen zur Cybersicherheit in Deutschland.



A handwritten signature in blue ink that reads "Nancy Faeser".

**Nancy Faeser,**  
Bundesministerin des Inneren und für Heimat

# VORWORT

---

CRA, CSA, RED, NIS-2 und DORA ... Nein, es handelt sich dabei nicht um den längst zum Klassiker gewordenen Hit der Fantastischen Vier. Hinter all diesen Abkürzungen stecken Gesetze, Verordnungen und Richtlinien zur Cybersicherheit in Europa, die jüngst in Kraft getreten sind oder kurz davorstehen. Diese Regulierungen gehen auf den immensen Handlungsbedarf zurück, den wir mit Blick auf Cyberangriffe und IT-Sicherheitsvorfälle haben: Die Notwendigkeit und auch die Dringlichkeit, auf breiter Front zu handeln, ist offensichtlich.

Allen, die den genannten Handlungsbedarf etwas „handfester“ illustriert sehen möchten, rufe ich den 19. Juli 2024 in Erinnerung – den Tag, an dem ein fehlerhaftes Update in einem Sicherheitsprodukt des Herstellers CrowdStrike den IT-Betrieb weltweit zum Erliegen brachte – und mit ihm den OP-Betrieb in Krankenhäusern, den internationalen Flugbetrieb, den Produktionsbetrieb unzähliger Unternehmen. Die wirtschaftlichen Schäden sind bis heute nicht genau bezifferbar, ebenso wenig wie der Schaden, den das Vertrauen in unsere digitalisierte Welt erlitten hat. Und dabei müssen wir uns immer vor Augen führen: Es handelte sich dabei nicht um einen Cyberangriff, sondern „nur“ um einen operativen Fehler.

Der Vorfall hat beinahe lehrbuchhaft gezeigt, dass und auf welche Art die Verantwortung für eine sichere Digitalisierung auf mehreren Schultern verteilt liegt: bei den Herstellern für sichere und fehlerfreie Produkte. Bei den Betreibern für resiliente Infrastrukturen und Prozesse. Bei den staatlichen Einrichtungen für Schutz und Präven-

tion, eine schnelle und ganzheitliche Lageerfassung und angemessene reaktive Maßnahmen. Erst, wenn wir alle guten Gewissens behaupten können, dass wir dieser Verantwortung gerecht werden, erst dann dürfen und müssen wir darüber sprechen, welchen Teil jede einzelne Bürgerin und jeder einzelne Bürger zu einer sicheren Digitalisierung beitragen kann.

So sind die eingangs genannten Regulierungsvorhaben nicht nur leider notwendig für den Schutz von Unternehmen und Behörden, sondern immer auch für uns alle als Bürgerinnen und Bürger: Der Cyber Resilience Act (CRA) wird dazu führen, dass Hersteller, die für ihre Produkte das bereits etablierte CE-Kennzeichen erhalten wollen, dafür Sorge tragen müssen, dass diese Produkte auch cybersicher sind. Mit Inkrafttreten von NIS-2 (Richtlinie zur Netzwerk- und Informationssicherheit) werden wir als BSI uns um rund 30.000 Betriebe und Organisationen kümmern, die uns künftig IT-Sicherheitsmaßnahmen nachweisen und IT-Sicherheitsvorfälle melden. Und auch die weiteren Regulierungsvorhaben wollen unsere digitale Welt sicherer machen: etwa bei Cloudprodukten, funktionsfähigen Geräten oder im Finanzsektor.

Selbstredend bringen Regulierungen immer auch Aufwände mit sich: für Unternehmen und Hersteller – und auch für die Aufsichtsbehörden. Das BSI wird sich dabei konsequent und in höchstem Maße kooperativ, beratend und helfend für die Stärkung der Cybersicherheit in Deutschland und Europa einsetzen – und das nicht nur von der Seitenlinie, sondern mitten auf dem Spielfeld.

Eines unserer wichtigsten Vorhaben für die kommenden Jahre ist es, die Cybersicherheit in Deutschland messbar zu machen – denn was man messen kann, das kann man auch verbessern. Grundstein dafür ist unser diesjähriger Bericht zur Lage der IT-Sicherheit in Deutschland. Er zeigt: Die Gefährdungslage ist und bleibt besorgniserregend, aber es liegt in unserer Hand, sie zu verbessern.

Gezielte Cyberattacken gegen staatliche wie politische Institutionen und KI-geboostete Desinformationskampagnen werten wir als Angriffe auf unsere Demokratie, gegen die wir uns entschieden zur Wehr setzen. Angriffe mit Ransomware, sogenannte Verschlüsselungstrojaner, haben erneut zahlreiche Kommunen und damit unmittelbar Bürgerinnen und Bürger getroffen. Auch unzählige Unternehmen sind auf diesem Wege zu Opfern cyberkrimineller Täter geworden. Es ist unabdingbar, dass wir uns – dass Kommunen und Unternehmen sich selbst – besser schützen. Gleiches gilt für Angriffe mit dem Ziel der Cyberspionage. Nicht zuletzt werden DDoS-Angriffe (Überlastangriffe) weiterhin insbesondere von Unterstützern des völkerrechtswidrigen russischen Angriffskrieges genutzt, um – im Wesentlichen – Propagandaeffekte zu erzielen.

Diese ebenfalls unvollständige Liste an Gefährdungen und Bedrohungen soll uns aber nicht dazu verleiten, den Kopf in den Sand zu stecken. Ja, die Angreifer werden besser und schneller. Wir aber auch – und das ist die gute Nachricht: Wir sind den Bedrohungen aus dem Cyberraum nicht schutzlos ausgeliefert! Der BSI-Lagebericht 2024 belegt nämlich auch: Unsere Maßnahmen wirken.

Genau deswegen ist es nun entscheidend, nicht nachzulassen, sondern gemeinsam noch eine Schippe draufzulegen. Unternehmen und Hersteller, Wissenschaft, Zivilgesellschaft und staatliche Institutionen: Wir alle müssen zusammen an einem sicheren digitalen Heute und Morgen arbeiten. Daher verfolgen wir im BSI so nachdrücklich das Ziel der Cybernation Deutschland. Lassen Sie uns diese Vision gemeinsam zur Wirklichkeit machen.



A handwritten signature in black ink, appearing to read "C. Plattner".

Claudia Plattner,  
Präsidentin des Bundesamts für Sicherheit in der Informationstechnik

# 1 – Einleitung

---

Als die Cybersicherheitsbehörde des Bundes beobachtet das Bundesamt für Sicherheit in der Informationstechnik (BSI) kontinuierlich die Gefährdungslage der IT-Sicherheit in Deutschland. Im Fokus des BSI stehen die Erkennung von Cyberangriffen auf staatliche sowie öffentliche Institutionen, Unternehmen und Privatpersonen, aber auch Maßnahmen zur Prävention und Abwehr spezifischer Gefahren für die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit der Kommunikationstechnik. Diese setzt das BSI um und arbeitet dabei mit den für die Gefahrenabwehr und Strafverfolgung zuständigen Polizeivollzugsbehörden zusammen.

Durch Bedrohungen im Cyberraum entstehen immense Schäden in Wirtschaft, Verwaltung und Gesellschaft. Darauf hat das BSI im Januar 2024 die Initiative Cybernation Deutschland gestartet. Neben der Erhöhung der Cyberresilienz soll die Initiative dazu dienen, insgesamt mehr Bewusstsein für das Thema Cybersicherheit zu schaffen, Cybersicherheit pragmatisch zu gestalten und messbar zu machen, technologische Expertise in Deutschland gezielter zu nutzen und in Deutschland den Markt für Cybersicherheitsprodukte und Dienstleistungen zu stärken.

Der vorliegende Bericht stellt die wichtigsten Entwicklungen für den Berichtszeitraum vom 1. Juli 2023 bis 30. Juni 2024 vor. Der aktuelle Berichtszeitraum umfasst wieder zwölf Monaten während der vergangene Berichtszeitraum zur Anpassung an Quartalsformate einmalig 13 Monate abdeckte. Direkte Vergleiche absoluter Zahlen sind daher nicht möglich. Im vorliegenden Bericht wird soweit möglich auf direkt vergleichbare Durchschnittswerte für Tage oder Monate abgestellt.

## 1.1 Zusammenfassung und Lagebewertung

Die Lage der IT-Sicherheit in Deutschland war im Berichtszeitraum angespannt. So differenzierte sich die cyberkriminelle Schattenwirtschaft weiter arbeitsteilig in Ransomware-Betreiber, deren Affiliates und Access Broker aus. Zugleich nutzte sie alternative Angriffsflächen, wie

etwa Zero-Day-Schwachstellen (Schwachstellen, für die es noch keine Sicherheitsupdates gibt), mit dem Ziel der Datenexfiltration, um ganz ohne Ransomware hohe Lösegelder mit der Drohung der Veröffentlichung der Daten erpressen zu können. Opfer waren neben überwiegend kleinen und mittleren Unternehmen insbesondere IT-Dienstleister und auch wieder Kommunen. Im Bereich der Cyberspionage und -sabotage setzte sich dagegen der Trend zu vergleichsweise einfachen Angriffen auf Perimeterversysteme fort. Dabei stellten die Angreifer vor allem die Schadwirkungen hacktivistischer Distributed-Denial-of-Service (DDoS)-Angriffe im Kontext geopolitischer Konflikte übertrieben in den sozialen Medien dar, um allgemeine gesellschaftliche Verunsicherung zu schüren.

Einhergehend mit der Zunahme der Bedrohungen und Gefährdungen war auch ein Anwachsen der Resilienz der Cybernation Deutschland spürbar. So gelang es internationalen Strafverfolgern mit einer Reihe von Abschaltungen (engl. Takedowns) beispielsweise, das Wachstum neuer Malware-Varianten einzudämmen.

Zugleich besteht breiter Handlungsbedarf insbesondere hinsichtlich der Angriffsfläche, die mit der allgemeinen Digitalisierung stetig zunimmt. Jedes Unternehmen, jede Behörde, jede wissenschaftliche oder soziale Einrichtung, jeder Einzelunternehmer – ganz Deutschland ist aufgerufen, eigene Angriffsflächen zu ermitteln und zu schützen. Das ist in historisch gewachsenen IT-Landschaften eine große Herausforderung, aber notwendig, denn die Angreifer suchen beständig nach neuen Angriffsvektoren.

### Die Lage im Einzelnen:

#### (1) Bedrohungslage:

**Ransomware-Gruppen:** Cyberkriminelle professionalisieren ihre Arbeitsweise, sind technisch auf dem neusten Stand und agieren aggressiv. Mehr und mehr cyberkriminelle Angreifer zögern die Detektion ihrer Angriffe hinaus, indem sie Detektionssysteme (Endpoint Detection and Response (EDR) Programme) in infizierten Netzen deaktivieren. Dazu werden spezielle Schadsoftware-

Varianten genutzt, die vermehrt als Dienstleistung (Malware-as-a-Service, MaaS) angeboten werden und daher vielen Angreifern offenstehen. Darüber hinaus haben sich Access Broker, die mit erbeuteten Zugangsdaten handeln, zu einem festen Teilgebiet cyberkrimineller Schattenwirtschaft entwickelt. Weiterhin zeigte sich im Berichtszeitraum, dass cyberkriminelle Angreifer über die nötigen Ressourcen verfügen, um Zero-Day-Schwachstellen aufzuspüren und für Datenexfiltrationen auszunutzen, wie durch die Angreifer hinter der Ransomware Clop geschehen. Aufgrund der bereits in der Vergangenheit gezahlten hohen Lösegelder wird dieses Risiko auf unabsehbare Zeit bestehen.

**Advanced Persistent Threats (APT):** Im Berichtszeitraum waren 22 verschiedene APT-Gruppen in Deutschland aktiv. Ihre Angriffe zielen auf Behörden und Unternehmen insbesondere der auswärtigen Angelegenheiten, der Verteidigung sowie der öffentlichen Sicherheit und Ordnung. Eine Reihe weiterer Entwicklungen prägte die APT-Bedrohungslage. So zeigte sich erneut, dass geopolitische und zwischenstaatliche Konflikte oftmals mit einer ganzen Bandbreite an Phänomenen im Cyberraum einhergehen: Desinformation, Hacktivismus, Spionage und Sabotage waren sowohl im russischen Angriffskrieg gegen die Ukraine als auch in der Folge des Terrorangriffs der Hamas auf Israel zu beobachten. Dabei bleibt ein großer Teil der Cyberaktivitäten regional begrenzt.

Weiterhin stellen hierbei Angreifer die Auswirkungen von Sabotage- oder DDoS-Angriffen in sozialen Medien übertrieben dar, um durch diese Form der „Öffentlichkeitsarbeit“ mehr Unsicherheit in den angegriffenen Regionen zu erzeugen, als angesichts der oft begrenzten Schadwirkungen eigentlich gerechtfertigt wäre.

## (2) Angriffsfläche:

**Schwachstellen:** Im Jahr 2023 wurden durchschnittlich täglich 78 neue Schwachstellen bekannt. Im Rahmen des Verfahrens zur koordinierten Veröffentlichung von Schwachstellen erreichten das BSI zudem durchschnittlich monatlich 18 Meldungen über Zero-Day-Schwachstellen in IT-Produkten deutscher Hersteller.

**Schwachstellen in Perimetern:** Im Berichtszeitraum wurde zudem eine Vielzahl kritischer Schwachstellen in Perimetersystemen, wie beispielsweise Firewalls und VPNs, bekannt. Teilweise handelte es sich dabei um die besonders gefährlichen Zero-Day-Schwachstellen, die Cyber-

angreifern bereits bekannt waren und ausgenutzt wurden, bevor die Hersteller der betroffenen Produkte Patches bereitstellen konnten. Der seit einigen Jahren beobachtete Trend zu einfachen und unkomplizierten Angriffen auf Perimetersysteme setzte sich im Berichtszeitraum damit deutlich verstärkt fort.

## (3) Gefährdungslage:

**DDoS-Angriffe:** Eine herausgehobene Entwicklung war im Berichtszeitraum bei DDoS-Angriffen zu verzeichnen. Insbesondere im ersten Halbjahr 2024 nahmen Qualität und Häufigkeit von DDoS-Angriffen deutlich zu. So lag der Anteil hochvoluminöser DDoS-Angriffe mit einer Bandbreite von über 10.000 Megabit pro Sekunde bei monatlich durchschnittlich 13 % und damit mehr als doppelt so hoch wie im langjährigen Durchschnitt mit 6,75 %. Sollte sich der Trend fortsetzen, wäre dies ein Indiz dafür, dass Angreifer gezielt Botnetz-Kapazitäten aufgebaut haben und künftig grundsätzlich mit mehr hochvoluminösen DDoS-Angriffen zu rechnen wäre.

**Ransomware-Angriffe:** Cyberangriffe insbesondere auf Wirtschaftsunternehmen waren im aktuellen Berichtszeitraum weiterhin breit gestreut. Einerseits wurden nach wie vor umsatzarstarke Großunternehmen angegriffen. Andererseits wurden aufgrund des geringeren technologischen Aufwandes bei Nutzung von Ransomware-as-a-Service (RaaS) vor allem Ransomware-Angriffe auch zum Massengeschäft: Zunehmend sind die kleinen und mittleren Unternehmen (KMU), aber auch Kommunen, Universitäten und Forschungseinrichtungen betroffen. Dabei gehen die Angreifer nach wie vor oft den Weg des geringsten Widerstandes. Auch wenn gezielte Angriffe auf umsatzarstarke Unternehmen registriert werden, suchen sich die Kriminellen tendenziell die am leichtesten angreifbaren Opfer aus. Je schlechter Organisationen ihre Angriffsflächen schützen, desto eher werden sie Opfer von Cyberangriffen.

**Angriffe auf Cloud-Infrastrukturen:** Im Berichtszeitraum kam es zu mehreren erfolgreichen Ransomware-Angriffen auf Public-Cloud-Dienste, die deren Verfügbarkeit einschränkten. Zudem wurden mehrfach Fälle von Angriffen auf die Vertraulichkeit von Cloud-Diensten durch Identitätsdiebstahl, sowohl der Identitäten der Anwenderinnen und Anwender als auch des Personals des Anbieters, bekannt. So verschafften sich mutmaßlich staatliche chinesische Cyberangreifer mittels zuvor

kompromittiertem Signaturschlüssel im September 2023 Zugriff auf die Microsoft-Cloud-Infrastruktur. Der Signaturschlüssel konnte aufgrund eines Validierungsfehlers sowohl für Consumer- als auch Enterprise-Accounts verwendet werden und ermöglichte den Angreifern somit die Imitation legitimer Nutzer.

**Angriffe auf politische Organisationen:** Im Berichtszeitraum wurden Vorfälle bekannt, bei denen E-Mail-Postfächer verschiedener politischer Organisationen angegriffen wurden. Dabei bedienten sich insbesondere staatliche Akteure verschiedener Methoden, um Zugriff auf E-Mails zu erhalten. Dazu gehörten Angriffe mit schwachen oder recycelten Passwörtern, über Zero-Day-Schwachstellen oder Phishing-Angriffe. Eine größere Angriffsfläche stellen insbesondere Webmail-Systeme dar, die frei über das Internet und ohne Multifaktor-Authentifizierung erreichbar sind.

#### (4) Schadwirkungen:

IT-Dienstleister waren 2023 Ziel von Angriffskampagnen. Wegen ihrer breiten Wirkung auf deren Kunden entfalten Cyberangriffe auf IT-Dienstleister erhebliche Schadwirkungen. Im Berichtszeitraum wurde ein solcher Ransomware-Angriff bekannt, bei dem rund 20.000 Arbeitsplätze in 72 Kommunen mit insgesamt rund 1,7 Millionen Einwohnern betroffen waren. Der angegriffene Dienstleister fuhr die Mehrheit seiner Systeme herunter, wodurch zahlreiche kommunale Dienstleistungen wie etwa Bürgergeld, Elterngeld und Kfz-Zulassungen nicht verfügbar und Meldeämter oder Bauämter nur eingeschränkt arbeitsfähig waren. Zum Redaktionsschluss des vorliegenden Berichts befand sich der Dienstleister weiterhin in der Wiederlaufphase, während der bestimmte Fachverfahren wiederhergestellt oder in einem Basisbetrieb laufen und andere Fachverfahren nicht zur Verfügung stehen.

Die Zahl der mutmaßlichen Opfer von Datenleaks nach Ransomware-Angriffen ist im Berichtszeitraum im Vergleich zum vorherigen Berichtszeitraum weiter gestiegen. Im zweiten Halbjahr 2023 wies die entsprechende Messzahl kurzzeitig sogar rund die doppelte Menge mutmaßlicher Leak-Opfer im Vergleich zum Referenzjahr 2021 aus. Wesentlicher Faktor für diesen Anstieg war wahrscheinlich eine anhaltend hohe bis sehr hohe Aktivität der bedrohlichsten Akteure. Weiter beobachtete das BSI mehrere Leak-Seiten, die nur kurze Zeit aktiv waren oder durch einzelne Kampagnen viele mutmaßliche Opfer nannten.

Zwei Zero-Day-Schwachstellen bei IT-Dienstleistern entfalteten im aktuellen Berichtszeitraum erhebliche

Schadwirkungen, da diese von einer Ransomware-Gruppe zur Exfiltration von Daten genutzt wurden, ohne dass eine Ransomware zum Einsatz gekommen wäre. Die Höhe der erpressten Lösegelder ist im Berichtszeitraum im Vergleich zum vorherigen Berichtszeitraum weiter gestiegen, wobei Opfer für exfiltrierte Daten in der Regel deutlich höhere Lösegelder zahlen mussten als für verschlüsselte Daten.

Auch Verbraucherdaten waren im Berichtszeitraum von Datenleaks betroffen. Cyberkriminelle nutzten dafür schwachstellenbehaftete sowie offen oder falsch konfigurierte Server aus, um Daten auszuleiten und für weitere Cyberangriffe weiterzuverkaufen. Im Zuge von Datenleaks durch Ransomware-Gruppen waren teilweise auch personenbezogene Daten von Verbraucherinnen und Verbrauchern betroffen. Namen und E-Mail-Adressen, postalische Adressen sowie Geburtsdatum und Telefonnummer waren die häufigsten geleakten Daten von Verbraucherinnen und Verbrauchern.

#### (5) Resilienz:

**Takedowns:** Im Berichtszeitraum gelangen Strafverfolgern in international koordinierten Maßnahmen mehrere Takedowns gegen RaaS, darunter auch die bis dahin sehr aktive Dropper/Loader-Malware QakBot (August 2023), die RaaS RagnarLocker (Oktober 2023), Alphv (Dezember 2023) und LockBit (Februar 2024).

**Resilienz in der Bundesverwaltung:** Im Berichtszeitraum hat das BSI die Infrastruktur der Bundesverwaltung systematisch auf Schwachstellen untersucht und durchschnittlich täglich 15 Schwachstellenwarnungen an betroffene Behörden übermittelt. Darüber hinaus wurden täglich durchschnittlich rund 368 zusätzliche maliziöse Webseiten für den Zugriff aus der Bundesverwaltung gesperrt und durchschnitt täglich 9.212 Zugriffsversuche auf maliziöse Webseiten blockiert. Zum Schutz vor Malware-Angriffen per Mail wurden zudem durchschnittlich rund 753.000 E-Mails pro Tag auf unerwünschte Inhalte oder maliziöse Anhänge überprüft.

**Resilienz in Cloud-Infrastrukturen:** Cloud-intrinsische Fähigkeiten, wie etwa umfassende Protokollierungs- und Detektionsmöglichkeiten, helfen, etwaige Angriffe zu entdecken und einzudämmen. Der hohe Automatisierungsgrad von Cloud-Diensten erhöht weiterhin die Widerstandsfähigkeit der Anwender gegen Angriffe, etwa durch das frühzeitige Einspielen von Sicherheitspatches und die Bereitstellung von Präventions-, Detektions- und Reaktionsmaßnahmen, welche auf aktuelle Entwicklungen in der Cyberbedrohungslandschaft eingehen.

**Resilienz Kritischer Infrastrukturen:** Betreiber Kritischer Infrastrukturen (KRITIS) sind zur Steigerung ihrer Präventionsfähigkeiten zum Einsatz eines Informationssicherheitsmanagementsystems (ISMS) und zur Steigerung ihrer Bewältigungsfähigkeiten zum Einsatz eines Business-Continuity-Management-Systems (BCMS) verpflichtet. Über die Wirksamkeit dieser Systeme gibt eine zweijährliche, verpflichtende Reifegradprüfung Aufschluss. Demnach konnten in den letzten zwei Jahren 140 von 671 Betreibern den Reifegrad ihrer ISMS verbessern. Die BCMS konnten bei 114 Betreibern um mindestens einen Reifegrad verbessert werden. Insgesamt bewegte sich die Resilienz der meldepflichtigen KRITIS-Betreiber damit auf mittlerem Niveau der 5-stufigen Reifegradskala. Hier ist somit ein leicht positiver Trend erkennbar.

**Elektronische Identitäten und Sicherheit mobiler Endgeräte:** Die im Mai 2024 in Kraft getretene eIDAS-Verordnung 2.0 sieht unter anderem die Entwicklung einer sogenannten Europäischen Digitalen Identitäts-Wallet (EUDI-W) vor. Die EUDI-Wallet soll danach als elektronisches Identifizierungsmittel grenzüberschreitend nutzbar werden und neben klassischen Identitätsattributen, wie Vorname, Name etc., noch weitere Attribute, wie zum Beispiel Bildungsabschluss, Führerschein, in verifizierbarer Art für Diensteanbieter bereitstellen können. Zudem soll die EUDI-Wallet die Möglichkeit zur qualifizierten elektronischen Signatur bieten.

**Europäische Rechtsetzungen zur Cyberresilienz:** Die EU begegnet den Problemen im Cyberraum mit verschiedenen gesetzlichen Regelungen. Im aktuellen Berichtszeitraum wurde die Umsetzung der NIS-2-Richtlinie in nationales Recht vorbereitet. Die Richtlinie sieht insbesondere neue Meldepflichten über IT-Sicherheitsvorfälle für Betreiber sogenannter „wichtiger und besonders wichtiger Einrichtungen“ vor. In Deutschland umfasst dies mehrere Zehntausend Unternehmen und andere Organisationen. Damit dürfte nicht nur das Hellfeld zur Lage der Cybersicherheit in Deutschland deutlich erweitert werden. Auch die Umsetzung von Cybersicherheitsmaßnahmen wird künftig erleichtert, was zu einer Erhöhung des Cybersicherheitsniveaus führt.

Während bei NIS-2 die Betreiber und Nutzerinnen und Nutzer im Fokus stehen, beinhaltet der Cyber Resilience Act (CRA) Regelungen auf Produkt- und Herstellerebene. Der CRA wurde im März 2024 im Europäischen Parlament angenommen und nach Ende des Berichtszeitraums im Oktober 2024 beschlossen und damit final verabschiedet. Er regelt die Zugangsvoraussetzungen vernetzter Geräte (IoT) zum Europäischen Binnenmarkt – vom Saugroboter über Software bis hin zu Produkten, die in kritischen Sektoren

zum Einsatz kommen. Dies umfasst grundlegende Anforderungen an die Produkte wie Security by Design, Security by Default und Gewährleistung von Vertraulichkeit und Integrität der verarbeiteten Daten. Darüber hinaus beinhaltet der CRA Anforderungen an die Hersteller zum Umgang mit Schwachstellen, zum Beispiel die Verpflichtung, Sicherheitsupdates über den gesamten Lebenszyklus des Produkts bereitzustellen sowie Schwachstellen zu melden und zu beheben.

## 1.2 Systematik der BSI-Lagebeobachtung

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

### (1) Bedrohungen (engl. Threat)

Unter dem Stichwort Bedrohungen werden Phänomene in der Cyberwelt beschrieben, die eine Gefahr für die Cybersicherheit darstellen können. Diese Bedrohungen, im Folgenden „Cyberbedrohungen“ genannt, existieren unabhängig von konkreten Opfern oder konkreten Angriffen und können sich potenziell jederzeit in einem konkreten Angriff manifestieren. Zu den Cyberbedrohungen gehören beispielsweise Ransomware-Gruppen, Botnetze, neue Malware-Varianten, Exploits, Access Broker und APT-Gruppen. Der Begriff umfasst also die Angreifer, deren Angriffsinfrastrukturen und deren konkrete Angriffsmittel (vgl. *hauptsächlich Teil A Bedrohungslage, Seite 14*).

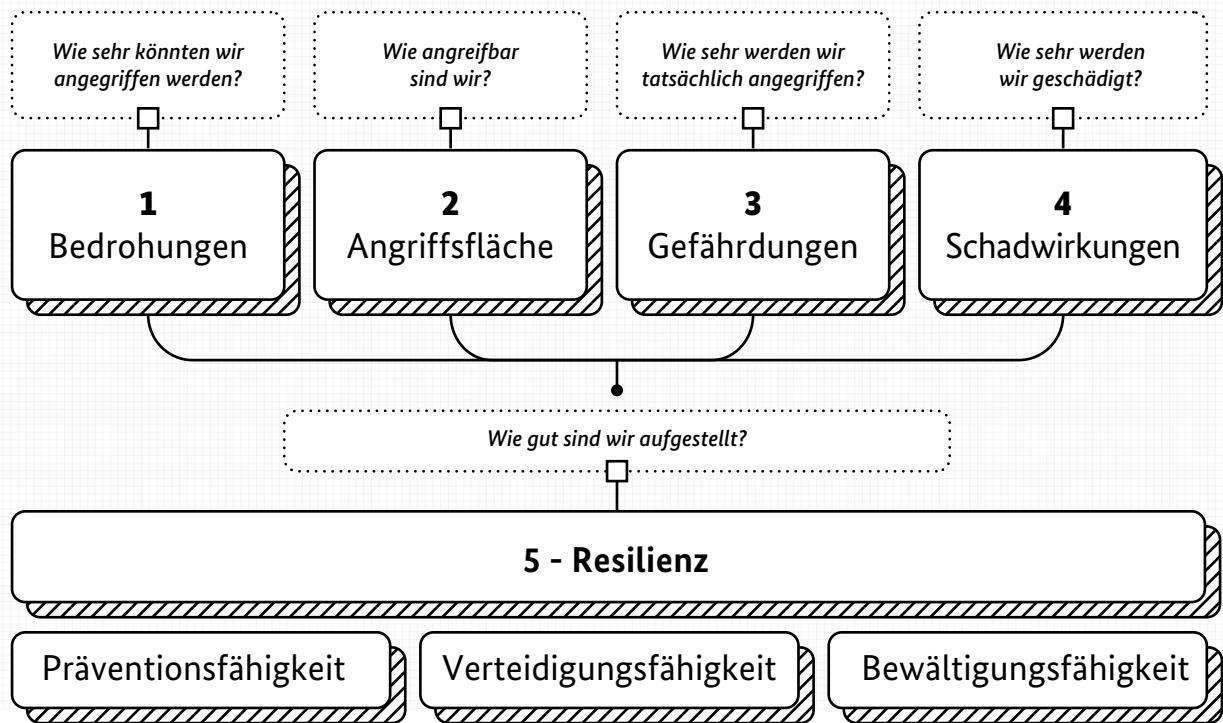


Abbildung 1: Systematik der BSI-Lagebeobachtung

## (2) Angriffsfläche (engl. Vulnerability)

Zur Angriffsfläche zählen alle IT-Systeme, Komponenten und Dienste, die ein Angreifer für einen Cyberangriff ausnutzen oder missbrauchen kann. Die größten Angriffsflächen im Cyberraum findet der Angreifer in Form von IP-Adressen, Domains und URLs sowie E-Mail-Adressen und Schwachstellen vor. Die Angriffsfläche für Cyberangriffe wächst simultan mit der Digitalisierung mit. Sie wächst jedoch auch schneller als Präventionsmaßnahmen, wenn diese nicht mithalten oder noch fehlen, wie etwa eine Segmentierung von Netzen oder ein wirksames Patchmanagement. Falsch konfigurierte Server oder schwachstellenbehaftete Anwendungen können die Folge sein (*vgl. hauptsächlich Teil B Angriffsfläche, Seite 30*).

## (3) Gefährdungen (engl. Attack)

Mit dem Begriff Gefährdungen sind konkrete Cyberangriffe gemeint. Wichtige Gefährdungen sind zum Beispiel Ransomware-Angriffe, bei denen Daten verschlüsselt oder exfiltriert werden, um Lösegeld von Opfern zu erpressen, oder Spionageangriffe durch APT-Gruppen, die Informationen oder Technologie in Form von Softwarecode stehlen wollen. Die Gefährdungslage kann sich je nach potenzieller Zielgruppe unterscheiden: Während beispielsweise Ransomware-Gruppen vorwiegend institutionelle Ziele in der Wirtschaft und der öffentlichen Verwaltung angreifen, richten sich Spam und Phishing hauptsächlich gegen Privatpersonen, das heißt Verbraucherinnen und Verbraucher (*vgl. vor allem Teil C Gefährdungslage, Seite 44*).

## (4) Schadwirkungen (engl. Impact)

Erfolgreiche Angriffe haben Schadwirkungen zur Folge. Beispielsweise werden wichtige Unternehmensdaten verschlüsselt oder exfiltriert, das Unternehmensnetzwerk kompromittiert oder eine Web-Dienstleistung lahmgelegt. Darüber hinaus haben Cyberangriffe unter Umständen mehr Opfer als angegriffene Ziele. So kann beispielsweise ein Ransomware-Angriff auf einen IT-Dienstleister zahlreiche weitere Opfer nach sich ziehen, die infolge von Service-Abschaltungen des IT-Dienstleisters mittelbar mit betroffen sind. Schadwirkungen eines einzelnen Angriffs können sich potenzieren und eine Vielzahl von Opfern zur Folge haben. Neben konkreten informationstechnischen Schäden kommt es in der Regel auch zu finanziellen Schäden, zum Beispiel zu entgangenen Einnahmen, Kosten für IT-forensische Untersuchungen, Wiederherstellungs-kosten und gegebenenfalls auch zu Reputationsschäden, wenn ein erfolgreicher Angriff bekannt wird.

## (5) Resilienz (engl. Resilience)

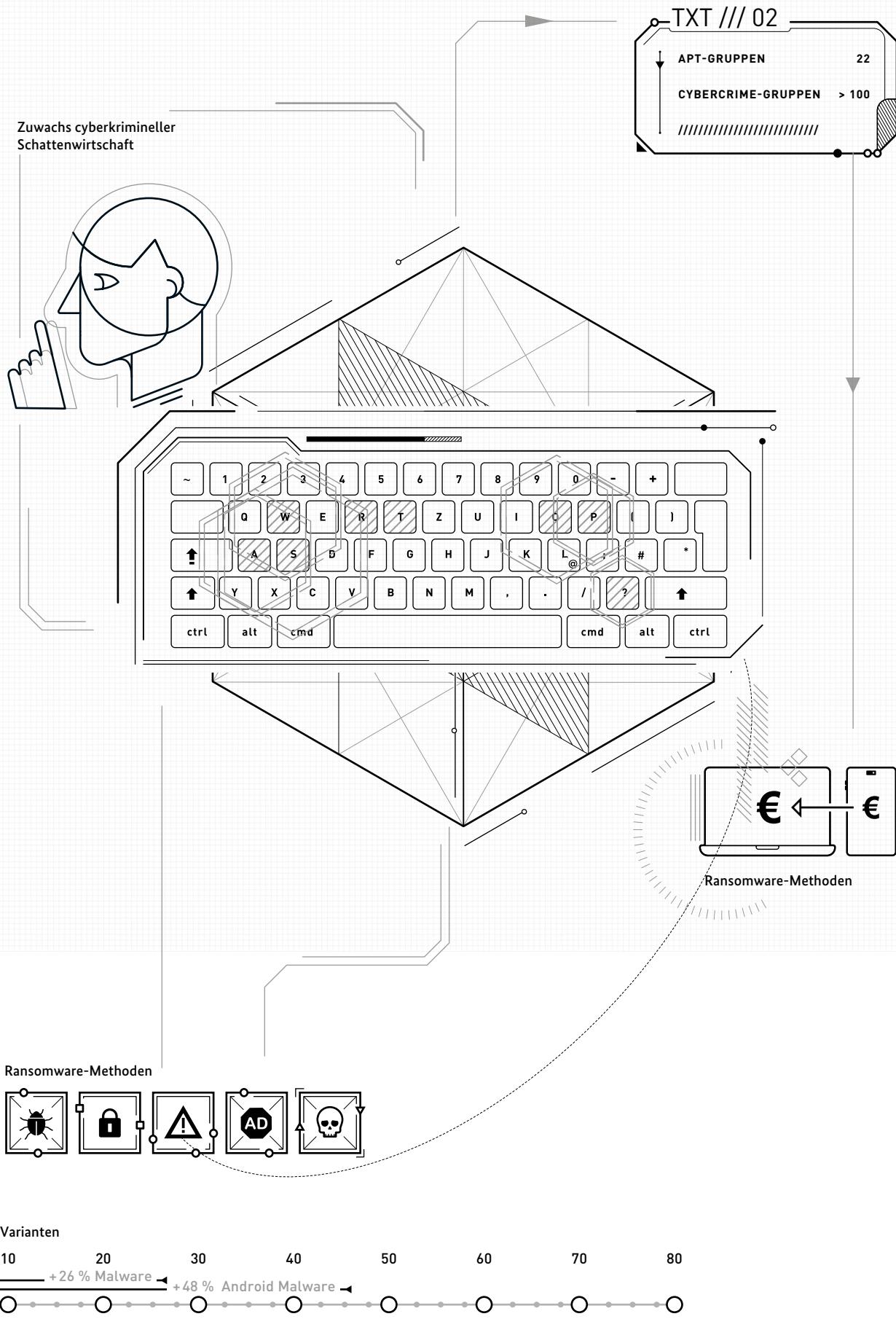
**Präventionsfähigkeiten:** Präventive Maßnahmen erhöhen die Resilienz potenzieller Opfer gegen Cyberbedrohungen. Zu den Präventionsmaßnahmen für lokale Netzwerke, wie etwa Unternehmensnetzwerke, gehören beispielsweise ein Informationssicherheitsmanagementsystem (ISMS) und ein Patchmanagement, aber auch Awarenessmaßnahmen und die Vorhaltung von qualifiziertem IT-Sicherheitspersonal. Präventive Maßnahmen haben das Ziel, die Angriffsfläche für Cyberangriffe zu verkleinern.

**Verteidigungsfähigkeiten:** Verteidigungsmaßnahmen schützen Opfer im Falle eines Cyberangriffs. Zu den klassischen Verteidigungsmaßnahmen zählen etwa Systeme zur Angriffserkennung, zum Beispiel Antivirenprogramme, und eine wirksame DDoS-Mitigation. Verteidigungsmaßnahmen zielen darauf ab, konkrete Angriffe abzuwehren.

**Bewältigungsfähigkeiten:** Hundertprozentige Sicherheit gibt es nicht und trotz bestehender Präventions- und Verteidigungsmaßnahmen können Cyberangriffe erfolgreich sein. Bewältigungsfähigkeiten zielen darauf ab, die Schadwirkungen so gering wie möglich zu halten und die betroffenen Systeme und Prozesse möglichst schnell wieder in den Normalbetrieb zu überführen. Ein funktionierender, geübter Plan für den IT-Notfall gehört in staatlichen und öffentlichen sowie wirtschaftlichen Institutionen ebenso dazu wie rückspielbare Backups. Für Verbraucherinnen und Verbraucher wird digitale Kompetenz immer bedeutsamer, um etwa eine Phishing-E-Mail erkennen und sich richtig verhalten zu können.

Resilienz ist ein wichtiger Schlüssel zu einer sicheren Digitalisierung in einer erfolgreichen Cybernation Deutschland, die den Cyberbedrohungen aus dem Internet immer einen Schritt voraus ist. Für die Erhöhung der Resilienz in Staat, Wirtschaft und Gesellschaft ergreift das BSI vielfältige Maßnahmen. Einige davon werden in Teil D dieses Berichts besonders herausgestellt (*vgl. Teil D: Resilienz, Seite 76*).

# A BEDROHUNGSLAGE



## 2 – Schadprogramme

---

Computerprogramme, die schädliche Operationen ausführen, werden als Schadprogramme (engl. Malware) bezeichnet. Zum Beispiel durch maliziöse E-Mail-Anhänge oder Links, auf die geklickt wird, kann sich ein Schadprogramm installieren. Auch manipulierte Links auf Webseiten oder manipulierte legitime Software, die zum Beispiel durch Supply-Chain-Angriffe in Umlauf kommt, sind typische Angriffsvektoren. In der Regel nutzen Schadprogramme zur Infektion von Computersystemen vorhandene Schwachstellen in Soft- und Hardware aus.

### 2.1 Neue Schadprogramme

Nimmt ein Angreifer an einem Schadprogramm Änderungen vor, entsteht eine neue Schadprogramm-Variante. Als neu gilt jede Variante, die im Hinblick auf ihre Prüfsumme (Hashwert) einzigartig ist. Während für bekannte Schadprogramm-Varianten Detektionsmethoden existieren, sind neue Varianten unmittelbar nach ihrem Auftreten unter Umständen noch nicht als Schadprogramm erkennbar und daher besonders gefährlich.

Im Berichtszeitraum wurden täglich durchschnittlich 309.000 neue Schadprogramm-Varianten bekannt (vgl. Abbildung 2, Seite 16). Das waren rund 26 Prozent mehr als im vergangenen Berichtszeitraum mit durchschnittlich täglich 250.000 neuen Schadprogramm-Varianten. Der Anstieg war insbesondere auf eine deutliche Zunahme neuer Schadprogramm-Varianten zurückzuführen, die Schwachstellen in 64-Bit-Varianten von Windows ausnutzen (+256 %). Zudem legten Android-Varianten im Berichtszeitraum überdurchschnittlich stark zu (+48 %). Nach der Abschaltung (engl. Takedown) des Flubot-Botnetzes, das für viele Infektionen mobiler Systeme verantwortlich war (vgl. Die Lage der IT-Sicherheit 2022, Seite 25), war das Aufkommen neuer Android-Schadprogramme im Juni 2022 zunächst eingebrochen. Das Wachstum im aktuellen Berichtszeitraum dürfte daher auf den neuerlichen Aufbau von Android-Angriffsinfrastrukturen hindeuten, wobei die Angreifer das Niveau aus der Zeit vor dem Take-down noch nicht wieder erreicht haben.

Schutz gegen Angriffe mit Schadprogrammen bietet neben regelmäßigen Sicherheitsupdates unter anderem Antivirensoftware, die die Schadprogramme entdecken, an einer erfolgreichen Ausführung hindern und vom System wieder entfernen kann. Manche Angriffe nehmen aber auch tiefgreifende Veränderungen am infizierten System vor, die sich nicht einfach rückgängig machen lassen.

### 2.2 Botnetze

Als Botnetz bezeichnet man den Zusammenschluss mehrerer mit einem Schadprogramm infizierter Systeme (Bots), die Kontakt zu einem oder mehreren zentralen Steuerungssystemen (Command-and-Control-Server, C2-Server) der Angreifer aufnehmen und von diesen ferngesteuert werden. Neben klassischen Bürocomputersystemen können Angreifer auch alle anderen internetfähigen Geräte mit einem Schadprogramm infizieren und in ein Botnetz integrieren. Das betrifft zum Beispiel Geräte wie Smartphones, Tablets, Router oder auch IoT-Geräte wie zum Beispiel Fernseher, Set-Top-Boxen, Webcams etc. Solche Geräte können mittels Schadprogrammen oder direkt über das Internet angegriffen werden. Im ersten Fall schleusen Angreifer in legitime Programme Schadcode ein, den die Nutzerinnen und Nutzer dann unwissentlich installieren, beispielsweise gemeinsam mit Systemupdates oder Apps. Im zweiten Fall nutzen Angreifer Schwachstellen in den Betriebssystemen der Geräte, um diese ohne Zutun des Systembesitzers über das Internet automatisiert zu kompromittieren.

Typischerweise sind aktuelle Botnetze modular aufgebaut, sodass die Angreifer die Funktionalitäten, die sie für bestimmte Angriffe benötigen, flexibel nachladen und anpassen können. So können die infizierten Systeme multifunktional eingesetzt und für verschiedene Arten von Angriffen genutzt werden. Die Schadfunktionalitäten können sich hierbei gezielt gegen die Nutzerinnen und Nutzer des Systems richten, beispielsweise für Informations- und Identitätsdiebstahl, Datenverschlüsselung, Cryptomining, oder das System zum Angriff Dritter missbrauchen, zum Beispiel für DDoS-Angriffe, Spamversand etc.

## Durchschnittlicher täglicher Zuwachs neuer Schadprogramm-Varianten

Anzahl in Tausend

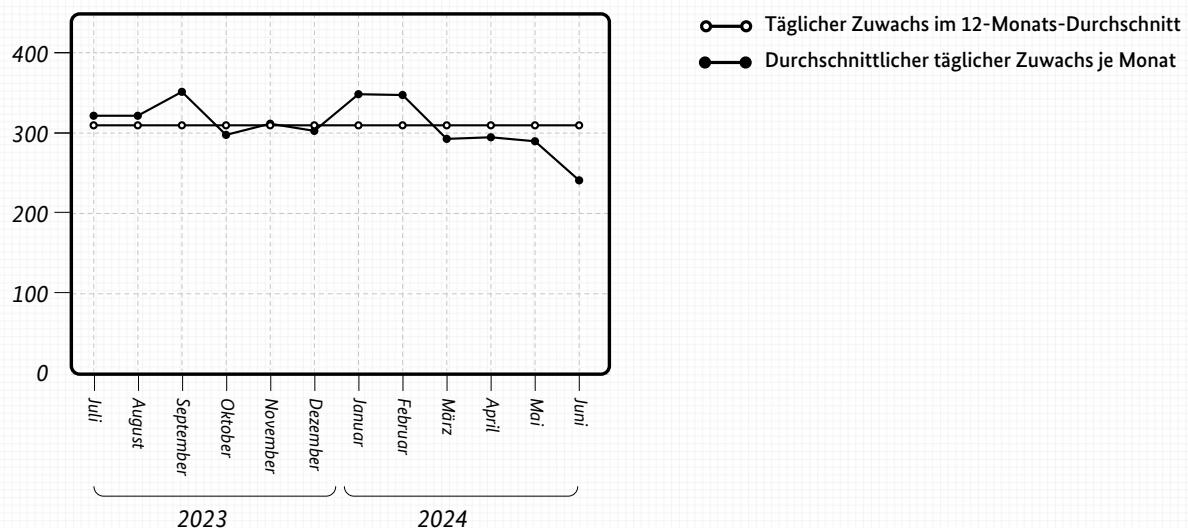


Abbildung 2: Durchschnittlicher täglicher Zuwachs neuer Schadprogramm-Varianten (Anzahl in 1.000)

## Durchschnittlicher täglicher Zuwachs neuer Android-Schadprogramm-Varianten

Anzahl

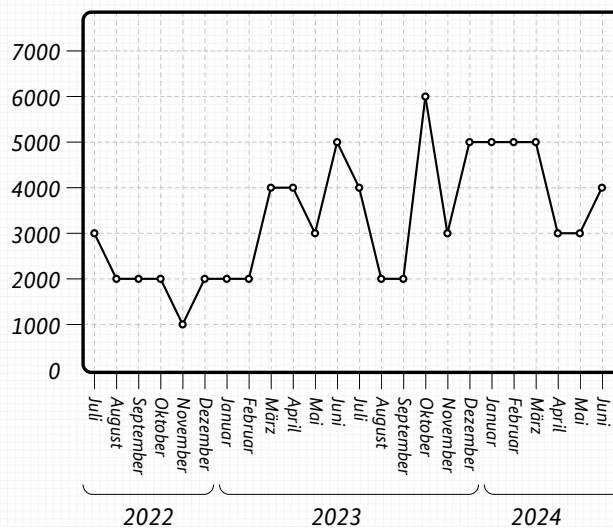


Abbildung 3: Durchschnittlicher täglicher Zuwachs neuer Android-Schadprogramm-Varianten

### Abbildung 2 & 3 / Malware-Statistik:

**Ziel der Statistik** Stand und die Entwicklung des neu bekannt gewordenen Schadprogramm-Aufkommens im Internet insgesamt. Berichtet wird monatlich. / **Grundgesamtheit** Alle im Internet verfügbaren Programme, die schädliche Operationen durchführen können, identifiziert anhand ihres Hashwertes. / **Stichprobe** Alle Detektionen des Instituts AV-Test GmbH und von dessen Kunden. / **Erhebungsdesign/-instrumente** Tagesaggregation der Detektionen aus Virenscannern, Spamfiltern, Spam-Traps, Sinkholes, Honeypots. / **Reichweite** Keine Aussagen über tatsächliche Angriffe möglich. / **Qualitätsbewertung** Vergleichsweise genau für das erfasste Hellfeld. Über das Dunkelfeld unbekannter Schadprogramme liegen keine Erkenntnisse vor.

Im Berichtszeitraum wurden Botnetze in erster Linie zum Diebstahl persönlicher Informationen, zum Komromittieren und zum Missbrauch von Onlinebanking-Zugängen sowie zur Verteilung weiterer Schadprogramme verwendet. Dabei standen im aktuellen Berichtszeitraum mobile Geräte mit Android-Betriebssystemen wieder im Fokus der Angreifer. Sechs der zehn aktivsten in Deutschland bekannten Botnetze richteten sich gegen Android-Geräte. Sie waren für 71,4 Prozent der Infektionen verantwortlich (vgl. Abbildung 4, Seite 18). Daher lag einer der Schwerpunkte der Lagebeobachtung des BSI weiterhin auf dieser Art von Botnetzen.

Smartphones sind besonders attraktive Ziele für Angreifer, denn sie sind zunehmend multifunktional einsetzbar. Vom Bezahlen an der Supermarktkasse über das Onlinebanking und das soziale Netzwerken bis hin zum Steuern smarter Heimgeräte und zum Monitoring der persönlichen Fitness: Auf kaum einem anderen Gerät sammeln sich heutzutage derart zahlreich passwortgeschützte Funktionen in Apps mit sensiblen Datenbeständen an wie auf Smartphones. Botnetze wie etwa ArrkiiSDK, das mit 20,5 Prozent der Unique IPs größte der im Sinkholing beobachteten Botnetze in Deutschland, ermöglichen daher neben missbräuchlicher Benutzerverfolgung und Werbetrug auch die stille Installation zusätzlicher Anwendungen ohne Zustimmung der Benutzenden. Den Angreifern hinter Botnetzen wie ArrkiiSDK ist es daher beispielsweise möglich, Spyware zu installieren, um Zugangsdaten der Benutzenden auszulesen und anschließend etwa an Ransomware-Gruppen weiterzuverkaufen (vgl. zu Access Brokern Kapitel Cyberkriminelle Schattenwirtschaft, Seite 19).

Darüber hinaus ist im Berichtszeitraum das Botnetz Socks5Systemz aufgefallen, das Windows-Systeme infiziert und sie in sogenannte Proxys verwandelt. Dabei handelt es sich um Systeme, die fremden Internetverkehr weiterleiten können, sodass der echte Absender nicht mehr feststellbar ist. Botnetzbetreiber vermieten solche Systeme auch zum Verteilen weiterer Schadprogramme sowie zur Umgehung regionaler Beschränkungen, zum Beispiel bei Streamingdiensten. Besonders nützlich sind sie aber vor allem im Rahmen von Cyberspionageangriffen zur Verschleierung der Absenderadressen von maliziösem Internetverkehr (vgl. dazu auch Kapitel APT-Gruppen, Seite 22).

Das BSI erfasst infizierte Systeme über sogenannte Sinkholes. Dabei handelt es sich um Server, die stellvertretend für die Steuerungssysteme der Angreifer die Kommunikation von Bots entgegennehmen und protokollieren. Im Berichtszeitraum wurden täglich durchschnittlich rund 20.650 infizierte Systeme erfasst und an die deutschen Provider gemeldet. Die Provider ermitteln anhand der

bereitgestellten Daten die betroffenen Kundinnen und Kunden und benachrichtigen diese. Eine Beschreibung des Sinkholing-Verfahrens sowie Steckbriefe zu den am häufigsten gemeldeten Botnetzen finden sich auf der BSI-Webseite.

#### Weiterführende Informationen zu Botnetzen:



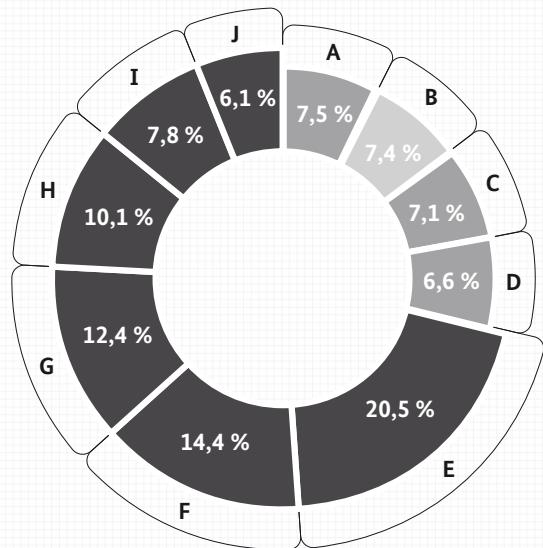
Auch basierend auf den Erfahrungswerten von Takedowns (vgl. z. B. Vorfällskasten Takedowns, Seite 52) ist davon auszugehen, dass die Gesamtzahl infizierter Systeme deutlich höher liegt. Dies liegt daran, dass einerseits in vielen Fällen Mehrfachinfektionen vorliegen, andererseits nur ein Teil der weltweit aktiven Botnetze durch klassisches Sinkholing erfasst werden kann. So ergreifen die Angreifer hinter prominenten Botnetzfamilien Maßnahmen gegen das Sinkholing, wie beispielsweise die Nutzung fester IP-Adressen, getunnelter DNS-Verbindungen (DNS over HTTPS, DoH) oder von Blockchain-Techniken zur Verschleierung der Kommunikation zwischen Steuerungsservern und Bots. Der Trend der letzten Jahre zeigt ebenfalls eine zunehmende Professionalisierung der Angreifer.

Wie auch in den Vorjahren ist die Bedrohungslage durch Botnetze hoch. Aus den vorgenannten Gründen stellen die aus dem Sinkholing ermittelten Infektionszahlen lediglich eine Untergrenze dar. Die zunehmend steigende Anzahl internetfähiger Geräte sorgt für ein Wachstum der Angriffsfläche, da insbesondere günstige Massen-IoT-Geräte oftmals nur kurze Supportzyklen durch die Hersteller haben und gravierende Schwachstellen nicht zeitnah oder überhaupt nicht geschlossen werden. Verwundbare Geräte können mit einfachen Mitteln von Angreifern im Internet gefunden und mit geeigneten Tools komromittiert werden.

Dies ermöglicht es auch Angreifern mit vergleichsweise wenig technischen Ressourcen, Systeme zu infizieren, um eigene Botnetze aufzubauen.

## Unique-IP nach den Top-10-Botnetzen

Anteil in %



### Betriebssystem Botnetz

Betriebssystem	Botnetz
A	Windows
B	Linux
C	Windows
D	Windows
E	Android
F	Android
G	Android
H	Android
I	Android
J	Android

Abbildung 4: Infizierte Systeme (Unique IP) Juli 2023 bis Juni 2024 nach den Top-10-Botnetzen (Anteile)

### Abbildung 4 / Botnetz-Struktur-Statistik:

**Ziel der Statistik** Strukturerhebung bekannter Botnetze weltweit. Berichtet wird monatlich. / **Grundgesamtheit** Alle Botnetze weltweit, die von Sinkhole-Servern aufgegriffen werden können. / **Stichprobe** Bewusste Auswahl der rund 300 bedrohlichsten Botnetze für das BSI-Sinkholing. / **Erhebungsdesign/-instrumente** Monatsaggregation einer laufende Erhebung der IP-Adressen, die mit den BSI-Sinkholing-Servern Kontakt aufnehmen. / **Reichweite** Infizierte Systeme (Bots) weltweit, darunter Deutschland. Es kann technisch nur ein Teil der weltweit aktiven Botnetze über Sinkholing erfasst werden. / **Qualitätsbewertung** Aufgrund von technischen Kapazitätsgrenzen kann das BSI nur einen kleinen Teil der infizierten Systeme (Bots) beobachten. Aussagen über Anzahlen infizierter Systeme sind daher nicht möglich.

## 3 – Ransomware-Gruppen

Als Ransomware werden Schadprogramme bezeichnet, die dem Opfer den Zugriff auf ein angegriffenes System verwehren und erst gegen eine Lösegeldzahlung wieder freigeben. Die ersten Formen von Ransomware setzten hierfür beispielsweise auf ein Sperren des Bildschirms. Heutzutage wird Ransomware überwiegend zum Verschlüsseln von Daten verwendet, die für den Betroffenen relevant sind. Hierbei kann es sich um jede Form von digitalem Gut handeln, von einfachen Dokumenten über Patientenakten bis hin zu ganzen Datenbanken und Systemsicherungen. Ransomware-Angreifer erpressen also, indem sie zunächst die Kontrolle über Daten und Systeme eines Betroffenen übernehmen und sodann als Gegenleistung für die Wiederherstellung der Verfügbarkeit und Vertraulichkeit der Daten und Systeme ein Lösegeld fordern. Eine solche Vorgehensweise wird Ransomware-Angriff genannt.

Es gibt jedoch keine Garantie dafür, dass die Angreifer die verschlüsselten Daten tatsächlich wieder freigeben oder die gestohlenen Daten tatsächlich löschen, auch wenn ein Lösegeld gezahlt wurde. Auch besteht die Möglichkeit, dass das vom Angreifer zur Verfügung gestellte Entschlüsselungstool fehlerhaft ist. Zudem müssen einmal ausgeleitete Daten grundsätzlich als kompromittiert betrachtet werden. Das BSI rät daher prinzipiell von der Zahlung eines Lösegelds ab.

Potenzielle Opfer sind Institutionen jeder Art und Größe – vom Kleinstunternehmen über Behörden und KRITIS-Unternehmen bis hin zu internationalen Konzernen, von der Kommunalverwaltung über Krankenhäuser bis hin zu wissenschaftlichen Einrichtungen, Schulen und Universitäten. Darüber hinaus werden dem BSI hin und wieder Massenkampagnen bekannt, die auch Verbraucherinnen und Verbraucher direkt betreffen.

Ransomware-Angriffe werden überwiegend aus finanziellen Motiven von kriminellen Angreifern verübt. Allerdings können auch APT-Gruppen Ransomware nutzen, um andere Angriffe zu verschleiern oder von diesen abzulenken (vgl. Kapitel APT-Gruppen, Seite 22). Zudem kann Ransomware auch zur reinen Sabotage eingesetzt werden. In diesem Fall wird die Ransomware ähnlich wie ein sogenanntes Wiper-Schadprogramm, welches Daten löscht, eingesetzt: Daten werden so verschlüsselt, dass sie sich technisch nicht wiederherstellen lassen.

Das BSI stellt Empfehlungen und Maßnahmen gegen Ransomware zentral zur Verfügung<sup>1</sup>. Zusammenfassend nach Angriffsphasen wurden Gegenmaßnahmen auch in *Die Lage der IT-Sicherheit 2023 (Seite 22 f.)* des BSI aufgeführt. Diese haben weiterhin Gültigkeit.

### 3.1 Cyberkriminelle Schattenwirtschaft

Finanziell motivierte Angriffe werden von einer ganzen Schattenwirtschaft aus kriminellen Dienstleistungen rund um den Cyberangriff begleitet. Diese wird auch als Cybercrime-as-a-Service (CCaaS, Cyberstrafat als Dienstleistung) bezeichnet. Diese CCaaS können einen Cyberkriminellen bei nahezu jedem Aspekt eines Cyberangriffs unterstützen. So bieten CCaaS beispielsweise Schadprogramme an oder unterstützen bei weiteren kriminellen Handlungen wie der Erpressung oder Geldwäsche (vgl. *Die Lage der IT-Sicherheit in Deutschland 2023, Seite 16 ff.*). Neue Methoden werden früher oder später in CCaaS aufgegriffen und damit vielen Angreifern zugänglich gemacht. Im aktuellen Berichtszeitraum betraf dies insbesondere sogenannte EDR-Killer sowie die Ausnutzung von sogenannten Zero-Day-Schwachstellen durch Ransomware-Gruppen.

#### 3.1.1 Malware-as-a-Service EDR-Killer

Zum Schutz von Systemen wird immer häufiger neben Antivirensoftware auch Software namens Endpoint Detection and Response (EDR) eingesetzt. Während Antivirensoftware zu dem Zeitpunkt Dateien untersucht, wenn ein Virenscan ausgeführt wird oder wenn eine Datei per E-Mail auf einem System eingeht, laufen EDR-Programme permanent. Das Ziel solcher Software ist es, mittels Signaturen und Verhaltensheuristiken im laufenden Systembetrieb Anomalien festzustellen, zum Beispiel ob sich ein ausgeführtes Programm maliziös verhält. Angreifer versuchen auf verschiedene Arten, einer Detektion durch eine Antiviren- oder EDR-Software zu entgehen. Als EDR-Killer werden Tools bezeichnet, die dazu dienen, die auf einem kompromittierten System installierte EDR-Software zu beenden und wenn möglich zu entfernen.

Viele EDR-Killer missbrauchen legitime, aber verwundbare Treiber von Antiviren- und EDR-Software. Diese Vorgehensweise ist auch bekannt als Bring Your Own Vulnerable Driver (BYOVD). Antiviren- und EDR-Software erfordert häufig für einen reibungslosen Betrieb, dass andere Antiviren- und EDR-Software deinstalliert wird, da solche Software zur Erkennung verdächtigen Verhaltens vergleichsweise tief in Prozessabläufe eingreift. Mehrere parallel laufende EDR-Programme würden eher zu Fehlern führen, da sie sich zum Beispiel gegenseitig behindern. Daher deinstallieren die Treiber konkurrierende EDR-Software. Diese und ähnliche Funktionalitäten machen sich Angreifer bei verwundbaren Treibern zunutze.

Das Ziel der Angreifer ist es, die Detektion ihrer Aktivitäten hinauszögern und möglichst wenige Spuren zu hinterlassen. Das BSI hat im Berichtszeitraum beobachtet, dass mehrere EDR-Killer als Malware-as-a-Service (MaaS) angeboten wurden. Dies dürfte eine Reaktion der Angreifer auf den zunehmenden Einsatz von EDR-Software zur Angriffsdetektion und -bewältigung sein.

### **3.1.2 Ausnutzen von Zero-Day-Schwachstellen durch Ransomware-Angreifer**

Einmal veröffentlichte Exploits, das heißt Schadprogramme zur Ausnutzung einer konkreten Schwachstelle, werden zeitnah von anderen Angreifern adaptiert. Im Berichtszeitraum hat das BSI zudem die Ausnutzung von Zero-Day-Schwachstellen durch Ransomware-Angreifer beobachtet. So haben beispielsweise die Angreifer hinter der Ransomware- und Leak-Seite Clop mehrfach gezielt Zero-Day-Schwachstellen in File-Sharing-Servern für groß angelegte Angriffskampagnen ausgenutzt. In den vom BSI beobachteten Vorfällen gibt es Hinweise darauf, dass die Angreifer mehrere Tage oder Wochen im Voraus eine Infrastruktur für den Angriff vorbereitet haben. Die Angreifer stellten sich also auf ein Wettrennen ein, um möglichst viele Daten mit dem Ziel der Erpressung zu stehlen, bevor die verwundbaren Server vom Netz genommen und ggf. bereinigt werden können.

Es ist davon auszugehen, dass auch in Zukunft Ransomware-Angreifer Zero-Day-Schwachstellen ausnutzen werden. Dafür muss die jeweilige Angreifergruppe nicht selbst über das technische Know-how zur Identifikation der Schwachstelle und Entwicklung eines Exploits verfügen. Aufgrund der bereits in den letzten Jahren erbeuteten Lösegelder in Millionenhöhe stehen den Angreifern ausreichend Mittel zur Verfügung, um beispielsweise die Suche nach einer ausnutzbaren Zero-Day-Schwachstelle bei kriminellen Dienstleistern zu beauftragen oder etwa einen Exploit oder Proof of Concept zu kaufen.

## **3.2 Für Deutschland relevante Ransomware-Gruppen**

Das BSI beobachtet mehr als 100 cyberkriminelle Gruppen, die in Deutschland aktiv sind. Dabei sind die fünf aktivsten Gruppen regelmäßig für rund die Hälfte der mutmaßlichen Opfer verantwortlich, die von Angreifern auf deren Leak-Seiten genannt werden (vgl. Abbildung 5, Seite 21).

Die Ransomware-Gruppe hinter der Ransomware-as-a-Service LockBit war im aktuellen Berichtszeitraum sowohl in Deutschland als auch weltweit am aktivsten. Strafverfolger berichteten von weltweit mehr als 2.500 Ransomware-Opfern dieser Gruppe in den vergangenen Jahren. Allein in Deutschland veröffentlichte die Gruppe im Berichtszeitraum 40 mutmaßliche Leak-Opfer auf ihrer Leak-Seite. Weltweit sollen es im selben Zeitraum 944 Leak-Opfer gewesen sein. Nach dem Takedown im Februar 2024 war die Gruppe weiter aktiv, jedoch bis zum Redaktionsschluss des vorliegenden Berichts noch weit von ihrem früheren Aktivitätsniveau entfernt.

Weiter dominant war im Berichtszeitraum in Deutschland auch die seit 2022 bekannte Gruppe hinter der Ransomware-as-a-Service Black Basta. Die Gruppe nutzte wiederholt Schwachstellen, die teilweise bereits seit mehreren Jahren bekannt sind. Im aktuellen Berichtszeitraum nannte die Gruppe 21 mutmaßliche Opfer aus Deutschland auf ihrer Leak-Seite.

Die Ransomware-Gruppe hinter der RaaS 8Base, deren Aktivitätsfokus bisher in Nord- und Südamerika lag, ist seit Mitte 2023 auch in Deutschland unter den Top 5 der RaaS. 8Base greift Opfer aus allen Branchen an und nannte im Berichtszeitraum mindestens 15 mutmaßliche Leak-Opfer aus Deutschland auf ihrer Leak-Seite. Für die Erstinfektion setzten die Angreifer wiederholt auf Zugänge von Access Brokern.

Die Ransomware-Gruppe hinter der RaaS Play ist bereits im Jahr 2023 durch ihre Aktivität gegen deutsche Organisationen aufgefallen. Dabei wurden 13 mutmaßliche Opfer auf der Leak-Seite der Gruppe veröffentlicht. Die Gruppe nutzte wiederholt für die Erstinfektion Schwachstellen in exponierten Services wie VPNs oder Mail-Servern. Wie andere Gruppen kaufen die Angreifer aber auch Zugänge von Access Brokern.

Access Broker gewinnen insgesamt an Bedeutung. Auch die Ransomware-Gruppe hinter Cloak kaufte im Berichtszeitraum kompromittierte Zugangsdaten legitimer Accounts, um Netzwerke initial zu infizieren. Deutschland

steht besonders im Fokus der Gruppe. Im Berichtszeitraum nannten die Angreifer zwölf mutmaßliche Opfer aus Deutschland auf ihrer Leak-Seite und spielten damit unter den Top-5-Leak-Seiten in Deutschland, wohingegen die Gruppe weltweit betrachtet nicht unter die Top 25 fällt.

## Top-5-Leak-Seiten Juli 2023 bis Juni 2024

Nach Anzahl der Leak-Opfer

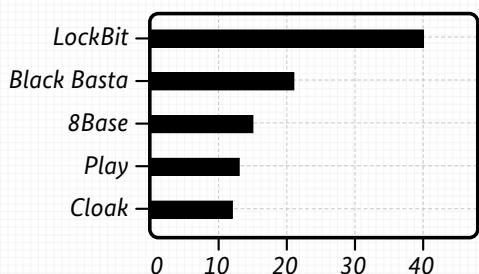


Abbildung 5: Top-5-Leak-Seiten Juli 2023 bis Juni 2024 nach Zahl der Leak-Opfer (Anzahl)

Abbildung 5: Top-5-Leak-Seiten Juli 2023

bis Juni 2024 nach Zahl der Leak-Opfer (Anzahl)

**Ziel der Statistik** Erhebung der Opfer von Daten-Leaks, die nach einem Ransomware-Angriff kein Löse-/Schweigegeld gezahlt haben und deren Daten daher auf einer Leak-Webseite einer Angreifergruppe veröffentlicht wurden, um den Erpressungsdruck zu erhöhen. Berichtet wird quartalsweise. / **Grundgesamtheit** Alle dedizierten Leak-Seiten, auf denen die Daten von Opfern von Daten-Leaks, die aus gezielten Cybercrime-Angriffen (Ransomware-Angriffe und Angriffe gegen neue Schwachstellen) stammen, veröffentlicht wurden. / **Stichprobe** Vollerhebung der bekannt gewordenen Leak-Opfer. / **Erhebungsdesign/-instrumente** Detektion von Daten-Dienstleistern, Meldungen von Opfern und öffentlichen Quellen. / **Reichweite** Keine Aussage über Anzahl der zugrundeliegenden Angriffe, sondern über die Anzahl zahlungsunwilliger Opfer, deren Daten auf einer Leak-Seite veröffentlicht wurden. Keine Unterscheidung von Ransomware-Opfern und Opfern von Datenexfiltration durch Schwachstellenausnutzung. / **Qualitätsbewertung** Hohe weltweite Abdeckung mit Abgleich verschiedener Datenquellen.

## 4 – APT-Gruppen

---

Während Schadprogramme von kriminellen Angreifern in der Regel massenhaft und ungezielt verteilt werden (*vgl. Kapitel Ransomware-Gruppen, Seite 19*), sind APT-Angriffe oft langfristig und mit großem Aufwand geplante Angriffe auf einzeln ausgewählte, herausgehobene Ziele. APT-Angriffe dienen also in der Regel nicht der kriminellen Gewinnerzielung, sondern der Beschaffung von Informationen über das Ziel und gegebenenfalls der Sabotage.

Im aktuellen Berichtszeitraum waren nach Kenntnis des BSI 22 verschiedene APT-Gruppen in Deutschland aktiv, deren Angriffe auf Behörden und Unternehmen insbesondere der auswärtigen Angelegenheiten, der Verteidigung sowie der öffentlichen Sicherheit und Ordnung zielten. Darüber hinaus gab es eine Reihe von Entwicklungen, die die APT-Bedrohungslage prägten.

### 4.1 Cyberaktivitäten im Rahmen geopolitischer Spannungen und Konflikte

Auch im aktuellen Berichtszeitraum zeigte sich, dass geopolitische und zwischenstaatliche Konflikte oftmals mit einer ganzen Bandbreite an Phänomenen im Cyberraum einhergehen. Desinformation, Hacktivismus, Spionage und Sabotage waren sowohl im russischen Angriffskrieg gegen die Ukraine als auch in der Folge des Terrorangriffs der Hamas auf Israel vom Oktober 2023 zu beobachten. Dabei blieb ein großer Teil der Cyberaktivitäten regional begrenzt. Kollateralschäden bei Drittstaaten können allerdings nie ausgeschlossen werden, insbesondere wenn technische oder organisatorische Beziehungen zu einer Konfliktpartei bestehen.

Die in den genannten Konflikten beobachteten Cybersabotage-Angriffe sind in den allermeisten Fällen technisch einfach gewesen. Statt komplexer Angriffe auf Prozesssteuerungsanlagen (*vgl. dazu etwa Industroyer, Die Lage der IT-Sicherheit 2022, Seite 51*) wurden meist einfache WiPer in Büronetzen eingesetzt. Geopolitische Spannungen führten also bisher nicht – wie mancherorts befürchtet – dazu, dass Angreifer zuvor entwickelte, fortschrittliche Cybersabotagemittel eingesetzt hätten. Diese Beobachtung muss aber nicht zwangsläufig für andere Akteure in zukünftigen Konflikten gelten.

Die beobachteten einfachen Sabotageangriffe, die meist wenig nachhaltige Schäden anrichteten, wurden oftmals durch Desinformation und Propaganda begleitet, um den Schaden übertrieben darzustellen. Dasselbe Phänomen wurde bei hacktivistischen DDoS-Angriffen beobachtet (*vgl. dazu auch Die Lage der IT-Sicherheit 2023, Seite 30*). Diese halten in der Regel nur für kurze Zeit an und erzeugen ebenfalls kaum nachhaltige Schäden. In sozialen Netzwerken werden die Störungen von den Angreifern aber als massiv und relevant dargestellt, um deren Wirkung in der Bevölkerung und auf die öffentliche Meinung zu maximieren. Hacktivismus und Cybersabotage zielen im Berichtszeitraum daher vor allem darauf ab, eine diffuse Unsicherheit in der öffentlichen Wahrnehmung zu erzeugen. In diesem Sinne bedeutet Vorfallsbewältigung in geopolitischen Spannungszeiten auch Öffentlichkeitsarbeit, um Angriffe in einen fachlich korrekten Kontext setzen und bewerten zu können.

Der Konflikt zwischen Israel und der Hamas ist ein weiteres Beispiel für den Einsatz von Cybermitteln in einer eskalierten Lage. Es zeigte sich aber auch, dass verschiedene Konflikte jeweils unterschiedliche Phänomene im Cyberraum mit sich bringen. Beispielsweise konnten laut Medienberichten die israelischen Streitkräfte bei ihrem Einsatz im Gazastreifen Server sicherstellen, die sie der Hamas zuordneten. Darauf seien Hinweise gefunden worden, dass im Vorfeld des Überfalls der Hamas im Oktober 2023 Überwachungskameras in israelischen Städten an der Grenze zum Gazastreifen kompromittiert worden waren. Außerdem seien Daten von kompromittierten Smartphones israelischer Militärangehöriger gestohlen worden. Die in diesen Spionageoperationen gesammelten Daten seien geeignet gewesen, den Überfall auf die israelischen Grenzregionen zu unterstützen. Allerdings gibt es derzeit keine Hinweise, dass der Überfall selbst durch Cybersabotage begleitet worden wäre. Dies ist ein Unterschied zu der Invasion russischer Streitkräfte im Februar 2022 in der Ukraine, zu deren Beginn unter anderem Cybersabotage gegen militärische Kommunikationssysteme beobachtet wurde. Ein weiterer Unterschied ist, dass sich im Rahmen des Gaza-Konflikts infolge des Überfalls der Hamas auf Israel deutlich mehr Hacktivismus-Gruppen, deren Mitglieder nach eigener Aussage aus verschiedenen Ländern kommen, zu Angriffen auf israelische Ziele bekennen, als dies im Rahmen des russischen Kriegs gegen die Ukraine der Fall ist.

Zudem schrieben sich Hacktivisten oder strategisch motivierte Akteure, die nur vorgaben, Hacktivisten zu sein, wiederholte Vorfälle zu, bei denen sie Angriffe auf ICS-Systeme durchgeführt haben wollten. Beispielsweise griff eine Gruppe namens CyberAv3ngers auf Unitronics-Systeme zu, die unter anderem für die Wasseraufbereitung in den USA verwendet wurden. Die Angriffsvektoren waren dabei technisch einfach und machten sich schwache Passwörter und weitere mangelnde Sicherheitsvorkehrungen wie Zugriffbarkeit aus dem Internet zunutze.

Angesichts der massiven Schäden und Kosten, die weltweit durch Ransomware verursacht werden, sieht das BSI mit Sorge die Möglichkeit, dass sich strategisch motivierte Akteure im Rahmen von geopolitischen Konflikten als Ransomware-Kriminelle ausgeben, um tatsächlich aber Cybersabotage gegen wichtige Infrastrukturen durchzuführen. Durch diese Tarnung können strategisch motivierte Akteure ihre Beteiligung plausibel abstreiten, ohne mit diplomatischen oder wirtschaftlichen Konsequenzen rechnen zu müssen.

In einem anderen strategischen Umfeld außerhalb der vom Ukraine- und Gaza-Krieg betroffenen Regionen machen internationale Behörden Hinweise auf sogenanntes Pre-positioning öffentlich. Demnach sammelten Gruppen wie Volt Typhoon für einen etwaigen Konfliktfall Zugänge zu Zielnetzen, um diese Zugänge im Fall einer Eskalation für Cybersabotage verfügbar zu haben und kurzfristig nutzen zu können. Dabei handelt es sich nach BSI-Einschätzung jedoch um sehr frühe Phasen von Prepositioning: Es wurde nicht berichtet, dass bereits Prozesssteuerungsumgebungen (OT-/ICS-Netze) umfangreich und systematisch aufgeklärt oder Backdoors mit destruktiven Fähigkeiten beobachtet worden wären. Zudem bleibt unklar, ob es sich dabei um regional begrenzte Aktivitäten handelt.

## 4.2 Informationsoperationen

Der Begriff „Informationsoperationen“ deckt sowohl Desinformation als auch Propaganda und ähnliche Aktivitäten ab, die dazu geeignet sind, mittels Narrative die öffentliche Meinung oder die Meinung von Entscheidern zu beeinflussen. Das BSI betrachtet die Phänomenebereiche APT und Informationsoperationen in der Regel getrennt, im Berichtszeitraum zeichnet sich jedoch ab, dass die Grenzen verschwimmen. Beispielsweise hat das BSI angesichts der Wahlen im Jahr 2024 politische und vorpolitischer Organisationen sensibilisiert, um vor der Möglichkeit von sogenannten Hack-and-Leak-Kampagnen zu warnen.

Dabei werden Accounts oder Geräte von politisch relevanten Personen kompromittiert, Daten gestohlen und diese, mit einem Narrativ versehen, veröffentlicht. APT-Gruppen, deren Kerngeschäft es ist, Informationen zu stehlen, können opportunistisch entscheiden, ob die erbeuteten Daten für Hack-and-Leak-Operationen geeignet sind und entsprechend veröffentlicht werden sollen. Im Berichtszeitraum sind jedoch keine solchen Veröffentlichungen in Deutschland oder zu deutschen Geschädigten beobachtet worden.

Auch die Effekte von Cybersabotage werden mittlerweile durch begleitende Informationsoperationen, zum Beispiel in sozialen Medien, in der öffentlichen Wahrnehmung verstärkt. Dabei werden die tatsächlichen Schäden und Konsequenzen von Angriffen übertrieben dargestellt, offenbar um Unsicherheit in der Bevölkerung zu säen und die zuständigen Behörden oder Regierungen zu diskreditieren. Dies wurde – wie oben beschrieben – vor allem im Kontext Angriff der Hamas auf Israel und des nachfolgenden Gaza-Kriegs beobachtet, bei dem die Angreifer zum Beispiel ihre technisch vergleichsweise einfachen Angriffe auf Unitronics-Systeme in den sozialen Medien spektakulärer darstellten, als sie eigentlich waren.

Diese beiden Phänomene – Hack-and-Leak-Operationen und Informationsoperationen im Rahmen von Cybersabotage – deuten darauf hin, dass die Akteure den Cyberspace weiter fassen als IT-Geräte und die damit verbundene Infrastruktur. Stattdessen rückt auch der Informationsraum, das heißt der Raum, in dem Medien und Öffentlichkeit eine Meinung und Interpretation der Welt verhandeln, in den Fokus der Angreifer. Eine rein technische Fokussierung der Verteidiger auf IT-Geräte greift daher zu kurz und muss durch Aufklärung und Sensibilisierung im Informationsraum ergänzt werden.

## 4.3 Technische Trends

Weltweit sind APT-Gruppen aktiv und zeigen vielfältige Angriffstechniken. Die hier vorgestellten Trends sind daher nur als Auswahl der wichtigsten Beobachtungen zu verstehen. Grundsätzlich nutzen APT-Gruppen alle Angriffswege und Schwachstellen, die sie für ihre Ziele benötigen.

**Verschleierungsnetze:** Fortgesetzt haben sich Trends, die bereits im vergangenen Berichtszeitraum beobachtet worden waren. Das BSI hat eine zunehmende Zahl an Verschleierungsnetzen festgestellt. Dabei handelt es sich um kompromittierte Router, IoT-Geräte und VPS-Server, die zu einem Botnetz zusammengeschaltet werden. Über dieses

Botnetz können die Angreifer ihren Verkehr über mehrere Zwischenstationen verschleiern (*vgl. auch Kapitel Botnetze, Seite 15.*) Dies erschwert sowohl die Detektion von Angriffen als auch die Zuordnung zu bekannten Gruppen. Diese Netze werden inzwischen professionalisiert betrieben, um den Kunden, das heißt APT-Gruppen, den größtmöglichen Komfort bei der Nutzung zu gewährleisten.

**EDR-Killer:** Der stetige Wettlauf zwischen Angreifern und Verteidigern wird durch das Phänomen des Unterlaufens von Endpoint-Detection-and-Response-Produkten (EDR) aufgezeigt. Mittlerweile haben sich in vielen Unternehmen und Behörden EDRs als Sicherheitskomponente etabliert und stellen nun eine weitere Hürde für Angreifer dar (*vgl. Kapitel Malware-as-a-Service EDR-Killer, Seite 19.*) Die Angreifer reagieren darauf und nutzen inzwischen vermehrt Techniken, um diese EDR-Produkte zu unterlaufen. Dies erfolgt teils über verwundbare Treiber, die es erlauben, EDR-Produkte zu deaktivieren, oder durch das Unterdrücken von Benachrichtigungen der Systeme, die der Detektion von Angriffen dienen.

**Cloud-Anwendungen:** Auch an neue Entwicklungen und Nutzungsgewohnheiten passen sich Angreifer an. So zielen sie mittlerweile zum Beispiel auf Daten, die in der Cloud liegen. Dabei ist der Angriffsvektor in vielen Fällen nicht Cloud-spezifisch. Beispielsweise stehlen Angreifer Zugangsdaten über Phishing-Seiten oder Information Stealer, die dann auch zum Login für Cloud-Anwendungen genutzt werden (*vgl. zu Information Stealern auch Die Lage der IT-Sicherheit 2023, Seite 17.*) Kommen Exploits zur Anwendung, betreffen sie oftmals Schwachstellen in Webanwendungen oder Serversoftware, die sowohl in Cloud-Umgebungen als auch auf eigenen Systemen verwendet werden. Erst wenn die Angreifer Zugriff auf die Cloud haben, beginnen sie mit Cloud-spezifischen Techniken. Viele Gruppen sind inzwischen sehr geübt darin, die Konfigurationen und APIs der Cloud zu nutzen, um sich innerhalb der Cloud-Umgebungen auszubreiten oder ihren Zugang zu persistieren. Oftmals werden Konfigurationen beispielsweise so geändert, dass Datenbanken oder Schnittstellen für die Angreifer direkt aus dem Internet zugänglich werden.

**Zero-Day-Schwachstellen:** Im Bereich der Zero-Day-Exploits, das heißt von Schadprogrammen zum Ausnutzen für Schwachstellen, für die es noch keine Sicherheits-updates gibt, setzte sich der Trend fort, Schwachstellen in Server-Anwendungen und VPN-Produkten auszunutzen. Zero-Days in Endnutzerprodukten, wie Smartphones oder Browern, wurden dagegen häufig mit kommerziellen Exploit-Brokern in Verbindung gebracht. Deren Kunden haben es typischerweise auf Einzelpersonen wie

Regimekritiker oder Journalisten abgesehen – anders als APT-Gruppen, die meist Unternehmens- oder Behörden-Netze angreifen.

Trotz dieser technisch fortgeschrittenen Methoden betreiben auch viele APT-Gruppen weiterhin klassisches Phishing, um Zugangsdaten zu sammeln. Dabei werden wie gewohnt die Login-Seiten von Webmail-Portalen von Unternehmen oder kommerziellen E-Mail-Anbietern nachgeahmt und die Opfer durch E-Mails dorthin gelockt, damit sie ihre Zugangsdaten eingeben. Für Angreifer bleibt diese Vorgehensweise attraktiv, da sie mit wenig Aufwand gegen eine Vielzahl von Opfern eingesetzt werden kann.

#### 4.4 Diplomatische, juristische und politische Maßnahmen

Wie sich Entwicklungen bei Angreifern und Verteidigern gegenseitig bedingen, zeigt sich auch auf der strategischen Ebene, die durch diplomatische, juristische und politische Maßnahmen geprägt ist. Als Reaktion auf die Verwendung von Verschleierungsbotsnetzen aus kompromittierten Routern und IoT-Geräten haben insbesondere US-Behörden mehrere koordinierte Gegenmaßnahmen durchgeführt. So nahmen sie beispielsweise Takedowns gegen ein Botnetz von APT28 vor, das aus kompromittierten Ubiquiti-Edge-Routern bestand, sowie gegen ein Botnetz aus kompromittierten Routern und IP-Kameras, das von der APT-Gruppe Volt Typhoon genutzt wurde. Dabei griffen die US-Behörden auch auf kompromittierte Geräte in den USA zu, um Schadprogramme zu entfernen und temporäre Konfigurationsänderungen vorzunehmen, die verhindern sollten, dass die Täter erneut Zugriff auf die Geräte erlangen. Begleitet wurden diese technischen Maßnahmen von Benachrichtigungen an die Besitzerinnen und Besitzer der kompromittierten Geräte, damit diese die Bereinigung und Absicherungen endgültig vornehmen konnten.

Zusätzlich erließen US-Behörden Sanktionen unter anderem gegen Personen und Unternehmen, die mit der APT-Gruppe APT31 und dem Desinformationsnetzwerk „Doppelgänger-Kampagne“ in Verbindung stehen sollen. Auch im Rahmen der EU und durch den nationalen Attribuierungsprozess haben europäische und deutsche Behörden einen Rahmen für formale Sanktionen gegen Angreifer im Cyberraum etabliert. Damit werden die technischen Maßnahmen zur Erhöhung der Cybersicherheit im Verbund mit diplomatischen und juristischen Maßnahmen ergänzt.

## 4.5 Für Deutschland relevante APT-Gruppen

Das BSI sieht aufgrund eigener Vorfallserkenntnisse und des Austauschs mit Partnern mindestens die ab Seite 26 aufgeführten APT-Gruppen für Deutschland als relevant an. Die Gruppen sind in der Regel vor allem gegen Ziele in den angegebenen Sektoren aktiv. Die aufgeführten typischen Angriffstechniken sollten nicht als vollständig angesehen werden, da manche der Gruppen sehr vielseitig agieren. Aus Platzgründen werden ausschließlich die Angriffstechniken aus der ersten Phase eines Angriffs angegeben.

Zusätzlich stehen beim BSI aufgrund von Vorfällen im benachbarten EU-Ausland die Gruppen APT30 (Naikon) und APT31 (Judgment Panda) sowie die Gruppe Gallium (Softcell/Phantom Panda/Alloy Taurus/Granite Typhoon) unter Beobachtung.

## APT-Gruppen in Deutschland

Gruppennamen und Aliasse	Wirtschaftszweig in Deutschland, nach WZ 2008	Besondere Eigenschaften
APT15 / Vixen Panda / Mirage / Ke3chang / Nylon Typhoon	<ul style="list-style-type: none"> <li>• Öffentliche Verwaltung</li> </ul>	Die Gruppe nutzt eigene Verschleierungsnetzwerke aus kompromittierten Routern und VPN-Servern.
APT28 / Fancy Bear / Sofacy / Forest Blizzard	<ul style="list-style-type: none"> <li>• Auswärtige Angelegenheiten, Verteidigung, Rechtspflege, öffentliche Sicherheit und Ordnung</li> <li>• Erbringung von Dienstleistungen der Informationstechnologie</li> <li>• Öffentliche Verwaltung</li> </ul>	APT28 nutzt diverse Angriffsvektoren, z. B. Outlook-Schwachstelle CVE-2023-23397 (via E-Mail) WinRAR-Schwachstelle CVE-2023-38831 (via E-Mail-Anhang) Bruteforcing und Password-Spraying gegen erreichbare Server
APT29 / Cozy Bear / Nobelium / Midnight Blizzard	<ul style="list-style-type: none"> <li>• Auswärtige Angelegenheiten, Verteidigung, Rechtspflege, öffentliche Sicherheit und Ordnung</li> <li>• Erbringung von Dienstleistungen der Informationstechnologie</li> <li>• Öffentliche Verwaltung</li> <li>• Politische Parteien und sonstige Vereinigungen</li> </ul>	Um im legitimen Internetverkehr nicht aufzufallen, nutzt APT29 oft legitime Cloud-Dienste als Kontrollserver.
APT43 / Velvet Chollima / Kimsuky / Emerald Sleet	<ul style="list-style-type: none"> <li>• Forschung und Entwicklung im Bereich Rechts-, Wirtschafts- und Sozialwissenschaften sowie im Bereich Sprach-, Kultur- und Kunswissenschaften</li> <li>• Öffentliche Verwaltung</li> <li>• Rechtsberatung</li> <li>• Tertiärer und post-sekundärer, nicht tertiärer Unterricht</li> </ul>	Die Gruppe betreibt Social Engineering und versendet zunächst mehrere E-Mails ohne Schadcode, bis der Empfänger schließlich Vertrauen aufgebaut hat. Erst dann wird Schadcode oder ein Phishing-Link übermittelt.
Bitter / Hazy Tiger	<ul style="list-style-type: none"> <li>• Auswärtige Angelegenheiten, Verteidigung, Rechtspflege, öffentliche Sicherheit und Ordnung</li> </ul>	Der Angriffsvektor sind meistens CHM- oder RAR-Mailanhänge.
Cosmic Wolf / Sea Turtle / Marbled Dust	<ul style="list-style-type: none"> <li>• Erbringung von Dienstleistungen der Informationstechnologie</li> </ul>	Die Täter kompromittieren mitunter zunächst Zwischenziele, um Informationen für Folgeangriffe auf die eigentlichen Ziele zu erlangen.
DarkHotel	<ul style="list-style-type: none"> <li>• Auswärtige Angelegenheiten, Verteidigung, Rechtspflege, öffentliche Sicherheit und Ordnung</li> </ul>	
Earth Estries	<ul style="list-style-type: none"> <li>• Unbekannt</li> </ul>	Die Gruppe legt kontinuierlich neue Phishing-Domains und Kontrollserver an.
Gamaredon / Primitive Bear / Aqua Blizzard	<ul style="list-style-type: none"> <li>• Auswärtige Angelegenheiten, Verteidigung, Rechtspflege, öffentliche Sicherheit und Ordnung</li> </ul>	

<b>Gruppennamen und Aliasse</b>	<b>Wirtschaftszweig in Deutschland, nach WZ 2008</b>	<b>Besondere Eigenschaften</b>
Ghostwriter / UNC1151 / Storm-0257	<ul style="list-style-type: none"> <li>• unspezifisch</li> </ul>	Private E-Mail-Postfächer bei kommerziellen Webmail-Anbietern werden mittels Spearphishing angegriffen.
Labyrinth Chollima / Lazarus / Diamond Sleet	<ul style="list-style-type: none"> <li>• Erbringung von Dienstleistungen der Informationstechnologie</li> <li>• Herstellung von Waffen und Munition</li> <li>• Luft- und Raumfahrzeugbau</li> </ul>	<p>Als Angriffsvektor dienen oft E-Mails mit maliziösen Dokumenten zu vermeintlichen Jobangeboten.</p> <p>In zwei Fällen in den Sektoren „Herstellung von Waffen und Munition“ und „Luft- und Raumfahrzeugbau“ ist die Gruppenzuordnung noch nicht abschließend erfolgt, hier gibt es auch Überschneidungen mit Charakteristiken der Gruppe APT43 / Kimsuky / Velvet Chollima.</p>
Mirage Tiger	<ul style="list-style-type: none"> <li>• Öffentliche Verwaltung</li> </ul>	
Mustang Panda	<ul style="list-style-type: none"> <li>• Öffentliche Verwaltung</li> </ul>	
Outrider Tiger / Fishing Elephant	<ul style="list-style-type: none"> <li>• Öffentliche Verwaltung</li> </ul>	
Red Dev 61 / UTA0178 / UNC5221	<ul style="list-style-type: none"> <li>• Öffentliche Verwaltung</li> <li>• Wirtschaftsförderung, -ordnung und -aufsicht</li> </ul>	Die Angriffe richten sich typischerweise gegen VPN-Systeme und andere Perimetersysteme.
RomCom / Storm-0978	<ul style="list-style-type: none"> <li>• Öffentliche Verwaltung</li> </ul>	
Salted Earth / Sturgeon Fisher / Yoro Trooper	<ul style="list-style-type: none"> <li>• Unbekannt</li> </ul>	
Sharp Panda	<ul style="list-style-type: none"> <li>• Öffentliche Verwaltung</li> </ul>	
Sidewinder / Razor Tiger	<ul style="list-style-type: none"> <li>• Auswärtige Angelegenheiten, Verteidigung, Rechtspflege, öffentliche Sicherheit und Ordnung</li> </ul>	
Snake / Venomous Bear / Turla / Secret Blizzard	<ul style="list-style-type: none"> <li>• Öffentliche Verwaltung</li> </ul>	
Storm-0558	<ul style="list-style-type: none"> <li>• Forschung und Entwicklung im Bereich Rechts-, Wirtschafts- und Sozialwissenschaften sowie im Bereich Sprach-, Kultur- und Kunstwissenschaften</li> </ul>	Die Gruppe nutzt eigene VPN-Netzwerke, um ihren Angriffsverkehr zu verschleiern.
Viceroy Tiger / Donot	<ul style="list-style-type: none"> <li>• Auswärtige Angelegenheiten, Verteidigung, Rechtspflege, öffentliche Sicherheit und Ordnung</li> </ul>	

Abbildung 6: Für Deutschland relevante APT-Gruppen

## 5 – Phishing

Die Phishing-Methoden von Cyberkriminellen gegenüber Verbraucherinnen und Verbrauchern veränderten sich im aktuellen Berichtszeitraum. Neben bereits bekannten Phishing-Kampagnen im Namen von Banken und Finanzinstituten wurde eine Zunahme von Kampagnen unter missbräuchlicher Nutzung von Markennamen einschlägiger Streamingdienste registriert. Thematisch lehnten sich diese an Maßnahmen zur Verhinderung von unerlaubtem Accountsharing, Änderungen in den Nutzungsbedingungen von Familien-Accounts und Änderungen von Preisen und Zahlungsbedingungen an. Es handelte sich also um Themen, die breit in Gesellschaft und Medien bekannt waren. Dies trug entsprechend erfolgreich zur Zunahme der inhaltlichen Phishing-Kampagnen bei.

Im Zusammenhang mit Streaming-Accounts zielen Cyberkriminelle insbesondere auf die im Profil hinterlegten sensiblen Informationen ab. Die Daten zu Zahlungsmitteln wie Kreditkarten, weitere Informationen von Zahlungsdienstleistern und persönliche Daten der Accountinhaberinnen und -inhaber werden anschließend für weitere Aktivitäten, beispielsweise den Datenhandel über Access Broker, missbraucht.

Eine weitere zunehmende Angriffstechnik, die im Kontext von Zahlungsdiensten beobachtet wurde, ist der absichtliche Zeitverzug von Folgeaktionen nach einem erfolgreichen Phishing-Angriff. Darüber berichtete bereits zuvor eine Untersuchung<sup>2</sup>: Angreifer sind dabei durchschnittlich fünf Tage inaktiv geblieben, bis sie eine

### Ausgewählte Phishing-URLs und Phishing-IPs weltweit nach nachgeahmter Branche

Anzahl der URLs und IPs

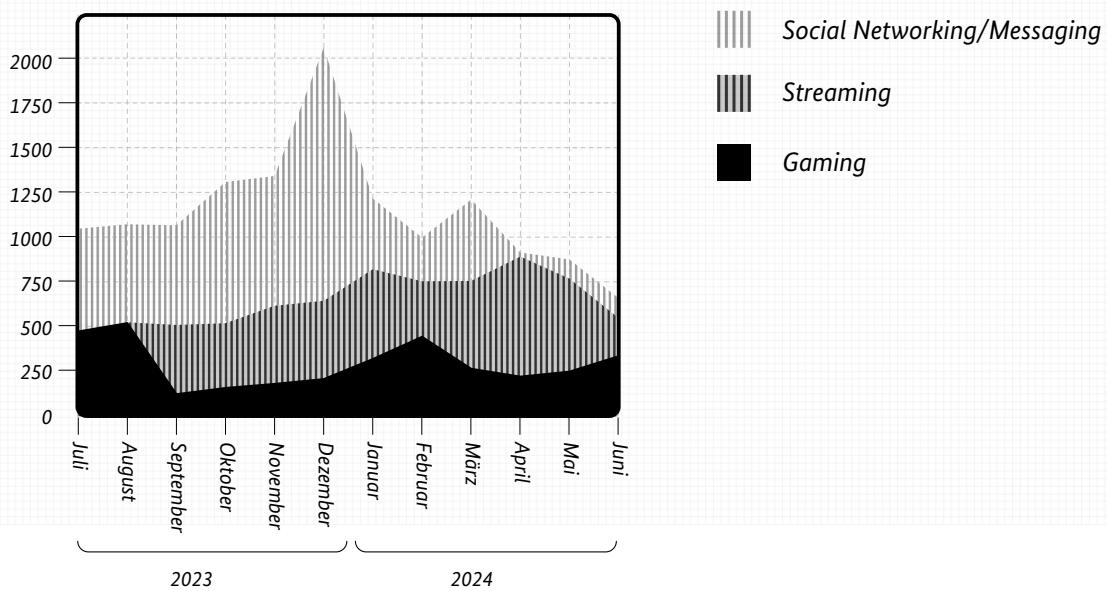


Abbildung 7: Ausgewählte Phishing-URLs und Phishing-IPs weltweit nach nachgeahmter Branche (openphish, absolute Zahlen)

Abbildung 7 / Statistik:

**Ziel der Statistik** Erhebung mutmaßlich maliziöser Webadressen, erhoben werden generische und markenspezifische Phishing-Adressen.

Berichtet wird monatlich. / **Grundgesamtheit** Alle im Internet vorhandenen Webseiten. / **Stichprobe** Alle der Plattform openphish.com bekannten, mutmaßlich malizösen Webseiten. / **Erhebungsdesign/-instrumente** Tagesaggregation einer laufenden Erhebung mittels Scanner. / **Reichweite** weltweit / **Qualitätsbewertung** Hellfeld-Statistik. Automatisierte Branchenkategorisierung benötigt gewisse Merkmale auf einer Webseite. Diese sind nicht immer zwingend genau bestimbar, wodurch sich eine unbestimmbare Dunkelziffer ergibt.

missbräuchliche Transaktion mit den zuvor gewonnenen Daten unternahmen. Die Anzahl dieser Transaktionen nahm insgesamt über einen Zeitraum von 14 Tagen nach den jeweiligen Phishing-Angriffen stetig zu.

Der Zeitverzug kann einerseits durch den Handel der Informationen auf Untergrundplattformen wie Darknet-Foren entstehen, wird aber andererseits auch als Instrument genutzt, um den Zusammenhang zwischen der Datenexfiltration und dem Ausnutzen dieser Informationen zu verschleiern. Für Verbraucherinnen und Verbraucher sind solche Phishing-Angriffe besonders fatal, da sie den akuten Sicherheitsvorfall meist nicht bewusst wahrnehmen und daher der Ansicht sind, dass keine Gefahr

besteht. Zudem wird es erschwert, spätere Schäden, beispielsweise durch Account- und Geldverlust, mit dem akuten Vorfall zu assoziieren, sich Hilfe zu suchen und Anzeige zu erstatten.

## Von Verbraucherinnen und Verbrauchern gemeldete Phishing-E-Mails nach Art der nachgeahmten Branche

Anteil in Prozent

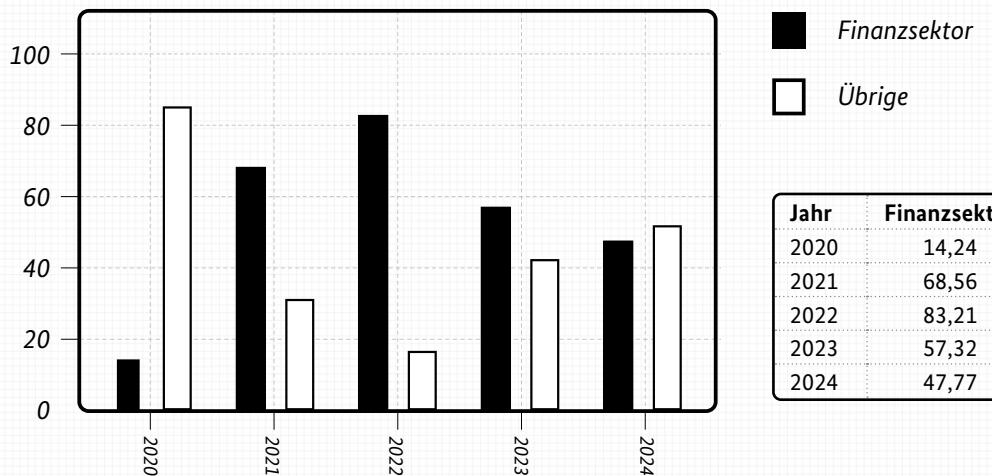


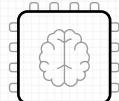
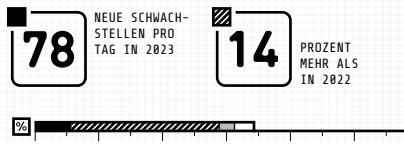
Abbildung 8: Von Verbraucherinnen und Verbrauchern gemeldete Phishing-E-Mails nach Art der nachgeahmten Branche (Phishing Radar 2020 bis 2024, Verbraucherzentrale NRW, in Prozent)

Abbildung 8 / Statistik:

**Ziel der Statistik** Erhebung maliziöser E-Mails in den Mail-Postfächern deutscher Verbraucherinnen und Verbraucher. Berichtet wird monatlich. **/ Grundgesamtheit** Alle maliziösen E-Mails, die an den Schutzmaßnahmen der Provider vorbei die Postfächer der Verbraucherinnen und Verbraucher erreichen. **/ Stichprobe** Meldungen mutmaßlich schadhafter E-Mails insbesondere deutscher Verbraucherinnen und Verbraucher an das Phishing-Radar der Verbraucherzentrale NRW. **/ Erhebungsdesign/-instrumente** Monatsaggregation laufender Verbrauchermeldungen. **/ Reichweite** Meldende müssen den Meldeweg kennen. Dies setzt eine Kenntnis über das Phishing-Radar der Verbraucherzentrale NRW voraus. **/ Qualitätsbewertung** Die Kategorisierung erfolgt durch individuelle Falleinschätzung durch Fachexpertinnen und -experten der Verbraucherzentrale NRW. Im Jahresmittel rund 30.000 E-Mails mit Markennennung (auf volle 10.000 gerundet).

# B ANGRIFFSFLÄCHE

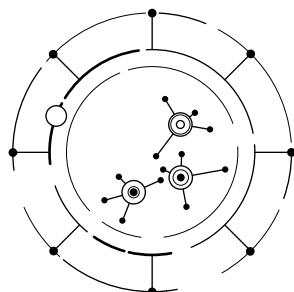
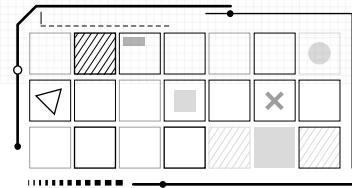
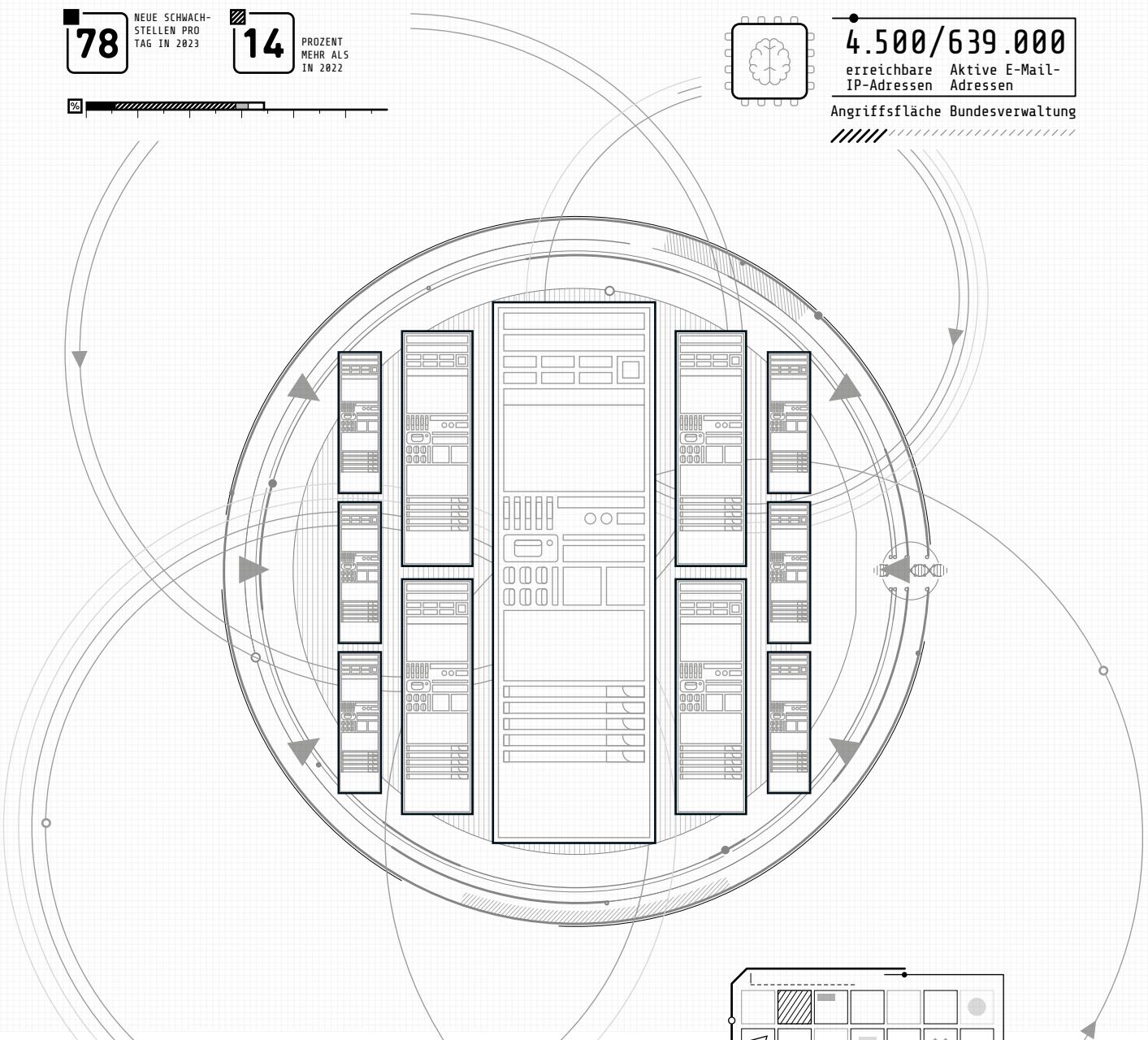
Wachstum Schwachstellen



**4.500 / 639.000**  
erreichbare Aktive E-Mail-  
IP-Adressen Adressen

Angriffsfläche Bundesverwaltung

||||| /|||||



Millionen DDoS-Angriffe



# 6 – Schwachstellen

Um Computersysteme infiltrieren zu können, nutzen Angreifer häufig Schwachstellen in der IT-Infrastruktur für einen Angriff aus. Schwachstellen stellen daher einen wesentlichen Teil der Angriffsfläche für Cyberangriffe dar. Ein Schadcode, der eine Schwachstelle ausnutzt, um einen Cyberangriff durchzuführen, wird als Exploit bezeichnet. Exploits werden zum Beispiel von Cyberkriminellen für die Erstinfektion von Systemen und zur Vorbereitung eines Ransomware-Angriffs eingesetzt.

Schwachstellen entstehen beispielsweise durch Fehler in der Programmierung, durch schwache Default-Einstellungen von IT-Produkten im Produktivbetrieb oder auch durch fehlkonfigurierte Sicherheitseinstellungen. IT-Systeme werden zunehmend komplexer und die Produktionsbedingungen immer arbeitsteiliger und modularer, sodass Schwachstellen sehr verbreitet sind. Wenn eine Schwachstelle in einem IT-Produkt entdeckt wird, stellen Hersteller in der Regel Sicherheitsupdates (Patches) bereit, um die Schwachstelle zu schließen und deren Ausnutzung für Cyberangriffe zu verhindern. Ein strukturiertes Patchmanagement ist daher eine der wichtigsten Präventivmaßnahmen für Organisationen jeder Art und Größe.

## 6.1 Schwachstellen in Softwareprodukten

Schwachstellen in Softwareprodukten dienen oftmals als erstes Einfallstor zur Kompromittierung von Systemen und ganzen Netzwerken – schließlich sind sie häufig über das Internet ausnutzbar und erlauben den Angreifern somit maximale Anonymität und Flexibilität aus der Ferne.

Im Jahr 2023 wurden durchschnittlich täglich 78 neue Schwachstellen bekannt, rund 14 Prozent mehr als im Jahr 2022. Dabei waren jegliche Arten von Softwareprodukten betroffen, von spezialisierten Fachanwendungen über komplexe Serverinfrastrukturen bis hin zu Smartphone-Apps. Wie schon in den vergangenen Jahren wirkten sich auch im aktuellen Berichtszeitraum die zunehmende Modularisierung und Arbeitsteilung bei der Softwareproduktion auf die Bedrohungslage aus. Wird eine

Schwachstelle in einer Softwarekomponente bekannt, die in einer Vielzahl verschiedener Anwendungen eingesetzt wird, dann kann solch eine einzelne Schwachstelle für Cyberangriffe gegen alle diese Anwendungen ausgenutzt werden. Nicht jede Schwachstelle ist für Angriffe aus dem Internet einfach ausnutzbar. Eine Schwachstelle in einer lokalen Anwendung ohne Verbindung zum Internet kann beispielsweise lediglich durch einen lokalen Angreifer ausgenutzt werden. Dagegen können Schwachstellen in Softwareprodukten, die direkt aus dem Internet erreichbar sind, leichter und von einer höheren Anzahl von Cyberkriminellen für Angriffe genutzt werden.

Neben Meldungen zu den allgemein bekannt gewordenen Schwachstellen in Softwareprodukten erhält das BSI auch spezielle Meldungen zu Schwachstellen von Sicherheitsforschenden, die auf verwundbare Komponenten in IT-Systemen gestoßen sind. Charakteristisch ist, dass hierbei diejenigen Schwachstellen im Fokus stehen, die bis dahin noch nicht öffentlich oder dem Hersteller noch nicht bekannt geworden sind, sogenannte Zero-Day-Schwachstellen. Im Rahmen einer koordinierten Offenlegung von Schwachstellen (Coordinated Vulnerability Disclosure, CVD) hat das BSI auf Basis der Entdeckungen anschließend die Möglichkeit, federführend oder vermittelnd zwischen Sicherheitsforschenden und Produktverantwortlichen oder Herstellern auf eine Beseitigung dieser Zero-Day-Schwachstellen hinzuwirken (vgl. Kapitel NIS-2-Richtlinie, Seite 84).

Im Berichtszeitraum hat das BSI monatlich durchschnittlich 41 Meldungen von Sicherheitsforschenden über schwachstellenbehaftete Softwareprodukte erhalten und nach dem System des Open Web Application Security Project (OWASP) klassifiziert. Während CWE (Common Weakness Enumeration) und CVSS (Common Vulnerability Scoring System) die Schwachstellen selber beschreiben, erlaubt OWASP eine Beschreibung des schwachstellenbehafteten Produkts. Rund 61 Prozent der Meldungen bezogen sich auf Schwachstellen, die die betroffenen Produkte anfällig für Injection-Cyberangriffe machten. Dabei gelingt es Angreifern, über die Schwachstelle maliziösen Programmcode in das Softwareprodukt einzuschleusen und dadurch weitere Cyberangriffe wie etwa die Exfiltration von Daten vorzubereiten.

Neben Meldungen über schwachstellenbehaftete Produkte gingen im Berichtszeitraum auch monatlich durchschnittlich sechs Meldungen über falsch konfigurierte Server oder fehlende Patches für bereits zuvor allgemein bekannt gewordene Schwachstellen ein.

Somit bestätigt die Entwicklung die verstärkten Aktivitäten des BSI in diesem Themenbereich: Der CVD-Prozess des BSI wurde in den vergangenen Monaten deutlich relevanter und sichtbarer durch die Bereitstellung eines Schwachstellenmeldeformulars, die Veröffentlichung einer CVD-Leitlinie sowie erste Anreize, Entdeckungen an das BSI zu melden, wie zum Beispiel die Hall of Fame für Schwachstellenforschende.

**Die Hall of Fame für Schwachstellenforschende finden Sie hier:**



## Meldungen über schwachstellenbehaftete Produkte Juli 2023 bis Juni 2024 nach möglicher Schadwirkung

Anteile in Prozent

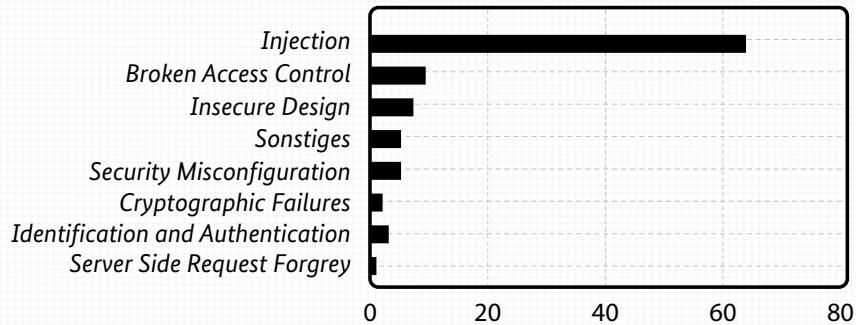


Abbildung 9: Meldungen über schwachstellenbehaftete Produkte Juli 2023 bis Juni 2024 nach möglicher Schadwirkung (Anteile)

### Abbildung 9 / Statistik:

**Ziel der Statistik** Meldungen schwachstellenbehafteter Produkte von Sicherheitsforschenden an das BSI im Rahmen des Coordinated Vulnerability Disclosure (CVD) mit Fokus auf Schwachstellen, die dem Hersteller nicht bekannt sind. Berichtet wird jährlich. / **Grundgesamtheit** An das BSI mittels CVD gemeldete Schwachstellen in IT-Produkten von deutschen Herstellern. / **Stichprobe** Vollerhebung. Gezählt werden Meldungen über schwachstellenbehaftete Produkte, nicht die Schwachstellen. / **Erhebungsdesign/-instrumente** Online-Meldeformular; Auswertung der Meldungen erfolgt mit der CVD-Leitlinie durch Mitarbeitende des BSI. / **Reichweite** Deutschlandweit. / **Qualitätsbewertung** Vollerhebung über CVD-Meldungen. Aussagen über Schwachstellen, Zero-Day-Schwachstellen oder die Verbreitung schwachstellenbehafteter Produkte sind nicht möglich.

# Ausnutzung von Zero-Day-Schwachstellen bei IT-Dienstleistern in Deutschland

## Sachverhalt

Wie schon im Berichtszeitraum 2023 sind Vorfälle bei IT-Dienstleistern weiter von Relevanz. Das BSI identifizierte 2023 eine seit 2022 durchgeführte Angriffskampagne gegen deutsche IT-Dienstleister und weitere deutsche Organisationen. Die Angreifer nutzten dabei Zero-Day-Schwachstellen auf Confluence-Systemen aus, die häufig exponiert im Internet betrieben werden. Dabei tarnten die Angreifer ihr Schadprogramm als Plug-in und nutzten unter anderem erbeutete Zugangsdaten, um sich im gesamten Netzwerk der Organisation auszubreiten.

Die betroffenen IT-Dienstleister waren auch für Bundesbehörden tätig.

## Bewertung

Gefahren durch die Ausnutzung von Zero-Day-Schwachstellen betreffen grundsätzlich alle IT-Produkte. In hohem Maße gefährdet sind Produkte, die direkt aus dem Internet erreichbar sind.

Die hier genannten Cyberangriffe wurden von einer professionell agierenden Cyberspionagegruppe mit hohem Aufwand durchgeführt. Die Angreifer entwickelten dabei jeweils spezielle, auf das Opfer zugeschnittene Angriffswege, nutzten die Schwachstelle teils Monate vor Bekanntwerden aus und wandten Techniken an, um die Infektion der betroffenen Systeme zu verschleiern und sich in den betroffenen Systemen zu verstecken. Die Angreifer waren daher schwer zu detektieren und konnten teils über Monate hinweg in den betroffenen Systemen spionieren. Von dieser und anderen ähnlich agierenden Angreifergruppen geht ein hohes Gefährdungspotenzial für IT-Dienstleister, die Bundesverwaltung und politisch relevante Organisationen aus.

IT-Dienstleister sind ein besonders wertvolles Angriffsziel, da sie stark vernetzt sind und so Zugang zu Infrastrukturen und Informationen ihrer Kunden ermöglichen können. Zudem verfügen sie häufig über weitgehende Administrationsrechte auf zumindest einem Teil der Systeme.

Für Betroffene sind die Auswirkungen besonders schwerwiegend und herausfordernd, zum Beispiel bezüglich der Krisenkommunikation oder der Bereinigungsaufwände. Die Funktionsausfälle der IT-Infrastruktur während der Bereinigung sind teils massiv und lang anhaltend. Ebenso stellt die Etablierung eines Notfallbetriebs während der Vorfallsbearbeitung und des IT-Neuaufbaus viele Betroffene vor immense Probleme.

## Reaktion

Primäres Ziel ist die Sicherstellung, dass ein Zero-Day-Exploit an einem exponierten System nicht zu einer Kompromittierung weiterer kritischer Systeme oder des internen Netzwerks führt. Ein wirksames Angriffsflächenmanagement ist daher eine der wichtigsten Präventionsfähigkeiten. Dazu gehören zum Beispiel folgende Aspekte:

1. Nur solche Systeme und Dienste sollten öffentlich zugänglich sein, für deren Funktionalität die Erreichbarkeit aus dem Internet zwingend notwendig ist.
2. Interne Netze sollten stark segmentiert werden, um im Falle einer Infiltration die Ausbreitung der Angreifer im Netzwerk zu begrenzen.
3. Allgemeine Präventionsmaßnahmen sollten umgesetzt werden, wie zum Beispiel die Beschränkung von Zugangsrechten auf das nötige Minimum, die Nutzung guter und individueller Passwörter, Multifaktor-Authentifizierung usw.

## 6.2 Schwachstellen in Hardware

Hardwareschwachstellen erlauben Angriffe auf den physischen Aufbau und die Materialeigenschaften von Produkten oder die Mikroarchitektur von Prozessoren. Im Gegensatz zu Softwareschwachstellen sind Hardwareschwachstellen in bereits hergestellten Produkten schwer zu beheben, was das Interesse von Angreifern weckt. Je nach Art des Angriffs kann die Ausnutzung der Schwachstelle einfach sein oder erhebliches technisches Know-how sowie teure Ausrüstung benötigen. Trotz hoher Aufwände werden Hardwareschwachstellen gerade bei gezielten Angriffen zunehmend auch in der Praxis ausgenutzt.

Mikroarchitekturelle Angriffe wie Spectre oder Meltdown lassen sich rein per Software auf dem anzugreifenden System ausführen. So sind auch im Berichtszeitraum einige neue Varianten dieser Angriffe veröffentlicht worden. Zum Beispiel nutzt GhostRace die spekulative Ausführung und weitere Architeureigenschaften, um das Auslesen beliebiger Speicherbereiche zu ermöglichen. Auch der Angriff Inception auf AMD-Prozessoren kombiniert zwei Angriffstechniken, um spekulative Ausführungen auszulösen und auf geschützte Speicherbereiche zuzugreifen. Zunehmend wird Fuzzing, eine etablierte Technik zur Fehlererkennung in Software, zum Aufspüren von CPU-Schwächen verwendet. Hierbei wird ein Programm mit zufälligen oder ungültigen Eingabedaten beschickt, um Fehler und Sicherheitslücken aufzudecken. Mithilfe dieser Technik wurde Zenbleed entdeckt. Auch hier erfolgt ein Angriff auf die speulative Ausführung in der AMD-Zen-2-Mikroarchitektur, um Speicherschutzmechanismen zu umgehen. GoFetch ist ein neuer Angriff auf Apple-ARM-CPUs, der einen Optimierungsmechanismus der CPUs angreift, um daraus Rückschlüsse auf verarbeitete Daten zu erhalten, und so in der Lage ist, zum Beispiel geschütztes Schlüsselmaterial zu rekonstruieren.

Neben Angriffen auf CPUs waren auch andere Hardwarekomponenten Ziel von Angriffen. Mit ZenHammer wurde ein Angriff auch auf DDR5-Speicher gefunden, bei dem der Hauptspeicher trotz Fehlerkorrektur anfällig für gezielte Manipulation ist. GPU.zip und sogenannte Drive-by-GPU-Cache-Angriffe ermöglichen das Auslesen sensibler Daten über Schwachstellen in Grafikkartenchips (GPUs).

Wenngleich rein softwarebasierte Angriffsmethoden geringere Kosten verursachen, können auch Angriffe, für die externe Hardware benötigt wird, für Angreifer interessant sein. Zwar sind hardwarebasierte Angriffe oft

aufwendiger und teurer durchzuführen, aber sie können dafür auch Systeme, auf die kein softwareseitiger Zugang besteht, kompromittieren. Das Induzieren von Fehlern wurde beispielsweise bei einem Angriff auf die Tesla-Auto-pilot-Hardware genutzt, um mittels Voltage-Glitching auf die Firmware des Systems zuzugreifen. Auch das Fraunhofer-Institut AISEC beschreibt in einer vom BSI in Auftrag gegebenen Studie einen Laser-Fehlerangriff auf Signaturverfahren, um Programmabläufe eines Chips zu verändern und so an sensible Daten zu gelangen.

Insbesondere Hardware- und Chipprodukte, bei denen Sicherheitsfunktionen nicht von Anfang an in der Entwicklung berücksichtigt wurden, bedürfen besonderer Aufmerksamkeit. Eine unabhängige Sicherheitsüberprüfung und Zertifizierung, zum Beispiel nach ISO-Standard 15408, ist ein Kennzeichen für gute Sicherheitsfunktionalität. Mit zunehmender praktischer Relevanz von Hardware- und Chipangriffen spielen hardwarebasierte Sicherheitsanker eine immer wichtigere Rolle für die Gesamtsicherheit von Produkten und Systemen.

## 6.3 Pfadbezogene Schwachstellen

Pfadbezogene Schwachstellen ziehen im Bereich der Webanwendungen seit vielen Jahren große Aufmerksamkeit auf sich. So ermöglichen Unwissenheit und Unachtsamkeit seitens Programmierender unzählige sogenannte Path-Traversal-Angriffe, bei denen auf Dateien und Verzeichnisse außerhalb der dafür vorgesehenen Bereiche zugegriffen werden konnte. Häufig war dabei sogar der Zugriff auf Passwörter und andere sensible Daten möglich.

Aber auch außerhalb von Webanwendungen sind pfadbezogene Schwachstellen ein beliebtes Ziel von Angreifern. Verschiedenste Rechteausweitungsschwachstellen der letzten Jahre basieren auf Datei- oder Gerätemeileitungen, realisiert durch zum Beispiel Symlinks oder die Möglichkeit, ausführbare Dateien direkt unter bestimmten Pfaden zu platzieren – unter Windows häufig in Verbindung mit einer Standardeinstellung, die es normalen Nutzenden erlaubt, Verzeichnisse im Root-Verzeichnis (C:\) zu erstellen.

Die damit verbundenen Gefahren werden häufig unterschätzt oder sind Programmierenden sowie Administratoren nicht bewusst. In der Folge kommt es auf der einen Seite unter anderem dazu, dass Programmierende auf Pfadangaben basierende Aktionen nicht oder nicht ausreichend absichern, sodass normale Nutzende die Pfadangaben

gabe oder das Ziel des Pfades beeinflussen können. Dies ist insbesondere dann problematisch, wenn der von den Programmierenden erstellte Code dafür vorgesehen ist, später mit erhöhten Rechten ausgeführt zu werden. Auf der anderen Seite versäumen es Windows-Administratoren, zum Beispiel die Berechtigung zum Erstellen von Ordnern im Wurzelverzeichnis (C:\) für die Gruppe der authentifizierten Benutzenden zu entfernen. Frei verfügbare Tools können Programmierenden und Administratoren dabei helfen, Schwachstellen im Zusammenhang mit Rechteausweiterungen, wie zum Beispiel DDL-, EXE- oder COM-Hijacking, zu identifizieren und zu beheben.

Eine weitere Art von pfadbezogenen Schwachstellen basiert auf dem fehlerhaften Versuch, anwendungsseitig anhand einer Pfadangabe, die durch Angreifer kontrollierbar ist, zu bestimmen, ob das durch den Pfad adressierte Ziel sich auf eine lokale Datei oder eine externe Quelle im Internet bezieht. Kommt die prüfende Funktion fälschlicherweise zu dem Ergebnis, dass der Pfad auf eine lokale Datei zeigt, und werden in der Folge Sicherheitsfunktionen für den Abruf von oder den Umgang mit dieser Datei nicht aktiviert, so kann es zu vielfältigen Schadensbildern kommen. Dabei ermöglicht die Existenz derartiger Schwachstellen regelmäßig erst erfolgreiche Angriffe und öffnet bereits versperrte Angriffswege erneut.

## 6.4 Schwachstellen in vernetzten Geräten

Mit der Digitalisierung wächst auch die Angriffsfläche für Cyberangriffe auf vernetzte Geräte. Die Digitalisierung des Autos und des Automobilverkehrs gehört zu jenen Bereichen, die sich am schnellsten vernetzen.

Mit der weiter voranschreitenden Elektrifizierung des Straßenverkehrs rückt auch die Frage der Cybersicherheit von Elektrofahrzeugen und der Ladeinfrastruktur weiter in den Fokus. Im März 2024 waren bundesweit 114.565 öffentlich zugängliche Ladepunkte in Betrieb<sup>3</sup>. Die Anzahl der öffentlichen Ladepunkte nahm 2023 gegenüber dem Vorjahr um circa 36 Prozent zu.

Bei Ladesäulen oder -punkten handelt es sich um stark vernetzte Geräte. Neben der eigentlichen Ladeschnittstelle zum Elektrofahrzeug verfügen diese typischerweise über weitere Schnittstellen für den notwendigen Datenaustausch. Hierzu gehören zum Beispiel mobilfunkbasierte Verbindungen über das Internet zu den Backendsystemen des Betreibers oder zu weiteren Beteiligten, wie zum

Beispiel zu Energieanbietern, Zahlungsdienstleistern oder E-Roaming-Anbietern. Zu Wartungszwecken können WLAN- oder Bluetooth-Zugänge an der Ladesäule vorhanden sein. Kundinnen und Kunden können sich mithilfe von RFID-Karten oder per Smartphone, ebenfalls über WLAN, Bluetooth oder auch NFC, am Ladepunkt anmelden.

Die Vielzahl der Schnittstellen und Datenverbindungen bedeutet aus IT-Sicherheitssicht eine potenziell große Angriffsfläche. Die klassischen Sicherheitsziele Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit sind auch in Bezug auf die Ladeinfrastruktur von Bedeutung. So werden bei der Abrechnung von Ladenvorgängen personenbezogene Daten übermittelt, die vertraulich zu verarbeiten sind. Die von der Ladesäule empfangenen oder gesendeten Daten müssen authentisch und integer sein, um etwa unberechtigte Ladenvorgänge oder unberechtigte Entladenvorgänge vom Fahrzeug ins Netz (Vehicle-to-Grid) oder unberechtigten Zugriff auf Wartungsfunktionen zu verhindern. Schließlich sollen die Ladepunkte den Nutzenden zuverlässig zur Verfügung stehen. Werden keine IT-Sicherheitsmaßnahmen umgesetzt, könnten Angreifer Ladesäulen etwa durch Denial-of-Service-Angriffe lahmlegen und im Extremfall potenziell die Stabilität der Stromnetze gefährden oder die Infrastruktur physisch beschädigen.

Im Berichtszeitraum sind mehrere Schwachstellen in Steuergeräten für Ladepunkte entdeckt worden. Im Zuge eines Automotive-Hackerwettbewerbs im Januar 2024 wurde Ladehardware von sechs unterschiedlichen Herstellern untersucht, die auch auf dem deutschen Markt vertreten sind. In allen sechs Fällen wurden Schwachstellen gefunden. Zum Berichtszeitpunkt lagen nicht alle Details der entdeckten Lücken vor. Es wurden jedoch teilweise hohe CVSS-Base-Scores von über acht von zehn Punkten erreicht. Zu den gefundenen Problemen bei einem Modell von Ladehardware gehörten unter anderem eine fehlende Authentisierung, unverschlüsselte Übertragung von sensiblen Daten oder eine unzureichende Validierung von Eingabedaten<sup>4</sup>. Durch die Schwachstellen wäre es einem Angreifer möglich gewesen, ferngesteuert beliebigen Code auszuführen und die Kontrolle über das Steuergerät zu übernehmen. Die Lücken in diesem Modell wurden zwischenzeitlich durch ein Firmware-Update des betroffenen Herstellers geschlossen.

## 6.5 Schwachstellen in Perimetersystemen

Das Aufkommen neuer Schwachstellen und das Aktualisieren betroffener Produkte ist Tagesgeschäft jeder IT-Organisation. Seit einigen Jahren nutzen Angreifer vermehrt kritische Schwachstellen in Perimetersystemen wie Firewalls, VPN- oder Applikation-Gateways (*vgl. Die Lage der IT-Sicherheit in Deutschland 2022, Seite 38*). Diese Systeme stellen aufgrund ihrer exponierten Position als Schutz- oder Perimetersystem an der Grenze zwischen einem lokal zu schützenden Netz, wie zum Beispiel einem Unternehmensnetz, und dem Internet attraktive Ziele für Cyberangriffe dar. Eine Kompromittierung dieser Systeme bietet Angreifern zahlreiche Optionen, sich in internen Netzwerken oder auf Server- und Client-Systemen weiter auszubreiten, die Authentisierung zu umgehen oder den Datenverkehr zu manipulieren. Hinzu kommt, dass Methoden zur Protokollierung und Angriffserkennung auf Perimetersystemen zum Teil beschränkt oder nicht üblich sind, sodass Angriffe nicht so gut erkennbar sind wie etwa auf Client-Systemen.

Im aktuellen Berichtszeitraum wurde eine Vielzahl kritischer Schwachstellen in Perimetersystemen bekannt, zum Beispiel eine Zero-Day-Schwachstelle in Ivanti Connect Secure und weiteren Ivanti-Produkten, kritische Schwachstellen in FortiGate-Produkten von Fortinet sowie kritische Schwachstellen im Citrix NetScaler. Diese Schwachstellen in weitverbreiteten Perimetersystemen wurden als Zero-Day-Schwachstellen bereits vor dem Bekanntwerden oder kurz nach Veröffentlichung durch den Hersteller von Cyberkriminellen oder von APT-Gruppen ausgenutzt. Generell zeigt sich das große Interesse, solche Schwachstellen auszunutzen, regelmäßig an internetweiten Scans, mit denen Angreifergruppen massenhaft versuchen, anfällige Geräte zu identifizieren und zu kompromittieren.

Die Nutzung von Schwachstellen in Perimetersystemen geht auch mit Änderungen im Angreiferverhalten einher. Während bei Angriffen auf Client-Systeme, zum Beispiel per Spear-Phishing, in der Regel Schadprogramme installiert werden, die aktiv aus dem Netzwerk eine Verbindung zu einem Command-and-Control-Server der Angreifer aufbauen, ist dies bei Angriffen über den Perimeter meist nicht der Fall. Stattdessen werden typischerweise sogenannte Webshells installiert. Diese warten passiv darauf, dass die Angreifer von außen eine Verbindung aufbauen. Dies ist möglich, da Perimetersysteme per definitionem aus dem Internet erreichbar sind.

Diese Vorgehensweise hat für Angreifer auch den Vorteil, dass sie von jedem System oder über Verschleierungsnetzwerke auf die kompromittierten Perimetersysteme zugreifen können. Für die Detektion hat dies den Nachteil, dass Indikatoren zum Erkennen einer Kompromittierung, wie zum Beispiel IP-Adressen der Command-and-Control-Server, in so einem Fall nicht anwendbar sind. Diese Entwicklung ist verbunden mit der Etablierung von sogenannten Verschleierungsnetzwerken, über die Angreifer ihre Zugriffe tarnen oder dynamisch umleiten (*vgl. Kapitel Technische Trends, Seite 23*).

Zu den im Berichtszeitraum bekannt gewordenen Schwachstellen hat das BSI-Lagezentrum jeweils Warnmeldung an seine Zielgruppen verschickt, um über die Schwachstellen, die Gefährdung, Maßnahmen, Sicherheitsupdates sowie Workarounds zu informieren.

Die kritischen Schwachstellen zeigen, dass in IT-Organisationen auch ein hohes Bewusstsein für die Absicherung von Perimetersystemen abseits vom etablierten Schutz von Client-Systemen erforderlich ist. In einzelnen Fällen reicht ein Patchen allein allerdings nicht aus. Stattdessen müssen Geräte zusätzlich auch auf eine Kompromittierung hin untersucht werden, bevor sie nach dem Einspielen eines Sicherheitsupdates sicher weiterbetrieben werden können.

## 6.6 Schwachstellen in kryptografischen Verfahren

Kryptografische Mechanismen zur Verschlüsselung sind wichtige Bausteine für die Umsetzung von Sicherheitsfunktionen in IT-Produkten. Dem Stand der Technik entsprechende Kryptoalgorithmen liefern hierfür grundsätzlich ausgezeichnete Sicherheitsgarantien. Das BSI empfiehlt in der Technischen Richtlinie TR-02102 eine Reihe kryptografischer Verfahren und Protokolle, die aufgrund eingehender mathematischer Kryptoanalyse allgemein als sicher angesehen werden.

**Zur Technischen Richtlinie  
TR-02102:**



Dagegen können folgende Aspekte dazu führen, dass das theoretische Sicherheitsniveau in der Praxis reduziert ist:

- Schwächen in kryptografischen Mechanismen oder Protokollen
- Implementierungsfehler
- Unzureichend abgesicherte Seitenkanäle
- Schwächen in der Zufallszahlen- und Schlüsselerzeugung

Die klassische Anwendung der Kryptografie ist der Schutz der Vertraulichkeit und Integrität von Daten, zum Beispiel wenn diese über offene Netzwerke wie das Internet übertragen werden. Dafür stehen verschiedene kryptografische Mechanismen und Protokolle zur Verfügung, für die gemeinhin angenommen wird, dass ein Angreifer mit Zugriff auf den Netzwerkverkehr weder die geheimen Schlüssel in Erfahrung bringen noch die ausgetauschten Daten entschlüsseln oder unbemerkt manipulieren kann. Um die Wirksamkeit kryptografischer Mechanismen und Protokolle zu gewährleisten, müssen geeignete Verfahren ausgewählt und korrekt implementiert werden. Im Infokasten *Angriffe auf SSH und seine Implementierung* (Seite 38) werden ein Angriff und eine Schwachstelle aus dem Berichtszeitraum beschrieben, die einmal die Sicherheit des Protokolls SSH (Secure Shell) selbst und einmal eine Implementierung des Protokolls betreffen.

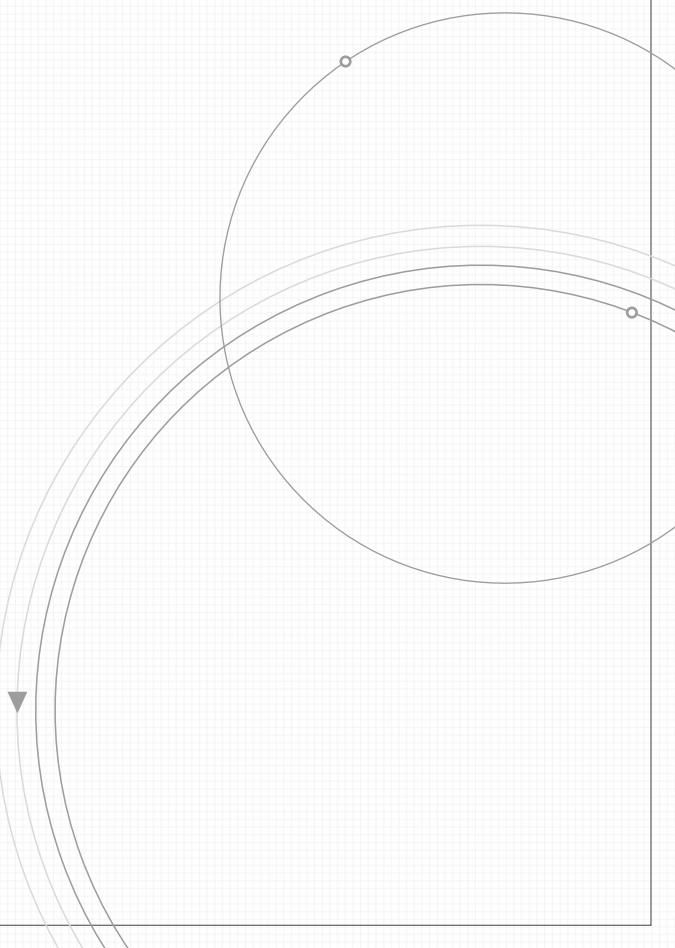
Seitenkanalangriffe gehören zu den derzeit erfolgreichsten Angriffsmethoden auf IT-Produkte und stellen eine ernst zu nehmende Bedrohung für die Sicherheit kryptografischer Implementierungen dar. Bei Seitenkanalangriffen werden Erkenntnisse aus beobachtbaren physikalischen Effekten, darunter Laufzeitverhalten, Energieverbrauch, elektromagnetische Abstrahlung und Cache-Verhalten, bei der Verarbeitung von sensitiven Daten gewonnen. Auch wenn eine völlig seitenkanalfreie Implementierung nicht möglich ist, kann man durch geeignete Maßnahmen erreichen, dass ein Seitenkanalangriff praktisch nicht durchführbar ist. Das BSI hat 2024 zu dieser Thematik aktualisierte und erweiterte Leitfäden veröffentlicht, die Empfehlungen zur Vorgehensweise bei der Evaluierung von Implementierungen hinsichtlich ihrer Seitenkanalresistenz enthalten.

**Weiterführende Informationen  
zur Seitenkanalresistenz:**



Eine wesentliche Voraussetzung für den sicheren Einsatz von Kryptografie ist die Erzeugung von echten Zufallszahlen, die gewisse Gütekriterien erfüllen müssen. Zufallszahlen werden unter anderem für die Schlüsselerzeugung benötigt. Für kryptografische Anwendungen dürfen Zufallszahlen nicht vorhersagbar sein und keine ausnutzbaren statistischen Defekte aufweisen. Um Angriffen durch schwache Zufallszahlen vorzubeugen, definiert das BSI in den Anwendungshinweisen und Interpretationen zu den Schemata AIS 20 und AIS 31 Funktionalitätsklassen von Zufallszahlengeneratoren für verschiedene Einsatzzwecke. Im Juni 2023 hat ein Workshop im BSI stattgefunden, in dem ein neuer Entwurf der mathematisch-technischen Anlage der AIS 20/31 vorgestellt wurde.

**Weiterführende Informationen  
zu Zufallszahlengeneratoren:**





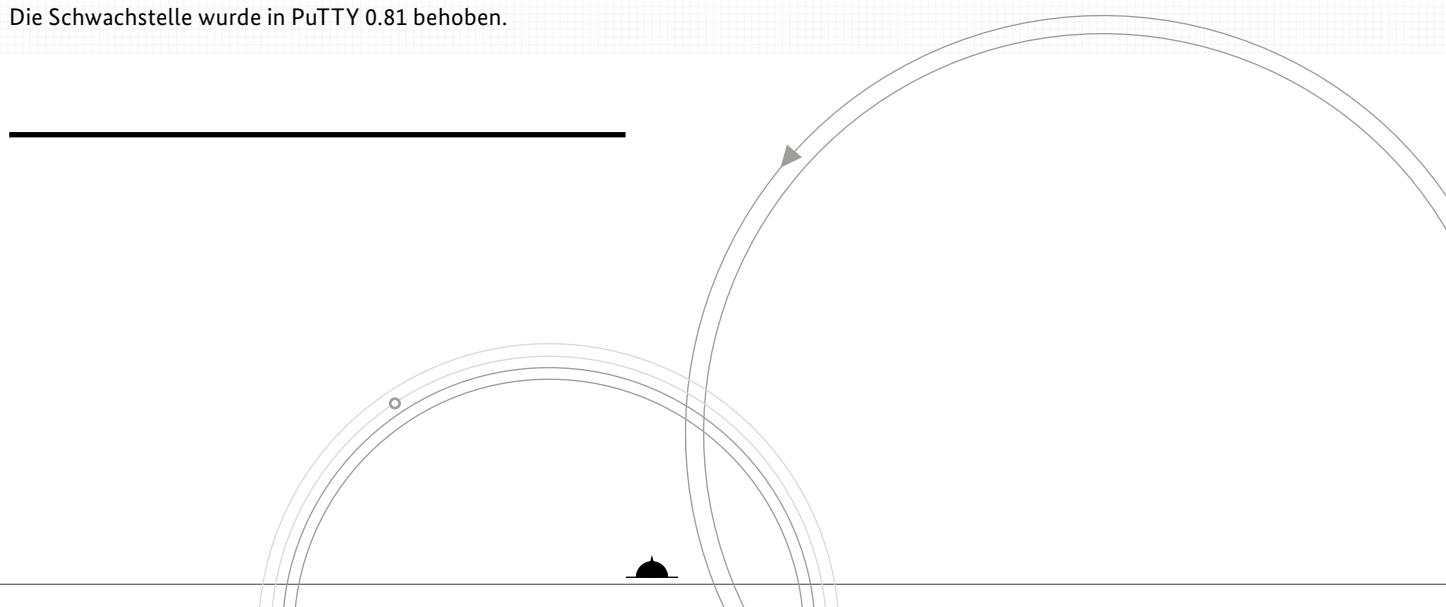
## Angriffe auf SSH und seine Implementierung

Das SSH-Protokoll dient dem Aufbau eines sicheren Kanals in einem unsicheren Netzwerk. Die gängigste Anwendung des SSH-Protokolls besteht darin, dass sich Administrierende mit ihrem Client-Rechner auf einem entfernten Server anmelden, um auf diesem Befehle auszuführen. Teil 3 der Technischen Richtlinie TR-02102 gibt Empfehlungen für die zu verwendenden kryptografischen Algorithmen und Schlüssellängen.

Sicherheitsforschende der Ruhr-Universität Bochum haben im Dezember 2023 den sogenannten Terrapin-Angriff auf SSH vorgestellt (CVE-2023-48795)<sup>5</sup>. Unter gewissen Rahmenbedingungen ist es hierbei einem Angreifer möglich, verschlüsselte und integritätsgeschützte Nachrichten vom Server an den Client unbemerkt zu blockieren. Da über solche Nachrichten auch Informationen zu noch auszuhandelnden Algorithmen ausgetauscht werden können, kann ein Angreifer durch das Blockieren dieser Nachrichten erzwingen, dass für die Verbindung gewisse Sicherheitsleistungen nicht verwendet werden. Die Webseite <https://terrapin-attack.com> listet Maßnahmen, um diesen Angriff zu vermeiden.

Die Sicherheitsforschenden der Ruhr-Universität Bochum veröffentlichten im April 2024 außerdem eine Schwachstelle in den Versionen 0.68 bis 0.80 des SSH-Clients PuTTY (CVE-2024-31497)<sup>6</sup>. Dieser Implementierungsfehler betrifft das Signaturverfahren ECDSA (Elliptic Curve Digital Signature Algorithm), falls die elliptische Kurve NIST P-521 verwendet wird, und hat zur Folge, dass die per ECDSA-Signatur erzeugten ephemeren Schlüssel stets neun führende Nullen haben, obwohl diese zufällig und gleichverteilt gewählt werden müssen. Dadurch wird es einem Angreifer ermöglicht, den privaten Signaturschlüssel durch ein mathematisches Verfahren aus circa 60 gültigen Signaturen zu berechnen.

Die Schwachstelle wurde in PuTTY 0.81 behoben.



# 7 – Große KI-Sprachmodelle

Künstliche Intelligenz (KI, engl. Artificial Intelligence, AI) nimmt in der öffentlichen Diskussion einen hohen Stellenwert ein. Große KI-Sprachmodelle (Large Language Models, LLMs), wie sie in ChatGPT, CoPilot, Claude und Luminous verwendet werden, haben in allen Branchen durch ihre breite Einsetzbarkeit großen Einfluss erlangt. In Abgrenzung zu klassischen IT-Systemen sind Sprachmodelle komplexe Architekturen aus neuronalen Netzen mit den folgenden Eigenschaften:

**Vektorverarbeitung:** Während bei der klassischen Programmierung explizit Regeln formuliert werden, bestehen neuronale Netze aus Modellen vordefinierter Funktionen, deren Parameter trainiert werden, das heißt die Modellparameter werden schrittweise angepasst bis Trainingsdaten möglichst gut wiedergegeben werden.

**Fehlertoleranz:** Durch ihre Architektur sind neuronale Netze, und damit Sprachmodelle, sehr flexibel und erzeugen für beliebigen Input Ergebnisse, ohne Fehlersituationen explizit anzuzeigen. Dabei sind die Sprachmodelle so trainiert, dass die Ergebnisse häufig der Erwartungshaltung der Nutzenden entsprechen. Das kann dazu führen, dass sie auf den ersten Blick richtig erscheinen, aber inhaltlich falsch sind. Fehler werden also erst auf einer semantischen Ebene, das heißt auf der Bedeutungsebene im konkreten Zusammenhang, sichtbar. So ist es zum Beispiel möglich, dass ein LLM ein unkorrektes Zitat „erfindet“. Hier spricht man von Halluzinieren.

**Unschärfe:** Das LLM muss auf jede Eingabe eine Ausgabe liefern. Hierfür bekommt es eine gegebenenfalls große, in jedem Fall jedoch begrenzte Anzahl Trainingsdaten. Daraus leitet es für Eingaben, die nicht in den Trainingsdaten vorkommen, die Ausgaben aus den vorliegenden Daten ab. Infolgedessen treten Unschärfen dergestalt auf, dass zwei anhand der gleichen Daten trainierte LLMs für die gleiche Eingabe unterschiedliche Ausgaben liefern können. Die Unschärfen können dabei zwischen verschiedenen Eingaben sehr stark variieren und sowohl wahre als auch falsche Aussagen (Halluzinieren) beinhalten, die nicht Teil der Trainingsdaten waren.

**Datenbasierte Funktionalität:** Die wesentlichen Funktionalitäten eines Sprachmodells werden durch die zum Training verwendeten Daten bestimmt. Ein Sprachmodell, das ausschließlich mit Lyrik trainiert wurde, wird voraussichtlich Gedichte generieren können, wird jedoch nicht in der Lage sein, die Logik und Strukturen eines Gesetzestextes zu reproduzieren.

## 7.1 Schwachstellen von Sprachmodellen und ihre Ursachen

Nicht zuletzt aufgrund scheinbarer „Allwissenheit“ – zu jeder Eingabe gibt es eine Ausgabe – erzielen LLMs große Erfolge. Jedoch sollten auch die damit verbundenen Herausforderungen oder Schwächen bekannt sein und berücksichtigt werden. Im Folgenden werden drei Herausforderungen betrachtet:

- mangelnde Erklärbarkeit,
- Abhängigkeit von Trainingsdaten,
- durch flexible Infrastrukturen begünstigte dynamische Entwicklung.

### 7.1.1 Erklärbarkeit

Gerade aufgrund der oben beschriebenen Unschärfe der Antworten eines LLMs, wäre es sinnvoll, nachvollziehen zu können, warum ein LLM eine bestimmte Ausgabe erzeugt hat. Dies ist jedoch systembedingt nicht möglich. Es ist also unklar, welche Eingaben auf welche Weise vom LLM verwendet wurden, um die Ausgabe zu generieren. Damit können die Ausgaben also im Nachhinein eben nicht „erklärt“ werden.

Sprachmodelle können Texte aus kleinsten Bestandteilen flexibel miteinander kombinieren. Dazu erlernen sie feine Sprachstrukturen wie Satzbau und Grammatik, aber auch semantische Zusammenhänge über statistische Korrelationen. Dies sind statistisch auftretende Abhängigkeiten, zum Beispiel wird der Satzteil „Autos fahren“ mit größerer Wahrscheinlichkeit durch „auf der Straße“ als durch „auf dem Wasser“ ergänzt. Grundsätzlich gilt: Je mehr Parameter die Modelle enthalten, desto besser können sie all diese Korrelationen abbilden.

Größere Modelle benötigen gleichzeitig auch steigende Datenmengen für das Training, um die damit einhergehende größere Parametermenge mathematisch bestimmen zu können. Eine größere Parametermenge bedeutet aber auch mehr Raum für ungewollte Antworten. Dies könnte zum Beispiel von Angreifern genutzt werden, um Informationen aus dem LLM zu gewinnen, die dieses nicht hätte herausgeben sollen, zum Beispiel Anleitungen zum Bau von Waffen.

Mit einer größeren Parametermenge in den Sprachmodellen gehen also nicht nur steigende Fähigkeiten, sondern auch größere, unbekannte Angriffsflächen einher, die nur verringert, aber nicht ausgeschlossen werden können.

### 7.1.2 Abhängigkeit von den Trainingsdaten

Während die Funktionalität bei klassischen Softwaresystemen durch die Programmlogik schematisch arbeitender Computerprogramme definiert wurde (Buchhaltungssoftware für Buchhaltung, Grafikprogramm für Grafiken usw.), besteht sie bei vielen LLM-basierten Anwendungen vor allem aus der Funktionalität der enthaltenen Sprachmodelle. Steuern solche Systeme mit LLM-basierten Anwendungen allerdings relevante Aktionen wie Verwaltungsvorgänge oder Finanztransaktionen, können Schwachstellen in den LLMs dann zu Schwachstellen des Gesamtsystems werden. Da die Funktionalität der LLMs aus den verwendeten Trainingsdaten stammt, kommt deren Kontrolle eine erhöhte Bedeutung zu. Hierfür spielen die folgenden Aspekte eine besondere Rolle.

**Datenselektion:** Die immense Größe der Modelle macht nur bei Verwendung entsprechend großer Mengen von Trainingsdaten Sinn. Die Hersteller von Basismodellen kontrollieren also durch die Auswahl der Daten auch die Qualität und Vielfalt der möglichen Ausgaben. Ihnen kommt damit eine hohe Verantwortung zu.

**Öffentliche Verfügbarkeit:** Der Zwang zu immer mehr Trainingsdaten macht auch die Verwendung von öffentlich verfügbaren Daten notwendig. Das Wissen darüber, mit welchen öffentlichen Daten, beispielsweise Wikipedia-Artikeln, große Sprachmodelle trainiert werden, kann zur Manipulation dieser öffentlichen Daten führen (Data Poisoning). Zudem bieten die öffentlichen Foren für Modelle und Entwickler weitere Möglichkeiten der Manipulation<sup>7</sup>.

Wer also öffentliche Daten manipulieren kann, die als Trainingsdaten verwendet werden, kann Funktionalität von LLMs manipulieren. Hersteller können dem entgegenwirken, indem die Gewinnung der Trainingsdaten für Angreifer weniger vorhersagbar wird. So könnte das Sammeln von Trainingsdaten in variablen zeitlichen Abständen stattfinden. Weiterhin kann durch geeignete Kriterien zur Selektion der Trainingsdaten das Risiko verringert werden.

**Finetuning:** Zunächst werden große LLMs anhand recht unspezifischer Aufgaben trainiert. Dies sind die sogenannten Foundation Models oder Originalmodelle. Um

damit eine bestimmte Art von Anwendung zu betreiben, werden sie noch durch das sogenannte Finetuning nachtrainiert. Dadurch soll die Wahrscheinlichkeit erwünschter Textausgaben, wie zum Beispiel Freundlichkeit und Fachwissen, erhöht und die Wahrscheinlichkeit unerwünschter Textausgaben, wie zum Beispiel Hassreden und Waffenbauanleitungen, verringert werden. Wird Finetuning in verschiedenen Schritten zu unterschiedlichen Zwecken angewandt, können Erfolge eines Schrittes von nachfolgenden Schritten verringert werden, da sich diese gegenseitig beeinflussen.

**Patchen:** Kann ein Angreifer eine (Text-)Eingabe finden, die zu einer ungewollten Ausgabe führt, so wird dies Adversarial Example genannt. Ein Chatbot kann zum Beispiel durch einen längeren Prompt, das heißt eine spezifische Kontextbeschreibung, zu unerwünschten Aussagen „überredet“ werden.

Fehler im programmierten Rahmenwerk einer KI-Applikation können im traditionellen Sinne durch ein Softwareupdate gepatcht werden. Dies ist bei inhaltlichen Fehlern im Sprachmodell nicht möglich. Stattdessen wird dem derzeit hauptsächlich mit zwei Ansätzen begegnet. Der erste ist ein entsprechend angepasstes Finetuning (siehe auch oben), ein sogenanntes Alignment, das die Ausgabe maliziöser Inhalte verhindern soll. Der zweite ist das sogenannte RAG (Retrieval Augmented Generation). Es extrahiert vor der Anwendung des LLM Texte aus einem, im Idealfall geprüften, Textkorpus, auf deren Inhalt sich die Ausgabe beziehen soll. Dadurch wird der generierte Text eng an den Inhalt der extrahierten Texte gekoppelt. Wenn beispielsweise nach dem Geschäftsführer eines bestimmten Unternehmens gefragt wird, könnte eine Beschreibungsseite des Unternehmens etwa in Wikipedia gesucht und das Sprachmodell angewiesen werden, die Frage aus diesem mitgegebenen Text zu beantworten.

Beide Ansätze bieten keinen abschließenden Schutz vor ungewollten Ausgaben. Das RAG erscheint hierbei aber erfolgreicher und robuster.

Zudem können Filter die Ein- und Ausgabemöglichkeiten einschränken. Bei Umsetzung von Filtern besteht im Allgemeinen eine Wechselwirkung zwischen der breiten Anwendbarkeit der Modelle (Utility) und der Wirksamkeit der Filter (Security).

Zusammenfassend ist festzuhalten, dass ein Patchen auf Codebasis von LLMs nicht geeignet ist, um unerwünschte Ausgaben, die aus dem Sprachmodell generiert werden, vollständig zu unterdrücken oder zu modifizieren. Damit ist es wichtig, das letztlich verwendete Modell umfänglich zu testen.

### 7.1.3 Einfluss der Infrastruktur

Einfach zu nutzende Cloudlösungen und vorbereitete Container bergen das Risiko, dass diese Technologie ohne notwendige Reflexion über Unschärfen und Gefahren eingesetzt wird.

Mit Einführung verschiedener Cloud- und Container-technologien ist durch einfach zu nutzende, skalierbare Softwareplattformen eine ideale Infrastruktur für die Entwicklung, den Austausch und die kommerzialisierte Nutzung von Sprachmodellen entstanden. Sprachmodelle benötigen zudem nur eine sehr einfache universelle Schnittstelle für die Textein- und -ausgabe, über welche die gesamte Komplexität der Funktionalität transportiert wird. Beides zusammen führt dazu, dass selbst technisch unbedarfte Nutzende in der Lage sind, eigene Applikationen zu erzeugen und zu betreiben.

Weil Sprachmodelle ohnehin oft als Cloud-Dienst eingeführt wurden und diese einfache Schnittstellen besitzen, steigt die Anzahl der Dienste rasant, die sich in virtuellen Lieferketten aus den Funktionalitäten von großen kommerziellen Sprachmodellen, selbst trainierten oder durch Finetuning veränderten öffentlichen Modellen und aus verknüpften traditionell programmierten Systemen bedient. Daraus erwächst eine große Anzahl von Diensten, zum Beispiel für kreatives Schreiben, Übersetzungen, Texterkennung (OCR), Diktieren (Speech-to-Text), Sprachsynthese (Text-to-Speech), Sentiment- und Sprachanalyse usw. Diese Dienste können durch interessante Gratisangebote zur Nutzung verleiten, ohne dass die Nutzenden sich über die Risiken, wie zum Beispiel Unschärfe, informieren.

Die fehlende Erklärbarkeit der Modelle oder fehlende Informationen zu Modellen aus der Lieferkette erschweren eine sicherheitstechnische Bewertung. Die Möglichkeit, Adversarial Examples, Texteingaben, die zu ungewollten Aussagen führen, zu verwenden, ist bei modifizierten Modellen in Lieferketten weniger an das konkrete Softwareprodukt als an die Trainingsdaten gebunden. Diese können wegen der Vektor-Architektur der Modelle nur im Gesamtmodell nachgewiesen, aber nicht effektiv analysiert werden.

Der großflächige Einsatz von Sprachmodellen, die damit verbundene kommerzielle Dynamik und die prinzipiellen Unschärfen der Modelle können je nach Kritikalität des Einsatzes ein hohes IT-Sicherheitsrisiko mit sich bringen. Die Auswirkungen damit einhergehender Bedrohungen sollten mittels Testen, zum Beispiel Pentesting, und der Betrachtung von Worst-Case-Szenarien im Rahmen einer Risikoanalyse eingeschätzt werden.

## 7.2 Missbräuchliche Verwendung von Sprachmodellen

Die Möglichkeiten zur missbräuchlichen Nutzung von Sprachmodellen ähneln denen im vergangenen Berichtszeitraum. Allerdings beobachtet das BSI eine steigende Bekanntheit und Verbreitung dieser Modelle im täglichen Leben. Das öffentliche Bewusstsein für die Chancen wie die Risiken ist gestiegen und die Nutzung ist für viele zum Alltag geworden. Wichtige Risiken sind:

**Phishing:** Angreifer setzen LLMs ein, um Texte für Phishing-Nachrichten und Webseiten mit Täuschungsabsicht zu erzeugen sowie um Desinformation zu gestalten, die insbesondere vor Wahlen direkte und kurzfristige Auswirkungen haben kann. Auch können jetzt leistungsfähigere KI-Chatbots zum Phishing sowie zur Verbreitung von Desinformation verwendet werden<sup>8</sup>. Diverse Angebote für entsprechende Dienste weisen auf eine rege Nutzung hin. Verbesserte und personalisierte Sprach- und Bildgenerierungen (Deepfakes) in hoher Qualität unterstützen sowohl Erpressungsversuche, wie zum Beispiel Sextortion, als auch die Kompromittierung öffentlich tätiger Personen.

**Technische Angriffsunterstützung:** Mit Sprachmodellen kann lauffähiger Schadcode generiert oder iterativ verfeinert werden. Ihre Anwendung ist allerdings schwer nachweisbar. Prinzipiell benötigen Schadsoftware-Angriffe noch immer umfangreiches Fachwissen. Es sind aber bereits autonom einzelne Vorgehensweisen zum Einbruch in Softwaresysteme implementiert worden<sup>9</sup>. Auch bei der Überwindung eines Passwortschutzes oder Captchas können Sprachmodelle helfen.

**Cyberespionage:** Sprachmodelle können Angreifern auch bei gezielten Angriffen nützlich sein. Beispielsweise kann ein mit zu vielen internen Daten trainierter Unternehmens-Chatbot Interna offenbaren. Zudem können mit weitreichenden Rechten ausgestattete firmeninterne Sprachmodelle nach initialer Kompromittierung bei der Exfiltration oder Manipulation von Daten nützlich sein.

## 7.3 Entwicklungen

**Aufgabenzerlegung:** Um den Blackbox-Charakter von Sprachmodellen zu reduzieren, gibt es Ansätze, die Lösung einer Aufgabe in kleinere Schritte zu zerlegen, die dann einzeln von Sprachmodellen erledigt werden können. Diese Forschungsrichtung könnte langfristig zu mehr Transparenz und stärkerer Regulierbarkeit führen. Entsprechende Forschung wird als XAI (Explainable AI) bezeichnet.

**Lokalisierung/Spezialisierung:** Größere Sprachmodelle bedeuten auch mehr Aufwand und Kosten bei Erstellung, Betrieb und Nutzung. Die hohe Leistungsfähigkeit dieser größeren Modelle ist für viele Anwendungszwecke jedoch gar nicht erforderlich. Kleinere lokale Systeme könnten hier auf die spezielle Umgebung, Aufgaben und Nutzenden angepasst werden.

Regionale und kulturelle Unterschiede in der Bewertung von Aussagen unterstützen die Entwicklung lokalisierter Sprachmodelle beispielsweise europäischer Staaten. Auch hierbei ist natürlich die Auswahl der Trainingsdaten der wesentliche Schritt zur Erreichung dieses Ziels.

Daher ist davon auszugehen, dass in Zukunft eine Lokalisierung der LLMs zu beobachten sein wird.

**Selbstreferenzialität:** Bereits heute gibt es viele generierte Texte im Netz. Weil Sprachmodelle mit Daten trainiert werden, die ihrerseits generierte Aussagen enthalten (vgl. *Die Lage der IT-Sicherheit 2023, Seite 42*), nimmt das Problem der Selbstreferenzialität zu. Die Folgen des Zusammenspiels dieser Rückkopplung mit absichtlich gestreuter Desinformation und unbeabsichtigt verfälschten Informationen sind heute nicht absehbar. Daher sind manuelle Kontrollen erforderlich, deren Qualität jedoch bei steigendem zeitlichem und ökonomischem Druck nicht immer sichergestellt werden kann.

## 7.4 Fazit

Der Einsatz von Sprachmodellen führt zu einer weitreichenden Veränderung im Umgang mit unerwünschten Ausgaben (Fehlern). Während entsprechende Fehler bei traditionellen Anwendungen in der Regel eindeutig festgestellt und durch einen Patch beseitigt werden konnten, steckt das unerwünschte Verhalten bei LLMs häufig in den erlernten Sprachmodellen, das heißt nicht im Programm-

code, sondern in den Daten, die das Modell beschreiben. Daher überträgt sich unerwünschtes Verhalten von LLMs unscharf auf der semantischen Ebene.

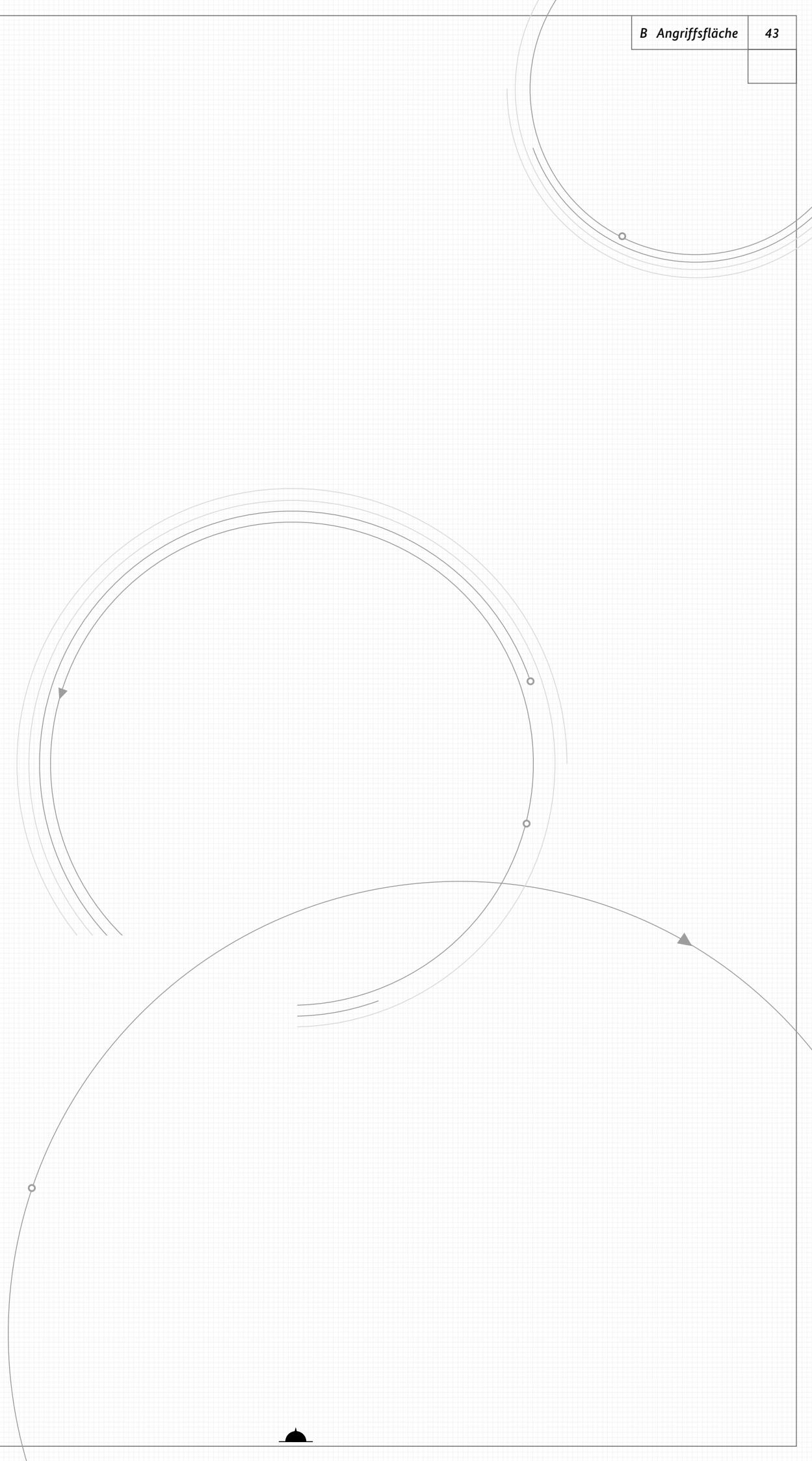
Eine nachhaltige Korrektur ist dabei aufgrund der Unschärfe nicht ohne Weiteres möglich.

Diese Unschärfe wirkt sich zum Beispiel auf das Sicherheitsziel Vertraulichkeit aus, weil Applikationen vertrauliche Informationen trotz entsprechender Gegenmaßnahmen ausgeben könnten und Eingaben von Nutzenden nicht in der Organisation gekapselt werden können, wenn Cloud-Dienste beteiligt werden. Werden Sprachmodelle bei der Informationsgewinnung genutzt, können richtige Informationen, die dem Modell als Eingabe zur Verfügung stehen, wie zum Beispiel Trainingsdaten, durch die systemimmanente Unschärfe verfälscht werden. Daher ist auch das Sicherheitsziel Integrität grundsätzlich gefährdet. Gefährdet die Unschärfe eines LLMs die Sicherheitsziele der Umgebung, in der es eingesetzt wird, stellt diese Unschärfe daher eine Schwachstelle dar.

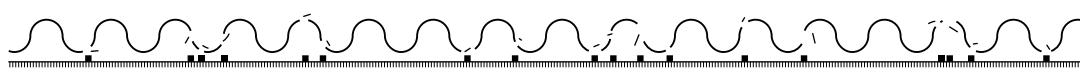
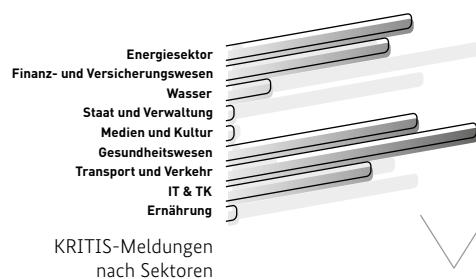
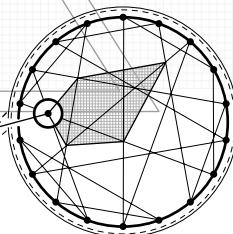
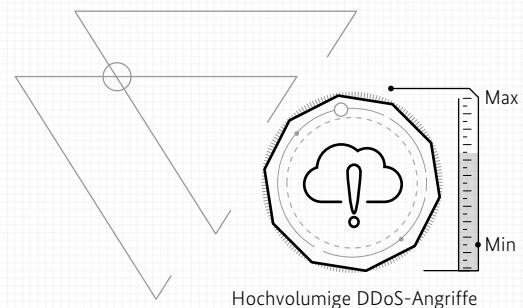
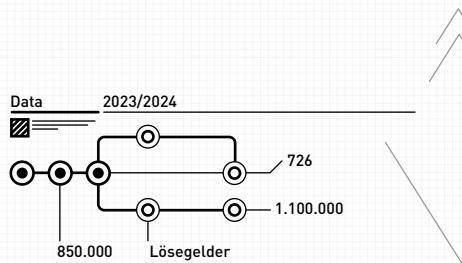
Die Interpretation der Ausgaben eines LLM kann entweder durch Menschen erfolgen oder auch technisch durchgeführt werden, um automatische Aktionen anzuschließen. Entfällt eine Prüfung durch Menschen, enthalten solche automatisierten Systeme unscharfe, schwer zu identifizierende Fehler oder gegebenenfalls auch Schwachstellen, die nicht mit letzter Sicherheit behoben werden können. Dies stellt etwas grundsätzlich Neues in der Cybersicherheit dar und ergänzt die weiterhin wirksamen klassischen Schwachstellen im Programmcode.

Bei kritischen Anwendungen sollten weiter gehende Maßnahmen ergriffen werden, zum Beispiel die menschliche Prüfung der Ergebnisse ähnlich dem Vier-Augen-Prinzip oder die Einschränkungen des Zugriffs (Least-Privilege).

Die Entwicklung und das technische Umfeld von Sprachmodellen besitzen eine hohe Dynamik, die zusammen mit der neuartigen, inhärenten Unsicherheit dazu führen, dass Sicherheitsmaßnahmen ständig hinterfragt und erneuert werden müssen. Durch neue Möglichkeiten und Rückkopplungseffekte entsteht eine hohe Komplexität. Daher sollten alle für den Einsatz Verantwortlichen sich in den genannten Themenbereichen umfassend informieren, Anwendungsbereiche kritisch hinterfragen und Chancen sowie Risiken in Lösungen abwägen und berücksichtigen. Erhöhte Aufmerksamkeit auf allen Ebenen muss dabei mit einer schnellen Reaktionsfähigkeit einhergehen, zum Beispiel durch vorbereitete Fallback-Mechanismen oder Filtermodifikationen. Das BSI verfolgt das Ziel, durch Veröffentlichungen Hilfestellungen zu geben, wie mit dieser Situation umgegangen werden kann.



# C GEFÄHRDUNGSLAGE



## 8 – Ausgewählte allgemeine Angriffsarten

Gegen Staat, Wirtschaft und Gesellschaft wurden im Berichtszeitraum unterschiedliche Angriffe beobachtet. Für DDoS-Angriffe beispielsweise werden spezialisierte Botnetze aufgebaut. Anschließend werden über diese Bots Webserver mit Anfragen überflutet, bis sie nicht mehr erreichbar sind.

Ein weiteres Beispiel sind Ransomware-Angriffe. Dabei dringen Angreifer in Systeme von Betroffenen ein, verschlüsseln Daten und fordern als Gegenleistung für die Wiederherstellung der Verfügbarkeit dieser Daten ein Lösegeld. Diese Angriffe gehen in der Regel mit einem Datenleak einher. Zahlen die Betroffenen nicht, drohen Angreifer mit der Veröffentlichung der erbeuteten Daten.

Zunehmend geraten auch Public-Cloud-Dienste in den Fokus von Angreifern. Schadsoftware sorgt etwa für eine eingeschränkte Verfügbarkeit oder verschlüsselt Daten von Kundinnen und Kunden inklusive deren Backups. Im Berichtszeitraum wurden auch Fälle von Angriffen auf die Vertraulichkeit von Cloud-Diensten durch Identitätsdiebstahl bekannt.

### 8.1 Distributed Denial of Service

Angriffe auf die Verfügbarkeit von Internetdiensten werden mit darauf spezialisierten Botnetzen durchgeführt (vgl. Kapitel Botnetze, Seite 15) und als Distributed-Denial-of-Service-Angriff (DDoS-Angriff) bezeichnet. Durch das Überfluten von (Web-)Servern mit Anfragen sind zum Beispiel Webseiten nicht mehr erreichbar. Das Ziel der Angreifer besteht darin, die angegriffenen Dienste so weit zu überlasten, dass diese lahmgelegt werden.

Die Folgen eines DDoS-Angriffs sind zum einen finanzielle Schäden für Dienstleister oder Onlineshops, wenn diese nicht erreichbar sind. Zum anderen können Imageschäden und gegebenenfalls Unsicherheit in der Bevölkerung folgen (vgl. Die Lage der IT-Sicherheit in Deutschland 2023, Seite 30).

Die Anzahl der bekannt gewordenen DDoS-Angriffe in Deutschland wird durch einen Index gemessen (vgl. Abbildung 10, Seite 46), der im Berichtszeitraum bei durch-

schnittlich 101 Punkten und damit nahezu exakt auf dem Durchschnittswert des Referenzjahres 2021 lag.

Dabei waren starke Schwankungen zu verzeichnen. Insbesondere im ersten Halbjahr 2024 ist die Zahl der Angriffe deutlich gestiegen. Im April 2024 erreichte der Index gar knapp 160 Punkte. Aber auch die Qualität der Angriffe stieg deutlich an.

Im ersten Halbjahr 2023 hatten die Hacktivisten-Gruppen NoName057 mit ihrem Botnetz DDoSia und Killnet für Aufsehen gesorgt, indem unter anderem medienwirksam mehrere Webseiten von Landesregierungen und Polizeien lahmgelegt wurden, ohne nachhaltigen Schaden anzurichten. Daraufhin sahen sich die Angreifer offenbar genötigt, ihre Botnetze für bandbreitenstärkere DDoS-Angriffe weiter aufzurüsten.

So lag der Anteil bandbreitenstarker Angriffe, die maximale Bandbreiten von über 10.000 Megabits pro Sekunde erreichten, bei monatlich durchschnittlich 13 Prozent und damit fast doppelt so hoch wie im langjährigen Durchschnitt mit 6,75 Prozent. Im April 2024 gehörten sogar 28 Prozent der DDoS-Angriffe zu der besonders bandbreitenstarken Kategorie. Sollte sich dieser Trend fortsetzen, ließe dies auf eine nachhaltig leistungsfähigere Angriffsinfrastruktur der Angreifer schließen.

Informationen zu DDoS-Prävention und -Mitigation sowie eine Liste qualifizierter Mitigationsdienstleister finden sich auf der BSI-Webseite.

Weiterführende Informationen  
zu DDoS-Prävention und  
-Mitigation:



## Bekannt gewordene DDoS-Angriffe in Deutschland

### Messzahl

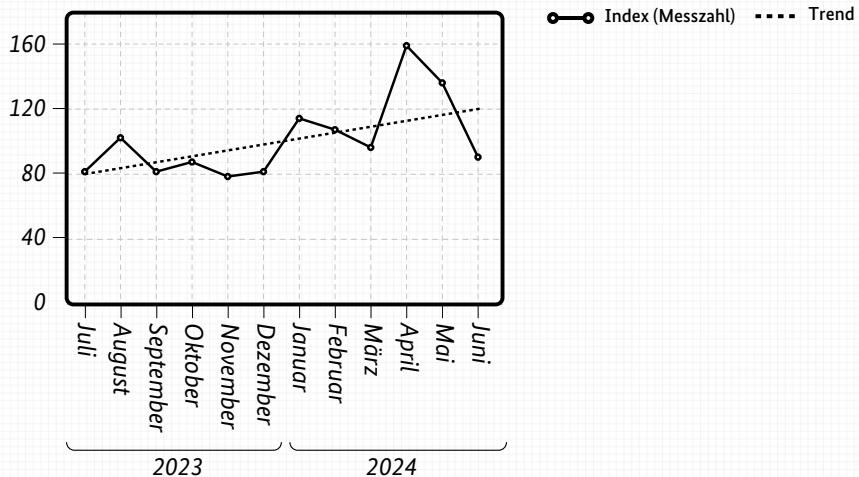


Abbildung 10 : Bekannt gewordene DDoS-Angriffe in Deutschland (Messzahl)

## Hochvoluminöse DDoS-Angriffe in Deutschland

### Anteile an allen bekannt gewordenen DDoS-Angriffe in Deutschland

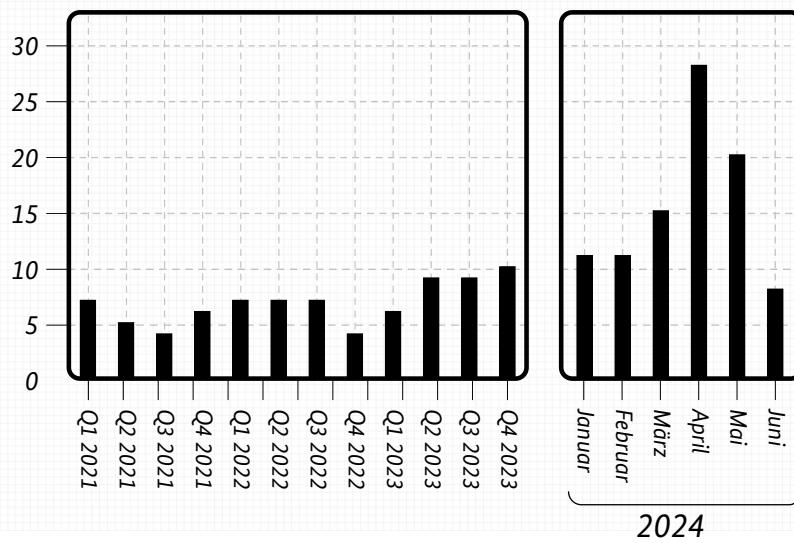


Abb. 11: Anteil hochvoluminöser Angriffe an allen bekannt gewordenen DDoS-Angriffen in Deutschland, Quelle: DDoS-Angriffsstatistik

### Abbildung 10 & 11 / DDoS-Angriffsstatistik:

**Ziel der Statistik** Strukturerhebung Distributed-Denial-of-Service-Angriffe (DDoS-Angriffe) gegen Ziele in Deutschland. Berichtet wird monatsweise. / **Grundgesamtheit** Alle DDoS-Angriffe gegen Ziele in Deutschland. / **Stichprobe** Alle DDoS-Angriffe gegen Ziele im AS 3320 (Deutsche Telekom). / **Erhebungsdesign/-instrumente** Monatsaggregation einer laufenden Erhebung aus der DDoS-Mitigation der Deutschen Telekom. / **Reichweite** Das AS 3320 der Deutschen Telekom umfasst zu etwa 98 % Ziele in Deutschland. / **Qualitätsbewertung** Abgleiche mit den Lageerkenntnissen der DDoS-Mitigationen anderer Dienstleister bestätigen regelmäßig die in der DDoS-Angriffsstatistik ermittelten Strukturen. Aussagen über das Aufkommen von DDoS-Angriffen in Deutschland insgesamt sind damit nicht möglich.

## 8.2 Leak-Opfer

Seit 2021 gehen Ransomware-Angriffe regelmäßig mit einem Datenleak einher. Dies dürfte auch auf die steigende Resilienz potenzieller Angriffsziele gegen Ransomware-Angriffe zurückzuführen sein.

Veröffentlichungen des IT-Sicherheitsdienstleisters Coveware zeigten für das dritte Quartal 2023<sup>10</sup> ein vorübergehendes Hoch von über 850.000 US-Dollar an durchschnittlich gezahlten Lösegeldern (vgl. Abbildung 12, Seite 47). Hintergrund ist die Leak-Angriffskampagne der Angreifer hinter Clop gegen MoveIT-File-Sharing-Server (vgl. Kapitel Ausnutzen von Zero-Day-Schwachstellen durch Ransomware-Angreifer, Seite 20, sowie Die Lage der IT-Sicherheit in Deutschland 2023, Seite 38). So forderten die Angreifer bei dieser Leak-Angriffswelle für die gestohlenen Daten wesentlich mehr Geld, als es sonst bei Ransomware-Angriffen und für verschlüsselte Daten der Fall ist. Auch wenn weniger Unternehmen auf diese Forderungen eingegangen sind, liegen erfolgte Zahlungen somit wesentlich höher als zuvor.

Im Rahmen der Kampagne gegen MoveIT-Server wurden über 250 mutmaßlich Betroffene auf der Leak-Seite der Angreifer hinter Clop im Juni und Juli 2023 verzeichnet. Dies ist eine außerordentlich hohe Anzahl mutmaßlich Betroffener für eine einzelne Angriffskampagne.

Die Angreifer stahlen dabei im großen Stil Daten von verwundbaren Servern. Die durchschnittlich pro Fall gezahlten Schweigegelder für die exfiltrierten Daten lagen fast dreimal so hoch, wie es bei reiner Lösegelderpressung zu erwarten gewesen wäre (vgl. Abbildung 10, Seite 46). Im 1. Quartal 2024 ist die durchschnittliche Höhe gezahlter Lösegelder jedoch wieder auf das Niveau von Ende 2022 zurückgefallen<sup>11</sup>.

Ransomware-Opfer, die beispielsweise mit einem funktionierenden, rückspielbaren Backup vorgesorgt haben, müssen sich hinsichtlich verschlüsselter Daten auf keinerlei Lösegeldverhandlungen mit den Angreifern einlassen. Dies illustriert auch der Anteil der Ransomware-Opfer, die nach einem Ransomware-Angriff noch Lösegeld zahlen. Berichten zufolge ist dieser von 56 Prozent zu Anfang 2021 auf inzwischen 36 Prozent gesunken (vgl. Abbildung 13, Seite 49)<sup>12</sup>.

Wenn Opfer aufgrund von Verschlüsselung ihrer Daten mit Ransomware nicht zahlen, drohen Angreifer im nächsten Schritt mit der Veröffentlichung exfiltrierter Daten, um den Erpressungsdruck aufrechtzuerhalten und die Opfer doch noch zu einer Zahlung zu bewegen.

Dieses Vorgehen ist bekannt als Schweigegelderpressung oder Double Extortion. Exfiltrierte Daten scheinen zudem wesentlich mehr Wert zu sein als verschlüsselte Daten (vgl. auch die Erpressungskampagne der Ransomware Gruppe Clop, die durch die Ausnutzung von Schwachstellen in

### Durchschnittliche Lösegeldzahlungen nach Quartal

In Dollar

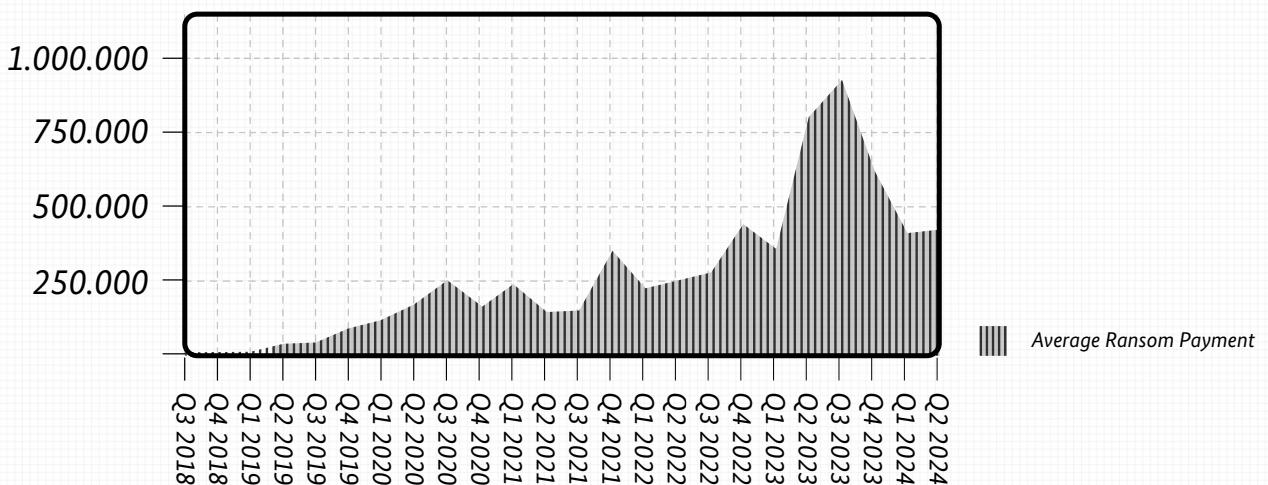


Abbildung 12: Durchschnittliche Lösegeldzahlungen nach Quartal (US-Dollar), (Quelle: Coveware)

Filesharing-Systemen ermöglicht wurde). Die Leak-Opfer-Statistik des BSI gibt Aufschluss über die Opfer von Schweigegelderpressungen. Zu diesem Zweck beobachtet das BSI sogenannte Leak-Seiten, auf denen Angreifer die Namen und die erbeuteten Daten von Opfern ihrer Ransomware-Angriffe veröffentlichen, wenn diese kein Lösegeld zahlen (vgl. auch *Die Lage der IT-Sicherheit in Deutschland 2023, Seite 19 f.*).

Über diese Leak-Seiten lassen sich also mutmaßliche Opfer erfassen, denen mit der Veröffentlichung ihrer Daten gedroht wurde. Die Leak-Opfer-Statistik ist insoweit keine Statistik über Ransomware-Angriffe, sondern über Opfer von Schweigegelderpressungen. Daher wird auch von mutmaßlichen Opfern gesprochen, denn die Nennung auf einer Leak-Seite unter Kontrolle eines Angreifers bedeutet nicht zwingend, dass es tatsächlich auch zu einem Angriff kam. In einigen Fällen nennen Angreifer Namen auch nur zum Zweck der Erpressung, ohne dass tatsächlich ein Angriff stattgefunden hat.

Die Anzahl an mutmaßlichen Opfern nahm in 2023, verglichen mit den Vorjahren, signifikant zu (vgl. Abbildung 14, Seite 50). Im Jahr 2023 wurde weltweit wie auch für Deutschland im Einzelnen fast das 1,7-Fache des Durchschnitts des Referenzjahres 2021 beobachtet. Weltweit betrachtet entsprach das einem Anstieg um nahezu 50 Prozent, in Deutschland um nahezu 30 Prozent binnen Jahresfrist. Der vorläufige Höhepunkt der Zeitreihe wurde im zweiten Quartal 2023 mit 1.395 erfassten mutmaßlichen Opfern weltweit und 65 mutmaßlichen Opfern aus Deutschland erreicht (vgl. Abbildung 15, Seite 51).

Wesentliche Faktoren für diesen Anstieg waren wahrscheinlich eine anhaltend hohe bis sehr hohe Aktivität der bedrohlichsten Akteure (vgl. Kapitel Ransomware-Gruppen, Seite 19).

Weiter beobachtete das BSI mehrere Leak-Seiten, die nur kurze Zeit aktiv waren oder durch einzelne Kampagnen viele mutmaßliche Opfer nannten. Daneben verzeichnete das BSI in der Breite aller beobachteten Leak-Seiten eine Zunahme der Aktivität.

Die fünf aktivsten Leak-Seiten sind regelmäßig für rund 40 Prozent der mutmaßlichen Opfer verantwortlich. Sie werden im Folgenden kurz vorgestellt. Weitere Informationen finden sich auf der BSI-Webseite<sup>13</sup>.

Die Ransomware-Gruppe hinter der RaaS LockBit unterhielt sowohl bei der Beschränkung auf Deutschland (vgl. Abbildung 16, Seite 52) als auch bei weltweiter Betrachtung (vgl. Abbildung 17, Seite 53) die aktivste Ransomware. Die Leak-Seite von LockBit nannte im Berichtszeitraum insge-

samt über 944 weltweit verteilte mutmaßliche Leak-Opfer. Die Ransomware-Gruppe Alphv (auch bekannt als Black-Cat) wurde erstmals im November 2021 beobachtet. Alphv zählte im Berichtszeitraum gemeinsam mit LockBit zu einer der bedrohlichsten Ransomware-Familien.

Die Ransomware-as-a-Service Alphv (auch bekannt als BlackCat) wurde erstmals im November 2021 beobachtet. Im März 2024 beendete die Betreibergruppe die Ransomware-as-a-Service Alphv mit einem Exitscam gegen ihre Affiliates. Die Betreiber behielten also rund um den Exitscam gezahltes Lösegeld ein, teilten dieses nicht mit Affiliates und waren sowohl für Affiliates wie auch Betroffene nicht mehr erreichbar. Alphv zählte im Berichtszeitraum gemeinsam mit LockBit zu einer der bedrohlichsten Ransomware-Familien.

Die Ransomware Play ist mindestens seit Juni 2022 aktiv. Die Angreifer setzen für die Erpressung neben Ransomware auch auf eine im November 2022 identifizierte Leak-Seite für Double Extortion. Die Ransomware Play ist nach derzeitigem Kenntnisstand einer exklusiven Gruppe von Affiliates (RaaS-Partnern) vorbehalten und wird daher als geschlossene Ransomware-Gruppe bewertet.

Die Angreifergruppe hinter der Ransomware Clop hat mit zwei größeren Angriffskampagnen im Jahr 2023 die Mehrheit der für diesen Angreifer beobachteten mutmaßlichen Opfer verursacht. In beiden Angriffskampagnen setzten die Angreifer nach Kenntnislage des BSI keine Ransomware ein, sondern stahlen Daten von verwundbaren File-Sharing-Servern.

Die Ransomware-Gruppe 8Base ist wahrscheinlich bereits seit 2022 aktiv. Im Mai 2023 wurde die Leak-Seite zu dieser Ransomware-Gruppe bekannt. Die Ransomware 8Base basiert auf der Ransomware Phobos. Anders als andere RaaS bietet Phobos ein Modell an, das ein eigenes Branding erlaubt. Dementsprechend sind viele Ransomware-Familien bekannt, die im Endeffekt Phobos mit anderem Namen sind. Auch bietet die Ransomware Phobos keine eigene Leak-Seite.

Die Ransomware-Gruppe Black Basta ist erstmals im April 2022 in Erscheinung getreten. In der öffentlichen Berichterstattung gibt es den Verdacht, dass die Black Basta in Verbindung mit der Gruppe Conti steht. Conti ist im Mai 2022 fragmentiert und seit Juni 2022 inaktiv. Das BSI betrachtet die Ransomware-Gruppe Black Basta unabhängig von Conti als eigenständige Bedrohung.

Ransomware-Angriffe werden gelegentlich mit weiteren Erpressungsmethoden flankiert, um den Zahlungsdruck beim Betroffenen zu erhöhen. So gehen einige Angreifer

aktiv auf Kundinnen und Kunden von Opfern zu und teilen ihnen mit, dass aufgrund eines nicht gezahlten Lösegelds sensible Daten über sie exfiltriert wurden. Verschiedene Angreifergruppen drohen auch damit, die erbeuteten Daten weiterzuverkaufen, sodass diese für weitere Cyberangriffe missbraucht werden können. Darüber hinaus setzen einzelne Angreifergruppen in der Verhandlungsphase auch zusätzlich DDoS-Angriffe ein, um ihren Lösegeldforderungen Nachdruck zu verleihen (*vgl. dazu detaillierter Die Lage der IT-Sicherheit in Deutschland 2023, Seite 21 f.*). Im aktuellen Berichtszeitraum wurde ein Fall bekannt, in dem Angreifer der Ransomware-Gruppe Alphv versucht haben sollen, ein Opfer gegenüber der US Securities and Exchange Commission (SEC) zu melden. Dies ist nach Kenntnislage des BSI der erste öffentlich bekannte Fall, in dem Angreifer ihrer Drohung nachgekommen sind, ein Opfer einer Regulierungsbehörde zu melden.

Ende 2022 beobachtete das BSI einen Trend unter cyberkriminellen Gruppen, auf Verschlüsselung zu verzichten und stattdessen die Daten nur zu stehlen. Dieser Trend hat sich im Berichtszeitraum nicht fortgesetzt. Zwar sind dem BSI weiterhin Gruppen bekannt, die wahrscheinlich nur auf Erpressung mit gestohlenen Daten setzen, aber diese Vorgehensweise hat sich nicht flächig verbreitet. Es ist jedoch davon auszugehen, dass auch in Zukunft reiner Datendiebstahl als Mittel der Erpressung – neben Datenverschlüsselung oder Double Extortion – eingesetzt werden wird.

## Ransomware-Opfer, die Lösegeld zahlten

Anteil in Prozent an allen Ransomware-Opfern

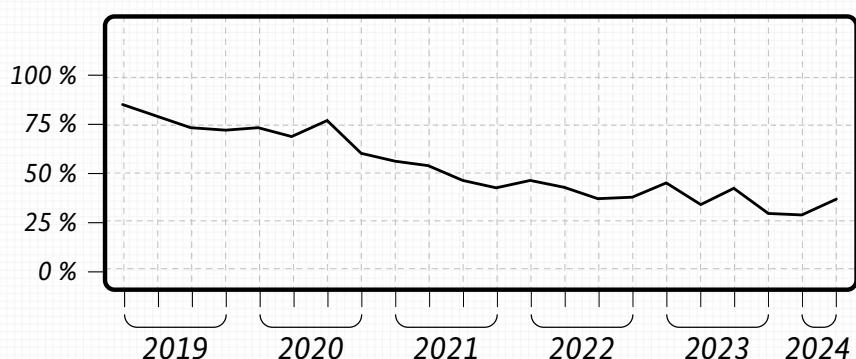


Abbildung 13: Ransomware-Opfer nach Zahlungsverhalten (Anteile) (Quelle: Coveware)

## Mutmaßliche Opfer auf Leak-Seiten aus Deutschland und weltweit

Anzahl

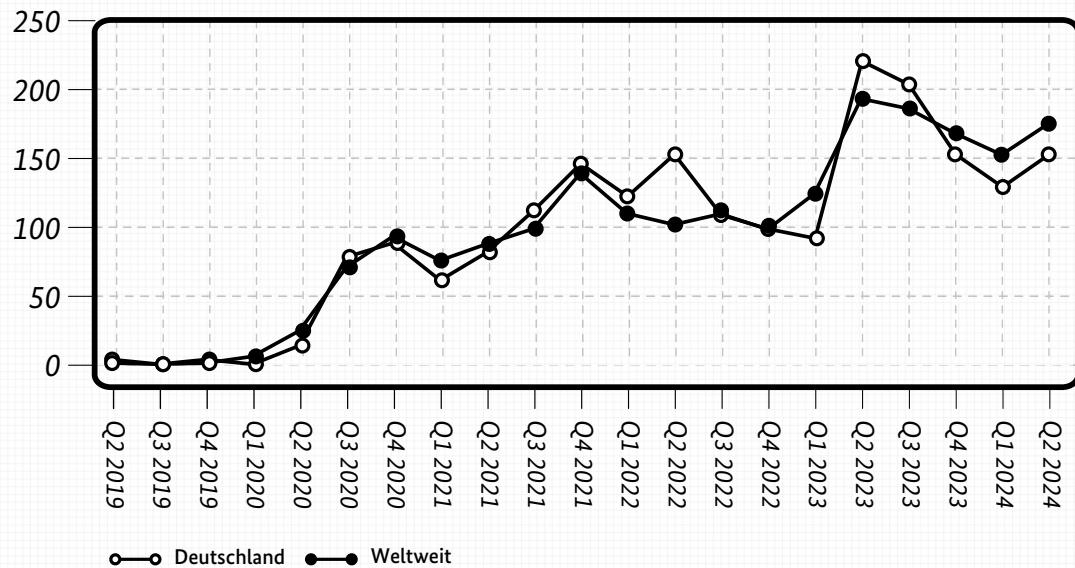


Abbildung 14: Mutmaßliche Opfer auf Leak-Seiten aus Deutschland und weltweit im Vergleich (2021 = 100)

## Mutmaßliche Opfer aus Deutschland auf Leak-Seiten

Anzahl

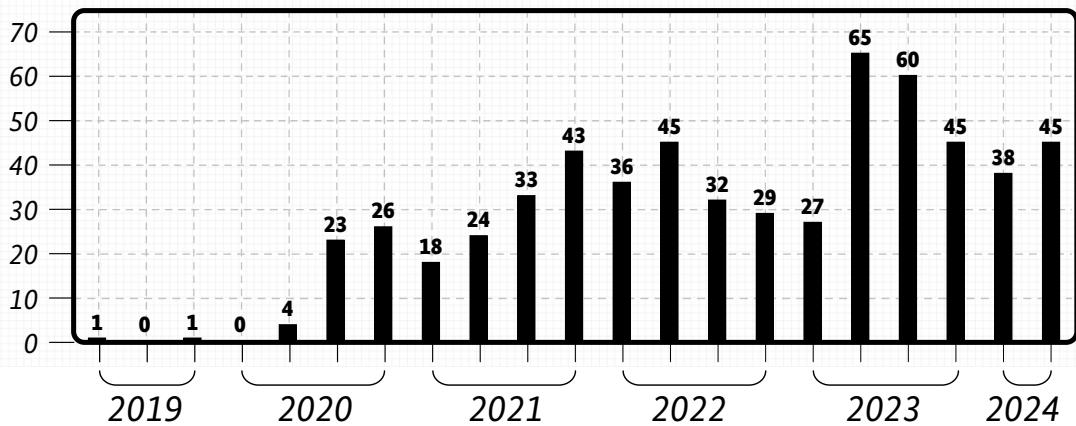


Abbildung 15: Mutmaßliche Opfer aus Deutschland auf Leak-Seiten (Anzahl)

## Mutmaßliche Opfer aus Deutschland nach Leak-Seiten

### Anteile

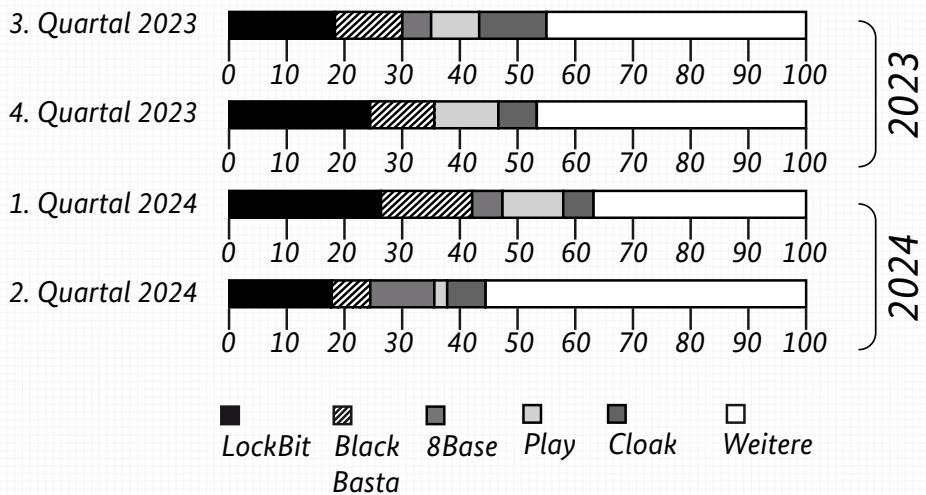


Abbildung 16: Mutmaßliche Opfer aus Deutschland auf Leak-Seiten (Anteile)

## Mutmaßliche Opfer weltweit nach Leak-Seiten

### Anteile

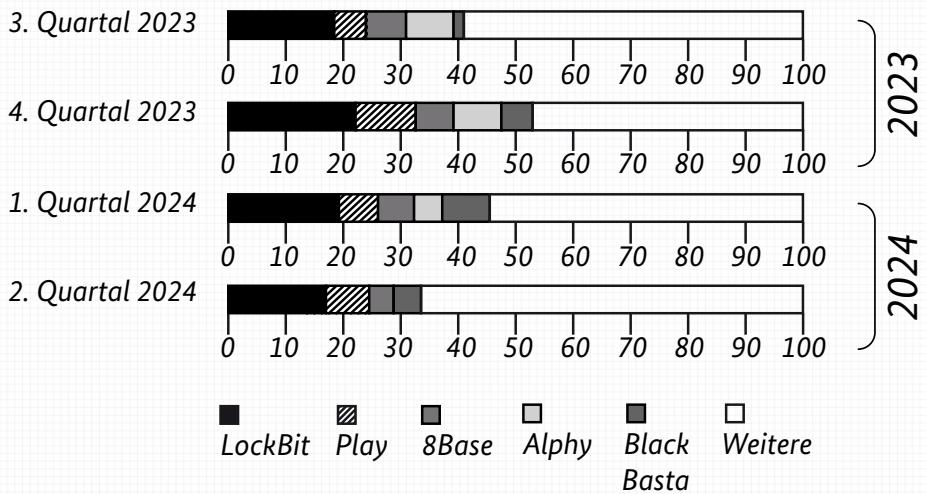


Abbildung 17: Mutmaßliche Opfer weltweit nach Leak-Seiten (Anteile)

### Abbildung 14, 15, 16 & 17 / Leak-Opfer-Statistik:

**Ziel der Statistik** Erhebung der Opfer von Daten-Leaks, die nach einem Ransomware-Angriff kein Löse-/Schweigegeld gezahlt haben und deren Daten daher auf einer Leak-Webseite einer Angreifergruppe veröffentlicht wurden, um den Erpressungsdruck zu erhöhen. Berichtet wird quartalsweise. / **Grundgesamtheit** Alle dedizierten Leak-Seiten, auf denen die Daten von Opfern von Daten-Leaks, die aus gezielten Cybercrime-Angriffen (Ransomware-Angriffe und Angriffe gegen neue Schwachstellen) stammen, veröffentlicht wurden. / **Stichprobe** Vollerhebung der bekannt gewordenen Leak-Opfer. / **Erhebungsdesign/-instrumente** Detektion von Daten-Dienstleistern, Meldungen von Opfern und öffentlichen Quellen. / **Reichweite** Keine Aussage über Anzahl der zugrundeliegenden Angriffe, sondern über die Anzahl zahlungsunwilliger Opfer, deren Daten auf einer Leak-Seite veröffentlicht wurden. Keine Unterscheidung von Ransomware-Opfern und Opfern von Datenexfiltration durch Schwachstellenausnutzung. / **Qualitätsbewertung** Hohe weltweite Abdeckung mit Abgleich verschiedener Datenquellen.

## Takedowns

Im Berichtszeitraum gelangen Strafverfolgern in international koordinierten Maßnahmen mehrere Takedowns gegen Ransomware-as-a-Service. Diese Erfolge zeigen den Verfolgungsdruck, der aktuell gegen Cyberkriminelle aufgebaut wird.

In einer international koordinierten Operation beschlagnahmten Strafverfolger zwischen dem 16. und 20. Oktober 2023 die Leak-Seite, Krypto-Wallets und Serverinfrastruktur der RaaS RagnarLocker. Auch wurde mindestens ein Hauptverdächtiger festgenommen. Aufgrund der Festnahme eines mutmaßlichen Entwicklers der Ransomware und Beschlagnahmung mehrerer Server ist nicht mit einer Rückkehr von RagnarLocker zu rechnen. Eine Rückkehr der Gruppe unter einem anderen Namen (Rebrand) konnte nicht beobachtet werden.

Am 19. Dezember 2023 gaben Strafverfolger eine internationale koordinierte Operation gegen die RaaS Alphv bekannt. Dabei wurden Teile der Serverinfrastruktur beschlagnahmt und teilweise Schlüsselmaterial sichergestellt. Wenige Tage nach den Maßnahmen setzten die Betreiber der RaaS Alphv eine neue Infrastruktur auf und versuchten, ihre Affiliates bei der RaaS zu halten. So konn-

ten auch weiter Angriffe mit Alphv beobachtet werden. Am 3. März 2024 wurde den Betreibern der RaaS Alphv ein Exit-Scam unterstellt und die Infrastruktur der Betreiber war seit 4. März 2024 nicht mehr verfügbar.

Am 19. Februar 2024 vollzogen Strafverfolgungsbehörden einen umfassenden Takedown gegen die RaaS LockBit. Zwischen dem 24. und 26. Februar 2024 wurde eine neue Leak-Seite für die RaaS LockBit beobachtet, auf der auch neue mutmaßlich Betroffene genannt wurden. Im März 2024 wurde auf der Leak-Seite eine Vielzahl an mutmaßlich Betroffenen veröffentlicht. Nach Einschätzung des BSI handelt es sich bei einer Vielzahl der seit März 2024 auf der Leak-Seite genannten mutmaßlich Betroffenen um Vorfälle, die noch vor dem Takedown stattgefunden haben und in denen wahrscheinlich auch ein Lösegeld gezahlt wurde. Es sind aber auch weiterhin tatsächliche Angriffe mit der RaaS LockBit zu beobachten.

Nach Takedowns gegen cyberkriminelle Services beobachtet das BSI häufig eine vorübergehende Abnahme der Aktivität in dem Feld, in dem der Service aktiv war. Allerdings war es bislang nur eine Frage von mehreren Wochen oder Monaten, bis bestehende oder neue cyberkriminelle Services die entstandene Lücke gefüllt haben. Auch lernen Angreifer aus den Gegenmaßnahmen der Strafverfolger, um diesen in der Zukunft zu entgehen.

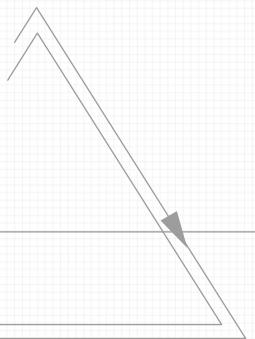
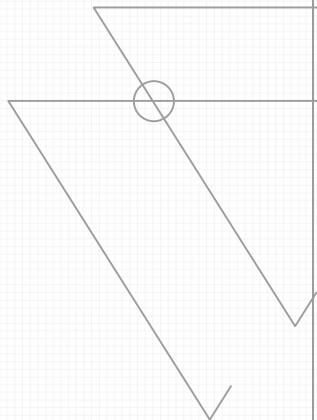
## 8.3 Angriffe auf die Cloud

Im Berichtszeitraum kam es zu mehreren erfolgreichen Ransomware-Angriffen auf Public-Cloud-Dienste, die deren Verfügbarkeit einschränkten, beispielsweise im Sommer 2023: Während des Umzugs eines Cloud-Anbieters in ein neues Rechenzentrum wurden die zu migrierenden Server an das interne Netz des Anbieters angeschlossen. Eine Schadsoftware, die sich zuvor bereits auf einem der Server befunden hatte, konnte dadurch auf die anderen Server übergreifen. Folglich wurde ein Großteil der Systeme des Anbieters und der Kundendaten inklusive deren Backups verschlüsselt. Die IT-Abteilung des Anbieters konnte die eigenen Systeme wiederherstellen. Kundendaten gingen in den meisten Fällen aber unrettbar verloren, wenn diese kein weiteres Backup hatten.

Zudem wurden mehrfach Fälle von Angriffen auf die Vertraulichkeit von Cloud-Diensten durch Identitätsdiebstahl, sowohl der Identitäten der Anwenderinnen und Anwender als auch des Personals des Anbieters, bekannt. So gelang es Angreifern, bei einem großen Cloud-Anbieter durch den Diebstahl eines Signaturschlüssels Token Forgery, das heißt Fälschung von Token, zu betreiben und die Identitäten legitimer Anwenderinnen und Anwender des Cloud-Dienstes zu imitieren. Dadurch war es den Angreifern möglich, auf deren Daten zuzugreifen. Nach Bekanntwerden des Angriffes wurden der Signaturschlüssel und die durch ihn signierten Token vom Anbieter gesperrt, um eine weitere Ausnutzung durch die Angreifer zu verhindern.

Bei einem anderen Cloud-Anbieter führte die Kompromittierung eines Dienstekontos dazu, dass Angreifer auf das Support-System für Kunden zugreifen und Support-Anfragen der Kunden exfiltrieren konnten. Die Anfragen enthielten auch vertrauliche Daten, die die Angreifer in einigen Fällen für Session-Hijacking-Angriffe gegen die betroffenen Kunden verwendeten. Nach Detektion der Kompromittierung wurde das betroffene Dienstekonto deaktiviert und mit diesem assoziierte Sessions terminiert.

Public Clouds werden kontinuierlich angegriffen und manchmal auch erfolgreich. Die größten Risiken bei der Cloud-Nutzung liegen jedoch bei der Anwenderin und dem Anwender selbst: Es gab viele in einen Datenverlust mündende Vorfälle, die auf Fehlkonfigurationen im ID-Management zurückzuführen waren. Auch der Bericht „2023 Cloud Security Study“ der Thales Group kommt zu dem Ergebnis, dass 55 Prozent aller cloudbezogenen Datenabflüsse in den befragten Unternehmen auf menschliches Fehlverhalten zurückzuführen waren.



# Kompromittierung der Microsoft-Cloud-Infrastruktur

## Sachverhalt

Am 11. Juli 2023 (sowie subsequent am 14. Juli 2023, 6. September 2023 und 12. März 2024) berichtete Microsoft in einem Blog-Beitrag über einen erfolgreichen Angriff auf OWA (Outlook Web Access) – und Outlook.com-Konten durch eine als Storm-0558 bezeichnete, mutmaßlich staatliche chinesische Angreifergruppe. Im Zuge dieses Angriffes sei den Angreifern der unberechtigte Zugriff auf die E-Mail-Konten von weltweit circa 25 Organisationen, inklusive Regierungseinrichtungen, gelungen.

Der Angriffsvektor war dabei die Kompromittierung eines Microsoft-Signaturschlüssels. Signaturschlüssel werden verwendet, um die Authentizität von Access Tokens, die bei der Authentisierung der Nutzerinnen und Nutzer zum Einsatz kommen, nachzuweisen. Durch den Zugriff auf den Signaturschlüssel war den Angreifern somit selbst die Auffertigung gültiger Access Tokens („Token Forgery“) möglich.

Der kompromittierte Signaturschlüssel war ausschließlich zur Signatur von Access Tokens für Microsoft Consumer Accounts berechtigt. Eine Regression in der Logik der Identitätsvalidierung, die von Microsoft bereitgestellt und von den betroffenen E-Mail-Diensten verwendet wurde, erweiterte jedoch den Gültigkeitsbereich des Signaturschlüssels auf Microsoft Consumer Accounts und Enterprise Accounts.

Zum aktuellen Zeitpunkt ist nicht bekannt, wie die Angreifer in den Besitz des Schlüssels gekommen sind.

## Bewertung

Laut Microsoft wurde der Zugriff, den die Angreifer sich verschafft haben, nur bei OWA und Outlook.com ausgenutzt, mutmaßlich hätten jedoch weitere Services betroffen sein können. Weiterhin war der Betroffenenkreis laut Microsoft auf circa 25 tatsächlich betroffene Organisationen beschränkt. Das tatsächliche Schadensausmaß war damit deutlich geringer als das Schadenspotenzial.

Der Vorfall zeigt, dass auch Public Clouds erfolgreich angegriffen werden können. Cloudinhärente Fähigkeiten, wie ausgeprägte Protokollierungs- und Detektionsmöglichkeiten, ermöglichen aber die Entdeckung, umfassende Analyse (inklusive belastbarer Bewertung des Schadensausmaßes) und Eindämmung des Angriffs.

## Reaktion

Die initiale Detektion des Angriffes erfolgte durch einen der betroffenen Microsoft-Kunden: Dieser wies Microsoft am 16. Juni 2023 darauf hin, dass eine Analyse seiner Protokolldaten anormalen Exchange-Online-Datenzugriff offenbart hatte. Microsoft setzte daraufhin bis zum 03. Juli 2023 Mitigationsmaßnahmen um, durch welche die Fortführung des Angriffs mit dem kompromittierten Schlüssel nach eigenen Angaben unterbunden wurde – eine Kundenintervention war somit nicht notwendig. Zu diesen Mitigationsmaßnahmen zählt insbesondere die Sperrung des Signaturschlüssels und der durch diesen signierten Access Tokens. Weiterhin konnte der Betroffenenkreis laut Microsoft durch die Analyse der vorhandenen Protokollierungsdaten exakt bestimmt und die Betroffenen informiert werden.

Infolge des Vorfalls hat das Department of Homeland Security's Cyber Safety Review Board (CSRB) der US-Regierung im August 2023 angekündigt, sich mit dem Fall zu befassen. Der daraus resultierende Bericht wurde am 2. April 2024 veröffentlicht und übt Kritik an Microsoft: Der Vorfall sei vermeidbar gewesen und die Sicherheitskultur von Microsoft sei unzureichend. Neben einer Darstellung der Untersuchungsbefunde enthält der Bericht auch eine Liste mit empfohlenen Sicherheitsmaßnahmen beziehungsweise technischen Verbesserungen, welche sich an Microsoft und andere Cloud-Anbieter richtet.

Das BSI hat sich ebenfalls intensiv mit den technischen Hintergründen des Vorfalls und möglichen Abwehrmaßnahmen angesichts der eingesetzten Angriffstechniken auseinandergesetzt und stand dabei von Beginn an im direkten Austausch mit Microsoft.

Als Ergebnis des gemeinsamen Austauschs veröffentlichte Microsoft ein technisches Informationsdokument zur korrekten Verwendung von Double Key Encryption (DKE). Dieses ermöglicht es Kunden erstmals, die Schutzwirkung von DKE und eventuell verbleibende Restrisiken in Abhängigkeit ihrer Einsatzkonfiguration zu bewerten und es dementsprechend korrekt einzusetzen. Unter diesen Bedingungen stellt DKE eine mögliche Abwehrmaßnahme gegen die hier eingesetzten Angriffstechniken dar.

# 9 – Erkenntnisse zur Gefährdungslage in der Gesellschaft

Um die Widerstandsfähigkeit (Resilienz) von Verbraucherinnen und Verbrauchern gegenüber Gefahren im Netz, wie beispielsweise Phishing, zu stärken, bedarf es verschiedener Ansatzpunkte. So stehen zum einen die Sensibilisierung, Aufklärung und Information der Verbrauchergruppen über Risiken und Sicherheitsmaßnahmen im Vordergrund. Dazu zählen auch die Notfallvorsorge und das Krisenmanagement im Umgang mit IT-Sicherheitsvorfällen im privaten Umfeld. Zum anderen ist die technische Sicherheit durch anbieterseitige aktive (technische) Schutzmaßnahmen und die Förderung sicherer, nutzerfreundlicher Produkte (Usable Security) von großer Bedeutung. Dazu gehören auch die Etablierung praktikabler Sicherheitsstandards bei der Entwicklung digitaler Produkte und Dienste (Security by Design, Security by Default) sowie eine Transparenzverpflichtung der Hersteller und Anbieter hinsichtlich ihrer IT- und Datensicherheitsmaßnahmen. Ein effektiver Digitaler Verbraucherschutz ist eine gesamtgesellschaftliche Aufgabe: So sollten Kooperation, Vernetzung und Austausch zwischen IT-Sicherheitsakteuren aus Zivilgesellschaft, Wissenschaft, Wirtschaft und öffentlichem Sektor weiter gefördert werden, um die Resilienz der Verbraucherinnen und Verbraucher im digitalen Raum zu stärken.

Das BSI nimmt eine zentrale Rolle bei der Prävention und Erkennung von IT-Sicherheitsrisiken sowie bei der Reaktion auf diese ein. Evidenzbasierte Arbeiten wie Umfragen oder Studien im Verbrauchermarkt bilden dabei eine wichtige Grundlage, um im Dialog mit Herstellern und Anbietern die IT-Sicherheit für Verbraucherinnen und Verbraucher kontinuierlich zu verbessern.

## 9.1 Gefährdungslage am digitalen Verbrauchermarkt

Im Cybersicherheitsmonitor (CyMon) 2024 ist die Betroffenheit von Verbraucherinnen und Verbrauchern von Cyberkriminalität auf ähnlich hohem Niveau wie in der Vorjahresbefragung. Etwa ein Viertel der Befragten war bereits von Cyberkriminalität betroffen (24 %; 2023: 27 %). Im Vergleich zum Vorjahr hat sich der erlittene Schaden in Bezug auf Vertrauensverlust (30 %; 2023: 33 %), zeitliche Schäden (24 %; 2023: 26 %) oder emotionale Schäden (23 %; 2023: 23 %) kaum verändert. Vertrauensverlust wird weiterhin am häufigsten genannt. Die Anzahl Betroffener, die in den letzten zwölf Monaten einen finanziellen Schaden erlitten, hat jedoch zugenommen (26 %; 2023: 18 %).

## Studie

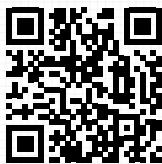
Zu Beginn des Jahres 2024 hat das BSI die Untersuchung „IT-Sicherheit am digitalen Verbrauchermarkt: Fokus Steuererklärungsapps“ veröffentlicht. Im Rahmen der Studie wurden 97 Sicherheitsmängel, darunter 75 Schwachstellen, in den neun untersuchten Apps entdeckt und im Dialog mit den Herstellern behoben. Fehlende Sicherheitsupdates, unzureichende Passwortrichtlinien und die teils fehlende Option für eine Zwei-Faktor-Authentisierung sind einige Mängel, die dabei an die Hersteller gemeldet wurden.

Weiterführende Informationen zur  
Studie zu Steuererklärungsapps:



Ebenfalls geht aus der Erhebung hervor, dass die Betroffenheit von Verbraucherinnen und Verbrauchern auf einem konstanten Niveau bleibt. Wie bereits 2023 geben 15 Prozent der Befragten an, in den letzten zwölf Monaten Opfer eines Phishing-Angriffs geworden zu sein.

**Weitere Informationen zur aktuellen Bürgerbefragung zur Cybersicherheit in Kooperation der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) und des BSI erhalten Sie unter:**



Innerhalb des Berichtszeitraums sind im Service-Center des BSI 8.244 Anfragen von Verbraucherinnen und Verbrauchern eingegangen. Das sind durchschnittlich 687 Anrufe pro Monat, die das BSI zu Anliegen von Verbraucherinnen und Verbrauchern entgegennimmt und beantwortet. Mehr als ein Drittel der Anfragen (39 %) handelt dabei von konkreten IT-Sicherheitsvorfällen. Unter den Anfragenden war auch hier Phishing, inklusive der Variationen Vishing und Smishing, das am häufigsten genannte Anliegen (35,3 % aller gemeldeten IT-Sicherheitsvorfälle).

### Anteile betroffener Verbraucherinnen und Verbraucher in Prozent

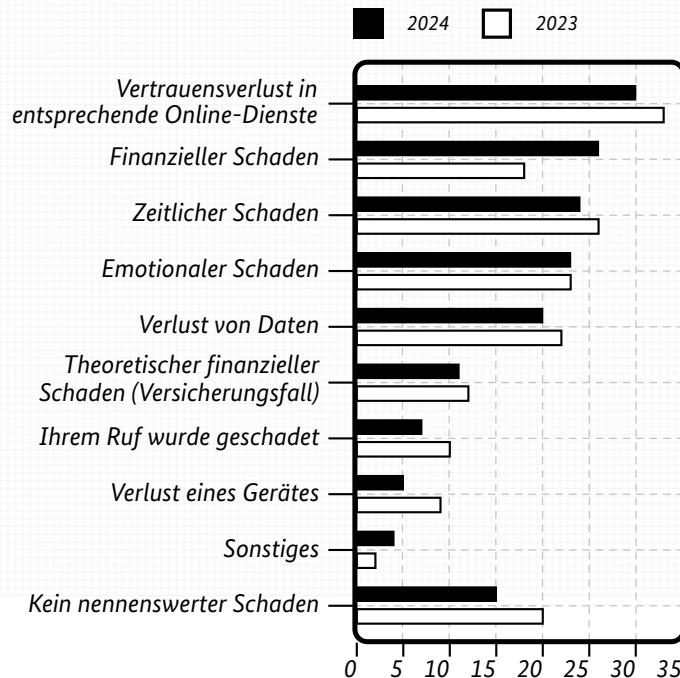


Abbildung 18: Anteile betroffener Verbraucherinnen und Verbraucher (CyMon 2023 und 2024, Mehrfachnennung möglich, in Prozent, n = 3.012 (2023) / 3.047 (2024))

## Anfragen von Verbraucherinnen und Verbrauchern an das Service Center des BSI

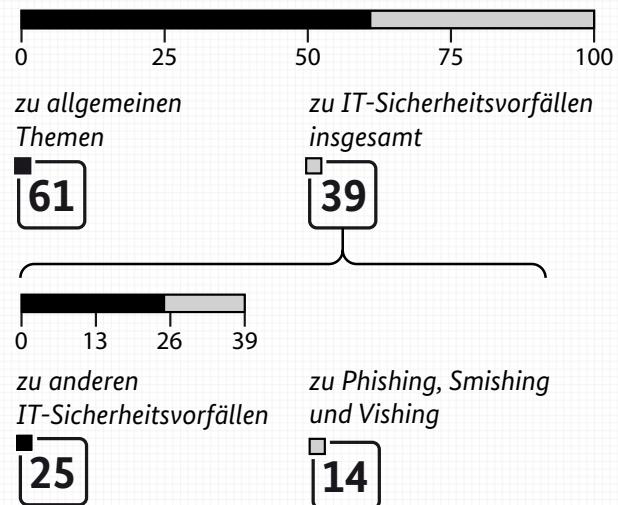


Abbildung 19: Anfragen von Verbraucherinnen und Verbrauchern an das Service-Center des BSI

### Datenleaks im Kontext der Verbraucherbetroffenheit

Seit Beginn des Jahres 2024 erfasst die Marktbeobachtung des BSI in strukturierter Art und Weise Datenleaks von Verbraucherdaten. Daraus werden Erkenntnisse über Ausmaß und Verlauf der Betroffenheit von Verbraucherinnen und Verbrauchern in Deutschland abgeleitet. Über die seitdem registrierten Datenleaks (Fälle mit Verbraucherbetroffenheit, Mehrfachnennung, n = 98) waren jeweils Namen (83 %) und E-Mail-Adressen (53 %) die am häufigsten geleakten Informationen. Auch weitere persönliche Informationen, wie Adress- und Geburtsdaten sowie Telefonnummern, sind in mehr als einem Drittel aller Fälle betroffen. Bei etwa einem Viertel der Datenleaks sind jeweils besonders sensible Informationen, wie Bezahldaten oder Sozialversicherungsnummern, abgeflossen.

Bei 14 Prozent der registrierten Datenleaks waren Verbraucherinnen und Verbraucher in Deutschland direkt betroffen. In 46 Prozent der registrierten Fälle ist davon auszugehen, dass keine Verbraucherinnen und Verbraucher aus Deutschland betroffen sind. Bei 40 Prozent der Fälle ist die Betroffenheit unbekannt oder nicht eindeutig feststellbar. Deutlich wird, dass Datenleaks nicht auf Landesgrenzen beschränkt sind.

### Fallbeispiel eines Datenleaks

Am 23. September 2023 wurde ein Dienstleister für Cloud-PC-Gaming mutmaßlich Opfer eines Datenleak-Vorfalls, bei dem Verbraucherdaten von einer Exfiltration betroffen waren. Den Informationen des Unternehmens zufolge wurde der Angriff überhaupt erst mit einer Erpressernachricht bekannt. Nach forensischer Prüfung der IT-Systeme waren gestohlene Session-Cookies und ein darauf folgender Missbrauch eines Accounts des Unternehmens Ursache des Datenleaks. Es wurden 500.000 Kundeninformationen exfiltriert, die auf circa 60.000 betroffene Verbraucherinnen und Verbraucher in Deutschland zurückzuführen waren. Zu den abgeflossenen Daten zählten Namen, E-Mailadressen, Geburtsdaten, Rechnungsanschriften und Ablaufdaten von Kreditkarten. Aus dem Gespräch mit dem Unternehmen geht zudem hervor, dass die Firma Kundinnen und Kunden über den Vorfall informiert hat. Es wurde vor möglichen Phishing-E-Mails auf Basis der gewonnenen Daten sowie vor potenziellen Risiken für Account-Übernahmen gewarnt.

Das BSI befürwortet den transparenten Umgang mit Datenleaks sowie das Kommunizieren von angemessenen Hilfestellungen gegenüber Verbraucherinnen und Verbrauchern, damit diese sich selbst vor weiteren potenziellen Schäden schützen können.

## Art der geleakten Informationen nach Häufigkeit

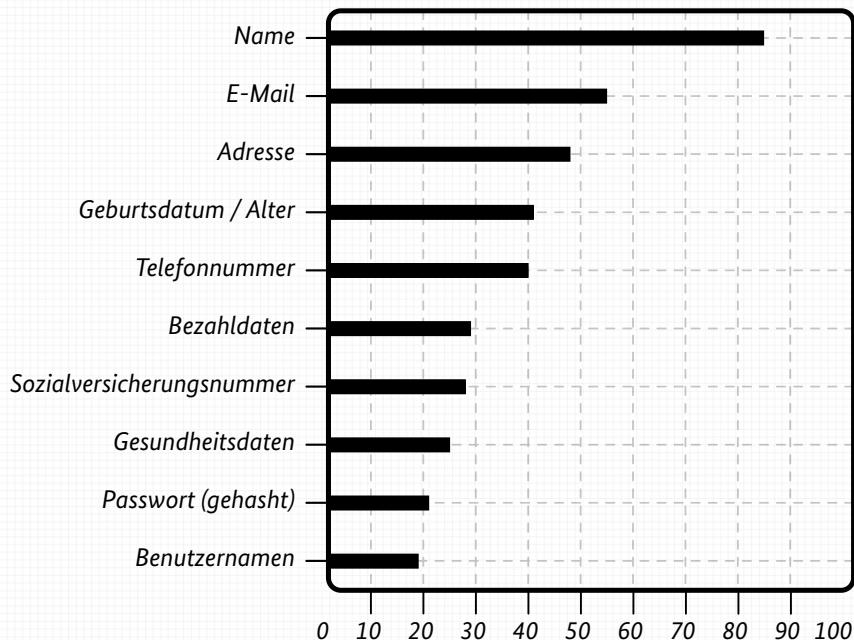


Abbildung 20: Art der geleakten Informationen nach Häufigkeit (Fälle mit Verbraucherbetroffenheit, Mehrfachnennung, in %, n = 98)

## Betroffenheit von Verbraucherinnen und Verbrauchern aus Deutschland

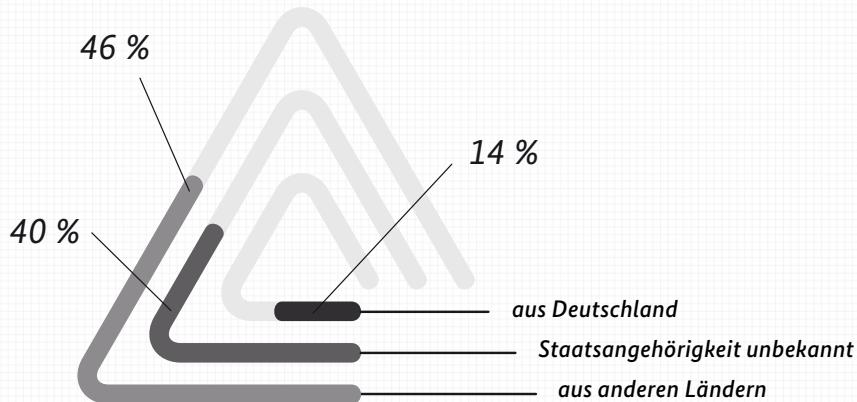


Abbildung 21: Betroffenheit von Verbraucherinnen und Verbrauchern aus Deutschland an registrierten Datenleaks (in Prozent, n = 141)

## 9.2 Gefährdungslage in sozialen Netzwerken

Der häufig synonym verwendete Begriff der sozialen Medien (engl.: Social Media) steht für viele unterschiedliche digitale Kommunikations- und Verbreitungswege. Neu ist, dass Texte, Bilder und Videos nicht mehr nur menschlichen

Ursprungs sind, sondern zu Teilen durch Anwendungen, die auf einer Künstlichen Intelligenz basieren, generiert werden. Die Gefährdungslage in sozialen Netzwerken hat sich durch KI-generierte Desinformation verschärft. Das liegt daran, dass sich Unwahrheiten durch die technischen Möglichkeiten schneller verbreiten, vor allem wenn sie nicht als manipuliert erkennbar sind. Desinformationskampagnen können mit vergleichsweise geringem Aufwand zielgruppen-spezifisch und algorithmenbasiert ausgespielt werden.

Gleichzeitig muss man konstatieren, dass Menschen soziale Netzwerke in ihr Informations- und Suchverhalten einschließen, im vorliegenden Fall in die Suche nach Informationen über Cybersicherheit (vgl. Abbildung 22, Seite 61). Mehr als ein Drittel der Befragten benutzt soziale Netzwerke für die Informationssuche – Tendenz steigend.

Insbesondere die Befragten in der Altersklasse zwischen 16 und 39 Jahren nutzen soziale Medien verstärkt als Informationsquelle (vgl. Abbildung 23, Seite 62). Hier stellt sich die Frage, ob Nutzerinnen und Nutzer erkennen können, was Fakt und was Fake ist.

Dies offenbaren zurückhaltende Interventionen der kontrollierenden Netzwerkbetreiber. Technische Einschränkungen und eine angestrebte Balance zwischen freier Meinungsäußerung und dem Schutz anderer Nutzender sind hier zentrale Herausforderungen.

### Schwerpunkt: Social Bots, Desinformation und Künstliche Intelligenz

Zur gezielten Beeinflussung und Manipulation von Nutzenden können automatisierte Accounts eingesetzt werden. Diese sogenannten „Social Bots“ können ähnlich wie Menschen agieren. Durch gezielte Likes sowie das Teilen und Kommentieren bestimmter Inhalte können sie vermeintliches Interesse simulieren und so die Empfehlungsalgorithmen der Plattformen so beeinflussen, dass sie gewünschte Inhalte häufiger vorschlagen. Auf diese Weise können manipulierte und gefälschte Inhalte automatisiert und in großem Maße verbreitet werden. Eine zunehmende Politisierung und damit verbundene Instrumentalisierungsversuche sind gerade vor dem Hintergrund geopolitischer Lagen oder bevorstehender Wahlen an der Tagesordnung. Die Plattformen verzeichnen insbesondere im Vorlauf von Wahlen eine signifikante Zunahme solcher Aktivitäten.

## Über welche der folgenden Kanäle suchen Sie Informationen über Cybersicherheit?

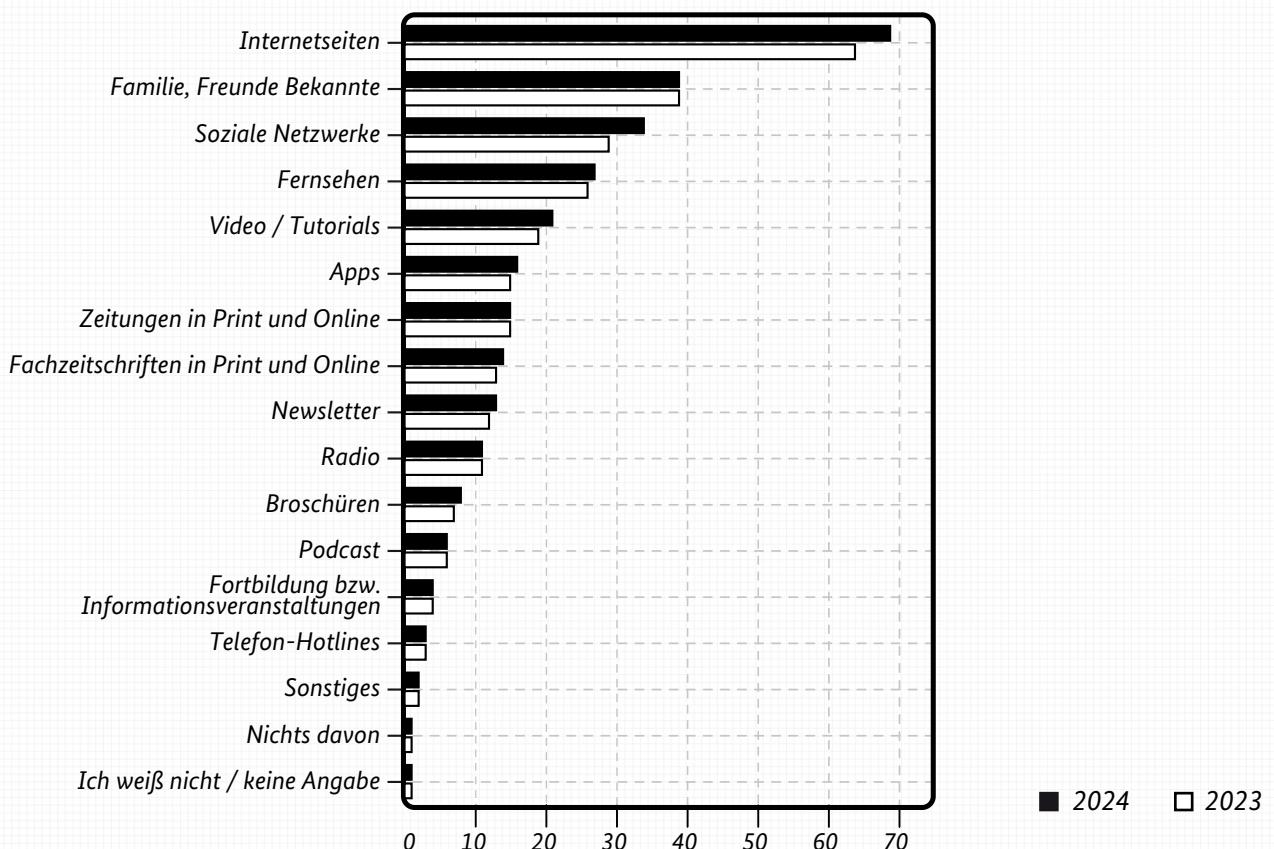


Abbildung 22: Über welche der folgenden Kanäle suchen Sie Informationen über Cybersicherheit? Quelle: Cybersicherheitsmonitor 2024

Obwohl Betreiber sehr großer Online-Plattformen laut EU-Verordnung über Digitale Dienste (Digital Services Act) verpflichtet sind, mit Blick auf systemische Risiken nach bestimmten Kriterien festgelegte Inhalte zu moderieren oder zu entfernen, sind diese Anforderungen in der Praxis noch nicht hinreichend umgesetzt worden. Ein Grund dafür ist, dass durch neue und schnellere Verschleierungstaktiken gefälschte Inhalte (Desinformation)

schwieriger von seriösen Informationen zu unterscheiden sind. Oftmals wird die Verbreitung gefälschter Informationen durch KI-basierte Social Bots gestützt.

Die Plattformen setzen zur Erkennung fragwürdiger Inhalte und Accounts inzwischen selbst zunehmend KI-basierte Methoden ein. Hier gilt es, die eingesetzten Mechanismen zur Erkennung dauerhaft zu verstärken.

## Genutzte Informationsquellen Cybersicherheit

Informationsquellen nach Alter in Prozent

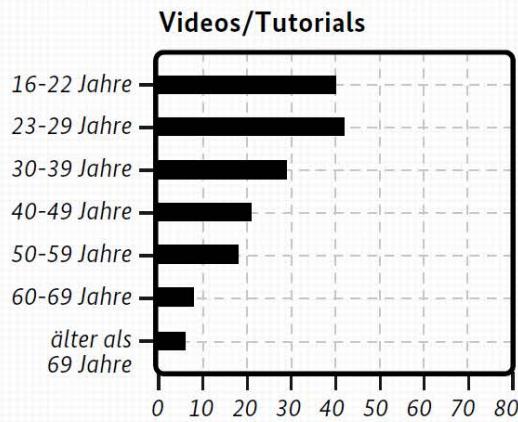
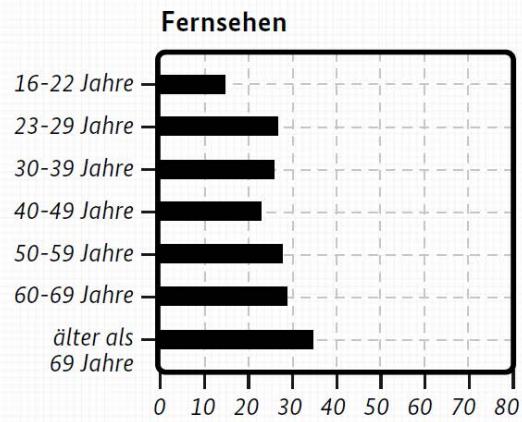
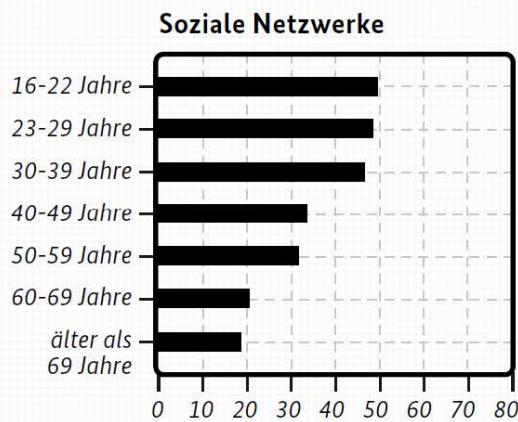
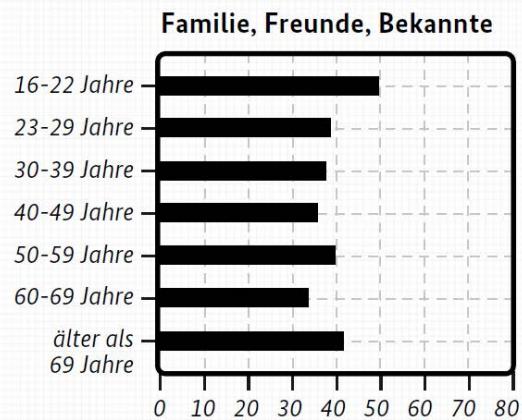
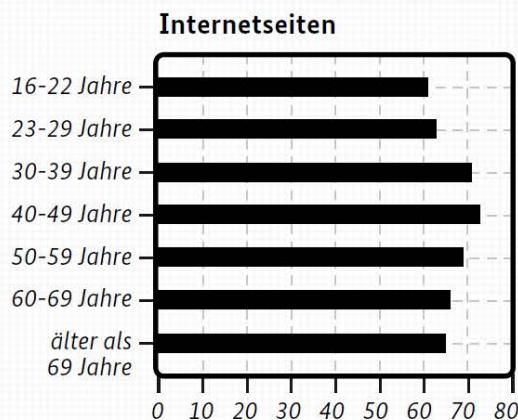


Abbildung 23: Genutzte Informationsquellen Cybersicherheit – Informationsquellen nach Alter

# 10 – Erkenntnisse zur Gefährdungslage in der Wirtschaft

Wie schon in den vergangenen Jahren zählen Cyberrisiken auch 2023 weiterhin zu den Top-10-Bedrohungen für Unternehmen weltweit<sup>14</sup>. Cybersicherheit muss seitens der Unternehmensleitung auf die Agenda gebracht und als unternehmensweites Risiko betrachtet werden. Einer aktuellen Studie von Pricewaterhouse Coopers zufolge ist das Bewusstsein in der Führungsebene gestiegen. So geben 42 Prozent der befragten Führungskräfte an, sich von Cyberrisiken bedroht zu fühlen<sup>15</sup>. Die Verantwortlichen nehmen Cybersicherheit als einen entscheidenden Faktor für die Unternehmenssicherheit, aber auch als Wettbewerbsvorteil wahr. Dies spiegelt sich in konkreten Maßnahmen wider. Unternehmen investieren mehr in den Bereich IT-Sicherheit. Seit 2020 sind die Ausgaben für das IT-Sicherheitsbudget in Unternehmen kontinuierlich gestiegen. Das Statistische Bundesamt geht für den Zeitraum von 2020 bis 2025 von einer jährlichen Wachstumsrate von 10,5 Prozent aus<sup>16</sup>. 2023 wurde mit rund 8,5 Milliarden Euro so viel wie noch nie in Cybersicherheit investiert. Das BSI begrüßt diese Entwicklung und empfiehlt seit Langem feste Mindestausgaben für eigene Cybersicherheitsmaßnahmen.

## Hohe Bedrohung

Gleichzeitig sehen sich Unternehmen zunehmend Cyberangriffen ausgesetzt. Deutsche Unternehmen haben nach Schätzungen des Digitalverbandes Bitkom im Jahr 2023 aufgrund von digitalen Angriffen, Industriespionage und Sabotage einen Schaden von rund 206 Milliarden Euro<sup>17</sup> erlitten. Davon fallen laut Bitkom 148 Milliarden Euro – also drei Viertel des Gesamtschadens – auf die größte Bedrohung Cyberangriffe. Die Angriffe auf Wirtschaftsunternehmen sind dabei breit gestreut. Einerseits werden nach wie vor umsatzstarke Großunternehmen angegriffen. Gleichzeitig werden vor allem Ransomware-Angriffe aufgrund des geringeren technologischen Aufwands bei der Nutzung von Ransomware-as-a-Service auch zum Massengeschäft. Dabei gehen die Kriminellen wie bereits beschrieben oft den Weg des geringsten Widerstandes, sodass zunehmend die kleinen und mittleren Unternehmen (KMU), aber auch Kommunen, Universitäten und Forschungseinrichtungen stärker betroffen sind. Gerade KMU haben oft ein niedrigeres Budget für Cybersicherheit oder das Thema generell nicht ausreichend auf der

Agenda (vgl. Kapitel *Gefährdungslage der KMU in Deutschland*, S. 68). Das BSI beobachtet in dieser Professionalisierung den Aufbau einer Cybercrime-Schattenwirtschaft (vgl. Kapitel *Ransomware-Gruppen*, Seite 19). Unternehmen stehen keinem einzelnen Angreifer, sondern einer arbeitsteiligen und effizient aufgestellten Angreiferindustrie gegenüber. Im internationalen Umfeld finden von einigen Staaten unterstützte oder geduldete Cyberkriminelle sichere Häfen für ihre Aktivitäten.

Die größte Bedrohung für Wirtschaftsunternehmen sieht das BSI nach wie vor in Ransomware (vgl. Kapitel *Cyberkriminelle Schattenwirtschaft*, Seite 19). Weitere häufige Schäden entstehen durch Phishing, Malware und Passwortdiebstahl<sup>18</sup>. Mit den Schäden durch solche Angriffe einher geht oft ein Gefühl der Unsicherheit gegenüber einer erfolgreichen Digitalisierung – mit teilweise gravierenden Folgen für die Innovationsfähigkeit und digitale Transformation betroffener Unternehmen.

Des Weiteren erleben Unternehmen die sich verändernde globale Sicherheitsarchitektur als große Herausforderung. Unternehmen und auch Forschungseinrichtungen haben Sorge, Ziel von politisch motivierter Spionage, Industriespionage oder politisch motivierten Cyberangriffen zu werden<sup>19</sup> (vgl. Kapitel *Cyberaktivitäten im Rahmen geopolitischer Spannungen und Konflikte*, Seite 22).

## Künftige Herausforderungen

Unternehmen setzen bereits heute vermehrt auf den Einsatz Künstlicher Intelligenz. Der Einfluss der KI auf die Wirtschaft wird in Zukunft ohne Zweifel weiter zunehmen. In einer aktuellen Studie geben 70 Prozent der befragten Unternehmen an, dass der Einsatz von KI die Entwicklung und Arbeitsweise der Unternehmen erheblich verändern wird<sup>20</sup>. Gleichzeitig sehen 64 Prozent hier aber auch ein erhöhtes IT-Sicherheitsrisiko und drücken so ihre gegenwärtige Verunsicherung hinsichtlich dieser neuen Technologie aus. Das BSI plädiert für einen pragmatischen Einsatz von KI und stellt Hilfestellungen für den Einsatz von KI in Unternehmen zur Verfügung. Unternehmen, die von den Produktivitätsgewinnen beim Einsatz von KI profitieren wollen, müssen in Cybersicherheit investieren, um diese Technologie sicher beherrschen zu können.

**Weiterführende Informationen  
zum Einsatz von KI in Unternehmen:**



Ein weiterer wesentlicher Faktor sind der Austausch und die Kommunikation zu Sicherheitsvorfällen: Immer mehr Unternehmen gehen transparent mit einem Vorfall um und informieren die Öffentlichkeit und ihre Kundinnen und Kunden. Dies trägt dazu bei, dass potenzielle Sicherheitslücken schneller geschlossen und Schäden von weiteren Unternehmen abgewendet werden können, aber auch, dass anhand von Best Practices Beispiele bekannt werden, wie Unternehmen erfolgreich ihre Cybersicherheit verbessern konnten. Das BSI bietet über das Melde- und Informationsportal die Möglichkeit, über einen Vorfall zu berichten und so zum Lagebild beizutragen<sup>24</sup>.

Cybersicherheit ist eine Teamaufgabe. Durch Kooperation entstehen resiliente, tragfähige Strukturen. Mit seinen Angeboten für die Wirtschaft, beispielsweise der Publikationsreihe „Management Blitzlicht“ und dem Netzwerk der Allianz für Cyber-Sicherheit, trägt das BSI dazu bei.

#### **Resilienz und Kooperation**

Das gestiegene Bewusstsein für Cyberrisiken sollte sich vor allem in passenden Schutzmaßnahmen niederschlagen. Konkrete Schritte zum Schutz des eigenen Unternehmens sind unerlässlich. Um sich in dieser Bedrohungslage gut aufzustellen, müssen Unternehmen weiter in ihre Resilienz investieren. Dazu gehören technische und organisatorische Maßnahmen wie regelmäßige Sicherheitsupdates, Backups und Mitarbeiter Schulungen, Zertifizierungen nach ISO 27001 und IT-Grundschutz. Während große Unternehmen hier zumeist gut aufgestellt sind, haben KMU dringenden Nachholbedarf (vgl. Kapitel *Gefährdungslage der KMU in Deutschland, Seite 68*). Das BSI stellt zahlreiche Angebote für KMU bereit. Wenn es um das Erstellen von Notfallplänen geht, können Unternehmen aller Größenordnungen ihre Maßnahmen intensivieren. Weniger als ein Drittel der Unternehmen verfügt über einen schriftlich fixierten Notfallplan. Das BSI bietet hier mit dem „Maßnahmenkatalog Notfallmanagement“<sup>21</sup> und einem Übersichtsdokument für die Zielgruppe KMU einen leichten Einstieg in das Notfallmanagement<sup>22</sup>. Ebenso wichtig wie Maßnahmen zur Steigerung der Resilienz ist auch das regelmäßige Einüben der getroffenen Maßnahmen. Ein Backup ist nur dann hilfreich, wenn es auch wieder eingespielt werden kann. Ein wichtiges Werkzeug für mehr Resilienz ist zudem der BSI-Standard 200-4 für ein gesamtheitliches Business Continuity Management (BCM). Die praxisnahe Anleitung hilft, nach einem konkreten IT-Sicherheitsvorfall die Unterbrechung des Betriebes zu minimieren<sup>23</sup>.

## **10.1 Gefährdungslage Kritischer Infrastrukturen**

Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. KRITIS bilden eine entscheidende Grundlage für das Funktionieren unserer Gesellschaft. Dennoch erkennt man ihre Bedeutung gelegentlich erst, wenn es zu Störungen kommt. Kritische Infrastrukturen sind besonders von einer störungsfreien arbeitenden IT abhängig.

#### **Anhaltend angespannte Gefährdungslage**

Die Gefährdungslage für Unternehmen bleibt ange spannt, die Zahl der Cybervorfälle steigt. Dies gilt auch für die Teilmenge der Unternehmen, die zu den Kritischen Infrastrukturen gehören. Erfolgreiche Angriffe auf KRITIS-Betreiber können nicht nur zu wirtschaftlichen Schäden führen, sondern sich auch auf die Versorgung der Bevölkerung mit kritischen Dienstleistungen auswirken. Um diesen Herausforderungen zu begegnen, müssen Betreiber ein hohes Niveau an Cybersicherheit erreichen und halten.

## Meldungen nach KRITIS-Sektoren

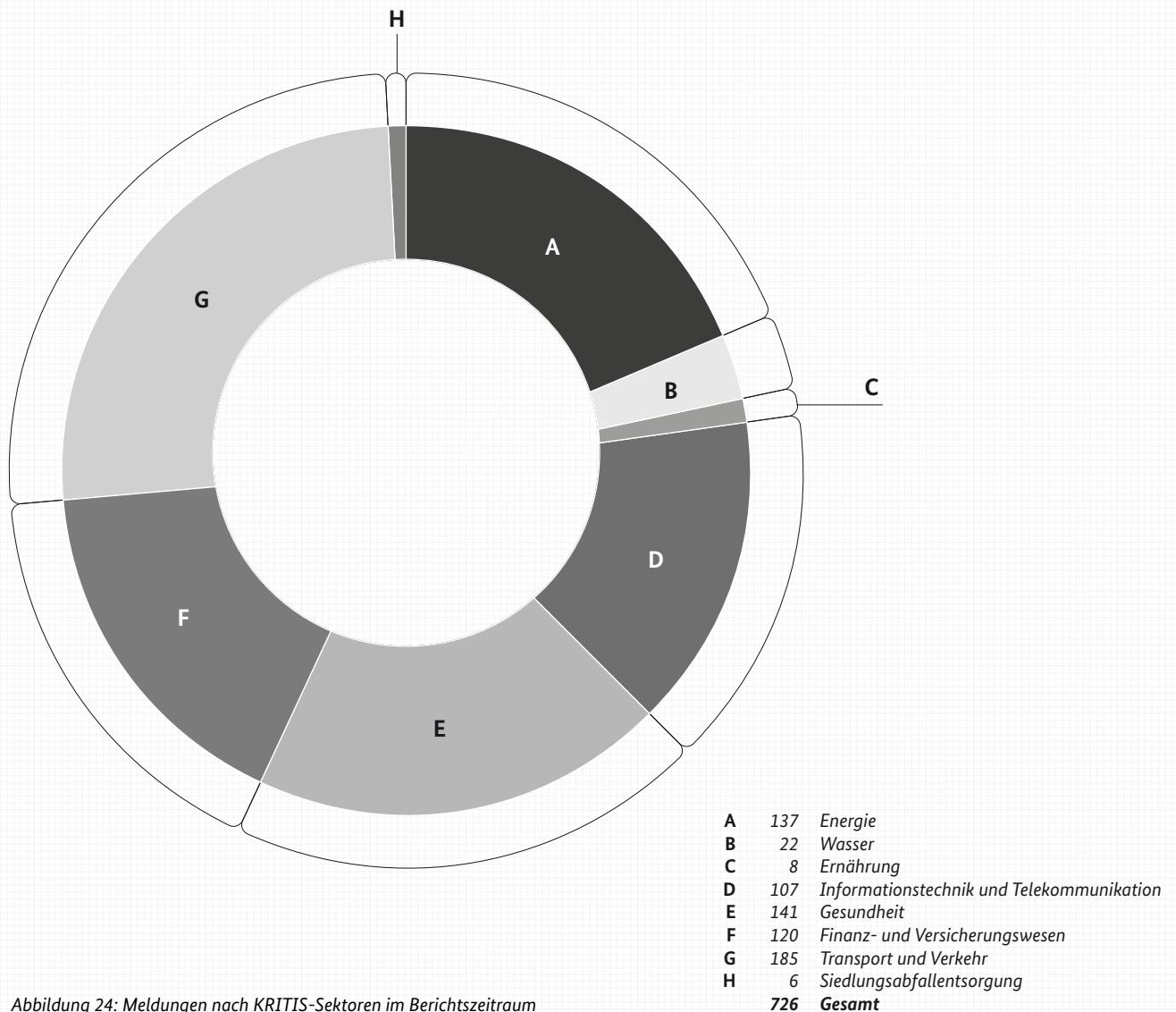


Abbildung 24: Meldungen nach KRITIS-Sektoren im Berichtszeitraum

### Meldungen verbessern das Lagebild

§ 8b Abs. 4 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) sieht eine Meldepflicht für KRITIS-Betreiber vor. Die Meldepflicht gilt für Störungen, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der KRITIS geführt haben oder führen können. Das Nationale IT-Lagezentrum nimmt aber auch freiwillige Meldungen entgegen. Im Berichtszeitraum gingen beim BSI 726 Meldungen (2023: 490) ein.

### Managementsysteme für Informationssicherheit und Geschäftskontinuität

Die turnusmäßigen Nachweise der KRITIS-Betreiber enthalten eine Einschätzung zur Wirksamkeit der Managementsysteme für Informationssicherheit (ISMS) und Geschäftskontinuität (Business Continuity Management System, BCMS). Mittels eines Reifegradmodells bewertet die prüfende Stelle die Ausprägung der beim Betreiber implementierten Managementsysteme. Die Orientierungshilfe des BSI zu Nachweisen gemäß § 8a Abs. 3 BSIG beschreibt folgende Reifegrade für ISMS und BCMS:

## ISMS-Reifegrade

gemäß dem jeweils letzten vorliegenden Nachweis

Sektor	Reifegrade				
	1	2	3	4	5
Energie	1	20	40	28	28
Wasser	0	8	13	28	30
Ernährung	0	11	20	8	10
Informationstechnik und Telekommunikation	0	2	9	10	18
Gesundheit	3	78	64	43	23
Finanz- und Versicherungswesen	0	8	35	20	42
Transport und Verkehr	3	24	30	6	8

## BCMS-Reifegrade

gemäß dem jeweils letzten vorliegenden Nachweis

Sektor	Reifegrade				
	1	2	3	4	5
Energie	2	28	51	23	13
Wasser	3	13	21	21	21
Ernährung	4	10	22	9	4
Informationstechnik und Telekommunikation	2	8	11	6	12
Gesundheit	15	104	52	26	14
Finanz- und Versicherungswesen	0	28	22	29	26
Transport und Verkehr	7	28	21	6	9

### ISMS- und BCMS-Reifegrade

1: geplant, aber bisher nicht etabliert / 2: weitestgehend etabliert / 3: etabliert und dokumentiert / 4: zusätzlich zu 3 regelmäßig auf Effektivität überprüft (ISMS) bzw. überprüft und beübt (BCMS) / 5: zusätzlich zu 4 regelmäßig verbessert

Abbildung 25: ISMS-Reifegrade und BCMS-Reifegrade nach Sektoren laut jeweils letztem vorliegendem Nachweis, Quelle: BSI

Die regelmäßige Ermittlung im Zuge der Nachweiserbringung ermöglicht es, den Reifegrad von ISMS und BCMS über Prüfzyklen hinweg zu dokumentieren. Die Ermittlung von Reifegraden hat sich als praxisnahe Methode erwiesen, um dem BSI einen ersten Eindruck über den Grad der Implementierung der Managementsysteme zu verschaffen.

### Systeme zur Angriffserkennung

Mit dem IT-Sicherheitsgesetz 2.0 wurde für KRITIS-Betreiber im Mai 2021 ausdrücklich der Einsatz von Systemen zur Angriffserkennung im BSIG vorgeschrieben

(§ 8a Abs. 1a BSIG). Diese gesetzliche Verpflichtung betrifft nicht nur KRITIS-Betreiber, die die Schwellenwerte der BSI-Kritisverordnung (BSI-KritisV) überschreiten, sondern über § 11 Abs. 1d Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz – EnWG) auch alle Strom- und Gasnetzbetreiber. Die Qualität der eingesetzten Systeme gemäß § 8a Abs. 1a BSIG und gemäß § 11 Abs. 1e EnWG lässt sich mithilfe eines Umsetzungsgradmodells bewerten. Dieses können Auditorinnen und Auditoren sowie Prüferinnen und Prüfer nutzen, um zu beurteilen, wie weit die organisatorischen und technischen Maßnahmen in der geprüften Kritischen Infrastruktur fortgeschritten sind.

Ziel der Anwendung eines Umsetzungsgradmodells ist es, die Qualität von Systemen zur Angriffserkennung zu erhöhen. Durch regelmäßige Analysen kann überprüft werden, welche Teilbereiche noch unzureichend gesteuert sind. Ein niedriger Umsetzungsgrad begründet einen besonderen Handlungsbedarf. Umsetzungsgradmodelle können folglich dabei unterstützen, Schwerpunkte für die Weiterentwicklung von Systemen zur Angriffserkennung zu setzen.

Die Anzahl der Nachweise entspricht nicht der Anzahl der Betreiber. Einige energiewirtschaftliche Betreiber sind gemäß § 11 Absatz 1f EnWG nachweispflichtig. Diese Nachweise enthalten Umsetzungsgrade der Systeme zur Angriffserkennung, aber keine ISMS-/BCMS-Reifegrade. Außerdem gibt es Betreiber, die nach § 8d Absatz 2 BSIG nicht nachweispflichtig sind. Schließlich gibt es kürzlich registrierte Betreiber, zum Beispiel im Sektor Siedlungsabfallsorgung, die erst zwei Jahre nach der Registrierung einen Nachweis einreichen müssen.

### Kooperation gewinnt – auch bei KRITIS

In der UP KRITIS, der unabhängigen Partnerschaft zum Schutz Kritischer Infrastrukturen in Deutschland, arbeiten KRITIS-Betreiber, deren Fachverbände und die zuständigen Behörden zusammen, um die Kritischen Infrastrukturen in Deutschland zu schützen. Teilnehmer in der UP KRITIS können alle KRITIS-Betreiber werden, auch kleinere Betreiber, die unterhalb der Schwellenwerte der BSI-KritisV bleiben und somit nicht von der gesetzlichen Registrierungs-, Nachweis- und Meldepflicht erfasst sind. Derzeit sind 960 Organisationen als Teilnehmer an der UP KRITIS angemeldet (Stand 30. Juni 2024). Der fachliche Austausch erfolgt insbesondere in Themen- und Branchenarbeitskreisen. Im Jahr 2024 wird sich die UP KRITIS im Rahmen einer organisatorischen Fortschreibung für Arbeitskreise öffnen, die den physischen Schutz Kritischer Infrastrukturen im Fokus haben. Durch die stärkere Verzahnung wird die UP KRITIS auf die zunehmend komplexe Bedrohungslage ausgerichtet, der mit einem integrierten, umfassenden Ansatz begegnet wird.

## SzA-Umsetzungsgrad

gemäß dem jeweils letzten vorliegenden Nachweis

Reifegrade

Sektor	0	1	2	3	4	5
Energie	2	7	39	28	3	2
Wasser	1	8	8	11	5	0
Ernährung	0	2	7	10	3	1
Informationstechnik und Telekommunikation	0	0	3	12	2	3
Gesundheit	1	44	87	35	13	0
Finanz- und Versicherungswesen	0	2	22	23	17	4
Transport und Verkehr	0	19	24	9	1	0

**Die Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung beschreibt folgende Umsetzungsgrade:**

**0:** Es sind bisher keine Maßnahmen zur Erfüllung der Anforderungen umgesetzt und es bestehen auch keine Planungen zur Umsetzung von Maßnahmen / **1:** Es bestehen Planungen zur Umsetzung von Maßnahmen zur Erfüllung der Anforderungen, jedoch für mindestens einen Bereich noch keine konkreten Umsetzungen / **2:** In allen Bereichen wurde mit der Umsetzung von Maßnahmen zur Erfüllung der Anforderungen begonnen. Es sind noch nicht alle MUSS-Anforderungen erfüllt worden / **3:** Alle MUSS-Anforderungen wurden für alle Bereiche erfüllt. Idealerweise wurden SOLLTE-Anforderungen hinsichtlich ihrer Notwendigkeit und Umsetzbarkeit geprüft. Ein kontinuierlicher Verbesserungsprozess wurde etabliert oder ist in Planung / **4:** Alle MUSS-Anforderungen wurden für alle Bereiche erfüllt. Alle SOLLTE-Anforderungen wurden erfüllt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Ein kontinuierlicher Verbesserungsprozess wurde etabliert / **5:** Alle MUSS-Anforderungen wurden für alle Bereiche erfüllt. Alle SOLLTE-Anforderungen und KANN-Anforderungen wurden für alle Bereiche erfüllt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Für alle Bereiche wurden sinnvolle zusätzliche Maßnahmen entsprechend der Risikoanalyse/Schutzbedarfsfeststellung identifiziert und umgesetzt. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.

Abbildung 26: Umsetzungsgrade SzA gemäß dem jeweils letzten vorliegenden Nachweis, Quelle BSI

Die Sicherheit Kritischer Infrastrukturen ist das Fundament der Cybernation Deutschland. Dieser Begriff schließt die Stärkung der Resilienz gegen Cyberangriffe mit ein, die vor allem durch eine enge Kooperation von Staat, Wirtschaft und Gesellschaft erreicht wird. Eine wichtige Rolle nimmt hierbei die UP KRITIS mit ihren Arbeitsgruppen ein.

### **10.1.1 Gefährdungslage im KRITIS-Sektor Energie**

Die Bedrohungslage im Sektor Energie ist unverändert hoch. Die Betreiber von Kritischen Infrastrukturen im Sektor Energie sehen sich mit verschiedensten Angriffs-szenarien konfrontiert.

Am Beispiel eines Softwareunternehmens, das unter anderem als Dienstleister im Energie-Sektor tätig ist, zeigt sich, dass Ransomware-Angriffe in Verbindung mit Lieferanten und Dienstleistern nach wie vor eine Bedrohung darstellen. Im Februar 2024 wurde bekannt, dass das Unternehmen Opfer eines Cyberangriffs geworden ist. Das international agierende Unternehmen beschäftigt nach eigenen Angaben an 13 Standorten in Deutschland und 16 internationalen Standorten 2.200 Mitarbeitende. Es entwickelt neben Leitsystemen auch Prozesssteuerungs- und Informationssysteme, insbesondere für Energiebetreiber. Des Weiteren werden Produkte des Unternehmens in der Industrie und Logistik sowie bei Betreibern von Verkehrsinfrastrukturen eingesetzt.

Die Angreifer verschafften sich unerlaubten Zugriff auf die IT-Infrastruktur des Softwareunternehmens und verschlüsselten anschließend Teile der IT-Systeme und Daten. Das Unternehmen trennte daraufhin alle externen Verbindungen zu Kunden. KRITIS-Betreiber aus den Sektoren Energie sowie Transport und Verkehr informierten das BSI darüber, dass Einschränkungen in Bezug auf die kritischen Dienstleistungen möglich sein könnten. Eine akute Betroffenheit der Betreiber war in allen Fällen auf Wartungszugänge beschränkt. Zu Beeinträchtigungen der kritischen Dienstleistungen kam es im weiteren Verlauf nicht. Das BSI stand mit vielen KRITIS-Betreibern in Kontakt und versandte regelmäßige Updates der Cyber-Sicherheitswarnung (CSW).

Ebenfalls Opfer eines Ransomware-Angriffs wurde ein Elektrotechnikkonzern. Die Angreifer konnten mehrere Terabytes an Daten erbeuten und drohten, diese zu veröffentlichen, wenn kein Lösegeld gezahlt würde. Das Unternehmen ist ein bekannter Hersteller von industriellen Steuerungs- und Automatisierungssystemen (ICS), unter anderem für die Mineralölbranche in Deutschland.

An den beobachteten Ransomware-Vorfällen lässt sich erkennen, dass cyberkriminelle Gruppierungen zunehmend Opfer mit hoher Lösegeld-Erwartung ins Visier nehmen. Ransomware-Akteure konzentrieren sich auf vermeintlich zahlungskräftige Ziele, bei denen mutmaßlich eine hohe Bereitschaft zur Lösegeldzahlung besteht. So rücken Unternehmen aus den KRITIS-Sektoren in den Fokus, bei denen die Notwendigkeit der Aufrechterhaltung der kritischen Dienstleistungen eine hohe Zahlungsbereitschaft begünstigen könnte.

#### **Phishing, DDoS und menschliche Fehler**

Neben Ransomware kann im Energiesektor weiterhin auch Phishing beobachtet werden. So konnten zum Beispiel seit November 2023 mehrere Phishing-Kampagnen aufgedeckt werden, die einer mutmaßlich prorussischen Gruppierung zugeschrieben werden. Ziel dieser Kampagnen war es, die Opfer dazu zu bringen, Schadsoftware herunterzuladen, die dem Informationsdiebstahl dient.

Ebenso berichtete die Bundesnetzagentur (BNetzA) von einer laufenden Phishing-Kampagne, bei der Phishing-E-Mails im Namen der BNetzA versandt wurden. Hierbei wurden potenzielle Opfer aufgefordert, sensible Daten auf einer gefälschten, der BNetzA-Webseite ähnelnden Webseite einzugeben.

Des Weiteren konnten im Berichtszeitraum DDoS-Attacken beobachtet werden. Infolge eines DDoS-Angriffs auf einen Energiebetreiber kam es zu einem vorübergehenden Teilausfall der Kritischen Infrastruktur. Der Betreiber gab an, dass es durch den Cyberangriff zu einer Überlastung der Firewall kam. Der DDoS-Angriff richtete sich gegen ein Abwicklungssystem zum Vertrieb von Kraftstoff und Heizöl. Für ungefähr zweieinhalb Stunden war die Verfügbarkeit der kritischen Dienstleistung bundesweit an mehreren Standorten eingeschränkt. Die Angriffsbreite konnte durch die Abschaltung von Systemen und damit die Verkleinerung der Angriffsfläche reduziert werden.

In die verschiedenen Angriffszenarien reihen sich technische und/oder menschliche Fehler ein, die eine Beeinträchtigung der kritischen Dienstleistung zur Folge hatten. Beispielsweise meldete der Betreiber einer Pipeline, dass beide Hauptdatenverbindungen versehentlich gleichzeitig unterbrochen wurden. Ursprünglich sollten diese schrittweise durch Glasfaserverbindungen ersetzt werden. Durch die gleichzeitige Unterbrechung der Datenverbindungen waren beide Router nicht mehr erreichbar. Die Ursache für die Störung war ein menschlicher Fehler, bei dem versehentlich Kupferdatenverbindungen irreparabel entfernt wurden. Als Sicherheitsmaßnahme wurde

der Öltransport durch die Pipeline gestoppt. Die Kundinnen und Kunden wurden frühzeitig durch den Betreiber informiert. Der Ausfall dauerte mehrere Tage. Ein längerer Ausfall hätte sich auf die kritische Versorgungsdienstleistung mit Rohöl(-produkten) ausgewirkt. In Kooperation mit einem Dienstleister konnte eine alternative Datenverbindung eingerichtet und die Erreichbarkeit der Router wiederhergestellt werden.

### 10.1.2 Gefährdungslage der Netzinfrastruktur (Schwerpunkt Mobilfunk/5G)

Der Austausch von Informationen ist in der modernen Gesellschaft zu einem sehr wichtigen Wirtschaftsfaktor und Bestandteil des täglichen Lebens geworden. Ein wichtiger Teil der deutschen Wirtschaft ist stark abhängig von einer unterbrechungsfreien Sprach- und Datenübertragung. Ein Ausfall der IKT-Basisinfrastruktur kann nach kurzer Zeit zu einem Stillstand in Produktionsunternehmen führen, da Produktion und Logistik nicht miteinander kommunizieren können. Insbesondere der Bereich Mobilfunk hat durch die Einführung neuer Mobilfunkstandards sowie die immer stärkere Vernetzung erheblich an Bedeutung gewonnen. Das BSI beobachtet und bewertet kontinuierlich die Sicherheitslage in den nationalen Telekommunikationsnetzen anhand von Meldungen zu Vorfällen und Schwachstellen.

#### Nationale Lage

Mit der Einführung und Integration neuer Mobilfunkstandards sowie moderner Technologiekonzepte erhöht sich auch die Komplexität der Netzstrukturen. Die dadurch entstehenden funktionalen Abhängigkeiten vergrößern die Angriffsfläche bei öffentlichen und privaten Mobilfunknetzen. Vor allem der parallele Betrieb verschiedener Mobilfunkgenerationen führt zu hochkomplexen Netzen mit der Notwendigkeit einer gesamtheitlichen Sicherheitsbetrachtung. Die intensive Beobachtung und Analyse von Cyberangriffen sowie Schwachstellen im Kontext Mobilfunk sind deshalb essenziell zur Sicherstellung der Resilienz nationaler Mobilfunknetze. Die aufgetretenen Ausfälle wurden oft durch Wartungsarbeiten oder Upgrades in den komplexen Netzstrukturen verursacht. Jedoch konnte das BSI ebenso eine steigende Anzahl physischer Angriffe auf einzelne Basisstationen feststellen. Vandalismus oder Sabotage führten dabei zu längeren, aber regional begrenzten Ausfällen, die meistens nur durch einen Austausch der defekten Infrastruktur behoben werden konnten. Das BSI beobachtete zudem in leitungsgebundenen Netzen mehrere Beeinträchtigun-

gen im Bereich der Notruftechnik. Des Weiteren führten Wartungsarbeiten oder fehlgeschlagene Updates sowie Beschädigungen von Infrastruktur auch in diesen Netzen zu Ausfällen und Störungen.

#### Internationale Lage

Das BSI konnte im Berichtszeitraum auch eine zunehmende Bedrohung im internationalen Raum durch staatliche Akteure beobachten. Aufgrund eines Cyberangriffs auf den größten ukrainischen Mobilfunkanbieter Kyivstar war dessen Mobilfunknetz über mehrere Tage weitestgehend nicht verfügbar. Neben dem Ausfall der mobilen Kommunikation waren auch zahlreiche vernetzte Anwendungen wie Zahlungsterminals, Alarmsysteme oder sogar die Straßenbeleuchtung betroffen. Bei einem weiteren Vorfall ist das gesamte Mobilfunknetz des australischen Netzbetreibers Optus für einige Stunden ausgefallen. Rund die Hälfte der australischen Bevölkerung, zahlreiche Krankenhäuser, Zahlungsterminals und der U-Bahn-Betrieb waren vom Ausfall betroffen, der mutmaßlich durch ein fehlgeschlagenes Update verursacht wurde. Diese beiden großflächigen Vorfälle verdeutlichen einmal mehr die Bedeutsamkeit von Mobilfunknetzen für digitalisierte Anwendungen.

#### Schwachstellen Mobilfunk

Im Berichtszeitraum wurden zudem zahlreiche Schwachstellen in kommerziell verbreiteten 5G-Modems zweier Chip-Hersteller für Mobilfunktechnik bekannt. Über gefälschte Basisstationen im Mobilfunknetz ist es dabei möglich, Implementierungsfehler in nicht gepatchten Modems auszunutzen und einen Denial-of-Service-Angriff durchzuführen. Das BSI konnte den Angriff auf diese Schwachstellen im eigenen 5G/6G-Security-Labor nachstellen und schätzt die breite praktische Umsetzbarkeit im öffentlichen Mobilfunknetz aufgrund der notwendigen technischen Voraussetzungen als unwahrscheinlich ein. Darüber hinaus lassen sich bestimmte Sicherheitsmechanismen der neuen Mobilfunkstandards durch Downgrade-Attacken auf ältere Mobilfunkgenerationen umgehen. Ältere, schwachstellenbehaftete Signalisierungsinfrastrukturen sind auch zukünftig für das Roaming zwischen verschiedenen Ländern, Netzbetreibern und Mobilfunkgenerationen notwendig und können bei erfolgreicher Kompromittierung für die Lokalisierung und Überwachung von Personen ausgenutzt werden. In diesem Zusammenhang beobachtet das BSI, dass Signalisierungsprotokolle wie beispielsweise SS7 weiterhin im Fokus der Angreifer bleiben und regelmäßig dazu führen, dass Mobilfunkbetreiber ihre Detektionsmechanismen anpassen müssen.

Signalisierungsprotokolle dienen dem Zweck, Informationen zur Steuerung der Kommunikationsverbindungen in Telekommunikationsnetzen zu übermitteln.

Insgesamt sieht das BSI eine zunehmende Bedrohung für private und öffentliche Telekommunikationsnetze im nationalen und internationalen Raum. Insbesondere Mobilfunknetze sind aufgrund von Virtualisierung und Cloudifizierung zunehmend anfällig für infrastrukturell bedingte Schwachstellen ihrer Hard- und Softwareplattformen. Mithilfe von ausgeprägten Detektions- und Reaktionsmaßnahmen der Netzbetreiber können Cyberangriffe auf Telekommunikationsnetze in der Regel frühzeitig erkannt und mitigiert werden, um Schäden und Auswirkungen für Endanwendende zu minimieren. Um die Sicherheit der Netze weiter zu erhöhen, beteiligt sich das BSI an der Erstellung neuer Sicherheitsanforderungen im Rahmen der Fortschreibung des durch die Bundesnetzagentur verantworteten Katalogs von Sicherheitsanforderungen gemäß § 167 TKG. Darüber hinaus wirkt das BSI an der Standardisierung von 5G/6G und Open RAN sowie der künftigen Signalisierungs- und Roaminginfrastruktur zwischen Mobilfunkanbietern mit. Außerdem unterliegen kritische 5G-Komponenten in öffentlichen Mobilfunknetzen einer Zertifizierungspflicht, um zu gewährleisten, dass die vorgegebenen Sicherheitseigenschaften vorhanden sind. Diese tritt nach einer Übergangsfrist 2026 in Kraft. Als qualifizierte unabhängige Stelle überprüft das BSI, wie vom Telekommunikationsgesetz gefordert, die Einhaltung der Sicherheitsanforderungen in den öffentlichen Netzen bei erhöhtem Gefährdungspotenzial.

### 10.1.3 Gefährdungslage der Satellitenkommunikation

Satellitengestützte Dienste spielen heute eine immer größere Rolle für Gesellschaft, Wirtschaft und Staat. Die Abhängigkeit von satellitengestützten Diensten steigt daher stetig. Vor allem Satellitenkommunikation in jeglicher Form, zum Beispiel satellitengestützter Internetzugriff für die unabhängige Kommunikation von Einsatzkräften, nimmt einen immer größeren Stellenwert ein. Moderne Satellitenkonstellationen wie Starlink oder OneWeb bieten dazu immer umfangreichere, passende Dienste, um an entlegenen Orten ohne terrestrischen Breitbandzugang einen Zugang zum Internet bereitzustellen. Auch Erdfernerkundung oder Navigation sind ohne weltraumbasierte Systeme und Dienste nicht vorstellbar. In Konsequenz werden diese Systeme zunehmend attraktiv für Angreifer. Der Aufwand für einen Angriff ist aufgrund der Signalstruktur moderat, der mögliche entstehende Schaden und die unvorhersehbaren Kollateralschäden sind allerdings durchaus gravierend.

Bei Satellitensystemen müssen neben den klassischen Angriffsvektoren auf terrestrische Infrastrukturen auch die möglichen Angriffspfade auf die Satelliten selbst explizit betrachtet werden. Für terrestrische Systeme gibt es bereits erprobte Konzepte zur Absicherung. Satelliten dagegen sind aufgrund ihrer globalen Verfügbarkeit ein verwundbares Element und bedürfen gesonderter Schutzmaßnahmen.

### NIS-2-Richtlinie mit erweiterten Anforderungen an Satellitenkommunikation

Ziel muss es sein, für Satelliten ein gutes Maß an möglichst standardisierten Sicherheitsanforderungen zu entwickeln. Rein national können Satellitensysteme nicht reguliert und abgesichert werden. Hier ist die Zusammenarbeit mit anderen Ländern und internationalen Organisationen, wie zum Beispiel der ESA oder der EU, unabdingbar. Mit der NIS-2-Richtlinie, die Weltraum als eigenen Sektor darstellt, wird dem in gewissem Umfang Rechnung getragen. Sie bedeutet einen wichtigen Schritt in Richtung einer europäischen Absicherung von Satellitensystemen. Dennoch bleibt es relevant, derartige Mindestanforderungen auch im globalen Kontext zu etablieren. Hier sieht sich das BSI in einer Vorreiterrolle und wird mit internationalen Partnern daran arbeiten. (*Mehr zum Thema NIS-2-Richtlinie finden Sie im Kapitel NIS-2-Richtlinie, S. 84*).

## 10.2 Gefährdungslage der KMU in Deutschland

3,1 Millionen kleine und mittlere Unternehmen in Deutschland stehen vor den Herausforderungen der Digitalisierung und damit einhergehend der Cybersicherheit. Dieser Teilbereich von Unternehmen, der zahlenmäßig 99,4 Prozent der deutschen Wirtschaftsunternehmen ausmacht, gliedert sich wie folgt auf:

Gerade die Kleinst- (< 10 Beschäftigte) und die kleinen (< 50 Beschäftigte) Unternehmen verfügen oftmals nicht über das erforderliche Personal, das sich um Betrieb und Absicherung der Informationstechnik des Unternehmens kümmert. Für diese Betriebe lohnt es sich beispielsweise schlicht nicht, eigenes IT-Personal einzustellen. Im Rahmen des klassischen „Make or Buy“-Entscheidungsprozesses wird dabei häufig der „Das bekommen wir schon irgendwie selbst hin“-Ansatz gewählt. Dem steht eine wachsende Bedrohungslage gegenüber.

Auch im Jahr 2024 besitzen viele Unternehmen nach Erfahrung des BSI weder eine ausreichende Kenntnis über die allgemeine Cyberbedrohungslage noch über das eigene Risikoprofil. So wissen sie gar nicht, dass sie mehr in ihre Sicherheit investieren müssen. Selbst elementare, oftmals kostenfrei umsetzbare Präventionsmaßnahmen werden daher häufig nicht ergriffen.

Diejenigen KMU hingegen, die bereits Problembewusstsein entwickelt haben und Personal einstellen möchten, erleben häufig, dass sie in einem Angebotsmarkt als potenzieller Arbeitgeber nicht gegen die Gehälter bei Großunternehmen oder IT-Dienstleistern bestehen können. Und diejenigen, die den Bereich IT/IT-Sicherheit an einen Dienstleister auslagern möchten, müssen durchaus feststellen, dass es in ihrer Region entweder zu wenig qualifizierte Dienstleister gibt oder nur solche, die nicht zu ihrer eigenen Unternehmensgröße passen.

Glücklicherweise steigt die Zahl derjenigen kleinen und mittleren Unternehmen (KMU), die gerne mehr für ihre IT-Sicherheit tun würden. Oftmals wissen diese aber nicht, wie sie dabei am besten vorgehen sollen. Bereits existierende Standardwerke zum Aufbau eines Informationssicherheitsmanagementsystems, wie das IT-Grundschutz-Kompendium des BSI oder die Norm

ISO/IEC 27001, eignen sich eher für Unternehmen, die einen eigenständigen IT-Betrieb haben. Dies trifft auf den überwiegenden Teil der Unternehmen mit weniger als 50 Beschäftigten jedoch nicht zu.

#### Konsortium zur Erarbeitung einer DIN SPEC

Um auch solche Unternehmen zu unterstützen, wurde in Kooperation mit dem Bundesverband mittelständische Wirtschaft (BVMW) ein Konsortium unter der Leitung des BSI zur Erarbeitung einer DIN SPEC gegründet. Insgesamt waren fast 20 Partner beteiligt, unter anderem das Deutsche Institut für Normung (DIN), Wirtschaftsförderungen, eine Tochter des Gesamtverbandes der deutschen Versicherungswirtschaft, IT-Grundschutz-Expertinnen und -Experten sowie Fachkundige zum Thema Datenschutz und IT-Dienstleister. Finanziert wurde das Projekt durch das Bundesministerium für Wirtschaft und Klimaschutz im Rahmen des Programmes „Mittelstand-Digital“.

Ergebnisse der achtmonatigen Arbeit des Konsortiums sind die im Mai 2023 veröffentlichte „DIN SPEC 27076 IT-Sicherheitsberatung für kleine und Kleinstunternehmen“ und der darauf basierende CyberRisikoCheck. Durch diesen können KMU bei IT-Dienstleistern eine standardisierte Beratung erhalten, die speziell auf ihre Bedürfnisse

## Aufteilung Unternehmen in Deutschland

Im Jahr 2019

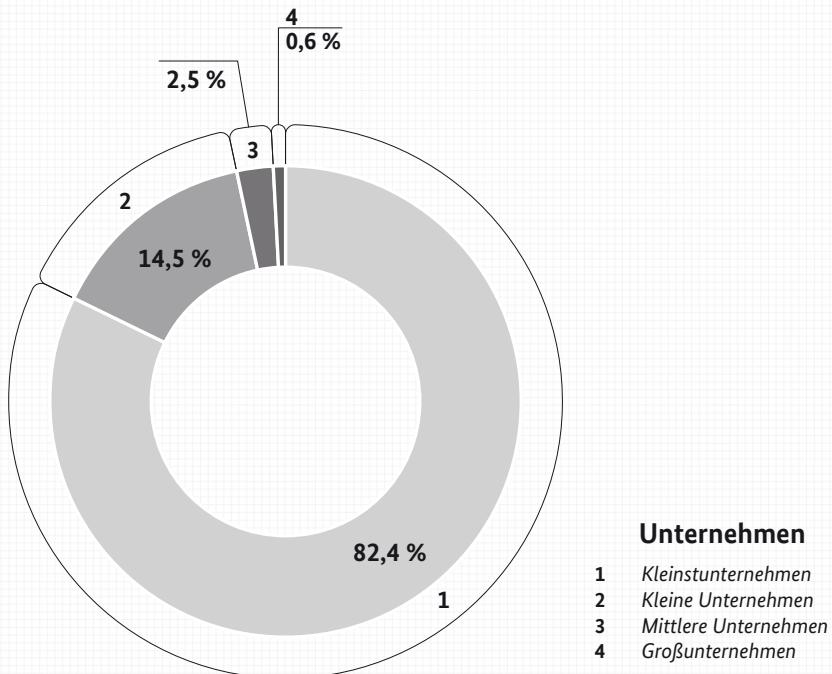


Abbildung 27: Aufteilung Unternehmen in Deutschland im Jahr 2019, Quelle: Statistisches Bundesamt, Stand: 6. Mai 2024<sup>25</sup>

angepasst ist. In der DIN SPEC wurden auch die Handlungsempfehlungen für KMU standardisiert. Dadurch wissen sowohl Auftraggeber als auch Auftragnehmer, welche Leistung zu erwarten und zu erbringen ist.

#### Durchführung des CyberRisikoChecks

Beim CyberRisikoCheck befragt ein IT-Dienstleister ein Unternehmen in einem ein- bis zweistündigen Interview, in der Regel per Videokonferenz, zur IT-Sicherheit im Unternehmen. Darin werden 27 Anforderungen aus sechs Themenbereichen daraufhin überprüft, ob das Unternehmen sie erfüllt. Für die Antworten werden nach den Vorgaben der DIN SPEC Punkte vergeben. Als Ergebnis erhält das Unternehmen einen Bericht, der unter anderem die Punktzahl und für jede nicht erfüllte Anforderung eine Handlungsempfehlung enthält. Die Handlungsempfehlungen sind nach Dringlichkeit gegliedert und enthalten Hinweise darauf, welche staatlichen Fördermaßnahmen, auf Bundes-, Landes- und kommunaler Ebene, das jeweilige Unternehmen in Anspruch nehmen kann. Der CyberRisikoCheck ist keine IT-Sicherheitszertifizierung. Er ermöglicht einem Unternehmen jedoch eine Positionsbestimmung des eigenen IT-Sicherheitsniveaus und zeigt auf, welche konkreten Maßnahmen das Unternehmen umsetzen oder bei einem IT-Dienstleister beauftragen sollte.

Auf Bundesebene werden der Check und sich daran anschließende Handlungsempfehlungen bereits jetzt über das Programm „go-digital“<sup>26</sup> mit 50 Prozent bezuschusst, in NRW über das Programm „Mittelstand Innovativ & Digital (MID)“<sup>27</sup> sogar mit 70 Prozent. Mehrere weitere Länder haben ebenfalls eine Förderbereitschaft signalisiert. Von März bis Juni 2024 hat das BSI 351 IT-Dienstleister in der Durchführung des CyberRisikoChecks geschult. Seit Mai 2024 stellt das BSI diesen auch eine webbasierte Software zur Durchführung des CyberRisikoChecks bei ihren Kunden zur Verfügung und erhält darüber die anonymisierten Erhebungsdaten der Checks. Dadurch kann das Nationale IT-Lagezentrum erstmals auf valide Daten zur Cybersicherheit von KMU zurückgreifen und in die BSI-Berichte zur Cybersicherheitslage mit aufnehmen. Der Lagebericht 2025 wird daher erstmals eine umfassende Darstellung der Situation von KMU bieten.

Der CyberRisikoCheck trägt somit zur Weiterentwicklung präventiver Angebote von Bund, Ländern und Kommunen bei. Weitere Informationen zum CyberRisikoCheck sowie eine Liste registrierter IT-Dienstleister, die den Check anbieten, sowie weitere nützliche Informationen für KMU finden sich auf der BSI-Webseite.



Weiterführende Informationen  
zum CyberRisikoCheck:



Weiterführende Informationen  
für KMU:



Zur Broschüre „Cybersicherheit  
für KMU – Die Top-14-Fragen“:



## CrowdStrike Falcon verursacht weltweit IT-Ausfälle

### Sachverhalt

Am 19. Juli 2024 verursachte eine IT-Security-Lösung von CrowdStrike weltweite IT-Ausfälle in zahlreichen Branchen. In Deutschland wurden zahlreiche IT-Ausfälle gemeldet, auch bei KRITIS-Betreibern und meldepflichtigen Organisationen. Die IT-Ausfälle traten in Zusammenhang mit einem durchgeführten Update der EDR-Software Falcon auf. Falcon ist ein Enterprise Tool, das nur in Unternehmen eingesetzt wird, daher waren Privatpersonen nicht betroffen. CrowdStrike hatte ein Inhalts-Update der Software ausgerollt, das zu einem Systemabsturz mit abschließendem „Bluescreen of Death“ (BSOD) auf Windows-basierten Installationen führte. Der Fehler trat nur auf, wenn der Falcon EDR Sensor installiert war. Es handelte sich ursächlich um einen Programmierfehler der in C++ programmierten IT-Security-Lösung. CrowdStrike kommunizierte am 19. Juli 2024 umgehend einen Workaround zur Lösung des Problems. Nach Angaben von Microsoft waren insgesamt circa 8,5 Millionen Windows-Systeme betroffen. Cyberkriminelle habe die IT-Ausfälle für unterschiedliche Formen von Phishing, Scam oder Fake-Webseiten ausgenutzt. Ab dem 21. Juli 2024 normalisierte sich die Lage wieder.

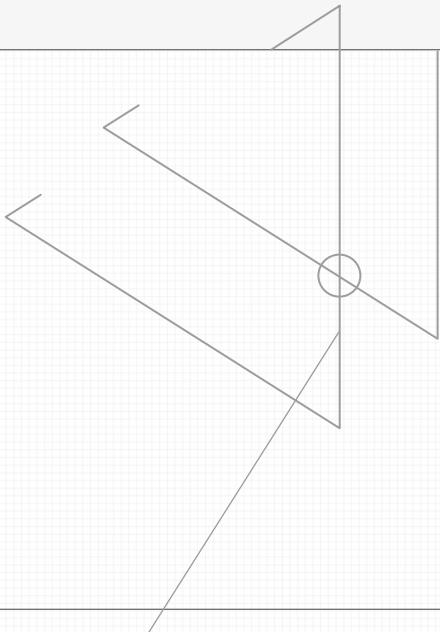
### Bewertung

Es handelte sich nicht um einen Cyberangriff, sondern um mangelnde Qualitätssicherung des Herstellers. Für die Betroffenen sind durch die von CrowdStrike verursachten IT-Ausfälle enorme, noch nicht bezifferte Kosten entstanden. Nach ersten Schätzungen liegen die Kosten vermutlich in Milliardenhöhe.

### Reaktion

Auf seinem Support-Portal stellte CrowdStrike am 19. Juli 2024 für verschiedene Systeme Mitigationsmaßnahmen zur Verfügung. Das BSI hat ebenfalls am 19. Juli 2024 eine Management-Information zu dem Sachverhalt und den möglichen Mitigationsmaßnahmen für seine Zielgruppen veröffentlicht. Microsoft hat am 21. Juli 2024 ein Wiederherstellungstool für die vom CrowdStrike-Ausfall betroffenen Systeme veröffentlicht.

Das BSI hat mit CrowdStrike und Microsoft erste Maßnahmen entwickelt, um vergleichbare Vorfälle künftig zu vermeiden. Darüber hinaus wird das BSI mit CrowdStrike Maßnahmen vereinbaren, durch die die Betriebsstabilität von Kundensystemen auch bei der Installation kurzfristig notwendiger Software-Updates sichergestellt wird. Die Maßnahmen umfassen kurz-, mittel- und langfristige Schritte bis Ende 2024 sowie weitergehende Maßnahmen bis 2025. Umgesetzte Maßnahmen wird das BSI auf Wirksamkeit überprüfen.



# Cybersicherheitsvorfall bei einem Remote-Screensharing-Anbieter

## Sachverhalt

Der Hersteller einer weitverbreiteten Software für Fernzugriff und Screensharing veröffentlichte im Februar 2024 eine Pressemitteilung zu einem erfolgreichen Cyberangriff mit erfolgter Kompromittierung interner Systeme.

Öffentliche Quellen berichten darüber, dass im Zuge dieser Kompromittierung auch Quellcode sowie Zertifikate zum Signieren der Software abgeflossen seien. Der Hersteller hat die Bereinigung und Wiederherstellung gemeinsam mit einem Dienstleister unmittelbar durchgeführt. In diesem Rahmen wurden Zertifikate zurückgezogen und Updates bereitgestellt, durch die die Zertifikate bei den Endnutzerinnen und Endnutzern ausgetauscht werden.

Der betroffene Hersteller äußerte gegenüber dem BSI, dass das Unternehmen derzeit keine positive Kenntnis einer Kompromittierung von Nutzerdaten habe, jedoch aus Gründen der Vorsicht einen Reset der Passwörter seines Kundenportals erzwungen habe.

## Bewertung

Nach Einschätzung des BSI besteht durch den möglichen Abfluss des Quellcodes sowie der Zertifikate die Gefahr, dass diese Informationen für weiterführende Angriffe auf Kunden des Anbieters genutzt werden könnten. In diesem Kontext sind unter anderem Man-in-the-Middle- sowie Supply-Chain-Angriffe denkbar. Insbesondere durch die womöglich abgeflossenen Zertifikate könnten diese

unbemerkt bleiben oder im schlimmsten Fall bereits erfolgte Angriffe unentdeckt geblieben sein. Durch die vom betroffenen Hersteller umgesetzten Maßnahmen wurde das Gefährdungspotenzial erheblich reduziert. Dennoch ist nicht auszuschließen, dass schädliche Versionen der Software, die mit einem kompromittierten Zertifikat signiert sind, durch Angreifer auf Drittseiten angeboten oder gezielt an Kunden gesandt werden.

Im Unternehmenskontext wird die Anwendung oft mit privilegierten Rechten verwendet, wodurch sich ein besonderes Gefährdungspotenzial eröffnet.

## Reaktion

Das BSI steht mit dem betroffenen Unternehmen in Kontakt, kann den Vorfall bestätigen und hat ebenfalls Anfang Februar mit einer Vorfallswarnung öffentlich informiert.

Das BSI empfiehlt generell, den Empfehlungen von Softwareherstellern Folge zu leisten und die jeweils aktuellste Version mit dem neuen Zertifikat einzuspielen. Updates sollten ausschließlich über die Update-Funktion innerhalb der Software oder über die Webseite des Herstellers bezogen werden. Darüber hinaus sollten Mitarbeitende sensibilisiert werden, verbunden mit dem Hinweis, dass Software niemals aus unsicheren Quellen bezogen werden sollte.



# 11 – Erkenntnisse zur Gefährdungslage in der Bundesverwaltung

Tagtäglich sind die Regierungsnetze überwiegend ungezielten Massenangriffen aus dem Internet ausgesetzt. Teilweise richten sich Angriffe aber auch gezielt gegen die Bundesverwaltung. Zum Schutz der Regierungsnetze vor diesen Angriffen setzt das BSI eine Reihe sich gegenseitig ergänzender Maßnahmen ein.

Eine präventive Komponente stellen Webfilter dar, die den Zugriff auf maliziöse Webseiten und Webserver blockieren. So wird zum Beispiel der Zugriff auf Schadprogramme verhindert, die sich hinter Download-Links verstecken. Diese Links werden im Rahmen von Social-Engineering-Angriffen über E-Mail, soziale Medien oder Webseiten verbreitet. Auch die Kommunikation von bereits aktiver Schadsoftware mit Webservern, die unter Kontrolle der Angreifer stehen, wird durch diese Schutzmaßnahme unterbunden. Die Schadsoftware kann dann auf diesem Weg keine neuen Komponenten und Befehle der Angreifer mehr erhalten. Zudem ist es der Schadsoftware dann auch nicht mehr möglich, Daten des Opfers an diese Webserver zu senden. Im aktuellen Berichtszeitraum wurden täglich durchschnittlich 375 maliziöse Webseiten neu gesperrt. Der Index über die neuen Sperrungen maliziöser Webseiten lag bei durchschnittlich 278 Punkten und damit mehr als zweieinhalb Mal höher als zu Beginn der Aufzeichnungen im Jahr 2018 (vgl. Abbildung 28, Seite 73).

Ergänzend wird die Sicherheit der Regierungsnetze mit einem zentralen Schutz vor Spam-E-Mails erhöht. Diese Maßnahme wirkt nicht nur gegen unerwünschte Werbe-E-Mails. Auch Cyberangriffe wie Phishing-E-Mails werden damit erkannt. Die Spam-Quote, also der Anteil unerwünschter E-Mails an allen eingegangenen E-Mails, lag im Berichtszeitraum bei durchschnittlich 53 Prozent.

Aufkommen und Entwicklung der Spam-E-Mails in den Netzen des Bundes werden durch den Spam-Mail-Index gemessen (vgl. Abbildung 29, Seite 74). Dieser erreichte im Berichtszeitraum durchschnittlich 88 Punkte (~ 30 % im Vergleich zum vergangenen Berichtszeitraum). Dabei waren leichte Schwankungen aufgrund verschiedener Spam-Wellen zu verzeichnen. Die Spam-Filter der Bundesverwaltung wehren solche Spam-Wellen zuverlässig ab, sodass sie die adressierten Nutzenden nicht erreichen.

## Index über die neuen Sperrungen maliziöser Webseiten

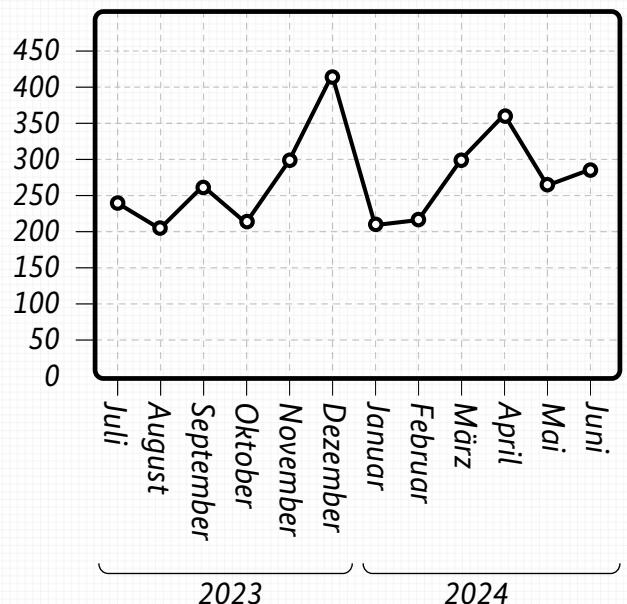


Abbildung 28: Index über die neuen Sperrungen maliziöser Webseiten (2018 = 100)

## Abbildung 28 / Webfilter-Messung in den Netzen des Bundes

**Ziel der Statistik** Aufkommen nötig gewordener neuer Sperrungen am Webfilter der Netze des Bundes, die den Zugriff aus der Bundesverwaltung auf maliziöse Webseiten blockieren. Berichtet wird monatlich. / **Grundgesamtheit** Alle neuen Sperrungen maliziöser Webseiten, die dem BSI aufgrund aktueller Lageerkenntnisse nötig erscheinen. / **Stichprobe** Alle neuen Sperrungen, d. h. Detektions- und Filterregeln am Webfilter der Netze des Bundes. / **Erhebungsdesign/-instrumente** Monatsaggregation einer laufenden Erhebung am Webfilter der Netze des Bundes. / **Reichweite** Ausgenommen sind Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen. Berichtet wird über Sperrungen maliziöser Webseiten, nicht über Zugriffsversuche auf maliziöse Webseiten. / **Qualitätsbewertung** Die den Sperrungen zugrunde liegende Lagebewertung gilt für die Netze des Bundes; Die Netze des Bundes bilden eine der größten Netzstrukturen in Deutschland überhaupt und können daher als Blaupause für das Internet insgesamt betrachtet werden.

## Spam-Mail-Index für die Bundesverwaltung

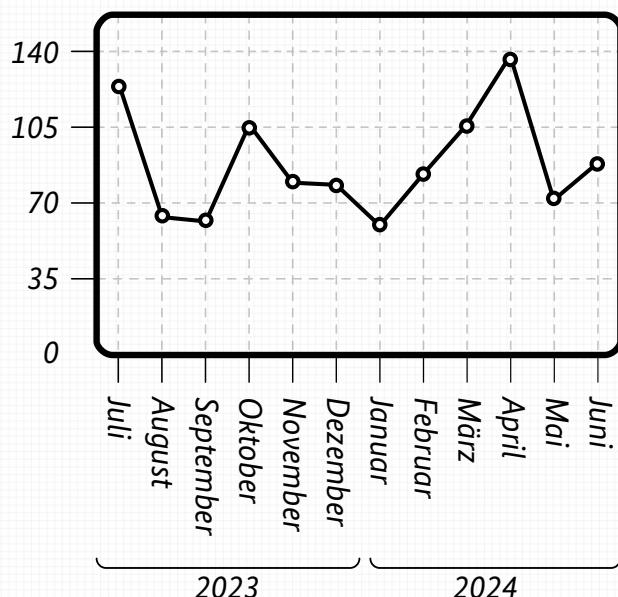


Abbildung 29: Spam-Mail-Index für die Bundesverwaltung (2018 = 100)

Abbildung 29 / Erhebung über den

### E-Mail-Verkehr mit der Bundesverwaltung

**Ziel der Statistik** Erhebung über den eingehenden E-Mail-Verkehr mit der Bundesverwaltung. Berichtet wird monatlich. / **Grundgesamtheit** Alle E-Mails, die am zentralen Mail-Transfer-Agent eingehen. / **Stichprobe** Vollerhebung. / **Erhebungsdesign/-instrumente** Tagesaggregation der Detektionen am Spam-Filter der Netze des Bundes. / **Reichweite** Ausgenommen sind Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen. Erfasst werden allgemeine statistische Merkmale, Spam-Status und Informationen über E-Mail-Anhänge. / **Qualitätsbewertung** Präzise, da Vollerhebung. Geringfügige Inkonsistenzen aufgrund sich verbessernder Detektion und unterschiedlicher Berechnungszeitpunkte.

## Angriffe auf E-Mail-Postfächer verschiedener Einrichtungen

### Sachverhalt

Im vergangenen Jahr wurde das BSI vermehrt auf Vorfälle aufmerksam, in denen E-Mail-Postfächer verschiedener relevanter, zum Teil politiknäher Organisationen angegriffen wurden. Dabei bedienten sich insbesondere staatliche Akteure verschiedener Methoden, um Zugriff auf E-Mails zu erhalten. Dazu gehörten Angriffe mit schwachen oder recycelten Passwörtern, Angriffe über Zero-Day-Schwachstellen oder Phishing-Angriffe. Eine größere Angriffsfläche stellen insbesondere Webmail-Systeme dar, die frei über das Internet und ohne Multi-Faktor-Authentifizierung erreichbar sind.

### Bewertung

Durch solche Angriffe können Daten abgeflossen sein, die im Rahmen hybrider Bedrohungen von staatlichen Akteuren genutzt werden könnten. Dies stellt insbesondere aufgrund der aktuellen geopolitischen Umstände und

der Wahlen im Jahr 2024 ein erhöhtes Risiko dar. Neben dem reinen Datenabfluss besteht zusätzlich das Risiko von gezielten sogenannten Spear-Phishing-Angriffen, entweder bedingt durch die abgeflossenen Informationen oder durch die aktive Nutzung kompromittierter Postfächer.

### Reaktion

Das BSI hat bei mehreren Vorfällen, teilweise in Zusammenarbeit mit weiteren Bundesbehörden, die betroffenen Einrichtungen durch forensische Untersuchungen und Beratung unterstützt. Eine bessere Umsetzung von Passwort-Richtlinien, die Nutzung von Multi-Faktor-Authentifizierung sowie die Einschränkung der Erreichbarkeit des internen Netzwerkes aus Webmail-Systemen heraus hätten Angriffe dieser Art und die Nutzung von gestohlenen Zugangsdaten in einigen Fällen verhindern können. Dies unterstreicht die Notwendigkeit der Umsetzung von grundlegenden Sicherheitsmaßnahmen.

## Ransomware-Angriff auf einen kommunalen IT-Dienstleister

### Sachverhalt

Ein kommunaler IT-Dienstleister ist Ende Oktober 2023 Opfer eines Cyberangriffs geworden. Laut Pressemitteilung des zuständigen Polizeipräsidiums fand der Angriff in der Nacht zum 30. Oktober 2023 statt. Am 31. Oktober 2023 teilte der IT-Dienstleister mit, dass verschlüsselte Daten auf Servern entdeckt worden seien. Aufgrund des Cyberangriffs habe der IT-Dienstleister vorsorglich die Mehrheit seiner IT-Systeme heruntergefahren.

Durch den Angriff seien eine Vielzahl kommunaler Verwaltungen, Fachverfahren und Webseiten betroffen.

Der IT-Dienstleister ist laut eigenen Angaben für die Betreuung von 20.000 kommunalen Arbeitsplätzen zuständig. Laut den Medienberichten hat der IT-Dienstleister 72 kommunale Kunden mit mindestens 1,7 Millionen Einwohnerinnen und Einwohnern, die von den Auswirkungen des Angriffs betroffen waren.

Im Januar 2024 hat der IT-Dienstleister einen Forensik-Bericht veröffentlicht, der die Ransomware-Gruppe Akira als Angreifer ausmacht. Der initiale Zugriff auf das Unternehmen erfolgte laut Bericht durch eine VPN-Lösung, mittels zuvor erbeuteter oder erratener Zugangsdaten oder mittels Ausnutzung einer Schwachstelle.

Bei Redaktionsschluss des vorliegenden Berichts befand sich der Dienstleister weiterhin in der Wiederanlaufphase, bei der bestimmte Fachverfahren wiederhergestellt werden oder in einem Basisbetrieb laufen und andere Fachverfahren weiterhin nicht zur Verfügung stehen.

### Bewertung

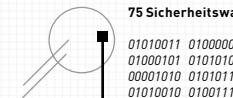
Während Bundesbehörden zentral über die Regierungsnetze abgesichert sind, gestalten die Behörden der Kommunen ihre IT-Sicherheitsmaßnahmen unterschiedlich. Die IT-Dienstleister der Kommunen sind eigenständig für die etablierten Abwehrmaßnahmen verantwortlich. Der Ausfall eines zentralen IT-Dienstleisters hat gravierende Auswirkungen für eine hohe Anzahl von kommunalen Diensten und damit verbunden auf die breite Bevölkerung.

Die Ransomware Akira basiert auf dem im Jahr 2022 öffentlich gewordenen Quellcode der Ransomware Conti. Die Angreifer setzen in der Regel auf die Kombination aus Verschlüsselung und Veröffentlichung von gestohlenen Daten auf einer Leak-Seite.

### Reaktion

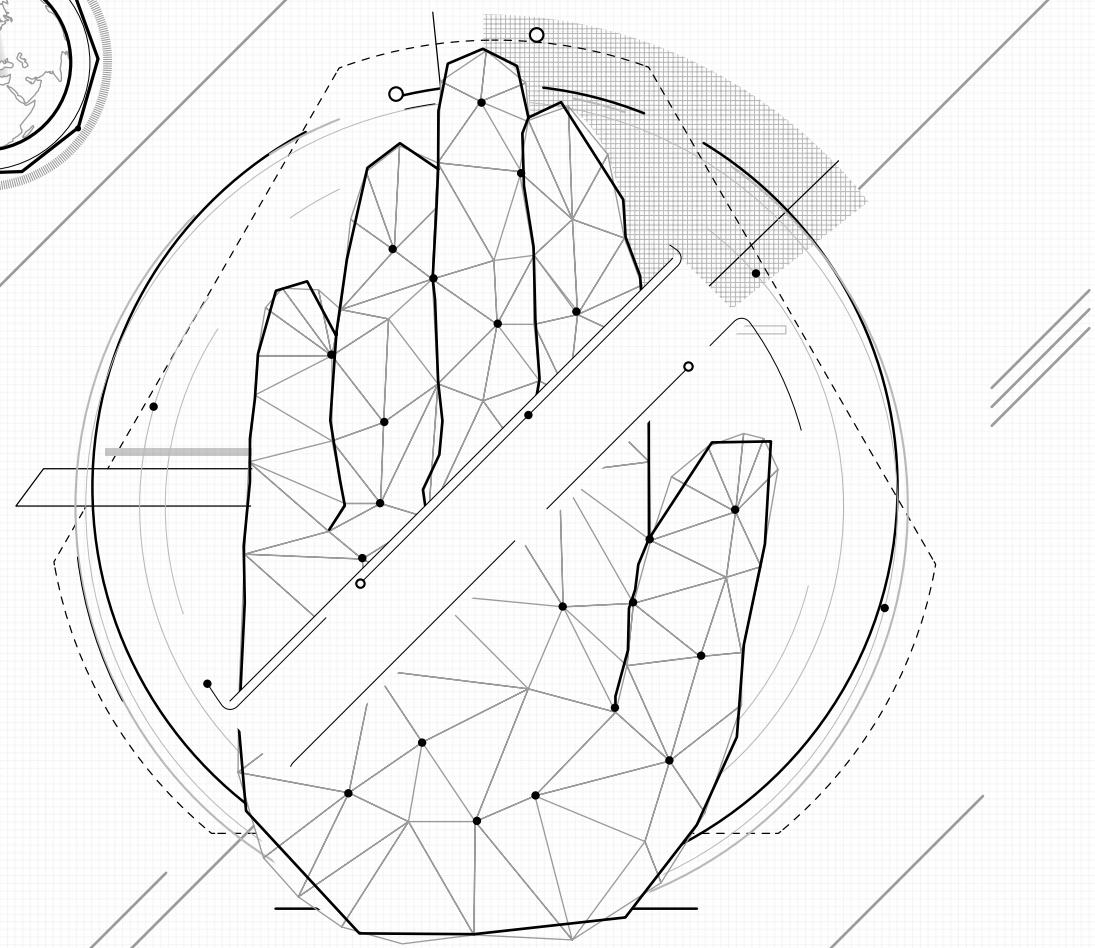
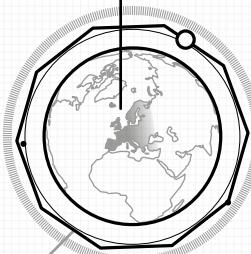
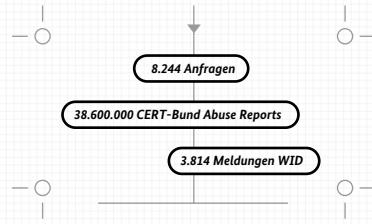
Der angegriffene IT-Dienstleister hatte vorsorglich die Mehrheit seiner IT-Systeme heruntergefahren und stand in Kontakt mit dem Landeskriminalamt, externen Sicherheitsdienstleistern und dem BSI. Als Reaktion auf den Cyberangriff wurde am 31. Oktober 2023 ein erweiterter Krisenstab gebildet, in dem neben dem Opfer auch externe IT-Forensiker sowie die IT-Verantwortlichen aller Kreisverwaltungen des Verbandsgebiets vertreten waren.

# D RESILIENZ

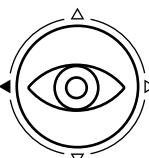


75 Sicherheitswarnungen

01010011 01000001 01000110  
01000101 01010100 01011001  
00001010 01010111 01000001  
01010010 01001110 01001001  
01001110 01000111



MY-ID123  
ELECTRONIC



# 12 – Cyberresilienz gesellschaftlicher und politischer Großveranstaltungen

Sicherheitskonzepte für Massenevents müssen auch den digitalen Raum umfassen. Vor der Fußball-Europameisterschaft im Sommer 2024 waren zum Beispiel ganze Infrastrukturen, aber auch einzelne Sportvereine durch Phishing-Kampagnen, DDoS-Angriffe und Ransomware-Infektionen bedroht.

Auch die Demokratie wird im digitalen Raum angegriffen. Durch Cyberangriffe auf Parteien werden Server lahmgelegt oder E-Mails und Dokumente erbeutet. Auf das politische Geschehen in Deutschland nehmen fremde Staaten illegitim Einfluss. Seit dem Angriffskrieg auf die Ukraine hat beispielsweise Russland seine Aktivitäten verstärkt. Gezielte Desinformation erschwert es der Bevölkerung, im Internet seriöse von unseriösen Informationsquellen zu unterscheiden. Durch den Einsatz Künstlicher Intelligenz werden Bilder, Audio- und Videodateien täuschend echt manipuliert. Desinformation und politische Einflussnahme vor Wahlen manipulieren die politische Willensbildung.

## 12.1 Cybersicherheit von Wahlen im Superwahljahr 2024

Im Jahr 2024 stehen weltweit mehr als 70 Wahlen an oder sind bereits erfolgt, darunter beispielsweise die Präsidentschaftswahlen in den USA, Indien und Russland. Für deutsche Staatsbürgerinnen und Staatsbürger fanden und finden nicht nur die Europawahl, sondern auch drei Landtagswahlen in Sachsen, Thüringen und Brandenburg sowie neun Kommunalwahlen statt. Sowohl der Wahlprozess und die Kommunikation durch Behörden und Medien als auch die Meinungs- und Willensbildung im Kontext von Wahlen sind mittlerweile in hohem Maße von Informationstechnik abhängig und damit auch im Fokus der Informationssicherheit.

### Bedrohungslage und Arten der illegitimen Einflussnahme und Angriffe im Kontext von Wahlen

Das BSI unterscheidet grundsätzlich zwischen direkter Einflussnahme (auf den Wahlprozess) und indirekter Einflussnahme (auf die öffentliche Meinung). Dabei soll gezielt die Legitimität der Wahlen in Zweifel gezogen werden, um das Vertrauen der Bürgerinnen und Bürger in

demokratische Prozesse und Institutionen zu schwächen.

Dazu gehören beispielsweise sogenannte Hack-and-Leak-Kampagnen gegen Parteien, bei denen E-Mails und Dokumente gestohlen und dann – teilweise manipuliert – veröffentlicht werden. Hinzu kommen immer wieder Angriffsversuche auf Webseiten und Server, die Wählerdaten enthalten oder Informationen zur Wahl zur Verfügung stellen.

Zu illegitimer Einflussnahme zählen beispielsweise:

- Verbreitung von Falschinformationen, um gesellschaftliche Gruppen gezielt, zum Beispiel mittels Reizthemen, gegeneinander auszuspielen und aufzuhetzen,
- Fälschungen und illegitime Übernahme von Social-Media-Accounts, Internetseiten von Personen (Defacement), Parteien, Medienunternehmen oder Behörden,
- der Einsatz von Künstlicher Intelligenz zur Manipulation von Bildern sowie Audio- und Video-Dateien (Deepfakes<sup>28</sup>),
- Delegitimation von demokratischen Institutionen und Personen, die das Vertrauen in den Staat und die Demokratie untergraben,
- gezielte Desinformation im Namen einer real existierenden Person, verbunden mit erheblichen Reputations-schäden.

### Was unternimmt das BSI konkret zum Schutz parlamentarischer Wahlen?

Das BSI verfolgt zum Schutz parlamentarischer Wahlen einen breiten gesamtgesellschaftlichen Ansatz. Es unterstützt unter anderem Bundes- und Landeswahlleitungen, Kandidierende und Parteien in Belangen der Informationssicherheit mit verschiedenen Informations-, Hilfs- und Beratungsangeboten.

Im Zuge stattfindender Wahlen zielen die Maßnahmen insbesondere auf:

- die Stärkung des Kernwahlprozesses,
- die Erhöhung der Resilienz gegen technische Manipulationsversuche und
- die Sensibilisierung von Kandidierenden und Mandatstragenden sowie den digitalen Persönlichkeitsschutz.

Zur **Stärkung des Kernwahlprozesses** hat eine Bund-Länder-Arbeitsgruppe zusammen mit dem BSI ein IT-Grundschutz-Profil Schnellmeldungen<sup>29</sup> erstellt. Dieses soll die Anpassung des Sicherheitsprozesses nach IT-Grundschutz für die Schnellmeldung bei bundesweiten parlamentarischen Wahlen bis zu den Kreiswahlleitungen erleichtern.

Darüber hinaus tauscht sich das BSI zur Notfallplanung und zum IT-Krisenmanagement über das Nationale IT-Lagezentrum mit den beteiligten Wahlbehörden und relevanten Akteuren aus und bewertet diese. Zusätzlich bietet das BSI Hilfestellung in der Vermittlung von geeigneten DDoS-Mitigations-Dienstleistern.

Um die **Resilienz gegen technische Manipulationsversuche bei Wahlen zu erhöhen**, bietet das BSI beispielsweise Webchecks, Pentests, Cybersicherheitschecks für expo nierte Personen (CYBEX-Checks) sowie Vorfallunterstützung bis hin zum Einsatz von Mobile Incident Response Teams (MIRT) an. Bei Vorfällen spielt insbesondere das zuständige nationale Computer Emergency Response Team Bund (CERT-Bund) im BSI eine zentrale Rolle.

Besonders wichtig ist dem BSI im politischen Bereich **Prävention** und vor allem die **Sensibilisierung der Zielgruppen**, wie zum Beispiel der Wahlbehörden, Parteien, Kandidierenden und Mandatstragenden. Mit zahlreichen Webinaren, Handreichungen, Merkblättern und Vorträgen informiert das BSI deshalb regelmäßig und passt seine Angebote fortlaufend an die Bedarfe der Zielgruppen an.

#### **Unterstützung der Länder**

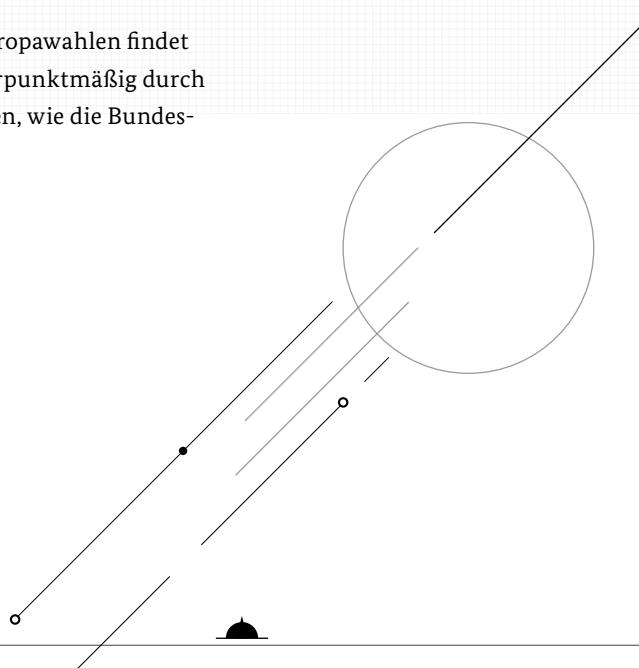
Das BSI nutzt die im Rahmen von Wahlen auf den unterschiedlichen Ebenen gewonnenen Erkenntnisse und Erfahrungen, um auch den Ländern Unterstützung für eine informationssichere Durchführung der jeweiligen Landtagswahl anzubieten.

Bei anstehenden Bundestags- oder Europawahlen findet eine Unterstützung der Länder schwerpunktmäßig durch eine Adressierung über Multiplikatoren, wie die Bundes wahlleitung, statt.

## **12.2 Cybersicherheit im Rahmen von Sportereignissen**

Durch die zunehmende Digitalisierung der Eventbranche, die aktuelle allgemeine Bedrohungslage und ihre gesellschaftliche, mitunter auch politische Relevanz sind Großveranstaltungen immer öfter direkt oder indirekt von Cyberangriffen betroffen. In den letzten Jahren kam es immer häufiger zu Vorfällen mit Eventbezug, von Phishing-Kampagnen<sup>30</sup> über Datenleaks<sup>31</sup>, DDoS-Angriffen<sup>32</sup> und Ransomware-Infektionen einzelner Infrastrukturen<sup>33</sup> und Sportvereine<sup>34</sup> bis hin zum gezielten Einsatz von Schadsoftware wie dem Olympic Wiper von 2021<sup>35</sup>. Die kontinuierliche Lagebeobachtung, mögliche Bedrohungsszenarien und entsprechende Reaktionsmaßnahmen sollten daher in Veranstaltungssicherheitskonzepte integriert sowie Melde- und Eskalationswege beübt werden.

Aus diesen Gründen war das BSI bereits frühzeitig an der Sicherheitsplanung der diesjährigen Fußball-Europameisterschaft in Deutschland beteiligt. In enger Zusammenarbeit mit der Euro 2024 GmbH, anderen deutschen Sicherheitsbehörden und dem Cybersicherheitsteam der UEFA beobachtete das BSI die Gefährdungslage im Cyberraum, sensibilisierte die ausrichtenden Städte sowie andere relevante Akteure und entsandte eine Verbindungsperson in das eigens für die Spiele eingerichtete International Police Coordination Center (IPCC 2024) in Neuss.



# 13 – Resilienz in der Cloud

Hohe Flexibilität, Leistungsfähigkeit und Verfügbarkeit – aufgrund seiner zahlreichen Vorteile ist Cloud Computing für viele Anwendungsfälle das Mittel der Wahl, manchmal sogar das einzige mögliche Mittel. So setzen laut Cloud-Monitor-2023 der KPMG AG Wirtschaftsprüfungsellschaft bereits mehr als neun von zehn Unternehmen auf Cloud Computing: Mehr als die Hälfte verfolgt eine Cloud-First-Strategie, knapp ein Fünftel eine Cloud-Only-Strategie.

## Angriffe verlagern sich in die Cloud

Diese hohe Nutzung macht Cloud-Anbieter zu Angriffszielen (vgl. Kapitel Angriffe auf die Cloud, Seite 53). Zudem kann die hohe Komplexität der Clouds dazu führen, dass sie nicht beherrscht werden und es teilweise zu erheblichen Ausfällen kommt. Hiervon sind in der Regel sehr viele Institutionen, die Cloud-Dienste nutzen (nachfolgend „Anwender“), teilweise sogar ganze Wirtschaftsbereiche betroffen.

## Verantwortung der Cloud-Anbieter

Die Cloud-Anbieter tragen eine sehr hohe Verantwortung und müssen daher über eine ebenso hohe Informations-sicherheit verfügen – zum eigenen Schutz und zum Schutz ihrer Anwender. Das BSI ist hier in vielfältiger Weise aktiv.

Der Cloud Computing Compliance Criteria Catalogue des BSI (BSI C5) beschreibt das Mindestmaß an Informations-sicherheit bei der Erbringung von Cloud-Diensten. Weit über 50 Cloud-Anbieter haben insgesamt mehrere Hundert Cloud-Dienste gemäß BSI C5 abgesichert und dies in einem Testat nachgewiesen. Der BSI C5 ist zudem eine der wichtigsten Grundlagen für das kommende EU-Cloud-Sicherheitszertifikat (EUCS).

Darüber hinaus steht das BSI mit vielen Cloud-Anbietern seit Langem in umfangreicher, vertrauensvoller Kommunikation. Dazu gehören zum Beispiel Kooperationsabkommen, die den Stellenwert des BSI für die Cloud-Anbieter unterstreichen. So erhält das BSI tiefgehende Einblicke und kann seine Expertise und Hinweise direkt einbringen.

Im Nachgang zum erfolgreichen Angriff auf die Microsoft Azure Cloud durch Storm-0558 (siehe Vorfall Kompromittierung der Microsoft-Cloud-Infrastruktur, Seite 54) hat das BSI im Januar 2024 ein Auskunftsverlangen nach §7a

Absatz 2 Satz 1 BSIG zum Thema Double Key Encryption (DKE) gestartet und Microsoft um Beantwortung der in diesem Zusammenhang aufgeworfenen Fragen aufgefordert. Die Beantwortung dieser Fragen erfolgte auf Basis etablierter und vertrauensvoller Kommunikation. Ein Ergebnis hiervon ist ein Whitepaper von Microsoft<sup>36</sup>, das M365-Anwendern nun erstmals ermöglicht, die Schutzwirkung von DKE und eventuell verbleibende Restrisiken in Abhängigkeit von ihrer Einsatzkonfiguration zu bewerten und entsprechend richtig einzusetzen.

## Verantwortung der Cloud-Anwender

Auch wenn der Cloud-Anbieter für einen Großteil der Informationssicherheit verantwortlich ist, verbleibt ein nicht unerheblicher Teil der Verantwortung beim Cloud-Anwender. Tatsächlich gehören Angriffe auf Anwender oder durch Anwender umgesetzte Fehlkonfigurationen zu den häufigsten Ursachen für Cloud-Vorfälle.

Deshalb muss der Anwender eine geeignete Sicherheitsarchitektur, zum Beispiel nach IT-Grundschutz, sowie eine Strategie und eine Vorgehensweise für die Cloud-Nutzung haben. Der IT-Grundschutz-Baustein zur Cloud-Nutzung und der Mindeststandard zur Nutzung externer Cloud-Dienste bieten hier wertvolle Anleitungen.

Cloud-Dienste bieten oft weitere Sicherheitsmaßnahmen, die von den Anwendern einfach genutzt werden können, zum Beispiel Identity- und Access-Management nach „Least Privilege“-/„Need to Know“-Prinzip, Multi-Faktor-Authentisierung oder den Einsatz gehärteter Server. Das sehr umfangreiche Monitoring in der Cloud macht alle Aktivitäten transparent und ermöglicht Dienste wie Intrusion Detection oder DDoS-Mitigation. Die Cloud bietet ideale Voraussetzungen für automatisierte Sicherheits-nachweise (Compliance as Code), die auch im IT-Grund-schutz und BSI C5 genutzt werden.

Das BSI arbeitet an der Bereitstellung sicherer Angebote mittels Infrastructure as Code, das heißt Bereitstellung, Konfiguration, Aktualisierung und Löschung von Cloud-Diensten per Code.

Verschlüsselung ist ein sehr wichtiges Mittel, um die Ver-traulichkeit von Daten sicherzustellen. Innerhalb der Cloud ist die Verschlüsselung für alle Daten „in transit“ und „at rest“ Standard. Entscheidend ist, dass der Grad der Kontrolle, den der Anwender über das Schlüsselmanagement hat, dem

Schutzbedarf der zu verschlüsselnden Daten entspricht. Das Spektrum an Möglichkeiten reicht von der Verwendung anbietergenerierter und -verwalteter Schlüssel bis hin zu Verfahren wie DKE, bei denen der Anwender selbst Schlüssel generiert und verwaltet.

Confidential Computing, also weitere Verschlüsselung bei der Verarbeitung („in use“), ist bei vielen Cloud-Anbietern möglich und bietet zusätzliche Sicherheit.

### **Cloud-Strategie des BSI**

Cloud Computing bietet hinsichtlich Funktionalität, Sicherheit und Resilienz viele Chancen, die es zum Rückgrat der Digitalisierung machen. Um eine sichere Nutzung von Cloud-Diensten auch in der Bundesverwaltung zu ermöglichen und dabei den mit Cloud Computing verbundenen Risiken Rechnung zu tragen, hat das BSI eine Cloud-Strategie entwickelt.

Ziel 1: Public Clouds der Hyperscaler aktiv und sicher in Deutschland nutzen. Dazu führt das BSI Risiko- und Bedrohungsanalysen durch.

Ziel 2: Eingestufte Informationen bis VS-NfD in Clouds verarbeiten. Das BSI untersucht dazu, unter anderem im Rahmen der RED-Cloud-Studie, durch welche Sicherheitsanforderungen und -maßnahmen in konkreten Anwendungsfällen ein hinreichender Schutz gewährleistet werden kann. Auch die Zulassung von Cloud-Infrastrukturkomponenten spielt dabei eine Rolle.

Ziel 3: Souveräne Nutzungsszenarien für europäische und nationale Clouds konkurrenzfähig gestalten. Hierfür ist das BSI in vielen Vorhaben, welche die Umsetzung von Souveränität zum Ziel haben, involviert.

Ziel 4: Resilienz der Digitalisierung durch sichere Cloud-Nutzung voranbringen. Hier plant das BSI, Werkzeuge zur Skalierung der sicheren Cloud-Nutzung bereitzustellen und zu unterstützen. Solche Werkzeuge können Code-Beispiele zur Umsetzung von Infrastructure as Code oder Compliance as Code sein, die eine sichere und richtlinienkonforme Nutzung von Cloud-Diensten erleichtern und zur Regulierung der Digitalisierung beitragen.

### **Cloud-Nutzung in der Verwaltung**

Das BSI begleitet Einrichtungen der öffentlichen Verwaltung bei der resilienten und souveränen Nutzung von Cloud-Diensten. Anhand konkreter Anwendungsfälle von Bundesbehörden untersucht und bewertet das BSI deren Cloud-Sicherheit und macht Vorgaben für die sichere

Nutzung. Zudem unterstützt es in großen Cloud-Vorhaben der Bundesverwaltung wie der Deutschen Verwaltungscloud und der Delos Cloud.

Darüber hinaus führt das BSI intensive Gespräche mit nationalen wie auch internationalen Cloud-Anbietern über die Nutzung von Cloud-Diensten in der öffentlichen Verwaltung, unter anderem im Kontext des Projekts „Cloud-Reallabor: Sichere Verarbeitung in der Cloud“ der Deutschen Rentenversicherung Bund im GovTech Campus Deutschland.

Der GovTech Campus Deutschland ist ein gemeinnütziger Verein, der durch das BMI und weitere Vertreter aus Verwaltung, Technologieszene, Unternehmen, Wissenschaft und Zivilgesellschaft gegründet wurde. Das BSI ist diesem zu Beginn des Jahres 2024 beigetreten. Der GovTech Campus bietet einen kollaborativen Diskurs zur Modernisierung und Digitalisierung des Staates und der Verwaltung.

Im Projekt Cloud-Reallabor bringt das BSI seine Expertise ein. In diesem Projekt soll die sichere Nutzung von Public-Cloud-Angeboten – unter anderem zur Verarbeitung sensibler Daten – auch für die öffentliche Verwaltung und KRITIS-Betreiber untersucht werden.

Zusammengefasst lässt sich sagen, dass die Nutzung von Cloud-Diensten mit Chancen und Risiken verbunden ist. Anwender müssen die Risiken sorgfältig und für jeden Anwendungsfall einzeln abwägen – dazu gehört auch die Planung geeigneter Maßnahmen zur Risikominderung. Die oben genannten Cloud-Produkte des BSI können den Anwender dabei unterstützen.

Die Chancen für die Informationssicherheit liegen auf der Hand: Cloud Computing erhöht die Resilienz gegen Angreifer und wird in dieser Funktion in der sich wandelnden Cyberbedrohungslandschaft zukünftig eine immer größere Rolle spielen.

Das BSI beobachtet und antizipiert Entwicklungen im Bereich der Cloud-Sicherheit – es hat bereits jetzt eine umfangreiche fachliche Expertise durch tiefe Einblicke in Public Clouds und ist in der Lage, deren Sicherheitseigenschaften zu bewerten. Diese Expertise nutzt das BSI, um Bundesbehörden bei der Migration in die Cloud und der sicheren Cloud-Nutzung zu unterstützen. Das BSI ebnnet somit den Weg für eine resiliente Digitalisierung der deutschen Verwaltung – mit Cloud Computing als Rückgrat und Treiber.

# 14 – Elektronische Identitäten

Elektronische Identitäten bilden die Grundlage für eine sichere Digitalisierung. Mit der Online-Ausweisfunktion verfügt Deutschland bereits seit mehr als zehn Jahren über eine hochsichere und datensparsame elektronische Identität (eID). Sie ist auch europaweit für Sicherheit und Datensparsamkeit bekannt und notifiziert sowie grenzüberschreitend nutzbar. Die Entstehung hierauf aufsetzender digitaler Dienste und deren Nutzung bleibt bisher jedoch hinter den Erwartungen zurück. Immerhin war im Berichtszeitraum ein signifikanter und stetiger Anstieg von Diensten und Nutzerzahlen zu beobachten.

## 14.1 Für die Zukunft: EUDI-Wallet

Die neue eIDAS-Verordnung ist in Kraft getreten und legt den rechtlichen Rahmen für das europäische Identitäten-Ökosystem mit EUDI-Wallet fest. Die EUDI-Wallet soll demnach als elektronisches Identifizierungsmittel grenzüberschreitend nutzbar werden und neben klassischen Identitätsattributen (Vorname, Name etc.) noch weitere Attribute (z. B. Bildungsabschluss, Führerschein) in verifizierbarer Art für Diensteanbieter bereitstellen können. Zudem soll sie die Möglichkeit zur qualifizierten elektronischen Signatur bieten.

### eIDAS Large Scale Pilots (LSP)

Im Zusammenhang mit der EUDI-Wallet möchte die Kommission in vier sogenannten Large Scale Pilots (LSPs) nachweisen, dass die Vorgaben umsetzbar sind. Für den LSP „POTENTIAL“<sup>37</sup> hat Deutschland zusammen mit Frankreich die Federführung.

In den zugehörigen technischen Unterarbeitsgruppen soll zum einen eine interoperable europäische Wallet-Infrastruktur definiert und implementiert werden, und zum anderen sollen Funktionalitäten in grenzüberschreitenden Nutzungsszenarien erprobt werden.

### eIDAS national – der Konsultationsprozess

Ein Konsultationsprozess des BMI hat zum Ziel, auf eine transparente Art und Weise zu einem nationalen Identitäten-Ökosystem zu kommen, welches eine deutsche Wallet als Kernbestandteil hat und den Anforderungen der

eIDAS-Verordnung entspricht. Im Kontext dieses Prozesses wird in sogenannten Streams auch an der Architektur für die eine deutsche EUDI-Wallet gearbeitet. Das BSI ist in viele Streams des Prozesses intensiv eingebunden.

### Erste Iteration einer nationalen EUDI-Wallet

Die „Evolutionslösung“ als erste Iteration einer nationalen EUDI-Wallet, die auch auf Betreiben des BSI das Ziel hat, die eID-Nutzung in die Breite zu bringen, soll eine schnell verfügbare, auf den meisten mobilen Endgeräten einsetzbare und rein mobil nutzbare eID sein.

Sichere Hardware in mobilen Endgeräten ist jedoch noch nicht in ausreichendem Maße verfügbar und nutzbar, sodass es zunächst notwendig sein wird, auf Backend-systeme zur Sicherung der Prozesse zurückzugreifen.

Für eine rein mobil nutzbare, voll dezentrale eID, die weitverbreitet ist und ein hohes Vertrauensniveau erfüllt, sind breitflächig verfügbare (zertifizierte) sichere Hardwarelemente, wie zum Beispiel Secure Element (SE), eSIM etc., auf den Endgeräten der Nutzenden notwendig. Hierfür müssen noch Grundlagen in der Standardisierung, Regulierung etc. gelegt werden, an denen das BSI aktiv mitwirkt.

### CSP

Regelmäßig erscheinen neue Generationen von Secure Elements (SEs) wie eSE und eSIM/eUICC mit stetig aktualisierter Hard- und Software. Um trotz dieser Dynamik verlässliche Sicherheitsaussagen treffen zu können, hat das BSI das Konzept des Cryptographic Service Providers (CSP) entwickelt. Der CSP<sup>38</sup> ermöglicht es, eID-Anwendungen mit hohem Schutzbedarf unabhängig von der Hardware nach Common Criteria zu zertifizieren. Der CSP wird derzeit bei GlobalPlatform<sup>39</sup> standardisiert und soll ab 2025 als internationaler Standard für SEs verfügbar sein. Der CSP wurde zudem von der ENISA als Komponente zur Zertifizierung von Third-Party-Anwendungen für eSIM/eUICC anerkannt.

## 14.2 Anerkennung von eIDs in Europa

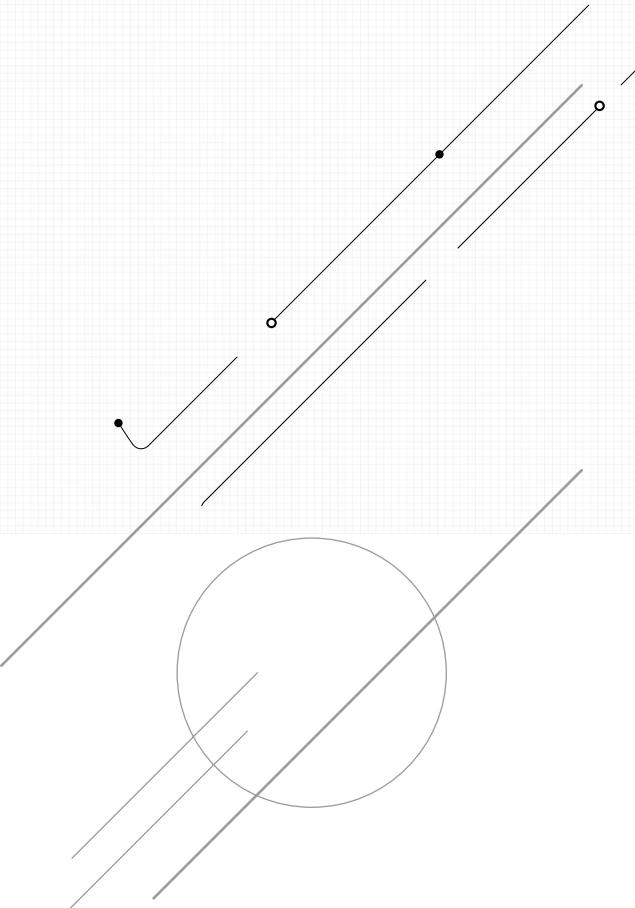
Im Rahmen der bisher gültigen eIDAS-Verordnung akzeptieren die EU-Mitgliedsstaaten gegenseitig notifizierte eIDs. Im Laufe des letzten Jahres hat sich das BSI im Rahmen der sogenannten Peer Reviews daran beteiligt, neue eIDs anderer EU-Staaten auf ihre Konformität zur eIDAS-Verordnung zu prüfen. Im letzten Jahr sind unter anderem eIDs aus Bulgarien und Zypern unter Beteiligung des BSI notifiziert worden.

Die endgültige Entscheidung zur Notifizierung findet in sogenannten eIDAS Cooperation Network Meetings statt, in denen auch allgemeine Herausforderungen und Lösungen der europäischen eID-Systeme diskutiert wurden. Im Februar 2024 war das BSI Gastgeber eines solchen Meetings des Cooperation Network, bei dem unter anderem Schwachstellen bei Biometrie und Gegenmaßnahmen demonstriert wurden.

## 14.3 AusweisApp

Mit der durch das BSI bereitgestellten AusweisApp<sup>40</sup> können sich Besitzerinnen und Besitzer eines Personalausweises, eines elektronischen Aufenthaltstitels oder einer eID-Karte für Bürgerinnen und Bürger der EU und des Europäischen Wirtschaftsraums (EWR) sicher online ausweisen.

Im Berichtszeitraum hat die AusweisApp ein neues moderneres Design erhalten. Im gleichen Zug wurde der Name AusweisApp2 in AusweisApp geändert.



# 15 – Europäisierung der Cybersicherheit

Cybersicherheit verlangt grenzüberschreitende Kooperation. Deshalb sorgt Europa mit gesetzlichen Vorgaben für ein gemeinsames Sicherheitsniveau. Diese Vorgaben tragen dazu bei, die Resilienz in den Mitgliedsländern zu steigern.

## 15.1 Cyber Resilience Act (CRA)

Im März 2024 wurde der Cyber Resilience Act (CRA) vom Europäischen Parlament angenommen. Diese EU-Verordnung zielt darauf ab, dass erstmalig horizontale – also von der Produktkategorie unabhängige – Cybersicherheitsanforderungen für den Schutz von digitalen Produkten über deren gesamten Lebenszyklus hinweg eingeführt werden. Hersteller müssen auch über den Zeitpunkt des Kaufs hinaus die Verantwortung für die IT-Sicherheit ihrer Produkte übernehmen. Das Gesetz wurde im März 2024 im EU-Parlament angenommen und nach Ende des Berichtszeitraums im Oktober 2024 beschlossen und damit final verabschiedet.

### Ein Upgrade für die Informationssicherheit

Das neue Regelwerk wird sich – bis auf wenige Ausnahmen – auf alle vernetzten oder vernetzbaren Produkte beziehen: vom Saugroboter über Software bis hin zu Produkten, die in kritischen Sektoren zum Einsatz kommen.

Der CRA definiert Zugangsvoraussetzungen für den EU-Binnenmarkt und erweitert den Geltungsbereich des CE-Kennzeichens. Die durch den Hersteller zu gewährleistende Sicherheit erstreckt sich damit erstmals nicht nur auf Betriebssicherheit (safety), sondern auch auf Informationssicherheit (security). Dies ist nicht nur bei Inverkehrbringen des Produktes, sondern über die übliche Nutzungsdauer eines Produktes verpflichtend.

Der CRA stellt Anforderungen sowohl an die Hersteller der Produkte als auch an die Produkte selbst – und dies bereits ab der Produktentwicklungsphase.

- Für Produkte wird Security by Design, Security by Default und Gewährleistung von Vertraulichkeit und Integrität der verarbeiteten Daten gefordert.
- Zum Umgang mit Schwachstellen werden Hersteller zum Beispiel verpflichtet, Sicherheitsupdates über den gesamten Lebenszyklus des Produkts bereitzustellen,

Schwachstellen zu melden und zu beheben sowie eine Software Bill of Materials (SBOM) zu pflegen.

- Für die Anwendenden müssen unter anderem verständliche Informationen zu bekannten Schwachstellen, verfügbaren Updates und einem sicheren Gebrauch des Produkts zur Verfügung gestellt werden.

Dies gilt nicht nur für die Hersteller, sondern auch für Importeure oder Händler, die entsprechende Produkte im EU-Binnenmarkt in den Verkehr bringen. In den einzelnen Mitgliedsstaaten werden Marktüberwachungsbehörden eingesetzt, die bei Nichteinhaltung der Anforderungen betroffene Produkte vom Markt nehmen können. Zudem drohen empfindliche finanzielle Strafen.

### Unterschiedliche Produktklassen – abgestufte Prüfungen

Auch wenn die grundlegenden Cybersicherheitsanforderungen für alle Produkte gleich sind, unterscheiden sie sich in der Art der Nachweispflicht und Prüfungstiefe. Unkritische Produkte benötigen mindestens eine Selbstbewertung durch den Hersteller. „Wichtige Produkte“ der Klasse I, wie zum Beispiel Passwort-Manager oder Router, können einer Selbstbewertung nach einem harmonisierten europäischen Standard unterzogen werden. Sollte für ein Produkt dieser Klasse kein harmonisierter Standard vorliegen, so muss das Produkt eine Konformitätsbewertung durch eine notifizierte Drittstelle durchlaufen. Für „Wichtige Produkte“ der Klasse II, wie zum Beispiel Firewalls, ist eine solche Konformitätsbewertung immer verpflichtend vorgeschrieben. Für Produkte der Risikoklasse „Kritisch“ ist eine Zertifizierung nach einem Zertifizierungsschema des Cybersecurity Acts verpflichtend vorgeschrieben. In dieser Klasse sind unter anderem Smart Meter verortet. Produkte dieser Klasse müssen nach einem Zertifizierungsschema des Cybersecurity Acts (CSA) zertifiziert werden. In dieser Klasse sind unter anderem Smart Meter verortet.

### Support durch das BSI – die Anforderungen des CRA umsetzen

Als EU-Verordnung braucht der CRA grundsätzlich keine nationalen Umsetzungsgesetze. Die Übergangsfrist von Inkrafttreten bis Geltungsbeginn wird 36 Monate betragen. Die Verpflichtung zur Meldung ausgenutzter Schwachstellen sowie schwerwiegender Cybersicherheits-

vorfälle besteht bereits nach 21 Monaten. Für Hersteller ist es ratsam, sich frühzeitig auf die neuen Marktzugangs-voraussetzungen vorzubereiten. Insbesondere bei längerfristigen Produktneuentwicklungen sollten die künftigen Anforderungen bereits jetzt mitgedacht werden, um zum Markteintritt die Konformität sicherstellen zu können.

Das BSI erarbeitet derzeit Handreichungen für betroffene Hersteller aller Formen und Größen sowie Entwicklerinnen und Entwickler. Sie sollen die Anforderungen vorab greifbarer machen.

- Die Anforderungen an Hersteller und Produkte bezüglich der Cyberresilienz werden konkret und übersichtlich in der TR-03183 beschrieben. Bereits im August 2023 wurde ein Teildokument mit Vorgaben zu Umfang, Inhalt und Format einer Software Bill of Materials (SBOM) zur Verfügung gestellt.
- Qualitätssicherung und sichere Entwicklungsprozesse werden mit weiteren Richtlinien und Empfehlungen abgedeckt.

Für viele konkretere Vorgaben im Rahmen des CRA greift die EU-Kommission auf das Fachwissen der europäischen Standardisierungsgremien zurück. Auch dort wirken die Expertinnen und Experten des BSI an einer sicheren Ausgestaltung der Produkte mit.

## 15.2 NIS-2-Richtlinie

NIS-2, die europäische Richtlinie für Cybersicherheit, soll bis Oktober 2024 in nationales Recht überführt werden. Sie legt zum Beispiel Kriterien für den Betrieb kritischer Anlagen fest und definiert Mindeststandards für deren Informationssicherheit. Darüber hinaus sind Mitgliedsstaaten dazu verpflichtet, ein Computer Security Incident Response Team (CSIRT) einzurichten, eine Zentrale für eine koordinierte Offenlegung von Schwachstellen. Diese Aufgabe nimmt das BSI als nationale Behörde für IT-Sicherheit bereits wahr.

Im europäischen Kontext ergeben sich aus der Umsetzung der sogenannten NIS-2-Richtlinie in nationales Recht aktuell wesentliche Handlungsfelder für das BSI. So wird das BSI gemäß Art. 31 Abs. 4 der NIS-2-Richtlinie die nationale Aufsicht über die Umsetzung der IT-Sicherheitsmaßnahmen führen, die in der Richtlinie festgelegt sind. Die Richtlinie verpflichtet die Mitgliedsstaaten zudem zur Einrichtung eines Computer Security Incident Response Teams (CSIRT), welches als zentrale Anlaufstelle für eine koordinierte Offenlegung von Schwachstellen (Coordina-

ted Vulnerability Disclosure, CVD) dienen soll. Diese Funktion wird bereits vom BSI, das als nationale Behörde für IT-Sicherheit agiert und maßgeblich an der Umsetzung der Richtlinie beteiligt ist, wahrgenommen. Für die Wirtschaft aber auch für die Bundesrepublik birgt die NIS-2-Richtlinie viele Neuerungen und Herausforderungen. Als einer der Vorreiter der europäischen Cybersicherheit ist Deutschland auf viele dieser Herausforderungen gut vorbereitet oder setzt einige der Anforderungen der EU-Richtlinie bereits um.

Als „Betreiber kritischer Anlagen“ sind die Betreiber Kritischer Infrastrukturen (KRITIS), deren Aufrechterhaltung essenzieller gesellschaftlicher Funktionen von zentraler Bedeutung ist, eine Teilmenge der in der NIS-2-Richtlinie adressierten „wesentlichen Einrichtungen“. In Deutschland existiert mit dem ersten IT-Sicherheitsgesetz (IT-SiG) bereits seit Juli 2015 ein einheitlicher Rechtsrahmen für mehr Cybersicherheit bei KRITIS.

Mit der Umsetzung der NIS-2-Richtlinie in nationales Recht wird das BSI durch eine Änderung des BSI-Gesetzes für deutlich mehr Unternehmen als zuvor zur Aufsichtsbehörde. Für die bestehenden Kritischen Infrastrukturen (KRITIS) ändert sich hierdurch voraussichtlich wenig, aber für ca. 29.000 nach dem Gesetz „besonders wichtige“ und „wichtige“ Einrichtungen ergeben sich erstmals Registrierungs-, Nachweis- und Meldepflichten. Das BSI bereitet sich aktuell mit der Anpassung bestehender Prozesse für Registrierung, Meldung und Entgegennahme von Nachweisen auf diese zusätzlichen Aufgaben vor.

Die Meldung von Sicherheitsvorfällen ermöglicht eine schnelle und koordinierte Reaktion auf Bedrohungen sowie die Erstellung eines detaillierten Lagebildes, das im kooperativen Austausch zur Verbesserung der Resilienz und des Cybersicherheitsniveaus in Deutschland und der EU führt.

Im Rahmen der Vorbereitungen zum nationalen Umsetzungsgesetz zu NIS-2 hat sich das BSI intensiv dafür eingesetzt, dass grundlegende Sicherheitsanforderungen an ein Informationssicherheitsmanagementsystem (ISMS) für die Bundesverwaltung verbindlich erklärt werden. Dies dient der Stärkung der Eigensicherung der Bundesverwaltung und der Gewährleistung eines notwendigen Mindestniveaus von Informationssicherheit in Deutschland. Die Anforderungen orientieren sich an den bereits heute nach § 8 Abs. 1 BSIG verbindlichen Mindeststandards. Diese verbindlichen Mindeststandards zielen auf ein einheitliches und angemessenes Sicherheitsniveau ab, um den wachsenden Bedrohungen im Cyberraum wirksam zu begegnen.

Der IT-Grundschutz stellt einen zuverlässigen Rahmen zur Implementierung eines ISMS dar. In diesem Rahmen sind Risikoanalysen zur Identifizierung und Bewertung von Sicherheitsrisiken sowie die Implementierung geeigneter Sicherheitsmaßnahmen vorgesehen. Ein nach IT-Grundschutz implementiertes ISMS deckt bereits heute die meisten in der NIS-2-Richtlinie geforderten Risikomanagementmaßnahmen ab oder bildet zumindest eine solide Grundlage, auf der Einrichtungen aufbauen können.

Die Umsetzung der NIS-2-Richtlinie ist ein bedeutender Fortschritt für die Cybersicherheit in Europa und in der Cybernation Deutschland. Das BSI ist dabei einer der zentralen Akteure und Treiber dieser Entwicklung und setzt sich dafür ein, dass die neuen Anforderungen effektiv in nationales Recht überführt und in die Praxis umgesetzt werden.

Das BSI unterstützt schon jetzt aktiv mit Hilfestellungen auf der BSI-Webseite:

- Die NIS-2-Betroffenheitsprüfung ist das zentrale Werkzeug zur Prüfung, ob ein Unternehmen voraussichtlich von der nationalen Umsetzung der NIS-2-Richtlinie in Deutschland erfasst sein wird.
- Die NIS-2-FAQ bieten eine Sammlung von Antworten auf die am häufigsten gestellten Fragen zur NIS-2-Richtlinie.
- Die Seite „NIS-2 – Was tun?“ enthält zahlreiche Hinweise, was wichtige und besonders wichtige Einrichtungen jetzt schon tun können.

Außerdem wird die Kommunikation des BSI zur Umsetzung der NIS-2-Richtlinie auch über weitere Kanäle und Formate kontinuierlich fortgesetzt. Das BSI wird in den kommenden Monaten bestehende Hilfestellungen aktualisieren und neue Hilfestellungen schaffen, sobald neue Informationen vorliegen.

**Weitere Informationen zur NIS-2-Richtlinie finden Sie auf der BSI-Webseite:**



## 15.3 Cybersecurity Act (CSA)

Der europäische Rechtsakt zur Cybersicherheit (Cybersecurity Act, CSA) ist am 27. Juni 2019 in Kraft getreten. Die europäische Cybersicherheitsagentur (ENISA) erhielt damit erstmals ein unbefristetes Mandat und wurde mit erweiterten Aufgaben und zusätzlichen Ressourcen ausgestattet, insbesondere im operativen Bereich. Weiterhin wurden Vorgaben für die europäische Cybersicherheitszertifizierung eingeführt.

Dieses neue System erhöht für die Informations- und Kommunikationstechnologie (IKT) die Resilienz von Produkten, Dienstleistungen und Prozessen gegenüber Cyberangriffen in der gesamten EU und setzt hohe Standards für Schutz und Vertrauenswürdigkeit in der digitalen Infrastruktur. Der CSA stellt sicher, dass Europa gut gerüstet ist, um den Herausforderungen der digitalen Zukunft zu begegnen.

### Rolle des BSI bei der Cybersicherheitszertifizierung

Im Berichtsjahr trat das Europäische Common-Criteria-Schema (EUCC) als erstes Zertifizierungsschema des CSA in Kraft. Weitere Schemata werden auf europäischer Ebene vorbereitet.

Das BSI ist die deutsche Nationale Behörde für Cybersicherheitszertifizierung (NCCA). Die aufsichtsführende NCCA stellt sicher, dass die für die Zertifizierung notwendige Infrastruktur bereitsteht, indem sie Konformitätsbewertungsstellen autorisiert. Zudem überwacht sie den Markt der zertifizierten Produkte. Die zertifizierende NCCA bewertet die Konformität von IKT-Produkten, -Dienstleistungen und -Prozessen mit hohen Vertrauenswürdigkeitsanforderungen.

### Auf dem Prüfstand: Die erste umfassende Evaluierung des CSA

Im Jahr 2024 stand die erste umfassende, alle fünf Jahre zu wiederholende Evaluierung des CSA an. Im Rahmen dieser Evaluierung wurden umfassende Interviews und Workshops organisiert, in denen verschiedene Stakeholder ihre Perspektiven und Erfahrungen einbrachten.

Als Ergebnis wird die Europäische Kommission eine Folgenabschätzung erstellen und darin verschiedene Optionen für die zukünftige Ausrichtung des CSA vorstellen. Die Resultate der Evaluierung sowie die daraus hervorgehenden Empfehlungen werden eine wesentliche Rolle bei der Konzeption der künftigen Cybersicherheitsstrategie

der EU spielen, um den fortwährenden Transformationen der digitalen Ära adäquat zu begegnen.

#### **Wie das BSI die Zukunft des CSA mitgestaltet**

Das BSI nimmt eine zentrale Rolle bei der Evaluierung des CSA ein. Durch diese aktive Beteiligung konnte die Rolle der ENISA geschärft und gestärkt werden. Bereits seit vielen Jahren engagiert sich das BSI aktiv bei der ENISA durch die Posten im Verwaltungsrat und im Exekutivrat. Im vergangenen Jahr wurde die Leiterin des BSI-Fachbereichs Verbindungswesen und Recht zur Vorsitzenden des Verwaltungsrats gewählt. Kolleginnen und Kollegen des BSI beteiligen sich in Arbeitsgruppen der ENISA und unterstützen durch Beiträge zu Studien, Konferenzen und Fachpublikationen. Es werden außerdem regelmäßig Mitarbeitende an die ENISA entsandt. Derzeit sind Kolleginnen und Kollegen im ENISA-Stab und im operativen Bereich tätig. Dies fördert Vertrauen und Austausch.

Das BSI engagiert sich in konstruktiver Weise für die Weiterentwicklung des Zertifizierungsframeworks. Auch in Zukunft wird das BSI darauf abzielen, seine Fachexpertise einzubringen, um zur Weiterentwicklung der europäischen Cybersicherheit beizutragen.

neben Aspekten der Cybersicherheit auf die wirtschaftliche und technische Umsetzbarkeit sowie die Prüfbarkeit der Standards.

Die europäische Standardisierung hat aus Sicht des BSI erheblich an Bedeutung gewonnen, denn die europäischen Regulierungen im Bereich der Cybersicherheit sind stark angewachsen und damit verbunden werden neue Standards durch die ESOs erarbeitet. Eine herausgehobene Rolle spielt dabei die Erstellung von harmonisierten Europäischen Normen (hEN). Diese hEN werden auf Grundlage offizieller Standardisierungsmandate der Europäischen Kommission durch die ESOs erarbeitet und, im Falle der Annahme durch die Kommission, im Amtsblatt der Europäischen Union veröffentlicht. Ihnen kommt im Bereich der Konformitätserklärungen des regulierten Marktes, erkennbar durch das CE-Kennzeichen, eine besondere Bedeutung zu.

Im Berichtszeitraum stellte daher die Beteiligung an der Erarbeitung der harmonisierten Standards zum Artificial Intelligence Act (AI Act), zum Cyber Resilience Act (CRA) und zur Radio Equipment Directive (RED) einen Schwerpunkt für das BSI dar. Besonders hervorzuheben ist hierbei die Erstellung der europäischen Norm-Entwürfe FprEN 18031-1 bis -3 im CEN/CENELEC zu den Cybersicherheitsanforderungen aus der RED, die mithilfe eines großen Ressourceneinsatzes des BSI noch rechtzeitig fertiggestellt werden konnten. Diese wurden bereits von den nationalen Normungsorganisationen der Mitgliedstaaten angenommen. Mit dem Beginn der Standardisierung im Rahmen des CRA gibt es weiterhin viele Möglichkeiten zur Mitgestaltung und Kooperation.

## **15.4 Lagebericht europäische Standardisierung**

Das Hauptziel der derzeitigen Standardisierungsarbeiten des BSI ist es, durch hochwertige und umsetzbare Normen auf dem europäischen Binnenmarkt das Sicherheitsniveau von Produkten und Infrastrukturen signifikant anzuheben, sodass Staat, Gesellschaft und Wirtschaft besser vor Angriffen und Ausfällen geschützt sind.

Das BSI beteiligt sich im Bereich der Standardisierung der Cybersicherheit auf europäischer Ebene an der Erstellung und Aktualisierung von Standards insbesondere von Europäischen Normen (EN) in den drei europäischen Standardisierungsorganisationen (ESOs). Das sind CEN, CENELEC und ETSI. Mitarbeitende des BSI setzen dort die Interessen der deutschen Bundesregierung als Vertretung der Bürgerinnen und Bürger durch.

Das BSI verfolgt bei seinen Standardisierungsaktivitäten insbesondere den Ansatz, nationale Vorgaben zu vereinheitlichen, indem bewährte Methoden und Ansätze (Best Practices) im Bereich der Cybersicherheit in den Europäischen Normen übernommen werden. Zudem achtet das BSI

## 16 – Zulassung von VS-Produkten

Das BSI stellt auf der Grundlage der allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschluss Sachen Anweisung, VSA) Zulassungsaussagen für IT-Sicherheitsprodukte aus. Mit der Zulassung wird diesen Produkten bescheinigt, dass sie im Rahmen des Geheim schutzes zum Schutz von elektronischen Verschluss Sachen (VS) in angemessen sicherer Weise verwendet werden können. Geprüfte VS-Produkte minimieren die Auswirkungen schädlicher Cyberzwischenfälle und schützen die Vertraulichkeit der VS bei Angriffen.

Die Zahl der ausgesprochenen Zulassungen liegt auf einem konstant hohen Niveau. Der überwiegende Teil der Zulassungsaussagen sind Re-Evaluierungen bereits zugelassener IT-Sicherheitsprodukte. Mit der Novellierung der VSA zum 1. April 2023 wurde die bisherige Freigabeempfehlung durch die Einsatz Erlaubnis ersetzt (vgl. Abbildung 30, Seite 88).

Neben der Ausstellung von Zulassungsaussagen für den Schutz nationaler Verschluss Sachen stellt das BSI auch Zulassungen für den Schutz von NATO- und EU-Verschluss Sachen aus (vgl. Abbildung 32, Seite 88). Dies erfolgt in den meisten Fällen in einem gemeinsamen Zulassungsverfahren, sodass mit Vorliegen der nationalen Zulassung auch die korrespondierende internationale Zulassung vorliegt oder die dazu erforderliche Zweitevaluierung angestoßen werden kann.

**Weiterführende Informationen zur VS-Zulassung:**



### Herstellerqualifizierung

Die dynamische und wachsende Bedrohungslage führt auch im Umfeld der elektronischen VS zu einer zwingend notwendigen Erhöhung der Resilienz. Eine Möglichkeit dafür ist die noch effektivere und effizientere Durchführung von Produktzulassungen, was durch die Herstellerqualifizierung erreicht werden kann.

Eine erfolgreich absolvierte Herstellerqualifizierung stellt die Voraussetzung für einen Hersteller dar, dass IT-Sicherheitsprodukte das „Qualifizierte Zulassungsverfahren für

VS-NUR FÜR DEN DIENSTGEBRAUCH“ durchlaufen können. In der Herstellerqualifizierung wird einem Hersteller nach erfolgreicher Bewertung der Entwicklungsprozesse durch das BSI das Vertrauen ausgesprochen, Produkte sicher im Sinne der VS-Zulassung entwickeln zu können.

Geprüfte, vertrauenswürdige Prozesse beim Hersteller erlauben es, Produktzulassungen mit einem erheblich reduzierten Evaluierungsumfang bei gleichzeitiger Aufrechterhaltung des Vertrauenswürdigkeitsniveaus durchzuführen. Damit ist ein „qualifizierter Hersteller“ in der Lage, eine Produktzulassung schneller zu durchlaufen, als dies bei einem herkömmlichen Zulassungsverfahren der Fall wäre. Die Effizienz des Verfahrens bestätigt sich durch eine Vielzahl erfolgreich durchlaufener Zulassungsverfahren, in denen eine Produktzulassung innerhalb von vier bis acht Wochen erteilt werden konnte.

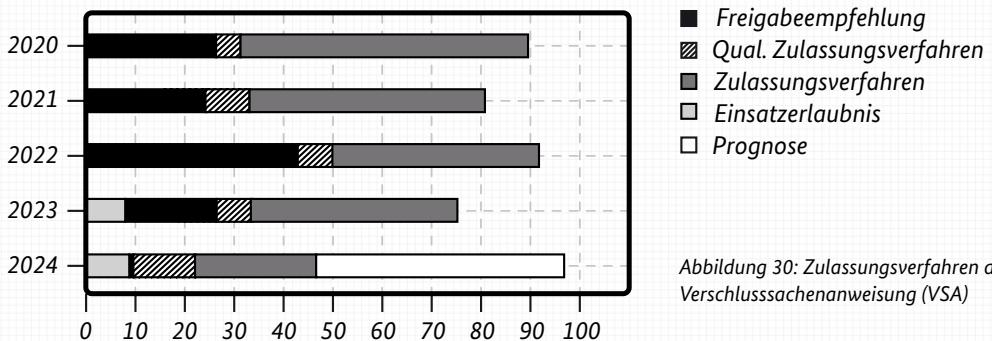
Derzeit haben sechs Hersteller eine Herstellerqualifizierung erfolgreich absolviert, drei weitere durchlaufen aktuell das initiale Qualifizierungsverfahren. Im Berichtszeitraum wurden 14 Verfahren zur kontinuierlichen Aufrechterhaltung der Herstellerqualifizierung durchgeführt.

Für die kontinuierliche Aufrechterhaltung der Herstellerqualifizierung wurden im Berichtszeitraum ein Prozessmodell und Evaluierungskriterien entwickelt. Das Prozessmodell unterstützt bei der transparenten und gleichen Durchführung verschiedener Re-Qualifizierungen. Die Evaluierungskriterien befinden sich aktuell in der Validierung. Sie helfen den Herstellern und dem BSI bei der Erstellung und Überprüfung der vom BSI geforderten Herstellernachweise.

### VS-Anforderungsprofile

Ein weiteres Instrument zur Erhöhung der Resilienz sind die Verschluss Sachen-Anforderungsprofile (VS-AP). Ein VS-Anforderungsprofil beschreibt IT-Sicherheitsanforderungen an zuzulassende IT-Sicherheitsprodukte. Sie werden in einem kooperativen Vorgehen gemeinsam von Bedarfsträgern, Betreibern, Herstellern und dem BSI erstellt. Auf diese Weise wird sichergestellt, dass Sicherheitsanforderungen in harmonisierter, bedarfsgerechter und effizienter Weise festgeschrieben werden. So kann schneller auf neue Trends und Veränderungen in der IT-Sicherheitslage reagiert werden, das heißt, die Resilienz nimmt zu. Somit sind die VS-Anforderungsprofile ein zentrales und steuerndes Element im BSI-Zulassungsschema.

## Zulassungsverfahren des BSI für VS-Produkte



- Freigabeempfehlung
- Qual. Zulassungsverfahren
- Zulassungsverfahren
- Einsatzerlaubnis
- Prognose

Abbildung 30: Zulassungsverfahren des BSI für VS-Produkte gemäß Verschlussachsenanweisung (VSA)

## Nationale und internationale Zulassungen des BSI für VS-Produkte

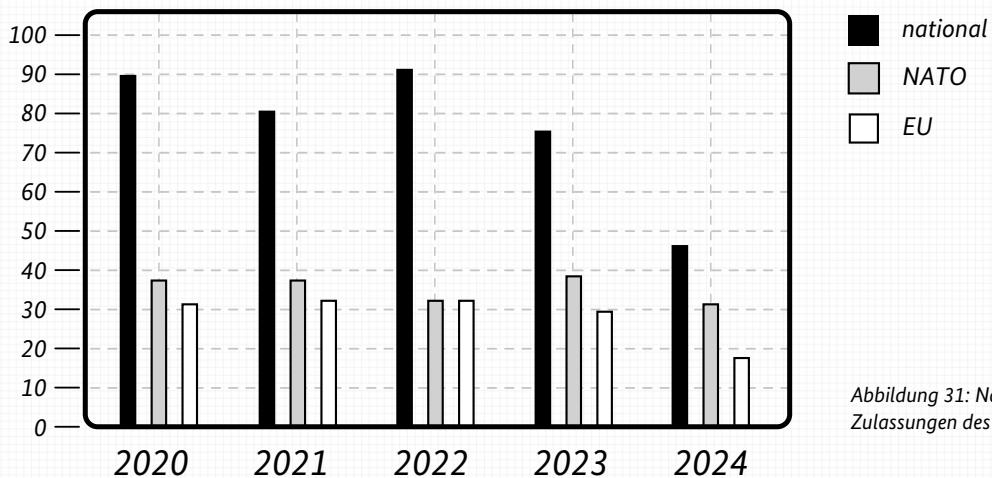


Abbildung 31: Nationale und internationale Zulassungen des BSI für VS-Produkte

## Gesamtzahlen der VS-Anforderungsprofile des BSI

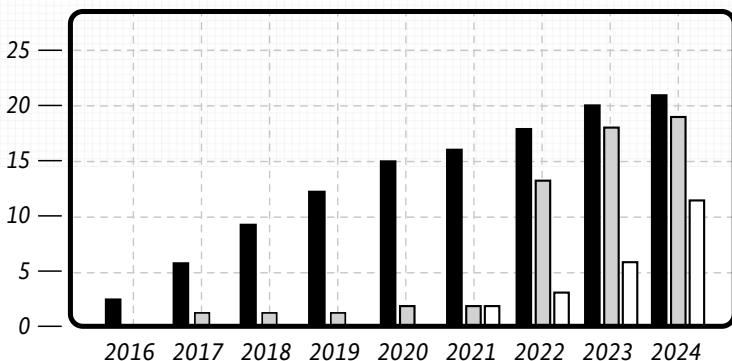


Abbildung 32: Gesamtzahlen der VS-Anforderungsprofile des BSI

- Gesamtanzahl veröffentlichter VS-AP
- Gesamtanzahl englischsprachiger Übersetzungen von VS-AP
- Gesamtanzahl überarbeiteter VS-AP

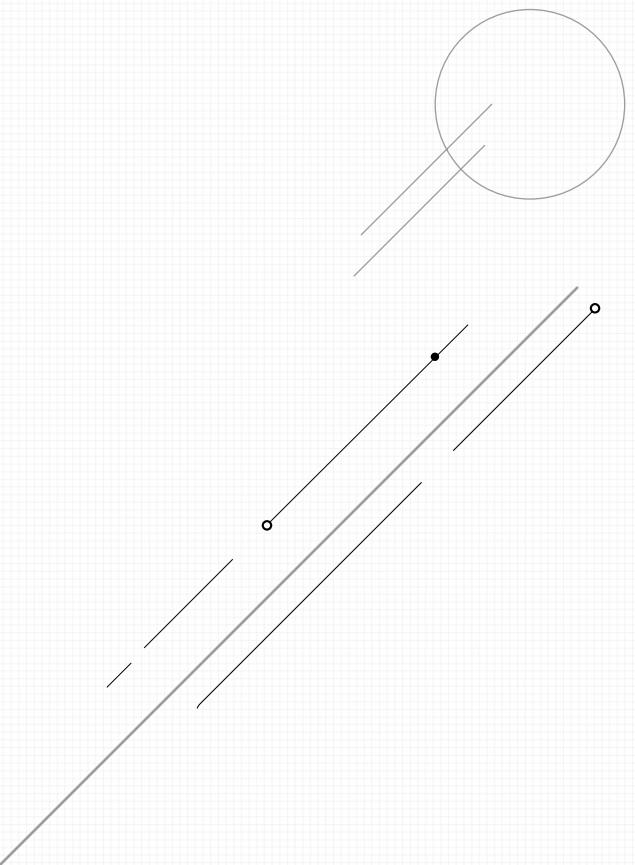
Mittlerweile gibt es 22 veröffentlichte VS-Anforderungsprofile zu verschiedenen Produkttypen und eine Vielzahl von IT-Sicherheitsprodukten, die konform zu diesen BSI-Anforderungen entwickelt und zugelassen wurden. Eine Auflistung und detaillierte Beschreibung vorhandener und in Arbeit befindlicher VS-Anforderungsprofile finden sich auf der BSI-Webseite.

**Weiterführende Informationen  
zu VS-Anforderungsprofilen:**



Im Berichtszeitraum wurden die VS-Anforderungsprofile „VS-Registratursystem“ und „Datendiode“ jeweils für die Geheimhaltungsgrade bis GEHEIM initial erstellt und veröffentlicht. Aktualisiert wurde das VS-Anforderungsprofil „Firewall“ für den Geheimhaltungsgrad bis VS-Nur für den Dienstgebrauch (VS-NfD). Für eine Mehrheit der veröffentlichten VS-Anforderungsprofile wurden darüber hinaus englische Übersetzungen erstellt. Da VS-Anforderungsprofile einen Standard darstellen, der fortlaufend an den aktuellen Stand der Technik angepasst wird, werden auch zukünftig kontinuierlich Überarbeitungen und Anpassungen an allen vorhandenen VS-Anforderungsprofilen vorgenommen.

Das Interesse von nationalen und internationalen Herstellern an der Erstellung und Überarbeitung von VS-Anforderungsprofilen ist in den letzten Jahren signifikant gewachsen. Das zeigt sich unter anderem an der gestiegenen Anzahl der beteiligten Stakeholder im Erstellungsprozess. Im Rahmen von durchgeföhrten Umfragen zeigt sich außerdem, dass Hersteller von IT-Sicherheitsprodukten und Bedarfsträger die VS-Anforderungsprofile positiv annehmen.



## 17 – Fazit

---

Die Lage der IT-Sicherheit in Deutschland war und ist besorgniserregend. Dabei unterliegt die Bedrohungslage weiterhin einer rasanten Entwicklung. Die digitale Angriffsfläche nimmt stetig zu, Schwachstellen bieten allzu oft gravierende Eingriffsmöglichkeiten und Angreifer finden immer schneller und geschickter Wege, diese auszunutzen. Doch niemand ist dem schutzlos ausgeliefert. Das Gebot der Stunde ist, Deutschlands Resilienz gegenüber Cyberbedrohungen und -vorfällen drastisch zu erhöhen. Das BSI hat im Rahmen der Cybernation Deutschland viele konkrete Schritte unternommen, um Unternehmen, Behörden und Bürgerinnen und Bürger besser auf IT-Sicherheitsvorfälle vorzubereiten und sie gegen Cyberangriffe zu schützen. Die Grundlage dafür ist die Lagebeobachtung in den Dimensionen Bedrohungen, Angriffsfläche, Gefährdungen, Schadwirkungen und Resilienz, wobei die Resilienz den vier anderen Dimensionen positiv entgegenwirkt.

### Die Dimensionen der Cybersicherheitslage

Bedrohungen gingen im vergangenen Berichtszeitraum von diversen Angreifergruppen aus. So zielten Cyberspionage-Angriffe von APT-Gruppen etwa auf Behörden insbesondere der auswärtigen Angelegenheiten, der Verteidigung sowie der öffentlichen Sicherheit und Ordnung sowie auf Unternehmen und Organisationen, die in diesen Bereichen tätig sind. Auch die arbeitsteilige cyberkriminelle Schattenwirtschaft hat sich weiter professionalisiert: Während einige Gruppierungen zunehmend mit erbeuteten Zugangsdaten handelten (Access Broker), nutzten andere Cybercrime-Gruppen Zero-Day-Schwachstellen zum Datendiebstahl. Immer häufiger wurden diese Daten zu Erpressungszwecken genutzt, ohne zuvor Ransomware, sogenannte Verschlüsselungstrojaner, einzusetzen. Auch menschliches Versagen kann zur Bedrohung werden, wie der CrowdStrike-Vorfall im Juli 2024 gezeigt hat, der durch eine versehentlich fehlerhafte Software ausgelöst wurde.

Die Angriffsflächen vergrößerten sich weiterhin im Berichtszeitraum, weil mit zunehmender Digitalisierung zugleich die Zahl komplexer und verwundbarer Systeme steigt. Neben dem Zuwachs an täglich bekannt gewordenen Schwachstellen wurde insbesondere eine Vielzahl kritischer Schwachstellen in Perimetersystemen, wie Firewalls und VPNs, bekannt. Gleichzeitig nahmen Angriffe auf Perimetersysteme weiterhin deutlich zu. Auffällig verwundbar waren zudem Android-Systeme – insbeson-

dere dann, wenn sie mit veralteten Software-Versionen betrieben wurden, für die zum Teil gar keine Updates mehr verfügbar sind.

Die Gefährdungen im Berichtszeitraum umfassten unterschiedlichste Angriffsarten. Die besonders im ersten Halbjahr 2024 immens gestiegene Zahl der hochvolumigen DDoS-Angriffe war alarmierend und die Schutzmaßnahmen sollten angepasst werden. Ransomware-Angriffe richteten sich massenhaft gegen leichte, weil häufig noch unzureichend geschützte Ziele wie kleine und mittlere Unternehmen und Kommunen. Allein vom Angriff auf einen kommunalen IT-Dienstleister Ende Oktober 2023 waren 72 kommunale Kunden mit rund 20.000 kommunalen Arbeitsplätzen betroffen. Auch Public-Cloud-Infrastrukturen wurden angegriffen. Die mutmaßlich chinesische und staatlich gelenkte Angreifergruppe Storm-0558 kompromittierte die Verschlüsselung von E-Mail-Accounts. Dies bedeutete eine potenzielle Gefährdung von Millionen Identitätsdaten.

Die Schadwirkungen im Berichtszeitraum waren beträchtlich: Hierzu zählen zum Beispiel die teils monatelangen Ausfallzeiten bei Kommunen durch Ransomware-Angriffe. Ebenfalls durch Ransomware-Angriffe wurden weltweit 1,1 Milliarden US-Dollar Lösegeld erbeutet, wobei die Dunkelziffer vermutlich sehr viel höher ist. Bemerkenswert ist, dass für erbeutete exfiltrierte Daten im Schnitt fast dreimal so viel gezahlt wurde wie für erbeutete verschlüsselte Daten. Auch die Zahl der mutmaßlichen Opfer von Datenleaks ist im Berichtszeitraum weiter gestiegen. Im zweiten Halbjahr 2023 wies die entsprechende Messzahl kurzzeitig sogar rund die doppelte Menge mutmaßlicher Leak-Opfer im Vergleich zum Referenzjahr 2021 aus.

## Die entscheidende Dimension: Resilienz

Die Auswirkungen in den vier Dimensionen Bedrohungen, Angriffsfläche, Gefährdungen und Schadwirkung sind gravierend, aber Deutschland ist alldem nicht schutzlos ausgeliefert. Das BSI hat im Berichtszeitraum mit der breiten Expertise seiner Mitarbeitenden maßgeblich dazu beigetragen, Bedrohungen frühzeitig zu entdecken, zu warnen und Hilfestellungen und Lösungen zur Verfügung zu stellen. Mithilfe seiner Sensorik konnte das BSI beispielsweise Botnetze durch Sinkholing aufspüren und dabei unter anderem zur Strafverfolgung beitragen. Weltweit konnten die zuständigen Behörden zahlreiche Takedowns gegen Botnetze cyberkrimineller Angreifergruppen durchführen. Dadurch konnte das Aufkommen neuer Malware-Varianten im Vergleich zu den starken Schwankungen nach oben in früheren Jahren auf einem stabilen Niveau gehalten werden. Um langen Ausfallzeiten nach erfolgten Cyberangriffen vorzubeugen, verbessern Institutionen ihre Reaktionsfähigkeit durch das Aufsetzen von Business-Continuity-Management-Systemen, kurz BCM-Systemen, die vom BSI im Standard 200-4 umfassend beschrieben und von KRITIS-Betreibern explizit eingefordert werden.

### Resilienz ist Gemeinschaftsaufgabe

Deutschland ist auf dem Weg zu einer resilienten Cybertechnik schon ein gutes Stück weit vorangekommen. Resilienz lässt sich jedoch nicht im Sprint umsetzen: Das BSI und alle weiteren Akteure benötigen hierfür Langstrecken-Qualitäten. Alle Beteiligten sind gefordert, ihren Beitrag zur Stärkung der Resilienz gegen Cyberkriminalität und IT-Sicherheitsvorfälle zu leisten. Aus Sicht des BSI ist es unerlässlich, dass Hersteller sichere Produkte bereitstellen, die nach den Grundsätzen von Security by Design und Security by Default entwickelt und gepflegt werden. Betreiber sind gefordert, die Grundsätze der Cybersicherheit umzusetzen, bestenfalls in einem strukturierten Informationssicherheitsmanagementsystem (ISMS). Das BSI und andere staatliche Stellen werden weiterhin unterstützen und steuern, etwa durch eine kooperative und wirksame Umsetzung der NIS-2-Regulierung. Verbraucherinnen und Verbraucher sollten Kompetenzen zu Cybersicherheit aufbauen, beispielsweise indem sie sich über mögliche Angriffswege oder Betrugsmaschen auf dem Laufenden halten.

## Das BSI als Partner und Helfer für mehr Cybersicherheit

Ziel aller Bemühungen um Resilienz ist auch die Reduzierung der Schadwirkungen. Das BSI trägt bereits heute einen erheblichen Teil dazu bei. So wurde zum Beispiel das BSI-Lagezentrum ausgebaut und modernisiert, um noch besser 24/7 und 365 Tage im Jahr die IT-Sicherheitslage in Deutschland beobachten und in besonders schweren Fällen zum Nationalen IT-Krisenreaktionszentrum aufzutreten zu können.

Die Zahl der Kooperationsvereinbarungen des BSI mit einzelnen Ländern für eine engere Zusammenarbeit konnte im Berichtszeitraum auf sieben erhöht werden. Darüber hinaus kooperiert das BSI mit anderen deutschen Behörden im Digital Cluster Bonn, um im Hinblick auf die aktuellen EU-Richtlinien gemeinsam und abgestimmt zu agieren und Bürokratieaufwände zu reduzieren. Zur Verbesserung der deutschen Kommunikationsinfrastruktur wurde das 5G/6G-Security-Lab am BSI-Standort Freital eingerichtet. Im Bereich Cloud hat das BSI die vielbeachtete BSI-Cloud-Strategie entwickelt, die technologisch führende und unmittelbar einsatzfähige Lösungsbeiträge für das gesamte Cloud-Betriebsspektrum liefert. Nicht zuletzt sind in diesem Jahr die Fußball-Europameisterschaft und die Europawahlen in Deutschland ohne nennenswerte Cybersecurityvorfälle abgelaufen, weil Deutschland – auch mit Unterstützung des BSI – gut vorbereitet war.

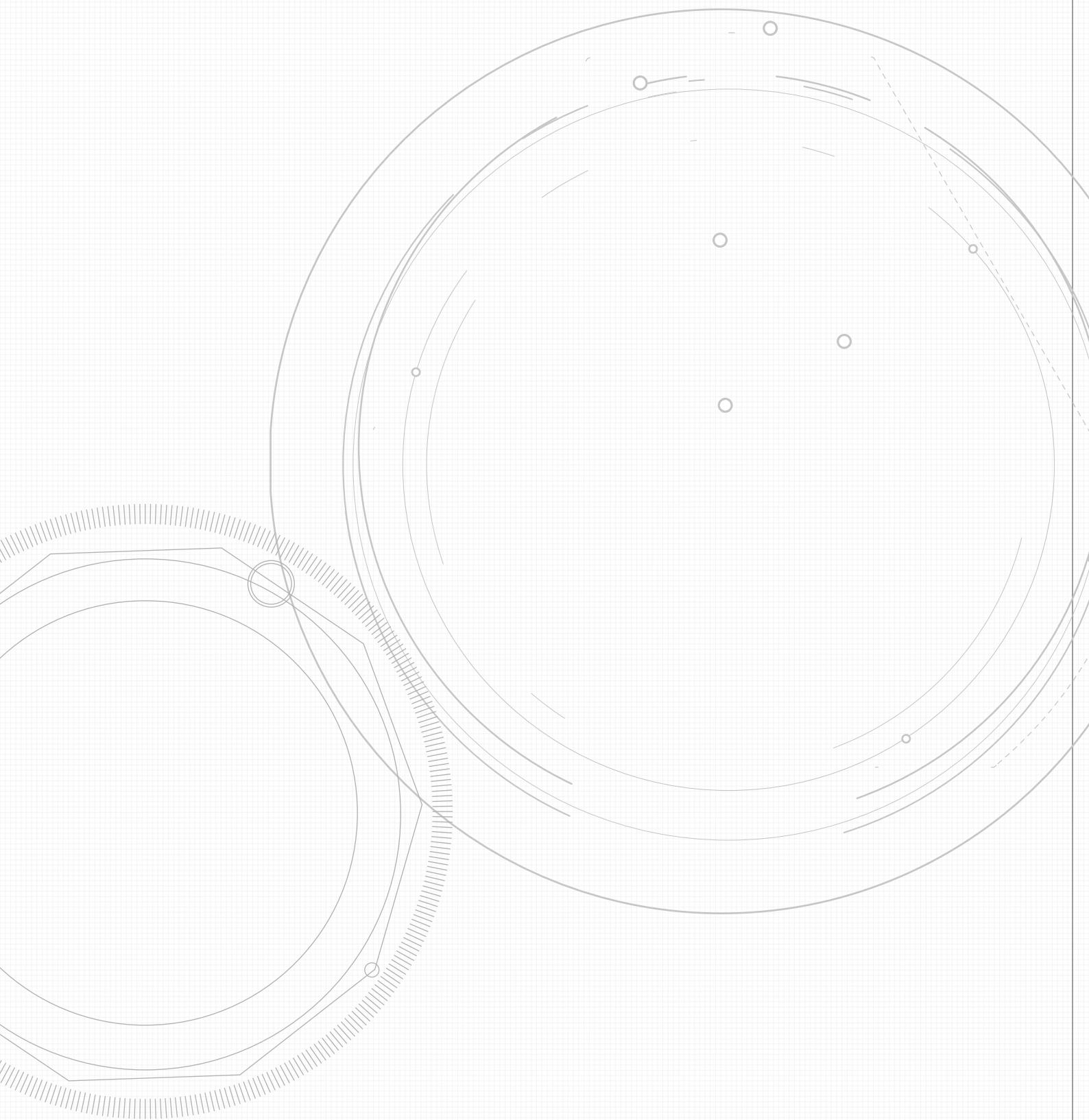
Das Engagement des BSI zur Erhöhung der Resilienz betrifft auch den europäischen und internationalen Cyberraum. Entsprechend dem deutschen Umsetzungsgesetz zur EU-NIS-2-Richtlinie führt das BSI als die deutsche Instanz für Cybersicherheit Meldepflichten für viele neue Unternehmen ein, was auch zu einem umfassenderen Lagebild beitragen wird. Zudem traten mit dem Cyber Resilience Act (CRA) und dem Cybersecurity Act (CSA) zwei neue EU-Richtlinien in Kraft. Im Rahmen des CRA bereitet das BSI sich darauf vor, eine Marktüberwachungsfunktion einzunehmen. Unter dem CSA ist unter Mitwirkung des BSI das erste Cyber Security Certification Scheme EUCC zur Sicherheitszertifizierung von IT-Produkten in Kraft getreten.

## Vision für die Cybersicherheit

Die Aufgabe, die Resilienz für die Cybernation Deutschland mit ihren zahlreichen Stakeholdern zu erhöhen, ist anspruchsvoll. Neben dem Cyber Resilience Act oder NIS-2 werden weitere regulatorische Neuerungen die Cybersicherheit in Deutschland und Europa erhöhen. Gleichzeitig müssen die damit verbundenen Anforderungen aber auch umgesetzt werden. Dabei sind insbesondere Unternehmen und Institutionen gefordert. Auch für die Aufsichtsbehörden wie das BSI ändern sich zahlreiche Rahmenbedingungen. So muss nicht nur die Marktüberwachung für das CE-Kennzeichen nach Cyber Resilience Act ausgebaut werden, auch zehntausende Unternehmen müssen im Rahmen der NIS-2-Richtlinie betreut werden. Diese Herausforderungen können nur gemeistert werden, wenn Staat, Wirtschaft, Wissenschaft und Gesellschaft eng kooperieren. Das BSI wird dabei ganz im Sinne der Cybernation Deutschland mit allen Akteuren an einem Strang ziehen, um das gemeinsame Ziel eines sicheren digitalen Alltags zu erreichen.

Die Folgen der weltweiten IT-Störungen im Juli 2024 haben eindrucksvoll gezeigt, wie abhängig unsere digitalisierte Welt von funktionierenden IT-Systemen ist. Dieser Vorfall war ein ungewollter Beleg dafür, dass aufgrund der bestehenden Vernetzungen und damit einhergehenden Abhängigkeiten nur das intensive Zusammenspiel aller Beteiligten zielführend ist. In kürzester Zeit konnte die Ursache ausfindig gemacht, eine Problemlösung gefunden und Betroffene und Öffentlichkeit informiert werden. Nutzer, Hersteller, Betreiber, Verbände und BSI agierten Hand in Hand, um diese Krise schnellstmöglich zu bewältigen. Damit solche Krisen künftig seltener auftreten, ist Prävention von entscheidender Bedeutung. Daher arbeitet das BSI auch nach der akuten Krise mit allen Akteuren und mit Beteiligung der Wissenschaft eng zusammen, um die richtigen Maßnahmen zu entwickeln und umzusetzen.

Das Beispiel CrowdStrike zeigt: Das große Ziel der Cybernation Deutschland kann nur mit vereinten Kräften realisiert werden. Die exzellente Technologiekompetenz in Deutschland trägt zur Entwicklung von Lösungen bei. Mit Wirtschaft, Wissenschaft und Politik werden diese Lösungen in einem lebendigen Ökosystem für Cybersicherheitsprodukte und -services zur Umsetzung gebracht. Zusammen steigern wir so die Sicherheit und Geschwindigkeit bei der Digitalisierung. Jetzt und in Zukunft muss das Motto lauten: „Kooperation gewinnt“.



# 18 – Glossar

---

## **Access Broker**

Als Access Broker werden Cyberkriminelle bezeichnet, die sich über verschiedenste Wege Zugang zu einem Opfernetzwerk verschaffen und diesen Zugang regelmäßig an andere Cyberkriminelle oder interessierte Parteien veräußern.

## **Advanced Persistent Threats**

Bei Advanced Persistent Threats (APT) handelt es sich um zielgerichtete Cyberangriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer persistenten (dauerhaften) Zugriff auf ein Netzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten auf Seiten der Angreifer aus und sind in der Regel schwierig zu detektieren.

## **Advisories / Security Advisories**

Empfehlungen der Hersteller an IT-Sicherheitsverantwortliche in Unternehmen und anderen Organisationen zum Umgang mit aufgefundenen Schwachstellen.

## **Affiliates**

Bei Cybercrime-as-a-Service wird der Cyberkriminelle, der den Service in Anspruch nimmt, in der Regel als Affiliate bezeichnet. Der Begriff leitet sich aus dem Affiliate-Marketing ab, bei dem ein kommerzieller Anbieter seinen Vertriebspartnern (Affiliates) Werbematerial zur Verfügung stellt und eine Provision anbietet. Im Kontext des Cybercrime wird statt Werbematerial beispielsweise eine Ransomware zur Verfügung gestellt und dem Affiliate eine Beteiligung am Lösegeld versprochen.

## **Angriffsvektor**

Als Angriffsvektor wird die Kombination von Angriffs-weg und -technik bezeichnet, mit der sich ein Angreifer Zugang zu IT-Systemen verschafft.

## **Authentifizierung**

Die Authentifizierung bezeichnet den Vorgang, die Identität einer Person oder eines Rechnersystems anhand eines bestimmten Merkmals zu überprüfen. Dies kann unter anderem durch Passworteingabe, Chipkarte oder Biometrie erfolgen.

## **Backdoor**

Eine Backdoor ist ein üblicherweise durch Viren, Würmer oder Trojanische Pferde installiertes Programm, das Dritten einen unbefugten Zugang (Hintertür) zum Computer verschafft, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen.

## **Backup**

Unter Backup versteht man das Kopieren von Dateien oder Datenbanken auf physischen oder virtuellen Systemen an einen sekundären Speicherort, um diese im Falle eines Geräteausfalls oder einer Katastrophe für eine Wiederherstellung zu nutzen und bis dahin sicher vorzuhalten.

## **Bitcoin**

Bitcoin (BTC) ist eine digitale Währung, sie wird auch Kryptowährung genannt. Durch Zahlungen zwischen pseudonymen Adressen wird die Identifizierung der Handelspartner deutlich erschwert.

## **Blockchain**

Blockchain beschreibt eine verteilte, synchronisierte, dezentrale und konsensuale Datenhaltung in einem Peer-to-Peer-Netzwerk. Dabei wird redundant in allen Netzwerkknoten eine hashverkettete Liste von Datenblöcken geführt, die mithilfe eines Konsensverfahrens aktualisiert wird. Blockchain ist die technologische Grundlage für Kryptowährungen wie Bitcoin.

## **Bot/Botnetz**

Als Botnetz wird ein Verbund von Rechnern (Systemen) bezeichnet, die von einem fernsteuerbaren Schadprogramm (Bot) befallen sind. Die betroffenen Systeme werden vom Botnetz-Betreiber mittels eines Command-and-Control-Servers (C&C-Server) kontrolliert und gesteuert.

## **Brute Forcing**

Angriffsmethode nach dem Versuch-Irrtum-Prinzip. Angreifer probieren automatisch viele Zeichenkombinationen aus, um zum Beispiel Passwörter zu knacken und sich Zugang zu passwortgeschützten Systemen zu verschaffen.

## **Bug Bounty**

Monetäre Belohnungen (Bounty) für das Finden von Schwachstellen (Bugs). Hersteller von Softwareprodukten verwenden legitime Bug-Bounty-Programme, um Sicherheitsforschende für das Finden und Melden einer Schwachstelle in ihrem Produkt zu belohnen.

## **CEO-Fraud**

Als CEO-Fraud werden gezielte Social-Engineering-Angriffe auf Mitarbeitende von Unternehmen bezeichnet. Der Angreifer nutzt dabei zuvor erbeutete Identitätsdaten (zum Beispiel Telefonnummern, Passwörter, E-Mail-Adressen etc.), um sich als Vorstandsvorsitzender (CEO), Geschäftsführung o. Ä. auszugeben und Mitarbeitende zur Auszahlung hoher Geldsummen zu veranlassen.

## **CERT / Computer Emergency Response Team**

Computer-Notfallteam, das aus IT-Spezialisten besteht. In vielen Unternehmen und Institutionen sind mittlerweile CERTs etabliert, die sich um die Abwehr von Cyberangriffen, die Reaktion auf IT-Sicherheitsvorfälle sowie um die Umsetzung präventiver Maßnahmen kümmern.

## **CERT-Bund**

Das CERT-Bund (Computer Emergency Response Team der Bundesverwaltung) ist im BSI angesiedelt und fungiert als zentrale Anlaufstelle für Bundesbehörden zu präventiven und reaktiven Maßnahmen bei sicherheitsrelevanten Vorfällen in Computersystemen.

## **Cloud / Cloud Computing**

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die im Rahmen von Cloud Computing angebotenen Dienstleistungen umfassen das komplette Spektrum der Informati-onstechnik und beinhalten unter anderem Infrastrukturen (Rechenleistung, Speicherplatz), Plattformen und Software.

## **Command-and-Control-Server (C&C-Server)**

Serverinfrastruktur, mit der Angreifer die in ein Botnetz integrierten infizierten Computersysteme (Bots) steuern. Bots (infizierte Systeme) melden sich in der Regel nach der Infektion bei dem C&C-Server des Angreifers, um dessen Befehle entgegenzunehmen.

## **Confidential Computing**

Confidential Computing verwendet hardwarebasierte, attestierte Trusted Execution Environments (TEE), um die Vertraulichkeit und Integrität von Daten während deren Verarbeitung („in use“) zu schützen. Ein TEE stellt einen isolierten Teil innerhalb eines Systems dar, der eine besonders geschützte Laufzeitumgebung bereitstellt. Das TEE kann bspw. Bestandteil des Hauptprozessors (CPU) oder Teil des Ein-Chip-Systems (SoC) eines Smartphones sein. Lediglich autorisierten Stellen ist es möglich, Anwendungen in das TEE einzubringen oder zu verändern. Die Attestierung des TEE und der in der TEE laufenden Anwendung dient der Validierung der Vertrauenswürdigkeit der Verarbeitung.

## **CVSS-Score**

Industriestandard, mit dem die Kritikalität von Schwachstellen international vergleichbar bewertet wird.

## **Cybercrime-as-a-Service (CCaaS)**

Cybercrime-as-a-Service (CCaaS, Cybercrime als Dienstleistung) beschreibt einen Phänomenbereich des Cybercrime, bei dem Straftaten von Cyberkriminellen auftragsorientiert begangen beziehungsweise dienstleistungsorientiert ermöglicht werden. So wird beispielsweise bei dem CCaaS untergeordneten Malware-as-a-Service (MaaS) einem Cyberkriminellen von einem Außenstehenden oder einer darauf spezialisierten Angreifergruppe die Malware für die Begehung einer Straftat gegen Entgelt zur Verfügung gestellt

und gegebenenfalls wird der Cyberkriminelle auch mit Updates und weiteren ähnlichen Services versorgt, ganz so wie bei der legalen Softwareindustrie. Eine Art des MaaS ist Ransomware-as-a-Service (RaaS), bei dem oft die Malware für die Verschlüsselung eines infizierten Systems, Aktualisierungen dieser Malware, die Abwicklung der Lösegeldverhandlungen und -zahlungen und weitere Erpressungsmethoden gegen Entgelt zur Verfügung gestellt werden. Die mit CCaaS einhergehende Zergliederung eines Cyberangriffs in einzelne Services ermöglicht auch wenig IT-affinen Angreifern technisch anspruchsvolle Cyberangriffe.

### **Deepfake**

Der Begriff „Deepfake“ ist eine umgangssprachliche Bezeichnung für Methoden, die dazu verwendet werden können, Identitäten in medialen Inhalten mithilfe von Methoden aus dem Bereich der Künstlichen Intelligenz gezielt zu manipulieren. Ein Beispiel hierfür sind Verfahren, die das in einem Video befindliche Gesicht einer Person mit dem Gesicht einer anderen Person tauschen, dabei jedoch die Gesichtsbewegungen unverändert lassen.

### **Defacement**

Das Wort „Defacement“ stammt vom Englischen „to deface“, was „entstellen“ oder „verunstalten“ bedeutet. Bei einem Defacement wird eine Webseite durch einen Angreifer unter Ausnutzung von Schwachstellen oder ausgespähten beziehungsweise erratenen Zugangsdaten mutwillig verändert.

### **DoS-/DDoS-Angriffe**

Denial-of-Service-(DoS-)Angriffe richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten DoS- oder DDoS-(Distributed Denial of Service-)Angriff. DDoS-Angriffe erfolgen häufig durch eine sehr große Anzahl von Computern oder Servern.

### **Double Extortion**

Angreifer versuchen nicht nur, Lösegeld für verschlüsselte Daten zu erpressen, sondern auch Schweigegeld für exfiltrierte Daten.

### **Downgrade-Attacke**

Eine Downgrade-Attacke im Mobilfunk bezeichnet einen Angriff, bei dem der Angreifer versucht, die Kommunikation zwischen einem mobilen Endgerät (zum Beispiel einem Smartphone) und dem Mobilfunknetzwerk auf eine weniger sichere Protokollversion (zum Beispiel von 5G-Verbindung auf 2G-Verbindung) herabzusetzen, um deren Sicherheitslücken auszunutzen.

### **Drive-by-Download / Drive-by-Exploits**

Drive-by-Exploits bezeichnen die automatisierte Ausnutzung von Schwachstellen auf einem PC. Dabei werden beim Betrachten einer Webseite ohne weitere Nutzerinteraktion Schwachstellen im Webbrowser, in Zusatzprogrammen des Browsers (Plug-ins) oder im Betriebssystem ausgenutzt, um Schadsoftware unbemerkt auf dem PC zu installieren.

### **eUICC**

Die Embedded Universal Integrated Circuit Card (eingebettete universelle integrierte Schaltkreiskarte, eUICC) ist eine SIM-Karte mit einem überschreibbaren Profil, das den Wechsel des Mobilfunkbetreibers ermöglicht, ohne die SIM-Karte physisch auszutauschen. Dieses SIM-Profil kann aus der Ferne per Luftschnittstelle (Over the Air, OTA) überschrieben werden. Damit ein Wechsel von SIM-Profilen möglich ist, benötigt eine eUICC einen Mindestspeicher von 512 KB.

### **Exit-Scam**

Der Begriff Exit-Scam (dt. Ausstiegsbetrug) beschreibt eine Form von Betrug, bei dem eine Person, die Transaktionen unter anderem als Krypto-Währung für Dienstleistungen vereinbart, ohne die vereinbarte Gegenleistung zu erbringen, mit den Einnahmen untertaucht.

### **Exploit**

Als Exploit bezeichnet man eine Methode oder einen Programmcode, mit dem über eine Schwachstelle in Hard- oder Softwarekomponenten nicht vorgesehene Befehle oder Funktionen ausgeführt werden können. Je nach Art der Schwachstelle kann mithilfe eines Exploits zum Beispiel ein Programm zum Absturz gebracht, Benutzerrechte ausgeweitet oder beliebiger Programmcode ausgeführt werden.

## Hacktivismus

Hacktivismus setzt sich aus den Begriffen Hacking und Aktivismus zusammen. Dabei handelt es sich um ideologisch motivierte Hacking-Aktivitäten unter anderem zur Verbreitung ideologischer, politischer und/oder sozialer Statements im digitalen Raum. Die bevorzugten strafrechtlich relevanten Vorgehensweisen der Hacktivisten, um im digitalen Raum Protest und/oder Propaganda auszuüben, sind WebDefacement, DDoS-Angriffe sowie das Ausspähen und Manipulieren von Daten.

## Hashwert

Ein Hashwert ist eine aus der Anwendung einer bestimmten Hashfunktion resultierende Zeichenkette aus Ziffern und Buchstaben. Der Hashwert besitzt eine definierte Länge und ermöglicht es daher, große Datenmengen (zum Beispiel ein Schadprogramm) exakt in vergleichsweise wenigen Zeichen abzubilden. Bei der Hashfunktion handelt es sich um eine mathematische Funktion zur Umrechnung von Daten. Eine anschließende Rückrechnung des Hashwertes in die ursprünglichen Daten ist praktisch kaum beziehungsweise nur unter extrem hohem Rechenaufwand möglich.

## Hybride Bedrohungen

Hybride Bedrohungen werden charakterisiert als koordinierte Handlungen staatlicher Akteure zur Durchsetzung eigener Ziele zum (systemrelevanten) Nachteil eines anderen Staates, die außerhalb des Rahmens einer konventionellen militärischen Auseinandersetzung bleiben. In diesem Kontext können zum Beispiel auch Cyberangriffe oder Desinformationskampagnen eingesetzt werden.

## Information Stealer

Information Stealer sind Schadprogramme, die es Cyberkriminellen ermöglichen, auf infizierten Geräten an unterschiedliche Arten persönlicher Daten, wie beispielsweise Login-Daten für verschiedene Onlinedienste, zu gelangen, ohne dass die Betroffenen dies bemerken.

## Internet der Dinge / Internet of Things / IoT

Unter Internet der Dinge oder Internet of Things (IoT) versteht man informations- und sensortechnisch aufgerüstete Gegenstände, die miteinander vernetzt sind und aus der physischen und der virtuellen Welt Daten erfassen, verarbeiten und speichern.

## ITSEF

Eine Information Technology Security Evaluation Facility (ITSEF) ist gemäß Durchführungsverordnung 2024/482 eine Einrichtung zur Evaluierung der IT-Sicherheit, die eine Konformitätsbewertungsstelle im Sinne des Art. 2 Nr. 13 der Verordnung (EG) Nr. 765/2008 ist und Evaluierungstätigkeiten durchführt.

## IT-Sicherheitsgesetz 2.0

Das „Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (IT-SiG 2.0) ist am 28. Mai 2021 in Kraft getreten. Das IT-SiG 2.0 ist die Weiterentwicklung des ersten IT-Sicherheitsgesetzes aus 2015.

## Krypto-Wallet

Eine Krypto-Wallet ist eine digitale Brieftasche für Kryptowährungen, die als Ablageort für private und öffentliche Schlüssel dient, mit denen Transaktionen mit der jeweiligen Kryptowährung durchgeführt werden.

## Legitime Programme

Programme, die unschädliche, erwünschte Operationen ausführen.

## MaaS

Malware-as-a-Service (siehe auch CCaaS).

## Maliziös

In der IT-Sicherheit werden Programme oder Webseiten, die schädliche Operationen auf einem Computersystem ausführen können, als maliziös (boshaft, schädlich) bezeichnet.

## Malware

Die Begriffe Schadfunktion, Schadprogramm, Schadsoftware und Malware werden häufig synonym benutzt. Malware ist ein Kunstwort, abgeleitet aus Malicious Software, und bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Beispiele sind Computerviren, Würmer und Trojanische Pferde. Schadsoftware ist üblicherweise für eine bestimmte Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben.

### **Man-in-the-Middle-Angriff**

Bei einem Man-in-the-Middle-Angriff schleust sich der Angreifer in eine private Kommunikation zwischen zwei oder mehreren Kommunikationspartnern ein, um Informationen auszuspionieren oder die Verbindung zu manipulieren.

### **Mark-of-the-Web/MOTW**

Ein MOTW kennzeichnet Download-Dateien, wenn diese aus einer wahrscheinlich nicht vertrauenswürdigen Quelle stammen. Öffnet eine Nutzerin oder ein Nutzer eine so markierte Datei, wird er entsprechend gewarnt.

### **Monero**

Monero ist eine digitale Währung, sie wird auch Kryptowährung genannt. Durch Zahlungen zwischen pseudonymen Adressen wird die Identifizierung der Handelspartner deutlich erschwert.

### **NCCA**

Das BSI ist die nationale Behörde für Cybersicherheitszertifizierung (engl. National Cybersecurity Certification Authority, kurz NCCA) im Sinne des Artikels 58 Abs. 1 der Verordnung (EU) 2019/881 (Cybersecurity Act, kurz: CSA) in Verbindung mit § 9a BSIG. Unter Beachtung des Artikels 58 Abs. 4 CSA führt das BSI als NCCA die Aufsichtsführung und Zertifizierung streng getrennt und unabhängig voneinander durch.

### **NESAS**

Zertifizierungsprogramm für 5G-Mobilfunkausrüstung (Network Equipment Security Assurance Scheme).

### **NESAS CCS-GI**

Das nationale Zertifizierungsprogramm für 5G-Mobilfunkausrüstung (NESAS Cybersecurity Certification Scheme – German Implementation).

### **Network Attached Storage (NAS)**

Ein mit einem Netzwerk verbundenes Speichergerät, das autorisierten Netzwerknutzerinnen und -nutzern das Speichern und Abrufen von Daten an einem zentralen Ort ermöglicht.

### **Password-Spraying**

Angriffsmethode, bei der der Angreifer beliebte oder typische Passwörter (zum Beispiel Test1234) verwendet, um auf zahlreiche Konten gleichzeitig Zugriff zu erlangen.

### **Patch/Patchmanagement**

Ein Patch (Flicken) ist ein Softwarepaket, mit dem Softwarehersteller Schwachstellen in ihren Programmen schließen oder andere Verbesserungen integrieren. Das Einspielen dieser Updates erleichtern viele Programme durch automatische Update-Funktionen. Als Patchmanagement bezeichnet man Prozesse und Verfahren, die helfen, verfügbare Patches für die IT-Umgebung möglichst rasch erhalten, verwalten und einspielen zu können.

### **Peer Review**

Im Rahmen von Peer Reviews werden von einer ausgewählten Gruppe von Fachleuten verschiedener EU-Staaten neue eIDs anderer EU-Staaten auf ihre Konformität zur eIDAS-Verordnung geprüft.

### **Phishing**

Das Wort setzt sich aus den englischen Wörtern password und fishing zusammen, zu Deutsch: nach Passwörtern angeln. Der Angreifer versucht dabei, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten einer Internetnutzerin oder eines Internetnutzers zu gelangen und diese für seine Zwecke, meist zulasten des Opfers, zu missbrauchen.

### **Plug-in**

Ein Plug-in ist eine Zusatzsoftware oder ein Softwaremodul, das in ein Computerprogramm eingebunden werden kann, um dessen Funktionalität zu erweitern.

### **Proliferation**

Der Begriff stammt ursprünglich aus der militärischen Verteidigung und bezeichnet die Weitergabe von Massenvernichtungswaffen einschließlich des für sie erforderlichen technischen Know-hows sowie des zu ihrer Herstellung benötigten Materials. In der IT-Sicherheit wird der Begriff entsprechend für die Weitergabe von Cyberwaffen (Software und Methoden) unter Angreifern verwendet. Durch Proliferation können sich Angriffsmittel und -wege sehr schnell unter verschiedenen Angreifergruppierungen verbreiten, ohne dass diese jeweils spezifische technische Kompetenzen aufbauen müssen.

## **Proof of Concept**

Nachweis, dass sich ein theoretisch erarbeitetes Vorhaben auch in der Praxis umsetzen lässt.

## **Provider**

Dienstanbieter mit verschiedenen Schwerpunkten, zum Beispiel Netzwerk-Provider, der als Mobilfunk-Provider, Internet-Service-Provider oder Carrier die Infrastrukturen für den Daten- und Sprachtransport bereitstellt, oder Service-Provider, der über die Netzwerkbereitstellung hinausgehende Dienstleistungen erbringt, beispielsweise den Netzbetrieb einer Organisation oder die Bereitstellung von sozialen Medien.

## **Public-Key-Kryptografie**

Bei der Public-Key-Kryptografie, das heißt der asymmetrischen Verschlüsselung, gibt es immer zwei sich ergänzende Schlüssel. Ein Schlüssel, der Public Key, dient zur Verschlüsselung einer Nachricht, ein anderer, der Private Key, dient zum Entschlüsseln. Beide Schlüssel zusammen bilden ein Schlüsselpaar.

## **Quellcode**

Der Quellcode eines Computerprogramms ist die in einer Programmiersprache verfasste, für Menschen lesbare Beschreibung des Ablaufs des Programms. Der Quellcode wird durch ein Programm in eine Abfolge von Anweisungen übersetzt, die der Computer ausführen kann.

## **Ransomware**

Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (engl. ransom) wieder freigeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.

## **RaaS**

Ransomware-as-a-Service (siehe auch CCaaS).

## **Resilienz**

Der Begriff bezeichnet im vorliegenden Zusammenhang die Widerstandsfähigkeit von IT-Systemen gegen Sicherheitsvorfälle oder Angriffe. Die Resilienz von Systemen ergibt sich aus einem komplexen Zusammenspiel von organisatorischen und technischen Präventivmaßnahmen wie zum Beispiel Fachpersonal, IT-Sicherheitsbudget, verfügbaren technischen Infrastrukturen oder Ähnlichem.

## **RSA**

Der Begriff bezeichnet ein Verfahren der Public-Key-Kryptografie, das für Signaturen und Verschlüsselung eingesetzt wird und nach den Entwicklern Rivest, Shamir und Adleman benannt ist. Ein Teil des öffentlichen Schlüssels von RSA besteht aus dem RSA-Modul  $n$ , einer natürlichen Zahl, die das Produkt zweier geheimer Primzahlen  $p$  und  $q$  ist. Die Sicherheit von RSA beruht insbesondere auf der Schwierigkeit, das RSA-Modul  $n$  zu faktorisieren, das heißt nur aus Kenntnis von  $n$  die beiden Primfaktoren  $p$  und  $q$  zu berechnen.

## **Scam-Mail**

Betrugsmail: Kategorie von Spam-Mails, mit denen Angreifer vorgeben, zum Beispiel Spendengelder zu sammeln.

## **Schnellmeldungen**

Schnellmeldungen sind beispielsweise für Bundestagswahlen in § 71 BWO geregelt: Die Wahlergebnisse jedes Wahlbezirks werden telefonisch, elektronisch oder auf andere Weise vom Wahlvorstand über Gemeinde, Kreiswahlleitung, Landeswahlleitung bis zur Bundeswahlleitung aggregiert und weitergeleitet. Liegen die Ergebnisse aller Wahlbezirke vor, wird das vorläufige amtliche Endergebnis veröffentlicht. Dies ist typischerweise bereits am Wahlabend der Fall.

## **Script-Kiddies**

Angreifer, die trotz mangelnder Kenntnisse versuchen, in fremde Computersysteme einzudringen oder generell Schaden anzurichten.

## Security Advisory

Empfehlungen an IT-Sicherheitsverantwortliche zum Umgang mit aufgefundenen Schwachstellen.

## Security Assurance Specification (SCAS)

Security Assurance Specifications (SCAS) definieren wichtige Sicherheitsfunktionen, die auch Grundlage für die Produktzertifizierung nach NESAS CCS-GI bilden.

## Security by Default

Ein Produkt, das nach Security by Default ausgeliefert wird, ist ohne zusätzlich notwendige Maßnahmen bereits in einem sicher vorkonfigurierten Auslieferungszustand.

## Security by Design

Nach dem Prinzip Security by Design gehen Hersteller vor, wenn Anforderungen aus der Informationssicherheit bereits bei der Entwicklung eines Produktes berücksichtigt werden.

## Seitenkanalangriff

Angriff auf ein kryptografisches System, der die Ergebnisse von physikalischen Messungen am System (zum Beispiel Energieverbrauch, elektromagnetische Abstrahlung, Zeitverbrauch einer Operation) ausnutzt, um Einblick in sensible Daten zu erhalten. Seitenkanalangriffe sind für die praktische Sicherheit informationsverarbeitender Systeme von hoher Relevanz.

## Sinkhole

Als Sinkhole wird ein Computersystem bezeichnet, auf das Anfragen von botnetzinfizierten Systemen umgeleitet werden. Sinkhole-Systeme werden typischerweise von Sicherheitsforscherinnen und -forschern betrieben, um Botnetzinfektionen aufzuspüren und betroffene Anwenderinnen und Anwender zu informieren.

## Smishing

Smishing (Phishing per SMS) zeigt sich in dem Versand von zahllosen SMS oder Kurznachrichten per Messenger an eine Vielzahl von Rufnummern, beispielsweise mit angeblichen Lieferbenachrichtigungen oder Anleitungen zum Download einer Sprachnachricht. Bei diesem Verfahren ist das Ziel meist, die Empfängerin oder den Empfänger zum Klicken auf einen Link zu verleiten, hinter dem sich schädliche Apps oder maliziöse Webseiten befinden.

## Social Engineering

Bei Cyberangriffen durch Social Engineering versuchen Kriminelle, ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren. Sowohl im Bereich der Cyberkriminalität als auch bei der Spionage gehen die Angreifer geschickt vor, um vermeintliche menschliche Schwächen wie Neugier oder Angst auszunutzen und so Zugriff auf sensible Daten und Informationen zu erhalten.

## Spam

Unter Spam versteht man unerwünschte Nachrichten, die massenhaft und ungezielt per E-Mail oder über andere Kommunikationsdienste versendet werden. In der harmlosen Variante enthalten Spamnachrichten meist unerwünschte Werbung. Häufig enthalten Spamnachrichten jedoch auch Schadprogramme im Anhang, Links zu verseuchten Webseiten oder sie werden für Phishing-Angriffe genutzt.

## Spear-Phishing-Angriff

Spear-Phishing ist ein gezielter Cyberangriff, der mit E-Mails durchgeführt wird, die für eine bestimmte Gruppe oder Einzelperson speziell präpariert wurden, um an personenbezogene Daten zu gelangen oder das Angriffsziel mit Malware zu infizieren.

## Spekulativer Ausführung

Eine mikroarchitekturelle Optimierung zur Steigerung der Effizienz von Prozessoren ist die spekulative Ausführung. Dabei wird versucht, die nächsten auszuführenden Befehle vorherzusagen und vorzeitig (spekulativ) zu bearbeiten. Falls die Vorhersage nicht eintritt, werden die Zwischenergebnisse verworfen, die ausgeführten Befehle bleiben ohne Effekt und werden flüchtig.

## Stack Overflow

Ein Stack Overflow oder Pufferüberlauf ist eine oft auftretende und häufig ausgenutzte Schwachstelle. Ein Pufferüberlauf tritt auf, wenn es gelingt, mehr Daten in einen Speicher zu schreiben, als der dafür vorgesehene Puffer aufnehmen kann. Dadurch werden auch angrenzende Speicherbereiche mit Daten beschrieben. Die Folge können Programmabstürze, Kompromittierung der Daten, Verschaffen erweiterter Rechte oder Ausführung von Schadcode sein.

## Supply-Chain-Angriff

Im Rahmen eines Supply-Chain-Angriffs (dt. Angriff auf die Lieferkette) bekommen Cyberkriminelle indirekt Zugriff auf das Angriffsziel, indem sie Hersteller, Dienstleister oder Lieferanten (also die Lieferkette) erfolgreich angreifen und die mit diesen etablierten Vertrauensbeziehungen nutzen, um das eigentliche Ziel anzugreifen (zum Beispiel durch Nutzung etablierter VPN-Verbindungen, bestehender Wartungszugänge oder die Manipulation von Patches).

## Symlink

Ein Symlink – auch symbolische Verknüpfung genannt – ist ein Dateisystemobjekt, das eine Datei oder ein Verzeichnis mittels einer Pfadangabe referenziert.

## Trusted Execution Environment (TEE)

Ein Trusted Execution Environment (TEE) bezeichnet einen isolierten Teil innerhalb eines Systems, der eine besonders geschützte Laufzeitumgebung bereitstellt. Das TEE kann beispielsweise Bestandteil des Hauptprozessors (CPU) oder Teil des Ein-Chip-Systems (SoC) eines Smartphones sein. Das TEE schützt die Integrität und Vertraulichkeit der enthaltenen Daten und des Schlüsselmaterials vor unautorisierten Dritten, zum Beispiel auch der Nutzerin oder dem Nutzer eines Geräts. Lediglich autorisierte Stellen ist es möglich, Anwendungen in das TEE einzubringen oder zu verändern.

## UP KRITIS

Der Umsetzungsplan Kritische Infrastrukturen (UP KRITIS) ist eine öffentlich-private Kooperation zwischen KRITIS-Betreibern, deren Verbänden und staatlichen Stellen wie dem BSI.

## Voltage Glitching

Voltage Glitching ist eine Methode, um den Programmablauf von Chips durch gezieltes kurzes (im Millisekundenbereich) Abschalten der Versorgungsspannung zu manipulieren. Beispielsweise können damit kritische Authentisierungs Routinen „übersprungen“ werden, um Zugriff auf sonst geschützte Daten zu erlangen. Im Dezember 2023 wurde ein erfolgreicher Angriff auf Tesla-Auto-pilot-Hardware mittels Voltage Glitching veröffentlicht, der es ermöglichte, Programmcode, Benutzerdaten sowie kryptografische Schlüssel aus dem System zu extrahieren.

## Virtuelles Privates Netz (VPN)

Ein Virtuelles Privates Netz (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes (oft des Internets) betrieben wird, jedoch logisch von diesem Netz getrennt wird. In VPNs können unter Zuhilfenahme kryptografischer Verfahren die Integrität und Vertraulichkeit von Daten geschützt und die Kommunikationspartner sicher authentifiziert werden, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind. Der Begriff VPN wird oft als Bezeichnung für verschlüsselte Verbindungen verwendet, zur Absicherung des Transportkanals können jedoch auch andere Methoden eingesetzt werden, beispielsweise spezielle Funktionen des genutzten Transportprotokolls.

## Vishing

Beim Vishing (Voice Phishing) wird die Zielperson telefonisch kontaktiert und mithilfe eines Gesprächsskriptes dazu verleitet, Informationen preiszugeben oder eine Zahlung zu tätigen. Weitverbreitete und noch immer aktuelle Inhalte der Telefonate sind gefälschte Anrufe von angeblichen IT-Supports oder Behörden, bei denen den Opfern suggeriert wird, sie müssten eine Zahlung durchführen oder persönliche Daten zur Überprüfung freigeben.

## Webshell

Schadcode, den Angreifer nach dem Einbruch auf einem Webserver installieren. Webshells ermöglichen Angreifern den Remote-Zugang zu Servern und können für die Ausführung von Schadcode verwendet werden.

## Wiper

Schadsoftware, die Daten vernichtet. Im Gegensatz zu Ransomware zielen Wiper nicht auf Verschlüsselung mit anschließender Erpressung, sondern auf Sabotage durch endgültige Vernichtung von Daten.

## Zwei- bzw. Multifaktor-Authentifizierung (2FA bzw. MFA)

Bei der Zwei- bzw. Multifaktor-Authentifizierung erfolgt die Authentifizierung einer Identität anhand verschiedener Authentifizierungsfaktoren aus getrennten Kategorien (Wissen, Besitz oder biometrische Merkmale).

## 19 - Quellenverzeichnis

---

- 1 <https://www.bsi.bund.de/dok/ransomware-links>
- 2 <https://www.usenix.org/system/files/sec20-oest-sunrise.pdf>
- 3 [https://nationale-leitstelle.de/verstehen/o-LIS-Report\\_der\\_Nationalen\\_Leitstelle\\_Ladeinfrastruktur/](https://nationale-leitstelle.de/verstehen/o-LIS-Report_der_Nationalen_Leitstelle_Ladeinfrastruktur/)
- 4 <https://cert.vde.com/en/advisories/VDE-2024-011>
- 5 <https://terrapin-attack.com/>
- 6 <https://www.openwall.com/lists/oss-security/2024/04/15/6>
- 7 <https://www.vice.com/en/article/xgwgn4/researchers-demonstrate-ai-supply-chain-disinfo-attack-with-poisonpt>
- 8 <https://slashnext.com/wp-content/uploads/2023/10/SlashNext-The-State-of-Phishing-Report-2023.pdf>
- 9 [https://www.medianama.com/2024/04/223-anthropic-writes-paper-jailbreak-claude-trick-answering-harmful-questions, https://www-cdn.anthropic.com/af5633c94ed2beb282f6a53c595eb437e8e7b630/Many\\_Shot\\_Jailbreaking\\_2024\\_04\\_02\\_0936.pdf](https://www.medianama.com/2024/04/223-anthropic-writes-paper-jailbreak-claude-trick-answering-harmful-questions, https://www-cdn.anthropic.com/af5633c94ed2beb282f6a53c595eb437e8e7b630/Many_Shot_Jailbreaking_2024_04_02_0936.pdf)
- 10 <https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payment, https://www.coveware.com/blog/2023/10/27/scattered-ransomware-attribution-blurs-focus-on-irfundamentals>
- 11 <https://www.coveware.com/blog/2024/4/17/raas-devs-hurt-their-credibility-by-cheating-affiliates-in-q1-2024>
- 12 <https://www.coveware.com/blog/2024/4/17/raas-devs-hurt-their-credibility-by-cheating-affiliates-in-q1-2024>
- 13 [https://www.bsi.bund.de/DE/Themen/\\_Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/\\_Threat-Intelligence/Aktive-Crime-Gruppen/\\_aktive-crime-gruppen\\_node.html](https://www.bsi.bund.de/DE/Themen/_Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/_Threat-Intelligence/Aktive-Crime-Gruppen/_aktive-crime-gruppen_node.html)
- 14 [https://www3.weforum.org/docs/WEF\\_The\\_Global\\_Risks\\_Report\\_2024.pdf](https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf)
- 15 <https://www.pwc.de/de/cyber-security/ceosurvey.html>
- 16 <https://de.statista.com/infografik/26033/ausgaben-fuer-it-sicherheit-in-deutschland/>
- 17 <https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz>
- 18 <https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz>
- 19 <https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz>
- 20 <https://www.pwc.de/de/cyber-security/ceosurvey.html>
- 21 [https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/Massnahmenkatalog/massnahmenkatalog\\_node.html](https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/Massnahmenkatalog/massnahmenkatalog_node.html)
- 22 [https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/Notfallkarte/One-Pager\\_Einstieg\\_ins\\_IT-Notfallmanagement\\_KMU.pdf](https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/Notfallkarte/One-Pager_Einstieg_ins_IT-Notfallmanagement_KMU.pdf)
- 23 [https://www.bsi.bund.de/DE/Themen/\\_Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/\\_BSI-Standard-200-4-Business-Continuity-Management/\\_bsi-standard-200-4\\_Business\\_Continuity\\_Management\\_node.html](https://www.bsi.bund.de/DE/Themen/_Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/_BSI-Standard-200-4-Business-Continuity-Management/_bsi-standard-200-4_Business_Continuity_Management_node.html)
- 24 <https://mip2.bsi.bund.de/meldungen/meldung-ohne-registrierung-erstellen>
- 25 <https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Kleine-Unternehmen-Mittlere-Unternehmen/Tabellen/wirtschaftsabschnitte-insgesamt.html>
- 26 <https://www.bmwk.de/Redaktion/DE/Artikel/Digitale-Welt/foerderprogramm-go-digital.html>
- 27 <https://www.mittelstand-innovativ-digital.nrw/>
- 28 [https://www.bsi.bund.de/DE/Themen/\\_Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/\\_Deepfakes/\\_Deepfakes\\_node.html](https://www.bsi.bund.de/DE/Themen/_Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/_Deepfakes/_Deepfakes_node.html)

- 29 [https://www.gesetze-im-internet.de/bwo\\_1985/\\_71.html](https://www.gesetze-im-internet.de/bwo_1985/_71.html)
- 30 <https://www.theguardian.com/money/2016/jul/28/last-minute-olympics-tickets-scam-warning>
- 31 <https://www.reuters.com/article/us-twitter-olympics-idUSKBN2090SA/>, <https://www.spiegel.de/sport/fussball/football-leaks-informant-rui-pinto-ich-habe-getan-was-ich-tun-musste-a-a586ab53-3bd7-4c72-9843-307b423f9c84>
- 32 <https://www.theverge.com/2022/12/14/23509674/fubo-tv-down-france-morocco-world-cup-semifinal>
- 33 <https://www.bleepingcomputer.com/news/security/ransomware-hits-garage-of-canadian-domain-registration-authority/>
- 34 <https://www.bild.de/sport/fussball/fussball-international/premier-league-cyber-angriff-hacker-erpressen-manchester-united-74168850.bild.html>
- 35 <https://www.fortinet.com/blog/threat-research/wiper-malware-riding-tokyo-olympic-games>
- 36 <https://news.microsoft.com/de-de/richtiger-einsatz-von-double-key-encryption/>
- 37 <https://www.digital-identity-wallet.eu>
- 38 <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Cryptographic-Service-Provider/csp.html>
- 39 <https://globalplatform.org>
- 40 <https://www.deutsche-rentenversicherung.de/DRV/DE/Kundenportal/kundenportal-node.html>
- 41 <https://www.ausweisapp.bund.de/home>

## Überblick Cybersicherheit in Deutschland 2024

- 1 BSI-Meldung 26.03.2024
- 2 BSI-Meldung 01.03.2024

## 20 – Abkürzungsverzeichnis

<b>Abkürzung</b>	<b>Langschreibung</b>
5G/6G	5./6. Generation (Mobilfunk)
AI	Artificial Intelligence
AIS	Anwendungshinweise und Interpretationen zum Schema
AISEC	(Fraunhofer-Institut für) Angewandte und Integrierte Sicherheit
AMD	Advanced Micro Devices, Inc. (Incorporated)
API	Application Programming Interface
APT	Advanced Persistent Threat
ARM	Advanced RISC (Reduced Instruction Set Computer) Machines
BCMS	Business-Continuity-Management-System
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI C5	Cloud Computing Compliance Criteria Catalogue des BSI
BSIG	BSI-Gesetz
BSI-KritisV	BSI-Kritisverordnung
BSOD	“Blue Screen of Death”
BVMW	Bundesverband mittelständische Wirtschaft
BYOVD	Bring Your Own Vulnerable Driver
C2-Server	Command-and-Control-Server
CCaaS	Cybercrime-as-a-Service
CE	Conformité Européenne
CEN	Europäisches Komitee für Normung
CENELEC	Europäisches Komitee für elektrotechnische Normung
CERT	Computer Emergency Response Team
ChatGPT	Chat Generative Pretrained Transformer
COM	Command (Dateinamenserweiterung)
CPU	Central Processing Unit
CRA	Cyber Resilience Act
CSA	Cyber Security Act
CSIRT	Computer Security Incident Response Teams
CSRB	Cyber Safety Review Board (USA)
CSW	Cyber-Sicherheitswarnung (des BSI)
CVD	Coordinated Vulnerability Disclosure
CVE	Common Vulnerabilities and Exposures

<b>Abkürzung</b>	<b>Langschreibung</b>
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CyMon	Cybersecurity monitor
DDL	Data Definition Language
DDoS	Distributed Denial of Service
DDR	Double Data Rate
DIN	Deutsches Institut für Normung
DIN SPEC	DIN Specification (Standard, Vorstufe zu DIN-Norm)
DKE	Double Key Encryption
DNS	Domain Name System
DoH	DNS over HTTPS
DORA	Digital Operational Resilience Act
ECDSA	Elliptic Curve Digital Signature Algorithm
EDR	Endpoint Detection and Response
eID	Elektronische Identifizierung
eIDAS	Verordnung über elektronische Identifizierungs- und Vertrauensdienste
E-Mail	Electronic Mail
EN	Europäische Normen
EnWG	Energiewirtschaftsgesetz
E-Roaming	Zugang zur öffentlichen Ladeinfrastruktur (Elektromobilität)
ESA	European Space Agency
eSe	Embedded Secure Element
eSIM	Embedded SIM
ETSI	Europäisches Institut für Telekommunikationsnormen
EU	Europäische Union
EUCC	Europäische Common-Criteria-Schema
EUCS	EU-Cloud-Sicherheitszertifikat
EUDIW	European Digital Identity Wallet
eUICC	Embedded Universal Integrated Circuit Card
EXE	Executable (Dateinamenserweiterung)
GPU	Graphics Processing Unit
hEN	Harmonisierte Europäischen Normen
HTTPS	Hypertext Transfer Protocol Secure

<b>Abkürzung</b>	<b>Langschreibung</b>
ICS	Industrial Control System
ID	Identifikation
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikationstechnologie
IoT	Internet of Things
IP	Internetprotokoll
IPCC	International Police Coordination Center
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IT	Information Technology
Kfz	Kraftfahrzeug
KI	Künstliche Intelligenz
KMU	kleine und mittlere Unternehmen
KRITIS	Kritische Infrastrukturen
LLM	Large Language Model (KI)
LSP	Large Scale Pilot
MaaS	Malware-as-a-Service
MID	Mittelstand Innovativ & Digital (NRW-Programm)
MIRT	Mobile Incident Response Team
NCCA	Nationale Behörde für Cybersicherheitszertifizierung
NFC	Near Field Communication
NIS	Network and Information Security
NIST	National Institute of Standards and Technology (USA)
NRW	Nordrhein-Westfalen
OCR	Optical Character Recognition (Texterkennung)
OP	Operation
OT	Operational Technology (Betriebstechnik)
OWA	Outlook Web Access
OWASP	Open Web Application Security Project (gemeinnützige Stiftung)
ProPK	Programm Polizeiliche Kriminalprävention
RaaS	Ransomware-as-a-Service
RAG	Retrieval Augmented Generation (KI)
RAN	Radio Access Network

<b>Abkürzung</b>	<b>Langschreibung</b>
RED	Radio Equipment Directive
RFID	Radio-Frequency Identification
SBOM	Software Bill of Materials
SE	Secure Element
SEC	Securities and Exchange Commission (USA)
SS7	Signalling System 7
SSH	Secure Shell (Netzwerkprotokoll)
SzA	Systeme zur Angriffserkennung
TKG	Telekommunikationsgesetz
TR	Technische Richtlinie
URL	Uniform Resource Locator
US(A)	United States (of America)
VPN	Virtual Private Network
VPS	Virtual Private Server
VS	Verschlusssachen
VSA	Verschlusssachenanweisung
VS-AP	Verschlusssachen-Anforderungsprofil
VS-NfD	Verschlusssachen – nur für den Dienstgebrauch
WLAN	Wireless Local Area Network
XAI	Explainable AI



# **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](mailto:bsi@bsi.bund.de)  
Telefon +49 (0) 22899 9582-0  
Telefax +49 (0) 22899 9582-5400

## **Stand**

Oktober 2024

## **Druck**

Appel & Klinger Druck und Medien GmbH, Schneckenlohe

## **Design**

KOMPAKTMEDIEN – Agentur für Kommunikation  
GmbH, Berlin

## **Texte und Redaktion**

Bundesamt für Sicherheit in der Informationstechnik  
(BSI)

## **Redaktion Infografiken**

Bundesamt für Sicherheit in der Informationstechnik  
(BSI)

## **Bildnachweise**

Bildnachweis Seite 5: © Bundesfoto/Christina Czybik;  
Seite 7: © BMI/Henning Schacht

## **Artikelnummer**

BSI-LB24/513

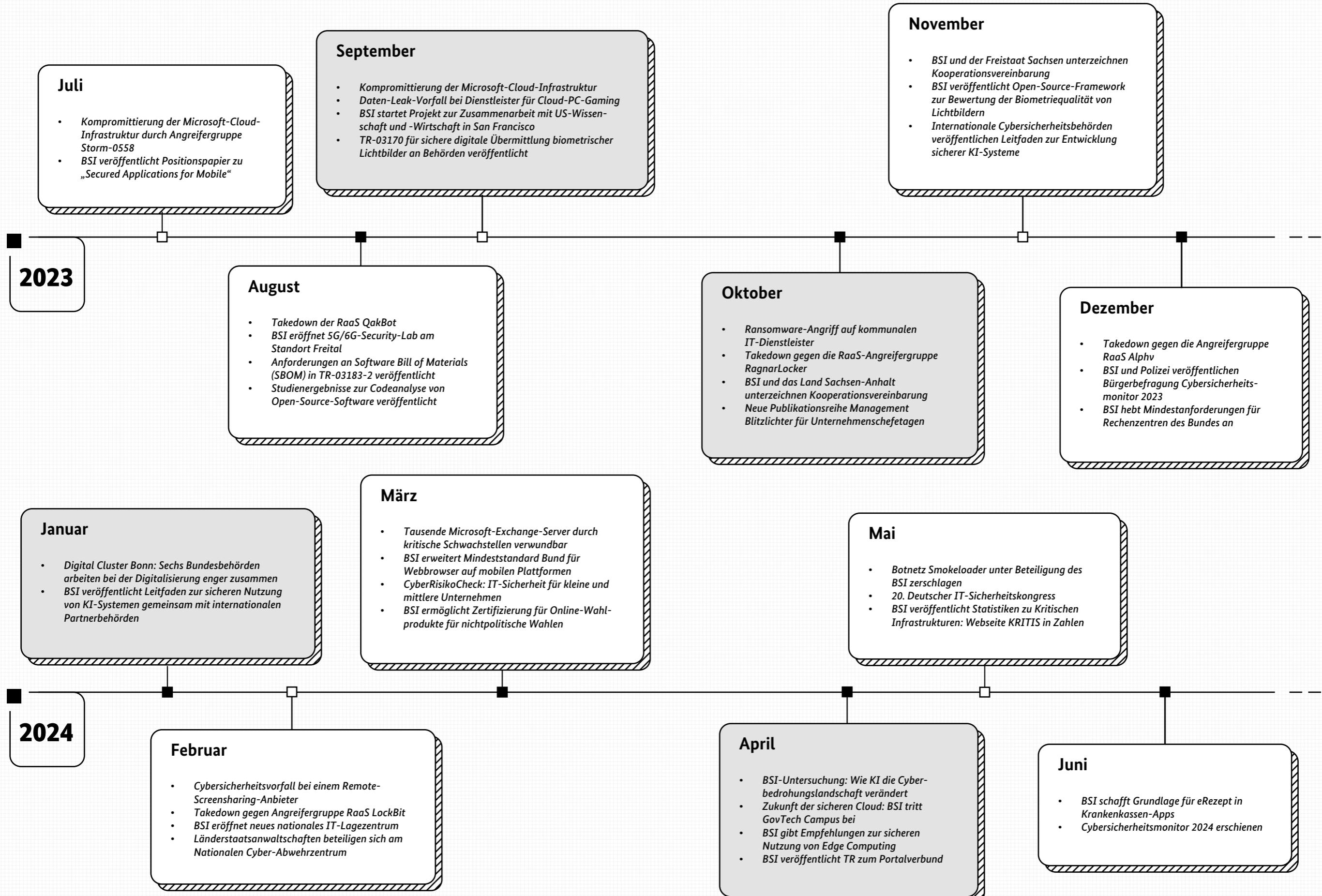
Diese Broschüre ist Teil der Öffentlichkeitsarbeit des BSI.  
Sie wird kostenlos abgegeben und ist nicht zum Verkauf  
bestimmt.



# 12 MONATE CYBERSICHERHEIT IM ÜBERBLICK

Die Lage der IT-Sicherheit in Deutschland 2024 im Überblick

## Zeitstrahl Lagebericht 2024 – Themen



# ANGESPANNTE LAGE, ENTSCHEIDENE ANTWORTEN: CYBERSICHERHEIT IN DEUTSCHLAND 2024

