

# Die Lage der IT-Sicherheit in Deutschland 2023



Bundesamt  
für Sicherheit in der  
Informationstechnik

Deutschland  
Digital•Sicher•BSI•

---

Vorwort

---



*Nancy Faeser*

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

Die Digitalisierung eröffnet für unser Land neue Horizonte. Sie ebnet vielfältige Wege, unsere Wirtschaft zu stärken, mehr gesellschaftliche Teilhabe zu ermöglichen und unsere Verwaltung schlicht bürger-näher und effizienter zu machen.

Die Anwendung Künstlicher Intelligenz, das viel zitierte „Internet der Dinge“ oder die Möglichkeit, komplexe Prozesse digital zu steuern, bieten jedoch nicht nur Chancen. Sie stellen auch Risiken dar. Und diese Risiken werden größer, je stärker diese Technologien sich verbreiten. Das Potenzial für Missbrauch wächst, neue Angriffsflächen entstehen. Das zu wissen, ist wichtig – und muss stärker ins öffentliche Bewusstsein rücken. Nur wer mögliche Gefahren kennt und erkennt, ist in der Lage, richtige Entscheidungen zu treffen und geeignete Maßnahmen zu ergreifen, um sich und andere zu schützen. Das ist für unsere digitale und damit öffentliche Sicherheit fundamental.

Mit dem vorliegenden Bericht zur Lage der IT-Sicherheit in Deutschland 2023 leistet das Bundesamt für Sicherheit in der Informationstechnik (BSI) einen wichtigen Beitrag, um unser Risikobewusstsein zu schärfen.

Nur so werden Gesellschaft, Wirtschaft, Politik und Verwaltung in die Lage versetzt, Angriffen aus dem Cyberraum zielsicher vorzubeugen. Nur so können sie die notwendigen Vorkehrungen treffen, um auf einen

möglichen Vorfall zu reagieren. Nur so können sie solche Ernstfälle auch realitätsnah proben und simulieren. Das ist unerlässlich, denn die Bürgerinnen und Bürger müssen darauf vertrauen können, dass wir gut vorbereitet sind.

Gemeinsam mit allen Bundesländern hat das Bundesministerium des Innern und für Heimat in diesem Jahr erneut eine länder- und ressortübergreifende Krisenmanagement-Übung (LÜKEX) durchgeführt. Beteiligt waren eine Vielzahl von Bundesbehörden sowie Unternehmen, die Kritische Infrastrukturen betreiben. Geübt wurde, wie Staats- und Regierungsfunktionen nach einem Cyberangriff aufrechterhalten werden können. Und es hat sich gezeigt: Wir sind gut auf den Ernstfall vorbereitet.

Aber wir haben auch gelernt: Es braucht den intensiven Austausch von Informationen und koordiniertes Handeln, um Bedrohungen aus dem Cyberraum erfolgreich zu begegnen. Deshalb müssen Bund und Länder diesen Gefahren gemeinsam entgegentreten. Ein starker Partner ist dabei das BSI. Es warnt nicht nur vor möglichen Bedrohungen und Gefährdungen, sondern sorgt zusammen mit den anderen Sicherheitsbehörden für verlässliche Cybersicherheit. Umso mehr verdient der vorliegende Bericht viele interessierte Leserinnen und Leser. Ich wünsche eine spannende Lektüre!

---

Vorwort

---



A handwritten signature in black ink, appearing to read 'C. Plattner', written on a light-colored rectangular background.

**Claudia Plattner, Präsidentin des  
Bundesamts für Sicherheit in der Informationstechnik**

Im Juni 2023 wurde die Nationale Sicherheitsstrategie des Bundes verabschiedet. In dem 76-seitigen Dokument kommt das Wort „Cyber“ ganze 62 Mal vor. Allein das macht die Bedeutung der Cybersicherheit für die umfassende Sicherheit Deutschlands und mithin jeder Bürgerin und jedes Bürgers augenscheinlich. Und es deckt sich mit der im BSI-Lagebericht festgestellten angespannten bis kritischen Lage:

Die anhaltende Digitalisierung und zunehmende Vernetzung vergrößert die Angriffsflächen – und diese werden genutzt. Im Bericht verzeichnen wir einen Anstieg der Bedrohung im Bereich Schwachstellen. So werden täglich knapp 70 neue Schwachstellen in Softwareprodukten entdeckt – rund 25 Prozent mehr als im vorherigen Berichtszeitraum. Auch die rasante Weiterentwicklung neuer und angepasster Angriffsmethoden und der zunehmende Dienstleistungscharakter (*Cybercrime-as-a-Service*) sind besorgniserregend. Dabei bleibt *Ransomware* die Hauptbedrohung.

#### Was also tun? Wir müssen

- Resilienzen so schnell wie möglich erhöhen, um Angriffen vorzubeugen,
- die Cybersicherheit aktiv gestalten, um "vor die Welle" zu kommen,
- gleichzeitig die Digitalisierung voranbringen, denn nur so werden wir auch in den Zukunftstechnologien sicher und wettbewerbsfähig.

Unser Ziel ist es, *Resilienzen* zu erhöhen, indem unsere Empfehlungen, Vorgaben und Hilfestellungen stärker angewandt werden. Die dringendsten Themen in der Umsetzung sind *Patching*, Updates und sicheres Identity-Access-Management, um Angriffen vorzubeugen. Hinzu kommt, *Backups*, Datensicherungen und Notfallpläne als Reaktion auf einen Vorfall zu erstellen und vor allem auch zu erproben. Dafür müssen wir Produkte und Services,

die den notwendigen Sicherheitsanforderungen genügen und niederschwellig einsetzbar sind, als Hilfe zur Selbsthilfe bereitstellen und deren Anwendung fördern wie auch fordern können.

Indem wir wichtige Standards und Produkte für mehr und mehr Cyberthemen und Technologien auch auf europäischer Ebene mitgestalten, kommen wir vor die Welle. So erhöhen wir die Cybersicherheit systematisch für Organisationen ebenso wie für Verbraucherinnen und Verbraucher.

Als BSI sind wir auch in der Entwicklung und Forschung zu den für die Digitalisierung notwendigen Schlüsseltechnologien dabei – von KI, *Cloud*, eID oder Smart Metering bis hin zu sicheren modernen Netzen. Indem wir schnell Klarheit über Sicherheitseigenschaften und die sichere Verwendung schaffen, bringen wir Handlungssicherheit. Auf diese Weise leisten wir unseren Beitrag für eine sichere Digitalisierung und beschleunigen diese zugleich.

Für all das sind und wollen wir weiterhin Möglichmacher und Gestalter sein! Wir können ein starker Partner in der deutschen Sicherheitsarchitektur sein.

Als BSI werden wir unsere Befugnisse nutzen: Wir müssen Sicherheitsthemen benennen und Lösungen zuführen können. Denn Cybersicherheit ist komplex und betrifft – wie nicht zuletzt dieser Lagebericht zeigt – alle, von Verwaltungsbehörden über KMU bis hin zu den einzelnen Bürgerinnen und Bürgern.

Unsere oberste Priorität ist es, Deutschland digital und sicher aufzustellen. Das gelingt nur mit koordinierter Zusammenarbeit aller Akteure in den Kommunen, den Ländern und im Bund, international sowie in ganz Europa! Dabei gilt es, auch in den Austausch mit Wirtschaft, Wissenschaft und Gesellschaft zu treten. Wir verstehen Cybersicherheit als Gemeinschaftsaufgabe, die auf Transparenz als Grundlage für Vertrauen beruht!

---

# Inhalt

---

	Vorwort Nancy Faeser, Bundesministerin des Innern und für Heimat	2
	Vorwort Claudia Plattner, Präsidentin des Bundesamts für Sicherheit in der Informationstechnik	4
<b>1</b>	<b>Einleitung</b>	<b>9</b>
<hr/>		
<b>A</b>	<b>Bedrohungslage</b>	<b>10</b>
<b>2</b>	<b>Zusammenfassung und Bewertung</b>	<b>11</b>
<b>3</b>	<b>Angriffsmittel</b>	<b>12</b>
3.1	Neue Schadprogramm-Varianten	12
3.2	Botnetze	13
<b>4</b>	<b>Angriffsarten</b>	<b>14</b>
4.1	Ransomware	14
4.2	Advanced Persistent Threats und Bedrohungen im Kontext des Ukraine-Kriegs	25
4.3	Distributed Denial of Service	28
4.4	Spam und Phishing	30
4.5	Angriffe im Kontext Kryptografie	32
<b>5</b>	<b>Schwachstellen</b>	<b>32</b>
5.1	Schwachstellen in Softwareprodukten	33
5.2	Schwachstellen in Hardwareprodukten	39
5.3	Schwachstellen in vernetzten Geräten	39
<b>6</b>	<b>Große KI-Sprachmodelle</b>	<b>40</b>
6.1	Technische Entwicklung	41
6.2	Neue Bedrohungen	41
6.3	Neue Gefährdungen – die KI als Angriffsfläche	42
6.4	Systemische Bedrohungsveränderung	43
<hr/>		
<b>B</b>	<b>Gefährdungslage</b>	<b>50</b>
<b>7</b>	<b>Erkenntnisse zur Gefährdungslage in der Gesellschaft</b>	<b>51</b>
7.1	Missbräuchliche Nutzung von Identitätsdaten	51
7.2	Handlungsfelder: Hersteller und Anbieter in der Verantwortung	52
<b>8</b>	<b>Erkenntnisse zur Gefährdungslage in der Wirtschaft</b>	<b>55</b>
8.1	Gefährdungslage Kritischer Infrastrukturen	58
8.2	Besondere Situation von KMU in Deutschland	64

<b>9</b>	<b>Erkenntnisse zur Gefährdungslage in Staat und Verwaltung</b>	<b>67</b>
9.1	Bundesverwaltung	67
9.2	Landes- und Kommunalverwaltungen	68
<hr/>		
<b>C</b>	<b>Herausgehobene Trends in der IT-Sicherheit</b>	<b>70</b>
<b>10</b>	<b>Künstliche Intelligenz</b>	<b>71</b>
10.1	Sicherheit großer KI-Sprachmodelle	71
10.2	Digitaler Verbraucherschutz und KI	72
10.3	Einsatz von KI in der Kryptografie	72
10.4	KI-gestützte Analyse der IT-Sicherheitslage	72
10.5	KI für autonomes Fahren und mediale Identitäten	73
10.6	Weitere Entwicklungen im Bereich KI	73
<b>11</b>	<b>Quantentechnologien</b>	<b>74</b>
11.1	Post-Quanten-Kryptografie	74
11.2	Quantum Key Distribution	75
<b>12</b>	<b>Sicherheit moderner Telekommunikationsinfrastrukturen (5G/6G)</b>	<b>76</b>
12.1	Vorgaben und Zertifizierung für 5G-Netze	76
12.2	Sicherheit in der Standardisierung von 5G und 6G	78
12.3	Förderung von Cybersicherheit und digitaler Souveränität in den Kommunikationstechnologien 5G/6G	78
<b>13</b>	<b>eID: Novellierung der eIDAS-Verordnung</b>	<b>79</b>
<b>14</b>	<b>Bund-Länder-Zusammenarbeit</b>	<b>81</b>
14.1	Nationales Verbindungswesen	81
14.2	Informationssicherheitsberatung für Länder und Kommunen	81
14.3	Roadshow Kommunen	82
14.4	Gremienarbeit	82
14.5	Verwaltungs CERT-Verbund (VCV)	83
14.6	Kooperationsvereinbarungen zwischen BSI und den Ländern	83
14.7	Weiterentwicklung der Zusammenarbeit mit den Ländern	83
<hr/>		
<b>15</b>	<b>Fazit</b>	<b>84</b>
<b>16</b>	<b>Glossar</b>	<b>88</b>
<b>17</b>	<b>Quellenverzeichnis</b>	<b>94</b>

---

## Vorfälle & Abbildungen

---

### Verzeichnis ausgewählter Vorfälle:

Supply-Chain-Angriff infolge eines anderen Supply-Chain-Angriffs	27
DDoS-Hacktivismus	30
Angriffskampagne gegen Schwachstelle in Filesharing-Software GoAnywhere	37
Angriffskampagne gegen Filesharing-Software MOVEit	38
Identitätsdiebstahl mit Phishing-as-a-Service (PhaaS)	54
Cyberangriffe auf IT-Dienstleister	57
Industrie- und Handelskammern nach Cyberangriff deutschlandweit offline	57
Ransomware-Angriffe auf Kommunalverwaltungen und kommunale Versorgungsbetriebe	69
Ransomware-Angriffe auf Bildungs- und Forschungseinrichtungen	69

### Abbildungsverzeichnis:

Abbildung 1: Durchschnittlicher täglicher Zuwachs neuer Schadprogramm-Varianten	12
Abbildung 2: Mutmaßliche Opfer auf Leak-Seiten aus Deutschland und weltweit im Vergleich	19
Abbildung 3: Mutmaßliche Opfer aus Deutschland auf Leak-Seiten (Anzahl)	20
Abbildung 4: Mutmaßliche Opfer aus Deutschland nach Leak-Seiten (Anteile)	20
Abbildung 5: Mutmaßliche Opfer weltweit nach Leak-Seiten (Anteile)	21
Abbildung 6: Supply-Chain-Angriff infolge eines Supply-Chain-Angriffs	27
Abbildung 7: Bekannt gewordene DDoS-Angriffe (Messzahl) in Deutschland	29
Abbildung 8: Spam im Berichtszeitraum nach Art des Spam	31
Abbildung 9: Bekannt gewordene Schwachstellen nach Schadwirkung	35
Abbildung 10: Bekannt gewordene Schwachstellen nach Kritikalität	35
Abbildung 11: Meldungen über schwachstellenbehaftete Produkte	36
Abbildung 12: WID-Meldungen	37
Abbildung 13: Beispiel einer Phishing-Mail im Namen von Banken	53
Abbildung 14: Beispiel einer Phishing-Mail im Namen eines Paketversanddienstleisters	53
Abbildung 15: Umgehung von Multifaktor-Authentifizierung	54
Abbildung 16: Bekannt gewordene Ransomware-Opfer in Deutschland	56
Abbildung 17: Gremien des UP KRITIS	61
Abbildung 18: Unternehmen in Deutschland nach Größe	64
Abbildung 19: Spam-Mail-Index für die Bundesverwaltung	67
Abbildung 20: Handlungsstränge der eIDAS-Revision	80
Abbildung 21: Schaubild Modulaufbau	81

---

# Einleitung

---

## 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 Cyberangriffe auf staatliche sowie öffentliche Institutionen, Unternehmen und Privatpersonen, aber auch Maßnahmen zur Prävention und Bekämpfung dieser Lagen. Der vorliegende Bericht zieht eine Bilanz für die Zeit vom 1. Juni 2022 bis zum 30. Juni 2023 (Berichtszeitraum).

Der Zeitraum weicht von dem des Berichts „Die Lage der IT-Sicherheit in Deutschland 2022“ ab, was in einer Veränderung der Zeiträume begründet liegt, in denen die Daten erfasst und ausgewertet werden. Um eine Vergleichbarkeit der Daten mit dem vorherigen Berichtszeitraum (1. Juni 2021–31. Mai 2022) und dem Berichtszeitraum des Berichts „Die Lage der IT-Sicherheit in Deutschland 2024“ (1. Juli 2023–30. Juni 2024) sicherzustellen, werden an den Stellen, an denen es möglich ist, Tagesdurchschnittswerte genutzt oder die Zahlen denen des gleichen Zeitraums aus dem Vorjahr gegenübergestellt.

Der vorliegende Bericht greift aktuelle und anhaltende Cyberbedrohungen auf und bewertet die IT-Sicherheitslage im Kontext des russischen Angriffskriegs auf die Ukraine. Anhand konkreter Beispiele aus unterschiedlichen Bereichen zeichnet der Bericht den Weg und die typischen Methoden der Angreifer nach, um zugleich aufzuzeigen, wie sich Nutzerinnen und Nutzer schützen können.

Teil A dieses Berichts gibt einen Überblick der allgemeinen Bedrohungslage und aktueller Cyberbedrohungen, unterteilt in Angriffsmittel, Angriffsarten und Schwachstellen. Hinzu kommt eine Zusammenfassung der Entwicklungen im Bereich Künstlicher Intelligenz (KI) und von deren Auswirkungen auf die Bedrohungslage. Trifft eine Cyberbedrohung wie zum Beispiel ein Schadprogramm auf eine Schwachstelle, entsteht eine Gefährdung. Während Bedrohungen also unabhängig von konkreten Angriffsflächen in Wirtschaft, Staat und Gesellschaft bestehen und damit allgemeine Phänomene auf Angreiferseite beschreiben, entstehen durch zunehmende Angriffsflächen aufseiten potenzieller Opfer konkrete Gefährdungen. Solche Gefährdungen für Staat, Wirtschaft und Gesellschaft werden in Teil B dargestellt. Schließlich werden in Teil C am Beispiel herausgehobener Themen aktuelle Entwicklungen im Bereich Cybersicherheit beschrieben.

Der Bericht „Die Lage der IT-Sicherheit in Deutschland 2023“ setzt erstmals Schwerpunkte bei der Darstellung der Arbeit des BSI. Tiefergehende Informationen zu weiteren Themen wie zum Beispiel Digitaler Verbraucherschutz, Automotive und Cybersicherheit im Gesundheitswesen finden Sie in den jeweiligen Berichten oder Lagebildern genauso wie in anderen Veröffentlichungen des BSI.

**Weiterführende Informationen finden Sie hier:<sup>a</sup>**



Lagebild Gesundheit



Lagebild Automotive



Bericht Digitaler Verbraucherschutz



Weitere BSI-Publikationen



## Teil A: Bedrohungslage

### 2. – Zusammenfassung und Bewertung

Insgesamt zeigte sich im aktuellen Berichtszeitraum eine angespannte bis kritische Lage. Die Bedrohung im Cyberraum ist damit so hoch wie nie zuvor. Wie schon in den vergangenen Jahren wurde eine hohe Bedrohung durch Cyberkriminalität beobachtet. *Ransomware* blieb die Hauptbedrohung. Auf Angreiferseite konnte hier eine von wechselseitigen Abhängigkeiten und Konkurrenzdruck geprägte Schattenwirtschaft cyberkrimineller Arbeitsteilung festgestellt werden. Kleine und mittlere Unternehmen (KMU) sowie besonders Kommunalverwaltungen und kommunale Betriebe wurden überproportional häufig angegriffen. Im Kontext des russischen Angriffskriegs gegen die Ukraine bestand eine Bedrohung vor allem durch prorussische Hacking-Angriffe, die aber keinen nachhaltigen Schaden verursachten und eher als Propagandamittel zu werten sind. Ein Anstieg der Bedrohung konnte ferner im Bereich Schwachstellen festgestellt werden. Hier wurden im Berichtszeitraum täglich 68 neue Schwachstellen in Softwareprodukten registriert – rund 24 Prozent mehr als im Berichtszeitraum davor.

#### Ausbau cyberkrimineller Schattenwirtschaft

Der Berichtszeitraum war gekennzeichnet durch den weiteren Ausbau einer cyberkriminellen Schattenwirtschaft. Die bereits in den vergangenen Berichtszeiträumen begonnene Ausdifferenzierung der cyberkriminellen „Wertschöpfungskette“ von *Ransomware*-Angriffen wurde im aktuellen Berichtszeitraum durch die Angreifer fortlaufend weiterentwickelt. Vom Zugang in ein Opfernnetzwerk über die benötigte *Ransomware* bis hin zur Unterstützung bei Lösegeldverhandlungen können Angreifer inzwischen Werkzeuge für jeden Schritt eines komplexen Angriffs als Dienstleistung einkaufen. Die Arbeitsteilung unter den cyberkriminellen Anbietern dieser Werkzeuge führt dabei zu einer doppelten Skalierung der Bedrohung: Zum einen können cyberkriminelle Anbieter sich auf einzelne Werkzeuge spezialisieren und diese somit schneller weiterentwickeln und verbessern. Zum anderen können die verbesserten Werkzeuge auf diese Weise auch schneller einer größeren Zahl interessierter Angreifer zur Verfü-

gung gestellt werden. Letztere, die sogenannten *Affiliates*, spezialisieren sich auf die tatsächliche Durchführung der *Ransomware*-Angriffe und zahlen von den eingetribenen Lösegeldern Provisionen an die cyberkriminellen Anbieter der verwendeten Dienstleistungen.

#### Cyberresilienz

Cyberkriminelle Angreifer gingen im Berichtszeitraum zunehmend den Weg des geringsten Widerstands und wählten verstärkt solche Opfer aus, die ihnen leicht angreifbar erschienen. Nicht mehr die Maximierung des potenziellen Lösegelds stand im Vordergrund, sondern das rationale Kosten-Nutzen-Kalkül. So wurden vermehrt kleine und mittlere Unternehmen sowie Behörden der Landes- und Kommunalverwaltungen, wissenschaftliche Einrichtungen sowie Schulen und Hochschulen Opfer von *Ransomware*-Angriffen. Cyberresilienz ist daher das Gebot der Stunde.

#### DDoS-Hacking

Im Kontext des russischen Angriffskriegs gegen die Ukraine kam es im Berichtszeitraum zu einer Reihe prorussischer Hacking-Angriffe in Deutschland. Die Hackinggruppen verwendeten dafür ausschließlich Distributed-Denial-of-Service-Angriffe (*DDoS-Angriffe*), die vornehmlich auf die Verfügbarkeit von Internetdiensten zielen und keinen nachhaltigen Schaden bewirken können wie etwa *Ransomware*-Angriffe. *DDoS*-Hacking ist daher im Wesentlichen als Propagandawerkzeug zu werten, welches gesellschaftliche Verunsicherung stiften und das Vertrauen in die Fähigkeit des Staates zum Schutz und zur Versorgung der Bevölkerung unterminieren soll.

#### Advanced Persistent Threats

Im Berichtszeitraum waren *Advanced Persistent Threats* (APTs) mit dem Ziel der Informationsbeschaffung prägend. Während in Südost- und Zentralasien beispielsweise Telekommunikationsanbieter angegriffen wurden, standen in Europa und Nordamerika unter anderem Regierungseinrichtungen im Fokus. Anders stellte sich die Lage in der Ukraine dar, in der sowohl Cyberspionage

als auch einfache Cybersabotage zu beobachten war. Technisch war zu beobachten, dass Angriffe über verwundbare Server am Netzwerkperimeter eine Vielzahl an Schwachstellen ausnutzten.

### Schwachstellen

Im Berichtszeitraum wurden durchschnittlich täglich knapp 70 neue Schwachstellen in Softwareprodukten entdeckt – rund 15 Prozent davon waren kritisch. Cybererpresser nutzten zum Beispiel zwei Schwachstellen in Filesharing-Produkten, um Daten von zahlreichen Betroffenen in Deutschland und der Welt abzugreifen und anschließend mit deren Veröffentlichung zu drohen. Aufgrund der Verbreitung der schwachstellenbehafteten Produkte ist von einer sehr großen Zahl von Betroffenen auszugehen. Darüber hinaus illustrierte ein Angriff auf die Webportale verschiedener Fahrzeughersteller die möglichen Schadwirkungen, die durch unzureichend abgesicherte Webserver entstehen: Angreifen war es dadurch möglich, sich als Händler auszugeben, somit Zugriff auf Fahrzeugfunktionen fremder Autos zu erlangen und diese über die offizielle Hersteller-App zu steuern.

Eine ausführliche Betrachtung der genannten Punkte folgt in den folgenden Kapiteln.

## 3. – Angriffsmittel

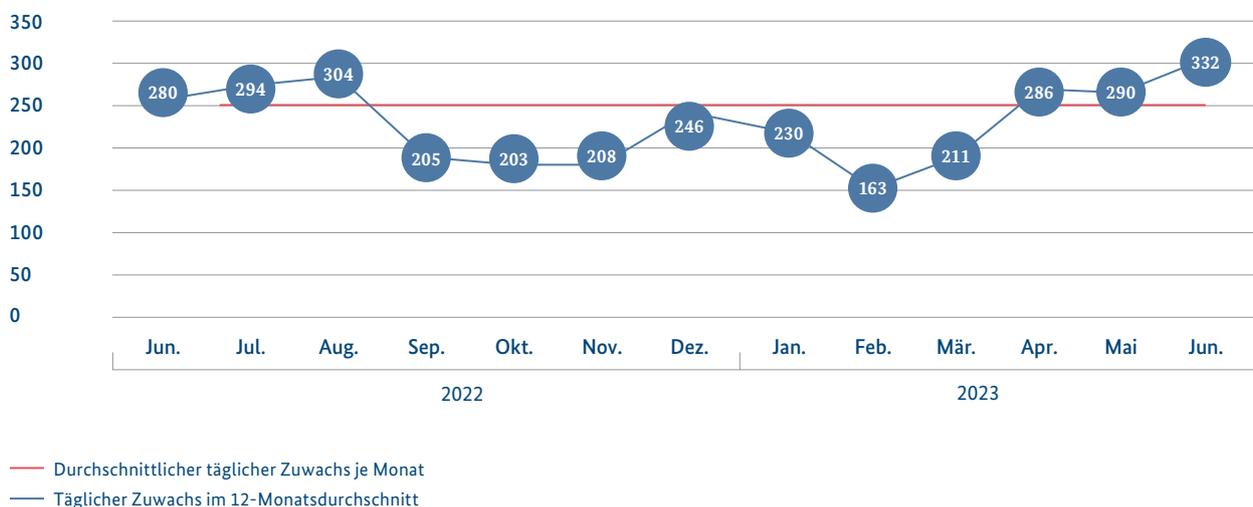
Cyberangriffe werden mithilfe von Schadprogrammen ausgeführt. Diese kommen auf unterschiedlichsten Wegen (zum Beispiel E-Mail-Anhang, *maliziose* Webserver, *Exploit* usw.) zum Einsatz und ermöglichen dadurch verschiedenste Arten von Cyberangriffen (vgl. Kapitel *Angriffsarten*, Seite 14). Werden zahlreiche Computersysteme mit einem Schadprogramm infiziert und dadurch fernsteuerbar, so spricht man von einem *Botnetz*, welches seinerseits für Cyberangriffe genutzt werden kann.

### 3.1 – Neue Schadprogramm-Varianten

Zu Schadprogrammen zählen alle Computerprogramme, die schädliche Operationen ausführen können oder andere Programme dazu befähigen, dies zu tun. Schadprogramme gelangen unter anderem im Anhang von oder über Verlinkungen in E-Mails auf einen Computer. Wenn die Nutzerin oder der Nutzer auf einen *maliziösen* Anhang klickt oder auf einen Link, der auf eine *maliziose* Webseite führt, kann sich das Schadprogramm installieren. Neben der E-Mail als Einfallstor zählen gefälschte

### Durchschnittlicher täglicher Zuwachs neuer Schadprogramm-Varianten Anzahl in Tausend

Abbildung 1: Durchschnittlicher täglicher Zuwachs neuer Schadprogramm-Varianten  
Quelle: *Malware*-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH



Links in Webseiten sowie der Missbrauch von legitimen Programmen zum Beispiel in Supply-Chain-Angriffen zu den typischen *Angriffsvektoren*. Für die Infektion angegriffener IT-Systeme nutzen Schadprogramme in der Regel Schwachstellen. Diese treten in Software- oder Hardwareprodukten, in vernetzten Geräten sowie an Netzübergängen auf. Darüber hinaus wird, wie im Fall von *Social Engineering*, der Faktor „Mensch“ für Cyberangriffe immer bedeutsamer.

Die einzelnen Schadprogramme unterscheiden sich im Hinblick auf ihre Funktionalität, wobei ein Schadprogramm auch mehrere Funktionalitäten aufweisen kann. Als *Ransomware* bezeichnet man beispielsweise Schadprogramme, die durch Verschlüsselung den Zugang zu Daten oder Systemen einschränken, damit der Angreifer anschließend ein Lösegeld (engl. ransom) erpressen kann (vgl. Kapitel *Ransomware*, Seite 14). Schadprogramme, die sich als gutartige Software tarnen oder in legitimen Dateien verstecken, werden als Trojanische Pferde bezeichnet. *Bots* heißen Schadprogramme, die sich zum Beispiel mithilfe von sogenannten *Command-and-Control-Servern* fernsteuern lassen (vgl. Kapitel *Botnetze*, Seite 13).

Nimmt ein Angreifer in einem Schadprogramm Änderungen am Programmcode vor, entsteht eine neue Variante. Als neu gilt somit 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 bedrohlich. Im Berichtszeitraum wurden durchschnittlich täglich 250.000 neue Schadprogramm-Varianten bekannt. Das waren 22 Prozent weniger als im vergangenem Berichtszeitraum – ein Wert, der nach den großen Emotet-Wellen in den Jahren 2021 und 2022 eine Rückkehr zur durchschnittlichen Bedrohungslage anzeigt.

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

### 3.2 – Botnetze

Ein mit Schadsoftware infiziertes System, das über ein zentrales Steuerungssystem, den *Command-and-Control-Server*, ferngesteuert werden kann, bezeichnet man als *Bot*. Unter einem *Botnetz* versteht man den Zusammenschluss mehrerer *Bots*, die von einem sogenannten *Botmaster* zentral ferngesteuert werden. Heutzutage können nahezu alle internetfähigen Systeme von *Bots*software befallen werden. Somit können neben klassischen Computersystemen auch Smartphones, Tablets, Router oder auch Geräte des Internets der Dinge (*Internet of Things, IoT*) wie Webcams oder Smart-TVs kompromittiert und übernommen werden.

Da aktuelle *Bots*software modular aufgebaut ist, können Angreifer die Funktionalitäten des *Botnetzes* auf ihren Bedarf zuschneiden und über Updates dynamisch anpassen. Neben gezielten Angriffen auf die persönlichen Daten der Opfersysteme (Informationsdiebstahl) können auch die Ressourcen des kontrollierten Systems für eigene Zwecke (z. B. Cryptomining) oder den Angriff auf Dritte (z. B. *DDoS-Angriffe*, *Spamversand* etc.) genutzt werden.

Im Berichtszeitraum wurden *Botnetze* wie in den Vorjahren primär zum Diebstahl persönlicher Informationen (vgl. zum Thema *Information Stealer* das Kapitel *Ransomware*, Seite 14) sowie zur Verteilung weiterer Schadsoftware verwendet. Hierbei liegt der Schwerpunkt der vom BSI beobachteten *Botnetze* klar auf mobilen Betriebssystemen auf Basis von Android. Klassische Desktop-Betriebssysteme verlieren weiter an Bedeutung.

Im Berichtszeitraum wurden durchschnittlich täglich rund 21.000 infizierte Systeme in Deutschland erkannt und vom BSI an die deutschen *Provider* gemeldet. Die Tageswerte schwankten dabei erheblich. In der Spitze wurden 45.000 infizierte Systeme gemeldet. Die *Provider* ermittelten und benachrichtigten die betroffenen Kunden. Die Anzahl der Gesamtinfektionen dürfte jedoch deutlich höher liegen, da in vielen Fällen Mehrfachinfektionen vorliegen. Die Infektionsdaten stammen überwiegend von BSI-eigenen sowie externen *Sinkhole*-Systemen, die anstelle der regulären *Command-and-Control-Server* die Kontaktanfragen von *Bots* entgegennehmen und protokollieren. Eine Beschreibung des *Sinkholing*-Verfahrens sowie Steckbriefe zu den am häufigsten

gemeldeten Schadprogrammfamilien werden auf der BSI-Webseite angeboten:

**Weiterführende Informationen  
finden Sie hier:**<sup>b</sup>



Basierend auf Erfahrungen aus *Botnetz*abschaltungen ist davon auszugehen, dass die Dunkelziffer an Infektionen deutlich höher liegt und sich für Deutschland mindestens in einem siebenstelligen Bereich bewegt. Durch die zunehmende Professionalisierung der Angreifer und deren Fokussierung auf bestimmte Opfer ist gegenüber den Vorjahren ein Rückgang der ermittelten Infektionszahlen bei großen *Botnetzen* zu verzeichnen. Durch die steigende Anzahl verwundbarer Mobil- und *IoT*-Geräte sowie die Verfügbarkeit von Schadsoftwarecodes im Internet ist jedoch anzunehmen, dass sogenannte *Script-Kiddies* oder politisch motivierte Gelegenheitstäter Systeme infizieren, um *Botnetze* für *DDoS*-Angriffe aufzubauen.

Wie auch in den Vorjahren ist die Bedrohungslage durch *Botnetze* hoch. Die aus dem Sinkholing ermittelten Infektionszahlen stellen dabei eine Untergrenze dar, auch weil nur ein Ausschnitt der aktuell bekannten *Botnetze* aktiv erfasst werden kann. *Botnetz*familien wie *Emotet*, *FluBot* oder *Glupteba* ergreifen Gegenmaßnahmen, um das klassische domänennamenbasierte Sinkholing zu umgehen, indem sie beispielsweise IP-Adressen, getunnelte DNS-Verbindungen (DNS over HTTPS, DoH) oder *Blockchain*-Techniken zur Verschleierung der Kommunikation zwischen Steuerungsservern und *Bots* einsetzen.

## 4. – Angriffsarten

Für wesentliche Angriffsarten wird im Folgenden die Lageentwicklung im Berichtszeitraum dargestellt. Wegen des herausgehobenen Gefährdungspotenzials liegt der Schwerpunkt der Darstellung auf der Bedrohungslage im Phänomenbereich „*Ransomware*“. Es folgen Lagekenntnisse im Bereich *Advanced Persistent Threats* und im Kontext des russischen *Angriffskrieges* gegen die Ukraine sowie zum Bereich „Distributed Denial of Service“ und zum neuen Phänomen des politisch motivierten *DDoS*-Hacking. Darüber hinaus wird auch auf *Spam* und *Phishing* sowie auf Angriffe im Kontext Kryptografie eingegangen.

### 4.1 – Ransomware

Bei einem *Ransomware*-Angriff handelt es sich um eine Form der digitalen Erpressung. Die Angreifer nutzen beispielsweise Fehler wie falsche Bedienung, Fehlkonfigurationen, veraltete Softwareversionen oder mangelhafte Datensicherungen aus, um Systeme tiefgreifend zu infiltrieren und Daten zu verschlüsseln. Für die Entschlüsselung verlangen die Angreifer ein Lösegeld. Häufig wird diese Erpressung noch mit der Drohung einer Veröffentlichung zuvor gestohlener Daten kombiniert. Diese Form der Erpressung ist auch als *Double Extortion* bekannt. Das Lösegeld fungiert in solchen Fällen in der Regel auch als Schweigegeld. Die Zahlung wird meist in elektronischen Währungen (üblicherweise *Bitcoin* oder *Monero*) gefordert.

Die Effektivität von *Ransomware* beruht auf ihrer unmittelbaren Wirkung. Im Unterschied zu klassischer Schadsoftware wie Banking-Trojanern, *Botnetzen* oder *Phishing*-Mails tritt der Schaden direkt ein und hat konkrete Konsequenzen für die Betroffenen. Bei einem *Ransomware*-Angriff können zum Beispiel alle gespeicherten Dokumente verloren gehen sowie wichtige Unternehmensdaten oder kritische Dienstleistungen nicht mehr verfügbar sein. Gegen solche Angriffe helfen am besten präventive Maßnahmen. Es gilt: Vorbeugen ist besser als heilen.

Weil der Druck zur Schadensbegrenzung der Betroffenen nach einem *Ransomware*-Angriff enorm hoch ist, zahlen viele Opfer das geforderte Lösegeld in der Hoffnung, schnell wieder arbeitsfähig zu sein. Es gibt jedoch keine Garantie dafür, dass die Cybererpresser die verschlüsselten Daten tatsächlich wieder freigeben oder die gestohlenen Daten tatsächlich löschen. Auch besteht die Möglichkeit, dass das vom Angreifer zur Verfügung gestellte Entschlüsselungstool fehlerhaft ist. Das BSI rät darum ausdrücklich von der Zahlung eines Lösegelds ab. Zudem müssen einmal ausgeleitete Daten grundsätzlich als kompromittiert betrachtet werden.

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 auch Massenkampagnen bekannt, die auch Verbraucherinnen und Verbraucher direkt betreffen, zum Beispiel gegen Network-Attached-Storage-(NAS)-Systeme.

Einen vollständigen Schutz vor *Ransomware*-Angriffen gibt es nicht, denn Angreifer können auch neue Angriffswege nutzen, für die noch keine Detektions- und Abwehrmethoden entwickelt wurden. Bestimmte Angriffe zum Beispiel auf Unternehmen, Behörden und IT-Dienstleister können aber durchaus auch verhindert werden. *Backups* und Notfallpläne unterstützen dabei, die Auswirkungen im Ernstfall zu begrenzen oder sogar vollständig zu kompensieren.

#### 4.1.1 – Angreifermotivation und Angriffsablauf

*Ransomware*-Angriffe werden überwiegend aus finanziell-motivierten Gründen von cyberkriminellen Angreifern verübt. Allerdings können APT-Angreifer *Ransomware* auch nutzen, um andere Angriffe zu verschleiern oder von diesen abzulenken. Zudem kann *Ransomware* auch zur reinen Sabotage eingesetzt werden. In diesem Fall agiert die *Ransomware* als *Wiper* und die verschlüsselten Daten lassen sich technisch nicht wiederherstellen (vgl. Kapitel *Advanced Persistent Threats und Bedrohungen im Kontext des Ukraine-Kriegs*, Seite 25).

##### 4.1.1.1 – Cyberkriminelle Angriffe auf staatliche Einrichtungen

Durch den zunehmenden Dienstleistungscharakter der arbeitsteiligen cyberkriminellen Schattenwirtschaft (vgl. Kapitel *Cyberkriminelle Schattenwirtschaft*, Seite 16) bieten sich deren Services auch für andere Cyberangreifer, insbesondere APT-Gruppen, an.

Größere *Ransomware*-Angriffe gegen wichtige staatliche Einrichtungen gab es im August 2022 in Montenegro mit der *Ransomware* Cuba sowie mit einer noch unbekanntem *Ransomware* im September in Bosnien-Herzegowina. In beiden Staaten wurde unter anderem das Parlament angegriffen.

Im Berichtszeitraum wurden zudem mehrere *Ransomware*-Vorfälle bekannt, die öffentlicher Berichterstattung zufolge wahrscheinlich staatlich gesteuert waren. So wurden zwischen Juli und September 2022 Angriffe auf albanische Regierungsinstitutionen mit der *Ransomware* GoneXML und dem *Wiper* ZeroShred berichtet. Diese Angriffe wurden in der Fach-Community der iranischen Gruppe Banished Kitten zuge-

ordnet. Darüber hinaus gibt es immer wieder Berichte über den Einsatz von *Ransomware* gegen israelische Organisationen durch iranische Angreifer, bei denen die finanzielle Motivation infrage gestellt wird. Im Oktober 2022 wurde durch das Microsoft Treat Intelligence Center (MSTIC) der Einsatz der *Ransomware* Prestige unter anderem gegen Unternehmen in Polen bekannt. Im November ordnete MSTIC diese Angriffe mit hoher Wahrscheinlichkeit IRIDIUM/Sandworm zu. Diese staatlich gesteuerte Gruppe hatte unter dem Deckmantel *Ransomware* auch Sabotage-Angriffe in der Ukraine durchgeführt. Im weiteren Verlauf des Ukraine-Kriegs verzichtete die Gruppe jedoch auf die Tarnung als *Ransomware* und setzte direkt *Wiper* ein. Im Kontext des Ukraine-Kriegs besteht in der IT-Sicherheitscommunity der Verdacht, dass einige cyberkriminelle Angreifer im Auftrag des russischen Staates agieren. Dem BSI liegen hierzu jedoch keine Erkenntnisse vor.

Bei cyberkriminellen Angriffen gegen staatliche Institutionen wird eine rein finanzielle Motivation oftmals infrage gestellt. Insbesondere bei höheren staatlichen Stellen wird die Bereitschaft zur Zahlung eines Lösegelds zunehmend unwahrscheinlicher. Es ist anzunehmen, dass solche Angriffe andere Hintergründe haben, wie etwa Interessen eines anderen Staates, eine ideologische Motivation der Angreifer oder auch ein Bedürfnis der Angreifer nach Anerkennung in der cyberkriminellen Community und Aufmerksamkeit in der Presse. Weiterhin kann es auch zu Verwechslung der Angriffsziele aufseiten der Angreifer kommen. Die Mehrheit der cyberkriminellen Angriffe sind nach Einschätzung des BSI opportunistische Angriffe (vgl. Vorfall *Ransomware-Angriffe auf Kommunalverwaltungen und kommunale Versorgungsbetriebe*, Seite 69).

Welche Motivation die Angreifer jeweils treibt, lässt sich meist nicht eindeutig beantworten. Die Angreifermotivation kann jedoch einen erheblichen Unterschied im Verlauf des Angriffs und auch bei der Angriffsbewältigung machen, etwa bei der Frage, ob es überhaupt um Lösegeld geht oder zum Beispiel um den Geltungsdrang des Angreifers.

##### 4.1.1.2 – Angriffsablauf

Cyberkriminelle Angreifer werden anhand der eingesetzten Schadsoftware und Vorgehensweise in Gruppen zusammengefasst. So wird beispielsweise die *Ransomware*

Alphv (auch bekannt als BlackCat) von einer anderen Gruppierung eingesetzt als die *Ransomware* LockBit 3.0.

**Angriffsphase 1 – Erstinfektion:** Ein *Ransomware*-Angriff beginnt häufig mit einer *maliziösen* E-Mail, der Kompromittierung eines Fernzugriff-Zugangs (Remote-Zugang) wie zum Beispiel Remote Desktop Protocol (RDP) oder der Ausnutzung von Schwachstellen (vgl. Kapitel *Schwachstellen in Softwareprodukten*, Seite 33). Diese initiale Infektion stellt den Ausgangspunkt für das weitere Vorgehen des Angreifers dar. Wenn der Einbruch von einem *Access Broker*, also einem „Makler“ für erbeutete Zugangsdaten, ausging, können mitunter Wochen und Monate vergehen, bis der Zugang an einen *Ransomware*-Angreifer verkauft wird.

**Angriffsphasen 2 und 3 – Rechteerweiterung und Ausbreitung:** Nach dem Einbruch verfügt der Angreifer nur über diejenigen Zugriffsrechte, die der kompromittierte Account besitzt. Deshalb laden Angreifende in der Regel weitere Schadsoftware nach, um die erlangten Zugriffsrechte zu erweitern und zum Beispiel an Administratorrechte zu gelangen. Ein Administrator kann zum Beispiel Software installieren oder auch deinstallieren. Mit erweiterten Zugriffsrechten breitet sich der Angreifer (teil-) automatisiert im Netzwerk der betroffenen Organisation aus – bis hinein in die zentralen Komponenten der Rechteeverwaltung (z. B. Active Directory) – und versucht, diese vollständig zu übernehmen. Passiert dies, ist das Unternehmens- oder Behördennetzwerk vollständig kompromittiert und nicht mehr vertrauenswürdig. Die Angreifer besitzen dann alle Rechte, um beispielsweise Benutzerkonten mit Administratorrechten anzulegen, Daten einzusehen oder auch sogenannte *Backdoors* einzurichten, Schadprogramme, die einen permanenten Zugriff auf das kompromittierte System ermöglichen.

**Angriffsphase 4 – Datenabfluss:** Anschließend können Angreifer Daten entwenden (Datenexfiltration), um später mit deren Veröffentlichung zu drohen, falls ein Opfer nicht zu einer Lösegeld- oder Schweigegeldzahlung bereit ist.

**Angriffsphase 5 – Verschlüsselung:** Daten werden auf möglichst vielen Systemen verschlüsselt, insbesondere auf *Backup*-Systemen, in der Regel ohne das Betriebssystem selbst zu beeinträchtigen. Stattdessen hinterlassen die Angreifer Nachrichten mit Hinweisen, wie die Opfer Kontakt für Löse- oder Schweigegeldverhandlungen aufnehmen können. Einzelne Angreifergruppen verzichten inzwischen auch ganz auf die Verschlüsselung und erpressen direkt mit den gestohlenen Daten.

**Angriffsphase 6 – Incident Response:** Die Betroffenen stehen vor der Herausforderung, ihre Systeme und Daten wiederherzustellen. Je nach Ausmaß der Betroffenheit muss dafür ein Übergangsbetrieb organisiert und der Vorfall an die Stakeholder, also an Eigentümer, Kunden und Partner, kommuniziert werden. In der Regel wird in dieser Phase ein IT-Sicherheitsdienstleister hinzugezogen, der Erfahrung in der Bewältigung von IT-Sicherheitsvorfällen hat.

#### 4.1.2 – Cyberkriminelle Schattenwirtschaft

*Ransomware*-Angriffe stellen unverändert die größte cyberkriminelle Bedrohung dar. Dabei trifft die zunehmend professionelle Arbeitsteilung der Angreifergruppen auf die zunehmend vernetzte Welt von teils multinationalen Unternehmen. Im Falle eines erfolgreichen *Ransomware*-Angriffs bleiben Schäden oft nicht mehr nur auf regionale Betriebseinheiten beschränkt, sondern breiten sich unter Umständen unabhängig von nationalen und territorialen Grenzen weltweit im Unternehmensnetzwerk aus.

Angesichts der millionenschweren Lösegelder, die *Ransomware*-Angriffe abwerfen, entwickelt sich auf Angreiferseite eine von wechselseitigen Abhängigkeiten und Konkurrenzdruck geprägte Schattenwirtschaft cyberkrimineller Arbeitsteilung: von der notwendigen technischen Infrastruktur und *Malware* über *Access Broker* bis zum cyberkriminellen Callcenter. Wenn sich eine neue Methode für Angriffe anbietet, bildet sich daraus früher oder später eine cyberkriminelle Dienstleistung, die diese Methode vielen Angreifern zugänglich macht.

Bestandteile eines Cyberangriffs werden an jeweils spezialisierte Angreifergruppen ausgelagert, vergleichbar mit dem Outsourcing von Dienstleistungen. Es wird als *Cybercrime-as-a-Service (CCaaS)*, Cyberstraftat als Dienstleistung bezeichnet. *CCaaS* erlaubt es einem Angreifer, nahezu jeden Schritt eines Angriffs als Dienstleistung von anderen Cyberkriminellen zu beziehen oder zumindest die dafür notwendige Schadsoftware. Dies ist ein herausragender Faktor für die Entwicklung der Bedrohungslage, denn die Spezialisierung auf eine bestimmte Dienstleistung ermöglicht es Angreifern, diese gezielt zu entwickeln und ihre Effektivität zu steigern. Darüber hinaus stehen die Dienstleistungen vielen Angreifern gleichzeitig zur Verfügung. Dadurch verkürzt sich der Zeitraum zwischen der Entwicklung einer neuen

Methode und deren verbreitetem Einsatz stark oder fällt ganz weg. Dies erklärt auch zum Teil die dynamischen Entwicklungen, die in den vergangenen Jahren im cyberkriminellen Raum beobachtet wurden.

Beispielhaft sei an dieser Stelle das Phänomen des Access-as-a-Service (AaaS) herausgegriffen. Die Angreifer werden hier häufig als *Access Broker* bezeichnet. Sie erbeuten auf verschiedenste Weise Identitätsdaten oder Zugänge zu konkreten Computersystemen. Im Kontext von *Ransomware* treten insbesondere zwei Formen des AaaS auf: der Diebstahl von Identitäts- und Zugangsdaten über *Information Stealer* zum einen und die Kompromittierung von Netzwerken zum anderen.

**Diebstahl von Identitäts- und Zugangsdaten:** *Information Stealer* sind Schadprogramme, die Angreifer über E-Mails mit *maliziosen* Anhang oder Link auf einen schadcodebehafteten Webserver verteilen (sogenannter *Malware-Spam*). Darüber hinaus tarnen Angreifer *Information Stealer* als legitime Software, die sie im Internet zum Download anbieten. *Information Stealer* zielen darauf ab, verschiedenste Informationen auf einem kompromittierten System zu sammeln. Dazu zählen zum Beispiel in Browsern hinterlegte Zugangsdaten, etwaige Krypto-Wallets und Informationen weiterer Softwareprodukte, die Aufschluss über eine Person oder Zugang zu Vermögenswerten erlauben könnten. Diese Daten werden nach der Infektion eines Systems gesammelt und an den Angreifer ausgeleitet. Dieser zusammengestellte Datensatz wird als Log bezeichnet und zum Beispiel auf Untergrundmarktplätzen wie Russian Market, 2easy oder Genesis Market für 10 bis 60 US-Dollar pro Log verkauft. Die Logs enthalten überwiegend Identitätsdaten und können für Angriffe im Rahmen des Identitätsdiebstahls verwendet werden. Befinden sich in diesen Logs Zugangsdaten zu einem Firmennetz oder Session-Cookies einer Cloudanwendung, können diese für einen *Ransomware*-Angreifer ein Einfallstor in das entsprechende Netzwerk darstellen.

**Kompromittierung von Netzwerken:** Im Unterschied zu einem *Ransomware*-Angriff richtet ein *Access Broker* keinen unmittelbaren Schaden an. Sein Ziel ist es, einen anhaltenden Zugang in das kompromittierte Netzwerk zu schaffen. Dieser wird über Untergrundforen und private Kanäle zum Beispiel an *Ransomware*-Angreifer oder auch APT-Gruppen weiterverkauft. Gelingt es dem *Access Broker* dabei bereits, die erlangten Zugriffsrechte zu erweitern, steigt der Verkaufswert dieses Zugangs.

Noch bis in den vergangenen Berichtszeitraum hinein waren *maliziose* Office-Dokumente das häufigste Angriffsmittel für die initiale Infektion. Im Laufe des Jahres 2022 ersetzten Angreifer diese durch *maliziose* Container-Dateien mit Formaten wie ISO oder IMG. Opfer erhielten dabei zwar weiterhin E-Mails mit den *maliziosen* Anhängen oder Links zum Download der Anhänge, jedoch änderten die Angreifer die Auswahl dafür verwendeter Dateien. Grund dafür dürfte die standardmäßige Deaktivierung von Makros in Office-Produkten durch Microsoft gewesen sein.

Die Verwendung von *maliziosen* Container-Dateien war für Angreifer besonders Erfolg versprechend, da eine Schwachstelle dafür sorgte, dass das *Mark-of-the-Web* (MOTW, eine zusätzliche Schutzmaßnahme für Endgeräte) nicht an Dateien innerhalb des Containers weitergegeben wurde. Am 8. November 2022 wurde die Schwachstelle behoben. In der Folge wurden *maliziose* Container-Dateien in Angriffskampagnen seltener verwendet. Anfang 2023 wechselten die Angreifer dann mehrheitlich zu *maliziosen* OneNote-Dateien für *Spam*- und *Phishing*-Mails.

OneNote-Dateien sind so ausgestaltet, dass sie verschiedene andere Dateien enthalten können. Mit ähnlichen Methoden wie bei *maliziosen* Office-Dokumenten (zum Beispiel *Social Engineering*) können Opfer dazu verleitet werden, diese eingebetteten *maliziosen* Dateien auszuführen.

Neben dem Einsatz von *Spam*- und *Phishing*-Mails zur Verteilung von *Malware* kam es im Berichtszeitraum gehäuft zu *Callback-Phishing* sowie SEO Poisoning und Malvertising.

**Callback-Phishing:** Hierbei sendet der Angreifer eine fingierte Rechnung oder ein ähnliches Dokument, um das Opfer zum Anruf bei einem Callcenter unter der Kontrolle des Angreifers zu bewegen. Das Callcenter leitet das Opfer dann zum Download und zur Ausführung der *Malware* an.

**SEO Poisoning und Malvertising:** Beide Methoden setzen oftmals auf legitime Software als Deckmantel. So ahmen die Angreifer die Webseiten und Webdomains legitimer Softwareprodukte nach. Fällt ein Opfer hierauf herein, lädt es sich neben der legitimen Software auch eine *Malware* nach, die im Hintergrund ausgeführt wird, ohne dass das Opfer es bemerkt. SEO Poisoning kommt vom englischen Begriff für Suchmaschinenoptimierung (Search Engine Optimization, SEO). Dabei wird die Web-

seite des Angreifers über die Position in den Suchergebnissen einer Suchmaschine ausgespielt. Der Angreifer versucht deshalb, eine möglichst hohe Platzierung in den Suchergebnissen zu erreichen. Bei Malvertising, zusammengesetzt aus *Malware* und Advertising, wird *Malware* gemeinsam mit legitimen Werbeanzeigen ausgespielt. Ein Nutzer wird auch hier zum Download einer zumeist legitimen Software verleitet, die mit *Malware* kombiniert wurde. Darin besteht der Unterschied zu *Drive-by-Exploits*, bei denen allein das Besuchen einer Webseite zu einer Kompromittierung führt.

Grundsätzlich passen Angreifer ihre Vorgehensweise zeitnah an, wenn sich die Gegebenheiten ändern.

### Ransomware-as-a-Service

Die aktivsten und damit auch bedrohlichsten *Ransomware*-Familien wurden im Berichtszeitraum in Form von *Ransomware* als Dienstleistung (*Ransomware-as-a-Service*, *RaaS*) betrieben und angeboten. Insbesondere die *RaaS* LockBit 3.0 und die *RaaS* Alphv stechen heraus. Im Mittelpunkt stand die Entwicklung von exklusiven Services für besonders erfolgreiche *Affiliates*. Dabei werden den *Affiliates*, die hohe Provisionen an Lösegeldern einbringen, zusätzliche Dienstleistungen jenseits der *Ransomware* zur Verfügung gestellt.

Sowohl LockBit 3.0 als auch Alphv boten so zum Beispiel im Berichtszeitraum ausgewählten *Affiliates* zusätzliche *Ransomware*-Varianten an, die auf einem anderen Quellcode aufbauten und weitere Funktionen umfassten. Auch weiterführende Services wie *DDoS-Angriffe*, Unterstützung bei der Verhandlung oder exklusive *Access Broker* wurden von Betreibern einiger *RaaS* angeboten.

Cyberkriminelle Gruppen konkurrieren durchaus um ihre *Affiliates*, daher spielt in der Szene auch die Reputation der eigenen „Marke“ eine wichtige Rolle. Diese Art der Rivalität führt zu einer zunehmenden Verschärfung der Bedrohungslage. Ein entscheidendes Argument für einen *Affiliate* bei der Auswahl der *RaaS* ist beispielsweise, wie viel Druck auf einen Betroffenen ausgeübt werden kann. So führt der Konkurrenzkampf zwischen cyberkriminellen Gruppen zu einer Maximierung des Drucks auf betroffene Opfer. Andere Unterscheidungsmerkmale zwischen *RaaS*-Angeboten sind auch der Anteil am Lösegeld, der beim *Affiliate* verbleibt, oder die fortlaufende Verbesserung der *Ransomware* selbst. Zum einen können solche exklusiven Services die erfolgreichsten *Affiliates* längerfristig an eine *RaaS* binden. Zum anderen dürften diese

Services andere *Affiliates* dazu motivieren, aktiver zu werden oder höhere Lösegelder zu verlangen.

Bemerkenswert für die *RaaS* LockBit 3.0 war im Sommer 2022 die Einführung einer monetären Belohnung für das Auffinden von Schwachstellen (*Bug Bounty*) für die *RaaS* selbst. Ganz ähnlich zu legitimen Bug-Bounty-Programmen rufen die Angreifer dabei dazu auf, Schwachstellen in der *Ransomware* oder dem *RaaS*-Angebot oder auch die Möglichkeit von Rückschlüssen auf die Identität der Angreifer gegen die Auszahlung einer *Bounty* zu melden.

### Too big to stay afloat

Es zeigen sich also Parallelen zwischen der legalen Wirtschaft und der cyberkriminellen Schattenwirtschaft, die sich, getrieben durch *Ransomware*-Angriffe, in den vergangenen Jahren weiterentwickelt hat. So ähnelt die Aufteilung von Aspekten eines Angriffs wie *AaaS* und *RaaS* dem Outsourcing von Aufgaben an Dienstleister. Die Maximierung des Erpressungsdrucks dient den Angreifern auch dazu, möglichst hohe Lösegelder einzunehmen, was dem Streben nach Gewinn in der Wirtschaft in der Intention nicht unähnlich ist.

Unternehmen und Institutionen, die als zu groß oder zu wichtig gelten, um zu scheitern, werden gemeinhin als „too big to fail“ bezeichnet. Dazu gehörten zum Beispiel in der weltweiten Finanzkrise 2008 zahlreiche Banken, die nur mit staatlichen Hilfen vor der Insolvenz gerettet werden konnten. Im Gegensatz zu Unternehmen und Institutionen können cyberkriminelle Gruppen jedoch nicht „too big to fail“ werden. Sie werden stattdessen „too big to stay afloat“ (zu groß, um den Kopf über Wasser zu halten). Ist eine Gruppe von Cyberkriminellen erfolgreich, steigt ihre öffentliche Bekanntheit und damit auch die Aufmerksamkeit, die sie bei Sicherheitsfachleuten und Strafverfolgungsbehörden genießt. Daher war es bisher nur eine Frage der Zeit, bis solche Gruppen unschädlich gemacht werden konnten oder sich gezwungen sahen unterzutauchen. So wurde etwa Emotet im Januar 2021 erstmals abgeschaltet. Die *RaaS* DarkSide löste sich nach einem besonders erfolgreichen Cyberangriff auf und auch die *RaaS* REvil verschwand nach einem besonders erfolgreichen Angriff. Das „Conti-Syndikat“ zersplitterte im Mai 2022, mutmaßlich wegen unterschiedlicher Auffassungen zum russischen Angriffskrieg gegen die Ukraine.

### 4.1.3 – Schweigegeld-Erpressung mit Datenleaks und weitere Erpressungsmethoden

Seit 2021 gehen *Ransomware*-Angriffe in der Regel mit einem Datenleak einher. Dieses Vorgehen ist bekannt als Schweigegeld-Erpressung oder *Double Extortion*. Die Leak-Opfer-Statistik des BSI gibt Aufschluss über die Opfer von Schweigegeld-Erpressungen. 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. Durch die Veröffentlichung ihrer Daten auf einer Leak-Seite werden *Ransomware*-Opfer gleichsam zum zweiten Mal Opfer einer Cybererpressung.

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 Schweigegeld-Erpressungen. 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 Zwecke der Erpressung, ohne dass tatsächlich ein Angriff stattgefunden hat.

Mit der Beobachtung von Leak-Seiten wird nur ein Teil der *Ransomware*-Opfer erfasst. So werden in der Regel

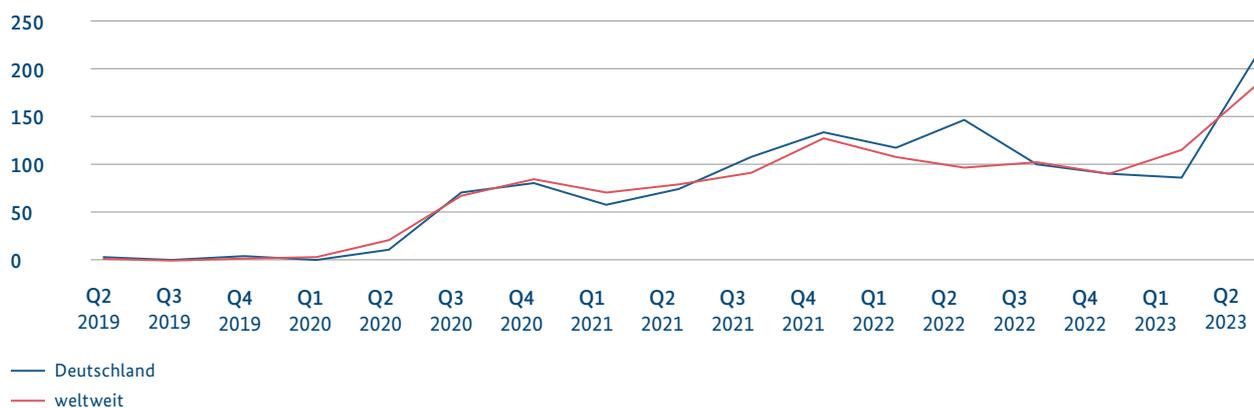
nur diejenigen Organisationen auf Leak-Seiten genannt und veröffentlicht, die die Zahlung eines Löse- oder Schweigegelds verweigern. Ein großes Dunkelfeld an *Ransomware*-Opfern verbleibt daher. Daher gibt diese Erfassung auch keinen Aufschluss darüber, wie viele der tatsächlichen Opfer sich zur Zahlung eines Löse- oder Schweigegeldes entscheiden. Zudem gibt der Zeitpunkt der Veröffentlichung keinen Aufschluss über den Zeitpunkt des *Ransomware*-Angriffs, der bereits lange zuvor stattgefunden haben kann. Die Kategorisierung der so erfassten mutmaßlichen Opfer nach Ländern ist darüber hinaus nur eine Annäherung, da sie in der Regel nach dem Standort der Hauptniederlassung des mutmaßlichen Opfers erfolgt. Das angegriffene Netzwerksegment kann sich daher insbesondere bei global agierenden Unternehmen auch in anderen Teilen der Welt befinden haben.

Die ersten Cyberangriffe mit Schweigegeld-Erpressung und Leak-Seiten wurden 2019 beobachtet. Im ersten Quartal 2019 griff die sich selbst „Team Snatch“ nennende cyberkriminelle Gruppe einige Opfer an. Im vierten Quartal 2019 begann die cyberkriminelle Gruppe hinter der *RaaS Maze*, *Ransomware*-Angriffe mit Leaks zu kombinieren.

Im Jahr 2020 setzte sich diese Vorgehensweise bei verschiedenen cyberkriminellen Gruppen durch, worüber das BSI als *Proliferation* cyberkrimineller Vorgehensweisen berichtete (vgl. Die Lage der IT-Sicherheit in Deutschland 2022). Mit dem Jahr 2021 wurden *Double-Extortion*-Angriffe zur Regel bei einem *Ransomware*-Angriff. Diese Entwicklung zeigte sich in der stetigen Zunahme bis ins vierte Quartal 2021.

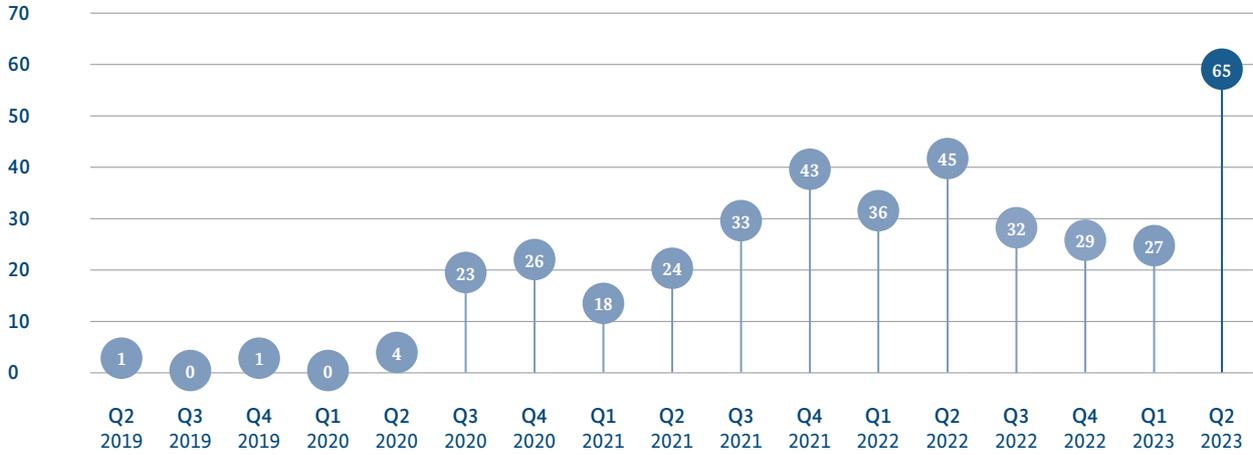
#### Mutmaßliche Opfer auf Leak-Seiten aus Deutschland und weltweit im Vergleich (2021 = 100)

Abbildung 2: Mutmaßliche Opfer auf Leak-Seiten aus Deutschland und weltweit im Vergleich (2021=100)  
Quelle: Leak-Opfer-Statistik des BSI



### Mutmaßliche Opfer aus Deutschland auf Leak-Seiten Anzahl

Abbildung 3: Mutmaßliche Opfer aus Deutschland auf Leak-Seiten (Anzahl)  
Quelle: Leak-Opfer-Statistik des BSI

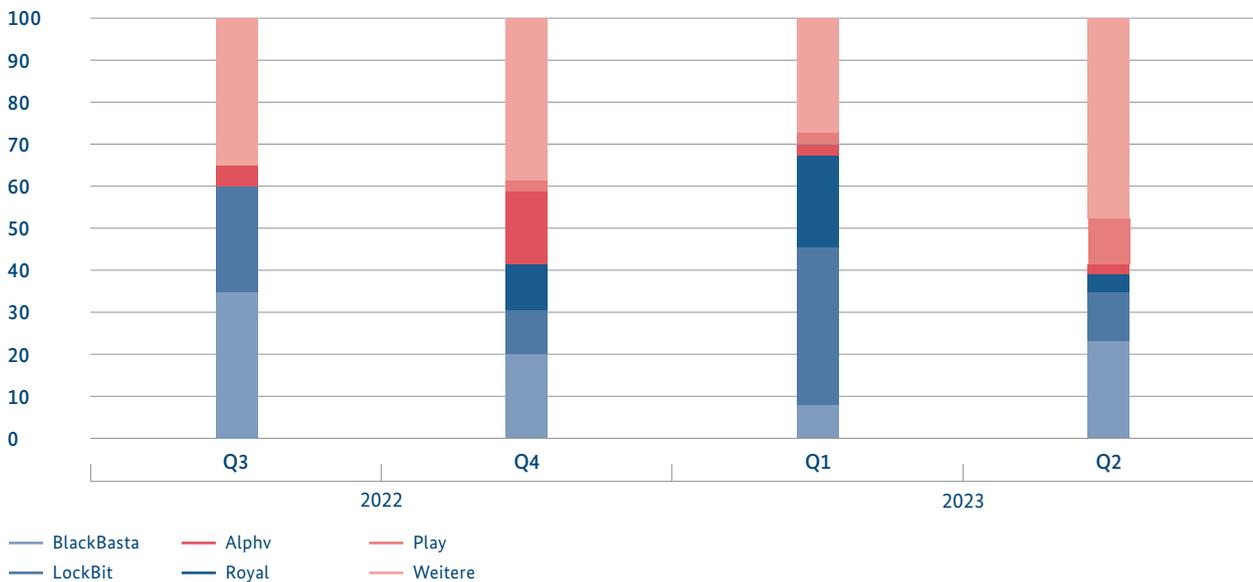


Mit 1.003 so erfassten mutmaßlichen Opfern weltweit im vierten Quartal 2021 und 45 Opfern aus Deutschland im zweiten Quartal 2022 waren die vorläufigen Höhepunkte der Zeitreihe erreicht. Sowohl bei der weltweiten Betrachtung als auch der Beschränkung auf die Deutschland zugeordneten Opfer ist in den folgenden Quartalen eine leichte Abnahme und anschließende Stabilisierung zu beobachten. Im zweiten Quartal 2023 war

dann die höchste Zahl an Leak-Opfern seit Beginn der Erfassung zu verzeichnen. Grund dafür waren zwei neue Leak-Seiten. MalasLocker war eine bislang einmalige Kampagne mit vermutlich hacktivistischem Hintergrund. Die Seite 8Base dagegen steht mit mindestens zwei Ransomware-Familien in Verbindung und dürfte sich etabliert haben.

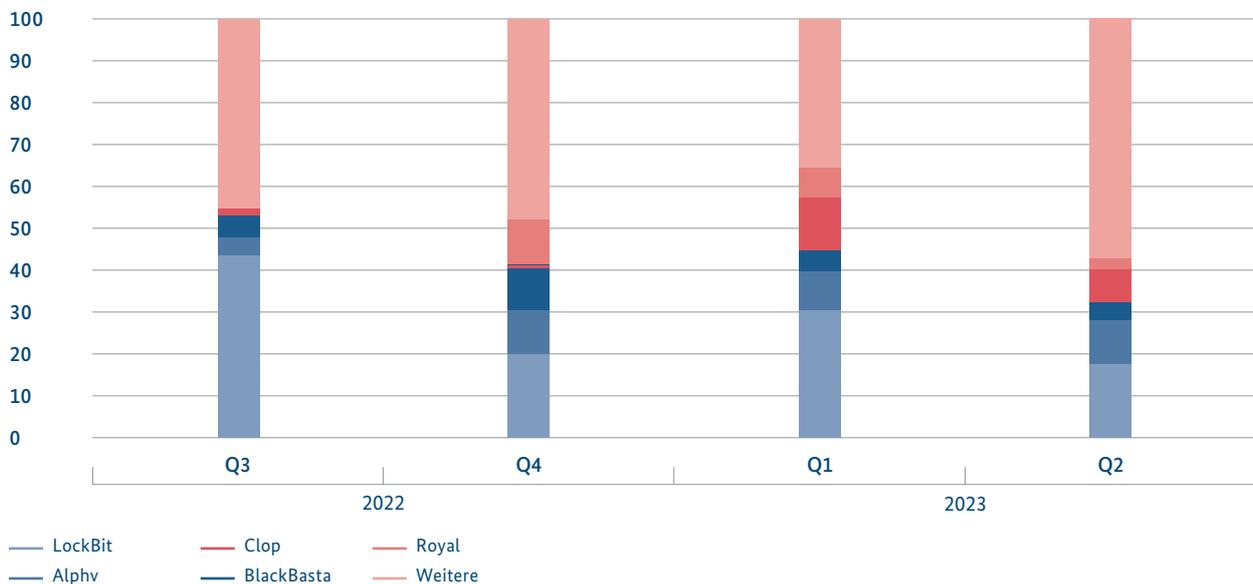
### Mutmaßliche Opfer aus Deutschland nach Leak-Seiten Anteile in %

Abbildung 4: Mutmaßliche Opfer aus Deutschland auf Leak-Seiten (Anteile)  
Quelle: Leak-Opfer-Statistik des BSI



## Mutmaßliche Opfer weltweit nach Leak-Seiten Anteile in %

Abbildung 5: Mutmaßliche Opfer weltweit nach Leak-Seiten (Anteile)  
Quelle: Leak-Opfer-Statistik des BSI



Die fünf aktivsten Leak-Seiten sind regelmäßig für rund 50 Prozent der mutmaßlichen Opfer verantwortlich. Die RaaS LockBit 3.0 ist sowohl bei der Beschränkung auf Deutschland (vgl. Abbildung 4) wie auch bei weltweiter Betrachtung (vgl. Abbildung 5) die aktivste Ransomware. Die Leak-Seite von LockBit nannte im Berichtszeitraum insgesamt über 800 weltweit verteilte mutmaßliche Opfer.

Die beiden RaaS Black Basta und Royal werden in der IT-Sicherheitscommunity als eine Art Nachfolger der aufgelösten RaaS Conti beobachtet. Beide RaaS sind erst 2022 in Erscheinung getreten und haben sich schnell unter den Top 5 der aktivsten Ransomware-Familien platziert.

Die RaaS Alphv (auch bekannt als BlackCat) wurde erstmals im November 2021 beobachtet und zählt mit LockBit zu einer der bedrohlichsten Ransomware-Familien. Im Jahr 2023 nahm die cyberkriminelle Gruppe Vice Society Platz 5 der Rangliste ein. Bemerkenswert an Vice Society ist, dass diese Gruppe keine eigene Ransomware entwickelte, sondern die Ransomware anderer RaaS verwendet.

Neben den oben beschriebenen Lösegeld- und Schweigegeld-Erpressung flankieren Angreifer die Verhandlungen mit dem Opfer häufig durch zusätzliche Erpressungsmethoden, um den Zahlungsdruck zu erhöhen. Verglichen mit vergangenen Berichtszeiträumen sind

diese weiteren im Folgenden beschriebenen Erpressungsmethoden weitestgehend unverändert geblieben (vgl. Die Lage der IT-Sicherheit in Deutschland 2022). Lediglich die Angreifer hinter der RaaS Alphv versuchten im aktuellen Berichtszeitraum in Einzelfällen eine neue Erpressungsmethode. Dabei stellten die Angreifer Daten der Betroffenen über das offene Internet in durchsuchbarer Form auf einer Webseite zur Verfügung. Dies erlaubte jeder Nutzerin und jedem Nutzer des Internets Zugriff auf die Daten. Eine Ausbreitung und Übernahme dieser Methode durch andere Angreifer ist möglich, konnte bislang jedoch noch nicht durch das BSI beobachtet werden.

**Erregung öffentlicher Aufmerksamkeit:** Einige Angreifer gehen aktiv auf Kundinnen und Kunden des Opfers oder die Öffentlichkeit zu, um zusätzlichen Druck auszuüben. Dies geht über die Veröffentlichung von Opferinformationen auf dafür eingerichteten Leak-Seiten hinaus. Beispielsweise wenden sich Angreifer per E-Mail an Kundinnen und Kunden oder Mitarbeitende eines Opfers und informieren diese darüber, dass aufgrund eines nicht gezahlten Schweigegelds sensible Daten über sie öffentlich wurden. Insbesondere bei einem intransparenten Umgang des Opfers mit dem Datenleak kann dies den Ruf des Opfers langfristig schädigen. Eine pflichtgemäße Meldung an zuständige Datenschutz- oder Regierungsbehörden kann die negativen Auswirkungen begrenzen (vgl. Kapitel *Erkenntnisse zur Gefährdungslage in der Gesellschaft*, Seite 51).

**Verkauf oder Veröffentlichung sensibler Daten:** Ist der Betroffene nicht bereit zu zahlen, versteigern oder verkaufen einige Angreifer erbeutete Daten an Dritte. Mit diesen Daten können die Käufer ihrerseits das Opfer erpressen. Dies gilt insbesondere dann, wenn es sich um wertvolle Geschäftsgeheimnisse oder kompromittierende Informationen über Einzelpersonen handelt. An wen solche Daten letztendlich versteigert werden, lässt sich in der Regel nicht mehr feststellen. Finden die Angreifer keinen Käufer, so veröffentlichen sie die Daten auf einer dafür vorgesehenen Leak-Seite. Daten, die einmal abgeflossen sind, gelten selbst im Fall einer erfolgten Schweigegeld- oder Lösegeldzahlung grundsätzlich dauerhaft als kompromittiert.

Abseits der Kombination dieser Erpressungsmethode mit *Ransomware* im Rahmen der *Double Extortion* beobachtet das BSI auch Leak-Seiten von Angreifern, die ihre Opfer ohne den Einsatz von *Ransomware* erpressen. Dabei kompromittieren die Angreifer die Opfer auf dieselbe Weise wie bei einem *Ransomware*-Angriff, verzichten jedoch auf den Einsatz von *Ransomware*. Das BSI nimmt an, dass die Angreifer dadurch schneller von der initialen Infektion zur Erpressung eines Schweigegelds übergehen können.

**Androhen einer Meldung bei der zuständigen Datenschutz- oder Regulierungsbehörde:** Im Zusammenhang mit einem Cyberangriff können Betroffene gegen die Datenschutz-Grundverordnung oder andere Regulierungen verstoßen, wenn sie beispielsweise ihren Meldepflichten nicht nachkommen oder nachweisbar ist, dass sensible Daten zum Beispiel auf schlecht abgesicherten Webservern lagen. Solche Sorgfaltspflicht- oder Meldepflichtverletzungen seitens der Opfer nutzen einige Angreifer als Druckmittel zweiter Ordnung. Sie drohen, die Regulierungsbehörden über den Verstoß zu informieren. Da der Angriff sowie kompromittierte Daten auch über andere Wege öffentlich werden können, sollten Betroffene Gesetzesverstöße vermeiden, indem sie frühzeitig und pflichtgemäß eine Meldung abgeben.

**Einsatz von DDoS-Angriffen in der Verhandlungsphase:** Einzelne Angreifer setzen während der Verhandlung eines Lösegelds zusätzlich *DDoS-Angriffe* ein, um das Opfer weiter unter Druck zu setzen. Diese Angriffe können zusätzliche Incident-Response-Maßnahmen erfordern und damit auch die Reaktion auf den *Ransomware*-Angriff behindern.

## 4.1.4 – Maßnahmen

Lösegeldzahlungen bieten grundsätzlich keine Garantie für die Freigabe verschlüsselter Daten. Sie tragen zudem dazu bei, dass sich kriminelle Organisationen und Schattenwirtschaften professionalisieren und wachsen. Daher empfiehlt das BSI, auf Lösegeldzahlungen zu verzichten. Wichtiger ist es, wirksame Vorkehrungen gegen *Ransomware*-Angriffe zu treffen.

### 4.1.4.1 – Schutzmaßnahmen nach Angriffsphasen

Ein *Ransomware*-Angriff besteht aus mehreren Schritten (vgl. Kapitel *Angriffsablauf*, Seite 15). Für jede Phase eines solchen Angriffs sind Gegenmaßnahmen möglich, um das Eindringen in Netzwerke oder das Verschlüsseln von Daten zu verhindern und möglichen Schaden zu begrenzen. Diese Maßnahmen werden der jeweiligen Angriffsphase zugeordnet dargestellt.

#### Angriffsphase 1 – Einbruch

Die drei häufigsten Einfallsvektoren von *Ransomware*-Gruppen sind *Malware-Spam* oder Links auf schadcodebehaftete Server, die Ausnutzung von Schwachstellen sowie der Zugriff über schlecht abgesicherte externe Zugänge. Für jedes dieser Einfallstore existieren wirksame Maßnahmen.

#### Gegenmaßnahme *Malware-Spam*: E-Mails und Sensibilisierung

Empfangene E-Mails sollten grundsätzlich als „Nur-Text“ oder „reiner Text“ codiert angezeigt werden. Dies kann durch die Endnutzerin und den Endnutzer oder die Systemadministratorin oder den Systemadministrator entsprechend eingerichtet werden. Im Gegensatz zur Darstellung als „HTML-Mail“ werden in der Darstellung als Nur-Text-Mails keine eventuell enthaltenen Makros oder versteckten Befehle ausgegeben. Zudem lassen sich Webadressen nicht mehr verschleiern. In einer HTML-codierten Mail könnte zum Beispiel ein Link mit der Bezeichnung „www.bsi.de“ in Wahrheit auf eine schadcodebehaftete Webseite verweisen. Ist eine Nur-Text-Codierung nicht möglich oder nicht erwünscht, sollte zumindest die Ausführung aktiver Inhalte in HTML-Mails unterdrückt werden, damit *maliziöse* Skripte nicht mehr ausgeführt werden können.

Mitarbeitende sollten im Rahmen von Sensibilisierungsmaßnahmen praxisnah bzgl. der Risiken im Umgang mit E-Mails geschult werden. Das gilt besonders für Mitarbeitende aus Behörden- und Unternehmensbereichen, die ein hohes Aufkommen an externer E-Mail-Kommunikation (etwa in der Personalabteilung oder im Marketing) zu bewältigen haben.

#### **Gegenmaßnahme Schwachstellen: Patches und Updates**

Um Infektionen zu vermeiden, die auf der Ausnutzung von Schwachstellen beruhen, für die es bereits Sicherheitsupdates gibt, sollten diese Updates nach der Bereitstellung durch den Softwareanbieter unverzüglich in die IT-Systeme eingespielt werden – über die zentrale Softwareverteilung des Netzwerks idealerweise auch in alle Desktop-Computer und Notebooks, die zum Firmennetzwerk gehören. Updates, die Schwachstellen von hoher Kritikalität schließen oder sich auf besonders exponierte Software wie Firewalls oder Webserver beziehen (oder beides), sollten priorisiert behandelt werden.

#### **Gegenmaßnahme Remote-Zugang: Multifaktor-Authentifizierung (MFA)**

Häufig versuchen Cyberkriminelle, *Ransomware* über kompromittierte Remote-Zugänge auf Systemen zu installieren. Daher sollte auch der Zugriff von außen abgesichert werden – normalerweise über Virtual Private Networks (VPNs) in Kombination mit einer Multifaktor-Authentifizierung.

#### **Angriffsphase 2 – Rechteerweiterung**

**Gegenmaßnahme: Administrator-Accounts absichern**  
Grundsätzlich sollten mit privilegierten Accounts nur Administratorentätigkeiten durchgeführt werden. Das Lesen von E-Mails oder das Surfen im Internet gehören nicht dazu. Administratorinnen und Administratoren sollten sich für solche Tätigkeiten, die keine erweiterten Zugriffsrechte erfordern, auch zusätzliche Nutzerkonten mit begrenzten Rechten anlegen. Privilegierte Konten sollten immer über eine Multifaktor-Authentifizierung geschützt sein. Zudem sollten für die Administration von Clients keine Domänen-Administrationskonten verwendet werden.

#### **Angriffsphase 3 – Ausbreitung**

##### **Gegenmaßnahme: Netzwerk segmentieren**

Eine saubere Netzwerksegmentierung hilft, Schäden zu begrenzen, da eine eventuell eingeschleuste *Ransomware*

zunächst nur die Systeme im jeweiligen Segment erreichen kann. Auch dafür ist die sichere Verwendung von Administrator-Accounts notwendig.

#### **Angriffsphase 4 – Datenabfluss**

##### **Gegenmaßnahme: Anomalie-Detektion**

Durch eine Anomalie-Detektion im Netzwerk ist es möglich, zeitnah einen potenziell unerwünschten Datenabfluss zu erkennen. Hierfür ist es nötig, den regulär anfallenden Netzwerkverkehr sehr gut zu kennen. Auf Basis dieses Normalzustands können dann Schwellenwerte gewählt werden, bei deren Über- oder Unterschreitung das System anschlägt. Auch können hierbei die Zeitzone und der Standort berücksichtigt werden. Außerhalb der regulären Arbeitszeiten für einen Betriebsstandort sollten die Schwellenwerte anders sein als während des regulären Betriebs.

#### **Angriffsphase 5 – Verschlüsselung**

##### **Gegenmaßnahme: Backups und Datensicherung**

*Backups* sind der beste Schutz vor den Auswirkungen einer Verschlüsselung durch *Ransomware*, denn sie gewährleisten die unmittelbare Verfügbarkeit von Daten auch für diesen Fall. Dafür müssen die Daten aber in einem *Offline-Backup* gesichert werden, das nach einem *Backup* von den übrigen Systemen des Netzwerkes getrennt wird. Erst dann sind sie vor Angriffen und Verschlüsselung geschützt. Zu einem *Backup* gehören immer auch die Planung und Vorbereitung des Wiederanlaufs und der Wiederherstellung der Daten. Dies sollte regelmäßig getestet werden, um Komplikationen und Herausforderungen bei der Wiederherstellung bereits vor einem Ernstfall zu erkennen.

#### **Angriffsphase 6 – Incident Response**

##### **Gegenmaßnahme: Notfallplan**

Für das Worst-Case-Szenario eines erfolgreichen Angriffs, bei dem alle Systeme im Netzwerk verschlüsselt wurden, sollte eine Notfallplanung für Notbetrieb und Wiederaufbau existieren. Die Prozesse zur Reaktion und Wiederherstellung geschäftskritischer Systeme sollten in regelmäßigen Abständen geübt werden. Insbesondere müssen vorab die geschäftskritischen Systeme identifiziert werden und alternative Kommunikationsmöglichkeiten außerhalb des kompromittierten Netzwerkes vorbereitet sein. Telefonnummern und Daten von wichtigen Kontaktpersonen sollten offline in Papierform vorgehalten werden.

#### 4.1.4.2 – Unterstützung durch das BSI

Das BSI kann im Rahmen seines gesetzlichen Auftrags bestimmte Betroffene bei der Bewältigung von IT-Sicherheitsvorfällen unterstützen. Die gesetzlich definierten Zielgruppen des BSI sind

- die Betreiber von Kritischen Infrastrukturen (gemäß BSI-Kritisverordnung – BSI-KritisV),
- Institutionen der Bundesverwaltung / Stellen des Bundes,
- Unternehmen im besonderen öffentlichen Interesse.

In begründeten Einzelfällen kann das BSI auch bei solchen Institutionen tätig werden, die nicht zu den drei genannten Zielgruppen zählen. Ein begründeter Einzelfall liegt insbesondere dann vor, wenn es sich um einen Angriff von besonderer technischer Qualität handelt, die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems von besonderem öffentlichem Interesse ist oder eine wichtige Stelle eines Landes betroffen ist.

Die Vorfallsbearbeitung im BSI wird federführend durch die Fachreferate des *CERT-Bund* durchgeführt. Dabei wird im Bedarfsfall auch auf die gesamte Expertise des BSI zurückgegriffen. Dazu zählen Expertinnen und Experten aus den Bereichen Forensik und *Malware-Reverse-Analyse*, Incident Response (Mobile Incident Response Team (MIRT)), Cybersicherheit in Industrieanlagen, Detektion (Bundes Security Operations Center, BSOC) und Betriebssysteme sowie Penetrationstesterinnen und -tester.

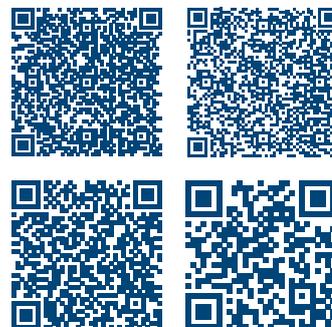
Über das im BSI angesiedelte Nationale Cyber-Abwehrzentrum (Cyber-AZ) können bei Bedarf auch weitere Sicherheitsbehörden zum Austausch, zur Bewertung oder zur Bearbeitung von Cybersicherheitsvorfällen hinzugezogen werden.

Das Nationale IT-Lagezentrum führt zusammen mit dem *CERT-Bund* eine Erstbewertung einer Vorfallsmeldung durch. Dazu wird in der Regel eine sogenannte Triage-Besprechung mit den Betroffenen durchgeführt. In dieser Besprechung werden ein gemeinsames Verständnis des Vorfalls erarbeitet sowie mögliche Maßnahmen diskutiert. Darauf aufbauend werden dann die geeigneten weiteren Maßnahmen vereinbart.

Das BSI bietet eine Vielzahl an Produkten und Dokumenten an, die Betroffenen sowohl präventiv als auch im Rahmen der Vorfallsbearbeitung reaktiv zur Verfügung

gestellt werden können. Dazu zählen zum Beispiel Dokumente zur Prävention, Detektion und Reaktion bei APT-Vorfällen, Hilfsdokumente für die Vorfallsbearbeitung bei schweren IT-Sicherheitsvorfällen wie *Ransomware*-Vorfällen und viele mehr.

Weitere Informationen und Hilfsdokumente:<sup>c</sup>



Das BSI kann Behörden und Unternehmen zudem hinsichtlich des koordinierten und strukturierten Vorgehens bei Sicherheitsvorfällen, der Umsetzung von geeigneten Maßnahmen, der Durchführung eines angemessenen IT-Krisenmanagements und der passenden Krisenkommunikation beraten.

In besonders herausgehobenen Fällen kann das BSI einen Vor-Ort-Einsatz mit einem Mobile Incident Response Team (MIRT) durchführen. Das MIRT kann das Opfer in einer Vielzahl von Bereichen unterstützen, so zum Beispiel bei der Erstbewertung, bei der Grobanalyse und Abschätzung der Konsequenzen sowie bei der Sichtung von Protokoll-daten und Alarmen. Darüber hinaus kann das BSI auch im Rahmen der technischen Beweissicherung tätig werden, wie zum Beispiel bei der Erstellung von Festplatten-Images oder der Aufzeichnung von Netzwerkverkehr sowie bei der technischen Analyse im Backoffice, und das lokale Betriebspersonal bei der Bereinigung beratend unterstützen. Weiterhin können Empfehlungen zur Härtung der Systeme gegen Cyberangriffe gegeben werden.

Das BSI kann Opfer nicht nur mit der eigenen Expertise unterstützen, sondern auch bei der Suche nach geeigneten Incident-Response-Dienstleistern helfen. Hierfür hat das BSI eine entsprechende Liste qualifizierter Dienstleister veröffentlicht. Alle darauf befindlichen Dienstleister wurden anhand der vom BSI festgelegten Kriterien auf ihre Kompetenz beim Umgang mit schwerwiegenden IT-Sicherheitsvorfällen überprüft und konnten sich entsprechend qualifizieren.

Die Liste der qualifizierten Dienstleister finden Sie hier:<sup>d</sup>



## 4.2 – *Advanced Persistent Threats* und Bedrohungen im Kontext des Ukraine-Kriegs

*Advanced Persistent Threats* (APT) unterscheiden sich von anderen Bedrohungen der Cybersicherheit durch die Motivation und die Vorgehensweise der Angreifer. Während zum Beispiel Schadprogramme von kriminellen Angreifern in der Regel massenhaft und ungezielt verteilt werden (vgl. Kapitel *Ransomware*, Seite 14), sind APT-Angriffe oft langfristig und mit großem Aufwand geplante Angriffe auf einzelne ausgewählte, herausgehobene Ziele. APT-Angriffe dienen nicht der kriminellen Gewinnerzielung, sondern der Beschaffung von Informationen über das Ziel und gegebenenfalls der Sabotage.

### Beobachtungen aus Cyberoperationen in der Ukraine

Im aktuellen Berichtszeitraum gab es eine Reihe von Entwicklungen, die die APT-Bedrohungslage prägten. So entstand durch den russischen Angriffskrieg auf die Ukraine erstmalig die Situation, dass ein Staat mit ausgeprägten Cyberfähigkeiten in einem bewaffneten Konflikt mit einem anderen hoch digitalisierten Staat stand. Zu beobachten war in diesem Zusammenhang eine große Bandbreite an Phänomenen im Cyberraum, darunter Cyberspionage, Hacking, Desinformation einschließlich Veröffentlichung gestohlener Daten sowie Cybersabotage. Dies ermöglichte erstmals einen empirischen Blick auf die Rolle von Cyberfähigkeiten in einem Krieg zwischen einem Aggressor und einem Partnerstaat Deutschlands.

**Cybersabotage:** Für die Bedrohungslage ist stets relevant, welche Arten von Zielen angegriffen werden. So haben sich die Angreifer in der Ukraine bei der Cybersabotage nicht auf Kritische Infrastrukturen im engeren Sinne beschränkt. Stattdessen wurden in der Ukraine vergleichsweise breitflächig in verschiedenen Sektoren und Branchen Sabotageakte durchgeführt. Zum Einsatz kam dabei *Wiper*-Schadsoftware, die Daten löscht. Diese Schadprogramme waren für Sabotage in normalen Büronetzen ausgelegt. Nur in einem Fall wurden Spezial-Schadprogramme wie *Industroyer2* für Prozesssteuerungsanlagen entdeckt, und zwar im ukrainischen Energiesektor, konkret bei Angriffsversuchen auf Umspannwerke in der Ukraine. Der Angriffsversuch auf die Umspannwerke ereignete sich erst einige Monate nach Kriegsbeginn. Dagegen wurde als eines der ersten Ziele – nämlich am Tag des Überfalls – ein Satelliten-Kommunikationsbetreiber angegriffen, der laut Medienberichten Dienste für das ukrainische Militär erbrachte (vgl. Die Lage der

IT-Sicherheit in Deutschland 2022). Seitdem liegen kaum Berichte über Cyberangriffe auf militärische Systeme vor, was allerdings auf eine unvollständige Informationslage zurückzuführen sein dürfte.

**Cyberspionage:** Eine weitere wesentliche Erkenntnis ist, dass die Cybersabotage gegen ukrainische Ziele auf wenige Angreiferguppen beschränkt war. Es waren im Berichtszeitraum zwar weitere Gruppen in der Ukraine aktiv, die jedoch größtenteils auf Informationsbeschaffung zielten. Diese Arbeitsteilung dürfte weniger technische Gründe als vielmehr organisatorische oder strategische Gründe gehabt haben.

Um *Malware* überhaupt einsetzen zu können, werden *Angriffsvektoren* benötigt. Mehrere öffentlich dokumentierte Fälle belegen, dass in der Anfangszeit des Kriegs von den Angreifern kompromittierte Netzwerkzugänge genutzt wurden, die bereits vor dem Krieg bestanden. Es wurden keine technisch neuen *Angriffsvektoren* wie zum Beispiel neue Schwachstellen oder neue Supply-Chain-Angriffe beobachtet.

### Hacking und Desinformationskampagnen in Deutschland und anderen westlichen Staaten

Ein Phänomen, das im Zusammenhang mit dem russischen Angriffskrieg gegen die Ukraine in Deutschland größere Medienaufmerksamkeit erhielt, ist prorussischer *DDoS*-Hacking, der allerdings nur begrenzte Schädigung entfaltete (vgl. zum *DDoS*-Hacking Kapitel *Distributed Denial of Service*, Seite 28). Proukrainischen Hacking gab es in wenigen Fällen, vor allem zu Beginn des Kriegs, als ein deutsches Unternehmen mit Verbindungen nach Russland kompromittiert wurde (vgl. Die Lage der IT-Sicherheit in Deutschland 2022).

Anders als *DDoS*-Hackern, die lediglich mit begrenzter Schädigung Internetdienste vorübergehend beeinträchtigen können, dringen Cyberspione oder -saboteure tief in IT-Netze ein, um Daten zu vernichten oder zu leaken. Dies ist ein Vorgehen, das zukünftig weiteres Potenzial für Angreifer bietet, denn je nach Sensibilität der gestohlenen Daten können diese in Desinformationskampagnen genutzt werden, um die öffentliche Meinung zu beeinflussen. Das wachsende Gruppengeflecht von Hackern wird es zudem in Zukunft auch staatlich gesteuerten Angreiferguppen zunehmend ermöglichen, sich als Hackern auszugeben.

Weiterhin waren Operationen zu beobachten, bei denen durch *Phishing*- oder *Malware*-Einsatz gewonnene Infor-

mationen für Desinformation genutzt wurden. Während dies in osteuropäischen Staaten wie Polen und im Baltikum für die Gruppe Ghostwriter bereits vor dem Krieg bekannt war, hat die Gruppe Callisto seit Beginn des Ukraine-Kriegs solche Operationen Berichten von Sicherheitsbehörden und Sicherheitsfirmen zufolge auch in Großbritannien durchgeführt. Aufgrund des heterogenen IT-Sicherheitsniveaus bei deutschen politischen Einrichtungen und Medien könnten solche Fälle von Datenleaks auch in Deutschland auftreten.

Jenseits des Kriegs in der Ukraine gab es weitere Entwicklungen im Cyberraum, die die Anstrengungen von Angreifergruppen zeigten, ihre Angriffe zu verschleiern und zu optimieren.

### Anonymisierungsnetze als Dienstleistung für APT-Gruppen

Prägnant ist die Etablierung mehrerer *Botnetze* aus Routern, *IoT*-Geräten und Virtual-Private-Servern, die von APT-Gruppen für unbefugte Zugriffe aus dem Internet (Scans, *Exploit*-Anwendung und *Webshell*-Zugriffe) betrieben werden. Diese *Botnetze* dienen der Anonymisierung des Angriffsverkehrs, vergleichbar mit legitimen Proxy-Serversystemen. Damit verstetigt sich eine Entwicklung, die bereits im vergangenen Berichtszeitraum

beobachtet wurde: Es werden zunehmend Server angegriffen, die direkt aus dem Internet erreichbar sind. Es werden also nicht mehr nur Angriffsmails versandt, sondern vermehrt bestehende Schwachstellen in Webservern, Firewalls oder *VPN*-Servern ausgenutzt. Um diese Systeme auszukundschaften und dann zu kompromittieren, benötigen die Angreifer anonymisierte Internetverbindungen, die sie über die neu geschaffenen *Botnetze* selbst ermöglichen.

### Überblick über relevante APT-Gruppen

Für deutsche Ziele stellten im Berichtszeitraum mindestens die in Tabelle 1 benannten APT-Gruppen eine Bedrohung dar. Die Gruppen sind in der Regel vor allem gegen Ziele in den angegebenen Sektoren aktiv. Institutionen, die bereits Basis-IT-Sicherheitsmaßnahmen umgesetzt haben, sollten Berichte über die folgenden Gruppen priorisiert auswerten. Die aufgeführten typischen Angriffstechniken beziehen sich allerdings auf die erste Phase eines Angriffs und sind daher nicht vollständig. Zudem agieren manche der Gruppen sehr vielseitig, sodass auch andere Techniken in der initialen Angriffsphase zum Einsatz kommen können.

APT-Gruppe	Bevorzugte Ziele	Bevorzugte Techniken
APT15   VixenPanda   Mirage   Ke3chang	Regierungseinrichtungen   NGOs	<i>Exploits</i> gegen aus dem Internet erreichbare Systeme
APT27   Emissary Panda   LuckyMouse	Energie   Telekommunikation   Pharma	<i>Exploits</i> gegen aus dem Internet erreichbare Systeme
APT28   FancyBear   Sofacy	Regierungseinrichtungen   Militär   Medien   NGOs	<i>Exploits</i> gegen aus dem Internet erreichbare Systeme
APT29   Nobelium   DiplomaticOrbiter	Regierungseinrichtungen	Mails mit Archivdaten als Anhang, die LNK-Dateien enthalten
APT31   JudgementPanda   ZIRCONIUM	Regierungseinrichtungen   NGOs	<i>Exploits</i> gegen aus dem Internet erreichbare Systeme; Bruteforcing
Ghostwriter bzw. Untergruppe UNC1151	Politik   NGOs   Medien	Mails mit Links auf <i>Phishing</i> -Seite
Kimsuky   VelvetChollima	Rüstung   Kanzleien	Word-Dokumente, die makrobehafete Remote Templates nachladen; <i>Social Engineering</i>
Lazarus   SilentChollima	Rüstung   Luftfahrt	Mails mit Archivdaten als Anhang, die trojanisierte Anwendungen enthalten; <i>Social Engineering</i>
MustangPanda (oder VertigoPanda)	Regierungseinrichtungen	Mails mit Archivdaten als Anhang, die LNK-Dateien enthalten
Snake   VenomousBear   Turla	Regierungseinrichtungen   Export	<i>Exploits</i> gegen aus dem Internet erreichbare Systeme
UNC2589	Logistik	Mails mit makrobehafeten Dokumenten im Anhang

Tabelle 1: Für Deutschland relevante APT-Gruppen  
Quelle: BSI

## Supply-Chain-Angriff infolge eines anderen Supply-Chain-Angriffs

### Sachverhalt

In einem spektakulären Einzelfall gelang einer APT-Gruppe ein Supply-Chain-Angriff, der durch einen vorhergehenden erfolgreichen Supply-Chain-Angriff ermöglicht wurde. Am 29. März 2023 berichteten mehrere IT-Sicherheitsunternehmen, dass Detektionen und Logdateien bei ihren Kunden auf einen Supply-Chain-Angriff hindeuten, der auf einen Anbieter im Bereich Voice-over-IP-Kommunikation (VoIP-Kommunikation) für Geschäftskunden mit mehreren Hunderttausend Kunden zielte. Es stellte sich heraus, dass mehrere vom Hersteller signierte Installationspakete einer VoIP-Software für Windows und MacOS eine manipulierte Softwarebibliothek enthielten und ausführten. Diese versuchte in mehreren Schritten, einen Command-und-Control-Server zu kontaktieren und weiteren Schadcode herunterzuladen. Diese Installationspakete waren offiziell vom Hersteller bereitgestellt und signiert, sodass von einem Supply-Chain-Angriff, also von einer erfolgreichen Kompromittierung des Herstellers, ausgegangen werden konnte. Der CEO des Anbieters bestätigte

in der Folge in einem Forenbeitrag die Medienberichte und den erfolgreichen Angriff auf das eigene Unternehmen.

Eine mit der Untersuchung des Vorfalls beauftragte Sicherheitsfirma fand Folgendes heraus: Der ursprüngliche Angriffsvektor für die Kompromittierung des Anbieters für VoIP-Kommunikation war die Installation einer anderen legitimen Software für Finanz-Transaktionen. Diese Finanz-Software, die ein Schadprogramm enthielt, hatte der Anbieter von der Webseite ihres Herstellers heruntergeladen. Es hatte also bereits ein Angriff auf den Hersteller der Finanz-Transaktionssoftware stattgefunden, sodass es zu einer Verkettung von Supply-Chain-Angriffen kam: Zuerst wurde das Unternehmen für Finanz-Software angegriffen und dessen legitime Software um ein Schadprogramm ergänzt. Diese legitime, aber schadprogramm-behaftete Software wurde dann bei dem Anbieter für VoIP-Kommunikation installiert, wodurch wiederum dessen Software um ein Schadprogramm ergänzt wurde, was Ende März 2023 bei dessen Kunden detektiert wurde.

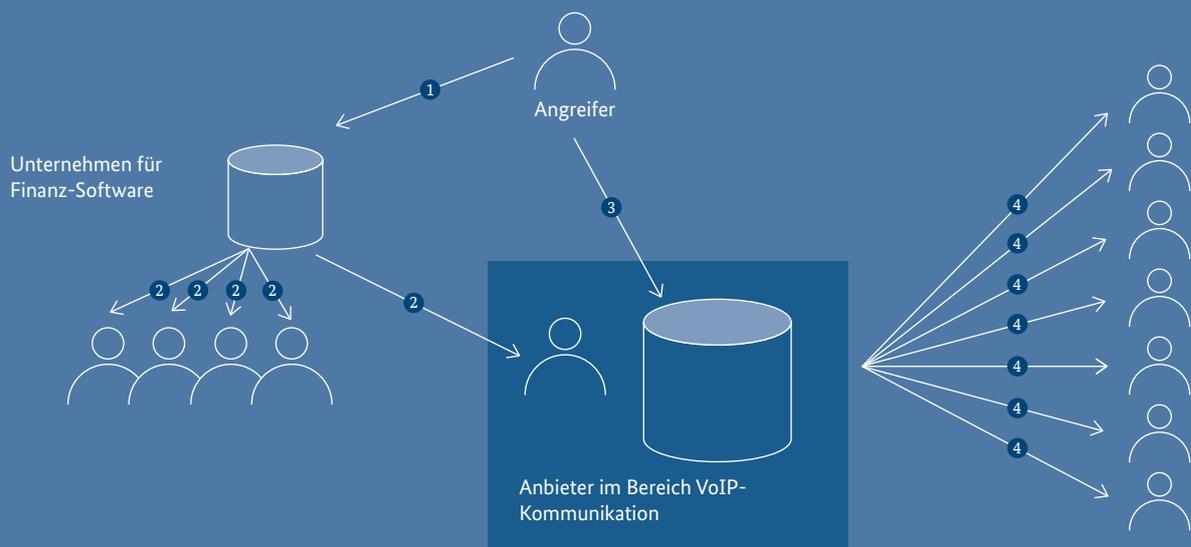


Abbildung 6: Supply-Chain-Angriff infolge eines Supply-Chain-Angriffs

1. Angreifer infiltriert Hersteller einer Software für Finanztransaktionen und kompromittiert legitime Software.
2. Opfer laden kompromittierte Software für Finanztransaktionen herunter, darunter ein Mitarbeiter eines Anbieters von VoIP-Software.
3. Angreifer kompromittiert VoIP-Software, um den Angriff auf eine Vielzahl potenzieller weiterer Opfer ausweiten zu können.
4. Weitere Opfer laden die kompromittierte VoIP-Software herunter.

**Bewertung**

Ein Supply-Chain-Angriff hat das Potenzial, eine Vielzahl von Opfern gleichzeitig zu kompromittieren. Maßnahmen wie die Signierung von Softwarepaketen und der Download von offiziellen Webseiten greifen hier nicht, da der Angreifer in der Lage ist, sein Schadprogramm bereits im Produktionsprozess der Software zu verankern, sodass dieses wie offizieller Programmcode signiert und bereitgestellt wird.

Die mehreren Hunderttausend Kunden im vorliegenden Fall zeigen eindrucksvoll das Potenzial eines solchen Angriffs. Möglich wären hier Ransomware-Angriffe oder Spionage bei den Kunden, wobei die tatsächliche Motivation hinter dem beschriebenen Fall bisher unklar ist. Hervorzuheben ist die Verkettung verschiedener Supply-Chain-Angriffe wie in diesem Fall: Sie zeigt, dass Angreifer willens und in der Lage sind, Zugänge sehr detailliert zu analysieren, über einen längeren Zeitraum zu beobachten und abzuwägen, ob diese Zugänge systematisch und

mit hohem Aufwand für Folgeangriffe genutzt werden können.

Laut öffentlicher Berichterstattung wird der Angriff dem Subcluster „Labyrinth Chollima“ zugeordnet, einem Teil der häufig als Lazarus bezeichneten APT-Gruppen.

**Reaktion**

Nach Bekanntwerden des Angriffs hat der Anbieter für VoIP-Kommunikation die Deinstallation der betroffenen Softwareversionen empfohlen und bereinigte Installationspakete bereitgestellt. Das BSI hat seine Zielgruppen ebenfalls gewarnt. Weiterhin wurde die Infrastruktur zum Nachladen weiterer Schadsoftware schnell blockiert, sodass die Infektionskette in diesem Fall frühzeitig unterbrochen werden konnte. Im Nachgang ist der Hersteller transparent mit dem Vorfall umgegangen und hat über den Stand der Untersuchungen und deren Ergebnisse informiert.

### 4.3 – Distributed Denial of Service

Denial-of-Service-Angriffe (DoS-Angriffe) sind Angriffe auf die Verfügbarkeit von Internetdiensten. Häufig sind Webseiten Ziel solcher Angriffe. Die zugehörigen Webserver werden dabei so mit Anfragen überflutet, dass die Webseiten nicht mehr erreichbar sind. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem Distributed-Denial-of-Service-Angriff (DDoS-Angriff).

Angreifer verfolgen mit DDoS-Angriffen unterschiedliche Ziele. Zum einen kann es sich auch um eine in den Cyberraum übertragene Form der Schutzgelderpressung handeln. Angreifer fordern dabei Geld vom Opfer, um die Angriffe zu stoppen. Auch im Rahmen eines Ransomware-Vorfalles kann DDoS eingesetzt werden, um den Druck auf das Opfer zu erhöhen und ein Lösegeld für verschlüsselte Daten zu erpressen. Zum anderen können Angreifer DDoS-Angriffe auch nutzen, um Institutionen direkt zu schaden. Gründe können zum Beispiel Wettbewerb unter konkurrierenden Unternehmen

oder Aktivismus sein (zum Beispiel durch sogenannte Script-Kiddies). Ein DDoS-Angriff kann weiterhin auch genutzt werden, um von einem anderen, anspruchsvolleren Angriff wie etwa Ransomware (vgl. Kapitel Ransomware, Seite 14) oder APT (vgl. Kapitel Advanced Persistent Threats und Bedrohungen im Kontext des Ukraine-Kriegs, Seite 25) abzulenken. Im Rahmen des russischen Angriffskriegs gegen die Ukraine kam es darüber hinaus international auch zu politisch motivierten DDoS-Angriffen, die unter das Phänomen des Hacktivismus fallen.

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, wenn im Fall von Hacktivismus kritische Dienstleistungen und Webseiten beispielsweise von Banken oder der Polizei in ihrer Verfügbarkeit beeinträchtigt werden.

Die Anzahl der bekannt gewordenen DDoS-Angriffe in Deutschland wird durch einen Index gemessen (vgl.

## Bekannt gewordene DDoS-Angriffe (Messzahl) in Deutschland 2021=100

Abbildung 7: Bekannt gewordene DDoS-Angriffe  
(Messzahl) in Deutschland (2021=100)  
Quelle: DDoS-Statistik des BSI

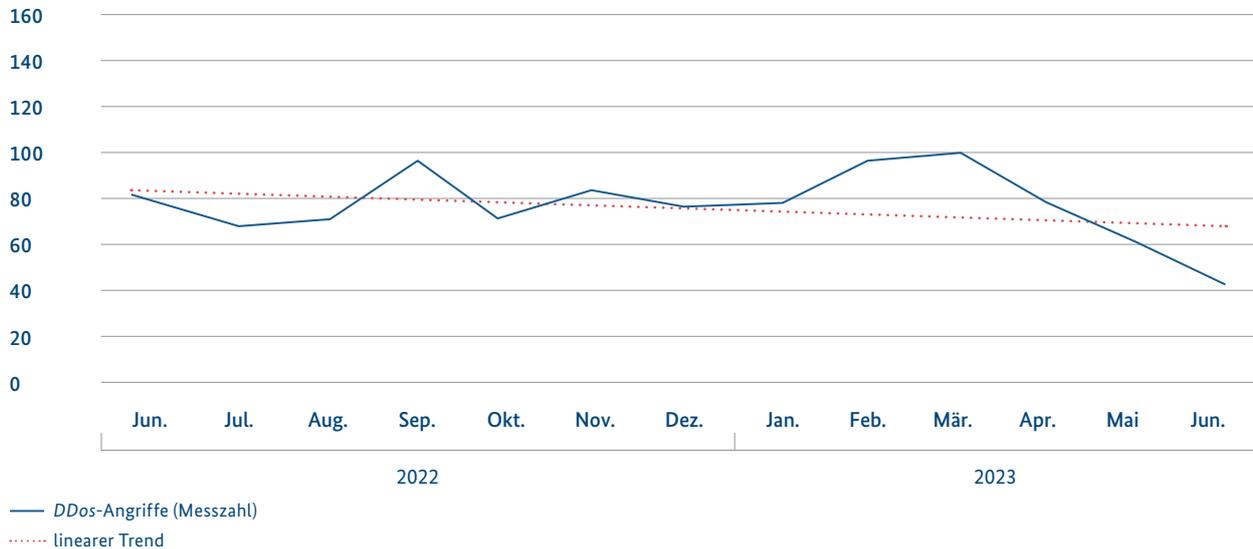


Abbildung 7). Ein Index von beispielsweise 95 Punkten im Februar 2023 bedeutet, dass die Anzahl der DDoS-Angriffe in Deutschland im Februar 0,95-mal so hoch war wie im Jahresdurchschnitt 2021.

Der Indikator zeigt im September 2022 sowie im Frühjahr 2023 DDoS-Angriffe prorussischer Hacktivistinnen in Deutschland an, die insgesamt nur geringe Schadwirkungen entfalteten und auch zahlenmäßig hinter den Häufigkeiten von kriminellen DDoS-Angriffen in früheren Berichtszeiträumen zurückblieben. Im Gegensatz zu Ransomware- oder APT-Angriffen können Angreifer mit DDoS keine Netzwerke hacken oder kapern, sondern lediglich Internetdienste vorübergehend beeinträchtigen. Es ist daher davon auszugehen, dass das Interesse des DDoS-Hacktivismus in Deutschland nicht darin bestand, tatsächlich umfangreichen materiellen Schaden anzurichten. Vielmehr dürfte das Ziel der Angreifer darin bestanden haben, gesellschaftliche Verunsicherung zu schüren und das Vertrauen in die Fähigkeiten des Staates zum Schutz und zur Versorgung der Bevölkerung zu beschädigen.

Im Gegensatz zum vergangenen Berichtszeitraum war im aktuellen Berichtszeitraum keine Steigerung von DDoS-Angriffen an absatzstarken Aktionstagen wie dem Black Friday, dem Cyber Monday oder auch dem Vorweihnachtsgeschäft zu erkennen. Insgesamt ist in der zweiten

Jahreshälfte 2022 die Anzahl der DDoS-Angriffe im Vergleich zur ersten Jahreshälfte 2022 deutlich zurückgegangen. Nach den hacktivistischen Kampagnen im ersten Quartal 2023 setzte sich im zweiten Quartal 2023 der schon länger zu beobachtende rückläufige Trend cyberkrimineller DDoS-Angriffe fort.

Im Dezember 2022 gelang den Strafverfolgungsbehörden ein Schlag gegen DDoS-as-a-Service-Angebote: Europol berichtete über die Abschaltung von etwa 50 Webseiten, die Dienste für gezielte DDoS-Angriffe anboten. Einer dieser Dienste soll für über 30 Millionen DDoS-Angriffe weltweit verantwortlich gewesen sein. Mehrere Administratoren der Webseiten konnten festgenommen werden. An der Aktion waren Behörden aus den USA, dem Vereinigten Königreich, den Niederlanden, Deutschland und Polen beteiligt.<sup>1</sup>

**Informationen zu DDoS-Prävention und -Mitigation sowie eine Liste qualifizierter Dienstleister für DDoS-Mitigation finden Sie hier:<sup>e</sup>**



---

## DDoS-Hackivismus

---

### Sachverhalt

Im Zuge des russischen Angriffskriegs gegen die Ukraine formierten sich verschiedene Gruppierungen pro-russischer Hacktivistinnen, die DDoS-Angriffe auch gegen deutsche Ziele durchführten. Im Sommer 2022 machte so die Hacktivistinnen-Gruppe Killnet von sich reden (vgl. Die Lage der IT-Sicherheit in Deutschland 2022). Zudem rief die Gruppe NoName057 das Projekt „DDoSia“ ins Leben. Dabei handelt es sich um ein Botnetz, das gezielt für hacktivistische Angriffe aufgebaut wurde. Im Herbst 2022 begannen die Anbieter von DDoSia mit der Anwerbung von Affiliates, die das Botnetz für Angriffe auf Internetdienste westlicher Behörden verwenden sollten. Potenziellen Affiliates wurde eine Geldprämie in Aussicht gestellt.

Die verschiedenen Hacktivistinnen-Gruppen zeichnen für zahlreiche DDoS-Angriffe auch in Deutschland verantwortlich; darunter auf Webseiten und Internetportale von Flughäfen, Polizeien und Landesregierungen. Kennzeichnend für die Angriffe ist, dass die Gruppierungen diese jeweils vorher öffentlichkeitswirksam auf ihren Social-Media-Kanälen ankündigten. Auf der Zielliste des DDoSia-Projekts befanden sich beispielsweise Webdienste mehrere Landespolizeien und Institutionen der Bundesländer. Aufgeführt wurden dabei Webseiten der Polizeien in Brandenburg, NRW, Niedersachsen, Bremen, Hessen, Mecklenburg-Vorpommern,

Rheinland-Pfalz sowie Landesdomains des Saarlands oder Sachsen-Anhalts. Darüber hinaus wurden auch Webseiten von Bundesbehörden sowie die Webseite [www.ukraine-wiederaufbauen.de](http://www.ukraine-wiederaufbauen.de) angegriffen.

### Bewertung

Die genannten Angriffe entfalteten nur begrenzte Schadwirkung. Grund dafür ist, dass DDoS-Angriffe generell keine tiefere Infiltration von Netzwerken oder nachhaltige Schäden ermöglichen, wie sie etwa durch Datenverschlüsselung entstehen. Sie können aber zu kurzzeitigen Ausfällen oder verlangsamtem Aufruf von Webseiten für einen begrenzten Zeitraum führen. Solche Angriffe lassen sich durch die Aktivierung entsprechender DDoS-Schutzmechanismen wirksam mitigieren.

Es ist daher davon auszugehen, dass das Ziel der Angreifer darin bestand, gesellschaftliche Verunsicherung zu schüren und das Vertrauen in demokratische Institutionen sowie in die Fähigkeiten des Staates zum Schutz und zur Versorgung der Bevölkerung zu beschädigen.

### Reaktion

Das BSI informierte die zuständigen Landes-CERTs über die Erkenntnisse und stand während der gesamten Zeit im direkten Austausch mit den Landes-CERTs.

## 4.4 – Spam und Phishing

Eine unerwünschte E-Mail bezeichnet man im Allgemeinen als *Spam*. Häufig wird *Spam* über kompromittierte oder angemietete Server versandt. Gleichermaßen können gestohlene E-Mail-Adressen hierfür ausgenutzt werden, die ursprünglich einem legitimen Account gehörten. Hinzu kommt, dass weitere mit dem Internet verbundene Systeme infiziert werden können, um diese für *Spam*-Dienstleistungen zu missbrauchen. Beispielsweise können IoT-Geräte und Geräte zur privaten Heimautomatisierung als Teile eines *Botnetzes* zusammenschaltet und missbraucht werden.

*Spam* lässt sich in unterschiedliche Kategorien aufteilen. Dabei wird unterschieden zwischen unerwünschtem,

aber im Grunde unschädlichem Werbe-*Spam* (28 %) und schädlichen Cyberangriffen, darunter Erpressungs- (34 %) und Betrugsmails (32 %). Wesentliches Unterscheidungsmerkmal ist, dass im Rahmen erpresserischer Nachrichten gedroht wird, vermeintliches oder tatsächliches Wissen über das Opfer weiterzugeben, und auf diesem Weg ein Schweigegeld gefordert wird. Das geschieht meistens unabhängig davon, ob ein echtes Erpressungspotenzial in Form von Informationen vorliegt. Demgegenüber wird beim Betrug ein Handlungsbedarf im Namen einer Institution oder Person vorgetäuscht, ohne dabei ein Schweigegeld zu erpressen. Ziel dabei ist es, sensible persönliche Daten abzufangen, um diese weiterzuverkaufen oder für eigene kriminelle Tätigkeiten zu verwenden.

Im Bereich der E-Mails mit betrügerischem Hintergrund nehmen *Phishing*-Mails den größten Anteil ein (84 %).

### Spam im Berichtszeitraum nach Art des Spam Anteile in %

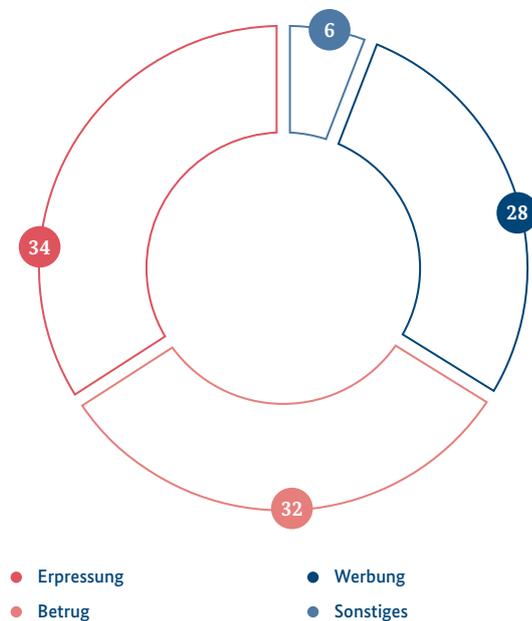


Abbildung 8: Spam im Berichtszeitraum nach Art des Spam  
Quelle: E-Mail-Verkehrsstatistik des BSI

Diese Nachrichten zielen darauf ab, das Opfer mittels Social-Engineering-Techniken dazu zu bringen, seine Identitäts- beziehungsweise Authentisierungsdaten offenzulegen.

Weitere Angriffsvariationen lassen sich anhand des für den Angriff gewählten Kanals unterscheiden. Hier sind insbesondere Smishing (*Phishing* per SMS) und Vishing (*Voice Phishing*) hervorzuheben. Smishing 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. Dagegen wird beim Vishing 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.

### Schwerpunkt- und Beobachtungsthemen im Bereich *Phishing* und Spam

Wie an den geschilderten *Phishing*-Techniken deutlich wird, nutzen Kriminelle meist bestimmte Themen aus, mit denen sie ihre Opfer erreichen wollen. Den meisten Betrugsversuchen lässt sich eine monetäre Motivation zuschreiben. Das führt dazu, dass vor allem im Bereich *Finance-Phishing* der größte Anteil an versendeten Spam-Nachrichten zu finden ist. Hierbei werden *Phishing*-E-Mails verschickt, die mit entsprechendem Corporate Design vorgeben, von bekannten Banken oder Finanzdienstleistern zu stammen. Ziel ist es, bei Verbraucherinnen und Verbrauchern einen vermeintlichen Handlungsbedarf zu suggerieren. Angeblich drohende Kontensperrung, notwendige Verifikation des Onlinebankings oder ausstehende Zahlungen sind dabei nur einige wenige Beispiele, mit denen Betroffene dazu gebracht werden sollen, ihre Zahlungs- und Accountdaten preiszugeben. Ergänzend dazu beobachtet das BSI *Phishing*-Kampagnen rund um die Themen Krypto-Wallets und FinTechs.

Gesellschaftliche Krisensituationen und Großereignisse im Berichtszeitraum boten den Kriminellen weitere Möglichkeiten für *Phishing* und Scam. Die angespannte Situation auf dem Energiemarkt im Winter 2022/23 sowie die von der Regierung beschlossenen Entlastungspakete führten zu *Phishing*-Nachrichten mit Betreffzeilen wie „Energiepauschale jetzt sichern!“ und „Wir überweisen Ihre Energiepauschale“. Angreifer gaben sich hier als Energieanbieter oder Teil der Regierung selbst aus und wollten die finanzielle Notsituation von Verbraucherinnen und Verbrauchern ausnutzen. Daneben trat vermehrt Charity-Scam im Namen von Hilfsorganisationen auf, die zum Beispiel Hilfeleistungen im Kontext des Kriegs in der Ukraine sowie des Erdbebens in der Türkei und Syrien versprachen. Hier sollte bei Verbraucherinnen und Verbrauchern das Gefühl einer emotionalen Betroffenheit geweckt werden, um im Rahmen von gefälschten Spendenaufrufen über Social Media oder E-Mail Geld einzutreiben.

Die Nutzung von großen KI-Sprachmodellen zur Verbesserung der Qualität von *Phishing*- und Scam-Angriffen ist eine weitere und zunehmende Herausforderung (vgl. Kapitel *Große KI-Sprachmodelle*, Seite 40). Durch den technologischen Fortschritt und die zunehmende Verfügbarkeit von KI-Systemen besteht die Gefahr, dass diese missbraucht werden. Dies führt zum Beispiel dazu, dass *Phishing*-Nachrichten authentischer gestaltet werden. Außerdem wird Sprache besser imitiert und klingt menschlicher. Auch der Einsatz von Chatbots, die

Gesprächsabläufe authentischer imitieren können, verleitet zur Preisgabe von Informationen und Daten.

## 4.5 – Angriffe im Kontext Kryptografie

Kryptografische Mechanismen sind wichtige Bausteine für die Umsetzung von Sicherheitsfunktionen in IT-Produkten. Dem Stand der Technik entsprechende Kryptgorithmen 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 gemeinhin als sicher angesehen werden.

### Die Technische Richtlinie TR-02102:<sup>f</sup>



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
- nicht ausreichend geschütztes Schlüsselmaterial

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 zum einen geeignete Verfahren ausgewählt und korrekt implementiert werden. Zum anderen muss sichergestellt sein, dass das an der Netzwerkschnittstelle beobachtbare Verhalten (z. B. Antwortzeiten eines Servers) keine Informationen über verarbeitete Geheimnisse preisgibt.

Bei der Absicherung von Kryptosystemen, die selbst Angreifern in räumlicher Nähe standhalten sollen, müssen weitere Seitenkanäle (z. B. Stromverbrauch oder elektromagnetische Abstrahlung der Geräte) berücksichtigt werden, über die ebenfalls Geheimnisse abfließen können. Die Seitenkanalanalyse, also die Analyse auf Anfälligkeit für *Seitenkanalangriffe*, ist heute ein eigener Forschungszeitweig, der neben Gegenmaßnahmen auch neue *Angriffsvektoren* hervorgebracht hat. Der im Info-Kasten HERTZBLEED (Seite 33) beschriebene Angriff nutzt einen neuartigen Seitenkanal in modernen Prozessoren aus, bei dem Unterschiede im Stromverbrauch zu unterschiedlichen Laufzeiten führen. Dieser Angriff demonstriert, dass Seitenkanäle, die eigentlich einen physischen Zugriff voraussetzen, in manchen Situationen auch durch einen entfernten Angreifer ausgenutzt werden können.

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 Schlüssel-erzeugung 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 zum Schema AIS 20 und AIS 31 Funktionalitätsklassen von Zufallszahlengeneratoren für verschiedene Einsatzzwecke. Ein neuer Entwurf der mathematisch-technischen Anlage der AIS 20/31 wurde im September 2022 veröffentlicht.

Die Sicherheitsgarantien vieler heute eingesetzter Kryptalgorithmen gelten allerdings nicht mehr, sobald ein hinreichend leistungsstarker Quantencomputer zur Verfügung steht. Das Kapitel Quantentechnologien (Seite 74) zeigt Möglichkeiten auf, dieser Bedrohung zu begegnen, und stellt die Aktivitäten des BSI in diesem Bereich dar.

## 5. – Schwachstellen

Um Computersysteme infiltrieren zu können, benötigen Angreifer Schwachstellen in der IT-Infrastruktur, die für einen Angriff ausgenutzt werden können. Ein Schadprogramm, das 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.



## HERTZBLEED – Timing-Angriff auf SIKE durch Taktfrequenz-Seitenkanal in Prozessoren

Der Stromverbrauch eines Prozessors hängt im Allgemeinen von den Daten ab, die in den Registern des Prozessors verarbeitet werden. Durch Messungen des Stromverbrauchs können somit Rückschlüsse auf die verarbeiteten Daten gezogen und, im Falle kryptografischer Operationen, auch Erkenntnisse über verarbeitete Geheimnisse gewonnen werden. Um den Stromverbrauch und die Wärmeentwicklung zu reduzieren, passen einige Prozessoren ihre Taktfrequenz dynamisch an. Eine solche Anpassung der Taktfrequenz beeinflusst wiederum die Laufzeit der vom Prozessor durchgeführten Berechnungen. Die Laufzeit einer Berechnung kann dadurch auch von den verarbeiteten Daten abhängen. Dieser neuartige Timing-Seitenkanal wurde im sogenannten HERTZBLEED-Angriff ausgenutzt, der im Juni 2022 veröffentlicht wurde.

In der Publikation von HERTZBLEED<sup>2</sup> wurde die Abhängigkeit der Taktrate von den verarbeiteten Daten

beschrieben, systematisch untersucht und experimentell verifiziert. Im Weiteren haben die Forschenden demonstriert, dass ein entfernter Angreifer durch Ausnutzung solcher Timing-Informationen den geheimen Schlüssel des Schlüsselaustauschverfahrens SIKE (Supersingular Isogeny Key Encapsulation) vollständig bestimmen kann. Wohlbemerkt waren die angegriffenen SIKE-Implementierungen dabei gegen bislang bekannte Timing-Angriffe gehärtet.

SIKE galt im Standardisierungsprozess für Post-Quanten-Verfahren des National Institute of Standards and Technology (NIST) lange Zeit als aussichtsreicher Kandidat. Durch einen im Juli 2022 veröffentlichten Angriff von Castryck und Decru<sup>3</sup> wurde SIKE aber letztendlich vollständig kryptoanalytisch gebrochen. Das Kapitel Quantentechnologien (Seite 74) enthält nähere Informationen zur Post-Quanten-Kryptografie und zum NIST-Auswahlprozess.

Schwachstellen entstehen beispielsweise durch Fehler in der Programmierung, durch schwache Default-Einstellungen von IT-Produkten im Produktivbetrieb oder auch durch fehlerkonfigurierte Sicherheitseinstellungen. IT-Systeme werden immer komplexer und die Produktionsbedingungen immer arbeitsteiliger und modularer, sodass Schwachstellen sehr verbreitet sind. Sie können daher auch sowohl in Betriebssystemen und Anwendungen (vgl. Kapitel *Schwachstellen in Softwareprodukten*, Seite 33) als auch in Hardware (vgl. Kapitel *Schwachstellen in Hardwareprodukten*, Seite 39) auftreten. Mit der Ausweitung des *Internet of Things* treten zunehmend auch Schwachstellen in vernetzten Geräten auf (vgl. Kapitel *Schwachstellen in vernetzten Geräten*, Seite 39).

Wenn eine Schwachstelle in einem IT-Produkt entdeckt wird, stellen Hersteller in der Regel Sicherheitsupdates (sog. *Patches*) bereit, um die Schwachstelle zu schließen und deren Ausnutzung für Cyberangriffe zu verhindern. Ein strukturiertes *Patchmanagement* ist daher eine der wichtigsten Präventivmaßnahmen, um den Risiken der Digitalisierung erfolgreich zu begegnen.

### 5.1 – 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 Angreifenden somit maximale Anonymität und Flexibilität aus der Ferne.

Im Berichtszeitraum wurden durchschnittlich täglich 68 neue Schwachstellen bekannt, rund 24 Prozent mehr als im vergangenen Berichtszeitraum. Es wurden also insgesamt knapp 27.000 neue Schwachstellen in jeglicher Art von Softwareprodukten bekannt, von spezialisierten Fachanwendungen über komplexe Serverinfrastrukturen bis hin zu Handy-Apps. Wie schon in den vergangenen Jahren wirkte sich auch im aktuellen Berichtszeitraum die zunehmende Modularisierung und Arbeitsteilung bei der Softwareproduktion auf die Bedrohungslage aus. Denn wenn eine Schwachstelle in einer Softwarekomponente bekannt

wird, die in einer Vielzahl verschiedener Anwendungen eingesetzt wird, kann solch eine einzelne Schwachstelle für Cyberangriffe gegen alle diese Anwendungen ausgenutzt werden.

Die im Berichtszeitraum bekannt gewordenen Schwachstellen unterschieden sich hinsichtlich ihrer Kritikalität sowie hinsichtlich der Schäden, die Angreifer durch Ausnutzung der Schwachstellen bewirken können. Für die Quantifizierung der Schadwirkungen wird im Folgenden die Common Weakness Enumeration (CWE-Klassifikation) herangezogen, eine von der IT-Sicherheitscommunity gepflegte Auflistung verschiedener Typen von Schwachstellen in Hard- und Software. Die Kritikalität wird anhand des Common Vulnerability Scoring System (CVSS-Score) gemessen.

**Schadwirkung:** Die Ausführung von unautorisierten Programmcodes oder Befehlen ist eine der wichtigsten Schadwirkungen. Rund 47 Prozent der im Berichtszeitraum bekannt gewordenen Schwachstellen eigneten sich dafür. Sie ermöglichten beispielsweise die initiale Erstinfektion bei einem *Ransomware*-Angriff (vgl. Kapitel *Angreifer-motivation und Angriffsablauf*, Seite 15). Viele Schwachstellen ermöglichten Angreifern auch, Sicherheitsvorkehrungen zu umgehen (40 %). Mit jeweils 20 Prozent der Schwachstellen konnten Angreifer Speicher sowie Anwendungsdaten manipulieren, um zum Beispiel die erlangten Zugriffsrechte zu erweitern. Und rund 40 Prozent ermöglichten schließlich das Auslesen von Daten. Solche Daten können Angreifer einerseits für Cybererpressungen nutzen (vgl. Kapitel *Schweigegeld-Erpressung mit Datenleaks und weitere Erpressungsmethoden*, Seite 19), andererseits auch an andere Angreifer weiterverkaufen, die diese Daten dann ihrerseits für Cyberangriffe verwenden können. Darüber hinaus konnte jede dritte im Berichtszeitraum bekannt gewordene Schwachstelle für einen *DoS*-Angriff genutzt werden.

**Kritikalität:** Die Kritikalität einer Schwachstelle ergibt sich jedoch nicht nur aus den möglichen Schadwirkungen, die Angreifer damit erzielen können. In den CVSS-Score, einen international anerkannten Industriestandard, mit dem die Kritikalität von Schwachstellen international vergleichbar bewertet wird, fließen auch *Angriffsvektoren* und andere Faktoren ein. Die Kritikalität der bekannt gewordenen Schwachstellen schwankte stark. Gut drei Prozent wiesen niedrige und 45 Prozent mittlere Scoring-Werte auf der zehnstufigen Skala auf (vgl. Abbildung 10). Mit 53 Prozent mehr als die Hälfte wiesen hohe (7–9) oder kritische (9–10) CVSS-Scores auf. Der Anteil kritischer Schwachstellen lag bei rund 15 Prozent. Wie im vorigen

Berichtszeitraum waren die häufigsten *Angriffsvektoren* Cross-Site Scripting (13 %), Out-of-Bounds Write (8 %) und SQL-Injection (7 %).

Nicht jede Schwachstelle ist für Angriffe einfach ausnutzbar. Eine Schwachstelle in einer lokalen Anwendung ohne Verbindung zum Internet kann beispielsweise lediglich durch einen lokalen Angreifer ausgenutzt werden. Dagegen können beispielsweise Schwachstellen in Softwareprodukten, die direkt aus dem Internet erreichbar sind, leichter und von einer höheren Anzahl von Cyberkriminellen für Angriffe missbraucht werden. Von den 13.500 Schwachstellen mit hohem oder kritischem CVSS-Score im Berichtszeitraum war knapp die Hälfte (49 %) leicht für Cyberangriffe ausnutzbar. Im Cyberraum findet ein ständiger Wettlauf zwischen Sicherheitsforschenden und den verschiedenen Angreifergruppierungen statt: Wer Schwachstellen zuerst entdeckt, kann diese entweder für Cyberangriffe nutzen oder im Darknet anderen Angreifern zum Kauf anbieten oder sie dem Hersteller melden, um die Bereitstellung eines *Patches* voranzutreiben.

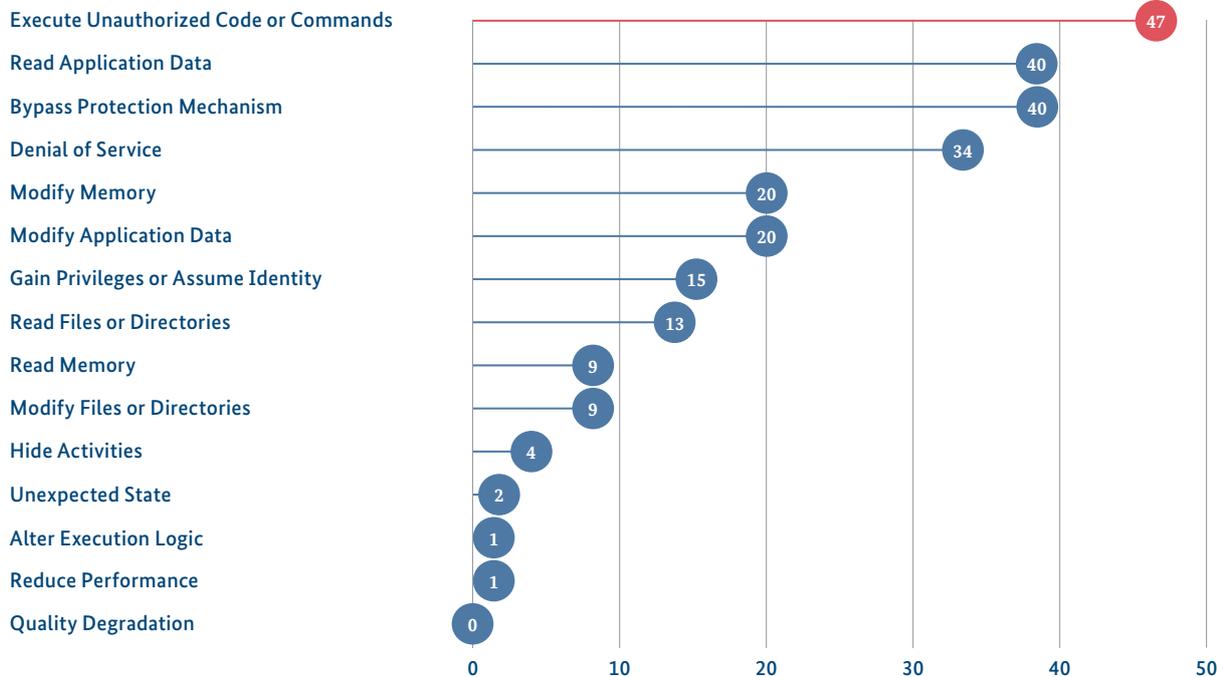
Im Berichtszeitraum hat das BSI monatlich durchschnittlich rund 20 Meldungen von Sicherheitsforschenden über schwachstellenbehaftete Softwareprodukte erhalten und nach dem System des Open Web Application Security Project (OWASP) klassifiziert. Während CWE und CVSS die Schwachstellen selber beschreiben, erlaubt OWASP eine Beschreibung des schwachstellenbehafteten Produkts. Demnach wiesen mit rund 21 Prozent der Meldungen die meisten gemeldeten Produkte im Berichtszeitraum Fehlkonfigurationen auf (Security Misconfiguration, vgl. Abbildung 36). Dazu zählen zum Beispiel eine fehlende Sicherheitshärtung des Produkts, unnötige Features wie etwa offene Ports, Zugriffsrechte oder Services oder auch unveränderte Default Accounts aus der Entwicklungsphase. In rund 18 Prozent der gemeldeten Fälle ermöglichte das schwachstellenbehaftete Produkt Angreifern das Einschleusen von Schadcode (Injection), weil Benutzereingaben von der Software nicht validiert, gefiltert oder bereinigt wurden. An dritter Stelle folgten im Ranking mit 13 Prozent Softwareprodukte ohne funktionierende Zugangskontrollen (Broken Access Control). Sie verletzten das Prinzip der standardmäßigen Verweigerung des Zugangs und erlaubten ohne weitere Zugangskontrolle jeglichem Nutzer den Zugriff, ermöglichten die Umgehung von Zugriffskontrollen oder gewährten authentifizierten Benutzern die Verwendung der Software mit Administratorrechten. Rund 13 Prozent

## Bekannt gewordene Schwachstellen nach möglicher Schädwirkung (Top 10)\*

Anteile in %

Abbildung 9: Bekannt gewordene Schwachstellen nach Schädwirkung  
Quelle: Schwachstellenstatistik des BSI

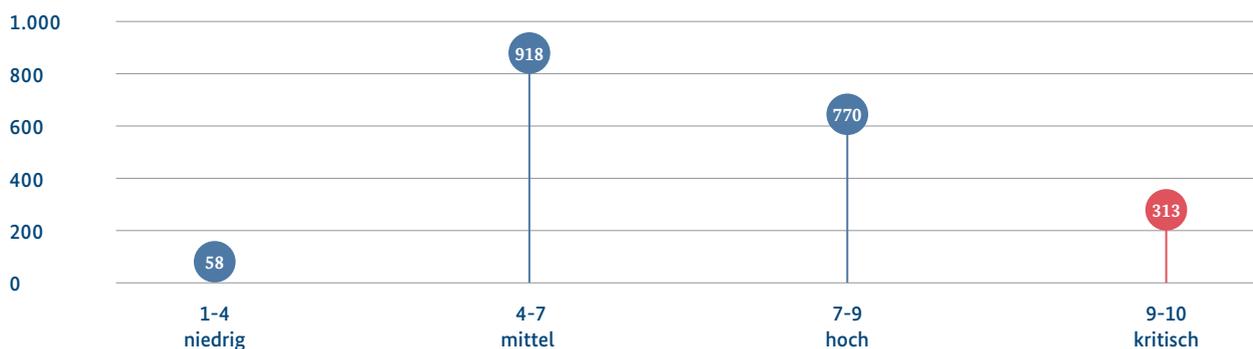
\* Mehrfachnennungen möglich



## Durchschnittlich monatlich bekannt gewordene Schwachstellen nach dem CVSS-Score\* für Kritikalität

Abbildung 10: Durchschnittlich monatlich bekannt gewordene Schwachstellen nach dem CVSS-Score für Kritikalität  
Quelle: Schwachstellen-Statistik des BSI

\* Risikobewertung nach CVSS-Version 3.1



der gemeldeten Produkte verletzen Security-by-Design-Prinzipien (Insecure Design). Jedes zehnte gemeldete Produkt wies verwundbare oder veraltete Komponenten auf und bei sechs Prozent der gemeldeten Produkte versagten kryptografische Schutzmechanismen (Cryptographic Failures). Weitere Produkte wiesen Schwachstellen bei der Sicherheitsüberwachung auf oder

erlaubten die Manipulation von Daten. Mit einem Anteil von sechs Prozent wurden Produkte mit Schwachstellen in den Identifikations- und Authentifizierungssystemen noch vergleichsweise selten gemeldet. In diese Kategorie fallen auch Multifaktor-Authentifizierungen. Inzwischen sind allerdings Schadprogramme bekannt, die diese Form der Benutzer-Authentifizierung umgehen können

(vgl. Vorfall *Identitätsdiebstahl mit Phishing-as-a-Service (PhaaS)*, Seite 54). Es ist daher zu erwarten, dass sich künftig mehr Produkte in dieser Kategorie als schwachstellenbehaftet erweisen werden.

Neben den genannten Schwachstellen in Softwareprodukten erreichten das BSI auch Meldungen über Schwachstellen in Industrial Control Systems (ICS). Industrial Control Systems sind Systeme zur Steuerung industrieller Produktion, zur Automatisierungskontrolle, zur Mensch-Maschine-Interaktion und zu anderem mehr. Im Berichtszeitraum wurden dem BSI insgesamt 24 schwachstellenbehaftete ICS-Systeme gemeldet.

Im Warn- und Informationsdienst (WID) des BSI werden täglich die verschiedenen Quellen zu neuen Schwachstellen in Softwareprodukten gesichtet und die identifizierten Sachverhalte über das Portal des WID veröffentlicht. Zu unterscheiden ist dabei zwischen *Advisories* (umfangreiche Schwachstellen-Informationen, die exklusiv der Bundesverwaltung zur Verfügung gestellt werden) und Kurzinformationen, die Sachverhalte für Organisationen aus anderen Sektoren in gekürzter Form zusammenfassen. Beide Formate können in Behörden,

Unternehmen und anderen Institutionen als Grundlage für das *Patchmanagement* genutzt werden, um das Ausrollen von Sicherheitsupdates voranzutreiben. Technische Warnungen für Verbraucherinnen und Verbraucher ergänzen das Angebot.

Im aktuellen Berichtszeitraum wurde das Webangebot erheblich ausgebaut. Auch ist das Portfolio der beobachteten Softwareprodukte deutlich angewachsen, sodass die Zahlen des aktuellen Berichtszeitraums nicht mit früheren Berichtszeiträumen vergleichbar sind.

Die Flut an neu bekannt gewordenen Schwachstellen ist eine tägliche Herausforderung für IT-Sicherheitsverantwortliche. Perspektivisch sieht das BSI durch (Teil-)Automatisierung das Potenzial, Prozesse im *Patchmanagement* weiter zu beschleunigen. Unter anderem ist es denkbar, die Masse der Schwachstellenmeldungen dadurch zu bewältigen, dass alle Meldungen automatisiert nach denjenigen gefiltert werden, die für die eigene Organisation von besonderem Interesse sind. Die technische Grundlage hierfür stellt das *Common Security Advisory Format (CSAF)* dar, an dessen Spezifizierung das BSI beteiligt war. Dieser neue Standard macht *Advisories* maschinenlesbar und somit automatisiert verarbeitbar.

## Meldungen über schwachstellenbehaftete Produkte

Anteile in %

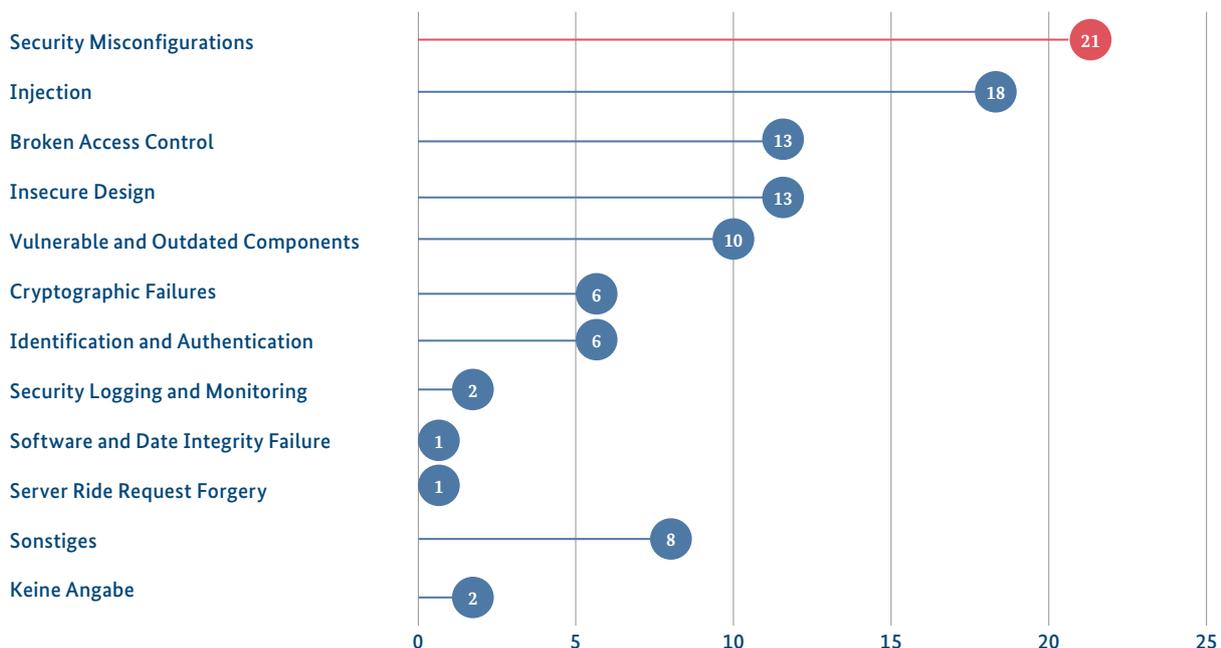
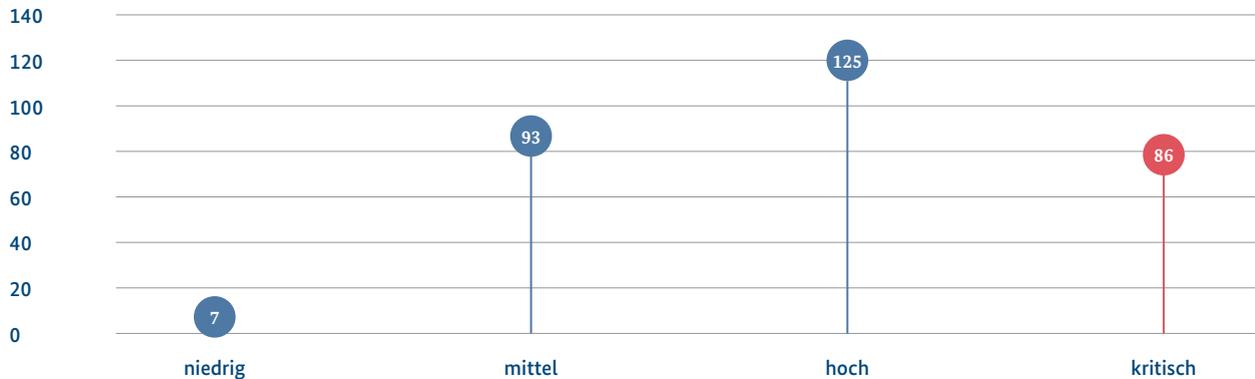


Abbildung 11: Meldungen über schwachstellenbehaftete Produkte  
Quelle: BSI

## Durchschnittliche monatliche WID-Meldungen nach Kritikalität, einschließlich Updates

Anzahl

Abbildung 12: Durchschnittliche monatliche WID-Meldungen nach Kritikalität  
Quelle: BSI



## Angriffskampagne gegen Schwachstelle in Filesharing-Software GoAnywhere

### Sachverhalt

Am 30. Januar 2023 wurde die Zero-Day-Schwachstelle CVE-2023-0669 in dem Produkt GoAnywhere Managed File Transfer (MFT) bekannt. Die Software GoAnywhere MFT wird zum Betrieb eines Filesharing-Servers verwendet und ist daher in der Regel aus dem Internet heraus erreichbar. Die Ausnutzung der Schwachstelle ermöglicht Zugang durch Fernzugriff (Remote Access) und damit die Ausführung von beispielsweise Malware durch einen Angreifer. Am 6. Februar 2023 berichtete ein Sicherheitsforscher öffentlich über die Schwachstelle und veröffentlichte Proof-of-Concept-(PoC-)Code, der die Ausnutzung der Schwachstelle ermöglichte. Kurz nach dieser Veröffentlichung wurde das Framework für Penetrationstesting Metasploit um ein entsprechendes Modul erweitert, womit jeder Angreifer zur Ausnutzung befähigt war. Am 7. Februar 2023 stellte der Hersteller einen Notfallpatch zum Schließen der Schwachstelle zur Verfügung. Seit dem 8. Februar 2023 wurden Ausnutzungsversuche der Schwachstelle beobachtet.

Anfang März 2023 veröffentlichten Angreifer der Ransomware Clop auf ihrer Leak-Seite die Namen mehrerer mutmaßlicher Opfer. Die Angreifer behaupten, 130 Organisationen durch diese Schwachstelle kompromittiert

und Daten gestohlen zu haben. Diese mutmaßlichen Opfer wurden anschließend durch die Angreifer um ein Schweigegeld erpresst.

### Bewertung

Nach Kenntnislage des BSI setzten die Angreifer in dieser Angriffskampagne keine Ransomware ein. Sie beschränkten sich mutmaßlich auf den Diebstahl von Daten auf den kompromittierten GoAnywhere-Servern. Die Zielauswahl erfolgte wahrscheinlich opportunistisch gegen verwundbare Server.

Dieser Vorfall ähnelt einer Angriffskampagne von Ende Dezember 2020. Dabei nutzte dieselbe cyberkriminelle Gruppe eine Schwachstelle in einer anderen Filesharing-Software aus. Auch in dieser Kampagne setzten die Angreifer keine Ransomware ein, sondern erpressten nur mit gestohlenen Daten.

### Reaktion

Um Kompromittierungen wie in diesem Fall zu verhindern, sind aktives Patchmanagement und die Umsetzung präventiver Maßnahmen notwendig. Zudem sollte geprüft werden, ob verwundbare Server bis zur Bereitstellung eines Patches vom Netz genommen werden können.

---

## Angriffskampagne gegen Filesharing-Software MOVEit

---

### Sachverhalt

Am 31. Mai 2023 veröffentlichte der Softwarehersteller Progress Informationen über eine Schwachstelle in seinem Filesharing-Produkt MOVEit und eine aktive Angriffskampagne dagegen. MOVEit-Server werden häufig zum Hochladen von Daten durch externe Nutzer eingesetzt. Angreifer nutzten die Schwachstelle CVE-2023-34362 mindestens seit dem 27. Mai 2023 in einer mehrtägigen Angriffskampagne aus. Ziel der Angreifer war der Diebstahl von Daten vom Filesharing-Server. Der Angriff wurde von mehreren IT-Sicherheitsdienstleistern der Angreifergruppe hinter der Ransomware Clop zugeordnet.

Am 5. Juni 2023 übernahm die Angreifergruppe hinter Clop gegenüber der Nachrichtenwebseite Bleeping Computer die Verantwortung für die Angriffe. Die Angreifer platzierten eine Webshell, welche zum Diebstahl der Daten diente. Diese Webshell wurde von dem IT-Sicherheitsdienstleister Mandiant als Lemurloot bezeichnet.

Seit dem 14. Juni 2023 veröffentlichten die Angreifer auf der Leak-Seite der Ransomware Clop Daten mehrerer Unternehmen. Diese Veröffentlichungen gehen wahrscheinlich auf diese Angriffskampagne zurück. Allerdings können sich auch Opfer darunter befinden, die nicht im Zusammenhang mit der Angriffskampagne gegen MOVEit stehen. Es ist unbekannt, wie viele Organisationen durch diese Angriffskampagne tatsächlich betroffen sind. Aufgrund der Verbreitung von MOVEit waren wahrscheinlich Hunderte Organisationen verwundbar.

### Bewertung

Das BSI hat keine Hinweise auf den Einsatz von Ransomware in dieser Angriffskampagne. Verwundbare MOVEit-Server wurden opportun mit dem Ziel des Datendiebstahls angegriffen. Dieser Vorfall ähnelt zwei anderen Angriffs-

kampagnen derselben Gruppe gegen verwundbare Filesharing-Server: auf den GoAnywhere-Server im Januar 2023 (vgl. Vorfall Angriffskampagne gegen Schwachstelle in Filesharing-Software GoAnywhere, Seite 37) und auf die Filesharing-Software des Herstellers Accellion im Dezember 2020.

Diese Angreifergruppe erpresst Opfer in der Regel mit Double Extortion, also der Verschlüsselung mit Ransomware und der Veröffentlichung gestohlener Daten. Die wiederholten Angriffskampagnen gegen Filesharing-Server zeichneten sich jedoch durch den Verzicht auf den Einsatz von Ransomware aus. Es ist auch nicht bekannt, dass die Angreifer den für den Diebstahl etablierten Zugang für einen späteren Ransomware-Angriff wiederverwendeten. Die Angreifer zielten in diesen Kampagnen darauf ab, möglichst viele Server in kurzer Zeit zu kompromittieren und Daten auszuleiten. Denn sobald die Angriffskampagne bekannt wird, können die verwundbaren Server bis zur Bereitstellung eines Patches vom Internet getrennt werden. Es ist daher davon auszugehen, dass die Angreifer gezielt auf ein hohes Angriffstempo bei der Ausnutzung der Schwachstelle setzten.

Abhängig vom Verwendungszweck des MOVEit-Servers können für die betroffene Organisation sensible Informationen gestohlen worden sein.

### Reaktion

Das BSI veröffentlichte in Reaktion auf die Angriffskampagne am 1. Juni 2023 eine BSI-IT-Sicherheitswarnung. Die IT-Bedrohungslage wurde zuerst mit 4 / Rot bewertet, da unmittelbarer Handlungsbedarf bestand. Am 2. Juni 2023 wurde die Sicherheitswarnung auf 3 / Orange heruntergestuft, nachdem der Softwarehersteller ein Patch zur Verfügung gestellt hatte.

---

## 5.2 – Schwachstellen in Hardwareprodukten

Hardware-Schwachstellen können normalerweise nicht durch Softwarepatches behoben werden, da ihre Ursache in der Herstellungsweise und der Architektur der Produkte begründet ist. Es gibt verschiedene Angriffsmöglichkeiten. Zum einen sind die Funktionsweisen der Transistoren das Ziel, die in integrierten Schaltungen verbaut werden, und somit auch die Mikroarchitektur von Prozessoren. Zum anderen geben im Lebenszyklus eines IT-Produktes auch verschiedene Schritte in der Lieferkette und der Produktion Angriffsmöglichkeiten. Da die Schwachstellen in bereits verbauter Hardware normalerweise nicht einfach behoben werden können, ist der mögliche Nutzen für einen potenziellen Angreifer sehr hoch. Allerdings sind die finanziellen Aufwendungen zur Ausnutzung im Gegensatz zu Schwachstellen in Software ebenfalls höher.

Seitdem 2017 die Angriffe MELTDOWN und SPECTRE bekannt geworden sind, gibt es immer weitere Versionen dieser Angriffe, die sich die spekulativen Ausführungen in modernen Prozessoren zunutze machen. Daher ist weiterhin mit neuen Schwachstellen dieser Angriffsklasse zu rechnen, solange die Mikroarchitektur der Prozessoren nicht grundlegend verändert wird. Jedoch ist die spekulative Ausführung zu einem substanziellen Teil für die Performance der Prozessoren verantwortlich. Eine andere Ausführung würde zu einer erheblichen Verringerung der Rechenleistung führen. Wie auch in den vorangegangenen Jahren dominieren immer noch die aus diesen Angriffen weiterentwickelten Variationen. Im Jahr 2022 wurden etwa die Angriffe Retbleed, SPECTRE-BHB, SQUIP und PACMAN veröffentlicht. Gegen diese Schwachstellen existieren entweder keine Gegenmaßnahmen-, oder diese führen zu großen Leistungsmininderungen.

Im Gegensatz zu auf SPECTRE basierenden Angriffen handelt es sich bei der Schwachstelle  $\text{ÆPIC}$ -Leak um einen echten Fehler in der Mikroarchitektur des Prozessors, bei dem geheime Schlüsseldata ausgelesen werden können, jedoch nur von Usern mit Administratorrechten.

Neue Kryptoalgorithmen sollten quantensicher sein (Post-Quantum Cryptography, PQC). PQC-Verfahren müssen nicht nur Quantencomputern standhalten, sondern auch hardwarenahen Seitenkanal- und Fehlerangriffen, da sie auf klassischen Plattformen implementiert werden.

So wurde zum Beispiel gezeigt, dass Schlüsselmaterial bei einer Hardware-Implementierung des PQC-Kryptoverfahrens CRYSTALS-Kyber mittels Seitenkanalanalyse in Kombination mit neuronalen Netzen ausgelesen werden kann (vgl. auch Kapitel *Post-Quanten-Kryptografie*, Seite 74). Für die zukünftige Verwendung von Hardware-Implementierungen müssen geeignete Gegenmaßnahmen entwickelt werden, damit PQC-Verfahren in Hardwareprodukten sicher implementiert werden können.

Im März 2023 wurden kritische Zero-Day-Schwachstellen in Exynos-Modemchips veröffentlicht, die nicht nur in Smartphones, sondern auch in Fahrzeugen verbaut sind. Diese Schwachstellen ermöglichen es Angreifern, Programme auf den mobilen Geräten auszuführen, ohne dass der Eigentümer davon etwas merkt oder etwas dagegen unternehmen kann. Für einen erfolgreichen Angriff reicht lediglich die Kenntnis der Telefonnummer. Nach dem derzeitigen Kenntnisstand gibt es jedoch keine breite Ausnutzung dieser Schwachstelle im Feld.

Da die Ausnutzung von Hardware-Schwachstellen im Vergleich zu den zahlreichen Software-Schwachstellen relativ aufwendig ist, ist Hardware seltener Ziel von Cyberangriffen. Wie in mehreren Studien gezeigt wurde, kann die Verwendung von dedizierten Sicherheitselementen oder vollständig logisch separierten Prozessoreinheiten zur Speicherung und Verarbeitung sensibler Daten das Angriffspotenzial stark senken. Ein Kennzeichen für eine gute Sicherheitsfunktionalität in IT-Produkten bietet dabei eine unabhängige Sicherheitsüberprüfung und Zertifizierung, zum Beispiel nach dem ISO-Standard 15408: Common Criteria for IT Security Evaluation.

## 5.3 – Schwachstellen in vernetzten Geräten

Neben Software und Hardware können auch Geräte und Komponenten des *Internet of Things* Schwachstellen aufweisen. Mit dem Grad der Vernetzung und der Komplexität der Produkte nimmt die digitale Angriffsfläche im *IoT*-Bereich stetig zu. Jede zusätzliche Schnittstelle und jeder zusätzliche Controller bietet potenzielle *Angriffsvektoren*. Insbesondere in modernen Fahrzeugen ist eine Vielzahl von Steuergeräten verbaut, die untereinander vernetzt sind. Zudem steigt der ohnehin große Softwareumfang durch die zusätzlichen Funktionalitäten weiter an, was typischerweise auch eine höhere Anzahl an

Schwachstellen nach sich zieht. Im Fall einer App- oder Cloud-Anbindung und einer gezielten Manipulation ist es für einen Angreifer daher prinzipiell möglich, aus der Ferne essenzielle Funktionen zu stören oder zu deaktivieren.

Die große Angriffsfläche, die das IoT bietet, erfordert einen aktiven Schutz, insbesondere durch Maßnahmen der Hersteller wie Sicherheitskonzepte und Penetrationstests. Die Schwachstellen, die die Angriffsvektoren ermöglichen, sind vielfältig: Zunächst sind viele ursprünglich konventionelle Produkte auf dem Markt, die seit Generationen existieren und mit der Zeit immer weiter digitalisiert und vernetzt wurden. In diesem Rahmen wurden zusätzliche Schnittstellen implementiert. Das ursprüngliche Produkt erforderte mangels Vernetzung keine Cybersicherheitsmaßnahmen. Inzwischen ist jedoch in den meisten Fällen ein grundlegendes Sicherheitskonzept zum wirkungsvollen Schutz erforderlich, das bereits beim Design des Produktes berücksichtigt werden muss (Security by design). Beispielsweise sind viele Komponenten nicht auf einen Schutz durch eine Transportverschlüsselung ausgelegt und enthalten keine Firewalls, die vor unberechtigtem Zugriff schützen. Häufig ist es durch Hardwarebeschränkungen und Abwärtskompatibilität nicht möglich, solche Maßnahmen im Nachhinein wirkungsvoll zu implementieren.

Eine weitere Ursache ist die fehlende Erfahrung von Herstellern im Umgang mit Cybersicherheit und potenziellen Schwachstellen. Da bei konventionellen, nicht vernetzten Produkten keine IT-Sicherheitsmaßnahmen notwendig waren, gibt es bei vielen Herstellern bisher weder Strukturen noch Fachwissen, um digitalen Angriffen auf ihre Produkte entgegenzuwirken. Durch das gestiegene Bewusstsein für Cybersicherheitsfragen und besonders durch neue regulatorische Rahmenbedingungen wie etwa Typgenehmigungsvorschriften zur Cybersicherheit in Fahrzeugen hat sich die Situation hier in jüngster Zeit geändert. Automobilhersteller beispielsweise sind verpflichtet, geeignete Prozesse zum Management der Cybersicherheit in der Produktion und zur Behebung von Schwachstellen zu etablieren.

### Schwachstellen im Bereich Automotive

Im Berichtszeitraum wurden neue Schwachstellen im Bereich Automotive bekannt. Der Sicherheitsforscher Sam Curry konnte zeigen<sup>4</sup>, dass mangelhaft abgesicherte Webportale verschiedener Hersteller Angreifern neben Zugriffen auf Hersteller- und Kundendaten

aus der Ferne auch Zugriff auf Fahrzeugfunktionen erlaubten. Das Manipulieren von Webanfragen ermöglichte Angreifern beispielsweise, sich im Webportal als Händler auszugeben. Händler genießen vonseiten der Hersteller ein besonderes Vertrauen und können Fahrzeuge bestimmten Kunden namentlich zuordnen. Entsprechend konnte ein Angreifer bereits vergebene Fahrzeuge einem eigenen Account zuordnen und Fahrzeugfunktionen fremder Autos über die offizielle App des Herstellers steuern. Auf diese Weise konnte ein betroffenes Fahrzeug aus der Ferne geöffnet oder dessen Motor gestartet werden. In einem weiteren Fall war es möglich, Live-Bilder der Heckkamera zu empfangen. Für eine Manipulation dieser Art war lediglich die Fahrzeugidentifikationsnummer (FIN) nötig, die in einigen Fällen auf der Windschutzscheibe des Fahrzeugs zu finden ist.

Im Falle eines großen nordamerikanischen Telematikbetreibers ermöglichten Schwachstellen die Ausführung von Fahrzeugfunktionen ganzer Flotten. Unter den über 15 Millionen betroffenen Fahrzeugen befanden sich auch Ambulanz- und Polizeifahrzeuge, deren Einsatz durch ein Ausnutzen dieser Schwachstellen behindert worden wäre.

Diese Vorfälle zeigen, dass nicht nur das Fahrzeug an sich und dessen interne Systeme betrachtet werden müssen. Darüber hinaus muss auch das ganze Ökosystem, in dem sich das Fahrzeug bewegt, einschließlich der Vertrauensbeziehungen zwischen verschiedenen Marktakteuren abgesichert werden.

Weitere Informationen zum Bereich Automotive finden Sie im Lagebild Automotive:<sup>5</sup>



## 6. – Große KI-Sprachmodelle

Die technische Entwicklung großer KI-Sprachmodelle (Large Language Models, LLMs) hat im aktuellen Berichtszeitraum ein Schlüsselmoment erfahren. Mit der Veröffentlichung des Chatbots ChatGPT des von Microsoft unterstützten Unternehmens OpenAI im November 2022 wurde erstmals eine Anwendung basierend auf einem großen KI-Sprachmodell einer breiten Öffentlichkeit zugänglich. Die Fähigkeiten des Modells bei der Erzeugung von Texten haben nicht nur die allgemeine Öffentlichkeit, sondern auch die Fachwelt überrascht. Sowohl technisch als auch bei den Anwen-

dungsfeldern dieses und vergleichbarer Modelle ist seitdem eine dynamische Entwicklung zu beobachten.

## 6.1 – Technische Entwicklung

Sprachmodelle können inzwischen wesentlich mehr als Texte erstellen, da sie in größere Kontexte eingebunden werden. Über die Integration in verschiedene Anwendungen oder die Verwendung von Plug-ins können diese Modelle auch im Internet agieren, zum Beispiel E-Mails verschicken, Flüge buchen oder bezahlen. In IT-Infrastrukturen in Unternehmen werden Sprachmodelle eingebaut, um vorwiegend repetitive Aufgaben zu übernehmen und Mitarbeitende bei ihrer Arbeit zu unterstützen.

Die Leichtigkeit der Automatisierung und die Variationsbreite der Ergebnisse geht dabei inzwischen weit über bisherige IT-Produkte hinaus. Waren zuvor noch Programmierkenntnisse erforderlich, um beispielsweise eine automatisierte Archivierung zu erstellen, so ist es inzwischen technisch möglich, diese Aufgabe einfach mittels natürlichsprachlicher Eingabe an ein Sprachmodell zu delegieren: „Erstelle bitte jeden Freitag um 16 Uhr eine Exceltabelle mit den Umsatzzahlen der Woche unterteilt nach Bereich und Gebiet. Reichere sie mit einer entsprechenden zweistufigen Kuchengrafik an und maile sie an den Vorstand.“ Eine solche Aufgabenstellung können LLMs mit Zugriff auf die entsprechenden Unternehmensdaten und Mailserver ohne Weiteres umsetzen. Sprachmodelle prüfen inzwischen Bewerbungen im Hinblick auf die Eignung von Bewerberinnen und Bewerbern auf ausgeschriebene Stellen, erstellen Geschäftsbriefe mit direkten finanziellen Auswirkungen, schließen Buchungen ab oder beauftragen Dienstleister.

Bedeutsam für die Bedrohungs- und Gefährdungslage ist zudem die Nutzung von LLMs durch Programmierinnen und Programmierer, die sich bei der Entwicklung komplexer IT-Produkte unterstützen lassen. Die inhaltliche Qualität der Ergebnisse wird hier unter Umständen nicht ausreichend durch Menschen gesichert.

Mit den zweifellos großen Chancen von LLMs gehen analog große Risiken einher. Einerseits können solche Modelle als Werkzeuge für Cyberangriffe missbraucht werden, andererseits können sie selbst angegriffen oder als Schwachstelle ausgenutzt werden. Da solche Modelle nicht nur in legalen Anwendungen eingesetzt werden

können, sondern auch im cyberkriminellen Kontext, sind erhebliche Skalierungseffekte bei bereits bekannten Cyberbedrohungen zu erwarten. Die folgende Darstellung liefert eine Betrachtung neuer Bedrohungen und Gefährdungen, die sich aus dem Entwicklungsstand großer KI-Sprachmodelle zum Redaktionsschluss dieses Berichts absehen lassen.

## 6.2. – Neue Bedrohungen

Neue, vormals unbekannte Bedrohungen entstehen im Wesentlichen durch die herausragende Bedeutung der Trainingsdaten einerseits sowie durch den Einsatz der KI in der Software-Entwicklung andererseits. Auf diese neuen Bedrohungen wird im Folgenden eingegangen.

### 6.2.1 – Trainingsdaten

Die Ausgaben und das Verhalten großer KI-Sprachmodelle hängen wesentlich von den Trainingsdaten ab, die für das Anlernen der KI verwendet wurden. Bei Sprachmodellen, die in einem abgeschlossenen, begrenzten Unternehmenskontext entwickelt und eingesetzt werden, können das die Informationen einzelner Fachbereiche oder Abteilungen sein, gegebenenfalls auch Daten und Infrastruktur-Metadaten des gesamten Unternehmens. Bei LLMs wie GPT-3 oder GPT-4, auf denen Anwendungen wie ChatGPT basieren, kommen dagegen Trainingsdaten aus dem gesamten Internet zum Einsatz. Je mehr und je diverser die Trainingsdaten sind, desto universeller kann das Modell bei der Erledigung von Anfragen und Aufgaben hilfreiche Ausgaben erzeugen. Von den Trainingsdaten können verschiedene Bedrohungen ausgehen.

**Schiefe Trainingsdaten:** Enthalten Trainingsdaten eine Schiefe, einen sogenannten Bias, kann das Modell unausgewogene Ausgaben liefern. Das kann Aussagen über bestimmte Marken oder Produkte betreffen, aber zum Beispiel auch Bewertungen von Menschen, Institutionen oder politische Tendenzen, wenn Modelle beispielsweise tendenziöse Aussagen aus sozialen Medien übernehmen. Wenn Trainingsdaten manipuliert werden, können zudem Falschnachrichten und Desinformationskampagnen getriggert werden, die die öffentliche Meinung bis hin zum gesellschaftlichen Wertekanon beeinflussen können.

**Selbstreferenzialität:** Trainiert man LLMs mit den Inhalten des allgemeinen, öffentlichen Internets, so nimmt mit der zunehmenden Menge KI-generierter Inhalte im Internet die Selbstreferenzialität der Sprachmodelle exponentiell zu. Anders gesagt: Je mehr KI-generierte Inhalte im Internet verfügbar sind, desto mehr bestehen auch die Trainingsdaten großer KI-Sprachmodelle aus KI-generierten Inhalten. Falschnachrichten oder Desinformationskampagnen lassen sich dann immer schwerer erkennen, da unterschiedliche, ggf. auch seriös wirkende Quellen durch die Nutzung von Sprachmodellen ähnliche inhaltliche Verzerrungen aufnehmen. Die Art und die Zahl der referenzierten Quellen ist nach längerer Etablierung der unreflektierten Sprachmodellnutzung immer weniger ein Qualitätsmerkmal in Bezug auf die Echtheit oder Korrektheit einer Information, wenn das gleiche Sprachmodell an vielen Stellen eingesetzt wird.

**Automatisiertes Social Engineering:** Sprachmodelle können auf menschliche Reaktionen Antworten generieren (zunächst in Textform, aber in Zukunft vermutlich auch als Ton, Bild oder Video) und gewinnen durch diesen Dialogcharakter an Glaubwürdigkeit in einer Gesellschaft, die nicht schnell und umfassend aufgeklärt wird. Es besteht die Gefahr, dass dies in einem automatisierten *Social Engineering* mündet, da als erfolgreich erkannte Textangriffe einer beschleunigten Weiterverbreitung unterliegen, weil sie ohne menschliche Interaktion gestreut werden können.

**Schwachstellen „lernen“ und finden:** Sprachmodelle werden zunehmend genutzt, um Programmcode in den verschiedensten Programmiersprachen zu generieren und dadurch Programmiererinnen und Programmierer bei ihrer täglichen Arbeit zu unterstützen. Enthalten Trainingsdaten für Programmcode beabsichtigt oder unbeabsichtigt Schwachstellen oder schlechten Code, so lernt das Modell diese mit und kann sie in generiertem Code reproduzieren. Dieser kann unter Umständen ungeprüft in neue IT-Produkte übernommen werden und damit zur Vervielfältigung von Schwachstellen beitragen.

LLMs können zudem helfen, im Internet nach bestehenden Schwachstellen in Programmcode und in Unternehmensnetzwerken zu suchen und den nötigen *Exploit* für die Ausnutzung einer identifizierten Schwachstelle zu finden und zu erstellen. Kenntnisse über entsprechende Werkzeuge, die bisher erforderlich waren, sind dann nur noch in reduzierter Form nötig.

## 6.2.2 – Fehlerhaft erzeugter Code

Große KI-Sprachmodelle machen Fehler. Insbesondere bei der Nutzung im Rahmen der Entwicklung von IT-Produkten stellt dies eine Bedrohung dar. Das betrifft zum einen die oben genannten gelernten Schwachstellen und schlechten Codes, zum anderen jedoch insbesondere auch die Anwendungsbedingungen von Sprachmodellen. Die Bedrohung, die sich aus einem in einer Unternehmensinfrastruktur eingebauten Sprachmodell ergibt, hängt wesentlich davon ab, auf welche Daten und Dienste das Modell zugreifen darf. Die Ausgaben, die es produziert, können von den Entwicklerinnen und Entwicklern des Modells nicht mehr im Einzelnen nachvollzogen werden. Diese können faktisch nicht mehr kontrollieren, was das KI-Sprachmodell in einem bestimmten Anwendungskontext tun wird.

Je nach erteilten Zugriffsrechten kann ein Modell ganz unterschiedlich auf eine gestellte Aufgabe oder eine Anfrage reagieren. Security-by-Design als Basisanforderung an die Sicherheit von IT-Produkten ist für Sprachmodelle daher kaum erfüllbar. Da es für LLMs kein Design gibt (die KI designt sich gleichsam selbst), kann es auch keine Security-by-Design geben. Eine große Herausforderung besteht daher darin, überhaupt allgemeingültige Sicherheitskriterien im Zusammenhang mit KI-Sprachmodellen – unabhängig von einem konkreten Anwendungsfall – anzugeben.

## 6.3 – Neue Gefährdungen – die KI als Angriffsfläche

Die Bandbreite möglicher Anwendungen für ein Sprachmodell in einem Unternehmen steigt mit der Menge der verwendeten Unternehmensdaten und der Menge der Zugriffsrechte des Softwaresystems, in welches das Sprachmodell integriert ist. Je mehr Informationen ein Modell über das Unternehmen verarbeiten kann und je mehr Zugriffsrechte das entsprechende System hat, desto besser wird es Mitarbeitende bei ihren täglichen Aufgaben unterstützen können. Die Reichweite der Zugriffsrechte, die einem solchen System gewährt werden, sollte jedoch einer gründlichen Risikoabwägung unterzogen werden. Zumindest die folgenden Risiken sollten dabei beachtet werden.

**Rekonstruktion von Trainingsdaten:** Sprachmodelle können prinzipiell sämtliche gelernten Informationen aus den Trainingsdaten in Ausgaben reproduzieren, selbst wenn ihr Training auf die Vermeidung bestimmter Ausgaben abzielte. Angreifer können dieses Verhalten umgehen, um ein Modell für Angriffe zu missbrauchen. So hat sich beispielsweise gezeigt, dass häufig Trainingsdaten im gelenkten Dialog oder mittels gezielter Anfragen, die dem Modell einen bestimmten Kontext suggerieren, rekonstruiert werden können. Beispielsweise konnten dem Modell Hassbotschaften oder Anleitungen zum Bombenbau als Antwort entlockt werden, wenn man vorgab, diese Informationen als Grundlage für einen warnenden Artikel zu benötigen und damit Gutes zu tun. Selbst wenn es inzwischen durch erneutes Training der Modelle schwieriger wird, explizite Äußerungen zu extrahieren, können immer noch abstrakte Beschreibungen schädlicher Ideen zurückgegeben werden und so für deren Verbreitung sorgen oder als Ideengeber oder Recherchehelfer fungieren. Wenn die Trainingsdaten sensible Unternehmensinformationen enthalten, wird die grundsätzliche sprachliche Manipulierbarkeit eines Sprachmodells auf diese Weise schnell zu einer Schwachstelle, die für Datenleaks ausgenutzt werden kann. Ein wirksames Rechte-Management, das verschiedenen Nutzerinnen und Nutzern unterschiedliche Zugriffs- und Informationsrechte gewährt, war zum Redaktionsschluss des vorliegenden Berichts nicht möglich. Es werden stets die gesamten Trainingsdaten herangezogen.

**Sammlung von Unternehmensinformationen in einer einzigen, schwer abzusichernden Anwendung:** Ein mit weitreichenden Zugriffsrechten und einem KI-Sprachmodell ausgestattetes System weiß unter Umständen mehr über ein Unternehmen als jede oder jeder menschliche Beschäftigte und kann Aktionen hochautomatisiert ausführen. Mehr noch: Die Gründe für bestimmte Aktionen oder Ausgaben eines Modells sind für Mitarbeitende und selbst für IT-Sicherheitsverantwortliche, Administratorinnen und Administratoren in Unternehmen schwer durchschaubar und teilweise sogar gänzlich unbekannt. Aus diesem Grund sind aktuelle Kriterien für ein wirksames IT-Sicherheitsmanagement, wie sie auch für andere IT-Produkte gelten, nur bedingt auf Softwaresysteme anwendbar, die mit großen Datenmengen und KI-Sprachmodellen arbeiten.

**Möglicher Missbrauch des Modells:** Die Nützlichkeit von Sprachmodellen ergibt sich wesentlich aus der Steuerbarkeit mittels natürlicher Sprache. Ziel der aktuellen

Modellentwicklung ist es, Befehle und auch komplexe Aktionen nicht mehr programmieren zu müssen, sondern als natürlichsprachliche Arbeitsanweisungen, sogenannte Prompts, an das Modell zu delegieren. Das Finden der richtigen Anweisungen wird „Prompt Engineering“ genannt. Dieses Konzept ermöglicht jedoch auch sogenannte „Prompt Injections“. Das sind Eingaben in manipulativer oder krimineller Absicht. So können Angreifer mittels eines spezifischen Dialogaufbaus ein Modell beispielsweise sukzessive dazu bringen, eine bestimmte schädliche Aktion auszuführen oder Daten wie etwa Identitätsdaten herauszugeben.

Darüber hinaus können diese *maliziösen* Eingaben in ein ansonsten nicht als *Malware* agierendes Sprachmodell („Adversarial Attacks“) in bestimmten Angriffsszenarien auch über zweistufige *Angriffsvektoren* ausgeführt werden. So können Angreifer Textabschnitte in Webseiten verstecken, die zwar für den Menschen nicht sichtbar sind, für ein KI-Sprachmodell aber ausführbare Befehle wie etwa zum Herunterladen von Schadcode enthalten. Bekommt ein harmloses Auskunftssystem, das solche Seiten mit einem KI-Sprachmodell analysiert, diesen versteckten Input und ist aufgrund seiner technischen Fähigkeiten und Berechtigungen in der Lage, als Agent zu handeln, kann Schadsoftware ins System der Nutzerin oder des Nutzers gelangen. Bei dieser Art von Angriff, bei dem eine andere Person als der Nutzende selbst eine Anweisung an das Sprachmodell übergibt, spricht man von sogenannten „Indirect Prompt Injections“.

Auch Angreifer, die auf konventionelle Art in ein Unternehmensnetzwerk eingebrochen sind, können mit der entsprechenden Berechtigung ein im Unternehmensnetz befindliches Sprachmodell entsprechend missbrauchen.

## 6.4. – Systemische Bedrohungsveränderung

Neben ganz neuen Bedrohungen der Cybersicherheit bringen KI-Sprachmodelle auch eine Veränderung bereits bekannter Bedrohungen hervor. Dies betrifft zum einen Skalierungseffekte, die durch die enorme Performanz der KI entstehen. Dies betrifft jedoch auch die informationstechnischen Infrastrukturen insgesamt bzw. die KI als Agent, also als gleichsam handelnden Akteur innerhalb dieser Infrastrukturen. Zur Manipulation der „Schwach-

stelle Mensch“ durch *Social Engineering* kommt nunmehr die Manipulation der „Schwachstelle KI“ durch Prompt Engineering hinzu.

#### 6.4.1 – Skalierungseffekte bekannter Bedrohungen

Neben den genannten neuen Bedrohungen und Gefährdungen werden große KI-Sprachmodelle wahrscheinlich Skalierungseffekte bei bekannten Cyberbedrohungen bewirken.

##### **Spam, Phishing, Social Engineering**

Durch die Sprachmodelle sind mehr *Spam*- und *Phishing*-Mails zu erwarten, die weniger Rechtschreib- und Grammatikfehler enthalten und somit schwerer zu erkennen sind. Da LLMs nicht nur qualitativ hochwertige Texte verfassen, sondern auch entsprechende Vorlagen in Wortwahl und Sprachstil überzeugend imitieren können, werden Social-Engineering-Angriffe wie *Spear-Phishing* und *CEO-Fraud* personalisierbar und damit weiter an Überzeugungskraft gewinnen. Diese Entwicklung kann durch die ebenfalls rasante Entwicklung im Bereich KI-generierter Bild-, Audio- und Videoformate zusätzlich verschärft werden. Verfahren, mit deren Hilfe Fälschungen von Stimmen erstellt werden können, haben sich in den letzten Jahren sowohl in ihrer Qualität, als auch in ihrer Verfügbarkeit und Zugänglichkeit signifikant verbessert. So ist es beispielsweise für Laien möglich, gefälschte Audiobeispiele von bekannten Politikern zu erstellen, die insbesondere in Bezug auf deren Klangfarbe nicht mehr vom Original zu unterscheiden sind (siehe auch Kapitel *KI für autonomes Fahren und mediale Identitäten*, S. 73). Die zunehmende Echtzeitfähigkeit dieser *Deepfakes* genannten Manipulationen bewirkt beispielsweise, dass man in Onlinemeetings in absehbarer Zeit nicht mehr sicher sein kann, ob man mit der realen Person, einem Angreifer oder sogar dem Avatar eines Chatbots spricht.

##### **Schadprogramme**

Große KI-Sprachmodelle, die auf Code-Beispielen trainiert wurden, sind grundsätzlich in der Lage, Programmcode zu erzeugen. Das schließt Schadprogramme ein. Zwar bemühen sich Entwickler, KI darauf zu trainieren, keine Hilfestellung für strafbare Handlungen zu geben. Mittels Prompt Engineering lassen sich derartig antrainierte Skrupel eines Modells jedoch potenziell

umgehen. Neben einer rascheren Neuproduktion von Schadsoftware ist daher künftig mit schnelleren Veränderungen bestehender Schadprogramme zu rechnen, was deren Detektion erschwert. Erwartet werden muss eine schnellere und bessere Weiterentwicklung von Angriffswerkzeugen jeglicher Art: vom *Information Stealer* über das *DDoS-Botnetz* bis hin zu den einzelnen Modulen eines komplexen *Ransomware*-Angriffs. Insbesondere die Möglichkeiten der Codegenerierung dürften die Zugangsvoraussetzungen zu cyberkriminellen Aktivitäten wie zumindest rudimentäre Programmier- und Systemkenntnisse deutlich senken. Die Zahl der Personen mit krimineller Energie, die zum Erzeugen von Schadprogrammen fähig sind, wird durch diese geringeren fachlichen Anforderungen vermutlich steigen.

##### **Ransomware und APT**

Im Zusammenhang mit komplexen Cyberangriffen dürften Sprachmodelle insbesondere einen Einfluss darauf haben, wie Angreifer sich in einem infiltrierten Unternehmensnetzwerk ausbreiten, wie sie dort Daten sammeln und wie sie ihre Zugriffsrechte erweitern können. Während sich Angreifer in herkömmlichen Unternehmensnetzwerken vergleichsweise mühsam von System zu System vorarbeiten müssen, finden sie künftig möglicherweise ein KI-Sprachmodell mit umfangreichem Wissen über das Unternehmen und weitreichenden Zugriffsrechten vor, welches verhältnismäßig leicht manipuliert und für Angriffe missbraucht werden kann. Derartige Modelle dürften nicht nur für cyberkriminelle Angreifer ein attraktives Angriffsmittel darstellen, sondern ebenso für Zwecke der Cyberspionage und Cybersabotage nutzbar sein.

##### **Effekte**

Durch die Skalierung dieser grundsätzlich bekannten Bedrohungen entstehen neue Dynamiken. Die Zahl der potenziellen Angreifer kann sich durch die Leichtigkeit des Zugangs deutlich erhöhen unabhängig davon, ob es sich um staatliche Akteure, finanziell motivierte Angreifer, Innentäter, durch Spieltrieb motivierte *Script-Kiddies* oder sogar leichtfertige Sicherheitsforscher handelt. Selbst wenn die Nutzung von KI-Elementen auch auf der Verteidigerseite für eine deutlich gestiegene Aufklärungsrate sorgt, kann sich eine negative Bilanz einstellen. Die Kapazitäten der Strafverfolgungsbehörden werden möglicherweise stark ausgelastet und insbesondere in Richtung der weniger kenntnisreichen KI-gestützten Angreifer umgelenkt, weil diese leichter zu ermitteln sind. Sie fehlen dann für die Verfolgung kennt-

nisreicher Angreifer. Wie sich die Angreifer-Verteidiger-Dynamik bei beidseitigem Gebrauch aktueller KI-Sprachmodelle entwickeln wird, ist nicht vorhersagbar. Die Vermutung liegt nah, dass die Seite, die die Technologie zuerst nutzt, größere Chancen hat. Bei der aktuell hohen Entwicklungsgeschwindigkeit reicht auch ein kleinerer zeitlicher Vorsprung für einen essenziellen Vorteil.

#### 6.4.2 – Schwachstellen, Unschärfe und Agentennetzwerke

Durch ihren Black-Box-Charakter stellen große KI-Sprachmodelle eine Schwachstelle an sich dar. Das Prompt Engineering als Mittel zur Ausnutzung von Schwachstellen eines Modells hat keine klar definierten Grenzen. Es handelt sich nicht um eine technische Fehlleistung wie einen *Stack Overflow*, der überprüft und verhindert werden kann. Auch gibt es aktuell keine Möglichkeit, einen Prompt als Schadcode zu identifizieren, weil der Input syntaktisch nicht überprüft werden kann, sondern semantisch überprüft werden müsste. Eine natürlichsprachliche Prompt-Injection ist daher nur unscharf und damit unsicher abzuwehren, weil der semantische Inhalt durch sehr viele verschiedene Formulierungen übermittelt oder auch anders kontextualisiert werden kann.

Dadurch wird das Schwachstellenmanagement von KI-Sprachmodellen zu einer Aufgabe mit unscharfem Ziel. Es muss nicht nur ein bestimmter Text unterbunden werden, sondern auch alle semantischen Äquivalente. Schwachstellenmanagement verschiebt sich daher von einer technischen auf eine wenig greifbare, weil semantische Ebene. Solche Schwachstellen können deshalb auch nicht mehr eindeutig klassifiziert werden. Beispielsweise kann ein Prompt, der in einem System als schadhaft erkannt wird, trotz Schließen der Schwachstelle in diesem System in einem anderen System noch wirksam sein, weil auch verschiedene Systeme aufgrund gleicher Trainingsgrundlagen unscharfe Überlappungen aufweisen. Damit wird der Unterschied zwischen einer Zero-Day-Schwachstelle und einer bekannten öffentlichen Schwachstelle ebenfalls unschärfer, was das Vorgehen für IT-Sicherheitsverantwortliche grundsätzlich infrage stellt.

Berücksichtigt man diese Unschärfe, gewinnt zudem eine weitere Entwicklung an Relevanz. Aktuell werden Sprachmodelle nicht nur für die Ausgabe von Text, den Menschen lesen sollen, in IT-Systeme integriert. Von

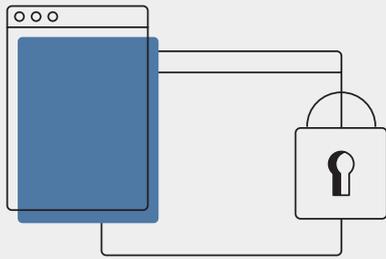
großer Bedeutung sind Agentensysteme, in denen die Ausgaben von KI-Sprachmodellen in (elektronische) Handlungen umgesetzt werden. Hier kommt es entscheidend darauf an, ob für diese Handlungen weiterhin Menschen Verantwortung tragen. Damit dies der Fall ist, dürfen diese Systeme nur unter menschlicher Kontrolle handeln können. Dazu gehören Abfragen wie „Jetzt kostenpflichtig kaufen/buchen?“ oder „Wollen Sie diese persönlichen Daten wirklich an den Anbieter XY/in den Cloudspeicher übermitteln?“. Solche Sicherheitsabfragen stehen jedoch dem Trend entgegen, Funktionalitäten in die *Cloud* zu verlagern und sie zu kompletten Agentennetzwerken auszubauen. Verbindet man die Unschärfe einzelner Schwachstellen mit der Vielzahl an künftig beteiligten externen Komponenten, die potenziell selbst KI-Komponenten mit Schwachstellen enthalten, wird die Größe der Aufgabe deutlich, solche Strukturen zu schützen. Vor diesem Hintergrund entwickelt das BSI gemeinsam mit nationalen und internationalen Partnern Kriterien für einen sicheren Betrieb von KI-Sprachmodellen und KI-Systemen allgemein (vgl. Kapitel *Künstliche Intelligenz*, Seite 71).

Die Lage der IT-Sicherheit in Deutschland 2023  
im Überblick

# Ransomware

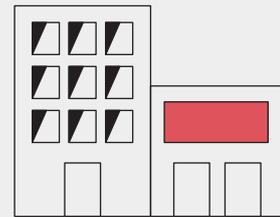
ist weiterhin die größte Bedrohung.

**2** Ransomware-Angriffe auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.



**68** erfolgreiche Ransomware-Angriffe auf Unternehmen wurden bekannt.

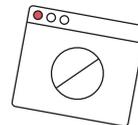
**15** davon richteten sich gegen IT-Dienstleister.



Mehr als **2.000** Schwachstellen in Softwareprodukten (15 % davon kritisch) wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %**.

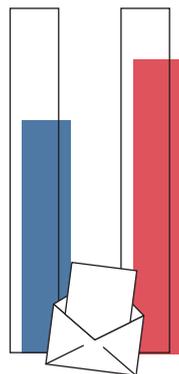
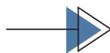


**Eine Viertelmillion** neue Schadprogramm-Varianten wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.



**66%**

aller Spam-Mails im Berichtszeitraum waren Cyberangriffe:  
34 % Erpressungsmails,  
32 % Betrugsmails

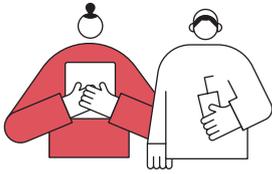


**84%**

aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.

### Top-3-Bedrohungen je Zielgruppe:

#### Gesellschaft



#### **Identitätsdiebstahl**

Sextortion  
Phishing

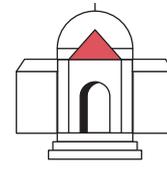
#### Wirtschaft



#### **Ransomware**

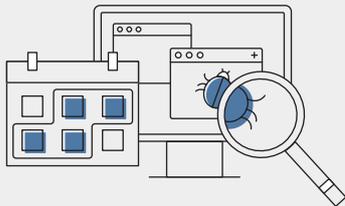
Abhängigkeit innerhalb der  
IT-Supply-Chain  
Schwachstellen, offene oder falsch  
konfigurierte Onlineserver

#### Staat und Verwaltung



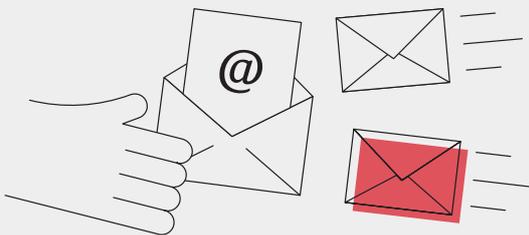
#### **Ransomware**

APT  
Schwachstellen, offene oder  
falsch konfigurierte Onlineserver



Rund **21.000** infizierte Systeme wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.

Durchschnittlich rund **775** E-Mails mit Schadprogrammen wurden an jedem Tag im Berichtszeitraum in deutschen Regierungsnetzen abgefangen.



**370** Webseiten wurden im Durchschnitt an jedem Tag des Berichtszeitraums für den Zugriff aus den Regierungsnetzen gesperrt. **Der Grund:** Die Seiten enthielten Schadprogramme.



6.220  
2022

5.100  
2021



7.120

Teilnehmer hatte die Allianz für Cybersicherheit im Jahr 2023.

Deutschland  
**Digital•Sicher•BSI**

## 13 Monate Cybersicherheit im Überblick

Juni

22

- *Ransomware*-Angriff auf alle Rathäuser eines Landkreises sowie mehrere kommunale Betriebe einer angrenzenden kreisfreien Großstadt
- Neue Technische Richtlinien zur Sicherheit in Telekommunikations-Infrastrukturen, Sicherheit von Digitalen Gesundheitsanwendungen und für Hersteller mobiler Finanzanwendungen
- Gegenseitige Anerkennung von IT-Sicherheitszertifikaten zwischen ANSSI und BSI
- Zweiter Bericht zum Digitalen Verbraucherschutz 2021 erscheint.

August

22

- Industrie- und Handelskammern nach Cyberangriff deutschlandweit offline
- *Ransomware*-Angriffe auf höhere staatliche Einrichtungen in Montenegro
- BSI warnt vor Einsatz unsicherer Funktürschlösser der Marke ABUS.
- BSI startet in Sachsen-Anhalt virtuelle Roadshow für Kommunen.

Oktober

22

- Einsatz der *Ransomware* Prestige unter anderem gegen Unternehmen in Polen
- BSI und Cybersicherheitsbehörde von Singapur erkennen gegenseitig Cybersicherheitskennzeichen an.
- BSI bestätigt Sicherheitseigenschaften von Betriebssystemen von iPhone und iPad.
- Erstes regionales Forum des Cybersicherheitsnetzwerks (CSN) im Rhein-Main-Gebiet durchgeführt

- Neues Zertifizierungsprogramm für Komponenten der 5G-Telekommunikationsnetze
- Saarland wird zweite Pilotregion des Cyber-Sicherheitsnetzwerks (CSN).
- Erste Prüfstelle für Programm NESAS CCS-GI anerkannt
- BSI stellt Tool zum Telementrie-Monitoring für Windows 10 zur Verfügung.

Angriffe auf albanische Regierungsinstitutionen mit der *Ransomware* GoneXML und dem *Wiper* ZeroShred

22

Juli

- Verstärkte *DDoS*-Angriffe durch Hacktivistens-Botnetz-Projekt „DDoSia“
- *Ransomware*-Angriffe auf höhere staatliche Einrichtungen in Bosnien-Herzegowina
- 10 Jahre Allianz für Cybersicherheit (ACS)
- BSI veröffentlicht Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung.

22

September

22

Dezember

- CSAF als internationaler Standard aufgenommen
- Digitalbarometer 2022 von BSI und Polizei

22

November



---

# Gefährdungslage

---



## Teil B: Erkenntnisse zur Gefährdungslage in der Gesellschaft

### 7. – Erkenntnisse zur Gefährdungslage in der Gesellschaft

Menschen in Deutschland leben digital wie nie. Ob Onlineshopping oder Onlinebanking, Nachrichtenkonsum und Information im Netz oder Zeitvertreib in sozialen Medien: Die Digitalisierung hat weitreichende Auswirkungen in zahlreiche Bereiche der Gesellschaft hinein. Das BSI arbeitet mit gezielten Angeboten für Verbraucherinnen und Verbraucher daran, seinen gesetzlichen Auftrag zum digitalen Verbraucherschutz zu erfüllen und Menschen Unterstützung bei der sicheren Nutzung digitaler Angebote zu bieten. Dabei stehen Prävention, Detektion und Reaktion im Mittelpunkt. Im Berichtszeitraum hat das BSI dem Thema Identitätsdaten besondere Aufmerksamkeit gewidmet. Neben Maßnahmen der Verbraucherinnen und Verbraucher, um ihre persönlichen Daten vor Missbrauch zu schützen, stehen insbesondere die Hersteller und Anbieter digitaler Dienste in der Verantwortung.

#### 7.1 – Missbräuchliche Nutzung von Identitätsdaten

Für Verbraucherinnen und Verbraucher war im Berichtszeitraum das Thema Datenleaks prägend. In vielen Fällen standen diese in Verbindung mit *Ransomware*-Angriffen, bei denen Cyberkriminelle große Datenmengen von Organisationen exfiltrierten, um später mit deren Veröffentlichung zu drohen, sofern keine Löse- oder Schweigegeldzahlung erfolgt (vgl. Kapitel *Ransomware*, Seite 14). Betroffen waren sowohl Unternehmen als auch Institutionen des öffentlichen Sektors, wie zum Beispiel Kommunalverwaltungen und Bildungseinrichtungen. Ein erfolgreicher *Ransomware*-Angriff bedeutet einerseits ein enormes Schadenspotenzial für das Angriffsoffer, andererseits wirkt sich dies negativ auf Verbraucherinnen und Verbraucher aus. Während die Angriffsoffer mit der Wiederherstellung der betroffenen informationstechnischen Systeme beschäftigt sind, sehen sich Verbraucherinnen und Verbraucher mit der Veröffentlichung ihrer teils sensiblen

Daten konfrontiert, die häufig Adress-, Bezahl- und/oder Login-Daten umfassen. Erfolgreiche Angriffe mittels *Ransomware* bedeuten für Verbraucherinnen und Verbraucher zudem erhebliche Verfügbarkeitseinschränkungen bis hin zum Ausfall von Behörden- und Unternehmensdienstleistungen. Insbesondere die Beeinträchtigung oder der Ausfall von kritischen Dienstleistungen, wie zum Beispiel ausbleibenden Zahlungen von Sozialleistungen oder Elterngeld, hat gravierende Auswirkungen.

Die infolge eines *Ransomware*-Angriffs erbeuteten Identitätsdaten ermöglichen es den Angreifern, zusätzlichen Druck auf die Angriffsoffer auszuüben, indem sie drohen, die Daten auf dafür eingerichteten Leak-Seiten im Darknet zu veröffentlichen. Einige Angreifer gingen einen Schritt weiter und erstellten dedizierte Webseiten, auf denen von einem Datenleak betroffene Verbraucherinnen und Verbraucher überprüfen konnten, ob ihre Daten gestohlen wurden. Da diese Webseiten im Clear Web, also im öffentlichen Internet, gehostet werden, sind diese von Suchmaschinen indexierbar und können zu Suchergebnissen hinzugefügt werden. Daher ist ein transparenter Umgang, ausgehend von dem Angriffsoffer bis hin zu den potenziell von einem Datenleak betroffenen Verbraucherinnen und Verbrauchern, essenziell, um durch zeitnahe Information und Hilfestellung die negativen Auswirkungen zu begrenzen.

Neben Organisationen waren auch Verbraucherinnen und Verbraucher unmittelbar von Angriffen mittels *Ransomware* betroffen. Cyberkriminelle erpressten, wenn auch vergleichsweise geringe Summen Lösegeld mit *Ransomware*-Angriffen auf private Endgeräte wie beispielsweise Netzwerkspeichergeräte (*NAS*). Die betroffenen Verbraucherinnen und Verbraucher hatten infolgedessen keinen Zugriff mehr auf ihre privaten Daten.

Neben Angriffen mittels *Ransomware* stellten auch sogenannte *Information Stealer* eine Bedrohung für die Datensicherheit von Verbraucherinnen und Verbrauchern dar. Während bei *Ransomware*-Angriffen die Betroffenen selbst das Ziel sind, da von diesen Lösegeld für die Entschlüsselung ihrer Daten verlangt wird, steht bei Angriffen mittels *Information Stealern* der Handel mit gestohlenen Identitätsdaten im Vordergrund. *Information*

*Stealer* sind Schadprogramme, die es Cyberkriminellen ermöglichen, auf infizierten Geräten unbemerkt an unterschiedliche Arten persönlicher Daten, wie beispielsweise Login-Daten für verschiedene Onlinedienste, zu gelangen. Die gestohlenen Daten umfassen auch Cookies und biometrische Daten, wie zum Beispiel Fingerabdrücke. Die entwendeten Anmeldeinformationen bieten Cyberkriminelle anschließend auf Marktplätzen im Darknet zum Verkauf an. Auf einem der größten Untergrundmarktplätze für Identitätsdaten boten Cyberkriminelle Interessenten ein *Browser-Plug-in* an, über das es möglich war, die gestohlenen Anmeldeinformationen direkt im Webbrowser zu importieren. Dadurch konnte die digitale Identität einer anderen Person mit wenigen Klicks angenommen werden.

### Datenleaks aufgrund von Schwachstellen

Datenleaks waren auch auf mangelnde Schutzmaßnahmen für Login-Daten bei Onlinediensten oder Schwachstellen in IT-Produkten, wie zum Beispiel im Onlineshopping, zurückzuführen. So gelang es verschiedenen Angreifern unter anderem, Onlineshops zu kompromittieren und dabei Daten wie Kundennamen, Rechnungs- und Lieferadressen, Telefonnummern, Bestelldetails und auch Zahlungsdaten zu stehlen. Schwachstellen in der von den Onlineshops verwendeten Shop-Software stellen dabei ein großes Risiko für die Sicherheit von Verbraucherdaten dar. Im Berichtszeitraum traten beispielsweise Schwachstellen in Shop-Softwareprodukten auf, die unberechtigte Datenbankzugriffe ermöglichten, durch Zugriff auf den SQL-Manager die Einsicht in abgeschottete Daten erlaubten oder bei Ausnutzung zu einem Cross-Site-Scripting-Angriff führen konnten. Dabei schleusen Angreifer Schadcode in Webformulare oder URLs ein und lassen die Benutzerin oder den Benutzer diesen unbemerkt ausführen.

Im Rahmen einer BSI-Studie zur IT-Sicherheit von Verbraucherdaten im Onlineshopping<sup>5</sup> ergab eine Schwachstellenanalyse von zehn zufällig ausgewählten Shop-Softwareprodukten eine Vielzahl von Schwachstellen mit teilweise gravierenden Auswirkungen auf die Datensicherheit von Verbraucherinnen und Verbrauchern. Nahezu alle getesteten Produkte wiesen eine unzureichende Passwortrichtlinie auf, wodurch ein angemessener Schutz von Kundenkonten nicht gegeben war. Darüber hinaus wies die Hälfte der getesteten Shop-Softwareprodukte JavaScript-Bibliotheken von Drittanbietern auf, die verwundbar durch bekannte Schwachstellen sind und somit ein unkalkulierbares Sicherheitsrisiko darstellen. Die geschilderten Fälle verdeutlichen, dass unzureichende IT-Sicherheits-

maßnahmen das Risiko für Verbraucherinnen und Verbraucher erhöhen, Opfer eines Datenleaks zu werden. Eine ebenfalls im Rahmen der Studie durchgeführte repräsentative Befragung ergab, dass rund ein Viertel der Befragten bereits von einem Datenleak im Onlineshopping betroffen war. Weiterhin gaben 68 Prozent der Befragten an, dass sie generell Bedenken beim Onlineshopping haben.

Angriffe auf Kundendatenbanken bei Onlinediensten oder der Diebstahl von Identitätsdaten infolge von *Malware* liegen meist außerhalb des Einflussbereichs der von einem Datenleak betroffenen Verbraucherinnen und Verbraucher. Derartige Sicherheitsvorfälle mit darauf folgender Veröffentlichung sensibler persönlicher Daten unterminieren daher in besonderer Weise das Vertrauen in die Nutzung digitaler Dienste sowie in die Digitalisierung insgesamt. Zudem können die entwendeten Daten für weitere Angriffe gegen Verbraucherinnen und Verbraucher genutzt werden. Der unbefugte Zugriff und die Veröffentlichung persönlicher Daten stellen daher ein hohes Risiko für Verbraucherinnen und Verbraucher dar.

## 7.2 – Handlungsfelder: Hersteller und Anbieter in der Verantwortung

Die Erkenntnisse zur aktuellen Gefährdungslage in der Gesellschaft machen deutlich, dass neben der Sensibilisierung und Aufklärung von Verbraucherinnen und Verbrauchern insbesondere das verantwortungsvolle Handeln der Hersteller und Anbieter entscheidend für einen wirksamen Digitalen Verbraucherschutz ist. Besonders deutlich wird dies beim Schutz vor drohenden Datenleaks (vgl. Kapitel *Spam und Phishing*, Seite 30), da die Auswirkungen für alle Beteiligten vielfältig und zugleich gravierend sein können. Bei der hersteller- und anbieterseitigen Datenverarbeitung wie auch -speicherung sind daher geeignete technisch-organisatorische Maßnahmen umzusetzen, um

- die Privatsphäre und sensible Kundendaten zu schützen,
- finanzielle Schäden sowohl aufseiten der Verbraucherinnen und Verbraucher (z. B. durch gestohlene Onlinebanking-Zugänge) als auch aufseiten der Hersteller und Anbieter (Bußgelder, Schadenersatzforderungen) zu vermeiden,
- die Reputation des Anbieters zu schützen,
- Vertrauen und langfristige Kundenzufriedenheit zu fördern.

Zu den Maßnahmen gehören unter anderem der Einsatz effektiver Verschlüsselungstechnologien, die regelmäßige Überprüfung und Stresstests der IT-Infrastruktur, die Schulung der Mitarbeitenden im Umgang mit sensiblen Daten sowie die transparente und schnelle Kundenkommunikation im Falle eines Datenabflusses.

Die skizzierten Anforderungen verdeutlichen die Komplexität sowie die Wirkungsmechanismen von IT-Sicherheitsfragen und setzen für Erfolg versprechende Antworten ein tiefes organisatorisches Verständnis für den verantwortungsbewussten Umgang mit digitalen Technologien voraus. Das als Corporate Digital Responsibility (CDR) bezeichnete Denken und Handeln erfordert dabei eine proaktive Herangehensweise, die sich unter anderem im „Security-by-Design“-Ansatz widerspiegelt. Dieser steht für die Berücksichtigung von IT-Sicherheitsaspekten in allen Phasen des Hard- und Softwareentwicklungsprozesses, von der Konzeption bis hin zur Implementierung und zum Betrieb. Durch die frühzeitige Identifikation und Berücksichtigung von Sicherheitsanforderungen können sowohl potenzielle Schwachstellen als auch hohe (monetäre) Aufwendungen für spätere Fehlerbehebungen minimiert werden.

Ein weiterer wichtiger Baustein in der verantwortungsvollen Entwicklung digitaler Alltagstechnologien ist die einfache, barrierefreie und intuitive Gestaltung von Sicherheitsfunktionen (Usable Security) in Geräten und Onlineanwendungen. Deren nutzerfreundliche und zugleich nutzergerechte Ausgestaltung erhöht die Bereitschaft der Verbraucherinnen und Verbraucher, sie zu aktivieren und durchgehend zu nutzen. Positive Nutzungsergebnisse (User Experience) von IT-Sicherheitsmechanismen erhöhen zudem deren Akzeptanz. Usable Security spielt damit auch eine wichtige unterstützende Rolle beim wirksamen Schutz vor *Spam* und *Phishing* im Verbraucheralltag (vgl. Kapitel *Spam und Phishing*, Seite 30).

All diese Anstrengungen zur Verbesserung der IT-Sicherheitseigenschaften von Geräten, Anwendungen und Diensten sollten für Verbraucherinnen und Verbraucher noch transparenter und sichtbarer werden. Klare Kennzeichnungen wie das IT-Sicherheitskennzeichen des BSI sind hierfür ein wirksames Instrument. Das BSI sieht hier die Notwendigkeit, noch stärker gestaltend tätig zu werden, um Informationssicherheit im digitalen privaten Alltag zu fördern.



**Volksbanken Raiffeisenbanken**

um die Auswirkungen der gestiegenen Energiepreise für die Verbraucher abzumildern, wird im September ein Pauschalbetrag von 300 Euro an alle Erwerbstätigen ausbezahlt. Dies ist ein Beschluss der Bundesregierung und Inhalt des Entlastungspakets 2022, welches die durch den Ukraine-Krieg entstandene Energiekosten-Explosion etwas abfedern soll.

Wer erhält die Energiepauschale?

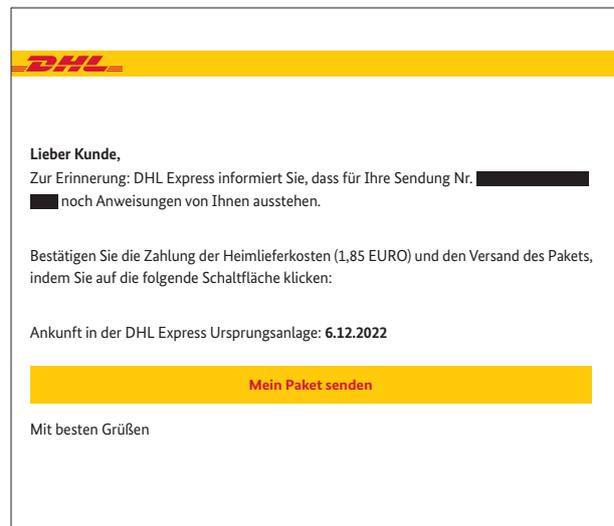
- **Steuerpflichtige** mit Einkünften aus Gewinneinkunftsarten (§ 13, § 15 oder § 18 des Einkommensteuergesetzes) und
- **Arbeitnehmerinnen und Arbeitnehmer**, die Arbeitslohn aus einem gegenwärtigen Dienstverhältnis beziehen und in die Steuerklassen I bis V eingereiht sind oder als **geringfügig Beschäftigte** pauschal besteuert werden.

Um Ihre Identität sowie den Anspruch auf eine Auszahlung feststellen zu können, benötigen wir eine Bestätigung Ihrer bereits angegebenen Daten bei der Erstellung Ihres Girokontos in einer unserer Filialien.

Geben Sie noch heute Ihre aktuellen Daten auf unserer Homepage an und erhalten Sie innerhalb der nächsten vier Wochen Ihre Auszahlung der Energiepauschale. Dies können Sie ganz bequem von zu Hause aus erledigen, anbei finden Sie einen Direktlink zu den geforderten ...

[Zur Homepage](#)

Abbildung 13: Beispiel einer *Phishing*-Mail im Namen von Banken  
Quelle: *Phishing*-Radar vom 09. September 2022<sup>6</sup>



**DHL**

Lieber Kunde,

Zur Erinnerung: DHL Express informiert Sie, dass für Ihre Sendung Nr. [REDACTED] [REDACTED] noch Anweisungen von Ihnen ausstehen.

Bestätigen Sie die Zahlung der Heimlieferkosten (1,85 EURO) und den Versand des Pakets, indem Sie auf die folgende Schaltfläche klicken:

Ankunft in der DHL Express Ursprungsanlage: **6.12.2022**

[Mein Paket senden](#)

Mit besten Grüßen

Abbildung 14: Beispiel einer *Phishing*-Mail im Namen eines Paketversanddienstleisters  
Quelle: *Phishing*-Radar vom 02. Dezember 2022<sup>7</sup>

## Identitätsdiebstahl mit Phishing-as-a-Service (PhaaS)

### Sachverhalt

Es gibt inzwischen eine Vielzahl an PhaaS-Anbietern, die einen unterschiedlichen Umfang an Services für Angreifer anbieten: von der Erstellung und dem Versand von Phishing-E-Mails über die Verwaltung von Weiterleitungswebseiten und den endgültigen Köderseiten bis hin zu technischem Support und Schritt-für-Schritt-Tutorials. Häufig gibt es schon fertige Phishing-Seiten für bekannte Webseiten wie unter anderem Google, Microsoft, LinkedIn, iCloud, Facebook, Twitter, Yahoo, WordPress und Dropbox. Daneben gibt es auch Angebote, auf Anfrage individuelle Phishing-Seiten für spezielle Angriffszwecke zu erstellen.

Gängig sind Phishing-Proxy-Services, die als Man-in-the-Middle (MITM) zwischen Opfer und der Login-Seite eines Unternehmens agieren. In der Regel können sie Zugangsdaten und Cookies stehlen und somit beispielsweise auch Multifaktor-Authentifizierung umgehen.

Ein Beispiel für einen Phishing-Proxy-Service ist EvilProxy. Besorgniserregend ist, dass EvilProxy neben den Phishing-Login-Seiten für Google, Microsoft & Co. auch Phishing-Login-Seiten für den Python Package Index (offizielles Softwareverzeichnis für die Programmiersprache

Python), npmjs (von über 11 Millionen Entwicklern weltweit genutzter JavaScript Package Manager) und GitHub (Softwareentwickler-Plattform) anbietet. Eine Kompromittierung solcher Seiten könnte zu Supply-Chain-Angriffen durch böartig modifizierte oder geklonte Code-Repositories führen und beispielsweise legitime Software mit Information Stealern infizieren, die Zugangsdaten stehlen.

### Bewertung

Phishing bleibt weiterhin ein verlässlicher Vektor für Angreifer, um initialen Zugang zu IT-Netzen zu erhalten. Durch die zuvor genannten PhaaS-Angebote können auch weniger fortschrittliche Angreifer mit geringen Ressourcen Phishing-Angriffe durchführen, was einen deutlichen Einfluss auf die weitere Entwicklung von Phishing haben wird. Darüber hinaus sind Phishing-Aktivitäten vielfältiger geworden und beinhalten Angriffe über Social Media, SMS und Voice-Calls.

### Reaktion

Das BSI warnt Nutzerinnen und Nutzer über seine Social-Media-Kanäle.

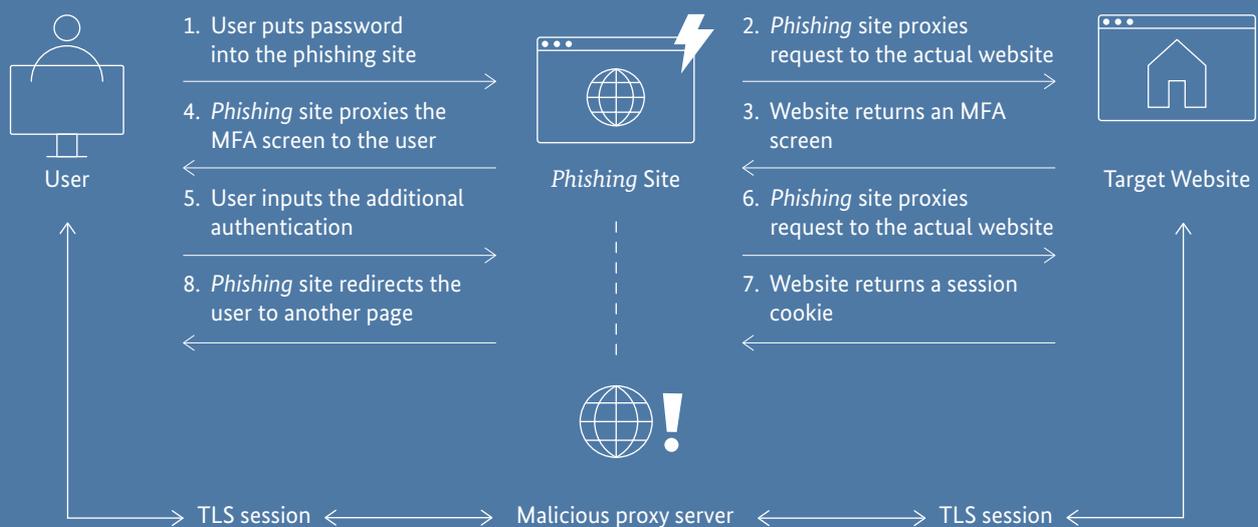


Abbildung 15: Umgehung von Multifaktor-Authentifizierung

## 8. – Erkenntnisse zur Gefährdungslage in der Wirtschaft

Mit einem Blick auf die Cybersicherheitslage in der Wirtschaft zeigt sich, dass ein großer Teil der deutschen Unternehmen die Bedeutung von Cybersicherheit erkannt hat. In einer Umfrage des TÜV-Verbandes aus 2023 gaben 95 Prozent der befragten Unternehmen an, dass Cybersicherheit ein Muss für den Schutz der Unternehmensdaten ist. Ebenso sehen sie 80 Prozent der Unternehmen als Grundvoraussetzung für einen reibungslosen Geschäftsablauf an<sup>8</sup>. Dies spiegelt sich auch in konkreten Maßnahmen wider. Seit 2020 sind die Ausgaben für das IT-Sicherheitsbudget in Unternehmen kontinuierlich gestiegen. Das Statistische Bundesamt geht von einer jährlichen Wachstumsrate von 10,5 Prozent aus<sup>9</sup>. 2022 wurde mit rund 7,8 Milliarden Euro so viel wie noch nie in Cybersicherheit investiert.

Gleichwohl sind weitere Schritte hin zu mehr Cybersicherheit dringend notwendig. Nach Schätzungen des Digitalverbandes Bitkom haben deutsche Unternehmen im Jahr 2022 einen Schaden von 203 Milliarden Euro<sup>10</sup> durch Cyberangriffe erlitten. Nahezu jedes deutsche Unternehmen sei dabei schon einmal von einem Angriff betroffen gewesen. Angesichts dieser Verluste ist eine Ausweitung der Cybersicherheitsmaßnahmen unerlässlich, auch wenn viele Unternehmen eine kontinuierliche Umsetzung von Cybersicherheitsmaßnahmen im laufenden Betrieb noch immer als Hemmnis empfinden<sup>11</sup>.

### Gestiegene Bedrohungslage

Die Corona-Pandemie hat einerseits die Digitalisierung in deutschen Unternehmen stark beschleunigt, andererseits neue Angriffsflächen geschaffen. Zudem erleben viele Unternehmen den russischen Angriffskrieg auf die Ukraine und die sich verändernde globale Sicherheitsarchitektur als große Herausforderungen. Obwohl diese Unsicherheit besteht, kann das BSI, wie bereits im Kapitel *Advanced Persistent Threats* und Bedrohungen im Kontext des Ukraine-Kriegs (Seite 25) beleuchtet wurde, aufgrund der vorliegenden Erkenntnisse keine gesteigerte Bedrohung im Kontext des Ukraine-Kriegs auf deutsche Unternehmen feststellen.

Wirklich angespannt wird die Bedrohungslage für Unternehmen durch finanziell motivierte Cyberangriffe. Die größte Bedrohung für Wirtschaftsunternehmen besteht nach wie vor durch *Ransomware* und *Ransomware as a Service* (vgl. Kapitel *Ransomware*, Seite 14). Es zeigt sich

eine fortschreitende Professionalisierung, gekoppelt mit einer Eskalationsspirale an Maßnahmen, um Druck auf die erpressten Unternehmen auszuüben. Längst wird das betroffene System nicht nur verschlüsselt. Es ist mittlerweile gängige Praxis, dass die Täter im nächsten Schritt dem betroffenen Unternehmen und im dritten Schritt (Triple Extortion) auch dessen Kunden mit der Veröffentlichung der Daten drohen. Damit werden Unbeteiligte, deren Systeme nicht betroffen waren, ebenfalls zu Opfern.

Unter den bekannt gewordenen *Ransomware*-Opfern stachen im aktuellen Berichtszeitraum IT-Dienstleister hervor. Von den insgesamt 68 bekannt gewordenen Opfern von *Ransomware*-Angriffen waren 15 IT-Dienstleister. Für Angreifer stellen IT-Dienstleister hochattraktive Opfer dar, da über deren Dienstleistungen oder Kundenbeziehungen potenziell eine Vielzahl weiterer Opfer angegriffen und erpressbar gemacht werden kann (vgl. Vorfall *Cyberangriffe auf IT-Dienstleister*, Seite 57).

### Cybercrime-Schattenwirtschaft

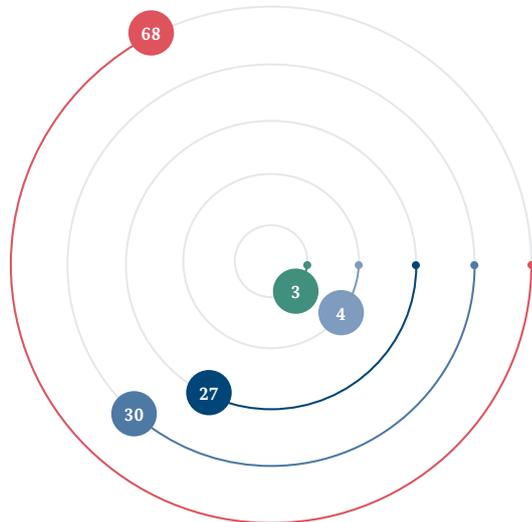
Die Angriffe auf Wirtschaftsunternehmen sind breit gestreut. Einerseits werden nach wie vor umsatzstarke Großunternehmen angegriffen. Gleichzeitig werden *Ransomware*-Angriffe aufgrund der niedrigen Kosten durch *RaaS* auch zum Massengeschäft. Dabei gehen die Kriminellen den Weg des geringsten Widerstandes, sodass jetzt zunehmend die kleinen und mittleren Unternehmen (KMU), aber auch Kommunen, Universitäten und Forschungseinrichtungen stärker betroffen sind.

Das BSI beobachtet in dieser Professionalisierung den Aufbau einer Cybercrime-Schattenwirtschaft (siehe auch Kapitel *Ransomware*, Seite 14). Unternehmen stehen keinem einzelnen Angreifer, sondern einer arbeitsteiligen und effizient aufgestellten Angreiferindustrie gegenüber.

Gleichzeitig führt die zunehmende Spezialisierung auch zu einer neuen Stufe der Bedrohung. Mit gut gemachten Angriffen wird eine höchstmögliche Zahl von Unternehmensnetzwerken erreichbar – mittlerweile sogar ohne dass der *Angriffsvektor* im betroffenen Unternehmen war. Diese neue Bedrohungsqualität wird beispielsweise anhand des Sicherheitsvorfalls bei einem Anbieter von VoIP-Software im März 2023 deutlich. Hier waren durch einen doppelten Lieferkettenangriff potenziell rund 600.000 Unternehmen über eine mit einem gültigen 3CX-Zertifikat signierte Anwendung bedroht (vgl. Vorfall *Cyberangriffe auf IT-Dienstleister*, Seite 57).

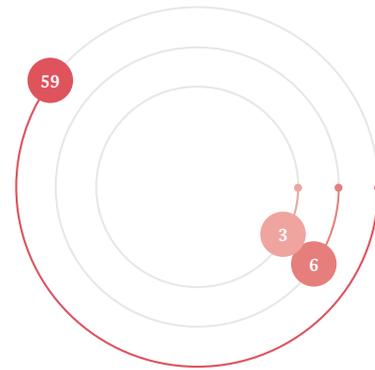
## Bekannt gewordene Ransomware-Opfer in Deutschland im Berichtszeitraum nach Art des Opfers

Anzahl



- Kommunen, kommunale Betriebe
- Krankenhäuser
- Sonstige
- Forschungs- und Bildungseinrichtungen
- Andere (Anteile siehe rechts)

Abbildung 16: Bekannt gewordene Ransomware-Opfer in Deutschland  
Quelle: Ransomware-Opfer-Statistik des BSI



- Mittlere Unternehmen
- Große Unternehmen
- Kleine, Kleinstunternehmen

### Ein starker Schutzschild: Cyberresilienz

Um sich in dieser Bedrohungslage gut aufzustellen, ist es notwendig, dass Unternehmen jetzt in ihre Cyberresilienz investieren. Dazu gehören technische und organisatorische Maßnahmen wie regelmäßige Sicherheitsupdates, Backups und Schulungen der Mitarbeitenden. Während große Unternehmen hier in der Regel gut aufgestellt sind, haben KMU meist noch dringenden Nachholbedarf. So geben beispielsweise laut einer Umfrage der DIHK nur 61 Prozent der Kleinstunternehmen an, regelmäßig Backups zu machen (vgl. Kapitel *Besondere Situation von KMU in Deutschland*, Seite 64). Wenn es um das Erstellen von Notfallplänen geht, haben sowohl große als auch kleinere Unternehmen noch Nachholbedarf. Weniger als ein Drittel der Unternehmen verfügt über einen schriftlich fixierten Notfallplan. Das BSI bietet hier für die Zielgruppe KMU mit dem „Maßnahmenkatalog Notfallmanagement“ und einem Einseiter einen leichten Einstieg in das Notfallmanagement.

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 weiterer wesentlicher Faktor sind der Austausch und die Kommunikation über Sicherheitsvorfälle. Immer mehr Unternehmen gehen transparent mit einem Vorfall um und informieren die Öffentlichkeit und ihre Kundinnen und Kunden. Dies trägt dazu bei, dass potenzielle Schwachstellen schneller behoben und Schäden von weiteren Unternehmen abgewendet werden können.

Das BSI bietet mit seinen Angeboten für die Wirtschaft und dem Netzwerk der Allianz für Cybersicherheit zahlreiche Unterstützungsangebote, damit Unternehmen resilienter werden und einen starken Schutzschild für mehr Cybersicherheit aufbauen können.

**Den Maßnahmenkatalog des BSI für Unternehmen finden Sie hier:<sup>h</sup>**



**Weiterführende Informationen für Unternehmen finden Sie hier:<sup>i</sup>**



---

## Cyberangriffe auf IT-Dienstleister

---

### Sachverhalt

Im Berichtszeitraum wurden mehrere Ransomware-Angriffe auf deutsche IT-Dienstleister bekannt. Betroffen waren neben den IT-Dienstleistern selbst häufig auch deren Kunden, sowohl in der öffentlichen Verwaltung als auch in Wirtschaft und Gesellschaft. So wurden neben verschiedenen Kommunalverwaltungen beispielsweise auch soziale und gemeinnützige Einrichtungen beeinträchtigt.

Die Arbeitsfähigkeit der betroffenen IT-Dienstleister wurde durch die Angriffe eingeschränkt. Für Kunden entwickelte Software konnte entweder nicht weiterent-

wickelt oder nicht ausgeliefert werden. Zudem wurde die Arbeitsfähigkeit der Kunden der betroffenen Dienstleister ebenfalls teilweise stark eingeschränkt.

### Bewertung

IT-Dienstleister stellen für Cyberkriminelle besonders interessante Ziele dar, da Angriffe auf einen einzelnen Dienstleister Schadwirkungen bei zahlreichen Opfern zur Folge haben können und der Erpressungsdruck damit vergleichsweise hoch ist. Das BSI empfiehlt grundsätzlich, keine Lösegelder oder Schweigegelder zu zahlen.

---

## Industrie- und Handelskammern nach Cyberangriff deutschlandweit offline

---

### Sachverhalt

Der IT-Dienstleister der Industrie- und Handelskammern entdeckte am 3. August 2022 ein auffälliges Verhalten in den bei ihm gehosteten IT-Systemen. Das IHK Cyber Emergency Response Team (IHK-CERT) hat diese Anomalien untersucht. In Zusammenarbeit mit externen IT-Sicherheitsfachleuten wurde entschieden, die Systeme aus Sicherheitsgründen herunterzufahren, um größeren Schaden durch Diebstahl von Daten oder die mögliche Verschlüsselung von Daten zu verhindern.

Dies hatte zur Folge, dass die Verbindung aller 79 Industrie- und Handelskammern in Deutschland zum Internet getrennt wurde und deren Dienste nicht mehr zur Verfügung standen. Dadurch waren Webseiten offline und die Mitarbeitenden weder telefonisch noch per E-Mail erreichbar. Auch interne Anwendungen funktionierten nicht oder nur mit Einschränkungen.

### Bewertung

Der Cyberangriff wurde höchstwahrscheinlich von professionellen Angreifern ausgeführt. Deren Vorgehensweise deutet auf Spionage- oder Sabotage-Ziele hin, auch wenn sich eine finanziell ausgerichtete Motivation der Angreifer nicht ausschließen lässt.

### Reaktion

Um das Risiko weiterer Angriffe und möglicher Kompromittierungen zu verringern, wurden sämtliche Anwendungen und IT-Systeme erst nach einer intensiven Prüfung schrittweise wieder hochgefahren. Einzelne Kammern und verschiedene Dienstleistungen der Organisation waren auch Monate später noch beeinträchtigt.

## 8.1 – Gefährdungslage Kritischer Infrastrukturen

Kritische Infrastrukturen sind Organisationen mit wichtiger Bedeutung für das Gemeinwesen. Die Betreiber Kritischer Infrastrukturen erbringen für die Bevölkerung kritische Dienstleistungen wie die Versorgung mit Strom, Wasser oder Lebensmitteln. Zu den kritischen Dienstleistungen zählen darüber hinaus unter anderem der öffentliche Nahverkehr, die Bargeldversorgung und die medizinische Versorgung. Kritische Infrastrukturen bilden eine entscheidende Grundlage für das Funktionieren unserer Gesellschaft. Dennoch erkennt man ihre Bedeutung gelegentlich erst, wenn es zu Störungen kommt.

**„Kritische Infrastrukturen sind Organisationen oder 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-Definition der Bundesressorts)

Alle kritischen Dienstleistungen sind ganz besonders von einer störungsfrei arbeitenden IT abhängig. Daher sieht das BSI-Gesetz (BSIG) für KRITIS-Betreiber Maßnahmen zur Prävention (§ 8a BSIG) und zur Bewältigung (§ 8b BSIG) von IT-Sicherheitsvorfällen oder IT-Störungen vor.

### Bedrohung und Bewältigung

Bei Betreibern Kritischer Infrastrukturen können erfolgreiche Angriffe auf die IT-Infrastruktur nicht nur zu Schäden beim Unternehmen selbst führen, sondern sie wirken sich auch auf die Versorgung der Bevölkerung mit kritischen Dienstleistungen und damit auf die Daseinsvorsorge aus. Umso wichtiger ist es, dass Betreiber und staatliche Stellen zusammenarbeiten, um Angriffe zu verhindern oder Auswirkungen zu mildern.

Betreiber Kritischer Infrastrukturen im Sinne des BSIG sind verpflichtet, Vorfälle dem BSI zu melden. So meldete zum Beispiel ein Klinikum im Mai 2023 einen Vorfall und arbeitete zudem mit dem zuständigen Landeskriminalamt zusammen, um die Lage zu bewältigen. Es wäre aber wünschenswert, dass sich auch Betreiber Kritischer Infrastrukturen, die wegen der Unterschreitung der Schwellenwerte laut BSI-KritisV nicht unter die Regelungen des BSIG fallen, bei entsprechenden Vorfällen an staatliche Stellen wenden. Der hierfür notwendige Vertrauensaufbau kann insbesondere in der öffentlich-pri-

vaten Kooperation UP KRITIS (vgl. Kapitel *Nicht regulierte KRITIS-Wirtschaft: UP KRITIS*, Seite 60) erfolgen und Vorteile für alle Seiten bieten. Das BSI ist grundsätzlich für alle Betreiber Kritischer Infrastrukturen ansprechbar und rät dazu, den Kontakt zu staatlichen Stellen bereits zu suchen, bevor etwas passiert. So lässt sich im Fall der Fälle einfacher und vertrauensvoller zusammenarbeiten und ein schwerer IT-Vorfall gemeinsam bewältigen, bevor er sich zur Krise ausweitet.

### Die Lage im Sektor Gesundheit

Die Auswertung von Vorfallmeldungen aus dem Bereich medizinische Versorgung zeigt eine hohe Bereitschaft der Betreiber, ihre Vorfälle an das BSI zu melden. Die Meldungen sind für die Erstellung eines detaillierten Lagebilds durch das BSI entscheidend und bilden die Basis für zielgruppenorientierte Warn- und Informationsmeldungen, die das BSI den regulierten Betreibern Kritischer Infrastrukturen und den Teilnehmern des UP KRITIS zur Verfügung stellt.

Hierzu werden die Meldungen durch das BSI sanitarisieren, das heißt, schutzbedürftige Informationen werden aus einer Meldung entfernt, während die für andere Betreiber relevanten Informationen bestehen bleiben.

Fast die Hälfte der eingegangenen Meldungen aus dem Sektor Gesundheit zeigten einen Ausfall oder eine Beeinträchtigung der durch den Betreiber erbrachten kritischen Dienstleistung an. Als Grund für die Störungen wurde in den meisten Fällen technisches Versagen angegeben. Dies korreliert mit den in den turnusmäßigen Nachweisen gemäß § 8a Abs. 3 BSIG festgestellten Mängeln: Die meisten Mängel im Sektor Gesundheit betreffen den Bereich „Technische Informationssicherheit“.

In etwa 20 Prozent der Meldungen aus dem KRITIS-Sektor Gesundheit spielten Angriffe eine Rolle. Bei diesen lässt sich ein zunehmender Fokus auf die Dienstleister der Betreiber als Einfallstor feststellen: Anstatt KRITIS-Betreiber und Behörden direkt anzugreifen, zielen diese sogenannten Supply-Chain-Angriffe auf Anbieter, Lieferanten und damit auf die etablierten Lieferketten ab. Indem Produkte bereits bei den Herstellern oder Drittanbietern kompromittiert werden, beschränkt sich der mögliche Schaden nicht nur auf das angegriffene Unternehmen selbst, sondern betrifft alle in der Wertschöpfungskette nachgelagerten Unternehmen. Dieser Multiplikatoreffekt macht Supply-Chain-Angriffe für Kriminelle besonders lukrativ, was das vermehrte Auf-

treten solcher Attacken erklären kann. Der beschriebene Trend ist nicht auf den Sektor Gesundheit beschränkt. Auch Betreiber in anderen Sektoren sind grundsätzlich Angriffen auf Lieferketten ausgesetzt, mit denen zahlreiche etablierte Maßnahmen der Prävention umgangen werden können.

In Prüfungen nach § 8a Abs. 4 BSIG hat das BSI mehrfach festgestellt, dass die Beziehungen zwischen Betreibern und Dienstleistern so gestaltet sind, dass die Betreiber ihrer Verantwortung in Bezug auf einen angemessenen IT-Schutz nicht ausreichend nachkommen können. Denn auch bei Auslagerung von IT-Dienstleistungen verbleibt die Sicherheitsverantwortung beim KRITIS-Betreiber. Auch eine Risikobewertung der Dienstleisterbeziehung findet häufig nicht statt. So ist manchmal unklar, wer welchen Teil der Betreiberverantwortung übernimmt und ob die getroffenen Maßnahmen tatsächlich ausreichen.

#### **Gesetzliche Verpflichtung zum Einsatz von Systemen zur Angriffserkennung**

Betreiber Kritischer Infrastrukturen sind verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen. 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 Systeme stellen eine effektive Maßnahme zur Erkennung von Cyberangriffen dar und unterstützen insbesondere die Schadensreduktion. Die Betreiber mussten die Einführung eines Systems zur Angriffserkennung erstmalig bis zum 1. Mai 2023 gegenüber dem BSI nachweisen. Die gesetzliche Verpflichtung betrifft aber nicht nur KRITIS-Betreiber, die die Schwellenwerte der BSI-KritisV überschreiten, sondern über § 11 Abs. 1d Energiewirtschaftsgesetz (EnWG) auch alle Strom- und Gasnetzbetreiber.

Insbesondere gegen die Bedrohung durch *Ransomware* bietet ein effektives System zur Angriffserkennung zusätzlichen Schutz. Solche Systeme ermöglichen es, einen Angreifer zu entdecken, der bereits im Netzwerk ist, aber noch nicht mit der Verschlüsselung begonnen hat. Zudem ermöglicht ein frühzeitiges Erkennen, die gewonnenen Erkenntnisse über den Angreifer oder den *Angriffsvektor* mit anderen Einrichtungen zu teilen und so zum kollektiven Schutz beizutragen.

#### **Neue EU-Richtlinien zum Schutz Kritischer Infrastrukturen und weiterer kritischer Einrichtungen**

Am 16. Januar 2023 sind zwei Richtlinien der EU in Kraft getreten:

- die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union mit Fokus auf IT-Sicherheit (NIS-2-Richtlinie, Network Information Security)<sup>12</sup>
- die Richtlinie über die *Resilienz* kritischer Einrichtungen mit Fokus auf physische Sicherheit (CER-Richtlinie, Critical Entities Resilience)<sup>13</sup>

Diese Richtlinien müssen in den Mitgliedsstaaten bis zum 17. Oktober 2024 in nationales Recht umgesetzt werden. Beide Richtlinien haben unter anderem zum Ziel, dass kritische Einrichtungen einheitlich besser vor Cyberangriffen, Sabotage und Naturgefahren geschützt werden. Hierbei wird auch in Deutschland der Kreis der durch gesetzliche Regulierung erfassten Einrichtungen erheblich ausgeweitet. Dies wird nicht nur bei den betroffenen Unternehmen zu verstärkten Investitionen in die Cybersicherheit führen, sondern auch für das BSI als Aufsichtsbehörde zahlreiche zusätzliche Aufgaben mit sich bringen.

#### **Zahl der regulierten Unternehmen wird stark ansteigen**

Derzeit sind Anforderungen an die Cybersicherheit Kritischer Infrastrukturen in Deutschland in erster Linie durch das BSI-Gesetz mit der zugehörigen BSI-KritisV festgelegt. Durch die beiden EU-Richtlinien werden zukünftig sowohl der Kreis der regulierten Unternehmen als auch die Anforderungen an diese erweitert. Für die EU werden harmonisierte Vorgaben zum Schutz von wichtigen, besonders wichtigen und kritischen Einrichtungen vor Cybersicherheits- und physischen Bedrohungen verpflichtend. Die von den Richtlinien erfassten Sektoren sind zu einem Großteil mit denen des § 2 Abs. 10 BSIG in Verbindung mit der BSI-KritisV identisch (vgl. Tabelle 2).

#### **NIS-2-Richtlinie – Stärkung der Cybersicherheit der wichtigen und besonders wichtigen Einrichtungen**

Durch ihren Fokus ist die NIS-2-Richtlinie für die IT-Sicherheit und deren regulatorischen Rahmen von besonderer Bedeutung. Sie ist die Fortentwicklung der ersten NIS-Richtlinie, die im August 2016 in Kraft getreten ist. Angesichts der gestiegenen Bedrohung, insbesondere durch Cyberangriffe, die mit der stark zunehmenden

KRITIS nach nat. KRITIS-Strategie	KRITIS gemäß §2 (10) BSIG	NIS-2-Richtlinie	CER-Richtlinie
Energie	Energie	Energie	Energie
Transport und Verkehr	Transport und Verkehr	Verkehr	Verkehr
Finanz- und Versicherungswesen	Finanz- und Versicherungswesen	Bankwesen und Finanzmarktinfrastrukturen	Bankwesen und Finanzmarktinfrastrukturen
Gesundheit	Gesundheit	Gesundheit	Gesundheit
Wasser	Wasser	Wasser	Wasser
Informationstechnik und Telekommunikation	Informationstechnik und Telekommunikation	Digitale Infrastruktur, Verwaltung von IKT-Diensten	Digitale Infrastruktur
Ernährung	Ernährung	–	Ernährung
Siedlungsabfallentsorgung	Siedlungsabfallentsorgung	–	–
Medien und Kultur	–	–	–
–	–	Weltraum	Weltraum
Staat und Verwaltung	–	Öffentliche Verwaltung	Öffentliche Verwaltung

Tabelle 2: KRITIS-Sektoren nach der nationalen KRITIS-Strategie, dem BSI-Gesetz und den aktuellen EU-Richtlinien  
Quelle: BSI

Digitalisierung in allen Bereichen der Wirtschaft und bei staatlichen Einrichtungen einhergehen, weitet die NIS-2-Richtlinie Vorgaben zur Cybersicherheit auf mehr Sektoren und mehr Unternehmen aus. Sie legt Sicherheitsanforderungen für eine deutlich größere Zahl von Unternehmen fest, als bisher durch die BSI-KritisV erfasst wurden, und erweitert den Handlungsrahmen zur Durchsetzung der gesetzlichen Anforderungen. Zusätzlich werden Teilen der öffentlichen Verwaltung entsprechende Pflichten auferlegt.

Ein wichtiges Merkmal in der NIS-2-Richtlinie ist die Unterscheidung zwischen wichtigen und besonders wichtigen Einrichtungen. Für besonders wichtige Einrichtungen gelten im Hinblick auf den Umfang der staatlichen Aufsicht schärfere Vorschriften als für wichtige Einrichtungen. Die Anzahl Letzterer ist dafür deutlich größer. Die heute bereits nach BSIG regulierten Kritischen Infrastrukturen gehören in aller Regel zu den besonders wichtigen Einrichtungen im Sinne der NIS-2-Richtlinie. Die in der NIS-2-Richtlinie adressierten

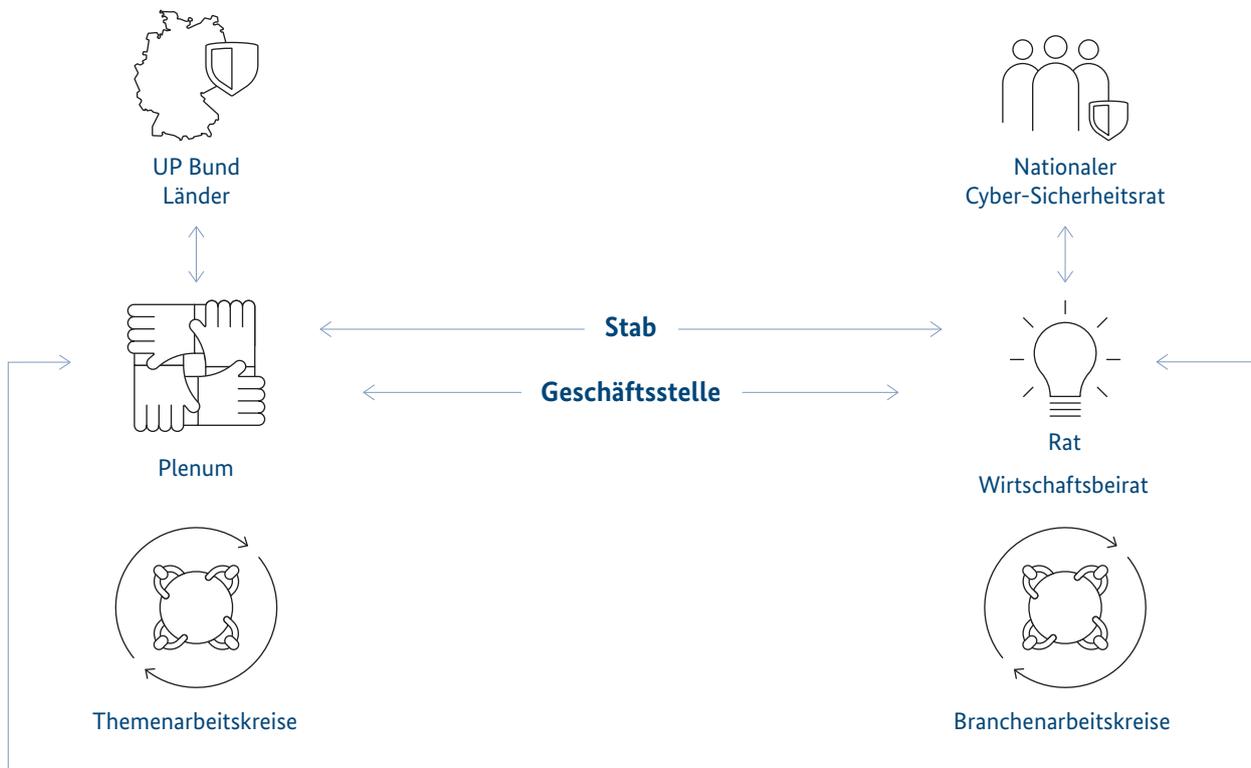
Sektoren gehen jedoch über die KRITIS-Sektoren aus dem BSIG hinaus. Für wichtige und besonders wichtige Einrichtungen, einschließlich bisheriger Betreiber Kritischer Infrastrukturen, ist daher mit veränderten Pflichten und Anforderungen aus der Umsetzung der NIS-2-Richtlinie in nationales Recht zu rechnen.

### 8.1.1 – Kooperation zwischen Staat und KRITIS-Wirtschaft: *UP KRITIS*

Im *UP KRITIS* arbeiten KRITIS-Betreiber, deren Fachverbände und die zuständigen Behörden zusammen, um die Kritischen Infrastrukturen in Deutschland zu schützen. Teilnehmer im *UP KRITIS* können alle Betreiber Kritischer Infrastrukturen werden, auch wenn im Einzelfall die jeweiligen Schwellenwerte der BSI-KritisV nicht erreicht werden. Es nehmen mehr als 900 Organisationen am *UP KRITIS* teil (Stand: Juni 2023). Der fachliche Aus-

## Gremien des UP KRITIS

Abbildung 17: Gremien des UP KRITIS



tausch erfolgt insbesondere in Themen- und Branchenarbeitskreisen. Die Selbstverwaltung des UP KRITIS geschieht über folgende Gremien:

- Rat – arbeitet auf politischer Ebene, besteht aus hochrangigen Personen aus den KRITIS-Sektoren sowie aus den Behörden Bundesministerium des Innern und für Heimat (BMI), Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BKK) und BSI,
- Plenum – in dieses Gremium entsenden alle Branchen- und Themenarbeitskreise einen Sprecher,
- Stab – der Arbeitskreis des Plenums, dessen Mitglieder im Plenum bestimmt werden,
- Geschäftsstelle – diese liegt im BSI und bearbeitet insbesondere Anmeldungen und übernimmt andere administrative Aufgaben.

Das BSI nimmt an den meisten Arbeitskreisen, dem Plenum, dem Stab und dem Rat des UP KRITIS teil (vgl. auch Abbildung 17: Gremien des UP KRITIS).

### Im Berichtszeitraum gab es unter anderem folgende Entwicklungen im UP KRITIS:

- Der Themenarbeitskreis „Anforderungen an Lieferanten und Hersteller“ hat ein Papier mit Empfehlungen zu Entwicklung und Bereitstellung von in Kritischen Infrastrukturen eingesetzten Produkten veröffentlicht.
- Der Themenarbeitskreis „Auswirkungen Ukraine-Krise“ wurde umbenannt in „Auswirkungen aktueller Krisen und Ereignisse“.
- Der UP KRITIS hat folgende Gesetzesvorhaben begleitet: Änderungsverordnung zur BSI-KritisV, die NIS-2-Richtlinie, die CER-Richtlinie und das KRITIS-Dachgesetz. Es fanden erste Aktivitäten statt, um den UP KRITIS für das Inkrafttreten der neuen Gesetze umzugestalten.

Weiterführende Informationen  
finden Sie hier:!



### 8.1.2 – Anbieter digitaler Dienste

Im Zusammenhang mit dem russischen Angriffskrieg gegen die Ukraine ist auch die Cybersicherheit der Anbieter digitaler Dienste stärker in den Fokus gerückt. Zu ihnen zählen Online-Marktplätze, Online-Suchmaschinen und *Cloud-Computing*-Dienste. Diese werden nach § 8c BSIG reguliert.

Da bisher noch keine Registrierungspflicht für die Anbieter digitaler Dienste bestand, war es für regulierende Behörden wie das BSI in vielen Fällen schwierig, die Anbieter zu identifizieren und einen Kontakt zu etablieren, damit diese (analog zu den Betreibern Kritischer Infrastrukturen) BSI-Produkte, wie zum Beispiel Sicherheitswarnungen, erhalten.

Mit der Überarbeitung der NIS-Richtlinie wurde eine Registrierungspflicht für die Anbieter digitaler Dienste eingeführt. Hierdurch sollen eine bessere Sichtbarkeit von Sicherheitsvorfällen und der unmittelbare Kontakt zu den Anbietern in diesem Bereich gewährleistet werden.

Mit der NIS-2-Richtlinie werden darüber hinaus die *Cloud-Computing*-Dienste den besonders wichtigen Einrichtungen zugeordnet und unterliegen denselben Pflichten wie Betreiber Kritischer Infrastrukturen. Zusätzlich sind die Social-Media-Plattformen als neue Kategorie in den Kreis der Anbieter digitaler Dienste aufgenommen worden.

### 8.1.3 – Statistiken

#### Meldungen nach KRITIS-Sektoren (§ 8b Abs. 4 BSIG)

Mit dem IT-Sicherheitsgesetz wurde im Jahr 2015 in § 8b Abs. 4 BSIG eine Meldepflicht für Betreiber Kritischer Infrastrukturen eingeführt. Die Meldepflicht gilt für Störungen, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben oder führen können.

Im Berichtszeitraum gingen beim BSI 490 entsprechende Meldungen ein, die Verteilung auf die KRITIS-Sektoren zeigt Tabelle 3. Ein hohes Meldeaufkommen ist nicht zwangsläufig ein Indikator für den Stand der Informationssicherheit des jeweiligen Sektors. Betreiber Kritischer Infrastrukturen melden zum Teil auch Vorkommen, die

unterhalb der gesetzlichen Meldeschwelle liegen, und tragen dadurch zum Lagebild bei. Die Anzahl der Meldungen entspricht nicht der Anzahl der Vorfälle, die gemeldet worden sind. Vorfälle, die über einen längeren Zeitraum andauern, beinhalten in der Regel eine Initialmeldung, ein oder mehrere aktualisierende Meldungen und eine Abschlussmeldung.

Sektor	Meldung
Energie:	99
Informationstechnik und Telekommunikation:	81
Transport und Verkehr:	111
Gesundheit:	132
Wasser:	16
Ernährung:	9
Finanz- und Versicherungswesen:	61
Siedlungsabfallentsorgung (neuer Sektor):	0
Gesamt:	490

Tabelle 3: Meldungszahlen nach KRITIS-Sektoren im Berichtszeitraum  
Quelle: BSI

#### Reifegrade der Managementsysteme für Informationssicherheit und Geschäftskontinuität bei KRITIS-Betreibern

Betreiber Kritischer Infrastrukturen sind nach § 8a Abs. 3 BSIG gesetzlich verpflichtet, alle zwei Jahre gegenüber dem BSI nachzuweisen, dass ihre IT-Sicherheit auf dem aktuellen Stand der Technik ist. Diese Nachweise enthalten eine Einschätzung der prüfenden Stelle zur Wirksamkeit der Managementsysteme für Informationssicherheit (ISMS) und Geschäftskontinuität (Business Continuity Management System, BCMS) beim geprüften Betreiber. Dies geschieht mittels eines Reifegradmodells, das es ermöglicht, den Fortschritt von ISMS und BCMS im Hinblick auf die Sicherstellung der kritischen Dienstleistung nachvollziehbar über Prüfzyklen hinweg zu dokumentieren, ohne sich dabei auf Einzelmaßnahmen zu fokussieren.

Die Einteilung in Reifegrade orientiert sich an klassischen Reifegradmodellen. Eine Reifegradbestimmung nach wissenschaftlichen Methoden wird vom BSI jedoch nicht gefordert. Der attestierte Reifegrad stellt eine potenzielle Kennzahl zur Steuerung in einer Institution dar.

Die Orientierungshilfe zu Nachweisen gemäß § 8a Abs. 3 BSIG beschreibt folgende Reifegrade für ISMS und BCMS<sup>14</sup>:

#### ISMS-Reifegrad

- Reifegrad 1 Ein ISMS ist zwar geplant, aber bisher nicht etabliert.  
 Reifegrad 2 Ein ISMS ist weitestgehend etabliert.  
 Reifegrad 3 Ein ISMS ist etabliert und dokumentiert.  
 Reifegrad 4 Zusätzlich zum Reifegrad 3 wurde das ISMS regelmäßig auf Effektivität überprüft.  
 Reifegrad 5 Zusätzlich zum Reifegrad 4 wurde das ISMS regelmäßig verbessert.

#### BCMS-Reifegrad

- Reifegrad 1 Ein BCMS ist zwar geplant, aber bisher nicht etabliert.  
 Reifegrad 2 Ein BCMS ist weitestgehend etabliert.  
 Reifegrad 3 Ein BCMS ist etabliert und dokumentiert.  
 Reifegrad 4 Zusätzlich zum Reifegrad 3 wurde das BCMS regelmäßig überprüft und beübt.  
 Reifegrad 5 Zusätzlich zum Reifegrad 4 wurde das BCMS regelmäßig verbessert.

Die Reifegrade sind in den verschiedenen Sektoren Kritischer Infrastrukturen unterschiedlich ausgeprägt, was sich auch an den in den Nachweisen enthaltenen Mängeln der Managementsysteme ablesen lässt. Die erheblichen Unterschiede unter anderem in der Größe der Anlagen, der Abhängigkeit von IT und den Anforderungen verschiedener Aufsichtsregime führen jedoch dazu, dass eine Vergleichbarkeit über Sektorgrenzen hinaus regelmäßig nicht gegeben ist.

Sektor	ISMS-Reifegrad laut jeweils letztem vorliegendem Nachweis					BCMS-Reifegrad laut jeweils letztem vorliegendem Nachweis				
	Reifegrad					Reifegrad				
	1	2	3	4	5	1	2	3	4	5
Wasser	0	6	15	27	24	1	13	27	17	14
Energie	2	7	27	23	25	2	20	34	15	13
Transport und Verkehr	6	13	27	7	7	9	18	16	11	6
Finanz- und Versicherungswesen	1	5	33	19	29	1	24	19	23	20
IT und TK	0	5	6	9	11	3	6	7	7	8
Ernährung	0	8	20	5	9	4	8	20	6	4
Gesundheit	14	88	59	26	12	34	79	49	24	13
Insgesamt	23	132	187	116	117	54	168	172	103	78

Tabelle 4: ISMS-Reifegrade und BCMS-Reifegrade nach Sektoren  
 Quelle: BSI

### BSI beobachtet fortwährend die Sicherheitslage der Kritischen Infrastrukturen in Deutschland

Die staatlichen und privatwirtschaftlichen Betreiber Kritischer Infrastrukturen tragen im Hinblick auf die Versorgung der Bevölkerung mit zum Teil lebensnotwendigen Dienstleistungen ein hohes Maß an Verantwortung für einen sicheren und störungsfreien Betrieb. Durch den russischen Angriffskrieg gegen die Ukraine steht die Sicherheit der Kritischen Infrastrukturen in Deutschland weiterhin im Fokus.

Auch im dritten Nachweiszyklus erreichen das BSI noch Nachweise mit Reifegraden 1 und 2. Durch die Überwachung der betreiberseitigen Mängelbeseitigung im Rahmen der Nachweisführung wirkt das BSI darauf hin, dass sich diese Situation kurzfristig verbessert, hin zu etablierten Managementsystemen. Auffällig ist darüber hinaus, dass trotz der Krisen, insbesondere der COVID-19-Pandemie und des Kriegs in der Ukraine, die BCMS-Reifegrade noch hinter den ISMS-Reifegraden zurückbleiben. Hier sieht das BSI dringenden Handlungsbedarf.

## 8.2 – Besondere Situation von KMU in Deutschland

2,6 Millionen kleine (weniger als 50 Mitarbeitende) und mittlere Unternehmen (50 bis 249 Mitarbeitende) 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- (weniger als zehn Mitarbeitende) und die kleinen Unternehmen verfügen oftmals nicht über das erforderliche Personal für den Betrieb und die Absicherung der Informationstechnik des Unternehmens. So ist ein kleiner Handwerksbetrieb, eine mittlere Steuerberatungs- oder Rechtsanwaltskanzlei, ein metallverarbeitender Betrieb oder ein Pflegedienst oft nicht in der Lage, dediziertes IT-Personal einzustellen. Im Rahmen der Entscheidung zwischen selber machen oder einkaufen („make or buy“) wird dabei häufig nach dem Ansatz gehandelt: „Das bekommen wir schon irgendwie selbst hin.“ Dem steht eine wachsende Bedrohungslage gegenüber.

Viele Unternehmen besitzen auch im Jahr 2023 weder eine ausreichende Kenntnis über die allgemeine Cyberbedrohungslage noch über das eigene Risikoprofil. Sie kommen daher überhaupt nicht auf die Idee, dass sie mehr in ihre Sicherheit investieren müssen. Selbst elementare und oftmals kostenfrei umsetzbare Präventionsmaßnahmen werden daher häufig nicht ergriffen. So installieren nur 62 Prozent der Kleinstunternehmen regelmäßig Sicherheitsupdates. Noch weniger (46 %) überlassen ihre IT-Sicherheit einem externen Dienstleister. Und einen Notfallplan besitzen gar nur 18 Prozent der Kleinstunternehmen<sup>15</sup>. Etwas mehr als die Hälfte der kleinen und der mittleren Unternehmen (51 %) geben als dominierende „IT-Sicherheitsbremse“ den Aufwand und die Kosten für den laufenden technischen Betrieb, Anpassungen und Aktualisierungen an. Nur für 28 Prozent ist der initiale Aufwand ein Hindernis. Dies deckt sich mit den Rückmeldungen von IT-Dienstleistern an das BSI<sup>16</sup>.

Diejenigen KMU hingegen, die ein Problembewusstsein entwickelt haben und Personal einstellen möchten, erleben häufig, dass sie in einem Angebotsmarkt als potenzieller Arbeitgeber nicht gegen die Gehälter bei

### Unternehmen in Deutschland nach Größe Angabe in %

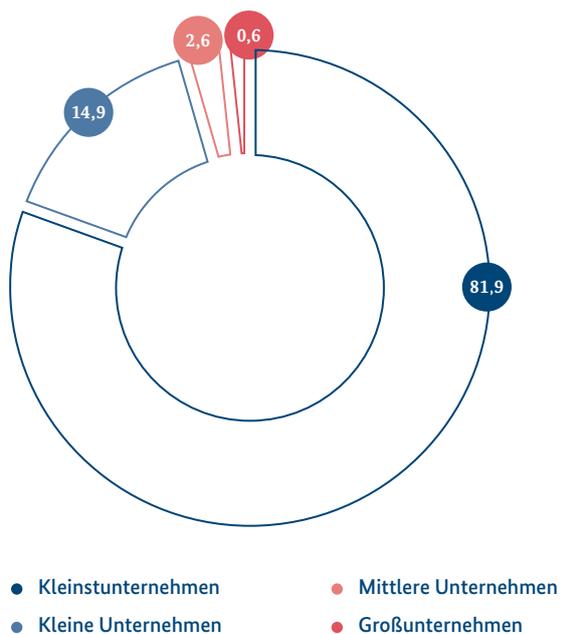


Abbildung 18: Unternehmen in Deutschland nach Größe  
Quelle: Statistisches Bundesamt  
Stand: Juli 2021

Großunternehmen oder IT-Dienstleistern bestehen können. Und diejenigen, die den Bereich IT/IT-Sicherheit an einen Dienstleister auslagern möchten, müssen häufig feststellen, dass es in ihrer Region entweder zu wenig qualifizierte Dienstleister gibt oder nur solche, die nicht zu ihrer eigenen Unternehmensgröße passen.

Dies alles führt dazu, dass KMU häufig zum Opfer Cyberkrimineller werden – und dann nicht wissen, was sie tun sollen. Eine im Auftrag des Bundesministeriums für Wirtschaft und Energie (jetzt Bundesministerium für Wirtschaft und Klimaschutz) im Jahr 2021 veröffentlichte Studie kam zu dem Ergebnis: „Im Ereignisfall wissen KMU oftmals nicht, an wen sie sich wenden können, um fachlich versierte Hilfe zu erhalten. Im Gegensatz zu Einbrüchen in der analogen Welt ist der digitale Schaden für viele KMU nicht immer und nicht unmittelbar ersichtlich. Die Hemmschwelle, Vorfälle und Angriffe an die Polizei, die Landeskriminalämter oder andere behördliche Stellen zu melden, ist hoch.“<sup>17</sup>

Dementsprechend ist der Bereich Cyberkriminalität gegen KMU von einem großen Dunkelfeld geprägt, was es schwer macht, verlässliche Zahlen zu gewinnen. Weiter kommt die oben genannte Studie zu folgender Empfehlung: „Der Aufbau einer bundesweiten Notfall-Hotline für IT-Vorfälle mit zentraler Erreichbarkeit zur Vermittlung an regionale Ansprechstellen würde Abhilfe schaffen.“



### Notfall-Hotline

*Aufgrund der Notwendigkeit einer solchen Hotline betreibt das BSI ein Service-Center. Dieses ist unter der Telefonnummer 0800 274 1000 kostenfrei zu erreichen. Von dort wird über das Cyber-Sicherheitsnetzwerk (CSN) bei Bedarf auch an regionale Ansprechstellen weitervermittelt, die vor Ort bei den Betroffenen helfen können.*

**Viele hilfreiche Tipps für KMU, inklusive eines Verzeichnisses von Dienstleistern, die im Notfall helfen können, und einer Möglichkeit, eine eigene Betroffenheit durch einen Cyberangriff an das BSI zu melden, finden sich hier:<sup>k</sup>**



Im Ernstfall eine Notfall-Hotline kontaktieren zu können ist wichtig, wichtiger ist aber, durch präventive Maßnahmen zu verhindern, zum Opfer zu werden. Oft wissen KMU jedoch nicht, wie sie mehr für ihre IT-Sicherheit tun können. Bereits existierende Standardwerke zum Aufbau eines Managementsystems für Informationssicherheit, 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.

### Durchführung des CyberRisikoChecks

Ein Angebot an KMU ist der vom BSI gemeinsam mit Partnern erarbeitete CyberRisikoCheck. Dabei 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 von einem Konsortium unter Leitung des BSI und des Bundesverbandes mittelständische Wirtschaft (BVMW) erstellten Richtlinie 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 erhalten 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 ein Unternehmen umsetzen beziehungsweise bei einem IT-Dienstleister beauftragen sollte.

Durch die anonymisierten Erhebungsdaten der CyberRisikoChecks kann das Nationale IT-Lagezentrum zukünftig erstmals auf valide Daten zur Cybersicherheit von KMU zurückgreifen und in die BSI-Berichte zur Cybersicherheitslage mit aufnehmen. Der CyberRisikoCheck trägt damit zur Weiterentwicklung präventiver Angebote von Bund, Ländern und Kommunen bei.

**Weitere Informationen zum CyberRisikoCheck sowie eine Liste registrierter IT-Dienstleister, die den Check anbieten, finden sich hier:<sup>l</sup>**



Darüber hinaus können Unternehmen Mitglied der von BSI und Bitkom e. V. gegründeten Public-Private-Partnership Allianz für Cybersicherheit werden, um von den zahlreichen Informationsangeboten der Mitglieder zu profitieren.

Einen guten Überblick über die wichtigsten IT-Sicherheitsmaßnahmen vermittelt die BSI-Broschüre „Cyber-Sicherheit für KMU – Die TOP 14 Fragen“.



## 9. – Erkenntnisse zur Gefährdungslage in Staat und Verwaltung

Staat und Verwaltung waren im Berichtszeitraum verstärkt Cyberangriffen ausgesetzt. Insbesondere hat sich in Deutschland das Phänomen des politisch motivierten Hacking im Kontext des russischen Angriffskriegs gegen die Ukraine verstetigt. Von wenigen Ausnahmen abgesehen (vgl. Die Lage der IT-Sicherheit in Deutschland 2022, Seite 49ff) nutzten die prorussischen Hacking-Gruppen *DDoS-Angriffe* (vgl. Vorfall *DDoS-Hacking*, Seite 30). Da mit dieser Art Cyberangriff Internetdienste nur vorübergehend abgeschaltet werden können und keine tiefere Infiltration von IT-Systemen und Netzwerken stattfindet, können Angreifer damit nur begrenzten Schaden verursachen. Es ist daher davon auszugehen, dass es sich bei *DDoS-Hacking* im Wesentlichen um ein Propaganda-Phänomen handelt, das Verunsicherung in der deutschen Gesellschaft verbreiten soll.

Demgegenüber hinterlassen Cyberangriffe mit *Ransomware* oder *Wipern* nachhaltigen Schaden. Die Wiederherstellung betroffener Systeme nimmt viel Zeit in Anspruch und die betroffenen Behörden sind oft monatelang nur eingeschränkt arbeitsfähig.

### 9.1 – Bundesverwaltung

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

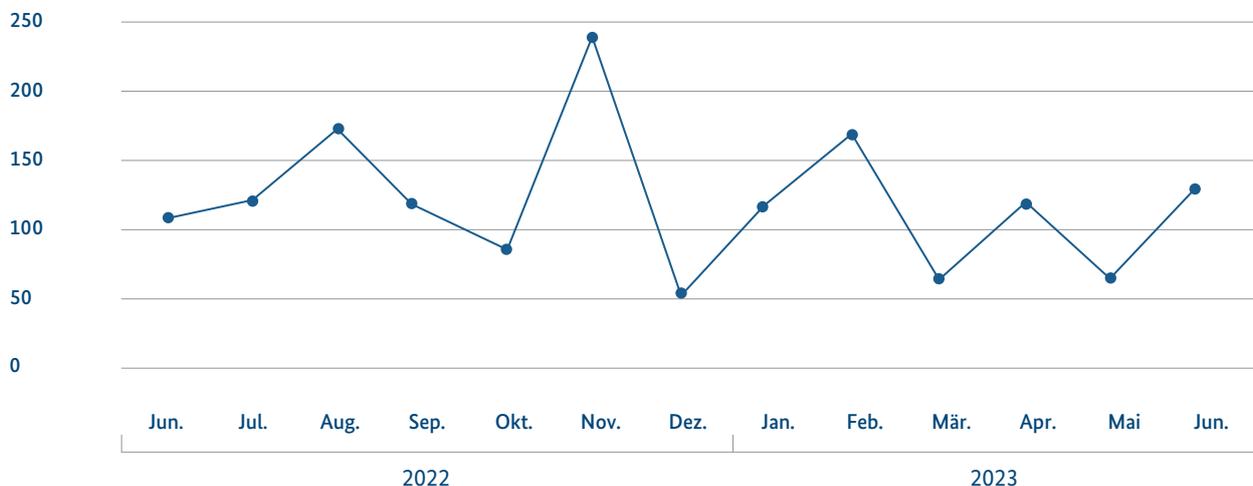
Webfilter stellen eine präventive Komponente dar, die den Zugriff auf *maliziöse* Webseiten bzw. Webserver blockieren. So wird zum Beispiel der Zugriff auf Schadprogramme verhindert, die sich hinter Download-Links verstecken, welche im Rahmen von Social-Engineering-Angriffen über E-Mail, Social Media oder Webseiten verbreitet werden. Auch die Kommunikation von Schadsoftware mit den entsprechenden Webservern, zum Beispiel zum Nachladen von weiteren Komponenten oder Befehlen, wird unterbunden. Im aktuellen Berichtszeitraum wurden täglich durchschnittlich gut 370 *maliziöse* Webseiten neu gesperrt.

Antivirus-Schutzmaßnahmen verhindern die Zustellung von direkt in E-Mail-Anhängen versendeten Schadprogrammen. Dies betraf im Berichtszeitraum durchschnittlich täglich rund 775 E-Mails. Rund 82 E-Mails pro

### Spam-Mail-Index für die Bundesverwaltung\* 2018=100

Abbildung 19: Spam-Mail-Index für die Bundesverwaltung  
Quelle: Erhebung über den E-Mail-Verkehr mit der Bundesverwaltung (BSI)

\*Ohne Spam-Mails an Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen



Tag wurden ausschließlich auf Basis eigens durch das BSI erstellter Antivirus-Signaturen als schädlich identifiziert.

Insbesondere um gezielte Angriffe auf die Bundesverwaltung erkennen zu können, betreibt das BSI zusätzlich zu den bereits beschriebenen Maßnahmen ein System zur Detektion von Schadprogrammen im Datenverkehr der Regierungsnetze. Mit einer Kombination von automatisierten Testverfahren und manueller Analyse konnten die Analytinnen und Analysten des BSI durchschnittlich weitere gut 78 Angriffe pro Tag identifizieren, die weder durch eine kommerzielle noch durch eine der oben genannten automatisierten Lösungen erkannt wurden.

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 58 Prozent. Aufkommen und Entwicklung der *Spam*-E-Mails in den Netzen des Bundes werden durch den *Spam*-Mail-Index gemessen. Dieser erreichte im Berichtszeitraum durchschnittlich 124 Punkte. Das war ein Plus von rund zwölf Prozent im Vergleich zum vergangenen Berichtszeitraum (111 Punkte).

Dabei waren erhebliche Schwankungen zu verzeichnen. Während das *Spam*-Aufkommen im Sommer 2022 auf durchschnittlichem Niveau lag, stiegen die Index-Werte im November 2022 erheblich an. Die *Spam*-Filter der Bundesverwaltung wehren solche *Spam*-Wellen zuverlässig ab, sodass sie die adressierten Nutzerinnen und Nutzer nicht erreichen.

## 9.2 – Landes- und Kommunalverwaltungen

Landes- und Kommunalverwaltungen wurden im Berichtszeitraum verstärkt Opfer cyberkrimineller *Ransomware*-Angriffe.

Im aktuellen Berichtszeitraum wurden monatlich durchschnittlich zwei Kommunalverwaltungen oder kommunale Betriebe als Opfer von *Ransomware*-Angriffen bekannt (vgl. Vorfall *Ransomware-Angriffe auf Kommunalverwaltungen und kommunale Versorgungsbetriebe*, Seite 69). Damit waren sie überproportional häufig von *Ransomware*-Angriffen betroffen (vgl. auch Abb. 16, Seite 56).

Wie inzwischen üblich wurden dabei nicht nur Server verschlüsselt, sondern auch Daten von Bürgerinnen und Bürgern ausgeleitet und teilweise auch auf Leak-Seiten veröffentlicht. Betroffen waren unter anderem ganze Verzeichnisse, die die Akten von Einzelpersonen enthielten. Die betroffenen Verwaltungen waren in der Regel mehrere Tage bis hin zu mehreren Wochen nicht in der Lage, ihre bürger- und wirtschaftsnahen Verwaltungsdienstleistungen zu erbringen, und teils noch Monate später beeinträchtigt.

Während Bundesbehörden separat gesicherte Regierungsnetze mit zentralen Abwehrmaßnahmen zur Verfügung stehen, gestalten die Behörden der Kommunen ihre IT-Sicherheitsmaßnahmen unterschiedlich. Derzeit bestehen keine bundesweit einheitlichen Vorgaben bezüglich IT-Sicherheit oder Meldepflichten zu IT-Sicherheitsvorfällen auf Kommunalebene.

Auch Bildungs- und Forschungseinrichtungen gerieten im aktuellen Berichtszeitraum zunehmend ins Visier von *Ransomware*-Angreifern (vgl. Vorfall *Ransomware-Angriffe auf Bildungs- und Forschungseinrichtungen*, Seite 69).

---

## Ransomware-Angriffe auf Kommunalverwaltungen und kommunale Versorgungsbetriebe

---

Im Berichtszeitraum wurden insgesamt 27 kommunale Verwaltungen und Betriebe als Opfer von Ransomware-Angriffen bekannt. Betroffen waren Kommunen jeder Art und Größe: von einer ländlichen Gemeinde mit 2.800 Einwohnerinnen und Einwohnern bis hin zu einer Großstadt mit mehr als 1,8 Millionen Einwohnerinnen und Einwohnern. Insgesamt hatten die betroffenen Kommunen knapp sechs Millionen Einwohnerinnen und Einwohner. Häufig waren die Stadt- oder Kreisverwaltungen direkt betroffen; jedoch wurden auch Nahverkehrsbetriebe, städtische Energieversorger oder Wohnungsbaugesellschaften, Stadtreinigungsbetriebe und ein Schulamt mit Zuständigkeit für 75 Schulen angegriffen. Selbst der Friedhofsbetrieb einer deutschen Großstadt blieb nicht verschont. Im Juni 2022 mussten nach einem besonders weitreichenden Ransomware-Angriff alle Rathäuser eines ganzen Landkreises sowie mehrere kommunale Betriebe einer angrenzenden kreisfreien Großstadt, darunter der Betrieb für den Nahverkehr, vom Internet getrennt werden.

Auch wenn sich die Angreifergruppierungen, die ausgenutzten Schwachstellen und die eingesetzten RaaS im Detail unterschieden, waren die Abläufe doch meist gleich: Nach

der Erstinfektion folgte das Auskundschaften der befallenen Systeme und die Verschlüsselung von Daten. Anschließend fanden sich die Opfer mit einer Lösegeldforderung konfrontiert. Die Opfer mussten ihre Systeme vollständig herunterfahren und vom Internet trennen, um weiteren Schaden und fortschreitende Verschlüsselung in ihren Netzwerken zu verhindern. Die Bereinigung der Systeme und die vollständige Wiederherstellung der Arbeitsfähigkeit nahmen oft Monate in Anspruch.

Das BSI empfiehlt, neben den verfügbaren Maßnahmen zur Abwehr von Ransomware-Angriffen das IT-Grundschutzprofil „Basis-Absicherung Kommunalverwaltung“ umzusetzen und dabei die Unterstützungsangebote des BSI zum leichteren Einstieg in die Informationssicherheit zu nutzen, wie zum Beispiel die neu erarbeiteten Checklisten zum „Weg in die Basis-Absicherung – WiBA“. Mit Hilfe der Checklisten ist eine erste Bestandsaufnahme der Informationssicherheit und die nahtlose Umsetzung des oben genannten Profils möglich. Langfristig sollte das Niveau der zertifizierungsfähigen Standard-Absicherung angestrebt werden.

---

## Ransomware-Angriffe auf Bildungs- und Forschungseinrichtungen

---

Dass Universitäten für Cyberangreifer attraktive Opfer darstellen, ist bereits seit einigen Jahren bekannt (vgl. zum Beispiel den Fall eines Universitätsklinikums, Die Lage der IT-Sicherheit in Deutschland 2022, Seite 15). Auch im aktuellen Berichtszeitraum wurden wieder fünf Universitäten als Opfer von Ransomware-Angriffen bekannt. Insbesondere nahmen kriminelle Cyberangreifer aber Fachhochschulen

ins Visier. Unter den insgesamt 23 bekannt gewordenen Ransomware-Opfern aus dem Bildungs- und Forschungsbereich befanden sich alleine 13 Universitäten und Fachhochschulen. Weiterhin wurden auch mehrere Institutionen namhafter Forschungsverbände sowie zehn allgemeinbildende Schulen zu Opfern.

---

---

# Trends

---



## Teil C: Herausgehobene Trends in der IT-Sicherheit

### 10. – Künstliche Intelligenz

Künstliche Intelligenz (KI, engl. Artificial Intelligence, AI) ist derzeit in aller Munde. Nicht zuletzt durch große KI-Sprachmodelle wie zum Beispiel ChatGPT hat das Thema Einzug in den Alltag der Menschen gehalten. Und die Entwicklung ist rasant. Egal, ob ein Text geschrieben oder ein Bild kreiert werden soll, Künstliche Intelligenz ist inzwischen so weit, dass das Ergebnis kaum noch von dem eines Menschen zu unterscheiden ist – und das mit großer Zeitersparnis.

Auch in anderen Bereichen spielt KI eine immer größere Rolle, wie zum Beispiel durch KI-gestützte Empfehlungen bei der Kreditvergabe oder bei der Entscheidung für medizinische Behandlungsmethoden. Weitere Themen sind die Verwendung von KI in der Kryptografie und der Kryptoanalyse oder in den Bereichen autonomes Fahren und mediale Identitäten.

Künstliche Intelligenz ist eine der Schlüsseltechnologien der Digitalisierung. Das BSI hat den Anspruch, die Digitalisierung als Thought Leader in all ihren Facetten sicher zu gestalten und eine zentrale Stelle zu Fragen der Sicherheit und der Prüfung von KI-Systemen im Bund zu werden, weshalb IT-Sicherheit für KI und durch KI Kernthemen sind, welche hierfür aktiv mitgestaltet werden. Zusammen mit Partnern aus Forschung und Entwicklung, Wirtschaft und Verwaltung entwickelt das BSI die technologischen Grundlagen und Kriterien zur Bewertung und Prüfung von KI-Systemen, um sie anschließend in die Praxis zu überführen. Darüber hinaus wirkt das BSI bei der Entwicklung von KI-Normen und KI-Standards aktiv mit und bringt seine langjährige Erfahrung und fachliche Expertise in nationalen und internationalen Standardisierungsprozessen und –gremien ein.

Der Einsatz von KI birgt Risiken und Herausforderungen (siehe Kapitel *Große KI-Sprachmodelle*, Seite 40), aber auch Chancen und Potenziale. Das BSI setzt sich durch die oben aufgeführten Aktivitäten für die Schaffung nachweisbar sicherer, vertrauenswürdiger sowie transparenter KI-Systeme ein. Somit können diese Potenziale,

die sich aus den derzeitigen Entwicklungen und Trends im Bereich der Künstlichen Intelligenz ergeben, für Wirtschaft und Gesellschaft sicher nutzbar gemacht und etabliert werden.

#### 10.1 – Sicherheit großer KI-Sprachmodelle

Große KI-Sprachmodelle (LLMs) stehen gegenwärtig im Fokus des öffentlichen Interesses. Sie eignen sich gut zur Textverarbeitung und -generierung und erzeugen qualitativ hochwertigen Text, der sich nur schwer von menschengeschriebenen Texten unterscheiden lässt.

Abteilungs- und standortübergreifend baut das BSI seit Mitte 2022 Expertise zu Sicherheitsaspekten rund um LLMs aus und bietet diese im Rahmen von Beratungsleistungen und Vorträgen innerhalb des BSI sowie anderen Behörden und der Öffentlichkeit an. Im Mai 2023 hat das BSI eine Publikation veröffentlicht, in der die Chancen und Risiken des Einsatzes von LLMs in Industrie und Behörden sowie für Verbraucherinnen und Verbraucher beleuchtet werden.

##### Die BSI-Publikation zu Großen KI-Sprachmodellen:<sup>m</sup>



Bereits durch die Funktionsweise und das Training von LLMs ergeben sich diverse Schwächen, die Sicherheitsrisiken nach sich ziehen können. Sind die Daten, die genutzt werden, um ein LLM „anzulernen“, nicht ausgeglichen, sondern enthalten eine sogenannte Schiefe (Bias) oder auch veraltete oder diskriminierende Aussagen, können sich diese auch bei der Nutzung des LLM zeigen. Ferner liefert ein LLM auf Eingaben zu ihm bisher unbekanntem Themen zwar ein Ergebnis (die sogenannte Ausgabe), dieses kann allerdings beliebig realitätsfern sein (sog. „Halluzinieren“). Ebenso kann ein durch das LLM erzeugter Programmcode für Schwachstellen anfällig sein (wenn diese beispielsweise in den Trainingsdaten vorhanden waren). Problematisch ist weiterhin, dass sich

die Entstehung der Ausgaben von LLMs wegen der hohen Komplexität dieser Modelle nur schwer erklären lassen.

Neben den bereits genannten Risiken ist auch der Einsatz von LLMs für die Generierung von *Spam*- und *Phishing*-E-Mails naheliegend. Durch die Fähigkeit, sprachlich korrekten, überzeugenden Text zu erzeugen, stellen ebenso die automatisierte Erstellung von Hate Speech, Desinformationen und gefälschten Rezensionen ein verbreitetes Missbrauchsszenario dar. Weiterhin können Kriminelle mittels LLMs Schadcode generieren und regelmäßig verändern, sodass dessen Erkennung erschwert wird.

Diese und weitere Szenarien machen es erforderlich, dass Hersteller und Anbieter von LLMs oder LLM-basierten Anwendungen entsprechende Vorkehrungen treffen, die die Erzeugung potenziell schädlicher Ausgaben weitestgehend verhindern oder erschweren. Nutzende dieser Anwendungen sollten über mögliche Sicherheitsrisiken bei der Verwendung von LLMs aufgeklärt werden, um verantwortungsvoll mit den Ausgaben eines solchen Modells umgehen zu können.

Die Integration von LLMs in Alltags- oder Office-Anwendungen kann durch die vielfältigen Möglichkeiten der Unterstützung bei Textverarbeitungs- und -produktionsaufgaben einen Schub für die Digitalisierung leisten. Gleichzeitig können aber je nach Anwendungsfall erhebliche Sicherheitsrisiken entstehen, die im Einzelfall gegen den Nutzen aufgewogen werden sollten.

## 10.2 – Digitaler Verbraucherschutz und KI

Entscheidungen eines KI-Systems sind wegen ihres Black-Box-Charakters für Verbraucherinnen und Verbraucher oft überraschend und wenig nachvollziehbar. Vor allem in Anwendungen mit weitreichenden Auswirkungen (z. B. Empfehlungen über Behandlungsmethoden oder Kreditvergabe) stellt die fehlende Transparenz dieser Systeme ein Problem dar. Aus diesem Grund untersucht das BSI, wie Verbraucheranwendungen, die KI einsetzen, evaluiert werden können. Ziel ist es, dass Verbraucherinnen und Verbraucher selbstbestimmt die Anwendung von KI-Systemen identifizieren, um somit ihre *Resilienz* in Bezug auf KI-Systeme zu stärken.

Des Weiteren untersucht das BSI Methoden, um die Robustheit von KI-Systemen zu bestimmen und deren Entscheidungen erklären und transparenter gestalten zu

können. Die Untersuchungsergebnisse sollen verbraucherfreundlich aufbereitet und über diverse Kommunikationskanäle verbreitet werden.

## 10.3 – Einsatz von KI in der Kryptografie

Künstliche Intelligenz hat längst auch Einzug in verschiedene Bereiche der Kryptografie gehalten. Insbesondere in der Seitenkanalanalyse haben sich Methoden des maschinellen Lernens (ML) inzwischen fest etabliert. Die besten Ergebnisse lassen sich erzielen, wenn maschinelles Lernen mit Expertenwissen über mögliche Quellen von Seitenkanalinformationen kombiniert wird, wobei der Einsatz neuronaler Netze besonders erfolgreich ist. Das BSI beschäftigt sich daher sowohl im Kontext verschiedener Projekte als auch im Rahmen eigener Forschung mit dem Thema.

KI-Techniken können auch im Bereich der Kryptoanalyse verwendet werden, beispielsweise bei der Analyse und Bewertung von symmetrischen Kryptoverfahren. Dies ist Thema zweier aufeinander aufbauender BSI-Projekte, deren Ziel unter anderem die Entwicklung KI-gestützter Werkzeuge ist, die zu einer Sicherheitsbewertung von Blockchiffren beitragen können.

## 10.4 – KI-gestützte Analyse der IT-Sicherheitslage

Das BSI testet in einem Projekt KI-Methoden, mit denen sich aktuelle Nachrichten zur IT-Sicherheitslage automatisiert erfassen und analysieren lassen. Ein sogenannter Wissensgraph (Ontologie), bestehend aus Begriffen der IT-Sicherheitsdomäne, dient dabei als Wissensbasis, die diese Analyse unterstützt. Gleichzeitig wird ML dafür eingesetzt, den Wissensgraphen halbautomatisch zu verbessern.

Mit dem Wissensgraphen und trainierten Sprachmodellen werden Entitäten im Text identifiziert, das heißt Textstellen als Nennung einer Entität erkannt – zum Beispiel „Browser“ als Software – oder sogar einem konkreten Objekt zugeordnet, etwa wie die Zeichenkette „BSI“ dem Bundesamt. Diese Entitäten dienen sowohl der semantischen Suche als auch zur Leseunterstützung oder zur gezielten statistischen Auswertung ganzer Objekt-Klassen (z. B. *Malware*). Sprachmodelle ermöglichen auch

Textklassifikation und natürlichsprachliche Fragen mit Textstellen zu beantworten, was wiederum der Transparenz der Ergebnisse zuträglich ist.

## 10.5 – KI für autonomes Fahren und mediale Identitäten

Seit Dezember 2021 führt das BSI Projekte durch, in denen anhand der Betrachtung praktischer Anwendungsfälle erste konkrete Kriterien und Prüfmethode für KI-Verfahren im autonomen Fahren erarbeitet werden. Im ersten Projekt<sup>18</sup> wurden unter anderem 50 technisch relevante Anforderungen an KI-Systeme zusammengestellt sowie eine erweiterbare Testumgebung für KI-Systeme entwickelt. Diese Anforderungen, Methoden und Werkzeuge werden seit Dezember 2022 in einem Folgeprojekt gezielt erprobt und weiterentwickelt. Mittelfristig plant das BSI, auf Basis dieser Vorarbeiten eine technische Richtlinie zu verfassen<sup>19</sup>.

**Weitere Informationen zum automatisierten Fahren:<sup>18</sup>**



Auch im vergangenen Berichtszeitraum wurde eine kontinuierliche Qualitätssteigerung der öffentlich zugänglichen Werkzeuge zur Manipulation von Identitäten in den Medien Audio und Video (*Deepfakes*) beobachtet (siehe auch Kapitel *Skalierungseffekte bekannter Bedrohungen*, S. 44). Die Verfügbarkeit solcher Werkzeuge ist zum einen durch Open-Source-Software und zum anderen durch neue *Cloud*-Dienste gegeben. Teilweise können Identitäten auf Basis von nur wenigen Sekunden Material mit „One-Shot“-Verfahren auf eine Zielidentität hin ausgerichtet werden. Dies kann beispielsweise dazu genutzt werden, um Systeme für Sprechererkennung zu überwinden<sup>20</sup>.

Das BSI konnte zeigen, dass mittlerweile sowohl im Audio- als auch im Videobereich Identitätsfälschungen mit annehmbarer Qualität in Echtzeit möglich sind. Im Projekt „Absicherung medialer Identitäten“ sollen bis 2025 Gegenmaßnahmen erarbeitet und evaluiert werden.

## 10.6 – Weitere Entwicklungen im Bereich KI

Der Themenbereich der KI-Sicherheit steht weltweit weiterhin im Fokus von Standardisierungsgremien und Expertengruppen, in denen das BSI seine Expertise einbringt. In einer wachsenden Anzahl unterschiedlicher Anwendungsdomänen arbeitet das BSI an der Entwicklung von Prüfkriterien und Prüfmethode für KI-Systeme, beispielsweise in den Bereichen Automotive, *Cloud*-Dienste, Medizin und Agrarwirtschaft. Damit werden die Kernthemen und Empfehlungen der Deutschen Normungsroadmap KI, an deren Erstellung das BSI aktiv mitwirkte, bearbeitet und umgesetzt.

**Weitere Informationen zu dieser und weiteren Studien finden Sie hier:<sup>9</sup>**



In einem Projekt wurde erfolgreich ein neuartiger Ansatz zur KI-gestützten statischen Code-Analyse implementiert und erprobt. Die Software ist als Open Source veröffentlicht, wodurch eine bessere Vernetzung mit der Forschungscommunity sowie weitere Impulse für die Forschung in diese Richtung erwartet werden.

Quantencomputer bieten Potenziale, die auch und speziell im Bereich des maschinellen Lernens von zunehmend hohem Interesse sind. Aktuell werden vor allem Ansätze diskutiert, die klassische und Quanten-Algorithmen in hybriden Methoden kombinieren<sup>21</sup>. In einer Grundlagenstudie<sup>22</sup> hat das BSI den aktuellen Forschungsstand zum Quantum Machine Learning (QML) erfasst und Chancen und Risiken hinsichtlich der IT-Sicherheit beleuchtet. In einem Folgeprojekt werden die Sicherheitseigenschaften von und die Bedrohungsszenarien für QML-Methoden und -Systeme anhand praktischer Experimente untersucht.

Im Bereich der Explainable AI untersuchte das BSI die fehlende Reproduzierbarkeit des Trainings von Machine-Learning-Modellen (ML-Modellen) und dessen Auswirkung auf Vorhersage und Erklärbarkeit der Ausgaben der Modelle. Weiterhin wurde der Einfluss der Dimensionalität von Daten auf die Qualität und Zuverlässigkeit wahrscheinlichkeitsbasierter ML-Modelle beleuchtet.

## 11. – Quantentechnologien

Die fortschreitende Entwicklung von Quantencomputern bedroht die Sicherheit vieler klassischer und weitverbreiteter Public-Key-Verfahren wie RSA und ECC. Deshalb ist die Migration zu kryptografischen Verfahren von hoher Dringlichkeit, die voraussichtlich auch mit Quantencomputern nicht gebrochen werden können (Post-Quanten-Kryptografie). Das BSI handelt dazu für den Hochsicherheitsbereich unter der Arbeitshypothese, dass kryptografisch relevante Quantencomputer Anfang der 2030er-Jahre zur Verfügung stehen werden. Dabei ist zu betonen, dass diese Aussage nicht als Prognose zur Verfügbarkeit von Quantencomputern zu verstehen ist, sondern einen Richtwert für die Risikobewertung darstellt.

Eine detaillierte Analyse „Entwicklungsstand Quantencomputer“ wurde im Auftrag des BSI bereits 2018 erstellt und seitdem zweimal aktualisiert. In einem weiteren BSI-Projekt erfolgten insgesamt drei weitere Updates.

**Weitere Informationen zur Studie:**<sup>p</sup>



In der Technischen Richtlinie TR-02102-1 des BSI werden mit FrodoKEM und Classic McEliece bereits seit März 2020 erste Post-Quanten-Verfahren zum Schlüsseltransport und die hashbasierten Signaturverfahren LMS und XMSS empfohlen. Einen Überblick zum gesamten Themenkomplex liefert der Leitfaden „Kryptografie quantensicher gestalten“ des BSI.

**Den BSI-Leitfaden „Kryptografie quantensicher gestalten“ finden Sie hier:**<sup>q</sup>



**Die technische Richtlinie TR-02102 finden Sie hier:**<sup>r</sup>



Auch andere europäische Cybersicherheitsbehörden wie die französische ANSSI und das niederländische NCSC haben erste Empfehlungen zur Migration auf quantensichere Verfahren veröffentlicht. Besonders umfassende und konkrete Maßnahmen hat die US-amerikanische Regierung eingeleitet. In zwei Memoranden vom Mai und

November 2022<sup>23</sup> wurden die verpflichtende Erstellung von Migrationsplänen, regelmäßige Berichtspflichten und ambitionierte Migrationszeitpläne für Behörden festgelegt. Bis 2035 soll die Gefährdung durch Quantentechnologien durch den flächendeckenden Einsatz von Post-Quanten-Kryptografie weitestgehend minimiert sein. Um dies zu erreichen, hat die NSA im November 2022 die Commercial National Security Algorithm Suite (CNSA) 2.0<sup>24</sup> veröffentlicht. Diese ist für Betreiber von National Security Systems bindend und beschreibt Zeitpläne für verschiedene technische Anwendungen. Beispielsweise ist ab 2027 Post-Quanten-Kryptografie als Standard für Web-Browser, Server und Cloud-Dienste vorgesehen.

Die Auswirkungen von Quantentechnologien auf die Cybersicherheit sind von der Bundesregierung und dem BMI aufgegriffen worden. Die Bundesregierung hat im September 2021 in der „Cybersicherheitsstrategie für Deutschland 2021“<sup>25</sup> die Förderung der „Entwicklung neuer Verschlüsselungslösungen, insbesondere im Bereich der Post-Quanten-Kryptografie“ als Ziel genannt. Dieses Ziel hat das BMI in der im April 2022 veröffentlichten Cybersicherheitsagenda<sup>26</sup> mit der Maßnahme „Ausstattung der Bundesbehörden mit weiterentwickelten IT-Produkten und -Systemen für sichere Kommunikation sowie Investition in Quantencomputing und Post-Quanten-Kryptografie“ hinterlegt.

Die Bundesregierung setzt sich im „Handlungskonzept Quantentechnologien“<sup>27</sup> das Ziel, bis 2026 eine Strategie der Migration zur Post-Quanten-Kryptografie zu erstellen.

### 11.1 – Post-Quanten-Kryptografie

Die Standardisierung von Post-Quanten-Verfahren geschah bisher hauptsächlich in einem vom US-amerikanischen National Institute of Standards and Technology (NIST) im Jahre 2016 initiierten Prozess mit internationaler Beteiligung. Im Juli 2022 hat NIST das Schlüsseltransportverfahren CRYSTALS-Kyber und die Signaturverfahren CRYSTALS-Dilithium, Falcon sowie SPHINCS+ zur Standardisierung ausgewählt<sup>28</sup> (vgl. auch Kapitel *Schwachstellen in Hardwareprodukten*, Seite 39).

Neben der Standardisierung der Post-Quanten-Verfahren laufen zurzeit viele konkrete Aktivitäten zur Migration auf Post-Quanten-Kryptografie. So sind erste Produkte für den Hochsicherheitsbereich, die hybride Schlüsseleinigung benutzen, bereits zugelassen und im Einsatz. Bei

## NIST-Auswahlverfahren

*Bis auf das hashbasierte SPHINCS+ beruht die Sicherheit dieser Verfahren auf Gitterproblemen in strukturierten Gittern. Standardisierungsentwürfe für Kyber, Dilithium und SPHINCS+ wurden im August 2023 veröffentlicht. Am Ende der zurzeit laufenden vierten Runde wird voraussichtlich ein weiteres Schlüsseltransportverfahren zur Standardisierung ausgewählt. Außerdem hat NIST einen neuen Aufruf zur Einreichung weiterer Signaturverfahren veröffentlicht, zu dem bis Anfang Juni 2023 Einreichungen akzeptiert wurden. Das vom BSI empfohlene FrodoKEM wird im NIST-Prozess nicht weiter betrachtet, weil es weniger effizient als Kyber ist. Classic McEliece, die zweite BSI-Empfehlung zum Schlüsseltransport, könnte eventuell am Ende der vierten Runde noch standardisiert werden. Das BSI hält an der Empfehlung von FrodoKEM und Classic McEliece auch nach der Entscheidung durch NIST fest. Diese Verfahren liefern eine eher konservative Alternative zur bisherigen NIST-Auswahl und werden derzeit bei ISO standardisiert.*

*In den letzten Jahren war die Forschungsaktivität im Bereich Post-Quanten-Kryptografie sehr hoch, was zum Teil an der hohen Öffentlichkeitswirksamkeit des NIST-Auswahlprozesses liegt. Tatsächlich haben sich einige der eingereichten Verfahren als unsicher erwiesen. So hat sich zum Beispiel das Sicherheitsniveau des multivariaten Signaturverfahrens Rainbow (ein Finalist in der 3. Runde des NIST-Prozesses) im Jahr 2022 durch neue Angriffe als unzureichend herausgestellt. Das isogeniebasierte Schlüsseltransportverfahren SIKE wurde, kurz nachdem es von der NIST in die 4. Runde aufgenommen wurde, sogar vollständig gebrochen. Die Sicherheit der vom BSI empfohlenen sowie der von NIST bislang zur Standardisierung ausgewählten Verfahren beruht jedoch auf ganz anderen mathematischen Problemen. Daher sind diese Verfahren von den neuen Angriffen nicht betroffen und gelten weiterhin als sicher. Auch sie müssen jedoch weiter aktiv untersucht werden und das BSI empfiehlt grundsätzlich den hybriden Einsatz von Post-Quanten-Kryptografie in Kombination mit klassischer Public-Key-Kryptografie.*

der Internet Engineering Task Force (IETF) wird in zahlreichen Arbeitsgruppen daran gearbeitet, Post-Quanten-Kryptografie in die Standards der IETF zu integrieren. In einem BSI-Projekt zur Weiterentwicklung der FOSS-Kryptobibliothek Botan werden aktuell Post-Quanten-Verfahren und eine hybride Schlüsseleinigung in TLS 1.3 implementiert. Ein weiteres BSI-Projekt hat sich zum Ziel gesetzt, quantensichere E-Mail-Verschlüsselung und -Signaturen im E-Mail-Client Thunderbird zu realisieren. Im Rahmen dieses Projektes ist auch ein Standardisierungsentwurf für Post-Quanten-Kryptografie in OpenPGP entstanden.

Das BSI ist außerdem Betreiber der Wurzelzertifizierungsstelle für die Public-Key-Infrastruktur der öffentlichen Verwaltung (V-PKI). Die aktuell verwendeten kryptografischen Algorithmen in dieser V-PKI sind nicht quantensicher. Um der drohenden Gefährdung durch kryptografisch relevante Quantencomputer rechtzeitig begegnen zu können, plant das BSI aktuell die Migration zu einer quantensicheren V-PKI.

Auch außerhalb des Hochsicherheitsbereichs und der öffentlichen Verwaltung ist die Migration auf Post-Quanten-Kryptografie wichtig. Deshalb muss die Awareness für die Sicherheitsbedrohung durch Quantencomputing und mögliche Schutzmaßnahmen erhöht werden. Eine im April 2023 veröffentlichte Umfrage<sup>29</sup> zeigt, dass Unternehmen nicht genügend Maßnahmen ergreifen, um der Bedrohung der Informationssicherheit durch Quantencomputer zu begegnen. Zwar haben 97 Prozent der teilnehmenden Unternehmen die Relevanz von Quantencomputing für die Sicherheit heutiger Kryptografie als „hoch“ oder „eher hoch“ eingeschätzt. Diese Bedrohung wird aber nur von 25 Prozent der Unternehmen im Risikomanagement berücksichtigt.

### 11.2 – Quantum Key Distribution

Quantum Key Distribution (QKD) soll quantensichere Schlüsseleinigung auf Basis quantenmechanischer Prin-

zipien ermöglichen und kann somit für spezielle Anwendungsfälle eine Ergänzung zu Post-Quanten-Kryptografie sein. Die Entwicklung von QKD wird derzeit auf nationaler und europäischer Ebene intensiv gefördert, beispielsweise durch das Projekt EuroQCI der Europäischen Kommission. Im Rahmen von EuroQCI soll eine Quantenkommunikationsinfrastruktur in Europa aufgebaut werden, die sowohl eine terrestrische als auch eine satellitengestützte Komponente umfasst. Seit März 2023 ist EuroQCI Teil von IRIS2, dem Projekt zur Entwicklung eines europäischen satellitenbasierten sicheren Kommunikationssystems. Das BSI ist in der Security Working Group von EuroQCI vertreten.

Aus Sicht des BSI sind noch wesentliche Grundlagenarbeiten zu Sicherheitsfragen erforderlich, bis QKD einsatzreif ist. Um einen Beitrag zur Entwicklung sicherer QKD-Systeme zu leisten, hat das BSI gemeinsam mit dem European Telecommunications Standards Institute (ETSI) ein erstes Protection Profile (PP)<sup>30</sup> nach Common Criteria für Prepare-and-Measure-QKD-Systeme entwickelt. Dieses Profil wurde in einer ersten Version im April 2023 von ETSI veröffentlicht. Derzeit wird es beim BSI zertifiziert und soll danach in einer aktualisierten Version bereitgestellt werden. Um das PP zur Zertifizierung von Produkten zu nutzen, ist jedoch die Erarbeitung weiterer Hintergrunddokumente wie Standards sowie einer Evaluierungsmethodologie erforderlich. Standards zu QKD werden derzeit in mehreren Gremien entwickelt.

Um die Entwicklung einer Evaluierungsmethodologie für QKD zu unterstützen, hat das BSI 2022 eine wissenschaftliche Studie zu *Seitenkanalangriffen* auf QKD-Systeme in Auftrag gegeben. Die Ergebnisse werden voraussichtlich Ende 2023 veröffentlicht.

Das Bundesministerium für Bildung und Forschung (BMBF) fördert verschiedene Projekte zur Quantenkommunikation, darunter das Projekt QuNET. Im Rahmen des Innovationshubs Quantenkommunikation wird zudem ein Schirmprojekt gefördert, das die deutschlandweit vorhandenen Kompetenzen zur Quantenkommunikation bündeln und fokussieren soll. Dieses Schirmprojekt Quantenkommunikation Deutschland (SQuaD) wird von der Physikalisch-Technischen Bundesanstalt im engen Schulterschluss mit dem BSI koordiniert.

## 12. – Sicherheit moderner Telekommunikationsinfrastrukturen (5G/6G)

Ein für das BSI besonders wichtiges Zukunftsthema ist eine sicher gestaltete 5G/6G-Infrastruktur für Deutschland. Mit 5G- und 6G-Technologien lassen sich Anwendungsszenarien verwirklichen, die vorher nicht über Mobilfunk zu realisieren waren. So steigen beispielsweise die Geschwindigkeiten der Datenübertragung bei gleichzeitig sinkender Verzögerung.

Die höheren Übertragungsgeschwindigkeiten verbessern dabei die Effizienz. Zudem ermöglichen die geringen Latenzzeiten Echtzeitkommunikation von Endgeräten und bieten so völlig neue Möglichkeiten. Damit schaffen die modernen Mobilfunktechnologien eine wichtige Voraussetzung für die weitere Digitalisierung und entwickeln sich immer stärker zu einer kritischen Infrastruktur.

Die Erfüllung des Ziels einer sicher gestalteten 5G/6G-Infrastruktur lässt sich in drei Bereiche unterteilen:

- Entwicklung von Vorgaben zur Aufrechterhaltung des sicheren Betriebes von 5G-Netzen
- Überprüfung der Vorgaben durch Instrumente der Zertifizierung und Auditierung
- Mitarbeit in Standardisierungsorganisationen zur Entwicklung und Fortschreibung von Schemata sowie für die Implementierung von Anforderungen an die IT-Sicherheit von 5G/6G-Netzen

### 12.1 – Vorgaben und Zertifizierung für 5G-Netze

Öffentliche Mobilfunknetze der 5. Generation unterliegen gesetzlichen Regularien, an deren Erarbeitung und Fortschreibung das BSI beteiligt ist. Die folgenden Unterkapitel geben einen Überblick und beleuchten verschiedene zur Anwendung kommende Zertifizierungsschemata. Für den Bereich der privaten 5G-Netze, auch 5G-Campusnetze genannt, existieren keine gesetzlichen Regularien. Stattdessen werden den Betreibern und Anwendern standardisierte Werkzeuge zur Einführung von IT-Sicherheit im Rahmen von IT-Grundschutz-Profilen zur Verfügung gestellt.

### 12.1.1 – Mitgestaltung des IT-Sicherheitskatalogs und Fortschreibung der Technischen Richtlinie TR-03163

Unter Federführung der Bundesnetzagentur gestaltet das BSI gemeinsam mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit den Katalog von Sicherheitsanforderungen gemäß Telekommunikationsgesetz (TKG), der sich aktuell in Überarbeitung befindet.

Der Sicherheitskatalog regelt verpflichtende Maßnahmen, um die im TKG genannten Schutzziele zu erreichen, und richtet sich an alle Telekommunikationsbetreiber und Diensteanbieter. Dabei werden für den 5G-Netzbetrieb erhöhte Anforderungen festgelegt, um der Bedeutung des 5G-Mobilfunknetzes für die Gesellschaft Rechnung zu tragen. Der Sicherheitskatalog benennt den Rahmen und die Fristen zur Zertifizierung von kritischen 5G-Netzwerkkomponenten und verweist für die Details auf die Technische Richtlinie TR-03163 „Sicherheit in TK-Infrastrukturen“ des BSI, die Schemata benennt und regelmäßig fortgeschrieben wird.

Die Technische Richtlinie TR-03163:<sup>5</sup>



### 12.1.2 – Umsetzung Zertifizierungspflicht für kritische Komponenten in öffentlichen 5G-Netzen

Mit der Veröffentlichung der TR-03163 sowie der Produktivsetzung des nationalen Zertifizierungsprogramms für 5G-Mobilfunkausrüstung (*NESAS CCS-GI*) hat das BSI begonnen, die gesetzliche Zertifizierungspflicht gemäß TKG umzusetzen. Derzeit arbeitet das BSI zusammen mit interessierten Partnern daran, die Anforderungen an die Sicherheitszertifizierung verschiedener Netzelemente eines 5G-Netzes zu erstellen.

Das *NESAS CCS-GI* ermöglicht es Herstellern, mittels eines IT-Sicherheitszertifikats nachzuweisen, dass sie die durch das internationale Standardisierungsprojekt 3rd Generation Partnership Project (3GPP) geforderten Sicherheitseigenschaften einhalten. Das Zertifikat basiert

auf dem Network Equipment Security Assurance Scheme (*NESAS*) der GSMA, der globalen Interessenvertretung der Mobilfunkanbieter und Hersteller, und umfasst eine Überprüfung der Produktentwicklungs- und Lebenszyklusprozesse sowie eine Evaluation des danach hergestellten Produkts. Im Berichtszeitraum wurden mit der TÜV Informationstechnik GmbH und der atsec information security GmbH zwei Unternehmen als Prüfstellen für *NESAS CCS-GI* anerkannt. Im Januar 2023 wurde das erste *NESAS-CCS-GI*-Zertifikat für eine 5G-Basisstation ausgestellt.

Ausgehend von den Produkteigenschaften und den Ansätzen zur Evaluierung innerhalb der verschiedenen vom BSI angebotenen Zertifizierungsschemata listet die TR-03163 weitere Zertifizierungsprogramme wie Common Criteria und Beschleunigte Sicherheitszertifizierung für definierte Produktklassen auf. Dies fördert die Verwendung von Produkten, die für ihren geplanten Einsatz bereits im Vorfeld bezüglich ihrer Sicherheitseigenschaften geprüft wurden.

### 12.1.3 – Überprüfung öffentlicher 5G-Netzbetreiber

Durch das *IT-Sicherheitsgesetz 2.0* erhielt das BSI die Aufgabe, Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste mit erhöhtem Gefährdungspotenzial alle zwei Jahre zu überprüfen. Überprüft wird im Bereich 5G, ob die Betreiber die gesetzlichen Vorgaben zur Informationssicherheit aus dem TKG einhalten. Die Anforderungen im TKG umfassen dabei organisatorische, technische und betriebliche Rahmenbedingungen, unter denen die Telekommunikationsnetze betrieben und die dazugehörigen Dienste erbracht werden. Dafür hat das BSI im Berichtszeitraum ein Prüfschema entwickelt und in Abstimmung mit den zuständigen Behörden die gesetzlichen Vorgaben durch eine Prüfgrundlage weiter untersetzt. Die ersten Überprüfungen werden im Laufe des Jahres 2023 stattfinden.

### 12.1.4 – IT-Grundschutz für sichere private 5G-Netze

Mit dem Einsatz von privaten 5G-Netzen ergeben sich neue Anforderungen an Unternehmen, Behörden, Forschungseinrichtungen und weitere Betreiber.

Das BSI widmet sich der Frage, wie sich 5G-Netze sicher betreiben lassen, und nutzt mit dem IT-Grundschutz ein erprobtes und anerkanntes Werkzeug für den Aufbau und Betrieb eines Managementsystems für Informationssicherheit.

Das „IT-Grundschutz-Profil zur Absicherung von 5G-Campusnetzen – Betrieb durch einen externen Dienstleister“ ist eine Anleitung, mit deren Hilfe sich Organisationen mit dem Thema Informations- und IT-Sicherheit in privaten 5G-Netzen vertraut machen können. Die darin enthaltene Risikoanalyse gibt konkrete Handlungsempfehlungen, mit denen sich ein 5G-Campusnetz schützen lässt. Diese Schablone kann individuell an das Unternehmen angepasst werden. Die gesammelten Erfahrungen dienen als Grundlage für zukünftige Sicherheitskonzept-Blaupausen im Bereich der 5G-Campusnetze.

## 12.2 – Sicherheit in der Standardisierung von 5G und 6G

Das BSI ist überzeugt, dass IT-Sicherheitsbelange bereits bei der Ausarbeitung von Standards eingebracht werden müssen, aktuell und dringlich im Bereich von 6G. Zudem ist die hinreichende Implementierung von IT-Sicherheitsvorgaben bereits in der Standardisierung Grundlage einer erfolgreichen Sicherheitszertifizierung. Das BSI beteiligt sich deshalb in verschiedenen internationalen Standardisierungsorganisationen. Nachfolgend werden die wichtigsten Aktivitäten zur Sicherheit in Standards der Mobilfunkkommunikation aufgeführt.

Die GlobalPlatform ist eine internationale Industrie-Standardisierungsorganisation, deren Technologie das technische Management von Applikationen auf Secure Elements, SIM-Karten und *Trusted Execution Environments* ermöglicht.

Die Basis für *NESAS CCS-GI* bildet das *NESAS*-Prüfschema, das von der GSMA herausgegeben wird. Das BSI ist in der zugehörigen Expertengruppe vertreten und arbeitet an der Überführung zu einem Zertifizierungsverfahren mit. Zudem beteiligt sich das BSI daran, die Harmonisierung von *NESAS* mit den Anforderungen an das EU5G-Zertifizierungsschema nach dem EU-Cybersecurity Act sicherzustellen.

Im 3GPP werden, aufbauend auf GSM (2G), die Spezifikationen für die Mobilfunkstandards UMTS (3G), LTE

(4G) und 5G entwickelt. Das BSI beteiligt sich seit 2022 mit eigenen Beiträgen zum Thema Roaming und bei der Gestaltung von Sicherheitstests gemäß *Security Assurance Specifications (SCAS)*. Die *SCAS* definieren wichtige Sicherheitsfunktionen, die auch Grundlage für die Produktzertifizierung nach *NESAS CCS-GI* bilden.

Die Testdurchführung ist bisher sehr unterschiedlich genau ausgeführt. Das BSI definierte daher zu 59 Testfällen sogenannte Refinements. Diese müssen unter *NESAS CCS-GI* von den Prüfstellen beachtet werden und fördern die Vergleichbarkeit und Nachvollziehbarkeit der Ergebnisse.

Bei den Open-RAN-Spezifikationen der O-RAN Alliance, die eine weitere Modularisierung in den Funkzugangsnetzen (RAN) möglich machen sollen, hat das BSI einerseits die Standardisierung über das European Telecommunications Standards Institute (ETSI) kommentiert, andererseits wurden durch eine vom BSI beauftragte Studie Kritikpunkte an früheren O-RAN-Versionen aufgeworfen.

Die Standardisierung der aufkommenden 6G-Technologie steht noch bevor. Das BSI beteiligt sich bereits heute zu Sicherheitsaspekten an der 6G-Plattform, einer vom BMBF geförderten Koordinierungsplattform für Deutschland. Mit wichtigen deutschen 6G-Forschungsprojekten besteht kontinuierlicher Austausch.

Um die Standardisierung in den Organisationen voranzutreiben, nutzt das BSI ein eigenes Testlabor. Mit der Zielsetzung der Erhöhung des Sicherheitsniveaus von Mobilfunknetzen befindet sich das 5G/6G Security Lab TEMIS (Test Environment for Mobile Infrastructure Security) im Aufbau. Im Fokus stehen Sicherheitsuntersuchungen von 5G-Komponenten sowie Entwicklung und Verifikation von sicherheitsrelevanten Tests und Vorgaben für die 5G-Technologie. Mitte 2023 geht TEMIS mit Mobilfunkkomponenten des ersten Herstellers in Betrieb.

## 12.3 – Förderung von Cybersicherheit und digitaler Souveränität in den Kommunikationstechnologien 5G/6G

Die Nr. 45 des Konjunkturprogramms (KoPa) der Bundesregierung zur Adressierung der Folgen der Corona-Pandemie fördert Investitionen in zukünftige Kommunikationstechnologien (5G/6G). Das BSI setzt die Nr. 45 KoPa

mit dem eigenen Förderprogramm „Cybersicherheit und digitale Souveränität in den Kommunikationstechnologien 5G/6G“ sowie flankierenden Studien und Beschaffungen um. Ziele sind die Förderung der digitalen Souveränität und die Stärkung der Innovationskraft deutscher Unternehmen im IT-Sicherheitskontext. Seit dem Start des Förderprogramms im Juni 2022 wurden 32 Projekte bewilligt.

### 13. – eID: Novellierung der eIDAS-Verordnung

Eine der größten Bedrohungen für Verbraucherinnen und Verbraucher ist im aktuellen Berichtszeitraum Identitätsdiebstahl und Online-Betrug (vgl. Kapitel *Erkenntnisse zur Gefährdungslage in der Gesellschaft*, Seite 51). Digitale Geschäftsprozesse haben nicht erst durch die COVID-19-Pandemie eine steigende Bedeutung erfahren. Dadurch stieg auch der Bedarf an sicherer elektronischer Identifizierung und sicheren elektronischen Identitäten, um die Integrität digitaler Prozesse sowie ein hohes Maß an Vertrauen zwischen Nutzer und Dienstleister zu gewährleisten. Dies trägt maßgeblich dazu bei, Online-Betrug sowie insbesondere Identitätsdiebstahl zu erschweren. Das BSI arbeitet dafür seit Jahren daran, die Online-Ausweisfunktion zugänglicher zu machen und weitere Use Cases zu ermöglichen. Mit der Technischen Richtlinie TR-03128 Teil 3 hat das BSI so die technischen Möglichkeiten geschaffen, dass sich Bürgerinnen und Bürger eine neue PIN von zu Hause aus bestellen oder sich online bei der Meldebehörde ummelden können. Während die Nutzerzahlen beim PIN-Rücksetzdienst im Berichtszeitraum anstiegen, ist die elektronische Wohnsitzanmeldung zum aktuellen Zeitpunkt als eine eFA-Leistung des Landes Hamburg umgesetzt und wird dort bereits genutzt.

Im Rahmen der eIDAS-Verordnung akzeptieren die EU-Mitgliedsstaaten gegenseitig notifizierte elektronische Identifizierungsmittel (eID) in nationalen Anwendungen. So ist es aktuell zum Beispiel möglich, mit einer italienischen eID einen Dienst in Deutschland zu nutzen. Im Berichtszeitraum haben weitere Staaten per Verordnung elektronische Identifizierungssysteme zur grenzüberschreitenden Anerkennung notifizierte, die nach Ablauf einer einjährigen Übergangszeit einer gegenseitigen Anerkennungsverpflichtung unterliegen. Hier hat sich das BSI im Rahmen von Peer Reviews beteiligt. Insgesamt

betrifft die Anerkennungsverpflichtung nun 23 elektronische Identifizierungssysteme aus 18 unterschiedlichen Staaten europaweit.

Für die Nutzung elektronischer Verwaltungsdienstleistungen im europäischen Ausland können Bürgerinnen und Bürger ihre deutsche eID-Karte (Personalausweis, elektronischer Aufenthaltstitel, Unionsbürgerkarte) zusammen mit der Online-Ausweisfunktion für die *Authentifizierung* und Identifizierung verwenden. Hierfür wird den EU-Mitgliedsstaaten eine Software bereitgestellt, die die Übersetzung vom deutschen eID-System zum europäischen eIDAS-System leistet: die eIDAS-Middle-ware. Momentan sind 20 Länder sowie die EU-Kommission an das deutsche eID-System angeschlossen. Im Berichtszeitraum wurden die europäischen technischen Richtlinien eIDAS Technical Specifications<sup>31</sup> aktualisiert und um zusätzliche Identitätsattribute erweitert. Darüber hinaus wurden die Stabilität und Nutzerfreundlichkeit der eIDAS-Middleware verbessert, um Ausfallzeiten zu minimieren und die Verwendung zu erleichtern. Weiterhin ist geplant, den Austausch zwischen den Mitgliedsstaaten zu verbessern, um schneller über Änderungen an den Schnittstellen zwischen dem nationalen eID-System und dem europäischen eIDAS-System zu informieren. Damit wird die Interkonnektivität zwischen den Mitgliedsstaaten weiter erhöht.

Neben vielen kleineren Änderungen sieht der 2021 im Rahmen der turnusgemäßen Revision der eIDAS-Verordnung veröffentlichte neue Verordnungsentwurf eine digitale Brieftasche, die „EU Digital Identity Wallet“ (EUDI Wallet) vor, die als elektronisches Identifizierungsmittel grenzüberschreitend nutzbar sein soll. Diese soll neben klassischen Identitätsattributen (Vorname, Name etc.) noch weitere Attribute (z. B. Bildungsabschluss, Führerschein) in verifizierbarer Art für Diensteanbieter bereitstellen können und die Möglichkeit zur qualifizierten elektronischen Signatur bieten. Im Berichtszeitraum ist die Entwicklung der Vorgaben zu dieser EUDI Wallet massiv vorangeschritten. So wurde Anfang 2023 das Architecture and Reference Framework (ARF), das als Grundlage für die zukünftigen Umsetzungsrechtsakte dienen soll, in einer ersten Version durch die europäische Kommission veröffentlicht. Das BSI ist an der Erstellung dieses Dokuments und auch an der Fortentwicklung des ARF beteiligt, bringt die bestehende deutsche Infrastruktur ein und setzt sich weiterhin für sichere und nutzerfreundliche eID-Lösungen ein, die grenzüberschreitend verwendet werden können.

Im Rahmen der EUDI Wallet möchte die Kommission in sogenannten Large Scale Pilots (LSP) nachweisen, dass die Vorgaben umsetzbar sind, und eine oder mehrere Wallets als Piloten auf den Markt bringen. Des Weiteren soll es den Mitgliedsstaaten die Möglichkeit bieten, auch andere, nicht durch das ARF beschriebene Technologien und Ideen zu erproben. Die Entwicklungserkenntnisse dieser Wallets sollen weitergehend auch in die aktuelle Fortschreibung und Weiterentwicklung des ARF und zukünftiger Dokumente einfließen.

Anders als in der älteren eIDAS-Verordnung, die nur die Anerkennung von national bestehenden eID-Lösungen in den Partnerstaaten vorschrieb, sollen nun Mitgliedsstaaten verpflichtet werden, entsprechende eID-Lösungen im Rahmen einer Wallet anzubieten. Außerdem sollen sowohl öffentliche Stellen als auch große private Unternehmen, die eine Anforderung an die Identifizierung ihrer Nutzer haben, die EUDI Wallet als Identifizierungsmittel akzeptieren. Die LSP sollen hier Staaten, die noch keine anerkannte eID-Lösung haben, die Möglichkeit bieten, technisches Know-how wiederzuverwenden.

Die Handlungsstränge der eIDAS-Revision werden in Abbildung 20 dargestellt.

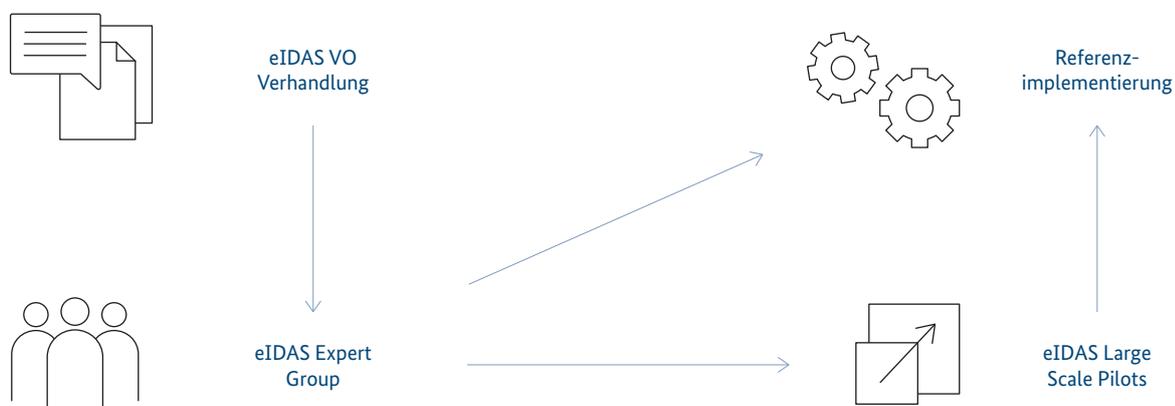
In den Verhandlungen zur eIDAS-Verordnung werden die Rahmenbedingungen definiert, unter denen die eIDAS Expert Group eine technische Ausarbeitung umsetzt. Diese Technik wird in der Referenzimplementierung und

den eIDAS Large Scale Pilots erprobt. Hierbei sollen die LSP die Referenz-Wallet, eine Wallet-Implementierung durch die Kommission, verwenden und im Feld erproben, um Feedback sowohl zur Expert Group als auch zur Entwicklung der Referenz-Wallet zu geben.

Für die Online-Identifikation arbeitet das BSI aktuell an der Umsetzung der Online-Ausweisfunktion in einem Wallet-Modul. Dadurch soll sichergestellt werden, dass die aktuellen Systeme weiterverwendet werden können, um mögliche Investitionen zu senken und das für die Online-Ausweisfunktion bereits notifizierte und anerkannte hohe Vertrauensniveau zu übernehmen. Mithilfe eines modularen Aufbaus der Wallet (siehe Abbildung 21) sollen im Anschluss weitere Nutzungsmöglichkeiten implementiert werden, die nicht auf die bereits vorhandene Technik setzen müssen, entweder, weil es dort bereits international verwendete Standards gibt, oder auch, weil diese Anwendungsfälle kein hohes Vertrauensniveau benötigen. Zusätzlich ermöglicht ein modularer Ansatz eine technische Trennung zwischen den Standards, die eine Online-Kommunikation ermöglichen sollen, und der Nutzung in Offline-Anwendungsfällen, die ohne Internetverbindung einem ganz anderen Anforderungsspektrum genügen müssen. Auch können über Module, neben verschiedenen Anforderungen an Protokolle, verschiedene Anforderungen an die Datenspeicherung abgebildet werden. So wäre für eine Smart-eID die Speicherung in einem eigenen Sicherheitschip, beispielsweise einem Secure Element, notwendig, während andere Nachweise aus der EUDI Wallet diese Sicherheitsanforderungen nicht benötigen.

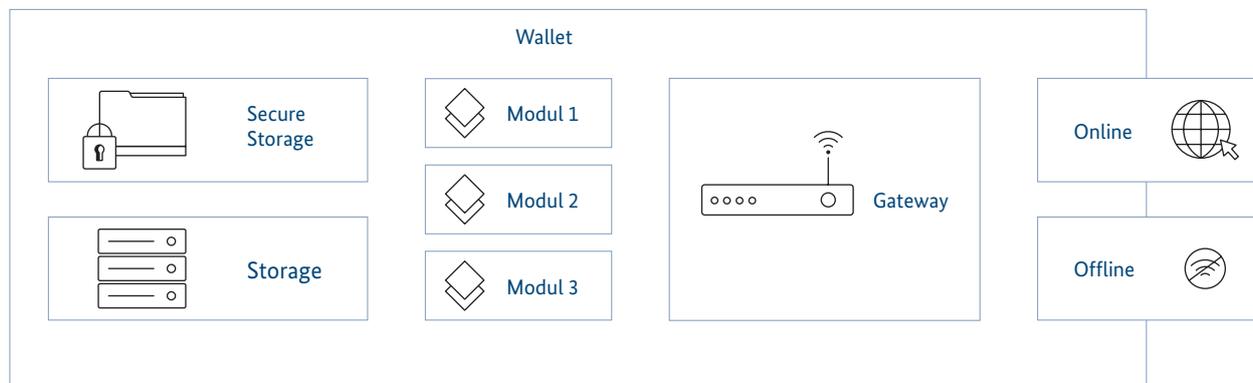
## Handlungsstränge der eIDAS-Revision

Abbildung 20: Handlungsstränge der eIDAS-Revision  
Quelle: BSI



## Schaubild Modulaufbau

Abbildung 21: Schaubild Modulaufbau  
Quelle: BSI



## 14. – Bund-Länder-Zusammenarbeit

Mit der zunehmenden Digitalisierung und Vernetzung von Bund und Ländern geht auch eine Erhöhung der Angriffsfläche einher (vgl. *Erkenntnisse aus der Gefährdungslage in Staat und Verwaltung*, Seite 67). *Ransomware* war im Berichtszeitraum insbesondere für Kommunen die größte Bedrohung, was an der hohen Anzahl bekannt gewordener *Ransomware*-Angriffe zu sehen ist (vgl. *Vorfall Ransomware-Angriffe auf Kommunalverwaltungen und kommunale Versorgungsbetriebe*, Seite 69). Die erfolgreiche Gestaltung der Informationssicherheit in der Verwaltungsdigitalisierung bedarf der fortgesetzten vertrauensvollen Zusammenarbeit zwischen Bund und Ländern.

Aus diesem Grund hat das BSI die Zusammenarbeit mit den Ländern im Berichtszeitraum weiter ausgebaut. Ziel ist es, ein einheitlich hohes IT-Sicherheitsniveau in Deutschland zu schaffen. Dafür ist das BSI unter anderem in den Bund-Länder-Gremien aktiv und gestaltet die Zusammenarbeit mit den Ländern durch bilaterale Kooperationen und Veranstaltungsformate.

### 14.1 – Nationales Verbindungswesen

Das BSI hat seit 2017 insgesamt fünf Verbindungsstellen eröffnet, die für jeweils unterschiedliche Regionen im Bundesgebiet zuständig sind. Durch die Schaffung direkter Ansprechpartnerinnen und Ansprechpartner ist das BSI in der Fläche besser erreichbar. Dadurch kann es seine Aufgaben effizienter wahrnehmen und einen zusätzlichen Beitrag zur Erhöhung des gesamtstaatlichen Cybersicherheitsniveaus in Deutschland leisten. Regionale Verbände, Wirtschaftsunternehmen und auch

Kommunal-, Landes-, Bundes- und EU-Behörden finden über die Verbindungsstellen einen kurzen Weg ins BSI und werden bei ihren Anliegen eng betreut. Ziel ist es, die Kooperation und Vernetzung zu stärken und einen aktiven Beitrag zu regionalen Netzwerkformaten zu leisten. Wesentliches Element ist hierbei der Abschluss von bilateralen Kooperationsvereinbarungen zwischen dem BSI und interessierten Ländern.

### 14.2 – Informationssicherheitsberatung für Länder und Kommunen

Die Informationssicherheitsberatung für Länder und Kommunen berät zielgruppenspezifisch Bedarfsträger auf Landes- und kommunaler Ebene zu allen Fragen der Informationssicherheit mit den thematischen Schwerpunkten Informationssicherheitsmanagement, Sicherheitskonzeption und IT-Grundschutz.

#### Länder

Die Beratung von Ländern konnte auf Basis der abgeschlossenen Kooperationsvereinbarungen ausgebaut werden. Neben den spezifischen Beratungen wurden praxisorientierte Lösungsansätze gemeinschaftlich mit Vertreterinnen und Vertretern aus Bund, Ländern und Kommunen weiterentwickelt. Dabei standen IT-Grundschutzprofile und skalierbare Handreichungen für den Einstieg und die Umsetzung des IT-Grundschutzes im Fokus. Hervorzuheben ist dabei das IT-Grundschutz-Profil „Schnellmeldungen – Absicherung der Schnellmeldungen bei bundesweiten parlamentarischen Wahlen“, das zum Jahreswechsel über den Bundeswahlleiter verteilt wurde.

## Kommunen

Eine effiziente Zusammenarbeit mit fast 11.000 Kommunen erfordert strukturierte Ansätze, die nur gemeinsam mit Multiplikatoren aus den kommunalen Spitzenverbänden und Institutionen der Länder erfolgen kann.

Cyberangriffe auf Kommunen können weitreichende Auswirkungen auf die Bevölkerung haben, da auf dieser Ebene ein Großteil an Verwaltungsdienstleistungen für Bürgerinnen und Bürger erbracht wird. Umso wichtiger ist es, Kommunen bei der Einführung und der Umsetzung von Informationssicherheit zu unterstützen. Daher unterstützt die Informationssicherheitsberatung bei der Sensibilisierung der Management-Ebene im Rahmen von Kongressen und Tagungen und stellt für Informationssicherheitsbeauftragte über den internen Bereich für Länder und Kommunen unter anderem einen Werkzeugkasten und spezifische Hilfestellungen zum IT-Grundschutz bereit. Außerdem wird derzeit mit dem „Weg in die Basis-Absicherung – WiBA“ eine Einstiegsstufe in die etablierte Methodik des IT-Grundschutzes entwickelt. Mit WiBA wird eine Brücke zum IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung exklusiv für den kommunalen Sektor entwickelt, um zum Beispiel OZG-Anforderungen umsetzen zu können.

Im Berichtszeitraum unterstützte das BSI auf Initiative der kommunalen Spitzenverbände bei der Erstellung verschiedener Handreichungen für Führungskräfte in Verwaltungen. Diese bieten konkrete Hilfestellungen bei ersten Schritten für mehr Informationssicherheit.

## 14.3 – Roadshow Kommunen

Wie bereits berichtet, werden dem BSI regelmäßig erfolgreiche Cyberangriffe auf Kommunen bekannt (vgl. Kapitel *Landes- und Kommunalverwaltungen*, Seite 67). Aufgrund der zunehmenden ebenenübergreifenden Vernetzung stellen diese Angriffe auch eine gemeinsame Herausforderung für Bund, Länder und Kommunen dar. Das BSI hat deshalb die Roadshow Kommunen, eine virtuelle Veranstaltungsreihe für die Kommunen, entwickelt, die gemeinsam mit interessierten Ländern für die Zielgruppe Kommunen durchgeführt wird.

Die Planung und Durchführung der Veranstaltung erfolgt unter Einbeziehung der Länder und der kommunalen Spitzenverbände. Das BSI bringt unter anderem Vorträge aus den Bereichen Informationssicherheits-

beratung für Länder und Kommunen, Nationales Verbindungswesen, *CERT-Bund*, BSI-Standards und IT-Grundschutz ein. Die Länder ergänzen diese mit unterschiedlichen, individuell auf das Land zugeschnittenen Vorträgen.

Ziel der Veranstaltung ist es, Kommunen bezüglich der Bedrohungen im Cyberraum zu sensibilisieren und Handlungsoptionen zur Erhöhung des Cybersicherheitsniveaus aufzuzeigen.

Im Berichtszeitraum wurden insgesamt sechs Roadshows Kommunen durchgeführt und weit über 700 Teilnehmende aus den Kommunen erreicht. Aufgrund der positiven Resonanz wird die Roadshow Kommunen fortgeführt und thematisch weiterentwickelt.

## 14.4 – Gremienarbeit

Das BSI arbeitet in beratender Rolle in unterschiedlichen Bund-Länder-Gremien im Bereich der Cyber- und Informationssicherheit mit, beispielsweise in der AG Informationssicherheit des IT-Planungsrates (AG InfoSic) und der Länderarbeitsgruppe Cybersicherheit (LAG Cybersicherheit) der Ständigen Konferenz der Innenminister und -senatoren der Länder (IMK).

### Arbeitsgruppe Informationssicherheit

Das BSI berät den Bund und die Länder bei der Umsetzung der verschiedenen Handlungsfelder der „Leitlinie für Informationssicherheit der öffentlichen Verwaltung“ des IT-Planungsrats, die die strategischen ebenenübergreifenden Ziele zur Informationssicherheit definiert. Hierbei bringt das BSI seine Expertise ein und arbeitet aktiv in Arbeitsgruppen mit, wie zum Beispiel bei der Erstellung von Konzepten zum IT-Notfallmanagement und eines Standards zur Erkennung und Abwehr von IT-Angriffen. Außerdem betreibt das BSI die Geschäftsstelle der AG Informationssicherheit und unterstützt den jeweiligen Vorsitz (im Berichtszeitraum: Sachsen und Saarland) bei der Sitzungsdurchführung.

### LAG Cybersicherheit

Die Innenministerkonferenz (IMK) unterhält eine LAG Cybersicherheit zur Abstimmung der länderübergreifenden fachlichen Zusammenarbeit im Themenfeld Cybersicherheit. Das BSI bringt seine Expertise hierbei in unterschiedlichen Unter-Arbeitsgruppen ein, im

Berichtszeitraum beispielsweise in die Arbeitsgruppe zur Umsetzung der Protokollerklärung zum IT-Sicherheitsgesetz. Ziel dieser Arbeitsgruppe ist es, die Informationsweitergabe zwischen BSI und den Ländern zu verbessern.

#### 14.5 – VerwaltungsCERT-Verbund (VCV)

Die operative Zusammenarbeit mit den Ländern erfolgt über *CERT-Bund* im Rahmen des Verwaltungs-CERT-Verbundes (VCV). Der Informationsaustausch innerhalb des VCV ermöglicht es, bundesweit effektiver und schneller auf IT-Angriffe reagieren zu können. Dabei teilen die 13 verschiedenen Landes-CERTs lagerelevante Vorfallsinformationen und sprechen vertrauensvoll über operative Themen wie aktuelle Schwachstellen, die allgemeine Lage und Best-Practice-Ansätze. Der gemeinsame Austausch wurde im Berichtszeitraum auch in Anbetracht der abstrakt erhöhten Bedrohungslage intensiviert und durch bilaterale Gespräche, zwei hybride Arbeitstreffen und eine Hospitation von mehreren Landes-CERTs im BSI begleitet.

#### 14.6 – Kooperationsvereinbarungen zwischen BSI und den Ländern

Bilaterale Kooperationsvereinbarungen zwischen dem BSI und den Ländern bilden den Rahmen der Zusammenarbeit und ermöglichen eine gegenseitige Unterstützung auf Augenhöhe im derzeit bestehenden Rechtsrahmen.

Das BSI kann gemäß § 3 BSIG die Länder in Fragen der Informationssicherheit beraten und warnen sowie auf deren Ersuchen bei der Sicherung ihrer Informationstechnik und Abwehr von Gefahren unterstützen. Basierend auf diesen Rahmenbedingungen hat das BSI einen Katalog von Kooperationsfeldern erarbeitet. Aus diesem können die Länder die Kooperationen auswählen, für die sie einen Bedarf haben.

Die Länder können diese Kooperationsangebote durch eigene Angebote ergänzen, die das BSI seinerseits nutzen kann. Es ist im Sinne der Kooperationsvereinbarung, dass mit dem BSI und den Ländern alle Kooperationspartner im gleichen Maße profitieren. Jede Vereinbarung kann so individuell auf die jeweiligen Bedarfe des Landes und des BSI zugeschnitten werden. In einem sogenannten Jahresarbeitsprogramm werden die Kooperationen, bei-

spielsweise Beratungen zum Aufbau eines Managementsystems für Informationssicherheit, konkretisiert und dann sukzessive umgesetzt.

Zum aktuellen Stand hat das BSI vier Kooperationsvereinbarungen mit Ländern geschlossen. Weitere Vereinbarungen sind bereits geplant oder unmittelbar in Vorbereitung.

#### 14.7 – Weiterentwicklung der Zusammenarbeit mit den Ländern

Die Kooperationsvereinbarungen zwischen dem BSI und den Bundesländern sind ein wichtiger Meilenstein auf dem Weg zu einer verbindlichen Bund-Länder-Zusammenarbeit im Bereich der Cybersicherheit. Sie schöpfen den derzeit gültigen Rechtsrahmen der ebenenübergreifenden Zusammenarbeit aus.

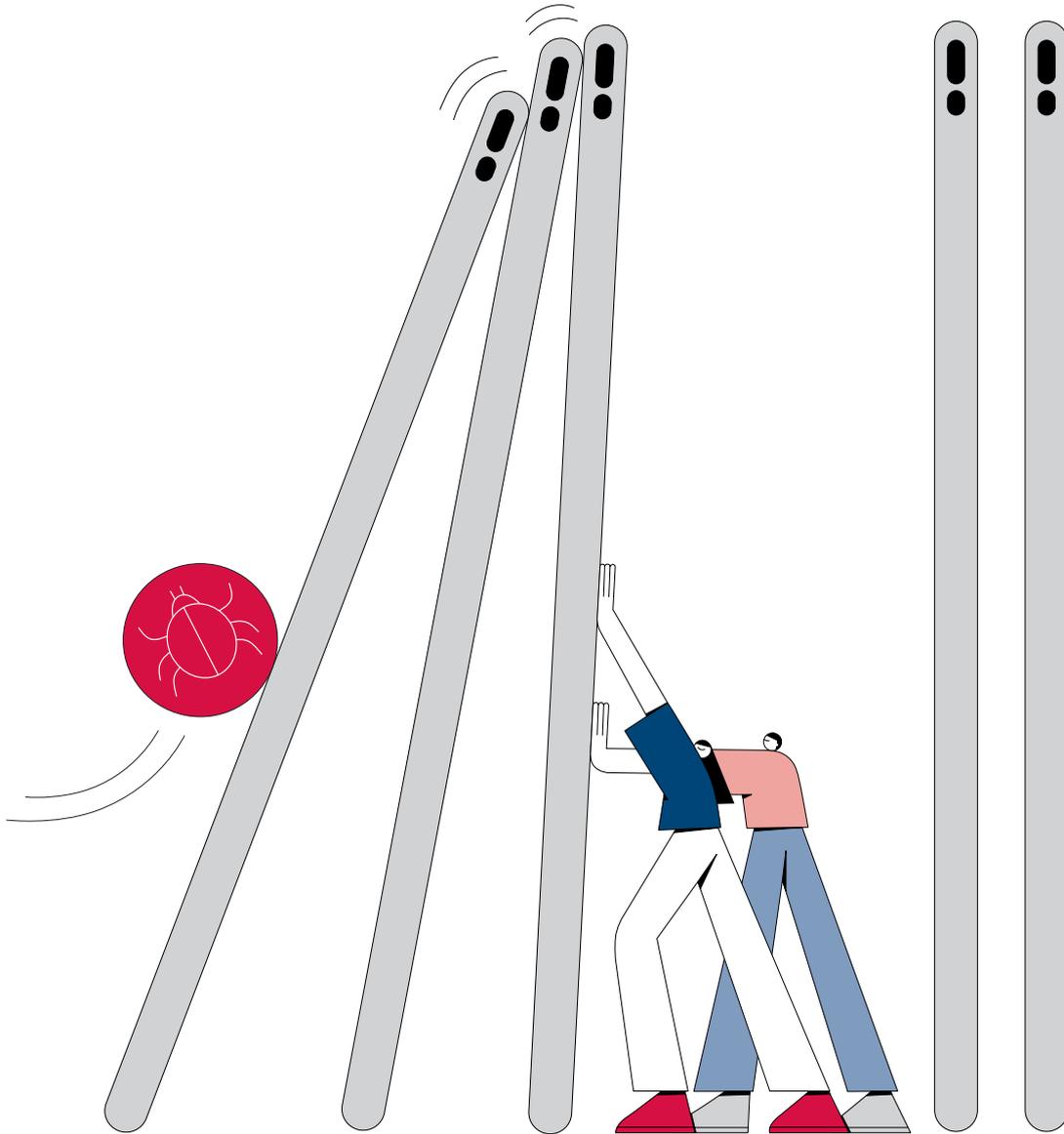
Allerdings gibt es den Bedarf an engerer Zusammenarbeit, um aktuellen und künftigen Bedrohungslagen im Cyberraum noch besser begegnen zu können. So hat das BSI aktuell zum Beispiel keine Möglichkeit, die Länder bei der Detektion von Schadsoftware in den Landesnetzen zu unterstützen, etwa durch Bereitstellung von Sensorik. Gleichzeitig ist es im Sinne einer ganzheitlichen Betrachtung der Lage der Informationssicherheit in Deutschland zielführend, ein einheitliches Bund-Länder-Lagebild anzustreben. Ein vernetztes Lagebild ermöglicht es, in Gegenüberstellung zu einzelnen bundeslandspezifischen Erfassungen, Gefährdungstrends und grenzübergreifende Phänomene schneller und spezifischer zu identifizieren. Deshalb erarbeiten das BMI, das BSI und die Länder aktuell ein Konzept zum Ausbau des BSI zur Zentralstelle im Bund-Länder-Verhältnis, das einen Ausbau der gesetzlichen Grundlagen der Bund-Länder-Zusammenarbeit im Bereich Cybersicherheit näher beschreibt.

Aktuell werden die Vorhaben bzw. Bedarfe zwischen Bund und Ländern abgestimmt. Ziel der Bundesregierung ist es, durch eine Änderung des Grundgesetzes, die Zusammenarbeit zwischen Bund und Ländern im Bereich der Cybersicherheit zu verstetigen und zu vertiefen.

---

# Fazit

---



## Fazit

### 15. – Fazit

#### Resilienz ist das Gebot der Stunde

Die Bedrohungslage im Bereich der Cybersicherheit ist weiterhin von einer hohen Dynamik geprägt. Die rasante Entwicklung im Bereich der Künstlichen Intelligenz zeigt, wie schnell technische Neuerungen fortschreiten können. Diese bringt neben großen Chancen für die Digitalisierung auch ein hohes Bedrohungspotenzial mit sich. Nach wie vor bleiben Angriffe mit Ransomware die größte Bedrohung für die Cybersicherheit in Deutschland. Daneben rücken Cyberangriffe auf Lieferketten weiter in den Mittelpunkt. Sie können die Cybersicherheit ganzer Branchen gefährden.

Im vorliegenden Berichtszeitraum setzt sich die Entwicklung der Bedrohungslage demnach unverändert fort – sie gilt als angespannt bis kritisch. Wichtig ist daher, die Resilienz der Bundesrepublik Deutschland auch gegen Cyberangriffe und IT-Sicherheitsvorfälle weiter zu steigern.

#### Hauptrisiko Ransomware: größte Bedrohung für die Cybersicherheit in Deutschland

Bei Cyberangriffen mit *Ransomware* ist im Berichtszeitraum zu beobachten, dass das zuletzt vorherrschende Big Game Hunting abgenommen hat. Statt sich auf große, zahlungsfähige Unternehmen zu konzentrieren, haben Cyberkriminelle wieder vermehrt kleine und mittlere Unternehmen und auch staatliche Institutionen und Kommunen zum Ziel von *Ransomware*-Angriffen gemacht.

Immer häufiger sind auch Kommunalverwaltungen und kommunale Betriebe von erfolgreichen Cyberangriffen betroffen. Bürgerinnen und Bürger sind dabei oftmals auch unmittelbar betroffen. Entweder weil bürgernahe Dienstleistungen oft über Wochen nicht zur Verfügung stehen oder weil persönliche Daten in die Hände Krimineller gelangen. Dies zeigt, wie wichtig *Resilienz* ist. Sie umfasst auch die Fähigkeit, nach einem IT-Sicherheits-

vorfall möglichst schnell wieder die erforderliche Handlungsfähigkeit zu erlangen und in den Normalzustand zurückkehren zu können.

#### Professionalisierung der Cyberkriminalität geht weiter

Bei der Cyberkriminalität ist eine stetig weiter voranschreitende Arbeitsteilung und Professionalisierung unter den Cyberkriminellen festzustellen, die sich in einem wachsenden Dienstleistungscharakter manifestiert. Die Schattenwirtschaft der Cyberkriminalität spiegelt damit in gewisser Weise die Realwirtschaft, die ebenfalls auf eine starke Arbeitsteilung setzt und sich immer stärker über Länder- und Branchengrenzen hinweg vernetzt.

Dieser Ausbau des Cybercrime-as-a-Service ist ein herausragender Faktor bei der Entwicklung der Bedrohungslage, denn die Spezialisierung auf bestimmte Dienstleistungen ermöglicht es Angreifenden, ihre Services gezielt zu entwickeln und zu professionalisieren. Dem lässt sich nur durch eine entsprechende Professionalisierung auf Abwehrseite entgegenwirken. Ein Mittel sind qualifizierte Sicherheitsexpertinnen und -experten – Dienstleister, die ihrerseits besonders gut geschützt sein müssen. Durch Standardisierung und Zentralisierung können Kommunen sowie kleine und mittlere Unternehmen ihre Cyberresilienz stärken. Eine Basisabsicherung nach dem IT-Grundschutz für Kommunen oder dem Cybersicherheitscheck für Unternehmen sind dafür wirksame Werkzeuge.

#### Schwachstellen bei Software auf besorgniserregendem Niveau

Eine beunruhigende Entwicklung ist auch im Bereich der Schwachstellen zu beobachten. Vor allem bei Schwachstellen von Softwareprodukten konnten starke Zuwächse registriert werden. Solche Lücken sind oft das erste Einfallstor für Cyberkriminelle auf ihrem Weg zu einer Kompromittierung von Systemen und Netzwerken. Die zunehmende und umfassende Vernetzung macht die Systeme überhaupt erst von außen zugänglich und erlaubt Angreifenden gleichzeitig, aus der Ferne zu agieren.

Im Berichtszeitraum wurden jeden Tag durchschnittlich knapp 70 neue Schwachstellen in Software-Produkten bekannt, rund ein Viertel mehr als im Berichtszeitraum davor. Mit der Anzahl der gefundenen Schwachstellen stieg auch ihre potenzielle Schädwirkung. 3.784 der identifizierten Lücken wurden als kritisch eingestuft (zuvor: 2.680). Das sind 15 Prozent aller festgestellten Schwachstellen. Die Entwicklung sowohl bei der Zahl als auch bei der Kritikalität sind besorgniserregend. Das BSI setzt dem unter anderem Initiativen zur (Teil-)Automatisierung von Unternehmens- und Security-Prozessen entgegen, beispielsweise durch die automatische Filterung der Meldung von Sicherheitslücken auf Relevanz für die eigenen Systeme. Die technische Grundlage hierfür ist das unter anderem vom BSI spezifizierte Common Security Advisory Format (CSAF), durch das Sicherheits-Advisories maschinenlesbar und automatisiert verarbeitbar sind.

### **Generative KI: Chance und Risiko für die Cybersicherheit**

Das Aufkommen generativer Künstlicher Intelligenz führt im Sicherheitsbereich zu neuen Herausforderungen. Mit der Veröffentlichung von ChatGPT und einer Vielzahl weiterer Tools ist KI auch in einer breiten, wenig technikaffinen Öffentlichkeit angekommen. Große KI-Sprachmodelle, die hinter Modellen wie ChatGPT, LLaMA oder Bard stehen, sind teilweise frei verfügbar. Zu ihrem Aufschwung hat die hohe Qualität der von KI generierten Texte und Bilder beigetragen, ebenso die einfache Zugänglichkeit dieser und weiterer Tools, unter anderem für *Deepfakes*. Manipulierte Bilder, Videos und Stimmen werden durch die kontinuierliche Qualitätssteigerung der öffentlich zugänglichen Werkzeuge immer authentischer und dadurch schwerer zu entlarven.

Die Folgen sind vielfältig. Neben bereits bekannten Angriffen wie CEO-Fraud oder dem Einzeltrick werden die angesprochenen Tools auch von Cyberkriminellen auf weitere Einsatzfähigkeit bei Angriffen geprüft, zum Beispiel bei der Generierung von Schadcode oder bei Social Engineering und Desinformationskampagnen. Zu dieser Skalierung bereits bekannter Bedrohungen kommen neue Bedrohungen, die in der neuen Technik und der damit verbundenen Vergrößerung der Angriffsfläche begründet liegt. Künstliche Intelligenz selbst ist angreifbar und kann eine Schwachstelle sein. Unter anderem durch die Unschärfe im Design von KI und LLM steht das Schwachstellenmanagement in Unternehmen und Behörden vor noch nie da gewesenen Herausforderungen.

Neben diesen Sicherheitsrisiken ist die große Herausforderung, mit der rasanten Entwicklung im Bereich KI Schritt zu halten. Ziel muss es sein, über mögliche Sicherheitsrisiken bei der Verwendung von KI aufzuklären, um verantwortungsvoll mit den Fähigkeiten und Arbeitsergebnissen dieser Modelle umgehen zu können. So muss es technische Maßnahmen geben, um den Output von KI identifizieren zu können. Darüber hinaus müssen Hersteller und Anbieter von LLMs und LLM-basierten Anwendungen Vorkehrungen treffen, um die Erzeugung potenziell schädlicher Ausgaben weitestgehend zu verhindern oder zu erschweren.

### **Auswirkungen des Ukraine-Kriegs auf die IT-Sicherheitslage in Deutschland**

Der russische Angriffskrieg gegen die Ukraine nahm im Berichtszeitraum weiterhin einen zentralen Platz in der öffentlichen Wahrnehmung ein. Die registrierten *DDoS-Angriffe* pro-russischer Aktivisten haben bisher wenig bis keinen bleibenden Schaden anrichten können. Da dies zum großen Teil auch an der gewählten Angriffsart *DDoS* liegt, sind die bisherigen Angriffe eher dem Bereich Propaganda zuzuordnen – mit dem Ziel, Verunsicherung zu stiften und das Vertrauen in den Staat zu untergraben. Die Vergangenheit hat gezeigt, dass sich dies jederzeit ändern kann, etwa durch Kollateralschäden oder Angriffe auf Kritische Infrastrukturen. Dem kann man mit einer ausgeprägten Cyberresilienz und der Lage angepassten Sicherheitsvorkehrungen durchaus erfolgreich begegnen.

### **Wachsam und handlungsfähig bleiben für eine erfolgreiche Digitalisierung**

Cyberresilienz bedeutet, mit Angriffen umgehen zu können, ohne umzufallen. Cyberresilienz heißt auch, schnell wieder auf die Beine zu kommen, wenn man Opfer eines Cyberangriffs geworden ist – und sich wenn nötig auch wehren zu können. Um das zu schaffen, braucht es eine tragfähige Cybersicherheitsarchitektur.

Das BSI versteht sich als zentrale Stelle in der Sicherheitsarchitektur Deutschlands, die allen Akteuren Handlungsmöglichkeiten und Unterstützungsmaßnahmen anbietet. Diese zentrale Position sorgt nicht nur für mehr Effizienz, sondern ist auch für einen nachhaltigen Einsatz von Ressourcen geeignet. Deshalb begrüßt das BSI den von der Bundesregierung angestrebten Ausbau des BSI zur Zentralstelle im Bund-Länder-Verhältnis.

Cybersicherheit ist eine Gemeinschaftsaufgabe von Bund, Ländern und Kommunen, die nur mit einem adäquaten Ressourceneinsatz bewältigt werden kann. Das allein reicht aber nicht aus. Nötig ist der immerwährende Austausch zwischen Politik, Wirtschaft, Wissenschaft und Gesellschaft – in Deutschland, aber auch über Landesgrenzen hinweg.

### **Resilienz erhöhen – Cybersicherheit gestalten – Digitalisierung beschleunigen**

Die Nationale Sicherheitsstrategie des Bundes betont die signifikant gestiegene Bedeutung von Cybersicherheit. Zu Recht, wie der BSI-Lagebericht zeigt. Als Cybersicherheitsbehörde des Bundes sieht das BSI seinen Auftrag darin,

- die Resilienz schnellstmöglich zu erhöhen, um Angriffen standzuhalten,
- Cybersicherheit pragmatisch zu gestalten, um Angreifern stets einen Schritt voraus zu sein,
- die Digitalisierung zu beschleunigen, um mit den Entwicklungen unserer Zeit Schritt zu halten.

Das alles kann gelingen, wenn die Positionen des BSI gehört, seine Vorgaben umgesetzt und seine Produkte genutzt werden. Das BSI wird seinen Beitrag dazu leisten, indem es seine Rolle als Partner, Helfer und Möglichmacher in Zukunft noch stärker ausfüllt: mit realistisch umsetzbaren Standards und einfach anwendbaren Lösungen für Staat, Wirtschaft und Gesellschaft. Ein Grundsatz, der das BSI dabei trägt: Abgrenzung gilt nicht – Kooperation gewinnt!

## Glossar

---

### **Access Broker**

Als *Access Broker* werden Cyberkriminelle bezeichnet, die sich über verschiedenste Wege Zugang zu einem Opfernnetzwerk 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 aufseiten 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 Angriffsweg 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 (z. B. 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 Informationstechnik und beinhalten u. a. Infrastrukturen (Rechenleistung, Speicherplatz), Plattformen und Software.

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

Server-Infrastruktur, 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.

***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 bzw. dienstleistungsorientiert ermöglicht werden. So wird beispielsweise bei der 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 ggf. auch mit Updates und weiteren ähnlichen Services versorgt, ganz so wie die legale 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.

***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.

***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.

***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* z. B. ein Programm zum Absturz gebracht, Benutzerrechte ausgeweitet oder beliebiger Programmcode ausgeführt werden.

***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 (z. B. 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 bzw. nur unter extrem hohem Rechenaufwand möglich.

### **Hybride Bedrohungen**

Illegitime Einflussnahme fremder Staaten mithilfe von Maßnahmen in verschiedenen Räumen. Physische Angriffe können zum Beispiel durch Cyberangriffe oder Desinformationskampagnen begleitet werden.

### **Information Stealer**

Schadprogramme, die es Cyberkriminellen ermöglichen, auf infizierten Geräten an unterschiedliche Arten persönlicher Daten, wie beispielsweise Login-Daten für verschiedene Online-dienste, 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 aus der physischen und virtuellen Welt Daten erfassen, verarbeiten und speichern und miteinander vernetzt sind.

### **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.

### **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.

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

Ein *MOTW* kennzeichnet Download-Dateien, wenn diese aus einer wahrscheinlich nicht vertrauenswürdigen Quelle stammen. Öffnet 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.

### **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 Netzwerk-Nutzerinnen und -Nutzern das Speichern und Abrufen von Daten an einem zentralen Ort ermöglicht.

### **Password-Spraying**

Angriffsmethode, bei der der Angreifer beliebige oder typische Passwörter (z. B. 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.

### **Phishing**

Das Wort setzt sich aus *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 ihres 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 Angreifergroupierungen verbreiten, ohne dass diese jeweils spezifische technische Kompetenzen aufbauen müssen.

**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* bzw. 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 Computerprogrammes 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, verfügbare technische Infrastrukturen oder Ähnliches.

**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, den *RSA*-Modul  $n$  zu faktorisieren, d. h. nur aus Kenntnis von  $n$  die beiden Primfaktoren  $p$  und  $q$  zu berechnen.

**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.

**Scam-Mail**

Betrugsmail: Kategorie von *Spam*-Mails, mit denen Angreifer vorgeben, z. B. Spendengelder zu sammeln.

**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 Sicherheitsfor-

scherrinnen und -forschern betrieben, um *Botnetz*infektionen aufzuspüren und betroffene Anwenderinnen und Anwender zu informieren.

#### **Script-Kiddies**

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

#### **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 *Spam*-Nachrichten meist unerwünschte Werbung. Häufig enthalten *Spam*-Nachrichten jedoch auch Schadprogramme im Anhang, Links zu verseuchten Webseiten oder sie werden für *Phishing*-Angriffe genutzt.

#### **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.

#### **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 bspw. 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 autorisierten 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 Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und staatlichen Stellen wie dem BSI.

#### **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.

#### **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).

## Quellenverzeichnis

---

- 1) <https://www.heise.de/news/Mehrere-Verhaftungen-Strafverfolger-gehen-gegen-DDoS-Booter-Dienste-vor-7396504.html>
- 2) <https://www.hertzbleed.com/hertzbleed.pdf>
- 3) <https://eprint.iacr.org/2022/975>
- 4) <https://samcurry.net/web-hackers-vs-the-auto-industry/>
- 5) <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/onlineshopping-plattformen.html>
- 6) <https://www.verbraucherzentrale.de/geld-versicherungen/phishing-gradar-archiv-71872>
- 7) <https://www.verbraucherzentrale.de/geld-versicherungen/phishing-gradar-archiv-71872>
- 8) Studie des TÜV-Verbandes: „2023: Cybersicherheit in deutschen Unternehmen“
- 9) <https://de.statista.com/infografik/26033/ausgaben-fuer-it-sicherheit-in-deutschland>
- 10) <https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022>
- 11) <https://www.dihk.de/resource/blob/91514/be8371c167a1468d387fdaa075327330/dihk-sonderauswertung-cybersicherheit-2023-data.pdf>
- 12) <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
- 13) <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>
- 14) <https://www.bsi.bund.de/OHNAchweise>
- 15) <https://www.dihk.de/resource/blob/91514/be8371c167a1468d387fdaa075327330/dihk-sonderauswertung-cybersicherheit-2023-data.pdf>
- 16) <https://www.dihk.de/resource/blob/91516/aac9a26dea81dc7c1bc1e5f28b6105e8/dihk-digitalisierungsumfrage-2022-2023-data.pdf>
- 17) NKMG mbH & BIGS gGmbH im Auftrag des Bundesministeriums für Wirtschaft und Energie: IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU in Deutschland, 2021, S. 5
- 18) [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/AI/MobilityAuditPrep\\_final\\_results.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/AI/MobilityAuditPrep_final_results.pdf)
- 19) <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive.html>
- 20) <https://www.vice.com/en/article/dy7axa/how-i-broke-into-a-bank-account-with-an-ai-generated-voice>
- 21) <https://iopscience.iop.org/article/10.1088/2058-9565/ab4eb5/pdf>
- 22) <https://www.bsi.bund.de/dok/QML>
- 23) <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/>, <https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf>
- 24) [https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA\\_CNSA\\_2.0\\_ALGORITHMS\\_.pdf](https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.pdf)
- 25) <https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf>
- 26) <https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislativ.pdf>
- 27) <https://dserver.bundestag.de/btd/20/066/2006610.pdf>
- 28) <https://csrc.nist.gov/publications/detail/nistir/8413/final>
- 29) <https://www.bsi.bund.de/dok/umfrage-pqc>
- 30) [https://www.etsi.org/deliver/etsi\\_gs/QKD/001\\_099/016/01.01.01\\_60/gs\\_QKD016v010101p.pdf](https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/01.01.01_60/gs_QKD016v010101p.pdf)
- 31) <https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eIDAS+eID+Profile>

## Verzeichnis der im Dokument abgebildeten QR-Codes

---

- a) [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/dvs-bericht\\_2022.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/dvs-bericht_2022.html)  
<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive-2022-2023.html>  
[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Lagebild\\_Gesundheit\\_2022.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Lagebild_Gesundheit_2022.html)  
[https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Broschueren/broschueren\\_node.html](https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Broschueren/broschueren_node.html)
- b) [https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Fragen-und-Antworten/fragen-und-antworten\\_node.html](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Fragen-und-Antworten/fragen-und-antworten_node.html)
- c) [https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/APT/apt\\_node.html](https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/APT/apt_node.html)  
[https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/ransomware-angriffe\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/ransomware-angriffe_node.html)  
[https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/unternehmen\\_node.html](https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/unternehmen_node.html)  
<https://www.bsi.bund.de/dok/CSN>
- d) [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister\\_APT-Response-Liste.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.pdf)
- e) <https://www.bsi.bund.de/ddos>
- f) [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html)
- g) <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive-2022-2023.pdf>
- h) [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)
- i) [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)
- j) [https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/UP-KRITIS/up-kritis\\_node.html](https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/UP-KRITIS/up-kritis_node.html)
- k) [www.bsi.bund.de/kmu](http://www.bsi.bund.de/kmu)
- l) [www.bsi.bund.de/dok/crc](http://www.bsi.bund.de/dok/crc)
- m) [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Grosse\\_KI\\_Sprachmodelle.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Grosse_KI_Sprachmodelle.pdf)
- n) [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Automotive/Automatisiertes\\_Fahren/Automatisiertes\\_Fahren\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Automotive/Automatisiertes_Fahren/Automatisiertes_Fahren_node.html)
- o) [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Security-of-AI-systems\\_fundamentals\\_considerations\\_symbolic\\_hybrid.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Security-of-AI-systems_fundamentals_considerations_symbolic_hybrid.pdf)  
[https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/ML-SAST/ml-sast\\_node.html](https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/ML-SAST/ml-sast_node.html)  
[https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/KI/P464\\_Provision\\_use\\_external\\_data\\_trained\\_models.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/KI/P464_Provision_use_external_data_trained_models.pdf)
- p) <https://www.bsi.bund.de/qcstudie>
- q) <https://www.bsi.bund.de/PQ-Migration>
- r) [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html)
- s) [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03163/tr03163\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03163/tr03163_node.html)

**Herausgeber**

Bundesamt für Sicherheit in der Informationstechnik (BSI)

**Bezugsquelle**

Bundesamt für Sicherheit in der Informationstechnik (BSI)  
Godesberger Allee 185–189  
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 2023

**Druck**

Appel & Klinger Druck und Medien GmbH, Schneckenlohe

**Gestaltung**

Faktor 3 AG

**Texte und Redaktion**

Bundesamt für Sicherheit in der Informationstechnik (BSI)

**Illustrationen**

Anne Albert c/o kombinatrotweiss.de  
Instagram: [annealbert\\_illustration](#) | [kombinatrotweiss\\_illustration](#)

**Grafiken**

Bundesamt für Sicherheit in der Informationstechnik (BSI)

**Bildnachweis**

Seite 2: © BMI; Seite 4: © BMI/Henning Schacht

**Artikelnummer**

BSI-LB23/512

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

