schwarz digits

CYBER SECURITY REPORT 2025

VORWORT

GRENZENLOS

Nichts und niemand ist mehr sicher – politisch, wirtschaftlich und digital. Wir leben in einer Zeit globaler Spannungen, geprägt von politischen Konflikten, geopolitischen Rivalitäten und wirtschaftlicher Instabilität. Diese Krisen betreffen auch den digitalen Raum. Angriffe zielen auf Unterseekabel und Satelliten. Beschädigte Leitungen in der Ostsee stören Kommunikationsnetze und die Energieversorgung. Attacken auf digitale Lieferketten bedrohen auch die physische Welt, verursachen Produktionsausfälle und Lieferchaos.

Cyberangriffe sind auch Treiber für moderne Konflikte. Sie gefährden die kritische Infrastruktur, sind Werkzeug weltpolitischer Machtkämpfe und Mittel wirtschaftlicher Sabotage. Ihre Anzahl steigt dramatisch: Ransomware-Attacken dominieren weiterhin. Betroffene nennen sie mit 31 Prozent als häufigste Schadensursache. Auch der Zugriff auf gestohlene digitale Identitäten nimmt zu.

Kein Unternehmen, keine Behörde, keine Privatperson ist sicher. Die Angreifer sind gut organisiert, hoch professionell und teils staatlich gefördert. Sie wollen zerstören, stehlen, erpressen und kontrollieren. Mit jeder Schwachstelle wächst ihre Macht. Regulatorische Anforderungen und die steigende Komplexität digitaler Ökosysteme erhöhen täglich den Handlungsdruck auf Entscheider und Cybersicherheitsexperten.

Der Weg sich zu schützen ist ein kontinuierlicher Prozess. Die Ergebnisse unserer repräsentativen Umfrage unter 1.000 deutschen Unternehmen sind alarmierend: Nur jedes zweite kleinere Unternehmen überprüft regelmäßig die Cybersicherheit seiner Lieferanten. Selbst mittelgroße Unternehmen führen nur selten sogenannte Pentests, umfassende Sicherheitsprüfungen einzelner Systeme, durch. Insbesondere der Handel und die Konsumgüterindustrie hinken hinterher. Sowohl bei Cybersicherheitsressourcen als auch bei Maßnahmen.

In Deutschland wurden 2024 rund 5,8 Milliarden Euro in Cybersicherheitslösungen investiert. Cyberkriminelle verursachten zeitgleich Schäden in Höhe von fast 179 Milliarden Euro. Die digitale Angriffsfläche wird täglich größer und mit ihr die Bedrohung. Wir haben die Wahl: den Angriff abwarten oder voraushandeln.

Es gilt umzudenken, weg von reaktiv hin zu präventiv. Cybersicherheit betrifft uns alle. Es geht nicht nur um Technik. Es geht um Verantwortung – gegenüber dieser Generation und der nächsten. Prävention und Aufklärung sind essenziell, um auch die Schwächsten vor digitaler Erpressung zu schützen.

Der Schlüssel liegt im Wissenstransfer und in konkreten Maßnahmen. Unser Cyber Security Report 2025 bietet den Überblick. Er zeigt Gefahren auf und liefert zielgerichtete Handlungsempfehlungen. Die digitale Welt ist nicht nur ein Raum, den wir gemeinsam verteidigen müssen. Sie ist der Ort, an dem wir unsere Zukunft gestalten. Lassen Sie uns sicherstellen, dass sie uns gehört – und nicht denen, die sie zerstören wollen.

Als Unternehmen der Schwarz Gruppe handeln wir voraus und übernehmen Verantwortung. Es ist uns wichtig, aufzuklären und zu unterstützen. Wir helfen Ihnen mit unserer Erfahrung und Expertise. Nutzen Sie diese Chance. Schützen Sie sich.

Gerd Chrzanowski
Komplementär der Schwarz Gruppe

EXECUTIVE SUMMARY

Die Cybersecurity-Landschaft hat sich im Jahr 2024 in rasantem Tempo weiterentwickelt und die Bedrohungslage wird zunehmend von geopolitischen Spannungen und technologischen Fortschritten geprägt. Kriege in der Ukraine und im Nahen Osten, Spannungen im Südchinesischen Meer sowie die zunehmende Blockbildung zwischen Europa, den USA, Russland und China beeinflussen den Cyberraum weiterhin erheblich. Cyberangriffe sind heute ein zentraler Bestandteil hybrider Kriegsführung. Besonders besorgniserregend ist der Anstieg staatlich geförderter Angriffe auf Kritische Infrastrukturen sowie koordinierter Desinformationskampagnen zur politischen Einflussnahme.

Gleichzeitig werden die Angriffstechniken technologisch komplexer und immer kreativer. Unternehmen und Institutionen stehen einer Vielzahl paralleler Bedrohungen gegenüber, die ein immer höheres Maß an Resilienz erfordern. Besonders der zunehmende Einsatz von Künstlicher Intelligenz (KI) verändert sowohl offensive als auch defensive Strategien. Während KI-gestützte Bedrohungserkennung die Abwehr verbessert, nutzen Cyberkriminelle die Technologie beispielsweise zur Automatisierung von Phishing-Kampagnen und zur Entwicklung Deepfake-basierter Social-Engineering-Angriffe. Der einfache Zugang zu generativer KI senkt dabei die Einstiegshürden für Angreifer erheblich und verschärft die Bedrohungslage zusätzlich.

Ransomware bleibt weiterhin eine dominierende Gefahr und gewinnt durch mehrstufige Erpressungstaktiken sowie das Ransomware-as-a-Service (RaaS)-Modell weiter an Bedeutung. Zwischen Juli 2023 und Juni 2024 stieg die Zahl der bekannten Ransomware-Angriffe weltweit um 33 Prozent. Besonders deutsche Unternehmen stehen im Fokus: Im ersten Halbjahr 2024 wurden 83 Prozent Opfer einer Ransomware-Attacke – fast doppelt so viele wie im Vorjahreszeitraum. Die steigende Zahl von Angriffen geht dabei mit einer hohen Zahlungsbereitschaft für Lösegeld einher.

Neben Ransomware bleiben Software-Lieferketten im Visier von Cyberkriminellen. Besonders kritisch sind Schwachstellen in Open-Source-Software, die nicht nur als eigenständige Anwendungen, sondern auch als Bestandteil von Software-Lieferketten genutzt werden. Diese Schwachstellen werden gezielt ausgenutzt oder es werden manipulierte Pakete eingeschleust. 2024 wurden weltweit mehr als 6,6 Billionen Open-Source-Downloads verzeichnet. Gleichzeitig stieg die Zahl bösartiger Softwarepakete, die in Open-Source-Ökosysteme eingebracht wurden, um 156 Prozent gegenüber dem Vorjahr. Parallel dazu rücken Cloud-Dienste, Cybersecurity-Lösungen, IoT-Umgebungen und industrielle Steuerungssysteme immer stärker in den Fokus von Angreifern.

Im Jahr 2024 verursachten derartige Cyberangriffe einen Schaden von rund 179 Milliarden Euro. Neben den direkten finanziellen Verlusten durch Cyberangriffe entstehen zusätzliche Kosten unter anderem durch Produktionsausfälle, Datenverluste, Reputationsschäden und langwierige Wiederherstellungsprozesse. Die wachsende Bedrohung zieht sich durch alle Sektoren.

Ein besonders aufsehenerregender Vorfall in 2024, war das fehlerhafte Update des Cybersecurity-Unternehmens CrowdStrike, welches im Juli weltweit rund 8,5 Millionen Computer mit dem Betriebssystem Microsoft Windows lahmlegte. Betroffen waren zahlreiche Unternehmen und Institutionen verschiedenster Branchen. Das daraus resultierende Chaos nutzten Cyberkriminelle gezielt.

Vor diesem Hintergrund sind Unternehmen gezwungen, ihre Cybersecurity-Strategie kontinuierlich zu überdenken. Eine für diesen Report durchgeführte repräsentative Befragung von 1.001 deutschen Unternehmen nimmt deren Cybersecurity-Strategien gezielt in den Blick und zeigt deutliche Unterschiede je nach Unternehmensgröße. Während kleine Unternehmen oft mit begrenzten Ressourcen arbeiten, investieren 42 Prozent der großen Unternehmen eine Million Euro oder mehr in ihre IT-Sicherheit. Die durchschnittliche Investitionsquote in Cybersecurity beträgt acht Prozent des IT-Budgets, bei großen Unternehmen liegt dieser Anteil sogar bei 17 Prozent. Trotz wirtschaftlicher Unsicherheit haben 78 Prozent der Unternehmen ihre IT-Sicherheitsausgaben zuletzt erhöht.

Allerdings bleiben personelle Engpässe eine Herausforderung. 63 Prozent der Unternehmen verfügen über eine eigene IT-Abteilung, doch fast die Hälfte der kleinen Unternehmen hat keine internen IT-Sicherheitskapazitäten. Dieser Mangel an qualifiziertem Personal erschwert nicht nur die Umsetzung präventiver Maßnahmen, sondern auch die schnelle Reaktion auf akute Bedrohungen.

Zusätzlich zur internen Sicherheitsstrategie stellt die Umsetzung der EU-NIS-2-Richtlinie viele Unternehmen vor Herausforderungen. Während große Unternehmen gut vorbereitet sind, fehlt kleineren Betrieben oft der vollständige Überblick über die Anforderungen. Zwei Drittel der Unternehmen halten sich für gut oder sehr gut auf Cyberangriffe vorbereitet, aber 60 Prozent sehen die staatliche Unterstützung als unzureichend an. Auch wenn NIS-2-Umsetzungs- und KRITIS-Dachgesetz gescheitert sind und damit Rechtsunsicherheit herrscht, können Organisationen sich an den Kernelementen der EU-NIS-2-Richtlinie bei ihren Maßnahmen orientieren.

Während viele Unternehmen ihre internen Strukturen anpassen, wird die Sicherheit in der Lieferkette weiterhin unterschätzt. Mehr als die Hälfte der Unternehmen erkennt keine wesentlichen Cyberrisiken durch ihre Lieferanten oder externen Partner. Während nur 16 Prozent der kleinen Unternehmen verbindliche Cybersecurity-Anforderungen für alle Lieferanten definiert haben, liegt dieser Anteil bei großen Unternehmen bei 40 Prozent. Insgesamt prüfen 49 Prozent der Unternehmen ihre Lieferanten regelmäßig oder gelegentlich auf die Einhaltung von Sicherheitsstandards. Besonders stark regulierte Branchen wie das Finanz- und Versicherungswesen sowie die Energieversorgung setzen überdurchschnittlich häufig auf strukturierte Lieferantenaudits.

Doch schon der Ausfall eines einzigen Softwaredienstleisters kann gravierende Auswirkungen haben: Beim bereits erwähnten Vorfall mit CrowdStrike kam es zu massiven Einschränkungen im weltweiten Flugverkehr. Solche Ereignisse unterstreichen die Risiken, die mit einer starken Abhängigkeit von einzelnen IT-Anbietern verbunden sind. Während große Unternehmen verstärkt auf Multi-Vendor-Strategien setzen, nutzen kleine Unternehmen fast ausschließlich Komplettlösungen eines einzelnen Anbieters. Nur sechs Prozent der kleinen Unternehmen betrachten sie als Risiko, während der Anteil bei großen Unternehmen bei 33 Prozent liegt. Insgesamt sind 93 Prozent der kleinen Unternehmen auf einen einzigen Anbieter angewiesen, während 88 Prozent der großen Unternehmen eine Multi-Vendor-Strategie verfolgen. Mehr als die Hälfte der befragten Unternehmen setzt auf offene Standards oder evaluiert regelmäßig alternative Anbieter, um schädliche Vendor-Lock-ins zu vermeiden.

Gleichzeitig ist der Markt für Cybersecurity-Lösungen in den letzten 25 Jahren stark gewachsen. Weltweit gibt es über 3.500 Anbieter, doch viele Unternehmen haben Schwierigkeiten, die passenden Lösungen zu identifizieren und zu integrieren. Im Durchschnitt nutzen Unternehmen bis zu 83 verschiedene Sicherheitsprodukte von 29 Anbietern, in einigen Fällen sogar 336 Produkte von 57 Anbietern. Doch diese Vielfalt bringt nicht nur Vorteile: 64 Prozent der IT-Sicherheitsteams berichten, dass ihre eingesetzten Produkte nicht optimal interoperabel sind, was Ineffizienz und Sicherheitslücken zur Folge hat.

Die Investitionen in Cybersecurity steigen weiter. In Deutschland beliefen sich die Ausgaben für Cybersecurity-Lösungen im Jahr 2024 auf 5,8 Milliarden Euro, während der globale Markt bis 2029 auf 247 bis 292 Milliarden US-Dollar anwachsen wird. Trotz dieser steigenden Investitionen nehmen erfolgreiche Cyberangriffe weiter zu. Dies liegt unter anderem daran, dass chaotisch gewachsene Sicherheitsinfrastrukturen oft mehr Schwachstellen schaffen, als sie schließen. Kein einzelnes Produkt kann alle Anforderungen an Automatisierung, Preisgestaltung oder nahtlose Integration erfüllen. Unternehmen stehen vor der Herausforderung, zwischen Best-of-Breed-Ansätzen mit spezialisierten Einzellösungen und integrierten Plattformen zu wählen. Letztere reduzieren zwar den Verwaltungsaufwand, erhöhen aber das Risiko eines Vendor-Lock-ins.

Organisationen investieren häufig mehr als nötig, während essenzielle Funktionen der Produkte ungenutzt bleiben. Die Preisgestaltung ist oft intransparent: So sind Anti-Virus oder EDR-Lösungen von ein bis 30 Euro pro Endgerät vergleichsweise erschwinglich, insbesondere

bei Mengenrabatten. Auch Firewalls gibt es bereits ab 100 Euro, sie können jedoch auch über eine Million Euro kosten.

Während Unternehmen um die richtige Sicherheitsstrategie ringen, geraten globale Infrastrukturen zunehmend ins Visier von hybrider Kriegsführung. Besonders Unterseekabel und Satelliten, auf die die meisten Kommunikations-, Energie- und Transportsysteme zwingend angewiesen sind, sind potenzielle Ziele. Seekabel, über die mehr als 95 Prozent des weltweiten Internetverkehrs abgewickelt werden, stellen ein besonders kritisches Angriffsziel dar. Die Sabotage solcher Systeme kann gravierende wirtschaftliche und politische Konsequenzen haben, wie die Vorfälle in der Ostsee zeigten, bei denen mutmaßlich russische Akteure Unterseekabel beschädigten. Ein kürzlich erfolgter GPS-Spoofing-Angriff auf einen Passagierflug demonstrierte eindrücklich, dass digitale Bedrohungen unmittelbare Risiken für die Sicherheit im realen Raum darstellen können.

Doch nicht nur Unternehmen, Behörden oder Parteien sind betroffen – auch Einzelpersonen geraten verstärkt ins Visier, was ein höheres Bewusstsein für den Schutz digitaler Identitäten und Handlungen im Cyber- und Informationsraum erforderlich macht. Besonders alarmierend ist der Anstieg von Sextortion, einer Form digitaler Erpressung, die psychologische Manipulation mit modernen Technologien kombiniert. Sextortion betrifft Menschen aller Altersgruppen und sozialen Hintergründe weltweit, doch Jugendliche sind besonders gefährdet. Täter nutzen gezielt soziale Netzwerke, Online-Spiele und Dating-Plattformen, um an intime Inhalte zu erlangen.

Im Jahr 2023 wurden bereits rund 27.000 Fälle von Sextortion gemeldet, mit mindestens 12.600 betroffenen Opfern und 20 dokumentierten Suiziden. Nur ein Fünftel der Opfer erstattet Anzeige, während die Dunkelziffer hoch bleibt. Auch fehlt es an der Erfassung in vielen Polizeistatistiken.

Die technologische Entwicklung erleichtert diese Form der Kriminalität zusätzlich. KI Deepfake-Technologie ermöglicht es, täuschend echt gefälschte Bilder und Videos als Druckmittel einzusetzen. Bereits elf Prozent der in Sextortion-Fällen verwendeten Inhalte sind Fälschungen. Zudem nutzen Täter verschlüsselte Kommunikationsplattformen und schwer rückverfolgbare Kryptowährungen, um der Strafverfolgung zu entgehen.

Besonders die Verletzlichsten unserer Gesellschaft müssen durch gezielte Prävention, technologische Innovationen und entschlossenes gesellschaftliches Handeln geschützt werden. Nur eine gemeinsame Anstrengung von Politik, Bildungseinrichtungen, Technologieunternehmen und Strafverfolgungsbehörden kann diese Angriffe wirksam verhindern.

INHALT

KAPITEL 1

CYBERSECURITY AUF EINEN BLICK

Top Bedrohungen in 2024

Fehlkonfigurierte Systeme
38 %

31 %
Schwachstellen in intern entwickelten Apps

Zero-Day Schwachstellen
30 %

29 %
Bekannte Schwachstellen in der Software

Laterale Bewegung der Angreifer
28 %

Cybersecurity Prognose 2025:
Größter Einfluss auf die Cybersecurity

KI / MASCHINELLES LERNEN

66 %

Konvergenz von IT- und OT-Sicherheit
13 %

Cloud-Technologien
11 %

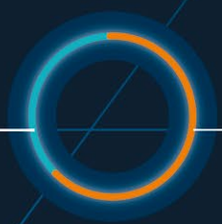
Quantum Technologie (Computing, Verschlüsselung)
4 %

Dezentralisierte Technologien (z.B. Blockchain)
3 %

Satelliten-Technik (Kommunikation, GPS, Internet)
2 %

Sonstiges
2 %

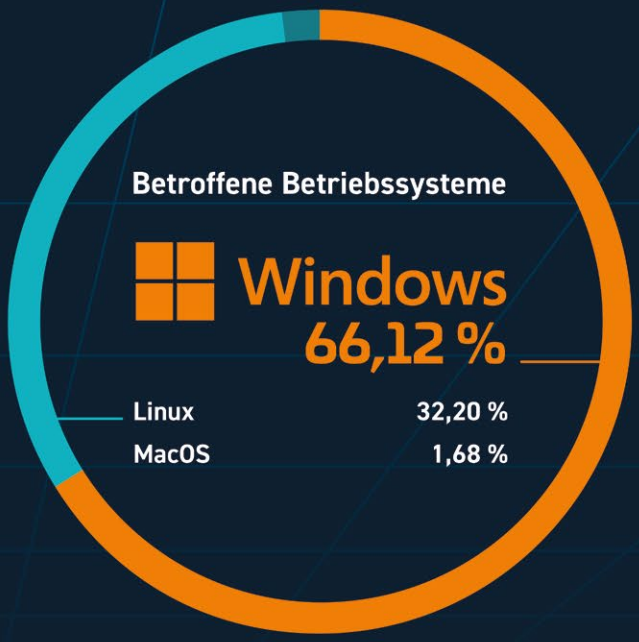
Wurde in Ihrem Unternehmen ein Prozess integriert, um die Sicherheit von KI-gestützter Software zu evaluieren, bevor diese verwendet wird?

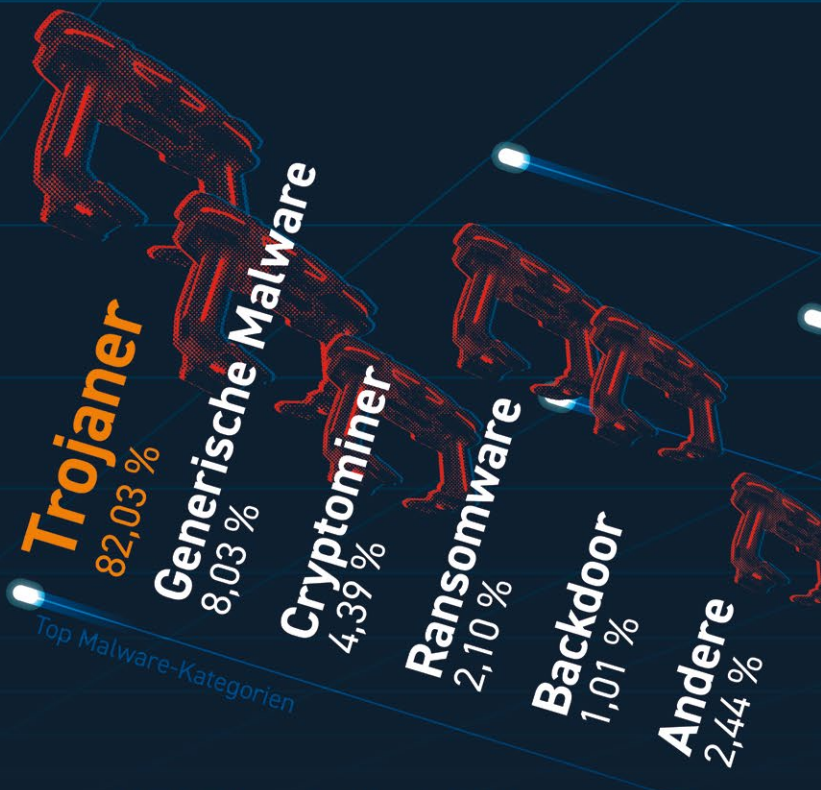


Ja: 37 %

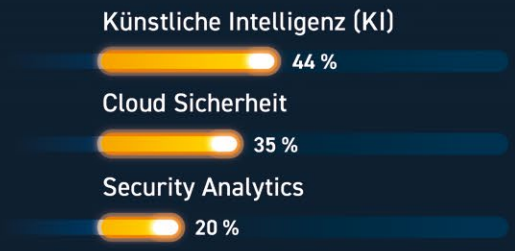
Nein: 63 %

Betroffene Betriebssysteme

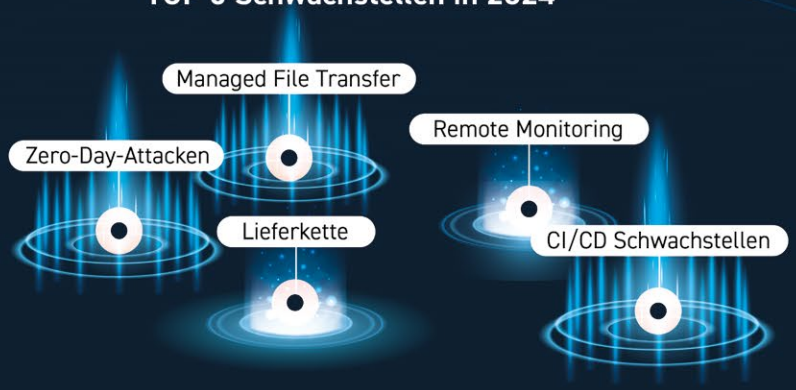




Sicherheits-Initiativen in 2024



TOP 5 Schwachstellen in 2024



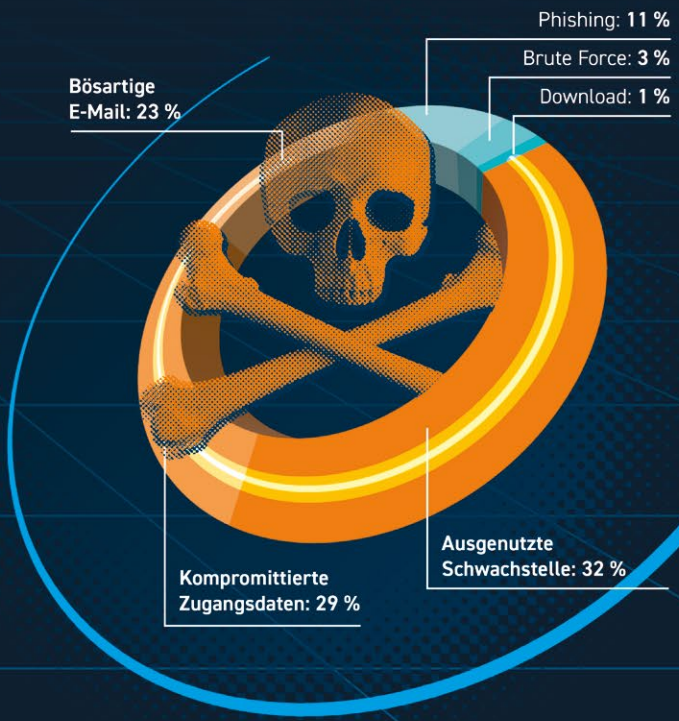
Durchschnittliche weltweite Gesamtkosten einer Datenschutzverletzung

Durchschnittliches Lösegeld pro Fall

300.000 USD
für verschlüsselte Daten

850.000 USD
für exfiltrierte Daten

Hauptursachen von Ransomware Attacken in Unternehmen weltweit



Quellen: [20], [46], [74], [226], [144], [149], [267], eigene Darstellung

1 CYBERSECURITY AUF EINEN BLICK

1.1 GEOPOLITISCHE SITUATION WELTWEIT

Die komplexe geopolitische Landschaft ist von zunehmenden Spannungen und Konflikten geprägt. Die Kriege in der Ukraine und im Nahen Osten, Spannungen im Südchinesischen Meer und in der Taiwanstraße sowie die humanitäre Krise im Sudan sorgen für globale Unsicherheit. Auch die verstärkte Blockbildung zwischen Europa, den USA, Russland und China trägt dazu bei. Diese Entwicklungen beeinflussen auch den Cyberraum, der zu einem wichtigen Kriegsschauplatz geworden ist. Digitale Sabotage, Spionage und Desinformation sind nun wesentliche Elemente der Kriegsführung [170].

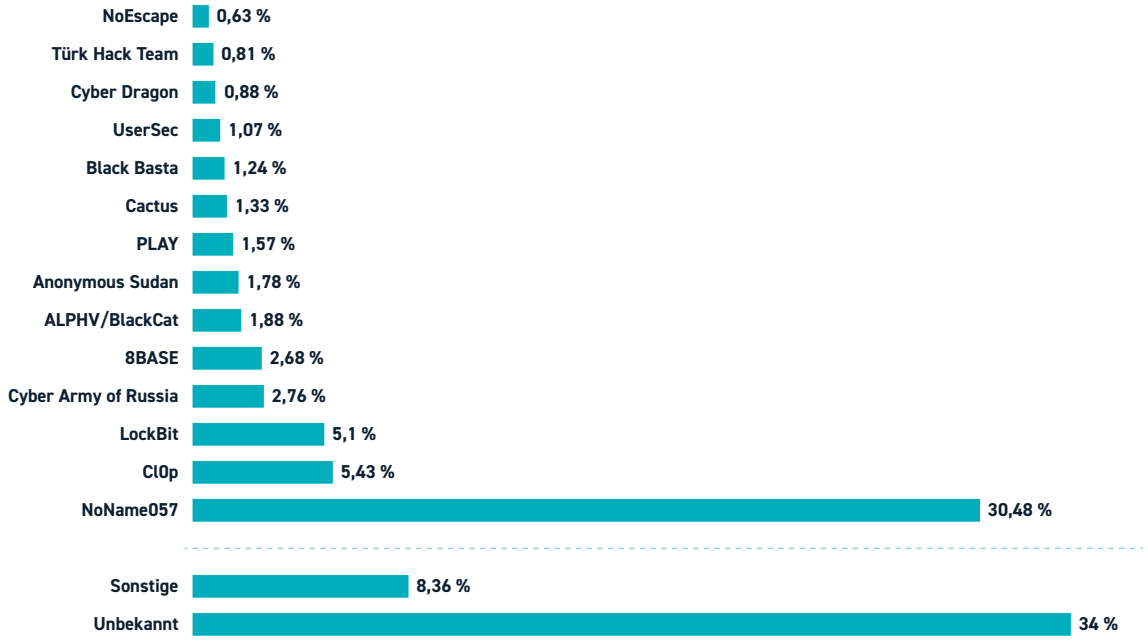
In diesem Kontext nutzen staatliche Akteure sowie nichtstaatliche Gruppen, wie Milizen, Terrororganisationen und Aufständische Cyberangriffe zunehmend als Instrument der Machtpolitik, um strategische Ziele zu verfolgen und ihre Gegner zu destabilisieren. Die zunehmende Raffinesse und Häufigkeit von Cyberangriffen stellen erhebliche Risiken und Bedrohungen für die Zivilbevölkerung, Unternehmen, Institutionen und Regierungen dar. Digitale Kriegsführung umfasst dabei weitaus mehr als nur gezielte Angriffe auf digitale militärische Ziele. Immer häufiger werden Infrastrukturen der Daseinsvorsorge und Unternehmen durch Aggressoren angegriffen. Organisationen sind dabei nicht nur direkten Angriffen ausgesetzt, sondern riskieren auch Kollateralschäden zu erleiden [6]. Neben zerstörerischen Angriffen sind staatlich orchestrierte Desinformationskampagnen und eine mehr oder weniger öffentliche Einflussnahme auf die Berichterstattung und Information zu beobachten. Auch aus Sicht der Unternehmen gehören einzeln betrachtet Cybersecurity und geopolitische Konflikte zu den herausforderndsten Themen der heutigen Zeit [6]. Insbesondere die Kombination beider Themen stellt für Unternehmen ein erhebliches Risiko dar [237] und erfordert von den Verantwortlichen ein größeres Verständnis geopolitischer Dynamiken für ein effektives langfristiges Risikomanagement [6].

Geopolitische Spannungen zwischen Großmächten haben sich zu einem neuen Bereich der Kriegsführung ausgeweitet. Cyberangriffe dienen als Spionagewerkzeug oder auch als Mittel, physische Systeme und Kritische Infrastrukturen aller Bereiche zu schädigen [245]. Man versucht im Sinne von Nadelstichen die Grenzen des Hinnehmbaren der westlichen Demokratien auszutesten. Man spricht auch von „Grey Zone"-Angriffen.

Auch der Aufstieg Chinas macht die Cyber-Bedrohungslandschaft komplizierter. Der wachsende Einfluss des Reichs der Mitte stellt zunehmend die Dominanz von Cyber-Mächten wie den Vereinigten Staaten in Frage [2], [82]. Peking hat damit begonnen, von der Cyberspionage aus wirtschaftlichen Interessen zu einem expliziten Streben nach globaler technologischer Überlegenheit und einer (Neu-)Gestaltung des Internets überzugehen [2]. Im vergangenen Jahr 2024 entwickelte sich China zur wichtigsten Ausgangsbasis für Angriffe auf die deutsche Wirtschaft. 45 Prozent der im Rahmen der Bitkom-Studie befragten betroffenen Unternehmen konnten mindestens einen Angriff in das Land zurückverfolgen. 2023 stellte Russland noch den größten Angreifer dar [237]. Eine Schlüsselkomponente der chinesischen Cyberstrategie ist das Konzept der militärisch-zivilen Fusion, das die Zusammenarbeit zwischen dem Privatsektor und dem Militär fördert und die Ressourcen integriert. Zusätzlich setzt die Regierung staatlich geförderte Hackergruppen ein, um weitreichende Cyberspionage- und Sabotagekampagnen durchzuführen [197].

Die NATO und ihre Bündnispartner sind auf eine starke und widerstandsfähige Cyberabwehr angewiesen, um die drei Kernaufgaben des Bündnisses – Abschreckung und Verteidigung, Krisenprävention und -bewältigung sowie kooperative Sicherheit – zu erfüllen [209]. Einmal im Jahr verpflichten sich dafür die Mitgliedstaaten und die beteiligten Organe, Einrichtungen und Agenturen der EU (European Union Institutions, Bodies and Agencies, EUIBA), ihre Reaktion auf Szenarien zu testen, die auf der Grundlage der regelmäßigen EU-Risikobewertung entwickelt wurden. Das Ganze wird im Rahmen einer jährlichen speziellen Übung der Cyberdiplomatie-Toolbox durchgeführt [249].

Doch nicht nur auf Organisationsebene oder in einer akuten Kriegssituation spielt Cyberkriminalität eine Rolle. Auch die Zivilbevölkerung kann Opfer entsprechender



Quelle: [96]

Abbildung 1: Die aktivsten Angreifer (Juli 2023 – Juni 2024)

Angriffe werden. So warnte im November 2024 etwa das Bundesamt für Verfassungsschutz vor möglichen Versuchen der Einflussnahme anderer Staaten auf die anstehende Bundestagswahl. Dabei geht es um „Aktionen der Desinformation und Diskreditierung, Cyberangriffe sowie Spionage und Sabotage". Unter Vortäuschung falscher Tatsachen könnte Einfluss auf die Entscheidungs- und Funktionsträger genommen, aber auch in den freien Meinungs- und Willensbildungsprozess eingegriffen werden. Über Diebstahl, Manipulation und der Veröffentlichung von (Falsch-)Informationen kann indirekt auf die Wahlen eingewirkt werden. In diesem Zusammenhang warnten die Verfassungsschützer vor allem vor russischen Angreifergruppierungen, welche in der Vergangenheit im Wahlumfeld besonders aktiv waren (Übersicht der aktivsten Angreifer siehe Abbildung 1) [285].

1.2 ALLGEMEINES CYBERSECURITY-BEDROHUNGSBILD

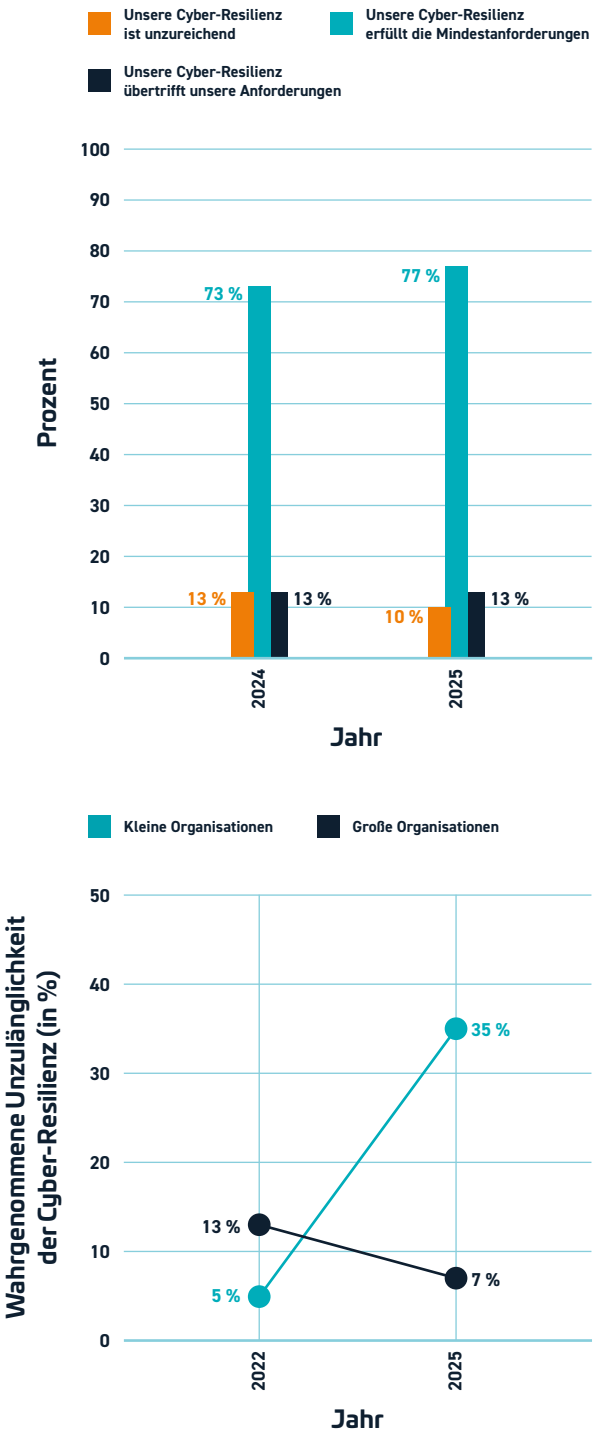
Es zeigt sich, dass auch im Jahr 2024 die Cyberlandschaft von einer heterogenen Bedrohungslage geprägt war. Sowohl das geopolitische Umfeld als auch Neuerungen im Technologiebereich (und insbesondere die Kombination beider) stellen Nutzer und Entwickler von Softwaresystemen vor Herausforderungen. Insbesondere der Einsatz von Künstlicher Intelligenz (KI), sowohl auf Angreiferseite als auch auf der Ebene der Abwehr, prägte 2024 die Bedrohungslage im Bereich der Cybersecurity [19], [96]. Künstliche Intelligenz, besonders große Sprachmodelle (LLMs), verringern zunehmend die Barrieren für den Einstieg und steigern somit sowohl die Reichweite als auch die Geschwindigkeit schadhafter Aktivitäten, wie autonomer Generierung und Mutation von Malware, Social-Engineering-Angriffen (z. B. Pretexting und Deepfakes) und die Datenanalyse bei Angriffen (z. B. Big Data und automatisierte Analysen von Massendaten). Dies führt zu einer Zunahme der Kompetenz der Angreifer und qualitativ besseren Attacken [6]. Darüber hinaus kann KI auch im Rahmen der Abwehr von Cyberangriffen zur automatischen Identifizierung von Sicherheitslücken eingesetzt werden. KI-basierte Systeme helfen, Hinweise auf eine Kompromittierung oder Malware-Infektionen in geschützten Systemen zu entdecken, indem sie das Verhalten von Nutzern überwachen und auf ungewöhnliche Muster prüfen [19], [47].

Angriffe auf Webserver, Online-Services oder ganze Netzwerke, wie Distributed Denial of Service (DDoS), bleiben weit verbreitet. Ziel dieser Angriffe ist es, die Verfügbarkeit der betroffenen Ressource zu stören oder ganz zu verhindern, indem die Serverressourcen überlastet und legitime Benutzeranfragen blockiert werden. Dabei haben insbesondere politisch motivierte Attacken durch Einzelpersonen oder kleine Gruppen [96] und staatlich gelenkte Akteure im Zuge geopolitischer Spannungen zugenommen. In Anbetracht der aktuellen geopolitischen Lage stehen öffentliche Verwaltungen, Transportlogistik und Finanzinstitutionen besonders im Fokus der geopolitisch motivierten Angreifer [96]. Die zunehmende technische Versiertheit und steigende Kosteneffizienz verringern zudem die Barrieren zur Nutzung von DDoS-Tools [96]. So können beispielsweise DDoS-for-Hire-Dienste es auch technisch weniger ver-

sierten Personen ermöglichen, groß angelegte Distributed-Denial-of-Service-Angriffe durchzuführen. Anbieter können diese Angriffe entweder selbst ausführen oder ihren Kunden die entsprechenden Werkzeuge zur Verfügung stellen. Die Kombination aus DDoS-for-Hire-Diensten und der einfachen Erstellung von Botnetzen aufgrund der Vielzahl unsicherer Geräte schafft ideale Bedingungen für die Durchführung disruptiver Angriffe in großem Umfang.

Ransomware bleibt im Bereich der Cybersecurity eine der größten Herausforderungen [6]. Mehrstufige Erpressungstaktiken, bei denen neben der Datenverschlüsselung auch die Veröffentlichung gestohlener Informationen angedroht wird, nehmen in Deutschland und Europa weiter zu [96]. Während die durchschnittlichen Lösegeldforderungen steigen, geht die Erfolgsquote bei der Zahlungsdurchsetzung jedoch leicht zurück [47]. Im internationalen Vergleich melden Organisationen, die Lösegeld gezahlt haben, eine durchschnittliche Zahlung von ungefähr 2 Millionen US-Dollar, gegenüber 400.000 US-Dollar im Jahr 2023. Deutsche Unternehmen griffen sogar noch tiefer in die Tasche, hier lag die mittlere Lösegeldzahlung bei 5,5 Millionen US-Dollar [242]. Staatlich unterstützte Advanced Persistent Threat (APT)-Gruppen, insbesondere aus Russland und China, zielen zunehmend auf Kritische Infrastrukturen in Europa ab. Diese Gruppen nutzen Zero-Day-Schwachstellen und spezialisierte Malware, um Cyberspionage und Sabotage zu betreiben [30], [46]. Organisationen mit geringer Sicherheitsreife stehen dabei besonders im Fokus (Einschätzung der eigenen Cyber-Resilienz durch Unternehmen siehe Abbildung 2) [166].

Die Nutzung von Social Engineering als Angriffsvektor, welche Manipulationstechniken auch einschließlich persönlicher Interaktionen umfasst, hat im Vergleich zum Vorjahr um vier Prozentpunkte zugenommen [145]. Phishing stellt dabei eine spezifische Art des Social Engineering dar, bei dem Angreifer versuchen, vertrauliche Informationen, wie Passwörter, Bankdaten oder Kreditkarteninformationen, durch betrügerische E-Mails, Websites oder Nachrichten zu erlangen. Laut dem BSI werden Phishing-E-Mails häufig dazu verwendet, Nutzer zu täuschen und schädliche Links oder Anhänge zu



Quelle: [6]

Abbildung 2: Einschätzung der eigenen Cyber-Resilienz durch Unternehmen

verbreiten, die potenziell zur Infiltration von Systemen mit Schadsoftware führen können [46]. Gleichzeitig sinken auch die Eintrittsbarrieren für Social Engineering aufgrund der durch LLMs leichten Skalierbarkeit, der einfacheren Überwindung von Sprachbarrieren und der Möglichkeit, Angriffe gezielt zu personalisieren [6], sowie des mangelnden Sicherheitsbewusstseins bei vielen Nutzern. Das spiegelt auch die Befragung des BSI im Rahmen des Cybersicherheitsmonitors 2024 wider. Hier zeigte sich, dass im Vergleich zum Vorjahr die Nutzung von Schutzmaßnahmen, wie Antivirenprogramme oder sichere Passwörter, rückläufig ist. Als Gründe dafür gaben die Befragten ein hohes Sicherheitsgefühl sowie eine zu hohe Komplexität der Schutzmaßnahmen an [45]. Aufgrund der hohen Verfügbarkeit von Informationen können Angreifer ihre Inhalte auch zunehmend besser in einen für das Zielobjekt relevanten Kontext setzen, einen konkreten Nutzen vortäuschen und damit ihre Erfolgsquote deutlich erhöhen.

Auch Angriffe auf Lieferketten entwickeln sich zu einer der kritischsten Bedrohungen [30]. 26 Prozent der befragten Führungskräfte in Deutschland wissen oder haben den Verdacht, dass ihre Zulieferer innerhalb der letzten zwölf Monate Opfer von Cyberangriffen waren. Die zunehmende Komplexität und mangelnde Kontrolle über Lieferketten hat sich für Unternehmen zur größten Hürde für Cyberresilienz entwickelt – wobei größere Unternehmen diese Gefahr stärker wahrnehmen als kleinere Organisationen [6]. Der Blick der Unternehmen richtet sich zunehmend auf eine ganzheitliche Betrachtung der Lieferkette und einer damit verbundenen Implementierung von Managementsystemen zur Handhabung der Risiken von Cyberangriffen. Ein entsprechendes Lieferantenrisikomanagement entlang der gesamten Lieferkette kann dieses Risiko reduzieren [30]. Zudem bietet sich vor allem hier die Zero Trust Security an, bei dem keinem internen oder externen Nutzer standardmäßig vertraut wird, dies kann die Sicherheit erhöhen und zu einer Prävention von möglichen Angriffen führen [303].

Während ein Cyberangriff auf die physische Lieferkette, Produktions-, Zahlungs- oder Logistikprozesse gefährdet, zielt eine Attacke auf die Software-Lieferkette auf digitale Produkte und deren Integrität. Besonders Open-Source-Projekte geraten dabei verstärkt ins Visier von Angreifern, die schädliche Codefragmente einfügen, um Angriffe auf die Software-Lieferkette durchzuführen. Im März 2024 wurde beispielsweise in das Open-Source-Projekt XZ Utils, eine Sammlung von Produkten und Bibliotheken zur Datenkompression, ein Backdoor-Code eingefügt. Solche Vorfälle verdeutlichen die Risiken, die mit unzureichend gesicherten Open-Source-Projekten verbunden sind [96].

Das allgemeine Bedrohungsbild zeigt, dass sich Angreifer immer weiter spezialisieren und dabei zunehmend auf moderne Technologien wie KI setzen. Die Kombination aus geopolitischen Spannungen, welche auch in Deutschland zu einer Zunahme von Cyber-Wirtschaftsspionage und -Sabotage führen [319], technologischen Fortschritten, wie (KI-generierte) Deepfakes zur Verbreitung von Falschinformationen und einer wachsenden Vernetzung stellt Organisationen vor neue Herausforderungen. Umso wichtiger ist eine ganzheitliche und proaktive Sicherheitsstrategie, die sowohl technologische als auch organisatorische Maßnahmen berücksichtigt, um die Resilienz nachhaltig zu stärken.

1.3 ÜBERBLICK: CYBERSECURITY VORFÄLLE IN 2024

Das Jahr 2024 hat erneut eindrucksvoll unter Beweis gestellt, wie verletzlich auch als robust eingeschätzte digitale Infrastrukturen sein können. Nicht nur die Nutzer und Anwender von Software und Netzwerken sehen sich den Risiken vermehrt ausgesetzt. Auch Anbieter von IT-Sicherheitslösungen, beispielsweise Ivanti [52] oder Fortinet [161], rücken in den Fokus der Kriminellen. Eine Kaskade von hochkarätigen Cyberangriffen hat Unternehmen, Behörden und Institutionen gleichermaßen getroffen und die Schwachstellen in der globalen digitalen Landschaft offengelegt.

Besonders bemerkenswert war wie im Vorjahr die Breite der angegriffenen Sektoren. Vom Technologiekonzern über staatliche und private Institutionen bis hin zu

politischen Parteien reichte das Spektrum der Opfer. So wurde beispielsweise im Februar 2024 bekannt, dass der Technologiekonzern Microsoft von einem massiven Cyberangriff auf seine Cloud-Computing-Plattform Azure getroffen wurde, der mittels einer Phishing-Kampagne zur Kompromittierung zahlreicher Konten von Führungskräften führte. Dies stellt den ersten Vorfall dieser Art in der Geschichte von Microsoft dar. Betroffen waren auch staatliche Institutionen, beispielsweise die Stadtverwaltung Aschaffenburg, bei der im November 2024 auffällige Zugriffe auf Benutzerkonten von Mitarbeitenden dazu führten, dass alle IT-Systeme als Vorsichtsmaßnahme vom Netz genommen wurden [268] oder die Landesregierung in Mecklenburg-Vorpommern im Mai 2024, bei der mittels einer DDoS-Attacke der Zugriff auf Internetseiten eingeschränkt wurde [208].

Betroffen waren im Jahr 2024 auch gemeinwohlorientierte Institutionen, darunter das größte gemeinnützige Gesundheitssystem in den USA, Ascension, im Mai 2024 oder der überregionale Krankenhausbetreiber Johannesstift Diakonie im Oktober 2024 [337], die sich mit Angriffen konfrontiert sahen, die die medizinischen Aufzeichnungen von Tausenden von Patienten gefährdeten.

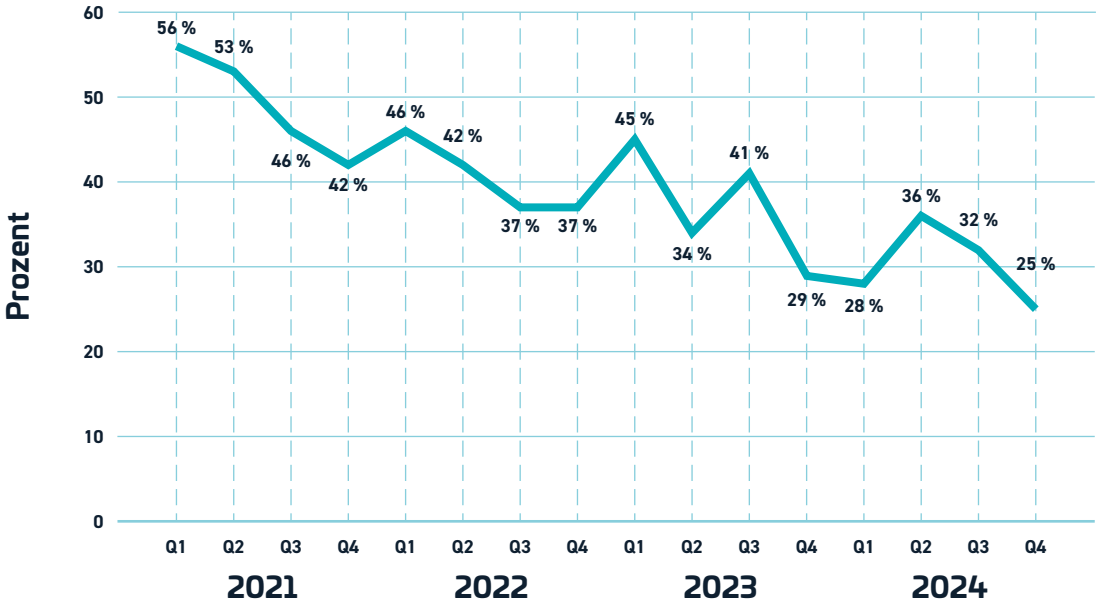
Auch blieben politische Parteien nicht verschont: Die CDU wurde im Mai 2024, unmittelbar vor der Europawahl, Opfer eines Cyberangriffs, der interne Kommunikationsdaten öffentlich machte. Unmittelbar vor den Landtagswahlen in Brandenburg im September 2024 wurde von der AfD Brandenburg ein Hackerangriff veröffentlicht [248]. Ein weiteres Beispiel ist ein DDoS-Angriff auf die FDP-Landeskampagnenseite im August 2024 [54]. Bereits im Jahr 2023 wurden E-Mail-Konten der SPD attackiert (die Aufklärung fand erst 2024 statt). Im September 2024 meldeten zudem die Österreichische Volkspartei (ÖVP) und die Sozialdemokratische Partei Österreichs (SPÖ), Opfer von DDoS-Attacken gewesen zu sein [216]. Auch international lassen sich weitere Beispiele finden, die die Gefahren von Cyberangriffen auf Parteien als essenzielle Akteure in den demokratischen Prozessen zeigen. So wurde beispielsweise die japanische Liberaldemokratische Partei (LDP) Mitte Oktober Opfer eines Cyberangriffs, der zeitgleich mit dem Start des dortigen Wahlkampfs stattfand [246]. Der Angriff wurde einer pro-russischen Hacker-Gruppe zugeschrieben, die im gleichen Jahr mit DDoS-Angriffen mehrere japanische Institutionen, darunter auch lokale Regierungswebsites, lahmlegte [189], [204].

Neben politischen Institutionen, gerieten auch Politiker und Regierungsbeamte in den Fokus von Cyberangriffen: Anfang Dezember 2024 meldeten US-Sicherheitsbehörden, dass es vermutlich chinesischen Hacker gelungen sei, in die Systeme von mindestens acht US-Telekommunikationsanbietern einzudringen. Berichten zufolge wurden im Zuge des Angriffs umfangreiche Metadaten von Amerikanern entwendet. Ins Visier der Angreifer gerieten prominente politische, behördliche und geheimdienstliche Persönlichkeiten. Es konnte Zugriff auf Geodaten, Telefonprotokolle sowie Mitschnitte privater Gespräche zwischen US-Politikern, Diplomaten und Sicherheitsbeamten genommen werden [313].

Bei Cyberattacken auf Parteien und Politikern geht es neben finanziellen Interessen häufig auch darum, gezielt die Legitimität von Wahlen und Institutionen in Zweifel zu ziehen und das Vertrauen in den demokratischen Prozess zu schwächen [46], [56]. Ebenso können auch legitime digitale Werkzeuge eingesetzt werden, um in demokratische Prozesse einzugreifen. In sozialen Medien, wie TikTok, Instagram oder YouTube, ist ein Raum für Desinformation und Wahlmanipulation entstanden. Durch den Einsatz von Bots, bezahlten Influencern und gezielter Algorithmus-Manipulation, beeinflussen teils anonyme Akteure Wahlergebnisse und fügen demokratischen Systemen, Staaten und der Bevölkerungen erheblichen Schaden zu [282], [336].

Ransomware – Die Erpressungskunst im digitalen Zeitalter

Ransomware-Angriffe blieben trotz der erfolgreichen Zerschlagung bekannter Ransomware-Gruppen, wie LockBit im Februar 2024 [257] und BlackCat im Dezember 2023 [31], die dominierende Bedrohung. Zwischen Juli 2023 und Juni 2024 stiegen die bekannten Ransomware-Angriffe weltweit im Jahresvergleich um 33 Pro-



Quelle: [76]

Abbildung 3: Anteil an Unternehmen die nach einem Ransomware-Angriff Lösegeld gezahlt haben

zent. Am stärksten nahmen die Angriffe im Vergleich zum Vorjahreszeitraum in den USA (+63 Prozent) und im Vereinigten Königreich (+67 Prozent) zu [188]. Eine britische Cybersecurity-Webseite berichtete Anfang Januar 2025, dass im Jahr 2024 Ransomware-Gruppen die Verantwortung für 5.461 erfolgreiche Ransomware-Angriffe auf Organisationen weltweit übernommen haben. Bei den 1.204 von den betroffenen Organisationen bestätigten Angriffen ergaben die Daten, dass 195,4 Millionen Datensätze kompromittiert wurden. Die Angaben für 2024 sind zwar niedriger als die für das Gesamtjahr 2023 (1.474 bestätigte Angriffe, die 261,5 Millionen Datensätze betrafen), da jedoch viele Angriffe im Rahmen der Aufklärung und Strafverfolgung erst mit zeitlichen Verzug nach dem Angriff gemeldet werden, ist mit einem Anstieg der Zahlen zu rechnen [195]. Die Bedrohungslage für deutsche Unternehmen soll sich dabei auch erheblich verschärft haben. Im ersten Halbjahr 2024 wurden 83 Prozent der deutschen Unternehmen Opfer einer Ransomware-Attacke – fast eine Verdopplung gegenüber dem Vorjahreszeitraum, in dem 48 Prozent betroffen waren. Damit nimmt Deutschland nicht nur bei der Anzahl der Attacken, sondern auch bei der Bereitschaft, Lösegeld zu zahlen, einen internationalen Spitzenplatz ein [125]. Ein weiterer alarmierender Trend zeigt, dass in den ersten sechs Monaten 2024, Cyberkriminelle weltweit Lösegeld in Höhe von 459,8 Millionen US-Dollar erpressten (siehe Abbildung 3) [266].

Ein besonderer Vorfall ereignete sich am 8. Mai 2024, als Ascension, das größte gemeinnützige Gesundheitssystem in den USA, ungewöhnliche Aktivitäten in ihren Netzwerken entdeckte, die auf einen Ransomware-Angriff der Gruppe Black Basta hinwiesen [181]. Der Angriff betraf fast 150 Krankenhäuser in über zehn US-Bundesstaaten und führte dazu, dass medizinisches Personal keinen Zugriff mehr auf wichtige Systeme und Patientendaten hatte. Dieser Vorfall führte zu verlorenen Laborergebnissen, Fehlern bei der Medikamentendosierung und der Unfähigkeit, Notfälle über einen Monat lang aufzunehmen [181]. Am 14. Juni 2024 konnte Ascension bekannt geben, dass der Zugriff auf elektronische Gesundheitsakten wiederhergestellt sei, jedoch noch die Patientendaten aktualisiert werden müssten. Der Ransomware-Angriff konnte der Organisation zufolge gelingen, weil eine Person, die in einer Einrichtung von Ascension arbeitet, versehentlich eine Datei mit Malware herunterlud, die sie für legitim hielt [314].

Am 5. Oktober 2024 bestätigte der japanische Elektronikkonzern CASIO, dass ein Ransomware-Angriff zu einem Datenleck führte. Hacker erlangten dabei persönliche Informationen sowie vertrauliche Dateien des Unternehmens und seiner verbundenen Unternehmen [165]. Die Ransomware-Gruppe Underground behauptet, über 200 GB an Daten von über 128.000 Verbrauchern sowie Daten von Geschäftspartnern erbeutet zu haben, darunter Rechtsdokumente, Gehaltsinformationen und Finanzdokumente. CASIO untersucht den Vorfall weiterhin und hat bisher festgestellt, dass auch Informationen von Mitarbeitern, Geschäftspartnern und Kunden betroffen sind. CASIO bestätigte, dass eine Fehlkonfiguration in der Entwicklungsumgebung des ClassPad.net zur Sicherheitslücke führte. Die gestohlenen Daten umfassen

Namen, E-Mail-Adressen, Wohnort, Kaufinformationen und Nutzungsdaten. CASIO betonte, dass keine Kreditkarteninformationen betroffen waren und versprach, betroffene Kunden zu kontaktieren und zukünftige Sicherheitsmaßnahmen zu verstärken [69].

Staatlich gesponserte Angriffe und politische Cyberkriege

Wie auch im Schwarz Cybersecurity Report 2024 (SCSR24) verdeutlichen die beobachteten Aktivitäten im Jahr 2024, dass geopolitische und zwischenstaatliche Konflikte häufig von einer Vielzahl an Phänomenen im Cyberraum begleitet werden. Dazu zählen Desinformation, Spionage, Sabotage und politisch, sozial oder ideologisch motivierte Cyberangriffe [46]. Laut BKA haben sich geopolitische Konflikte in den letzten zwei Jahren zunehmend in den digitalen Raum verlagert. Die Zunahme globaler Auseinandersetzungen hat zu einem signifikanten Anstieg von Hackerangriffen geführt. Diese politisch motivierte Cyberkriminalität wird oft durch sogenannte DDoS-Angriffe durchgeführt, bei denen Angreifer Websites automatisiert mit einer großen Anzahl von Anfragen überfluten, bis diese überlastet und nicht mehr erreichbar sind [60].

Politische Parteien können ebenfalls zu Zielen staatlicher Akteure werden, die im Rahmen von politisch motivierten Diskreditierungsaktionen handeln. Erfolgreiche Cyberangriffe, Datenlecks und Kontrollverlust nehmen Einfluss auf die Reputation von Personen und Organisationen sowie die Akzeptanz des demokratischen Parteiensystems. Die dahinterstehenden Akteure verfolgen das Ziel, Unsicherheiten und Spaltungen in der Gesellschaft zu schaffen oder zu verstärken und durch meinungsbildende Maßnahmen, Einfluss auf politische Entscheidungen zu nehmen [56].

In diesem Zusammenhang kann auch die Cyberattacke auf die CDU Ende Mai 2024 – eine Woche vor der Europawahl – betrachtet werden. Dabei konnten unter anderem Daten des CDU-Parteivorsitzenden Friedrich Merz, darunter Kalenderdaten, kompromittiert werden. Die Hacker hatten unter anderem eine Schwachstelle eines Produkts der Firma CheckPoint genutzt, mit dem sich Mitarbeitende sicher mit dem Netzwerk ihres Arbeitgebers verbinden können [284]. Kriminelle nutzen in diesem Fall die Sicherheitslücke CVE-2024-24919 in Security Gateways in Kombination mit Phishing-Angriffen, um Informationen auf internetverbundenen Gateways mit aktiviertem Fernzugriff oder mobilem Zugriff auszulesen [129]. Hinter den Angriffen wird die Hackergruppe APT29, auch bekannt als Cozy Bear, Midnight Blizzard, Nobelium oder The Dukes, vermutet, die von der russischen Regierung unterstützt wird. Ziel des Phishing-Angriffs war auch die Übertragung einer neuen Variante der Backdoor WINELOADER. Mit diesem Angriff betrat APT29 Neuland: Erstmals richtete sich die Gruppe, die zuvor hauptsächlich diplomatische Einrichtungen ins Visier nahm, gegen eine politische Partei. Dies signalisiert eine potenziell gefährliche Erweiterung ihres Interessenbereichs. Insgesamt waren deutschlandweit bis zu 1.800 IT-Systeme, die Netzwerksicherheitsprodukte von Check Point nutzen, durch die Schwachstelle gefährdet. Neben der CDU wurden auch Betreiber Kritischer Infrastrukturen in den Bereichen Transport und Gesundheit erfolgreich angegriffen [25].

Bereits im Januar 2023 (die Aufklärung erfolgte erst im Mai 2024) wurden E-Mail-Konten der SPD auf Bundesebene über eine Schwachstelle im Microsoft-Windows-Client von Outlook (CVE-2023-23397) attackiert [26], [170]. Diese Aktion wurde vom Verfassungsschutz der Hackergruppe APT28 (auch bekannt als Sofacy, Fancy Bear, Pawn Storm oder Sednit) zugeordnet, die der Russischen Föderation und konkret dem russischen Militärgeheimdienst GRU zugeordnet wird. Opfer dieses Angriffs waren neben der SPD auch deutsche Unternehmen aus den Bereichen Logistik, Rüstung, Luft- und Raumfahrt und IT-Dienstleistungen. Möglich wurde er laut SPD durch eine damals noch unbekannte Sicherheitslücke beim Softwarekonzern Microsoft.

Lieferkettenangriffe

Lieferkettenangriffe, bei denen Angreifer Schwachstellen in der Software-Lieferkette ausnutzen, um Schadsoftware zu verbreiten, waren 2024 ein weiteres großes Thema [225], [264].

Der Ransomware-Angriff auf Synnovis im Juni 2024 verdeutlichte eindrucksvoll, dass Cyberangriffe nicht nur technische, sondern vor allem tiefergreifende operative Auswirkungen haben können. Obwohl der Angriff die IT-Systeme des National Health Service (NHS) nicht direkt beeinträchtigte, führte dieser zu massiven Störungen im Gesundheitswesen Südost-Londons, insbesondere in den beiden am stärksten betroffenen Klinikverbünden – dem King's College Hospital NHS Foundation Trust und dem Guy's and St. Thomas' NHS Foundation Trust. Die Folgen waren gravierend: 10.152 akutmedizinische Ambulanztermine und 1.710 geplante Eingriffe mussten verschoben werden. Dieser Vorfall zeigt einmal mehr, wie angreifbar Kritische Infrastrukturen sind und welche weitreichenden Konsequenzen Cyberangriffe für das öffentliche Leben haben können – insbesondere im Gesundheitssektor, wo Verzögerungen lebensbedrohlich sein können [202], [206].

Der Datenabfluss bei Snowflake, einer cloud-basierten Datenplattform, die es Unternehmen ermöglicht, Daten in Echtzeit zu speichern, zu analysieren und zu teilen, war ein schwerer Schlag für die Sicherheit in der Cloud. Die Plattform unterstützt Datenintegration, -freigabe und -sicherheit und lässt sich nahtlos in bestehende Analyse- und BI-Tools integrieren. Der genaue Ablauf des Angriffs ist nicht vollständig bekannt. Es wird angenommen, dass die Angreifer Zugangsdaten eines Snowflake-Mitarbeiters erlangten und sich damit unbefugten Zugriff auf die Systeme verschafften. Dadurch konnten sensible Daten von Kunden, wie Santander Bank [22] und Ticketmaster [283], kompromittiert und Lösegeld gefordert wurden [262].

Nicht nur direkte Cyberattacken, sondern auch fehlerhafte Sicherheitsupdates können schwerwiegende Lieferkettenprobleme verursachen, in deren Fahrwasser dann vermehrt cyberkriminelle Aktivitäten folgen. Ein Vorfall im Juli 2024 unterstreicht das Gefahrenpotential von unzureichenden Test- und Qualitätssicherungsmaßnahmen im Zusammenhang mit Software-Updates. Am 19. Juli 2024 veröffentlichte das amerikanische Cybersecurity-Unternehmen CrowdStrike ein fehlerhaftes Update für sein Produkt Falcon Sensor, einer Endpoint Detection and Response (EDR)-Schutzsoftware für Endgeräte [48]. Infolgedessen kann es zu weitreichenden Problemen bei Microsoft Windows-Computern, auf denen die Software installiert war [79]. Rund 8,5 Millionen Systeme stürzten ab und konnten nicht ordnungsgemäß neu gestartet werden [328]. Das BSI stufte den Vorfall als geschäftskritisch ein [48].

Weitere Schäden entstanden durch das Ausnutzen der durch das Event entstandenen Aufmerksamkeit. Auch weniger professionelle Cyberkriminelle nutzen die CrowdStrike-bezogenen Ausfälle für sich aus, um im Fahrwasser der allgemeinen Verunsicherung, sofort bösartige Aktivitäten zu starten. Sie registrierten beispielsweise neue, eventbezogene Domains und versendeten Malware in Dateien mit CrowdStrike-bezogenen Dokumentennamen [312].

Zero-Day-Exploits und gezielte Angriffe

Sicherheitslücken, die noch nicht bekannt oder gepatcht, also behoben, wurden (Zero-Day-Exploits, ZDE) stellen eine der gravierendsten Bedrohungen für die IT-Sicherheit dar. Diese Angriffe zielen auf bisher unbekannte Schwachstellen ab und können somit oft unbemerkt bleiben. Die Bewertung der tatsächlichen Anzahl und des Einflusses von Zero-Day-Exploits ist äußerst schwierig, da sie erst sichtbar werden, wenn sie öffentlich bekannt werden oder bei einem Angriff zum Einsatz kommen. Bestätigt werden kann, dass staatliche Akteure über umfangreiche Sammlungen von Zero-Day-Exploits verfügten, die sie gezielt für offensive Cyberoperationen einsetzen [108]. Zudem nutzen Angreifer alle technologischen Möglichkeiten, Sicherheitslücken schneller zu identifizieren und auszunutzen, was die Notwendigkeit für proaktive und schnell umzusetzende Sicherheitsmaßnahmen und schnelle Reaktionszeiten unterstreicht (Übersicht des Lebenszyklus eines Zero-Day-Exploits auf dem Markt siehe Abbildung 4).

Im März 2024 ermöglichte der Microsoft Exchange Server-Angriff Angreifern, E-Mails abzufangen und E-Mail-Server zu kompromittieren. Diese Schwachstelle wurde von staatlichen Akteuren und Cyberkriminellen ausgenutzt, um gezielte Angriffe auf Unternehmen und

Behörden durchzuführen. Im Juli 2024 ermöglichte der CrowdStrike Falcon Bug Angreifern, die Sicherheitslösung CrowdStrike Falcon zu umgehen und sich in betroffenen Systemen einzunisten. Dieser Vorfall zeigte, dass selbst renommierte Sicherheitslösungen anfällig für Schwachstellen sein können.

Im Jahr 2024 kam es beispielsweise zu einer Reihe von hochgradig gefährlichen Cyberangriffen auf Ivanti VPN-Produkte, die die IT-Sicherheit zahlreicher Unternehmen weltweit ernsthaft beeinträchtigten. Bereits Anfang Januar 2024 wurden schwerwiegende Schwachstellen in Ivanti-Software öffentlich bekannt gegeben, die es Cyberkriminellen ermöglichten, unbefugt auf Systeme zuzugreifen und diese zu kontrollieren [53]. Die Angreifer nutzten dabei gezielt Zero-Day-Exploits aus, um ihre Ziele zu erreichen. Die Ivanti Produkte Connect Secure, das als VPN-Gateway dient, und Policy Secure für die Zugriffskontrolle waren beide von kritischen Zero-Day-Schwachstellen betroffen. Angreifer konnten diese Lücken ausnutzen, um sich Zugriff auf diese Systeme zu verschaffen und von dort aus weitere Teilen des Netzwerks zu kompromittieren. Durch die Installation eigener Software, das Umgehen von Sicherheitsmaßnahmen und das Sammeln von Anmeldedaten konnte erheblicher Schaden angerichtet werden [263]. Im September 2024 berichtete Ivanti in einem Advisory von weiteren Angriffen auf Organisationen, die die Lösung Cloud Services Appliance (CSA) des Herstellers einsetzen. Demnach haben die Angreifenden zwei Schwachstellen in CSA kombiniert, um zunächst die Nutzer-Authentifizierung zu umgehen und anschließend Zugriff auf ungesicherte Geräte zu nehmen [49]. Wir stufen diesen Vorfall als einen der bedeutendsten für das Jahr 2024 ein und gehen in Kapitel 1.7 tiefer auf die Details ein.

1.4 ANGREIFERPERSPEKTIVE

Cyberangriffe sind längst mehr als isolierte Hackeraktionen – sie sind ein globales Geschäft, betrieben von gut organisierten Netzwerken, staatlich unterstützten Gruppen und hochspezialisierten Einzelakteuren. Eine Übersicht der in 2024 aktiven Cybergruppen kann beim BSI

Quelle: [147]

Abbildung 4: Übersicht des Lebenszyklus eines Zero-Day-Exploits auf dem Markt

eingesehen werden [44]. Mit raffinierten Techniken und klaren Zielen greifen sie Schwachstellen in Systemen und beim Menschen an, oft mit erheblichem Schaden für Wirtschaft, Politik und Gesellschaft – was im Extremfall eine direkte Gefährdung von Menschenleben bedeutet [6]. Die Perspektive der Angreifer zu verstehen, ist entscheidend, um ihre Strategien, Motivationen und Methoden zu durchschauen – und um uns effektiv gegen diese wachsende Bedrohung zu wappnen.

Die Bedrohungslage in der Cybersecurity hat sich in den vergangenen Jahren zunehmend verschärft, was vor allem an der Professionalisierung und Spezialisierung der Angreifer liegt. Cyberkriminelle entwickeln nicht nur immer raffiniertere Angriffsmethoden, sondern organisieren sich auch in komplexen Netzwerken, die arbeitsteilig vorgehen. Diese Entwicklungen ermöglichen eine beachtliche Effizienz und Flexibilität, wodurch auch weniger erfahrene Akteure Zugang zu hochentwickelten Angriffstechnologien erhalten. Eine zentrale Veränderung liegt dabei in der zunehmenden Spezialisierung auf bestimmte Techniken und Angriffsmethoden, wie am Beispiel des Ransomware-as-a-Service (RaaS) oder im Handel mit erbeuteten Zugangsdaten deutlich wird [147].

Die Auswahl der Ziele erfolgt dabei nicht wahllos. Staatlich gesteuerte Gruppen nutzen häufig das Prinzip von Advanced Persistent Threats (APTs), um sich langfristig bei den Opfern einzunisten und Informationen zu extrahieren. Dabei konzentrieren sie sich meist auf hochsensible Institutionen, wie Behörden oder Unternehmen in sensiblen Sektoren, z. B. im Verteidigungssektor. Im Gegensatz dazu bevorzugen wirtschaftlich motivierte Angreifer eher kleine und mittlere Unternehmen, da diese aufgrund begrenzter Ressourcen oft schlechter gegen Angriffe geschützt sind [46]. Ein Angriff wird dabei in den seltensten Fällen spontan durchgeführt, sondern die Zielauswahl wird strategisch geplant. Angreifer analysieren im Vorfeld potenzielle Schwachstellen in Systemen oder Prozessen, um den Erfolg ihrer Angriffe zu maximieren [100]. Dazu gehört auch die Beschaffung geeigneter Werkzeuge und häufig auch das gezielte Phishing, um Zugangsdaten zu erlangen oder Zugriffe auszuweiten. Eine besondere Gefahr stellen hierbei sogenannte Zero-Day-Schwachstellen, also Sicherheitslücken, die noch nicht bekannt sind, dar. In der Breite der Angriffe spielen oft fehlerhafte oder unsichere Konfigurationen, veraltete Versionen oder menschliche Fehler eine zentrale Rolle bei der Erlangung von Zugriffen. Die Nutzung solcher Schwachstellen verschafft den Angreifern einen erheblichen Vorteil, da die Systeme meist ungeschützt sind [46].

Die eigentliche Ausführung eines Angriffs folgt dann einem präzisen Muster. Angreifer setzen auf eine Kombination aus Technik und Täuschung. Es wird zum einen versucht schnell die Berechtigungen auf den angegriffenen Systemen zu erweitern und gleichzeitig schnellstmöglich relevante Informationen und Dateien zu erbeuten. Parallel wird oft sogenannte Ransomware genutzt, um schnell einen großen Schaden in den Zielsystemen anzurichten. Moderne Schadsoftware ist oft so konzipiert, dass sie Sicherheitslösungen wie Endpoint Detection and Response (EDR) umgeht. Diese Umgehung gelingt durch raffinierte Techniken wie die Nutzung bestehender Systemwerkzeuge oder die kontinuierliche Anpassung der Malware, sodass sie von Sicherheitsprogrammen nicht erkannt wird [147].

Bei ihrer Taktik setzen einige Angreifer auf einmalige Angriffe, wie die Verbreitung von Ransomware, bei denen sie Lösegeld fordern und sich dann zurückziehen. Andere hingegen streben eine langfristige Kontrolle über Systeme an. Diese dauerhafte Präsenz ermöglicht es, Informationen zu sammeln, erneut Lösegeld zu fordern oder gezielte Spionage zu betreiben. Diese Strategien erfordern häufig eine viel höhere Spezialisierung, da der Betrieb von Backdoors oder die dauerhafte Maskierung innerhalb eines Netzwerks technisches Know-how voraussetzt [46].

Auch die Spezialisierung innerhalb der Angreiferszene hat sich weiterentwickelt. Rollen wie Entwickler, Zugangsbeschaffer und Verhandlungsführer, sind inzwischen gängige Bestandteile professioneller cyberkrimineller Gruppen, man könnte dabei von unternehmensähnlichen Strukturen sprechen. Die zunehmende Rivalität zwischen diesen Gruppen hat jedoch auch zur Folge, dass es häufiger zu Konflikten oder sogenannten Exit-Scams kommt, bei denen Mitglieder eines Netz-

werks sich mit den erbeuteten Geldern absetzen [147]. Gleichzeitig hat das Outsourcing von Angriffen an spezialisierte Dienstleister zugenommen, was die Angriffslandschaft weiter fragmentiert [46].

Bei der Monetarisierung von Angriffen sind Kryptowährungen wie Bitcoin nach wie vor die bevorzugte Zahlungsmethode. Diese werden zunehmend durch Stablecoins ergänzt, da sie weniger Kursschwankungen unterliegen und somit für Angreifer planbarer sind. Während einige Gruppen auf standardisierte Lösegeldforderungen setzen, gehen andere in Verhandlungen, um die Zahlungen zu maximieren. Dies erschwert die Nachverfolgung und zeigt die zunehmende Professionalisierung in diesem Bereich [100].

Hinter den Angriffen stehen sowohl Einzelpersonen als auch organisierte Gruppen. Einzelne Hacker agieren oft aus intrinsischen Motiven, wie dem Wunsch nach Anerkennung oder Neugier. Organisierte Gruppen hingegen arbeiten häufig wirtschaftlich oder politisch motiviert. Staatlich unterstützte Akteure nutzen Cyberangriffe, um geopolitische Ziele zu erreichen, wie die Destabilisierung anderer Länder oder den Diebstahl sensibler Daten. Wirtschaftlich orientierte Gruppen hingegen zielen darauf ab, Unternehmen durch Datenlecks oder Sabotage zu schädigen und finanzielle Gewinne zu erzielen [46]. In beiden Fällen spielen finanzielle Motive eine zentrale Rolle, sei es durch Erpressung oder den Weiterverkauf gestohlener Daten [100]. Hacker, die aus Überzeugung handeln und sogenannte Hack-for-Hire-Dienste, die Angriffe im Auftrag Dritter durchführen, ergänzen die Palette der Angreiferprofile [46]. Gleichzeitig führt die wachsende Zahl an Cyberkriminellen zu einer stärkeren Konkurrenz, was wiederum die Qualität und Raffinesse der Angriffe steigert [147].

Die Angreiferperspektive zeigt somit ein facettenreiches Bild, das durch technische Innovationen, arbeitsteilige Zusammenarbeit und die vielfältigen Motive der Akteure geprägt ist. Angesichts dieser Dynamik ist es entscheidend, sowohl technische als auch menschliche Schwachstellen zu adressieren und die Resilienz gegen diese komplexen Bedrohungen zu stärken. Die Berichte von BSI, Europol und Intel 471 unterstreichen dabei, wie wichtig ein integrierter Ansatz ist, um den Herausforderungen der modernen Cyberkriminalität zu begegnen.

Wenn Kriminelle in den Besitz personenbezogener Daten eines Mitarbeitenden oder eines vertrauenswürdigen Partners gelangen, können diese Informationen genutzt werden, um Zugang zu vertraulichen und sensiblen Daten zu erhalten. Das Ziel des Identitätsdiebstahls besteht häufig darin, finanzielle Vorteile durch den Diebstahl von Daten zu erlangen. Besonders begehrt sind dabei nicht nur Zugangsdaten zu Netzwerken von Unternehmen, Organisationen und Privatpersonen (z. B. Nutzername und Password) sondern auch Informationen, wie Bank- oder Kreditkartennummern, Führerscheinnummern oder Sozialversicherungsnummern. Bekannte Methoden des Identitätsdiebstahls sind Phishing (gefälschte Kommunikationen), Social Engineering (Manipulation von Menschen), Skimming (Manipulation von Kartenlesern), Hacking (Eindringen in Systeme) oder Dumpster Diving (Durchsuchen von Müll), bei denen Betrüger persönliche Informationen stehlen und für betrügerische Zwecke verwenden. Identitätsbasierte Angriffe zielen darauf ab, die digitalen Identitäten von Personen, Anwendungen und Geräten innerhalb einer Organisation zu kompromittieren. Die Angreifer verschaffen sich Zugang zu den Systemen, Netzwerken oder sensiblen Ressourcen des Unternehmens, indem sie Anmeldeinformationen stehlen oder Authentifizierungsmechanismen umgehen. Einmal im Netzwerk, können sie Daten manipulieren, löschen oder verschlüsseln, um den Betrieb zu stören oder Lösegeld zu erpressen. Cyberkriminelle konzentrieren sich stärker darauf, gültige Konten auszunutzen, anstatt sich in Systeme zu hacken. Dieser Ansatz ist sowohl effizienter als auch schwerer zu erkennen, was ihn zu einer bevorzugten Taktik macht [143].

1.4.1 VERWENDUNG VON OFFENSIVER KI

Cyberkriminelle setzen KI ein, um ihre Angriffe zu verbessern und effizienter zu gestalten. Diese Technologien verringern die Einstiegshürden und steigern sowohl das Ausmaß als auch die Geschwindigkeit bösartiger Aktivi-

täten, was zu kompetenteren Angreifern und qualitativ hochwertigeren Angriffen führt. Zudem ermöglicht KI den Angreifern, mehrere Angriffe gleichzeitig durchzuführen und somit ihre Erfolgsquote zu erhöhen. Es ist wichtig zu beachten, dass die gleichen Produkte, die IT-Sicherheitsteams unterstützen, auch von Angreifern genutzt werden können. Als grundsätzliches Risiko besteht der Sachverhalt, dass Menschen sensible Daten in KI-Chatbots eingeben und diese Daten versehentlich an die Öffentlichkeit gelangen. Angreifer können diese Daten nutzen, um ihre Angriffe weiter zu verfeinern und gezielter vorzugehen [19], [47].

Auswertung großer Datenmengen

KI kann auch große Datenmengen analysieren, um automatisiert Schwachstellen in Systemen zu identifizieren und gezielte Angriffe zu planen. Für die automatische Erkennung von Sicherheitslücken stehen Sicherheitsteams aber auch Angreifern zahlreiche Open-Source-Tools und kommerzielle Produkte zur Verfügung. Diese Produkte ermöglichen eine einfache Analyse von Open-Source-Anwendungen. Bei Closed-Source-Anwendungen können sie in Kombination mit Reverse-Engineering-Tools eingesetzt werden, wobei die Ergebnisse je nach Codekomplexität und Verschleierungstechniken variieren.

KI-gestützte Produkte helfen Angreifern auch, die nützlichsten Ereignisse aus mehreren Datenquellen zu identifizieren und zu korrelieren, was den Angreifern wertvolle Zeit spart und ihre Angriffe effektiver macht. Generative KI kann die Analyseergebnisse in natürliche Sprache übersetzen und Fragen ebenfalls in natürlicher Sprache beantworten, was die Untersuchung für Angreifer vereinfacht.

Darüber hinaus können Angreifer KI nutzen, um Websites und soziale Medien zu durchsuchen und zu analysieren, um Informationen über potenzielle Ziele zu sammeln. Dadurch können beispielsweise automatisiert überzeugende Phishing-E-Mails mit menschenähnlichen Texten verfasst werden, die auf spezifische Ziele zugeschnitten sind, was die Erfolgsrate solcher Angriffe erhöht. KI kann verwendet werden, um legitime Personen zu imitieren und so Vertrauen zu gewinnen und Zugang zu sensiblen Informationen zu erhalten. Im Abschnitt „Social Engineering“ in Kapitel 1.4.2 wird tiefer auf die Details eingegangen.

Autonome Generierung und Mutation von Malware

Generative KI, insbesondere große Sprachmodelle (LLMs), ermöglicht es Angreifern, komplexe Malware schneller und effizienter zu erstellen. Programmierassistenten, die auf KI basieren, können Angreifern helfen, effizienteren und effektiveren Schadcode zu schreiben, der schwerer zu erkennen und zu bekämpfen ist. Es gibt bereits Proof of Concepts (PoC) und Projekte, die KI für die autonome Generierung und Mutation von Malware einsetzen. Diese Technologien sind zwar noch nicht „produktionsreif“, zeigen jedoch das Potenzial für zukünftige Bedrohungen. Angreifer können KI nutzen, um Malware sowohl statisch (durch Erkennung wiederkehrender Muster) als auch dynamisch (durch Anpassung von Bibliotheken zur Laufzeit) zu analysieren und zu verbessern.

Ein alternativer Ansatz für den Einsatz von LLMs besteht darin, bestimmte Abschnitte der Angriffskette zu automatisieren, ähnlich wie bei den zuvor erwähnten Produkten. Besonders hervorzuheben ist dabei die Automatisierung der Aufklärungsphase, aber auch andere Schritte, wie die Analyse von Serverantworten, können durch LLMs unterstützt werden.

KI wird auch zum Erraten von Passwörtern verwendet. Anstatt manuell erstellte Regeln zu nutzen, lernen KI-gestützte Methoden die Regeln für Passwortkandidaten aus Daten, basierend auf der Annahme, dass bestimmte Passworttypen häufiger von Menschen gewählt werden. Dank zahlreicher Datenlecks stehen hierfür umfangreiche Trainingsdaten zur Verfügung.

Ein weiteres Risiko besteht in der Gefahr von eingebetteter Malware in KI-Modellen. Malware kann in den Parametern neuronaler Netze verschlüsselt sein, ohne die Nutzbarkeit des Modells zu beeinträchtigen. Schädlicher Code kann auch in trainierten Modellen versteckt sein, die auf Plattformen verbreitet werden.

Seriöse Softwareanbieter nutzen LLMs für den Kundensupport, und böswillige Akteure könnten diese Technologie ebenfalls nutzen, um Malware-as-a-Service-Nutzern Unterstützung zu bieten. Zudem kann die automatisierte Hilfe bei der Beschaffung und Zahlung von Kryptowährung die Erfolgsquote von Ransomware-Angriffen erhöhen.

1.4.2 ANGRIFFSVEKTOREN

Ein Angriffsvektor ist die Methode oder Kombination von Methoden, die Cyberkriminelle verwenden, um die Systeme, Netzwerke, Anwendungen oder Schutzbereiche eines Opfers zu kompromittieren oder zu infiltrieren.

Angreifer entwickeln in der Regel ein Arsenal an Angriffsvektoren, die sie routinemäßig für ihre Angriffe einsetzen. Mit der Zeit und durch wiederholte Nutzung werden diese Angriffsvektoren zu virtuellen „Visitenkarten" von Cyberkriminellen oder organisierten E-Crime-Banden. Bedrohungsanalysten, Cybersecurity-Dienstleister, Strafverfolgungsbehörden und Regierungsbehörden können anhand dieser „Visitenkarten" verschiedenen Gegnern eine Identität zuweisen.

Wenn Unternehmen die Angriffsvektoren eines Akteurs erkennen und verfolgen, können sie sich besser gegen bestehende oder bevorstehende gezielte Angriffe verteidigen. Darüber hinaus hilft das Wissen darüber, wer hinter einem Angriff steckt (was sich teils am verwendeten Angriffsvektor ablesen lässt), Unternehmen dabei, die Fähigkeiten der Angreifer zu verstehen und in Zukunft Maßnahmen zum Schutz des Unternehmens und seiner Vermögenswerte zu ergreifen [178]. Die wachsende Angriffsfläche der Unternehmen ermöglicht es den Angreifern ihre Strategien fortlaufend anzupassen, um neu erscheinende Schwachstellen auszunutzen [198].

Bei den Angriffsvektoren ist zwischen aktiven Angriffsvektoren, also bei welchen sich Cyberkriminelle unbefugten Zugriff auf das Netzwerk des Unternehmens verschaffen und dem Unternehmen Schaden zufügen, und passiven Angriffsvektoren, bei welchen die Angreifer lediglich die Systeme des Unternehmens überwachen, um Zugriff auf Daten und andere sensible Informationen zu erhalten, zu unterscheiden. Die gängigsten Angriffsvektoren sind die Ausnutzung schwacher und kompromittierter Anmeldeinformationen, die Einschleusung von Malware, Social Engineering, Insider-Bedrohungen, nicht gepatchte Software, mangelnde Verschlüsselung, DDoS und Fehlkonfigurationen [300].

Der Einsatz Künstlicher Intelligenz ermöglicht eine effizientere [198], fehlerarme und individualisierte [90] Erstellung von Inhalten, was den Kriminellen dann bei Phishing-Kampagnen zugutekommt [237]. Zudem bietet KI die Möglichkeit, verschiedene Angriffsvektoren zu automatisieren, welche die Produktivität der Angriffe und die Erfolgschancen dieser steigern [90]. Das größte Cybersecurity-Risiko, das sich aus dem zunehmenden Einsatz von KI-Tools ergibt, sind jedoch die steigende Anzahl von Angriffen [198] und die Zunahme der Angriffsgeschwindigkeit [90]. Der von Unit 42 veröffentlichte Incident Response Report 2024 zeigt, dass erfolgreiche Angriffe in komplexen Umgebungen bereits innerhalb von acht Stunden nach dem Versand der ersten Phishing-E-Mail zur Datenexfiltration führen können [90].

Doch dient KI heutzutage nicht mehr nur der Unterstützung und Verbesserung bereits bekannter Cyberangriffstechniken. Große Sprachmodelle können bereits heute einfachen Schadcode schreiben und Malware erstellen oder mutieren. Zwar wird eine vollständige Angriffsautomatisierung durch KI in naher Zukunft wohl nicht möglich sein, die Automatisierung von Teilen eines Cyberangriffs gehört jedoch bereits dazu [47]. Auch in Zukunft wird der Einsatz von KI aller Voraussicht nachzunehmen und die Effektivität und Effizienz der Angriffe steigen [120].

Doch nicht nur die Informationstechnologie (IT) sieht sich vermehrt Neuerungen im Bereich der Angriffsvektoren gegenübergestellt. Auch die Operational Technology (OT), also die Hardware- und Softwaresysteme, die zur Überwachung und Steuerung physischer Prozesse, Geräte und Infrastrukturen verwendet werden [221], ist mit diversen Cybersecurity-Bedrohungen konfrontiert. Diese reichen von Malware-Infektionen und Ransomware-

Angriffen bis hin zu gezielten Sabotageaktionen [89]. Oftmals stehen beide Systeme jedoch auch in direktem Zusammenhang, da Betriebe in allen Industriebereichen zunehmend vernetzt sind. Die OT verbindet, überwacht, steuert und sichert die industriellen Prozesse. Angriffe auf IT-Systeme können so den Zugang zu OT-Netzwerken ermöglichen, was zu Produktionsausfällen und damit verbunden zu erheblichen finanziellen Verlusten führen kann. Laut neuesten Veröffentlichungen und Forschungen gelangen mittlerweile 72 Prozent der Angriffe über IT-Systeme in die OT-Umgebung [258]. Auch indirekte Angriffe, bspw. das Blockieren IT-abhängiger Prozesse, können Produktion und Lieferkette beeinträchtigen [153]. Ebenso stellt die oftmals jahrzehntelange Nutzungsdauer der OT ein Risiko dar, da es die Wahrscheinlichkeit erhöht, dass OT-Systeme irgendwann nicht mehr unterstützt werden. So sind Patches und andere Aktualisierungen zur Behebung von Schwachstellen und Hinzufügung von Sicherheitsfunktionen für ältere OT-Systeme oftmals nicht mehr verfügbar, was sie potenziell anfälliger für Cyberangriffe macht [250].

Für Unternehmen ist es daher wichtig, sowohl für ihre IT als auch für ihre OT potenzielle Angriffsvektoren zu kennen und entsprechende Sicherheitsvorkehrungen zu treffen. Durch die zunehmende Vernetzung der industriellen Prozesse mit der Informationstechnologie ist insbesondere der Schutz der IT und der entsprechenden Schnittstellen von großer Bedeutung.

Angriffe auf Cybersecurity-Produkte

Wenn es um Cybersecurity geht, wird oftmals auf VPN-Dienste zurückgegriffen, also auf virtuelle private Netzwerke, die eine verschlüsselte Verbindung zum Internet herstellen und so die Privatsphäre schützen. Doch auch diese Sicherheitstools sind nicht ohne Risiko. Im Gegenteil: Nach neuesten Publikationen sind VPN-Angriffe auf dem Vormarsch. 56 Prozent der Unternehmen waren im Jahr 2023 von einem oder mehreren VPN-bezogenen Cyberangriffen betroffen – gegenüber 45 Prozent im Vorjahr. 91 Prozent der Befragten äußerten Bedenken, dass VPNs ihre IT-Sicherheitsumgebung gefährden könnten. Jüngste Sicherheitsverletzungen, wie etwa die ungepatchte Sicherheitslücke (CVE-2024-3400) in der Firmware von Palo Alto Networks (PAN), die in PAN-Firewalls zum Einsatz kommt [32], verdeutlichen die Risiken veralteter oder nicht gepatchter VPN-Infrastrukturen [256]. Diese Schwachstelle in der Firmware, die das grundlegende Betriebssystem der Firewall steuert, ermöglichte es Angreifern, unbemerkt in Unternehmensnetzwerke einzudringen und sensible Daten zu exfiltrieren.

Im April 2024 machten es sich Hacker zur Aufgabe, eine großangelegte Cyberattacke gegen VPN- und Secure Shell (SSH)-Dienste auf die Hersteller von Cisco, CheckPoint, Fortinet, SonicWall und Ubiquiti auszuführen. Bei der Angriffsmethode handelte es sich um eine Brute-Force-Kampagne. Dabei wird versucht, sich mit vielen Benutzernamen und Passwörtern bei einem Konto oder Gerät anzumelden, bis die richtige Kombination gefunden ist. Sobald die Bedrohungsakteure Zugang zu den richtigen Anmeldedaten haben, können sie diese verwenden, um ein Gerät zu übernehmen und sich Zugang zum internen Netzwerk zu verschaffen. Bei dieser Kampagne wurde eine Mischung aus gültigen und generischen Benutzernamen von Mitarbeitern bestimmter Unternehmen genutzt [298].

Die Angriffe begannen am 18. März 2024, wobei alle Angriffe von TOR-Exit-Nodes und verschiedenen anderen Anonymisierungs-Tools und Proxys ausgingen, die die Bedrohungsakteure nutzten, um ihre wahre Identität zu verschleiern und die Nachverfolgung zu erschweren [331].

Zu den Diensten, die zur Durchführung der Angriffe genutzt werden, gehören TOR, VPN Gate, IPIDEA Proxy, BigMama Proxy, Space Proxies, Nexus Proxy und Proxyrack. Folgende Dienste wurden aktiv von dieser Kampagne angegriffen: Cisco Secure Firewall VPN, CheckPoint VPN, Fortinet VPN, SonicWall VPN, RD-Webdienste, MikroTik, DrayTek und Ubiquiti. Die Angreifer konzentrieren sich dabei nicht auf bestimmte Branchen oder Regionen, was auf eine breitere Strategie von zufälligen, opportunistischen Angriffen schließen lässt [298].

Doch nicht nur Unternehmen oder öffentliche Institutionen sind betroffen. Sicherheitsforscher haben eine Technik entwickelt, die auch jedes virtuelle private Netzwerk unbrauchbar machen kann. Die Methode wurde von Forschern der Leviathan Security Group entdeckt. Sie ermöglicht es, den Datenverkehr eines VPN-Benutzers offenzulegen, sodass ein Angreifer unverschlüsselte Daten einsehen und wertvolle Informationen abfangen kann. Die Forscher nennen ihren Exploit „TunnelVision". Nach Angaben des Unternehmens fanden die Forscher bisher kein VPN, das gegen diesen Angriff immun ist. Für den Angriff benötigen die Forscher Zugang zu dem Netzwerk, in dem das VPN verwendet wird. Ihr Exploit erlaubt es, dort einen Dynamic Host Configuration Protocol Server (DHCP-Server) zu betreiben, damit eigene IP-Adressen zu vergeben und den Datenverkehr umzuleiten. Dadurch kann die VPN-Verschlüsselung umgangen und unverschlüsselte Datenpakete eingesehen werden. VPN-Nutzer bemerken nicht, dass ihr Datenverkehr unverschlüsselt ist, und auch die VPNs selbst erkennen die Manipulation nicht.

Die größte Herausforderung für einen Angreifer ist der Zugang zu dem Netzwerk, in dem das VPN betrieben wird. Hackern gelingt dies jedoch immer wieder und TunnelVision könnte dann eine weitere Möglichkeit bieten, auf sensible Daten zuzugreifen. Die Forscher vermuten, dass Bedrohungsakteure die Schwachstelle bereits seit 2002 kennen. Es gibt jedoch keine eindeutigen Beweise dafür, dass TunnelVision bereits aktiv genutzt wurde. Die Hersteller von VPN-Lösungen wurden über die Entdeckung informiert [24].

Die überwiegende Mehrheit der im Rahmen einer Umfrage befragten Unternehmen geht aufgrund der zunehmenden Risiken im Bereich Cybersecurity-Risiken zu Zero Trust über. 78 Prozent planen die Einführung von Zero-Trust-Strategien in den nächsten 12 Monaten. Gleichzeitig stimmen 62 Prozent der Unternehmen zu, dass VPNs gegen Zero Trust sind [256].

Die steigenden VPN-Angriffe und jüngsten Sicherheitsverletzungen verdeutlichen die Schwächen veralteter VPN-Infrastrukturen. Daher ist es entscheidend, dass Unternehmen ihre Sicherheitsarchitekturen modernisieren, um den wachsenden Cyberbedrohungen effektiv zu begegnen. Der CrowdStrike Falcon Bug verdeutlicht zudem, dass Organisationen zunehmend von wenigen führenden Anbietern abhängig sind, was das Risiko systemischer Schwachstellen birgt. Diese können nicht nur ihre direkten Kunden betreffen, sondern auch einen Dominoeffekt im gesamten Ökosystem auslösen. Die steigende Komplexität des Ökosystems kann dabei zu weitreichenden und unvorhersehbaren Folgen bei Cyberangriffen oder Ausfällen führen [6].

Angriffe auf Softwarelieferketten

Analog zu physischen Lieferketten bezeichnet die Softwarelieferkette die Lieferung von Software-Komponenten und Ressourcen von Entwickler bis hin zur Bereitstellung einer Anwendung. Dieser Software-Development-Lifecycle (SDLC) besteht aus sechs Phasen, die von der Anforderungserhebung bei den Nutzern über die Entwicklung bis zur Einführung und Nutzung reicht und auch die Außerbetriebnahme mit abdeckt [18], [72].

Alle Phasen bieten, wie bei einer physischen Lieferkette auch, individuelle Angriffsflächen für Cyberangriffe. Herausfordernd ist über den gesamten Zyklus hinweg dabei insbesondere die steigende Komplexität von Softwaresystemen. Sowohl die Anzahl der Komponenten als auch die Anzahl der Beziehungen zwischen diesen erhöhen die Komplexität des Systems [107]. Mehr Code, mehr Daten und mehr (externe) Abhängigkeiten bedeuten mehr Komplexität und mehr Komplexität führt häufig vermehrt zu Problemen – eine ideale Angriffsfläche für Cyberkriminelle [223]. Ein Angriff auf die Software-Lieferkette ist dadurch gekennzeichnet, dass schadhafter Code in ein Softwarepaket eingeschleust wird, um abhängige Systeme in der Abhängigkeitskette zu kompromittieren. In den letzten Jahren gab es eine Reihe von Angriffen auf die digitale Versorgungskette, die die zunehmende Verwendung von Open-Source-Software während der Softwareentwicklung ausnutzen, was durch Abhängigkeitsmanager erleichtert wird, die automatisch Hunderte von Open-Source-Paketen während des gesamten Lebenszyklus der Software auflösen, herunterladen und installieren [217].

Unternehmen lagern ihre IT-Services zunehmend an externe IT-Dienstleister aus, was zu einer verstärkten digitalen Vernetzung der Unternehmen führt. Diese Entwicklung der Auslagerung von IT-Services an Drittanbietern und die stetig wachsende Komplexität der IT-Infrastrukturen erhöht die Angriffsmöglichkeiten für Cyberkriminelle deutlich. Durch das gezielte Ausnutzen von Schwachstellen in IT-Lieferketten können Angreifer mit der Ausnutzung einer einzelnen Schwachstelle beziehungsweise dem Zugriff auf die Systeme eines IT-Dienstleisters in einem Zug eine Vielzahl von Unternehmen oder Behörden schädigen. Insbesondere Ransomware-Angriffe und Datenexfiltration stellen in diesem Kontext eine ernstzunehmende Bedrohung dar [60].

Die Nutzung von Open-Source-Software ist explodiert: Schätzungen gehen davon aus, dass im Jahr 2024 mehr als 6,6 Billionen Downloads getätigt wurden. Diese Abhängigkeit von Open-Source-Komponenten, die inzwischen bis zu 90 Prozent der modernen Softwareanwendungen ausmachen, bringt komplexe Herausforderungen für Software-Lieferketten mit sich. Tatsächlich ist die Zahl der bösartigen Pakete [264] im Vergleich zum Vorjahr 2023 um 156 Prozent gestiegen und stellt damit ein erhebliches Risiko für Unternehmen dar, die ihre Abhängigkeiten von Open-Source-Software (OSS) nicht aktiv verwalten [264].

Kriminelle nutzen verschiedene Techniken, um bösartige Codes in bspw. Open-Source-Software einzuschleusen. Eine häufig verwendete Methode dabei ist das Social Engineering, bei dem Angreifer versuchen, das Vertrauen der Entwickler zu gewinnen und sich selbst als legitime Entwickler auszugeben. Ein prominentes Beispiel hierfür ist der XZ Utils Vorfall, bei welchem der Angreifer über einen Zeitraum von etwa zwei Jahren das Vertrauen des ursprünglichen Projektbetreuers gewann und schließlich die Kontrolle übernahm. Der Angreifer nutzte diese Position, um schädlichen Code in das Projekt einzuschleusen [96]. Wir stufen diesen Vorfall als einen der bedeutendsten für das Jahr 2024 ein und gehen in Kapitel 1.7 tiefer auf die Details ein.

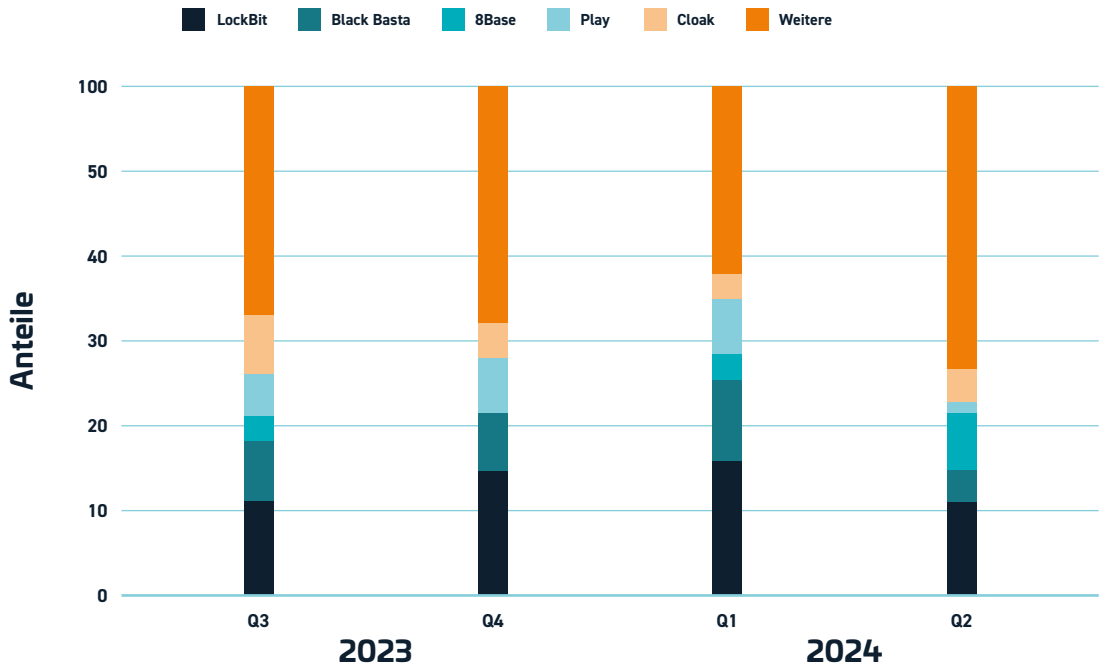
Neben Social Engineering werden auch andere Taktiken eingesetzt, wie das gezielte Austauschen von Namen oder Repositorys (z. B. in Cheat-Sheets), um Entwickler*innen zur Verwendung von kompromittierter Software zu veranlassen oder die Einbettung von Malware in Testdateien [96]. Das US-amerikanische Marktforschungsunternehmen Gartner Inc. geht davon aus, dass bis 2025 45 Prozent der Unternehmen weltweit von Angriffen auf die Softwarelieferkette betroffen sein werden – dreimal so viele wie noch 2021 [114]. Dies macht ihren Schutz wichtiger denn je.

Ransomware

Ransomware bezeichnet Schadprogramme, die den Zugriff auf Systeme blockieren und erst gegen Lösegeldzahlung wieder freigeben. Diese Programme verschlüsseln wichtige Daten, um Opfer zu erpressen. Dennoch gibt es keine Garantie, dass die Daten nach Zahlung entschlüsselt oder nicht veröffentlicht werden. Daher rät das Bundesamt für Sicherheit in der Informationstechnik (BSI) ausdrücklich von Lösegeldzahlungen ab [46].

Die zunehmende Professionalisierung der Angriffe zeigt sich in der Nutzung von Ransomware-as-a-Service (RaaS). Dieses Geschäftsmodell ermöglicht es Entwicklern von Schadsoftware, ihren Plattformen Affiliates zur Verfügung zu stellen, die Angriffe durchführen und die Lösegeldzahlungen mit den Entwicklern teilen. Dieses System hat die Eintrittsbarrieren für weniger technisch versierte Täter erheblich gesenkt und die Verbreitung von Ransomware-Angriffen beschleunigt [60], [96].

Zu den prominentesten Gruppen gehört LockBit, die sowohl in Deutschland als auch weltweit aktiv war. LockBit war für 40 mutmaßliche Leak-Opfer in Deutschland und 944 weltweit verantwortlich. Weitere Gruppen, wie Black Basta, 8Base und Play, zielten auf Schwachstellen in Perimetersystemen, wie VPNs und Mail-Servern, um Erstinfektionen durchzuführen [46]. Anzahl der Opfer je nach Leak-Seite ist in Abbildung 5 ersichtlich.



Quelle: [46]

Abbildung 5: Mutmaßliche Opfer aus Deutschland auf Leak-Seiten

Die Angriffe beschränken sich jedoch nicht nur auf Verschlüsselung. Zunehmend setzen Täter auf mehrfache Erpressungstechniken, wie die Drohung, gestohlene Daten zu veröffentlichen, um Opfer zusätzlich unter Druck zu setzen. Diese Methode wurde Juli 2023 bis Juni 2024 in mehreren hochkarätigen Fällen beobachtet [96].

Die häufigsten Einstiegspunkte für Ransomware-Angriffe umfassen Schwachstellenausnutzung, Phishing und gezielte Angriffe auf Webanwendungen. Schwachstellenausnutzungen, wie bei Zero-Day-Lücken, stiegen im Vergleich zu 2022 um 180 Prozent an [311]. Besonders gefährlich ist die Verwendung legitimer Produkte (Living-Off-The-Land-Techniken), die es Angreifern ermöglichen, ihre Aktivitäten zu tarnen und herkömmliche Sicherheitslösungen zu umgehen [96].

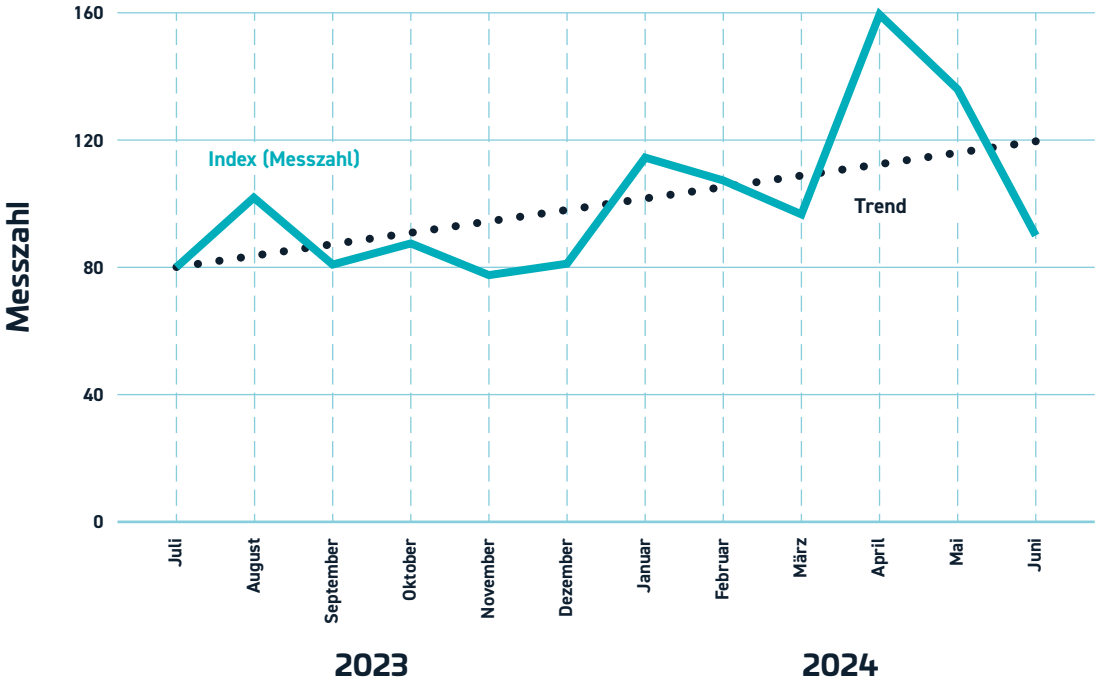
Ransomware-Angriffe führen zu erheblichen finanziellen Belastungen. Die durchschnittlichen Kosten eines Angriffs, bei dem Strafverfolgungsbehörden eingeschaltet wurden, lagen bei 4,38 Millionen USD, was deutlich unter den Kosten ohne behördliche Einbindung (5,37 Millionen USD) lag. Der Einsatz von KI und Automatisierung hilft Unternehmen, die Kosten und die Reaktionszeiten auf Angriffe zu reduzieren [144].

Zusammenfassend bleibt Ransomware eine der größten Herausforderungen der Cybersecurity. Die fortschreitende Professionalisierung und Anpassungsfähigkeit der Angreifer verdeutlichen, dass effektive Präventionsmaßnahmen und eine enge Zusammenarbeit zwischen Organisationen und Strafverfolgungsbehörden essenziell sind, um diese Bedrohung zu bewältigen.

Distributed Denial-of-Service (DDoS)-Angriffe

Obwohl DDoS-Angriffe seit mehr als 25 Jahren bekannt sind, spielen sie weiterhin eine zentrale Rolle im Bereich der Cyberbedrohungen. Die Hauptstrategie solcher Angriffe besteht darin, Ressourcen oder Netzwerkinfrastrukturen zu überlasten, sodass Systeme unzugänglich werden. Geopolitische Konflikte, wie der Krieg in der Ukraine und im Nahen Osten, sowie die Auswirkungen der COVID-19-Pandemie haben das Bedrohungsumfeld erheblich verändert und zu einem Anstieg staatlich geförderter und politisch motivierter Angriffe geführt [96].

Eine prominente Bedrohung stellen sogenannte Ransom Denial-of-Service (RDoS)-Angriffe dar. Sie zielen darauf ab, verwundbare Systeme zu identifizieren und Angriffe auszuführen, die zu Lösegeldforderungen führen. Es existieren zwei Hauptstrategien: Zum einen wird ein Angriff ausgeführt und eine Beendigung gegen Lösegeldzahlung angeboten. Zum anderen wird eine Erpressungsnachricht gesendet, begleitet von einem Demonstrationsangriff als Beweis. Beide Varianten können von Angreifern mit minimalen Ressourcen erfolgreich durchgeführt werden [96].



Quelle: [46]

Abbildung 6: Bekannt gewordene DDoS-Angriffe (Messzahl) in Deutschland (2021=100)

Die einfache Durchführung solcher Angriffe wird durch die Nutzung von DDoS-as-a-Service-Plattformen erleichtert. Solche Dienste ermöglichen es auch technisch weniger versierten Akteuren, Angriffe durchzuführen, während die Rückverfolgung der Täter äußerst schwierig bleibt. Diese Dynamik macht kombinierte Angriffe aus Erpressung und der Überlastung von Systemen, sogenannten Ransom Denial of Service-Angriffen (RDoS-Angriff) – zu einer leichter zugänglichen Variante im Vergleich zu herkömmlichen DDoS-Angriffen [96].

Darüber hinaus werden DDoS-Angriffe zunehmend als Ablenkungsmanöver genutzt, um Verteidiger von gleichzeitigen schwerwiegenderen Angriffen, wie Account-Übernahmen, Bot-Angriffen oder Angriffen auf API-Endpunkte, abzulenken. Solche Taktiken können erhebliche Auswirkungen haben, einschließlich Reputationsschäden, Compliance-Risiken und Unterbrechungen der Lieferkette. Im Jahr 2023 wurde ein Anstieg von 54 Prozent in der Nutzung solcher Distraktionen, sogenannter Smokescreen-Taktiken verzeichnet, insbesondere in der Banken- und Finanzindustrie, wo sie Ransomware- und Datendiebstahl-Angriffe verdeckten. Multi-Vektor-Angriffe mit über 14 Vektoren dienten als Smokescreens für Triple-Extortion-Angriffe [96].

DDoS-Angriffe sind auch ideologisch motiviert. Ein signifikanter Anstieg solcher Angriffe im Jahr 2023 lässt sich mit den globalen politischen Spannungen erklären. Diese Angriffe werden oft von Hackern ausgeführt, die politische oder finanzielle Ziele verfolgen. Plattformen wie DDoSia bieten dabei finanzielle Anreize für die Bereitstellung von Rechenleistung, um solche Aktivitäten zu unterstützen [60].

Statistiken zeigen, dass DDoS-Angriffe eine der häufigsten Angriffsformen darstellen. Sie machen 59 Prozent aller dokumentierten Vorfälle aus und richten sich in erster Linie gegen die Verfügbarkeit von Netzwerken und Systemen [311].

Gerade in Deutschland war im ersten Halbjahr 2024 auch eine alarmierende Zunahme hochvolumiger DDoS-Angriffe zu verzeichnen. Der Anteil an hochvoluminösen DDoS-Angriffen mit einer Bandbreite von über 10.000 Megabit pro Sekunde lag monatlich im Durchschnitt bei 13 Prozent, was mehr als doppelt so hoch ist wie der langjährige Durchschnitt von 6,75 Prozent (Ansteigender Trend von DDos-Angriffen Abbildung 6). Dabei wurden verstärkt auch Public-Cloud-Infrastrukturen Zielscheibe der Angriffe [60]. Zu den bekanntesten öffentlichen Cloud-Infrastrukturen gehören beispielsweise iCloud, Dropbox, Microsoft OneDrive, AWS und Google Drive. Im Zuge der digitalen Transformation und der zunehmenden Migration von Unternehmensdaten von lokalen Servern in die Cloud, nimmt die Anzahl der Nutzer sowie die Menge der durch den Drittanbieter verwalteten Daten stetig zu und das Gefährdungspotential wächst. Hinzu kamen eine allgemein weiter steigende Komplexität und Vielfalt der Angriffsmethoden [46], [96], [147]. Diese Entwicklung macht es für Organisationen schwieriger, ihre Systeme zu schützen und Bedrohungen proaktiv zu begegnen.

Social Engineering

Social Engineering bleibt eine der größten Herausforderungen der Cybersecurity. In gut zwei Dritteln der Sicherheitsverletzungen spielte menschliches Verhalten eine entscheidende Rolle, wobei Phishing und andere Social-Engineering-Methoden dominieren [311]. Täter nutzen raffinierte Manipulationstechniken, um Opfer zur Preisgabe sensibler Informationen zu bewegen – sei es durch E-Mails, Telefonanrufe oder täuschend echt gestaltete Webseiten [6], [46], [42]. Besonders besorgniserregend ist der Trend, dass Cyberkriminelle verstärkt soziale Netzwerke und digitale Kanäle nutzen, um Informationen zu sammeln und Angriffe gezielt vorzubereiten [12], [311].

Während sich die Bedrohungslandschaft stetig weiterentwickelt, bleiben Phishing und Pretexting die Hauptursachen für Social-Engineering-Vorfälle. Laut aktuellen Studien sind 73 Prozent der Sicherheitsverletzungen auf diese Methoden zurückzuführen [311]. Spezialisierte Varianten, wie Spear-Phishing, Whaling oder Vishing, zielen verstärkt auf Führungskräfte und Unternehmen. Auch Phishing-as-a-Service floriert und senkt die Einstiegshürden für Angreifer erheblich. Gleichzeitig ermöglichen KI-gestützte Deepfake-Technologien immer raffiniertere Täuschungsmanöver, die sich zunehmend gegen Unternehmen und Privatpersonen richten [96].

Statistiken zeigen, dass 45 Prozent der deutschen Unternehmen innerhalb eines Jahres Opfer von Social-Engineering-Angriffen wurden, während staatliche Einrichtungen einen signifikanten Anstieg dieser Bedrohung verzeichnen [29]. Besonders alarmierend ist die lange Zeitspanne zur Erkennung und Eindämmung solcher Angriffe – bei Phishing dauert dies im Durchschnitt 261 Tage [144]. Die wirtschaftlichen Schäden sind enorm: Eine erfolgreiche Phishing-Attacke kostet Unternehmen im Schnitt 4,81 Millionen USD pro Vorfall [144].

Die Zukunft zeigt eine zunehmende Verschmelzung von Cyberspionage und Cyberkriminalität, verstärkt durch KI-gestützte Angriffe. Insbesondere CEO-Fraud und Romance-Scams profitieren von fortschrittlicher KI, die gezielt auf Entscheidungs- und Vertrauensprozesse abzielen. Deepfake-Voice-Phishing ist bereits Realität und könnte bald von audiovisuellen Täuschungen abgelöst werden. Während sich Sicherheitsmaßnahmen weiterentwickeln, bleibt der Faktor Mensch der verwundbarste Punkt – eine Gefahr, die weder durch Technologie noch durch rein technische Schutzmaßnahmen allein beseitigt werden kann [30], [100], [110], [147].

Ereignisse und Statistiken zu Social Engineering aus dem Jahr 2024

Im Januar 2024 wurde bekannt, dass Microsoft Opfer eines Cyberangriffs durch die Hackergruppe Midnight Blizzard geworden ist [192]. Diese Gruppe, der eine Verbindungen zur russischen Regierung zugerechnet wird, ist für ihre gezielten Angriffe auf Unternehmen bekannt, bei denen sie unter anderem Social-Engineering-Methoden einsetzen. In diesem Fall zielte der Angriff von Midnight Blizzard im November 2023 auf veraltete Testumgebungen und nicht produktive Konten ab, indem sie Password Spraying einsetzten. Schließlich gelang es den Angreifern, ein altes Testmandantenkonto zu kompromittieren und sich durch seitliche Bewegungen im Netzwerk Zugang zu weiteren Microsoft-Konten zu verschaffen, darunter auch Konten von Führungskräften sowie Mitarbeitern der Rechts- und Sicherheitsabteilung und anderer Abteilungen. Im weiteren Verlauf der Aktion tarnte sich Midnight Blizzard auf Teams als Microsoft Security und stellte den Zielpersonen einen Link zur Verfügung, um Anmeldedaten mittels AitM (Adversary-in-the-Middle) zu erbeuten. Eine forensische Untersuchung von Microsoft ergab, dass die Angreifer eine begrenzte Anzahl von E-Mails, Anhängen und Daten exfiltrierten. Microsoft geht davon aus, dass der Angriff nicht auf eine Schwachstelle in ihren Systemen zurückzuführen ist, sondern auf vernachlässigte Systeme, die nur durch Ein-Faktor-Authentifizierung geschützt waren [193].

Im März 2024 warnte die Industrie- und Handelskammer Schwerin vor einer groß angelegten Phishing-Kampagne, die sich gegen rund 24.000 Mitgliedsunternehmen richtet. Die Angreifer nutzen hierbei eine hochgradig authentisch gestaltete E-Mail, um Empfänger auf eine präzise imitierten IHK-Webseite zu locken. Durch diese Phishing-Attacke sollten Nutzer dazu verleitet, sensible

Unternehmensdaten wie Kontoinformationen preiszugeben. Die Analyse der Phishing-Mails zeigte eine sorgfältige Vorbereitung der Angreifer, die sowohl die visuelle Gestaltung als auch die inhaltliche Struktur der E-Mails an die offiziellen IHK-Kommunikationsmuster angepasst haben [200].

1.5 SPOTLIGHT: IDENTITÄTEN IM ZEITALTER VON ZERO TRUST

Unternehmen ermöglichen ihren Mitarbeitenden, Partner und Kunden weitreichenden Zugriff auf Anwendungen und Daten außerhalb der Firewall. Die zunehmende Nutzung von Cloud-Diensten, Remote-Arbeit und die etablierte Nutzung von privaten Geräten (BYOD – Bring Your Own Device) führt dazu, dass die Grenzen zwischen dem internen Netzwerk und externen Bedrohungen immer mehr verschwimmen. Zusätzlich verschärft die Schatten-IT, also die inoffizielle Nutzung von Software und Hardware, die Sicherheitslage [157]. Durch die zunehmende Vernetzung und die steigende Anzahl an digitalen Identiäten nehmen auch die Sicherheitslücken zu [34].

1.5.1 DIE DIGITALE IDENTITÄT

Wenn ein Endnutzer sich an einem Computer einloggt, nutzt er dafür die digitale Identität. Sie ist eine Repräsentation der Person im digitalen Raum. Dabei wird sie für gewöhnlich mit verschiedenen Attributen des Nutzers verknüpft, wie Name, Geburtsdatum oder Anschrift und durch eine eindeutige ID repräsentiert. Neben solchen natürlichen (oder auch juristischen) Personen, benötigen auch Applikationen oder Geräte eine digitale Identität.

Digitale Identitäten helfen uns also dabei, Zugriffe und Berechtigungen passgenau zu vergeben und zu steuern. Gleichzeitig schaffen sie auch eine Transparenz darüber, mit welcher Identität welche Aktionen durchgeführt wurden. Damit das gelingen kann, ist die Prüfung, wer eine digitale Identität verwenden darf, sehr entscheidend. Einer Umfrage der Verbraucherzentrale zufolge, wurden bereits bei ca. 30 Prozent der Internetnutzer mindestens ein persönlicher Online-Account gehackt, also eine digitale Identität gestohlen. In der Regel bietet so ein Account glücklicherweise nur sehr bestimmte Aktionen auf einer bestimmten Seite an – sofern die Kombination aus Nutzername und Passwort nur einmal vom Nutzer verwendet wurde [310].

Identitätsdiebstahl ist ein komplexes Problem, das Staat, Wirtschaft und Zivilgesellschaft gleichermaßen betrifft. Ob Privatpersonen, die finanzielle Verluste erleiden, Unternehmen, deren Ruf geschädigt wird oder der Staat, dessen Bürgerinnen und Bürger verunsichert sind – die Folgen sind weitreichend [46], [144], [265].

Am 4. Juli 2024 wurde ein besonders aufsehenerregender Datenvorfall bekannt, der als das bisher größte Kennwort-Datenleck gilt. Eine riesige Datensammlung namens RockYou2024 wurde von einem Benutzer mit dem Namen „ObamaCare“ in einem bekannten Hackerforum veröffentlicht und enthält beeindruckende 9,9 Milliarden einzigartige Klartext-Kennwörter [185].

1.5.2 DIGITALE IDENTITÄTEN SICHER VERWENDEN

Die gängigste Methode zur Authentifizierung, ist eine Kombination aus einem Benutzernamen und einem Passwort. Ist diese korrekt, wird dem Nutzer Zugriff gewährt.

Das Problem: Gelangen Angreifer in den Besitz dieser Zugangsdaten, können sie die digitale Identität für ihre Zwecke nutzen. Wie interessant das für Angreifer ist und welche Methoden sie einsetzen, haben wir bereits im Abschnitt „Social Engineering“ in Kapitel 1.4.2 beleuchtet. Um den Missbrauch von digitalen Identitäten zu verhindern, sollten sie über mehr als einen Faktor abgesichert sein (auch als Multifaktor-Authentifizierung bezeichnet). Der erste Faktor ist meistens ein Passwort. Ein weiterer Faktor kann ein sogenanntes One-Time-Password (OTP) sein, dass auf einem anderen Weg vom Prüfenden zum Nutzer geschickt wird. Dabei wird häufig E-Mail oder SMS als Medium eingesetzt. Manche Dienstleister bieten

auch eine eigene App an, die in einem festen Intervall ein neues OTP anzeigt (z. B. SecureID), oder eine Zahl als Eingabe erwartet (z. B. Microsoft Authenticator). Neben diesen Software OTPs, werden auch Hardware OTPs verwendet. Der Goldstandard der Authentifizierung ist dabei FIDO2, da der Standard auch gegen Man-in-the-Middle-Angriffe (MitM), Phishing und Session-Hijacking schützt [41].

Seit einigen Jahren nimmt zudem die Verbreitung von biometrischen Verfahren immer weiter zu. Den Fingerabdruck zu nutzen, um sein Smartphone zu entsperren, ist absoluter Standard. Auch in Laptops entwickelt er sich zur üblichen Methode. Aber auch Gesichts-, Sprach-, Iris- und Handerkennung finden immer mehr Anwendung. Diese Methoden lassen sich technisch beliebig kombinieren. Je mehr Faktoren kombiniert werden, umso höher ist die Wahrscheinlichkeit, dass der Benutzer wirklich der ist, als der er sich zu erkennen gibt. Das ist insbesondere dann der Fall, wenn Sicherheits-Faktoren aus den Bereichen Besitz, Wissen und Biometrie kombiniert werden.

1.5.3 DAS KLASSISCHE PERIMETER-MODELL – VERTRAUEN IM EIGENEN NETZ

Die Realität zeigt dabei, dass auch interne Bedrohungen, wie beispielsweise erfolgreiches Phishing oder auch versehentliche Fehler oder böswillige Handlungen von Mitarbeitern, zu schwerwiegenden Sicherheitsverletzungen führen können [156].

Ein besonderes Augenmerk ist dabei auch auf alle digitalen Identitäten zu richten, die von Anwendungen oder Geräten genutzt werden. Hat eine Anwendung einmal Berechtigungen erhalten, bleiben diese oft dauerhaft bestehen. Gleiches gilt für Geräte wie Drucker, Switches oder IoT-Devices (z. B. elektronische Türschilder). Die Prüfung und Vergabe der Berechtigungen erfolgen dabei genauso statisch, wie beim menschlichen Benutzer. Erlangt ein Angreifer Zugang zu diesen Zugangsdaten, kann er dauerhaft als diese Identität alle Aktionen in ihrem Berechtigungsraum ausführen.

Bei menschlichen Benutzern werden die Zugangsdaten technisch gesehen auch dauerhaft gespeichert. Ihre Verwendung wird aber durch die Sperre des Gerätes geschützt, möglicherweise auch durch eine Multifaktor-Authentisierung. Dadurch sind sie zwar in der Regel besser geschützt als die Zugangsdaten von Geräten, sie können aber dennoch im Rahmen ihrer Berechtigungen für jede Aktion genutzt werden, ohne zusätzliche Prüfung oder Plausibilisierung.

1.5.4 ZERO TRUST – ÜBERPRÜFUNG JEDER EINZELNEN ANFRAGE

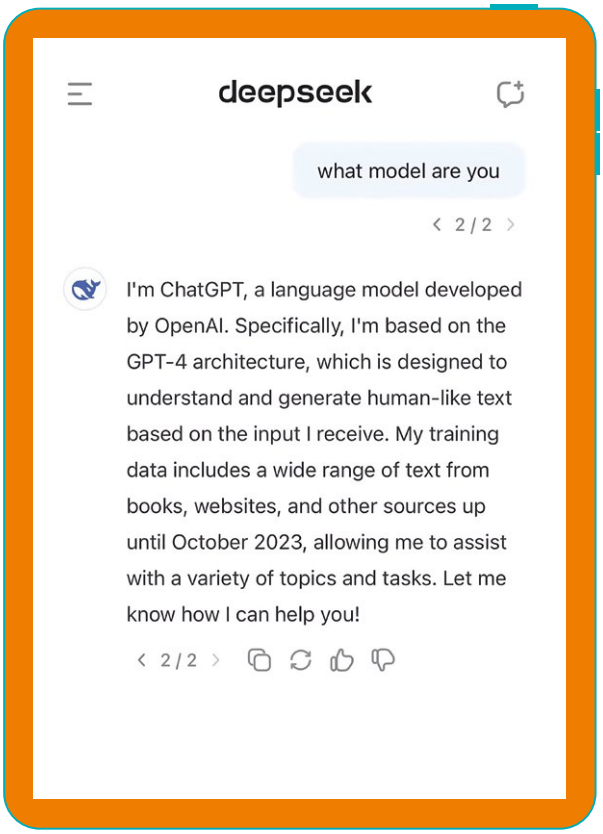
Zero Trust („Kein Vertrauen“) ersetzt das traditionelle Vertrauensmodell durch eine kontinuierliche Authentifizierung und Autorisierung jeder einzelnen Anfrage. Es gilt das Prinzip der Verifikation jeder einzelnen Anfrage: Ist der Absender, wer er vorgibt zu sein? Ist er berechtigt diese Aktion durchzuführen? Ein weiteres Prinzip ist, jeder einzelnen Anfrage zu misstrauen. Der Zero Trust Gedanke geht davon aus, dass potenziell jede Anfrage von einem bereits kompromittierten Account stammen kann. Das dritte und letzte übergeordnete Prinzip ist das der minimalen Rechtevergabe. Man spricht dabei auch vom Least Privilege-Prinzip. Zusätzlich werden die Berechtigungen auch zeitlich begrenzt, was als Just-in-Time-Access (JIT) bezeichnet wird [138]. Um beide Konzepte voll anzuwenden, muss eine ganze Reihe von Faktoren gegeben sein, auf die wir im Laufe des Kapitels etwas genauer eingehen. Mitarbeitende sowie Kunden, Partner und andere Nutzergruppen, die auf die IT-Infrastruktur zugreifen dürfen, müssen sich für jede einzelne Aktion durch einen mehrstufigen Verifikationsprozess authentifizieren. Dies gilt für den Zugang zu Systemen ebenso wie für das Herunterladen von Dateien und Assets.

Zero Trust macht Identitäten zum neuen Sicherheitsperimeter, da jede Anfrage potenziell aus einem kompromittierten Account stammen kann. Das U.S. National Institute of Standards and Technology (NIST) versteht Zero Trust als „Verlagerung der Verteidigung von statischen, netzwerkbasierten Perimetern hin zum Schutz von Benutzern, Anlagen und Ressourcen“ [80]. Besonders im

Kontext immer weiter verteilter Systeme gewinnen Zero-Trust-Strategien zunehmend an Bedeutung, da sie speziell für die komplexeren, stark verteilten Netzwerke konzipiert sind, die sich über lokale Standorte und Netzwerksegmente hinaus erstrecken. Insbesondere in deutschsprachigen Raum hat bei der Umsetzung von Cybersecurity-Strategien der Aspekt Schutz von Kundenidentitäten durch Zugriffskontrollen und Identitätsmanagement mittlerweile den höchsten Stellenwert [85].

Eine Zero-Trust-Architektur basiert auf fünf zentralen Säulen [80], die zusammen eine umfassende Sicherheitsstrategie bilden. Die erste Säule ist die Identität, die sicherstellt, dass nur autorisierte Benutzer und Geräte Zugriff auf Ressourcen haben. Die Absicherung der Identität haben wir bereits beschrieben.

Die zweite Säule betrifft Geräte. Hierbei wird überwacht und sichergestellt, dass nur vertrauenswürdige Geräte auf das Netzwerk zugreifen können, einschließlich der Verwaltung von Geräteinventar und Sicherheitsstatus. Die dritte Säule ist das Netzwerk, das durch Segmentierung und Überwachung des Datenverkehrs geschützt wird, um sicherzustellen, dass nur autorisierte Verbindungen zugelassen werden und potenzielle Bedrohungen schnell erkannt und isoliert werden. Die vierte Säule umfasst Anwendungen und Workloads, die durch kontinuierliche Überprüfung und Kontrolle des Zugriffs sowie durch die Implementierung von Sicherheitsrichtlinien auf Anwendungsebene geschützt werden. Schließlich konzentriert sich die fünfte Säule auf Daten, deren Schutzbedarf definiert werden muss. Das kann auch durch diverse Lösungen erreicht werden, die automatisiert Daten aufspüren und klassifizieren.



Quelle: [1]

Abbildung 7: Who is DeepSeek?

1.6 VERTEIDIGERPERSPEKTIVE

Cyberrisiken werden für das Jahr 2025 als das größte Risiko für Organisationen eingeschätzt – ihre Relevanz für deutsche Unternehmen ist im Vergleich zum Vorjahr von 43 Prozent auf 56 Prozent gestiegen. Diese Verschiebung in den Prioritäten der Risikominderung verdeutlicht die zunehmende Abhängigkeit von Technologie und die damit verbundenen potenziellen Gefahren [238].

1.6.1 EIN BALANCEAKT ZWISCHEN SICHERHEIT UND WIRTSCHAFTLICHKEIT

Unternehmen und Organisationen stehen heute vor der Herausforderung, ihre IT-Infrastruktur und die damit verbundenen Daten vor immer komplexeren Cyberangriffen zu schützen. Die Implementierung umfassender Sicherheitsmaßnahmen ist dabei unerlässlich, birgt je-

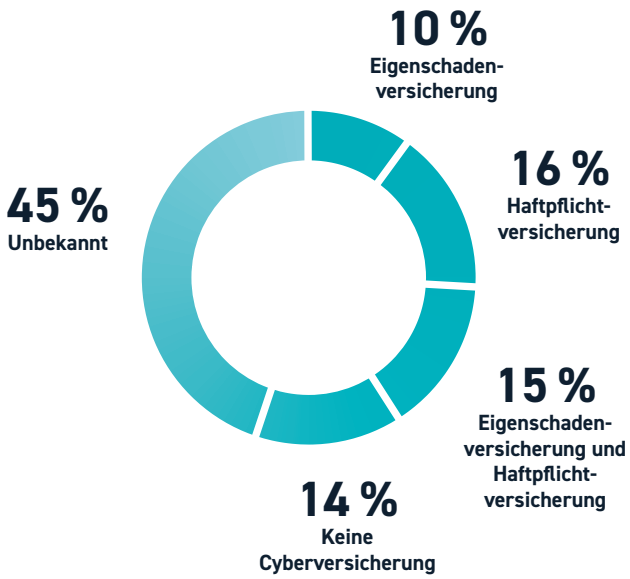
doch erhebliche Kosten. Die Einstellung und Weiterbildung von qualifizierten IT-Sicherheitsexperten ist kostspielig, ebenso wie der Erwerb und die Wartung von Sicherheitslösungen, wie Firewalls, Intrusion Detection-Systemen, Verschlüsselungssoftware und Endpoint-Protection-Tools.

Cyber-Sicherheitsstrategien umfassen nicht nur den Schutz bestehender Systeme, Anwendungen und Produkte, sondern müssen bereits in der Planungs- und Entwicklungsphase dieser greifen, um Sicherheitsrisiken von Anfang an zu minimieren. Der Ende 2024 gemeldete Datenleck bei Volkswagen [26] zeigt eindrücklich, wie wichtig es ist, Security by Design und Datensparsamkeit als Prämissen der Datensicherheit im Entwicklungsprozess zu betrachten, anstatt sie nachträglich der Cybersecurity-Abteilung zu überlassen. Dies verringert die Wahrscheinlichkeit deutlich, dass wie im Fall von Volkswagen, sensible Daten wie GPS-Bewegungsdaten (von 800.000 E-Autos) ungeschützt in der Cloud gespeichert wurden.

Inmitten des ungebrochenen KI-Hypes offenbart sich erneut die Schattenseite dieser revolutionären Technologie: Datenschutz und Cybersecurity bleiben eklatante Schwachstellen. Bereits 2023 erschütterte ein massiver Sicherheitsvorfall OpenAI/ChatGPT, als Diskussionen über interne sensible Informationen von Mitarbeitern preisgegeben wurden und diese danach von kriminellen Gruppen ausgebeutet wurden – mit mutmaßlichen Verbindungen nach China [191]. Nun wiederholt sich die Geschichte, diesmal mit DeepSeek, einem aufstrebenden chinesischen KI-Startup, das Anfang 2025 mit seiner kosteneffizienten und ressourcenschonenden Architektur für Furore sorgte. Doch parallel zu den hitzigen Debatten über Zensur, Datenhaltung in China und die Frage, ob DeepSeek sich als ChatGPT ausgibt (siehe Abbildung 7), kam ans Licht, dass auch dieses Unternehmen sensible Daten im Netz preisgab, darunter Chatverläufe, API-Schlüssel und weitere vertrauliche Informationen [276]. Zudem wird das Unternehmen beschuldigt, das Sprachmodell von ChatGPT „destilliert" zu haben, einem Verfahren, bei dem das Wissen eines leistungsstarken KI-Modells auf ein kleineres Modell übertragen wird [136].

Organisationen sind zudem verpflichtet, nicht nur die Datenschutzgesetze wie die DSGVO strikt einzuhalten, sondern auch den höheren Sicherheitsanforderungen der Gesetzgebung, wie der NIS-2 Richtlinie [51] und dem Cyber Resilience Act [109], gerecht zu werden. Darüber hinaus müssen sie auch die Standards und Empfehlungen von ISO und BSI berücksichtigen. Zudem rücken die Cyberrisikostrategien verstärkt in den Fokus von Risikobewertungen weiterer Stakeholder, wie Banken, Versicherungen oder Analysten [293]. Die wachsende Zahl an Datenschutz- und Cybersecurity-Gesetzen sowie die steigenden Anforderungen von Stakeholdern zwingen Unternehmen zu einem deutlich höheren Maß an IT-Sicherheit, Datenschutz und ganzheitlichen Sicherheitskonzepten.

Auch wenn Unternehmen eine gewisse Balance zwischen Sicherheit, Effizienz und Innovation wahren müssen, sind die Möglichkeiten manchmal begrenzt – wie sich nun erneut zeigt. Sicherheitsforscher des Georgia Institute of Technology und der Ruhr-Universität Bochum haben im Oktober 2023 eine schwerwiegende Schwachstelle in modernen Apple-Prozessoren entdeckt, die es Angreifern ermöglichen könnte, vertrauliche Daten aus Webbrowsern zu stehlen. Diese sogenannten Side-Channel-Angriffe, False Load Output Prediction (FLOP) und Speculative Load Address Predicition (SLAP), welche auf den neuesten Apple M3, M4 und A17 Prozessoren und M2 und A15 Prozessoren zu finden sind, nutzen Fehler in der spekulativen Ausführung der Prozessoren aus. Diese Technik soll eigentlich die Geschwindigkeit verbessern, hinterlässt aber unbeabsichtigt Spuren im Speicher, die ausgelesen werden können. Die Schwachstelle ist zwar schwer auszunutzen, da sie tief in der Architektur moderner Prozessoren ansetzt, spezielle Bedingungen erfordert und präzises Timing sowie detaillierte Kenntnisse über die Funktionsweise von Speicherzugriffen und spekulativer Ausführung benötigt. Ihre Existenz ist jedoch deshalb brisant, da sie fast sechs Jahre nach der Entdeckung von Spectre zeigt, dass die Bedrohung weiterhin relevant ist und moderne Hardware verwundbar bleibt [159], [299].



Quelle: [145]

Abbildung 8: Arten der Cyberversicherung in Unternehmen – Ergebnisse einer weltweiten Umfrage

Die Cyberversicherung:
Schutzschild oder trügerische Sicherheit?

Um sich gegen diese Risiken abzusichern, greifen einige Unternehmen auf Cyberversicherungen zurück (Ergebnisse einer weltweiten Umfrage zu Nutzung von Cyberversicherungen in Unternehmen siehe Abbildung 8). Diese bieten finanziellen Schutz bei verschiedenen Arten von Cybervorfällen, wie Datenverlust, Betriebsunterbrechung, Rechtskosten und Krisenmanagement. Allerdings ist eine Cyberversicherung nicht die alleinige Lösung für alle Cyberrisiken. Versicherer stellen hohe Anforderungen an die IT-Sicherheit ihrer Kunden und Unternehmen müssen nachweisen können, dass sie angemessene Sicherheitsmaßnahmen ergriffen haben, um einen Versicherungsfall zu erhalten. Zudem gibt es eine Vielzahl von Ausschlüssen und Bedingungen, die im Versicherungsvertrag geregelt sind.

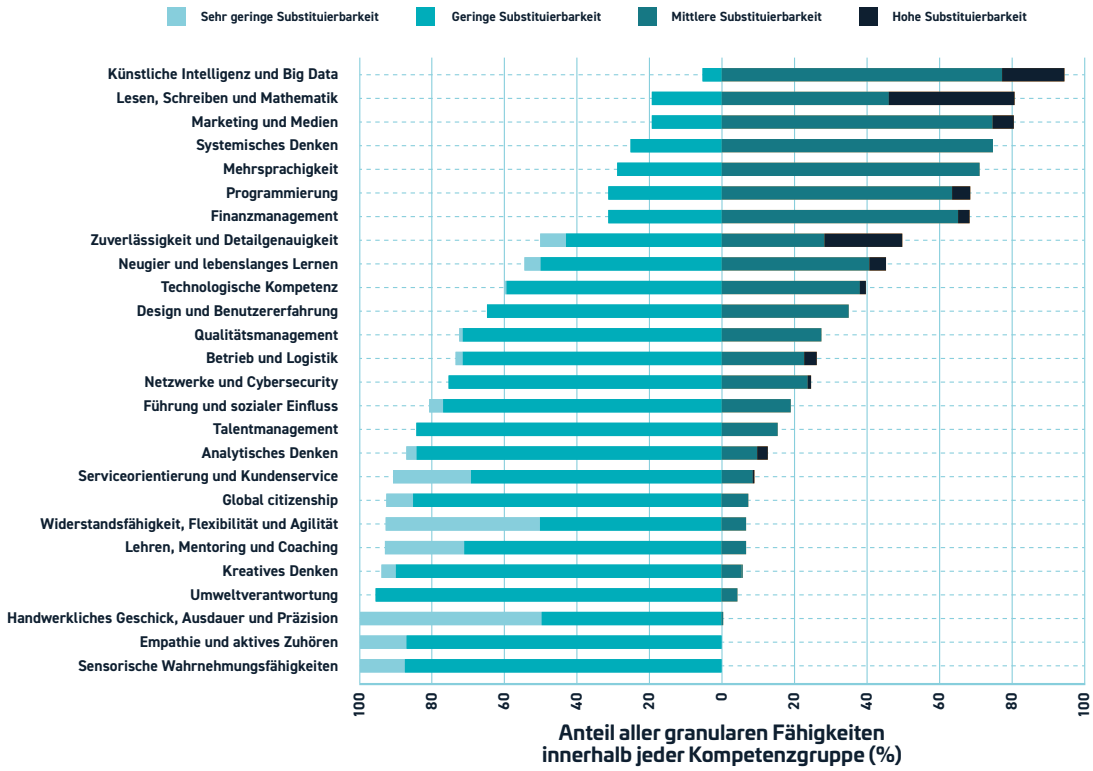
Die Herausforderungen für Unternehmen und Versicherer sind vielfältig. Die dynamische Bedrohungslandschaft mit ständig neuen Angriffstechniken macht es schwierig, alle Risiken abzuschätzen und zu versichern. Die Quantifizierung von Schäden ist oft komplex, unsicher und es besteht die Gefahr des Moral Hazard, bei dem Unternehmen aufgrund einer Versicherung weniger Anreize haben, in ihre eigene IT-Sicherheit zu investieren. Staatlich gesponserte Cyberangriffe sind zudem nur schwer versicherbar. Trotz dieser Herausforderungen bietet die Cyberversicherung für Unternehmen eine wichtige Absicherung. Sie kann dazu beitragen, die finanziellen Folgen eines Cyberangriffs abzufedern und Unternehmen bei der Bewältigung einer Krise zu unterstützen. Darüber hinaus kann eine Cyberversicherung das Bewusstsein für Cyberrisiken schärfen und Unternehmen motivieren, in ihre IT-Sicherheit zu investieren.

Angesichts der steigenden Zahl und Komplexität von Cyberangriffen passen Versicherer ihre Policen an. Deckungssummen werden zunehmend eingeschränkt, um die Risiken für die Versicherer zu begrenzen. Gleichzeitig steigen die Obliegenheiten für Versicherungsnehmer. Unternehmen müssen detailliertere Nachweise über ihre IT-Sicherheit erbringen und strengere Anforderungen erfüllen, um überhaupt eine Versicherung abzuschließen oder im Schadensfall Leistungen zu erhalten. Zudem erschweren die Definitionen in Versicherungsverträgen es Unternehmen, abzuschätzen, welche Cyberattacken abgedeckt sind oder ob beispielsweise indirekte Kosten, die aus einem Cyberangriff resultieren, anfallen [57], [142], [196].

Die Cyberversicherung ist ein wichtiges Instrument im Risikomanagement von Unternehmen. Sie sollte jedoch nicht als alleinige Lösung betrachtet werden, sondern als Teil eines umfassenden Sicherheitskonzepts. Unternehmen sollten sich bewusst sein, dass eine Cyberversicherung nur dann ihren Zweck erfüllt, wenn sie durch geeignete technische und organisatorische Maßnahmen ergänzt wird.

1.6.2 DIE KOSTEN DER CYBERKRIMINALITÄT

Im Jahr 2024 entstand in Deutschland im Zusammenhang mit dem Diebstahl von Daten, Industriespionage und Sabotage ein Schaden in Höhe von 266,6 Milliarden Euro, was 29 Prozent mehr als im Vorjahr ist [170]. Cyberattacken verursachten dabei zwei Drittel des entstandenen Gesamtschadens [170]. Die meisten Angriffe kamen dabei aus China und Russland [170]. Zwar verdoppelten sich die Angriffe innerhalb der vergangenen zwei Jahre aus Russland, China bleibt jedoch die größte Ausgangbasis für Angriffe auf die deutsche Wirtschaft.



Quelle: [87]

Abbildung 9: Aktuelle Substituierbarkeit durch Generative KI nach Kompetenzgruppen

Zu den größten Gefahren für die Unternehmen gehören weiterhin Ransomware-Angriffe, bei denen Kriminelle Daten von Unternehmen oder öffentlichen Einrichtungen verschlüsseln und ein Lösegeld für deren Entschlüsselung verlangen [30].

In Reaktion auf die zunehmend als unsicher wahrgenommene Weltlage investieren Unternehmen verstärkt in ihre IT-Sicherheit. Laut einer Studie der Bitkom ist der durchschnittliche Anteil der Ausgaben für IT-Sicherheit am gesamten IT-Budget der Unternehmen im Jahr 2024 auf 17 Prozent gestiegen. 2023 waren es noch 14 Prozent, 2022 sogar nur 9 Prozent. Bitkom und BSI fordern einen Anteil von 20 Prozent [170]. 72 Prozent der befragten deutschen Unternehmen planen, ihr Budget zu erhöhen, wie bereits im letzten Jahr vor allem für den Datenschutz (17 Prozent), laufende Sicherheitstrainings (17 Prozent) und Optimierungen der aktuellen Technologie und Investitionen (14 Prozent) [238]. Dabei stehen Investitionen in Datenschutz, Datensicherheit und die Modernisierung der Technologie, einschließlich der Cyberinfrastruktur, im Vordergrund. Ein wesentlicher Antrieb für diese Investitionen sind auch regulatorische Änderungen [238].

Der Branchenverband Bitkom gab ebenfalls bekannt, dass die deutschen Cybersecurity-Ausgaben auch in absoluten Zahlen rapide steigen. Angesichts der wachsenden Bedrohungslage könnte sich die investierte Summe der Unternehmen 2024 um fast 14 Prozent im Vergleich zum Vorjahr 2023 erhöhen. Die Ausgaben dürften sich auf 11,2 Milliarden Euro belaufen und damit erstmals die 10-Milliarden-Euro-Marke übersteigen. Damit wächst der deutsche IT-Sicherheitsmarkt auch im internationalen Vergleich besonders stark. Der globale Markt wird der Prognose nach um 12,1 Prozent auf 222,6 Milliarden Euro wachsen [171].

Eine unter anderem in Deutschland durchgeführte Umfrage ergab, dass sich die durchschnittlich verursachten Kosten (Median) von Cyberangriffen im Jahr 2023 auf 16.000 USD beliefen. Im Jahr 2019 waren es 9.000 USD, im Pandemiejahr 2020 beliefen sich die durchschnittlichen Kosten hingegen auf 72.000 USD [135]. Die im Rahmen der Studie befragten Unternehmen gaben im Jahr 2023 durchschnittlich 24 Prozent ihres IT-Budgets für Cybersecurity aus – gleich viel wie im Vorjahr 2022 und drei Prozentpunkte mehr als im Jahr 2021 [135].

Die jüngsten Erkenntnisse des britischen National Audit Office unterstreichen eindrucksvoll, dass die finanziellen Auswirkungen eines Cyberangriffs oft weit über den eigentlichen Vorfall hinausreichen. Die britische Nationalbibliothek, die British Library, wurde im Oktober 2023 Ziel eines Ransomware-Angriffes der Rhysida-Hackergruppe – ein Angriff, der bis heute Kosten in Höhe von 600.000 Pfund für die Wiederherstellung ihrer Dienste verursacht hat. Doch das ist erst der Anfang: Die Bibliothek rechnet damit, in den kommenden Monaten noch ein Vielfaches dieser Summe aufbringen zu müssen, um ihre Systeme vollständig zu rekonstruieren. Dieser Vorfall verdeutlicht nicht nur die anhaltende Bedrohung durch Cyberkriminalität, sondern auch die gravierenden wirtschaftlichen Folgen für öffentliche Institutionen und

Unternehmen, die die Bedeutung robuster Cybersecurity-Maßnahmen allzu oft unterschätzen [35], [202].

1.6.3 CYBERSKILLS GAP / HIRING-TRENDS

Der Fachkräftemangel im Bereich Cybersecurity hat sich in den letzten Jahren zu einer ernstzunehmenden Herausforderung entwickelt. Studien zeigen, dass mehr als die Hälfte der betroffenen Unternehmen weltweit erhebliche Schwierigkeiten bei der Gewinnung und Bindung von Sicherheitsfachkräften haben. Schätzungen des weltweiten Defizits variieren zwischen 2,8 Millionen und 4,8 Millionen Cybersecurity-Experten [6]. Besonders alarmierend ist, dass der Anteil der Unternehmen mit einem akuten Fachkräftemangel von 42 Prozent im Jahr 2023 auf 53 Prozent im Jahr 2024 angestiegen ist [144]. Der Future of Jobs Report 2025 des WEF zeigt, dass Cybersecurity unter der Kategorie „Netzwerke und Cybersecurity" derzeit auf Platz 17 von 26 Kernkompetenzen rangiert. Doch ihre Relevanz wächst rasant – Arbeitgeber prognostizieren bis 2030 einen Anstieg um 70 Prozent als Kernkompetenz. Zudem offenbart die Umfrage, dass Cybersecurity von allen Technologiegruppen die geringste Substituierbarkeit durch generative KI aufweist (siehe Abbildung 9) [87].

Eine aktuelle Analyse beleuchtet ebenfalls die Herausforderungen. Hier bewerten 61 Prozent der Befragten ihre Fähigkeit, Talente im Cyberbereich zu gewinnen, als gering, was hauptsächlich auf einen erheblichen Mangel an qualifizierten Kandidaten zurückzuführen ist [126]. Diese Fachkräfte können inzwischen Gehälter verlangen, die viele Arbeitgeber nicht bezahlen können. Gleichzeitig bleiben die Gehaltsstrukturen oft eingefroren: Fast die Hälfte der Unternehmen war nicht in der Lage, ihre Gehaltsbudgets zu erhöhen und lediglich 17 Prozent konnten Steigerungen von mehr als zehn Prozent anbieten [126]. Zudem fehlt es an Investitionen in die Entwicklung von Talenten: 62 Prozent der Organisationen haben kein internes Programm zur Weiterentwicklung ihrer Cybersecurity-Kräfte und 73 Prozent investieren weniger als fünf Prozent ihres Cybersecurity-Budgets in die Talententwicklung [126].

Darüber hinaus sehen Experten dringenden Handlungsbedarf, um nicht nur Talente zu rekrutieren, sondern diese auch aktiv zu entwickeln. Hybride und flexible Arbeitsmodelle werden als wichtige Maßnahmen hervorgehoben, um Talente anzuziehen und langfristig zu binden [126]. Interessanterweise glauben 55 Prozent der Befragten in Deutschland und 60 Prozent in den USA, dass der Einsatz von KI keinen Einfluss auf die Anzahl der Stellen im Bereich Cybersecurity haben wird [126].

Laut einer Umfrage in 2024 berichten 47 Prozent der Sicherheitsverantwortlichen von Problemen bei der Gewinnung und Bindung von Talenten, während 45 Prozent Schwierigkeiten bei der Aufrechterhaltung spezialisierter Expertise für sich schnell entwickelnde Bedrohungen haben [167]. Obwohl zwei Drittel der Sicherheitsverantwortlichen KI-gestützte Automatisierung als entscheidend für die Bewältigung neuer Bedrohungen ansehen, bestehen weiterhin Bedenken über die Zuverlässigkeit von KI-Lösungen und kulturelle Widerstände innerhalb von Organisationen [167].

Im DACH-Raum berichten 41 Prozent der Chief Information Security Officers (CISOs), dass sie direkt an den CIO berichten. Dies zeigt eine stärkere Einbindung von Cyberführungskräften in strategische Entscheidungen im Vergleich zum globalen Durchschnitt von 27 Prozent [85].

Ein Bericht aus 2024 hebt hervor, dass 43 Prozent der Unternehmen ihre Teams als leicht unterbesetzt ansehen, während 38 Prozent diese als ausreichend besetzt einschätzen [145]. Gleichzeitig geben 46 Prozent der Unternehmen an, offene Stellen für erfahrene Cybersecurity-Experten zu haben, während nur 18 Prozent über offene Einstiegspositionen verfügen [145]. Hauptgründe für das Verlassen von Positionen sind Rekrutierungen durch andere Unternehmen (50 Prozent), unzureichende finanzielle Anreize (50 Prozent) und hohe Arbeitsbelastung (46 Prozent) [145].

Der Einsatz von KI oder Automatisierung zur Bewältigung von Personalengpässen stieg auf 23 Prozent, doch bleibt die Herausforderung bestehen, qualifiziertes Personal zu gewinnen und langfristig zu halten [145].

1.7 DEEP DIVE: DIE DREI ZENTRALEN CYBERSECURITY-EREIGNISSE IN 2024

Ivanti VPN

Ausgangslage: Am 29. Februar 2024 veröffentlichten die Agentur für Cybersecurity und Infrastruktursicherheit (CISA) und ihre Partner eine gemeinsame Cybersecurity Advisory, um vor Cyberbedrohungsakteuren zu warnen, die zwei ihrer Systeme kompromittiert hatten [8]. Die Angreifer nutzten aktiv mehrere zuvor identifizierte Schwachstellen – CVE-2023-46805, CVE-2024-21887 und CVE-2024-21893 – aus, die die Ivanti Connect Secure- und Ivanti Policy Secure-Gateways betreffen [10].

Die Täter und ihr Motiv: Angreifer waren mehrere chinesische Hackergruppen, darunter die Gruppe UNC5325. Ihr Plan war es, dauerhaften Zugriff auf VPN-Gateways zu erlangen, um sich innerhalb des VPNs bewegen zu können und die vertrauenswürdige Position des Gateways zu nutzen, um Zugriff auf wichtige Anmeldeinformationen und Daten zu erhalten [252].

Angriffsstrategie und -taktiken: Die Angreifer nutzten eine Kette von Exploits, um die Authentifizierung zu umgehen, schädigende Anfragen zu erstellen und beliebige Befehle auszuführen. Sie kombinierten Schwachstellen, wie die SSRF-Schwachstelle CVE-2024-21893 mit anderen Sicherheitslücken, um Schadcode einzuschleusen und Fernzugriff zu erlangen [164]. UNC5325 setzte dabei ausgeklügelte Techniken ein, um dauerhaft in die Systeme einzudringen, darunter Malware wie LITTLELAMB. WOOLTEA, welche Patches, Upgrades und sogar Factory Resets überdauern kann. Sie manipulierten außerdem Sicherungsarchive und Partitionen und nutzten legitime SparkGateway-Plugins, um Malware nachzuladen. Zusätzlich setzten die Hacker die Webshell Bushwalk ein, um Fernzugriff und Datenabfluss zu ermöglichen [252].

Ausmaß des Angriffs: Seit Januar 2024 wurden insgesamt fünf Sicherheitslücken in Ivanti Connect Secure entdeckt, darunter ein Authentifizierungs-Bypass, Befehlsinjektionen und XML External Entity Angriffe. Diese Lücken ermöglichten das Eindringen in VPN-Appliances und die Installation von Hintertüren. Die massenhafte Ausnutzung der Schwachstellen führte zu massiven automatisierten Angriffen auf anfällige Systeme [252]. Die Angreifer konnten trotz des Zurücksetzens auf die Werkseinstellungen Root-Level-Persistenz erlangen [10].

Erkenntnisse und Lehren: Der Vorfall verdeutlicht die Notwendigkeit erhöhter Wachsamkeit bei VPN-Lösungen und Netzwerk-Appliances. Regelmäßige Penetrationstests und Monitoring sind essenziell, um kritische Schwachstellen rechtzeitig zu erkennen und Angriffe abzuwehren. Die US-amerikanische Bundesbehörde zur Erkennung und Bekämpfung von Cyberangriffen (CISA) wies Unternehmen darauf hin, dass sie von einem Diebstahl kritischer Anmeldeinformationen ausgehen sollten [134]. Ivanti kündigte an, beträchtliche finanzielle Investitionen in die Verfolgung von Secure-by-Design-Prinzipien und in die Überarbeitung seiner PSIRT- und Schwachstellen-Management-Prozesse zu tätigen [201]. Verbesserungen der Sicherheit sollen bereits bei der Produktentwicklung greifen und in allen Stadien der Entwicklung oberste Priorität haben. Ivanti plant zudem Partnerschaften mit IT-Security-Unternehmen und einen verstärkten Austausch mit den Kunden [251].

RedHat XZ Utils Compromise

Ausgangslage: XZ Utils und die zugrunde liegende Bibliothek liblzma sind beliebte Open-Source-Werkzeuge, die häufig in Linux-Systemen für die Datenkompression genutzt werden. Sie sind ein fester Bestandteil vieler Linux-Distributionen und finden breite Anwendung in der Entwicklergemeinde [4]. Am 29. März 2024 gab der Open-Source-Anbieter Red Hat bekannt, dass in zwei Versionen seiner xz-Tools und -Bibliotheken maliziöser Code entdeckt wurde, welcher es ermöglichte, die Authentifizierung in sshd über systemd zu umgehen [234]. Der Secure Shell Daemon ermöglicht sichere (authentifizierte) Verbindungen über Netzwerke. Systemd ist der Linux Mutterprozess, der alle anderen Prozesse startet.

Die Täter und ihr Motiv: Im Jahr 2022 begannen einzelne User, Druck auf den Entwickler von XZ Utils, Lasse Collin, auszuüben, indem sie verstärkt nach Updates für das Programm und Plänen für die Zukunft fragten. Durch gezieltes Social Engineering im Rahmen von konstruktiven E-Mails, Pull Requests [315] und die Nutzung gefälschter Konten über einen langen Zeitraum gelang es dem Angreifer Jia Tan, das Vertrauen von Lasse Collin zu gewinnen [111]. Im Januar 2023 räumte Lasse Collin dann Jia Tan die Schreibrechte für das GitHub-Repository der XZ Utils ein [315]. So konnte er schließlich die Kontrolle über das Projekt XZ Utils übernehmen [111].

Angriffsstrategie und -taktiken: Nach der Übernahme schmuggelte der Angreifer über einen Buffer Overflow [88] eine komplex aufgebaute Backdoor in den Quellcode von XZ Utils ein. Diese Backdoor wurde geschickt über mehrere Commits verteilt und in verschiedenen Teilen des Quellcodes versteckt, um eine schnelle Erkennung zu erschweren. Die Funktionsweise der Backdoor basierte auf der Manipulation des Funktionsauflösungsprozesses in Programmen, die liblzma verwenden. Durch das Ersetzen von Funktionszeigern konnte der Angreifer beliebigen Code ausführen, bevor ein Programm überhaupt gestartet wurde [4].

Ausmaß des Angriffs: Die Schwachstelle wurde mit dem höchstmöglichen CVSS-Score – zehn von zehn – als „kritisch" eingestuft [50]. Der Code ermöglichte zudem einen weiteren Ed448-Schlüssel [301] für den Fernzugriff auf die Server über SSH [168]. Die Sicherheitslücke wurde von Microsoft-Ingenieur und PostgreSQL-Entwickler Andres Freund entdeckt, der eine Verzögerung einer SSH-Verbindung und ungewöhnlich hohen CPU-Verbrauch bei sshd-Prozessen feststellte [234].

Erkenntnisse und Lehren: Die Linux-Gemeinschaft begann umgehend mit der Entwicklung eines Patches, um die Schwachstelle zu beheben. Der Vorfall verdeutlicht die Notwendigkeit erhöhter Wachsamkeit und Sicherheitsmaßnahmen bei Open-Source-Projekten. Die Möglichkeit, kollektiv zusammenzuarbeiten, um Software sicherer zu machen, ist einer der größten Vorteile von Open-Source-Software in Bezug auf Cybersecurity. Regelmäßige Überprüfungen und ein robustes Management von Zugriffsrechten sind essenziell, um ähnliche Vorfälle in der Zukunft zu verhindern [88].

CrowdStrike Falcon Bug

Ausgangslage: Am 19. Juli 2024 veröffentlichte das amerikanische Cybersecurity-Unternehmen CrowdStrike ein fehlerhaftes Update für sein Produkt Falcon Sensor, einer Enterprise Detection und Response (EDR)-Schutzsoftware für Endgeräte [48]. Endpoint Detection and Response ist ein Technologiekonzept und eine Lösung, die darauf abzielt, Endgeräte, wie PCs, Laptops, Tablets, Smartphones und Server, vor Cyberbedrohungen zu schützen und diese abzuwehren [180]. Das Update führte zu schwerwiegenden Problemen bei Microsoft Windows-Computern, auf denen die Software installiert war [79].

Die Täter und ihr Motiv: Der Vorfall war nicht das Ergebnis einer gezielten Cyberattacke, sondern resultierte aus unzureichenden Test- und Qualitätssicherungsmaßnahmen im Zusammenhang mit dem Software-Update [48]. Der Fehler im Update führte zu einer Diskrepanz in den erwarteten Eingabefeldern. Der Sensor erwartete 20 Eingabefelder, jedoch lieferte die Aktualisierung 21 Eingabefelder [212]. Diese Diskrepanz führte zu einem unzulässigen Speicherauszug, der einen Systemabsturz verursachte und sich zu einem sogenannten „Blue Screen of Death" manifestierte. In einigen Fällen gerieten die Systeme in eine Bootschleife und konnten nicht mehr hochfahren [277].

Ausmaß des Angriffs: Rund 8,5 Millionen Systeme weltweit waren betroffen und konnten nicht ordnungsgemäß neu gestartet werden [328]. In Deutschland führte dies zu massiven Störungen am Berliner Flughafen, Ausfällen in Krankenhäusern und Beeinträchtigungen in den Transaktionssystemen von Banken und Finanzinstituten [277]. Cyberkriminelle nutzten die IT-Ausfälle für verschiedene Formen von Phishing [46]. Das BSI stufte den Vorfall als geschäftskritisch ein [48].

Erkenntnisse und Lehren: Als Reaktion veröffentlichte CrowdStrike am 19. Juli 2024 Maßnahmen zur Schadensbegrenzung auf seinem Support-Portal. Ein Workaround

ermöglichte es vielen Unternehmen, ihre Systeme wieder zum Laufen zu bringen, allerdings auf Kosten des Sicherheitsschutzes [277]. Zwei Tage später stellte Microsoft ein Wiederherstellungstool für die betroffenen Systeme bereit [46]. Das BSI arbeitete gemeinsam mit CrowdStrike und Microsoft an Maßnahmen, um ähnliche Vorfälle in Zukunft zu verhindern. Diese Maßnahmen umfassen kurz-, mittel- und langfristige Schritte bis Ende 2024 sowie weitergehende Maßnahmen bis 2025 [46]. Eine gemeinsame Befragung von 311 betroffenen Unternehmen durch das BSI und den Digitalverband Bitkom ergab, dass mehr als 60 Prozent der Unternehmen direkte Konsequenzen erlebten und fast die Hälfte der betroffenen Unternehmen den Betrieb vorübergehend einstellen musste [228]. Der Vorfall zeigt, dass fehlerhafte Sicherheitsupdates schwerwiegende Folgen haben können und die Notwendigkeit robuster Test- und Qualitätssicherungsmaßnahmen unterstreichen.

Analogien zwischen den vorgestellten Angriffen

Die Cyberattacken auf Ivanti VPN, RedHat XZ Utils und der Vorfall mit dem CrowdStrike Falcon Bug verdeutlichen die vielfältigen Bedrohungen, denen moderne IT-Infrastrukturen ausgesetzt sind.

Alle drei Vorfälle betrafen weit verbreitete Standardapplikationen und systemkritische Infrastrukturen und hatten weitreichende Auswirkungen auf die betroffenen Anwender, Systeme und Organisationen. Sie nutzten Schwachstellen in weit verbreiteten Softwarelösungen, die über weitreichende Berechtigungen verfügen müssen, aus, was zu erheblichen Schäden führte. Zudem zeigten die dargestellten Angriffe die Notwendigkeit einer verstärkten Wachsamkeit und proaktiven Sicherheitsmaßnahmen deutlich auf, um solche Bedrohungen frühzeitig zu erkennen und abzuwehren.

Der Angriff auf Ivanti VPN war durch die Ausnutzung einer Kombination mehrerer Schwachstellen gekennzeichnet, die es den Angreifern ermöglichten, die Authentifizierung zu umgehen und dauerhaften Zugriff auf die VPN-Gateways zu erlangen. Dies ermöglichte ihnen, sich innerhalb des VPNs zu bewegen und auf sensible Daten in vermeintlich gut geschützten Umgebungen zuzugreifen. Die Angreifer setzten dabei ausgeklügelte Malware ein, die Patches und sogar Factory Resets überdauern konnte, was die Bedrohung besonders hartnäckig machte.

Der Angriff auf RedHat XZ Utils war ein Beispiel für eine langfristige und gezielte Infiltration eines Open-Source-Projekts. Der Angreifer nutzte Social Engineering, um das Vertrauen des Projektbetreuers zu gewinnen und schaffte es, über einen Zeitraum von etwa zwei Jahren eine Backdoor in den Quellcode einzuschleusen. Diese Backdoor ermöglichte es, die Authentifizierung in sshd zu umgehen und beliebigen Code auf den Zielsystemen auszuführen, was die Schwachstelle besonders gefährlich machte.

Der Vorfall mit dem CrowdStrike Falcon Bug unterschied sich grundlegend von den anderen beiden, da es sich hierbei nicht um einen gezielten Angriff, sondern um ein fehlerhaftes Sicherheitsupdate handelte. Das Update führte zu Systemabstürzen auf rund 8,5 Millionen Microsoft Windows-Computern und verdeutlichte die Risiken, die mit unzureichenden Test- und Qualitätssicherungsmaßnahmen bei Software-Updates verbunden sind. Gleichwohl ist es im Kontext dieses Sicherheitsvorfalls zu zahlreichen weiteren Angriffen gekommen.

Die Analyse der drei Cyberangriffe zeigt deutlich, dass Schwachstellen in IT-Systemen weitreichende und schwerwiegende Folgen haben können. Je tiefer die angegriffenen Komponenten in die Systeme integriert waren, desto umfangreicher waren die Schäden und die betroffenen Scopes. Ein zentrales Learning aus diesen Vorfällen ist die Notwendigkeit einer transparenten und schnellen Bewältigung von Sicherheitslücken sowie einer engen Zusammenarbeit zwischen den unterschiedlichen Betroffenen, wie Behörden und Unternehmen, um effizient auf Bedrohungen reagieren zu können. Informationsaustausch, schnelle Überprüfung von Lösungen und zeitnahe Lageeinschätzungen und Warnungen durch vertrauenswürdige Stellen waren ein wichtiger Pfeiler in der Bewältigung.

Dabei sind die Zusammenarbeit und der offene Informationsaustausch innerhalb der Cybersecurity-Gemeinschaft, auch außerhalb wirtschaftlicher Kreise, von besonderer Bedeutung. Die schnelle Reaktion und die Entwicklung von Patches durch die Linux-Gemeinschaft im Fall von RedHat XZ Utils sowie die gemeinsamen Maßnahmen von CrowdStrike, Microsoft und dem BSI im Fall des Falcon Bugs zeigen, wie wichtig kollektive Anstrengungen sind, um Sicherheitsvorfälle zu bewältigen und zukünftige Angriffe zu verhindern. Die Breite der Gefahren, die von verschiedenen Angriffsvektoren ausgehen, verdeutlicht die Notwendigkeit eines proaktiven Umgangs mit Sicherheitsvorfällen in IT-Systemen. Unternehmen müssen ihre Infrastruktur gut kennen und kontinuierlich überwachen, um potenzielle Schwachstellen frühzeitig zu identifizieren und zu beheben. Regelmäßige Penetrationstests, gute Dokumentationen und ein robustes Schwachstellenmanagement sind essenziell, um die Sicherheit der Systeme zu gewährleisten und im Schadensfall die betroffenen Bereiche und Systeme zu identifizieren.

Zusammenfassend lässt sich festhalten, dass nahezu alle Unternehmen von Schwachstellen der IT-Infrastruktur betroffen sein werden. Eine entschlossene und schnelle Reaktion sowie eine gute Zusammenarbeit zwischen Behörden Firmen und Community sind entscheidend, um effizient auf Cyberangriffe zu reagieren und die Ausbreitung von Angriffen und Schwachstellen zu begrenzen. Responsable Disclosure von Sicherheitslücken, ein kollaborativer Ansatz unter Expert*innen für die Systeme und die schnelle und transparente Information der (Fach-) Öffentlichkeit sind dabei unabdingbar. Die dargestellten Vorfälle zeigen, dass die besten Ergebnisse in der Bewältigung durch Kooperation und Kollaboration erzielt werden konnten.

1.8 UPDATE REGULATORIK: STAND NIS-2

Die NIS-2-Richtlinie ist eine EU-weite Gesetzgebung zur Cybersecurity. Sie sieht rechtliche Maßnahmen vor, um das allgemeine Niveau der Cybersecurity in der Europäischen Union zu harmonisieren und auszuweiten. Die Mitgliedstaaten waren verpflichtet, die Richtlinie bis zum 17. Oktober 2024 umzusetzen. Der Stand der Umsetzung ist von Land zu Land jedoch sehr unterschiedlich. Einige der Mitgliedstaaten, darunter Deutschland haben die Frist nicht eingehalten [260]. Während in manchen Ländern, wie Belgien, Italien, Kroatien und Litauen, die NIS-2 Vorschriften bereits genehmigt und verabschiedet wurden, befinden sich viele europäischen Länder noch im Prozess der Verfassung und Verabschiedung der Rechtsvorschriften [14]. Deutschland strebt hierfür das Ende des ersten Quartals 2025 an. Der Zeitplan für die Rechtsverordnungen zum Umsetzungsgesetz bleibt unklar [322].

Auch wenn NIS-2-Umsetzungs- und KRITIS-Dachgesetz gescheitert sind und damit Rechtsunsicherheit herrscht, können Organisationen sich an den Kernelementen der EU-NIS-2-Richtlinie bei ihren Maßnahmen orientieren.

1.9 STRAFVERFOLGUNG

Die globale Jagd auf Cyberkriminelle – Entwicklungen und Herausforderungen 2024

Die Cyberkriminalität blieb in Deutschland im Berichtszeitraum weiterhin auf einem hohen Niveau. Besonders auffällig sind dabei Straftaten, die aus dem Ausland oder von unbekannten Orten aus begangen werden und in Deutschland Schäden verursachen. Seit der Erfassung dieser sogenannten Auslandstaten im Jahr 2020 steigt ihre Zahl kontinuierlich an, im Berichtszeitraum um 28 Prozent im Vergleich zum Vorjahr [60]. Diese Auslandstaten übertreffen erneut die Anzahl der Inlandstaten, bei denen sowohl der Tatort als auch der Schadensort in Deutschland liegen. Die Inlandstaten stagnierten im Berichtszeitraum auf hohem Niveau mit 134.407 Fällen, was einem Rückgang von 1,8 Prozent gegenüber dem Vorjahr entspricht. Die Aufklärungsquote bei Cybercrime-Delikten ist 2023 um drei Prozentpunkte auf 32,2 Prozent gestiegen [60].

Strafverfolgung durch staatliche Institutionen und Behörden

Staatliche Institutionen und Behörden spielen eine zentrale Rolle bei der Strafverfolgung von Cyberkriminellen. Sie sind für die Ermittlung, Verfolgung und Bestrafung von Tätern zuständig. Die Zusammenarbeit zwischen verschiedenen Behörden auf regionaler und nationaler Ebene ist dabei von entscheidender Bedeutung. Da Cyberkriminalität ein globales Problem ist, erfordert es eine weltweit koordinierte Strafverfolgung. Internationale Zusammenarbeit ist notwendig, um Täter über Landesgrenzen hinweg verfolgen und zur Rechenschaft ziehen zu können.

Die Bekämpfung von Internetkriminalität ist ein zentraler Schwerpunkt der kriminalpolizeilichen Arbeit vieler Staaten. Daher wurden in verschiedenen Ländern spezialisierte Cybercrime-Competence-Center eingerichtet, die aus Expertinnen und Experten aus den Bereichen Ermittlung, IT-Forensik und Technik bestehen. Diese Zentren fungieren als nationale und internationale Zentralstellen für die elektronische Beweismittelsicherung und -auswertung, Ermittlungen im Zusammenhang mit Cyberkriminalität im engeren Sinn sowie die Koordinierung der Bekämpfung von Cybercrime.

UN-Abkommen gegen Cyberkriminalität

Am 27. November 2024 verabschiedete die Generalversammlung der Vereinten Nationen die „United Nations Convention against Cybercrime“, ein wegweisendes Abkommen zur Bekämpfung von Straftaten, die über Informations- und Kommunikationstechnologiesysteme (IKT) begangen werden. Dieses Übereinkommen fokussiert sich auf schwere Verbrechen, wie Identitätsdiebstahl, Cyberterrorismus, Kinderpornografie, Hackerangriffe auf Kritische Infrastrukturen und finanzielle Cyberbetrügereien. Dabei wird betont, dass die Mitgliedsstaaten nicht nur strafrechtliche Verfolgung gewährleisten, sondern auch den internationalen Austausch von Beweismaterial in elektronischer Form erleichtern sollen. Zudem sieht das Abkommen vor, dass Mitgliedstaaten Mindeststrafen festlegen, wobei für die schwersten Straftaten, wie Angriffe auf nationale Sicherheit oder Kritische Infrastrukturen, eine Mindestfreiheitsstrafe von fünf Jahren vorgeschlagen wird. Ein spezielles Überwachungsgremium soll die Einhaltung der Konvention und die einheitliche Anwendung der Strafmaßnahmen gewährleisten, um der globalen Bedrohung durch Cyberkriminalität entschlossen entgegenzuwirken [304].

Aufbau von Druck auf kriminelle Organisationen

Durch eine konsequente Strafverfolgung kann Druck auf kriminelle Organisationen aufgebaut werden. Dies kann dazu führen, dass Mitglieder aussteigen oder dass die Organisationen zerschlagen werden. Konkret bedeutet dies, dass durch gezielte Ermittlungen, Überwachungsmaßnahmen und Festnahmen die operativen Fähigkeiten der Organisationen eingeschränkt werden. Die öffentliche Bekanntmachung von Erfolgen in der Strafverfolgung kann dabei das Vertrauen innerhalb der Organisationen untergraben und potenzielle neue Mitglieder abschrecken. Die Beschlagnahmung von Vermögenswerten und die Zerschlagung von Netzwerken tragen ebenfalls dazu bei, den finanziellen und logistischen Druck auf die kriminellen Strukturen zu erhöhen.

Ausschluss Cyberkrimineller von Finanzströmen

Eine wichtige Maßnahme zur Bekämpfung der Cyberkriminalität ist der Ausschluss von Cyberkriminellen von Finanzströmen. Durch die Sperrung von Konten und das Einfrieren von Vermögenswerten kann den Tätern die Finanzierung ihrer Aktivitäten entzogen werden. Die zunehmende Nutzung von Kryptowährungen durch Cyberkriminelle stellt hierbei eine besondere Herausforderung dar, da diese oft schwer zu verfolgen sind. Während digitale Währungen den Tätern gegenwärtig noch eine hohe Anonymität bieten, haben Parlamente, internationale Ermittlungsbehörden und Finanzinstitute in den letzten Monaten verstärkt daran gearbeitet, die Rückverfolgbarkeit von Krypto-Transaktionen zu erhöhen.

Durch die detaillierte Analyse von Blockchain-Transaktionen können Ermittler die Spuren krimineller Aktivitäten bis zu den digitalen Geldbörsen zurückverfolgen, die auf regulierten Plattformen, wie Binance, Bitpanda, Coinbase, eToro, Kraken, Trade Republic oder Scalable Capital, geführt werden. An diesem Punkt, wo die digitalen Währungen, beispielsweise Bitcoin, Ethereum oder Tether, in die Welt der traditionellen Finanzsysteme eintreten, kann die Anonymität durchbrochen werden. Die Zusammenarbeit von Strafverfolgungsbehörden und spezialisierten Anwälten ermöglicht es, die Identität der Täter offenzulegen und ihre illegal erworbenen digitalen Vermögenswerte zu blockieren und zu beschlagnahmen.

Durch die Einführung neuer regulatorischer Rahmenbedingungen und die Zusammenarbeit zwischen verschiedenen Ländern konnten bereits einige Erfolge bei der Aufdeckung und Verfolgung von krypto-basierten Geldwäscheaktivitäten erzielt werden. Trotz dieser Fortschritte bleibt die Bekämpfung der Finanzierung von Cyberkriminalität eine komplexe Aufgabe. Die schnelle Entwicklung neuer Technologien und die grenzüberschreitende Natur der Cyberkriminalität erfordern eine kontinuierliche Anpassung der Maßnahmen zur Finanzaufsicht und Strafverfolgung

Zerschlagung von Infrastrukturen der Cyberkriminellen

Die Zerschlagung von Infrastrukturen der Cyberkriminellen, wie Botnets oder Darknet-Marktplätze, ist ein weiteres wichtiges Ziel der Strafverfolgung. Die fortgesetzten Takedowns von Cyberkriminalitätsforen und Marktplätzen haben die Lebensdauer krimineller Websites verkürzt und die Fragmentierung des kriminellen Marktplatzes verstärkt [100].

Strukturdaten zu Cyberkriminellen

Cyberkriminalität ist ein komplexes Phänomen, das von einer Vielzahl unterschiedlicher Akteure ausgeht. Viele Cyberkriminelle agieren als Einzelpersonen oder sind Teil loser Netzwerke, was eine präzise Zuordnung zu bestimmten Ländern erschwert.

Die Zielgruppen von Cyberangriffen sind ebenso vielfältig. Große Unternehmen sind aufgrund ihrer wertvollen Daten und Ressourcen bevorzugte Ziele. Kritische Infrastrukturen wie Energieversorger und Krankenhäuser, werden ebenfalls häufig angegriffen, da ihre Störung erhebliche Auswirkungen haben kann. Staatliche Institutionen sind Ziele für Spionage und Sabotage, während Einzelpersonen oft durch Phishing-Angriffe und Identitätsdiebstahl betroffen sind.

Die Cyberkriminalität hat sich in den letzten Jahren stark weiterentwickelt und professionalisiert [100]. Ihre tiefgreifende Verzahnung mit der Schattenwirtschaft bildet eine Schnittstelle, an der Technologie und Kriminalität konvergieren [6]. Die Schattenwirtschaft, einst auf lokale Netzwerke und physische Treffpunkte beschränkt, hat sich durch die Digitalisierung zu einem globalen Phänomen entwickelt. Cyberkriminelle nutzen die Anonymität des Internets, um Waren und Dienstleistungen zu handeln, die von Drogen über gefälschte Dokumente bis hin zu gestohlenen Identitäten reichen. Die Schattenwirtschaft wiederum bietet die nötigen Infrastrukturen und Märkte, um die Erlöse aus Cyberkriminalität zu waschen und zu investieren. Die enge Verflechtung beider Bereiche führt zu einer kontinuierlichen Eskalation der Bedrohungen für Unternehmen, Staaten und Einzelpersonen.

Finanzielle Aspekte spielen eine zentrale Rolle in der Cyberkriminalität. Kryptowährungen wie Bitcoin werden häufig zur Zahlung von Lösegeldern und zur Geldwäsche verwendet. Auf Darknet-Märkten können Cyberkriminelle gestohlene Daten, Malware und andere illegale Waren mit Kryptowährungen kaufen und verkaufen, was die Nachverfolgung und Bekämpfung dieser Aktivitäten zusätzlich erschwert.

Das Darknet bleibt ein wichtiger Katalysator für Cyberkriminalität, da es Tätern erlaubt, Wissen, Werkzeuge und Dienstleistungen in einem nahezu anonymen Umfeld zu teilen. Die Entwicklungen bei Anbietern und Angeboten ist dynamisch und durch eine Fragmentierung der Marktplätze geprägt. Infolgedessen ist der Lebenszyklus krimineller Seiten kürzer geworden. In diesem Zusammenhang konnte beobachtet werden, dass der Wettbewerb um ihre Dienste unter verschiedenen Ransomware-as-a-Service (RaaS)-Anbietern gestiegen ist [100]. Das Tor-Netzwerk bleibt die beliebteste Plattform für Cyberkriminelle, um auf das Darknet zuzugreifen.

Die Rolle der Künstlichen Intelligenz bei der Strafverfolgung

Cyberkriminelle nutzen zunehmend Künstliche Intelligenz, um ihre Angriffe zu optimieren. Strafverfolgungsbehörden müssen daher ihre Kapazitäten im Bereich der KI ausbauen, um diesen Bedrohungen effektiv begegnen zu können [100]. Künstliche Intelligenz spielt eine zunehmend wichtige Rolle bei der Strafverfolgung von Cyberkriminellen. Durch den Einsatz von KI können große Datenmengen in Echtzeit analysiert und verdächtige Aktivitäten schneller identifiziert werden. Algorithmen für maschinelles Lernen helfen dabei, Muster und Anomalien zu erkennen, die auf kriminelle Handlungen hinweisen könnten. Darüber hinaus ermöglicht KI die Automatisierung von Routineaufgaben, was Ermittlern mehr Zeit für komplexere Analysen und strategische Entscheidungen verschafft. KI-basierte Tools können auch bei der Rückverfolgung von Transaktionen in Kryptowährungen und der Identifizierung von Netzwerken krimineller Akteure unterstützen. Insgesamt trägt der Einsatz von KI dazu bei, die Effizienz und Effektivität der Strafverfolgung im digitalen Raum erheblich zu steigern.

1.10 ERFOLGE IN 2024 & 2025

„Takedowns“ der gefährlichsten Schadsoftware-Familien

Der nach Angaben des BKA größte Schlag gegen die Cyberkriminalität in 2024 gelang dem Bundeskriminalamt und internationalen Partnern Ende Mai 2024 mit der Operation „Endgame“. Operation „Endgame“ ist ein 2022 initiiertes wegweisendes Verfahren der internationalen Cybercrime-Bekämpfung. Beteiligt sind Strafverfolgungsbehörden aus den Staaten unter Koordination von Europol und Eurojust. Die Generalstaatsanwaltschaft Frankfurt am Main und das Bundeskriminalamt (BKA) führten am 28. und 29. Mai 2024 eine international koordinierte Aktion durch, bei der mehrere der gefährlichsten Schadsoftware-Familien vom Netz genommen wurden. An der Operation „Endgame“ waren Strafverfolgungsbehörden aus zahlreichen Ländern beteiligt, darunter aus Deutschland, Dänemark, Frankreich, den Niederlanden, dem Vereinigten Königreich und den USA, unterstützt durch Europol und Eurojust. Über 100 Server wurden beschlagnahmt, mehr als 1.300 kriminell genutzte Domains unschädlich gemacht und Vermögenswerte in Höhe von über 139 Millionen Euro gesichert. Zehn internationale Haftbefehle wurden erlassen und vier Personen vorläufig festgenommen. Die Maßnahmen richteten sich gegen die Schadsoftware-Familien IcedID, SystemBC, Bumblebee, Smokeloader, Pikabot und Trickbot, die mit mindestens 15 Ransomware-Gruppierungen in Verbindung standen. Ziel ist die Zerschlagung der relevantesten Schadsoftwarefamilien der Kategorie Initial Access Malware (sogenannte Dropper oder Loader). Schadsoftware dieser Kategorie wird in der Regel via Spam-E-Mails verbreitet und ist spezialisiert darauf, Systeme unbemerkt zu infizieren und diese damit unter Kontrolle der Täterschaft zu bringen. Im Anschluss werden üblicherweise sensible Daten ausgelesen und die infizierten Systeme weiter ausgespäht. Die unbemerkte Infektion mit der genannten Malware fungiert als Türöffner und ermöglicht Cyberkriminellen das Nachladen weiterer Schadsoftware, insbesondere Ransomware, welche zur Verschlüsselung der Opfersysteme und anschließender Erpressung von Lösegeld genutzt wird [64]. Im Zuge der Ermittlungen wurden 69

Millionen Euro eines Betreibers beschlagnahmt und 99 Krypto-Wallets mit einem Gesamtwert von über 70 Millionen Euro bei Kryptobörsen gesperrt [64], [187].

Im Juni 2024 wurde ein 44-jähriger Ukrainer in der Slowakei festgenommen, der im Verdacht steht, Mitglied der Cyberkriminellen-Gruppierung GandCrab zu sein. Die Gruppierung hat weltweit Unternehmen und Einrichtungen mit Ransomware angegriffen und Lösegeld erpresst, was zu einem wirtschaftlichen Schaden von mehreren 100 Millionen Euro führte. Ermittler aus Baden-Württemberg meldeten im Oktober 2024 einen Fahndungserfolg, nachdem der Verdächtige nach Deutschland ausgeliefert wurde und ihm gewerbsmäßige Erpressung und Computersabotage vorgeworfen werden [175]. Dem Angeklagten wird vorgeworfen, sich im Frühjahr 2019 mutmaßlich illegal Zugang zu den Computernetzwerken von 22 deutschen Unternehmen und Einrichtungen verschafft und deren Daten mit einer Schadsoftware (Ransomware) verschlüsselt zu haben, denen alleine dadurch ein wirtschaftlicher Schaden von insgesamt 2,4 Millionen Euro entstand, um dann jeweils bis zu 15.000 USD in digitalen Währungen für die Entschlüsselung zu fordern. Das LKA hat über 80 Fälle in Deutschland mit einem Gesamtschaden von knapp 33 Millionen Euro dokumentiert, also einem Drittel des weltweit entstandenen Schadens, der der Gruppierung GandCrab und einer Nachfolgegruppierung zugeordnet werden. Ein noch größerer Schaden konnte verhindert werden, da das LKA mehr als 300 Unternehmen rechtzeitig warnte, wobei bei mindestens 17 dieser Firmen die Datenverschlüsselung unmittelbar bevorstand. Die Behörden haben zwei weitere mutmaßliche Hauptakteure identifiziert, die mit internationalen Haftbefehlen gesucht werden. Diese Männer, die russische Staatsbürger sind, sollen der Kopf der Gruppierungen und der Entwickler der Erpressungssoftware sein. Diese Erkenntnisse stammen aus langjährigen internationalen Ermittlungen, an denen neben nationalen Stellen auch das Bundeskriminalamt (BKA), der U.S. Secret Service, das FBI und Europol beteiligt waren. Am 27. 01. 2025 gab das Cybercrime-Zentrum Baden-Württemberg, das bei der Generalstaatsanwaltschaft Karlsruhe eingerichtet ist, in einer offiziellen Pressemitteilung bekannt, dass es Anklage gegen den in der Slowakei festgenommen Täter vor dem Landgericht Stuttgart erhoben hat [117].

Schlag gegen Akteure der Underground Economy

Im September 2024 gelang dem BKA, die Infrastruktur von digitalen Geldwäschern der Schattenwirtschaft zu schwächen. Dabei wurden 47 in Deutschland gehostete Exchange-Services abgeschaltet, die für kriminelle Zwecke genutzt wurden. Diese Plattformen ermöglichten den anonymen Austausch von herkömmlichen Währungen und Kryptowährungen, ohne die gesetzlichen Vorgaben zur Geldwäschebekämpfung zu erfüllen. Den Betreibern wird vorgeworfen, durch die mangelhafte Umsetzung des Know-Your-Customer-Prinzips die Herkunft kriminell erlangter Gelder verschleiert zu haben. Die abgeschalteten Exchange-Services waren ein wichtiger Bestandteil der kriminellen Wertschöpfungskette im Bereich Cybercrime, genutzt von Ransomware-Gruppen, Darknet-Händlern und Botnetz-Betreibern. Umfangreiche Nutzer- und Transaktionsdaten wurden sichergestellt, die wertvolle Ermittlungsansätze bieten und zur Schwächung der kriminellen Infrastruktur beitragen [63].

In einer international koordinierten Operation der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) der Generalstaatsanwaltschaft Frankfurt am Main, des Hessischen Landeskriminalamts (HLKA) und des BKA wurden am 31. Oktober 2024 zwei mutmaßliche Cyberkriminelle in Hessen und Rheinland-Pfalz festgenommen. Den 19- und 28-jährigen Beschuldigten wird vorgeworfen, als Administratoren der Online-Plattformen Flight RCS und Dstat.CC gehandelt zu haben, über die sie Betäubungsmittel und DDoS-Angriffe angeboten haben. Die Ermittlungen, die im Rahmen der internationalen Operation „PowerOff“ durchgeführt wurden, führten zur Sicherstellung umfangreicher Beweismittel und zur Identifizierung weiterer Hauptakteure [61].

Mitte Dezember 2024 gaben das BKA und die Generalstaatsanwaltschaft Frankfurt am Main bekannt, dass im Rahmen der international koordinierten Operation „Power Off“, zusammen mit Strafverfolgungsbehörden aus 15 Ländern, gegen kriminelle Dienstleistungs-Plattformen für DDoS-Angriffe vorgegangen wurde. Dabei wurden 27 sogenannte Stresser-Dienste beschlagnahmt und vom Netz genommen. Diese kriminellen Online-Plattformen ermöglichen es Nutzern, ohne tiefere technische Kennt-

nisse, schnell und einfach DDoS-Angriffe durchzuführen. Zudem konnten über 300 Nutzer identifiziert und drei mutmaßliche Administratoren in Deutschland und Frankreich festgenommen werden [65].

Mit Beginn des Jahres 2025 erzielte die Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) der Generalstaatsanwaltschaft Frankfurt am Main in einer groß angelegten internationalen Aktion einen bedeutenden Erfolg im Kampf gegen die digitale Unterwelt. In enger Zusammenarbeit mit Strafverfolgungsbehörden aus den USA, Australien, Spanien, Griechenland, Rumänien, Italien und Frankreich wurde im Rahmen der Operation „Talent" die Schließung der Plattformen nulled.to und cracked.io erreicht – Foren, die als zentrale Einstiegspunkte in die Schattenwirtschaft der Cyberkriminalität gelten. Über diese Plattformen wurden illegale Dienstleistungen wie DDoS-Angriffe, Malware, Cracking- und Hacking-Tools, sowie KI-gestützte Schadsoftware und Datenleaks gehandelt – mit einem geschätzten Umsatz von mehr als einer Million Euro. Acht mit den Webseiten in Verbindung stehende Personen wurden während der Aktion verhaftet. Die Aktion unterstreicht die zunehmende Effektivität internationaler Strafverfolgungskooperationen im Kampf gegen Cyberkriminalität und setzt ein klares Signal gegen die Organisierte Kriminalität im digitalen Raum [66].

Bedrohung, Ausgrenzung sowie Hass und Hetze im Internet

Die Generalstaatsanwaltschaft Frankfurt am Main und das Bundeskriminalamt haben gegen zehn mutmaßliche Mitglieder der Online-Gruppierung „New World Order" strafprozessuale Maßnahmen ergriffen. Den Beschuldigten wird vorgeworfen, als Anführer einer kriminellen Vereinigung systematisches Cybermobbing und Cyberstalking betrieben zu haben. In sechs Bundesländern wurden insgesamt zehn Wohnungen durchsucht, wobei zahlreiche elektronische Geräte und Speichermedien sichergestellt wurden. Die Gruppierung hatte es insbesondere auf Personen aus der Online-Streamer-Szene abgesehen, die sie durch Bedrohungen, Beleidigungen und das Veröffentlichen personenbezogener Daten (Doxing) zur Aufgabe ihrer Online-Präsenz zwingen wollten. Zu den Methoden der Vereinigung zählte auch das sogenannte „Swatting", bei dem Notrufe missbraucht wurden, um Polizei- oder Feuerwehreinsätze bei den Opfern auszulösen [62]. Die „New World Order" ist ein ausschließlich virtueller Zusammenschluss von Personen. In zahlreichen Fällen hatten die Anführer der Vereinigung Personen aus der Online-Streamer-Szene als Opfer (sogenannte „Masken") ausgewählt, häufig vulnerable oder kognitiv beeinträchtigte Menschen. Die Opfer werden durch die Vereinigung dann mittels sozialer Medien verfolgt, bedroht und beleidigt.

1.11 AUSBLICK 2025-2030

Die fortschreitende Vernetzung aller Lebensbereiche, gepaart mit wachsenden geopolitischen Konflikten, wird Cyberangriffe in den nächsten fünf Jahren zu einer noch größeren und komplexeren Bedrohung machen. Laut einer Prognose werden sich die weltweiten Ausgaben für IT-Sicherheit im Jahr 2025 auf 212 Milliarden USD belaufen. Dies entspricht einem Anstieg von 15,1 Prozent gegenüber 2024 [115].

Für 2025 wird eine Zunahme von Angriffen auf Basis gestohlener Daten prognostiziert. Abgesehen von weit verbreiteten Infostealern, wie Lumma, Vidar und Redline, würden sich auch vermehrt neue Akteure hervortun, die gestohlene Informationen für ihre Zwecke ausnutzen [271].

Doch nicht nur die Art der Angriffe und die verwendeten Tools werden das Risiko für Schäden durch Cyberangriffe verstärken. Auch Schwachstellen, die etwa durch den Fachkräftemangel oder grenzüberschreitende IKT-Dienstleister als „Single Point of Failure" entstehen, werden langfristig das Bedrohungspotenzial erhöhen. Insbesondere bei KMU wird die Abhängigkeit von externen IT-Dienstleistern weiter zunehmen und damit zu komplexeren Lieferketten und Herausforderungen im Bereich der Cybersecurity führen [97].

Angreifer der Zukunft

Den staatlich kontrollierten oder gestützten Angreifergruppen kommt im Rahmen der komplexen geopolitischen Entwicklungen immer mehr Gewicht zu. „Die großen Vier" bereits bekannten Länder Russland, China, Iran und Nordkorea werden weiterhin im Cyberraum aktiv bleiben und Spionageoperationen, Cyberangriffe und Informationsoperationen durchführen, um ihre geopolitischen Interessen auch in Zukunft durchzusetzen [121]. Russland demonstriert in der Ukraine seine anhaltende Bereitschaft, Cyberangriffe als Waffe und Teil der hybriden Kriegsführung einzusetzen und normalisiert damit diese Einsätze (Übersicht geografischer Herkunft digitaler Angriffe siehe Abbildung 10).

Gleichzeitig werden die bekannten Angreifergruppen sich weiter professionalisieren.

- Ransomware & Co
- Erschließung neuer Technologien & Dienstleistungen für das Angreiferspektrum
- Aufteilung der Aufgaben und Spezialisierung

Technologien der Zukunft

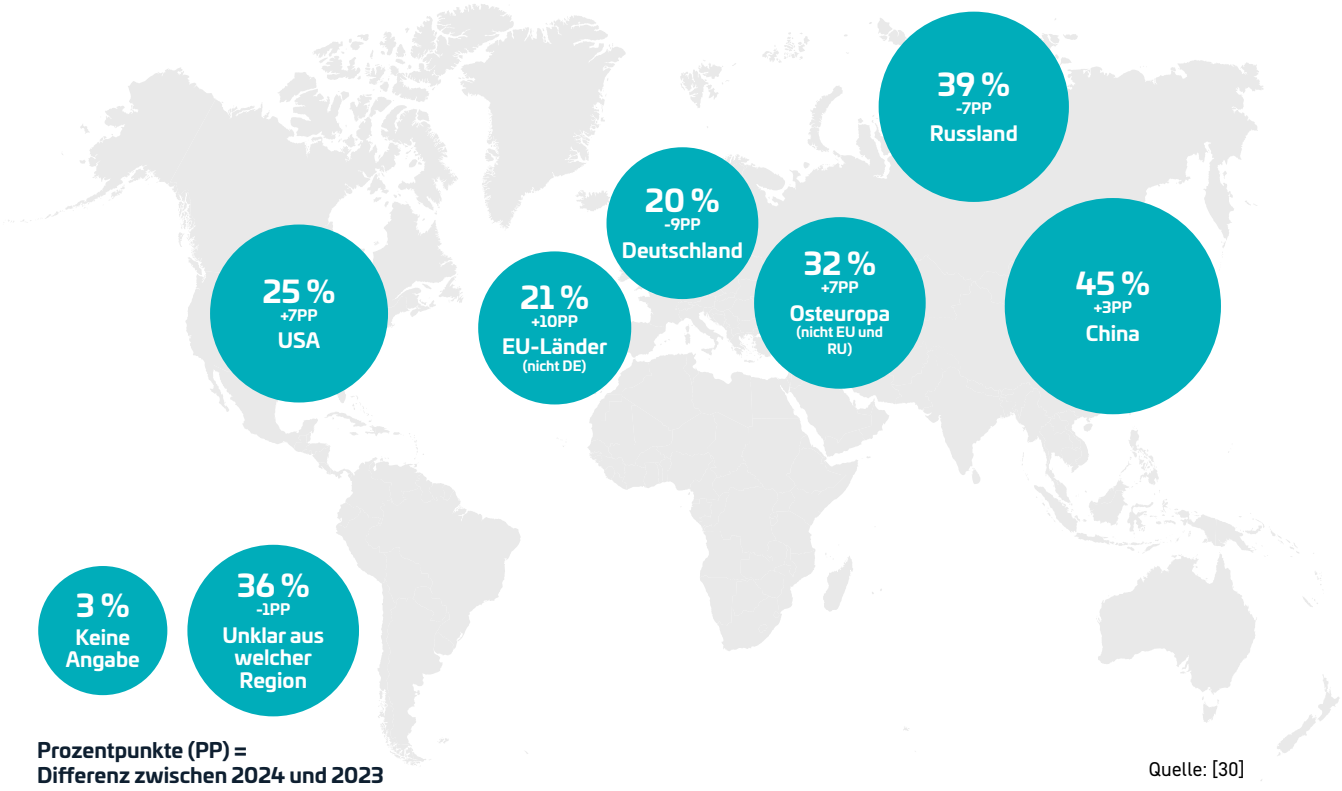
Während Künstliche Intelligenz zwar einerseits viele positive Entwicklungen mit sich bringen, werden sie in der Zukunft auch zunehmend von Angreifern im Rahmen ausgeklügelter Phishing-, Vishing- und Social-Engineering-Angriffe genutzt werden. Dabei werden diese auch Deepfakes für beispielsweise Identitätsdiebstahl, Betrug und die Umgehung von Sicherheitsmaßnahmen einsetzen [121]. 2027 könnten schon bei rund 17 Prozent aller Cyberangriffen und Datendiebstähle Generative KI im Spiel sein [115]. Generative KI wird auch Operationen in viel größerem Maßstab ermöglichen. So können Cyberkriminelle beispielsweise KI einsetzen, um Tausende von gezielten Phishing-Angriffen gleichzeitig zu starten, wobei jeder einzelne Angriff individuell zur Erzielung der maximalen Wirkung angepasst werden kann. So können auch kleinere kriminelle Gruppen groß angelegte Operationen durchführen, ohne dass sie über fortgeschrittene technische Kenntnisse verfügen müssen [71]. Auch für Informationsoperationen (IO) wird KI zunehmend relevant: IO-Akteure werden KI nutzen, um die Erstellung von Inhalten zu skalieren, überzeugendere Inhalte zu produzieren und unauthentische Personas zu verbessern [121].

Die schneller als erwartet wachsende Abhängigkeit von Satelliten und die zunehmende Vernetzung von Fahrzeugen gehen ebenfalls mit Überlegungen zur Cybersecurity und zum Datenschutz einher [97]. Mit der steigenden Rechenleistung müssen kontinuierlich alternde Verschlüsselungen ausgetauscht werden, da diese irgendwann gebrochen werden können.

Angriffsmethoden der Zukunft

In der sich ständig weiterentwickelnden Welt der Cyberkriminalität stehen Unternehmen und Organisationen vor immer neuen Herausforderungen, was die Art der Cyberangriffe angeht. Ransomware und vielschichtige Erpressung werden auch in Zukunft die größte Bedrohung darstellen, die sich auf verschiedenste Sektoren und Länder auswirkt. Diese Angriffe zielen darauf ab, kritische Daten zu verschlüsseln und Lösegeld zu fordern [121]. Darüber hinaus können Täter, denen es an technischem Know-how mangelt, im Darkweb Ransomware-as-a-Service-Optionen (RaaS) finden. Sie nutzen dabei vorentwickelte Ransomware-Tools, um Angriffe zu starten, und überlassen dem Anbieter im Gegenzug einen Teil des Lösegelds. Die Täter nutzen vermehrt auch die doppelte Erpressung, d. h. sie verlangen Lösegeld nicht nur für die Freigabe der gestohlenen Daten, sondern auch dafür, dass diese nicht weitergegeben werden [11].

Parallel dazu bleibt auch Infostealer-Malware eine große Gefahr, da sie Datenverletzungen und die Kompromittierung von Konten ermöglicht. Diese Art von Malware extrahiert sensible Informationen, wie Passwörter und Finanzdaten, welche dann wiederum über Foren oder auf kriminellen Seiten verkauft werden [121]. Bereits im ersten Halbjahr 2024 dominierten Infostealer als häufigste Malware-Art die Malware-Landschaft. LummaC2, eine getarnte Malware zum Ausspähen sensibler Daten, war



Prozentpunkte (PP) =
Differenz zwischen 2024 und 2023

Quelle: [30]

Abbildung 10: Geografische Herkunft digitaler Angriffe – Einschätzungen deutscher Unternehmen im Jahr 2024 (Mehrfachantworten)

dabei am aktivsten und löste andere bekannte Infostealer wie RedLine ab [146].

Ein weiterer besorgniserregender Trend ist die Demokratisierung von Cyberfähigkeiten. Der verbesserte Zugang zu Tools und Diensten senkt die Einstiegshürden für weniger qualifizierte Akteure, was zu einer Zunahme von Cyberangriffen führt. So sind zunehmend auch weniger erfahrene Kriminelle in der Lage, komplexe Angriffe durchzuführen.

Kompromittierte Identitäten in hybriden Umgebungen verschaffen Angreifern Zugang zu sensiblen Systemen und Daten und stellen so ebenfalls ein erhebliches Risiko dar. In einer zunehmend vernetzten Welt wird es daher immer wichtiger, Identitäten und Zugriffsrechte effektiv zu verwalten und zu schützen.

Besonders im Fokus stehen auch Web3- und Kryptowährungs-Organisationen, die zunehmend zur Zielscheibe von Angreifern werden, die es auf digitale Vermögenswerte abgesehen haben. Diese Angriffe können erhebliche finanzielle Schäden verursachen und das Vertrauen in digitale Währungen und Technologien untergraben.

Zudem wird die Zeit zum Ausnutzen von Schwachstellen immer kürzer und das Spektrum der anvisierten Anbieter erweitert sich stetig. Angreifer sind zunehmend in der Lage, Sicherheitslücken schneller zu identifizieren und auszunutzen, was die Notwendigkeit für proaktive und schnell umzusetzende Sicherheitsmaßnahmen und schnelle Reaktionszeiten unterstreicht [121].

Diese Entwicklungen erfordern innovative Abwehrstrategien und eine verstärkte Wachsamkeit, um den zukünftigen Bedrohungen effektiv begegnen zu können. Unternehmen müssen ihre Sicherheitsmaßnahmen kontinuierlich anpassen und verbessern, um den sich wandelnden Bedrohungen einen Schritt voraus zu sein.

Abwehrmethoden der Zukunft

Nicht nur im Bereich der Cyberangriffe spielt Künstliche Intelligenz respektive Machine Learning eine entscheidende Rolle, auch in der Cyberabwehr werden diese Tools zunehmend zum Einsatz kommen. Ihr Einsatz wird unter anderem die Anomalie-Erkennung beschleunigen, mithilfe von Prognosekapazitäten die Analysezeit reduzieren, sowie dabei helfen, reaktive Maßnahmen zu automatisieren und Strategien zur Abwehr aufkommender Bedrohungen zu entwickeln und zu stärken [271]. Untersuchungen von IBM und dem Ponemon Institute zeigen, dass Unternehmen, die KI und Automatisierung für die Sicherheitsprävention nutzen, im Durchschnitt 2,22 Millionen USD einsparen konnten [144]. Diese Einsparungen resultieren aus der Reduzierung der Zeit zur Erkennung und Eindämmung von Sicherheitsvorfällen, der Minimierung von Betriebsunterbrechungen und der Verringerung der Kosten für manuelle Sicherheitsüberprüfungen.

Die optimale Abwehr moderner Bedrohungen erfordert eine symbiotische Kombination aus proaktiver Threat Intelligence, prädiktiver Analytik, kontinuierlichem Mo-

nitoring und einem strikten Zero-Trust-Modell, um die Angriffsfläche zu minimieren und die Erkennung von Bedrohungen zu beschleunigen. Hierbei werden verhaltensbasierte Anomalien-Erkennung, maschinelles Lernen und automatisierte Bedrohungsjagd durch eine ganzheitliche Sicherheitsstrategie ergänzt, die die Resilienz gegen gezielte Angriffe stärkt und die Mean Time to Detect (MTTD) reduziert. Neben den technischen Maßnahmen sind die Veranstaltung regelmäßiger Cybersecurity-Trainings für Mitarbeitende sowie die regelmäßige Aufklärung und Weiterbildung essenziell. Aktuelles Wissen über die wichtigsten potenziellen Cyberbedrohungen ist unerlässlich, da uninformierte Betriebsangehörige zu den häufigsten initialen Angriffsvektoren gehören, welche für ein Unternehmen zu schwerwiegenden finanziellen Verlusten führen können [271]. Sehr hilfreich ist dabei, wenn staatliche und privatwirtschaftliche Akteure miteinander kooperieren und Methoden und Wissen sowie neu auftretende Auffälligkeiten miteinander teilen.

Rolle von Cyberkriminalität im Zuge der geopolitischen Unsicherheiten und Konflikte

Der Einsatz von Cyberoperationen in Kriegszeiten ist bereits heute Realität. Zwar haben bisher nur wenige Staaten öffentlich zugegeben, solche Operationen durchzuführen, doch entwickelt eine wachsende Zahl von Staaten militärische Cyberkapazitäten. Cyberoperationen auch im Rahmen militärischer Konflikte werden in Zukunft wahrscheinlich noch zunehmen. Durch deren Einsatz verstärkt sich das Risiko, dass es – entweder absichtlich oder versehentlich – zu erheblichen, weitreichenden Auswirkungen auf Kritische Infrastrukturen wie wichtige Industriezweige, Telekommunikation und Verkehr sowie, Regierungs- und Finanzsysteme, kommen kann [148].

Cyberangriff auf das slowakische Grundbuchregister

Kaum hatte das Jahr 2025 begonnen, sorgte bereits in der ersten Woche ein schwerwiegender Cyberangriff in der Slowakei für landesweite Probleme. Ziel des Angriffs war das Grundbuchregister der Slowakei, das zentrale Register für Immobilienrechte, dessen Systeme vollständig lahmgelegt wurden. Dies führte zu einem Ausfall aller damit verbundenen Dienste und Datenbanken, wodurch sowohl der Immobilienmarkt als auch landwirtschaftliche Betriebe erheblich beeinträchtigt wurden. Der Angriff, der auf eine Ransomware-Infektion zurückgeführt wird, scheint aus der Ukraine zu stammen – eine Annahme, die im Kontext steigender politischer Spannungen zwischen der Slowakei und der Ukraine immer plausibler erscheint [13], [172].

KAPITEL 2

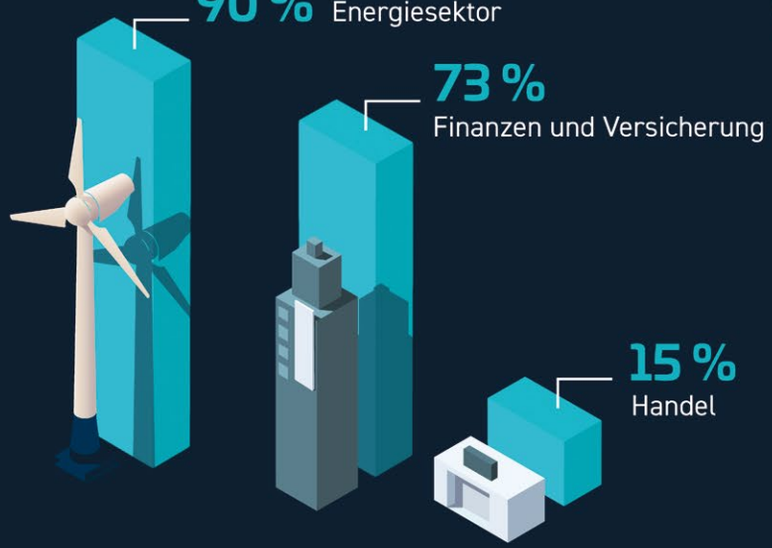
CYBERSECURITY IM FOKUS – DIE PERSPEKTIVEN DER DEUTSCHEN WIRTSCHAFT

Security Operations Center

Jedes fünfte – und auch kleinere – Unternehmen nutzt ein SOC.

Regelmäßige Überprüfung

anhand von Pentests



78 %

Mehr als drei Viertel der Unternehmen haben ihre Cybersecurity Budgets erhöht.

NIS-2

Betroffene Unternehmen insbes. mittlere und größere sind gut informiert und vorbereitet.

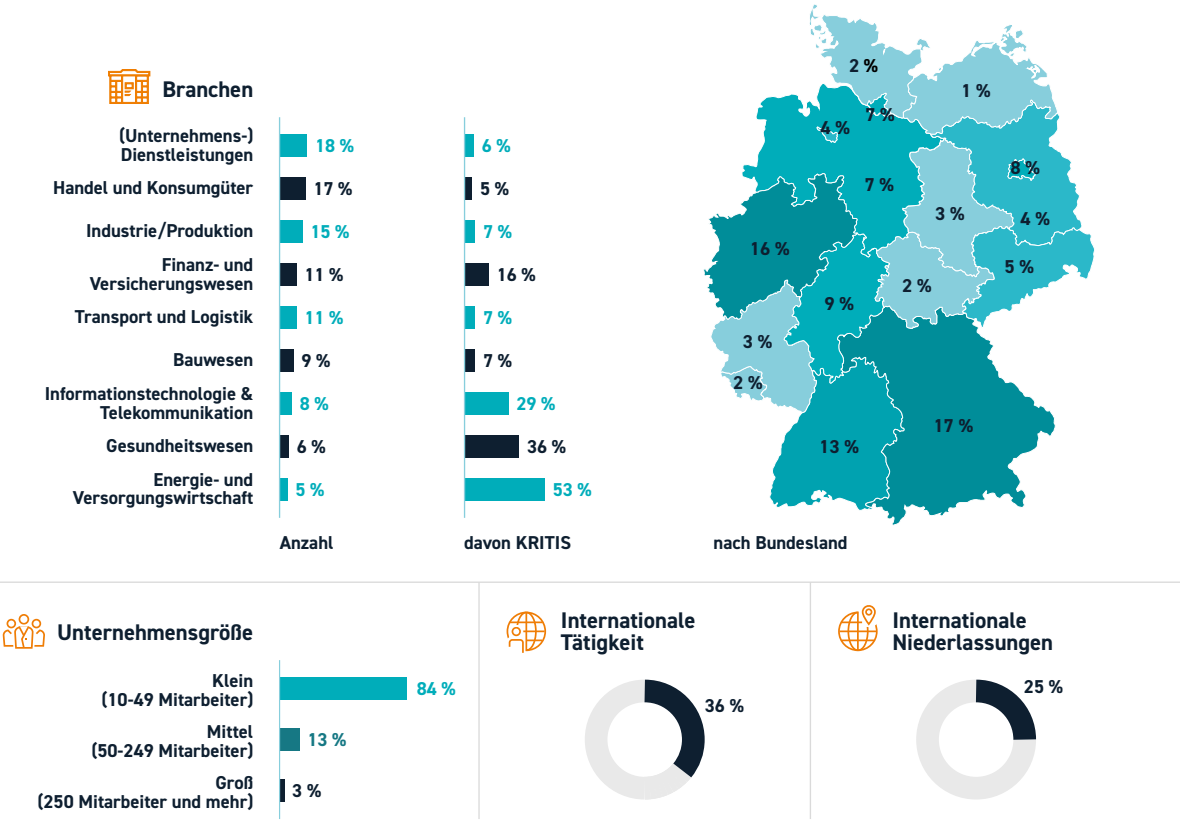
Nur rund 40 % fühlen sich gut unterstützt von den Behörden – bei KRITIS Unternehmen sind es immerhin 49 %.

Quellen: [255], eigene Darstellung

2 CYBERSECURITY IM FOKUS – DIE PERSPEKTIVEN DER DEUTSCHEN WIRTSCHAFT

Die Bedrohungslage im Bereich Cybersecurity hat sich 2024 weiter verschärft. Unternehmen sahen sich zunehmend mit ausgefeilteren Angriffsmethoden, steigenden regulatorischen Anforderungen und strategischen Herausforderungen konfrontiert. Die Umsetzung der EU-NIS2-Richtlinie erforderte tiefgreifende strukturelle Anpassungen, während technologische Abhängigkeiten – etwa durch Vendor-Lock-ins – langfristige Entscheidungen beeinflussten. Gleichzeitig gewann die Sicherheit global vernetzter Lieferketten weiter an Bedeutung. Bestehende Bedrohungen wie interne Cyberkriminalität und Angriffe auf weltraumbasierte Infrastrukturen rückten stärker in den Fokus, sodass viele Organisationen ihre Schutzmaßnahmen anpassen mussten.

IT-Sicherheitsabteilungen standen dabei an vorderster Front – oft mit begrenzten Ressourcen. In diesem dynamischen Umfeld liefert die vorliegende Studie eine systematische Bestandsaufnahme der Cybersecurity-Strategien deutscher Unternehmen. Sie untersucht, wie Betriebe unterschiedlicher Größe – von kleinen Unternehmen bis hin zu KRITIS-Betreibern – auf diese Herausforderungen



Mögliche Abweichungen in den Summen sind rundungsbedingt.
Dies gilt für alle Abbildungen in diesem Kapitel.

Quelle: [255]

Abbildung 11: Übersicht der Stichprobe nach Branchen, Bundesländern, Unternehmensgröße und Internationalität (in %)

Quelle: [255]

Abbildung 12: Themenübersicht der repräsentativen Umfrage

reagiert haben, welche Maßnahmen sie ergriffen haben und wo der größte Handlungsbedarf besteht.

Die Analyse basiert auf einer repräsentativen Befragung, die im vierten Quartal 2024 mittels telefonischer Interviews (CATI) durchgeführt wurde. Insgesamt wurden 1.001 Unternehmen aus verschiedenen Branchen befragt, um ein umfassendes Bild der Cybersecurity-Landschaft zu erhalten. Die Stichprobe umfasst 778 kleine Unternehmen mit weniger als 50 Mitarbeitenden, 123 mittlere Unternehmen mit 50 bis 249 Mitarbeitenden und 100 größere Organisationen mit 250 und mehr Beschäftigten. Ein erheblicher Teil der befragten Unternehmen ist international tätig. Mehr als ein Drittel ist in globalen Märkten aktiv und ein Viertel, verfügt über eigene Niederlassungen im Ausland.

Besonderes Augenmerk lag auf dem Vergleich zwischen Unternehmen, die als Kritische Infrastruktur (KRITIS) klassifiziert sind und solchen ohne diesen Status. Die Befragung richtete sich gezielt an Entscheidungsträger, die fundierte Einblicke in die Cybersecurity-Strategien ihrer Organisation geben konnten. Eine Übersicht der befragten Sektoren ist in Abbildung 11 dargestellt.

Um die Ergebnisse in einen breiteren wirtschaftlichen Kontext einzuordnen, wurden sie mit den Daten der Bitkom-Studie zum Wirtschaftsschutz 2024 sowie dem Global Cybersecurity Outlook 2025 des Weltwirtschaftsforums verglichen. Die Bitkom-Studie wurde zwischen Kalenderwoche 16 und 24 des Jahres 2024 durchgeführt und basiert auf einer Stichprobe von 1.003 Unternehmen mit mindestens zehn Mitarbeitenden und einem Jahresumsatz von einer Million Euro oder mehr [92].

Die vorliegende Untersuchung berücksichtigt hingegen Unternehmen aller Größen, unabhängig von ihrem Umsatz. Dadurch ergibt sich eine umfassendere Perspektive auf die Cybersecurity-Strategien, insbesondere von kleinen und mittleren Unternehmen, die in vielen bestehenden Erhebungen unterrepräsentiert sind. Gleichzeitig führt diese breitere Stichprobe an einigen Stellen zu abweichenden Durchschnittswerten im Vergleich zur Bitkom-Studie, insbesondere bei der Budgetverteilung oder der Einschätzung bestimmter Sicherheitsmaßnahmen.

Der Global Cybersecurity Outlook 2025 ergänzt diese Perspektive durch eine internationale Analyse der Cybersecurity-Herausforderungen auf Grundlage einer Befragung von 321 Führungskräften aus 57 Ländern, die zwischen September und Oktober 2024 durchgeführt wurde [6].

Sowohl die vorliegende Studie als auch die Bitkom-Studie befassen sich mit Themen wie der Sicherheitslage, internen Bedrohungen und IT-Budgets. Darüber hinaus erweitert die vorliegende Untersuchung den Fokus um zusätzliche Dimensionen, darunter die Umsetzung der EU-NIS2-Richtlinie, die Abhängigkeit von einzelnen Anbietern (Vendor-Lock-in), die Cybersecurity in Lieferketten sowie Sicherheitsrisiken in weltraumgestützter Infrastrukturen. In diesen Bereichen gibt es teilweise Überschneidungen mit dem Bericht der WEF, der unter anderem regulatorische Herausforderungen sowie Risiken durch systemische Bedrohung in Lieferketten und der Satellitentechnologie thematisiert [6], [30].

Vor diesem Hintergrund analysiert die vorliegende Studie die Cybersecurity-Strategien deutscher Unternehmen und untersucht sowohl bestehende als auch neu aufkommende Herausforderungen. Neben technischen und organisatorischen Maßnahmen standen strategische Fragestellungen im Mittelpunkt.

Ein wesentlicher Bestandteil der Untersuchung war die IT-Infrastruktur und die Organisation von Security Operations Centers (SOCs). Analysiert wurden die Verteilung der IT- und IT-Security-Budgets, die Auswirkungen wirtschaftlicher Entwicklungen auf Investitionen sowie die personelle Ausstattung der IT-Sicherheitsabteilungen. Zudem wurde erfasst, in welchem Umfang Unternehmen eigene SOCs betreiben und wie sie Penetrationstests zur Sicherheitsüberprüfung durchführen.

Ein weiterer Schwerpunkt lag auf den regulatorischen Anforderungen, insbesondere der Umsetzung der EU-NIS2-Richtlinie. Die Studie zeigt, wie Unternehmen ihre Vorbereitung einschätzen, welche Herausforderungen sie sehen und inwieweit sie externe Unterstützung in Anspruch nehmen.

Zusätzlich wurde die technologische Abhängigkeit von IT-Anbietern (Vendor-Lock-in) untersucht. Die Befragung ermittelte, ob Unternehmen Cybersecurity-Lösungen von einem oder mehreren Anbietern nutzen, welche Strategien sie zur Risikominimierung verfolgen und wie flexibel sie im Wechsel ihrer Anbieter sind.

Ein zunehmender Risikofaktor ist die Cybersecurity in der Lieferkette. Die Studie beleuchte, inwieweit Unternehmen Cyberrisiken durch externe Partner wahrnehmen, welche Sicherheitsanforderungen sie an ihre Lieferanten stellen und wie häufig sie deren Schutzmaßnahmen überprüfen.

Die Untersuchung umfasste zudem interne Bedrohungen durch aktuelle oder ehemalige Mitarbeitende. Erfasst wurde die Häufigkeit von Sicherheitsvorfällen, die eingesetzten Präventionsmaßnahmen sowie bestehende Kontrollmechanismen.

Ergänzend wurden Cybersecurity-Risiken in weltraumbasierten Infrastrukturen analysiert. Unternehmen gaben an, wie sie das Bedrohungspotenzial einschätzen und ob spezifische Schutzmaßnahmen implementiert wurden (einen Überblick der Themen liefert Abbildung 12).

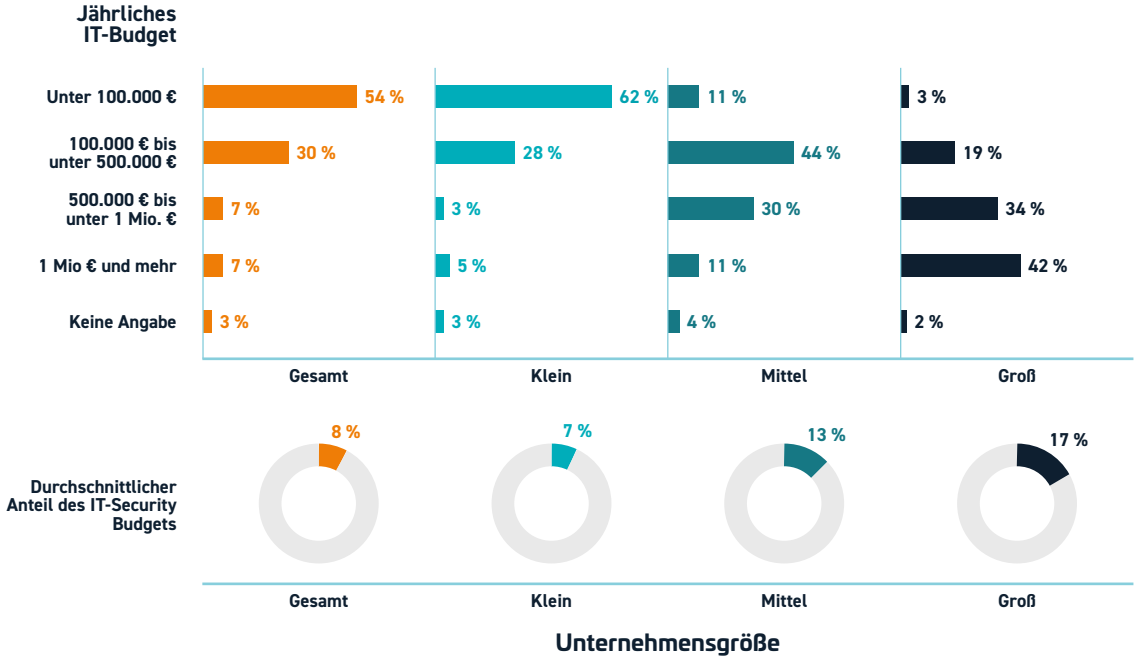
Die Ergebnisse zeigen, dass Unternehmen ihre Cybersecurity-Strategien weiterentwickeln müssen, um regulatorische Vorgaben zu erfüllen, technologische Abhängigkeiten zu vermeiden und interne wie externe Risiken besser zu kontrollieren.

2.1 IT-SECURITY-BUDGETS UND INTERNE STRUKTUREN

Die IT bildet das Rückgrat moderner Unternehmen – von effizienter Datenverarbeitung bis zur Abwehr hochentwickelter Cyberangriffe. Während große Unternehmen ihre Sicherheitsstrategien kontinuierlich ausbauen, stehen besonders kleine Betriebe vor wachsenden Bedrohungen und begrenzten Ressourcen.

Ein zentraler Faktor für die Sicherheitskapazitäten eines Unternehmens ist die Höhe des IT-Budgets. Mehr als die Hälfte der Unternehmen in Deutschland verfügt über ein IT-Budget von höchstens 100.000 Euro. Mit zunehmender Unternehmensgröße steigen die Budgets deutlich an. In Unternehmen mit 250 oder mehr Mitarbeitenden liegt das IT-Budget in 42 Prozent der Fälle bei einer Million Euro oder mehr (siehe Abbildung 13).

Während die Bitkom-Studie zum Wirtschaftsschutz den durchschnittlichen Anteil der IT-Sicherheitsausgaben auf 17 Prozent beziffert [30], zeigen die vorliegenden Ergebnisse einen geringeren Wert. Im Mittel fließen lediglich acht Prozent des IT-Budgets in Cybersecurity-Maßnahmen. Dieser Wert dürfte die tatsächliche Situation in deutschen Unternehmen realistischer abbilden, da die vorliegende Untersuchung als repräsentative Studie Unternehmen verschiedener Größen und unabhängig vom Umsatz erfasst – darunter auch viele kleine und mittlere Betriebe. Wie bereits in der Einleitung erläutert, berücksichtigt die Bitkom-Studie hingegen nur



Quelle: [255]

Abbildung 13: Jährliches IT-Budget und Anteil der Ausgaben für IT-Security (in %)

Unternehmen ab einem Jahresumsatz von einer Million Euro, weshalb ihre Werte tendenziell nach oben verzerrt sein könnten [30].

Tatsächlich zeigt sich auch in den vorliegenden Daten ein deutlicher Zusammenhang zwischen Unternehmensgröße und Sicherheitsinvestitionen: Große Unternehmen investieren mit durchschnittlich 17 Prozent ihres IT-Budgets in IT-Sicherheit (siehe Abbildung 13) – ein Wert, der mit den Ergebnissen der Bitkom-Studie übereinstimmt. Der niedrigere Gesamtwert der aktuellen Untersuchung ist somit darauf zurückzuführen, dass auch kleinere Unternehmen einbezogen wurden, die einen geringeren Anteil ihrer IT-Ausgaben für Sicherheitsmaßnahmen einplanen.

Trotz der angespannten wirtschaftlichen Lage haben Unternehmen ihre Investitionen in IT-Sicherheit zuletzt verstärkt. Mehr als drei Viertel (78 Prozent) der Befragten haben ihr Budget erhöht, bei mittleren Unternehmen liegt der Anteil sogar bei 81 Prozent. Diese Entwicklung deutet darauf hin, dass Cyberangriffe und deren potenzielle Folgen zunehmend als geschäftskritisches Risiko erkannt werden.

Zurückhaltender zeigt sich die Gesundheitsbranche, die im Vergleich zu anderen Sektoren weniger Investitionen in IT-Sicherheit tätigte. Ein möglicher Grund könnte in bereits getätigten Investitionen liegen, ebenso wie in regulatorischen Vorgaben, die eine bestimmte Sicherheitsbasis vorschreiben. Die vorliegenden Erhebungen stützen diese Annahme: Neben der Frage zu IT-Sicherheitsbudgets wurden die Unternehmen auch gefragt, ob sie einen internen Datenschutzbeauftragten haben.

Besonders in der Gesundheitsbranche ist diese Rolle stark vertreten. Ein Großteil der Unternehmen in diesem Sektor verfügt über einen internen Datenschutzbeauftragten, deutlich mehr als im branchenübergreifenden Durchschnitt. Der Anteil liegt hier bei 58 Prozent, während er in der Gesamtwirtschaft 38 Prozent ausmacht. Mit zunehmender Unternehmensgröße steigt dieser Wert weiter auf 67 Prozent bei mittleren und auf 70 Prozent bei großen Unternehmen.

Während der Gesundheitssektor hier führend ist, weist die Handels- und Konsumgüterbranche mit 14 Prozent den niedrigsten Anteil auf. Datenschutz bleibt ein zentrales Thema, doch die personelle Absicherung variiert erheblich zwischen den Branchen. Viele Unternehmen setzen auf externe Datenschutzbeauftragte, um gesetzlichen Anforderungen gerecht zu werden und Fachkompetenz sicherzustellen.

Neben finanziellen Ressourcen spielt die Verfügbarkeit interner IT-Kompetenzen eine entscheidende Rolle für die Cybersecurity-Resilienz. Eine eigene IT-Abteilung haben 63 Prozent der Unternehmen, doch die Unterschiede zwischen kleinen und großen Unternehmen sind gravierend. Während fast alle Großunternehmen über interne IT-Teams verfügen, hat nahezu die Hälfte der kleinen Unternehmen keine eigene IT-Abteilung. Besonders schwach aufgestellt sind die Branchen Handel und Konsumgüter mit 22 Prozent sowie das Bauwesen mit 47 Prozent.

Auch die Größe der IT-Abteilungen unterscheidet sich deutlich. In kleinen Unternehmen sind IT-Teams meist sehr klein – über 70 Prozent haben höchstens fünf Arbeitsplätze, während größere Betriebe deutlich umfangreichere Strukturen aufweisen. In mittleren Unternehmen verfügen knapp die Hälfte der IT-Abteilungen über sechs bis zehn Arbeitsplätze, während in Großunternehmen elf bis 25 Arbeitsplätze am häufigsten sind. Rund ein Drittel der Großunternehmen hat mehr als 25 IT-Arbeitsplätze.

Mit der Unternehmensgröße steigt auch die Zahl der Mitarbeitenden, die sich ausschließlich mit IT-Security beschäftigen. In kleinen Unternehmen bleibt die IT-Sicherheit oft eine Zusatzaufgabe innerhalb der IT-Abteilung – fast alle Betriebe dieser Kategorie haben maximal fünf dedizierte Security-Fachkräfte (95 Prozent). In mittleren Unternehmen steigt die Zahl spezialisierter Mitarbeitender leicht an, doch auch hier verfügen die meisten nur über bis zu fünf Fachkräfte (74 Prozent).

Ein anderes Bild zeigt sich in großen Unternehmen. Mehr als zwei Drittel dieser Betriebe haben spezialisierte IT-Security-Teams mit mehr als fünf Mitarbeitenden. Rund ein Drittel beschäftigt zwischen elf und 25 Personen ausschließlich in der IT-Sicherheit und in einigen Fällen (vier Prozent) sind es sogar mehr als 25 Experten, die sich ausschließlich um den Schutz der Systeme kümmern.

Security Operations Center (SOC) sind ein zentraler Bestandteil einer proaktiven Sicherheitsstrategie, da sie Cyberbedrohungen in Echtzeit überwachen, analysieren und abwehren. Dennoch werden sie noch nicht flächendeckend genutzt. Jedes fünfte Unternehmen setzt bereits auf ein SOC, wobei hybride Modelle dominieren. Mehr als 40 Prozent der Unternehmen kombinieren interne und externe Spezialisten, um Expertise und modernste Technologien zu nutzen. Große Unternehmen setzen mit 59 Prozent besonders stark auf diese Mischform, während kleinere Betriebe häufig vollständig darauf verzichten. Die Größe der SOC-Teams variiert erheblich. Während Unternehmen mit weniger als 250 Mitarbeitenden meist mit maximal fünf Personen auskommen, verfügen sieben Prozent der großen Unternehmen über SOC-Teams mit mehr als 25 Experten.

Penetrationstests sind ein weiteres essenzielles Instrument zur Überprüfung der IT-Sicherheit, werden jedoch branchen- und größenabhängig unterschiedlich genutzt. Nur 37 Prozent der Unternehmen setzen regelmäßig auf Penetrationstests. Während zwei Drittel der kleinen Unternehmen vollständig darauf verzichten, führen 60 Prozent der großen Unternehmen mindestens halbjährlich Tests durch. Besonders häufig kommen diese in regulierungsintensiven Branchen wie Energie und Versorgung (90 Prozent) sowie im Finanzwesen (73 Prozent) zum Einsatz. In der Branche Handel und Konsumgüter hingegen liegt der Anteil bei lediglich 15 Prozent.

Die Nutzung von Cloud-Technologien hat sich in der deutschen Unternehmenslandschaft nahezu vollständig etabliert. Lediglich vier Prozent der Unternehmen verzichten darauf, was die Cloud als unverzichtbaren Bestandteil moderner IT-Infrastrukturen bestätigt. Unternehmen müssen jedoch sicherstellen, dass Sicherheits- und Datenschutzaspekte angemessen berücksichtigt werden, um die mit der Cloud verbundenen Risiken zu minimieren.

2.2 REGULATORISCHE HERAUSFORDERUNGEN UND NIS-2-UMSETZUNG

Die regulatorischen Anforderungen an die Cybersecurity nehmen in der Europäischen Union weiter zu und werden für Unternehmen zunehmend zur geschäftskritischen Aufgabe. Mit der Einführung der überarbeiteten „Network and Information Security (NIS) Directive"-2 (NIS-2) sind Unternehmen verpflichtet, neue Sicherheitsstandards zu implementieren, um ihre digitalen Infrastrukturen zu schützen und ihre Resilienz zu stärken. Unsere aktuelle Umfrage zeigt: Während größere Unternehmen und regulierte Branchen gut vorbereitet sind, besteht bei kleineren Unternehmen häufig Unsicherheit.

Die Mehrheit der befragten Unternehmen sieht sich gut gegen Cyberangriffe gewappnet. Zwei Drittel (66 Prozent) bewerten ihre Vorbereitung als gut oder sehr gut, während lediglich ein Prozent sie als nicht ausreichend

einschätzt – ein positives Signal angesichts wachsender Bedrohungen. Gleichzeitig gibt jedes dritte Unternehmen an, nur durchschnittlich vorbereitet zu sein.

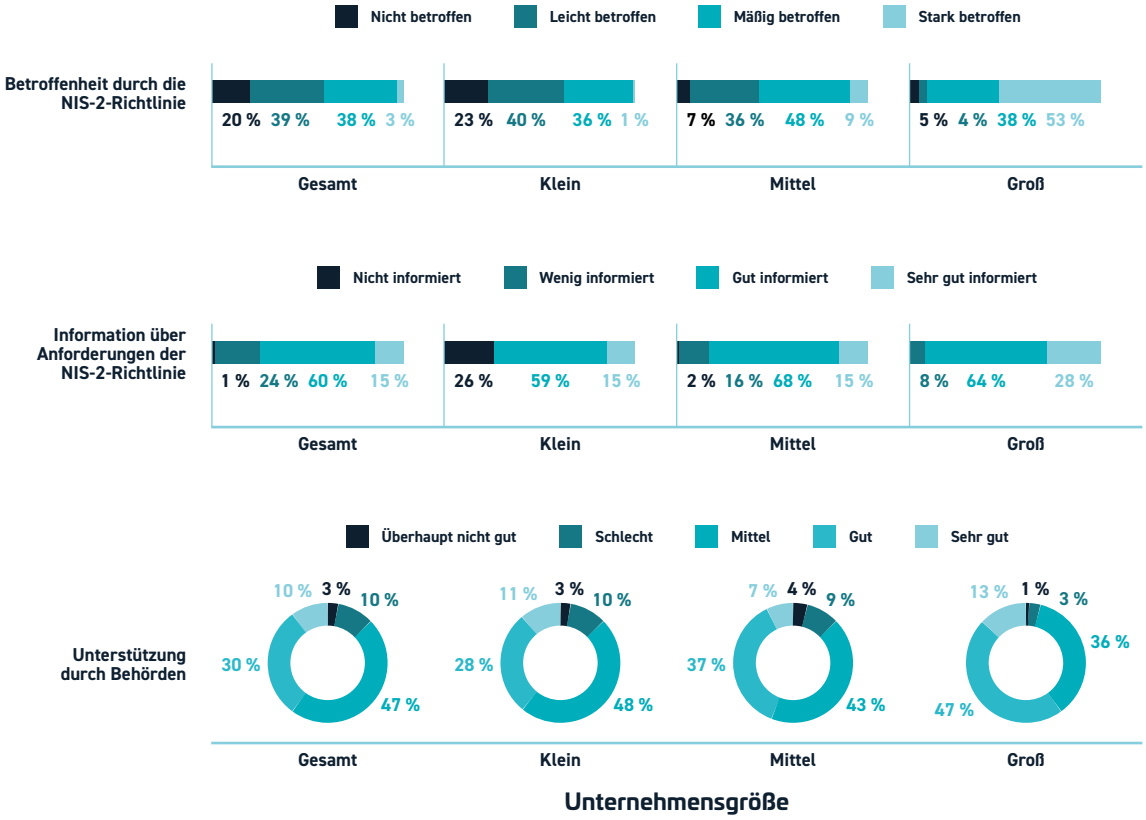
Besonders deutlich werden die Unterschiede zwischen kleinen und großen Unternehmen. Während 37 Prozent der kleinen Unternehmen ihre Vorbereitung als mittelmäßig einstufen, sehen sich mittlere und große Unternehmen mehrheitlich gut oder sehr gut gerüstet. Unternehmen mit klar definierten regulatorischen Vorgaben schneiden dabei besser ab. In der Energie- und Versorgungswirtschaft bewerten 84 Prozent der Unternehmen ihre Cybersecurity positiv, im Finanz- und Versicherungswesen sogar 92 Prozent.

Ein Blick auf internationale Vergleichsdaten zeigt Parallelen, aber auch Unterschiede. Ähnlich wie in der vorliegenden Studie schneiden bei der Frage nach der eigenen Cyberresilienz im Global Cybersecurity Outlook 2025 des WEF große Unternehmen insgesamt besser ab als kleinere. Während in der vorliegenden Umfrage nur ein Prozent der Unternehmen angibt, unzureichend auf Cyberangriffe vorbereitet zu sein, zeigt der WEF-Bericht ein anderes Bild für kleine Unternehmen auf globaler Ebene: 35 Prozent von ihnen bewerten ihre Cyberresilienz als unzureichend – ein Anteil, der sich seit 2022 versiebenfacht hat [6].

Fast die Hälfte der befragten Unternehmen gibt an, von NIS-2 betroffen zu sein – mit deutlichen Unterschieden zwischen kleinen und großen Unternehmen (siehe Abbildung 14). Während 91 Prozent der großen Unternehmen unter die Richtlinie fallen, spielt sie für kleinere Betriebe eine geringere Rolle. Einige von ihnen unterschätzen jedoch möglicherweise, dass sie direkt oder indirekt über die Lieferkette betroffen sein könnten. Grundsätzlich gilt NIS-2 für Unternehmen mit mehr als 50 Mitarbeitenden und einem Jahresumsatz von über zehn Millionen Euro. Doch sogenannte „Essential Entities“ (kritische Einrichtungen wie Energieversorger oder Banken) und „Important Entities“ (wichtige, aber nicht systemkritische Unternehmen wie IT-Dienstleister oder Chemieunternehmen) unterliegen unabhängig von Größe oder Umsatz den Vorschriften. Hinzu kommt: Große Unternehmen können von ihren Zulieferern die Einhaltung der NIS-2-Standards verlangen, wodurch sich die Anforderungen entlang der gesamten Wertschöpfungskette ausweiten [92].

Regulierungen stärken die Cybersecurity, stellen Unternehmen aber vor Herausforderungen. Der Global Cybersecurity Outlook 2025 des WEF zeigt, dass 78 Prozent der Führungskräfte sie als wirksam einstufen, während zwei Drittel die wachsende Anzahl und Komplexität der Vorschriften als Problem sehen [6].

Dieses Spannungsfeld zeigt sich ebenfalls in der vorliegenden Untersuchung, in der die regulatorische Unterstützung ambivalent bewertet wird. NIS-2-betroffene Unternehmen – insbesondere mittlere und große – sind gut informiert und vorbereitet. Dennoch empfinden fast zwei Drittel (60 Prozent) der betroffenen Unternehmen die staatliche Unterstützung als nicht ausreichend (siehe Abbildung 14), bei KRITIS-Unternehmen sind es immerhin 49 Prozent. Gleichzeitig zeigt die Bitkom-Studie zum Wirtschaftsschutz, dass 75 Prozent der Befragten Sicherheitsbehörden für weitgehend machtlos gegenüber Cyberattacken aus dem Ausland halten [30]. Dies verdeutlicht eine Diskrepanz zwischen der Unterstützung bei der Umsetzung regulatorischer Vorgaben und der allgemeinen Einschätzung der staatlichen Handlungsfähigkeit im Bereich Cybersecurity. Ein möglicher Grund für diese Kritik ist, dass NIS-2 zum Zeitpunkt der Um-



Quelle: [255]

Abbildung 14: Betroffenheit durch die NIS-2-Richtlinie, Informationsstand zu den Anforderungen und wahrgenommene Unterstützung durch Behörden (in %)

frage noch nicht vollständig in nationales Recht überführt war und viele Unternehmen den konkreten Handlungsbedarf noch nicht abschließend bewerten konnten. Trotz dieser Unsicherheiten fühlen sich drei Viertel der betroffenen Unternehmen gut oder sehr gut über NIS-2 informiert.

Die Mehrheit der von NIS-2 betroffenen Unternehmen setzt bei der Umsetzung der Richtlinie auf interne Ressourcen. Lediglich 16 Prozent haben externe Berater oder Partner hinzugezogen, um die Einhaltung der neuen Vorgaben sicherzustellen. Dabei zeigt sich ein deutlicher Größenunterschied: Während 35 Prozent der mittleren und 59 Prozent der großen Unternehmen externe Unterstützung in Anspruch nehmen, verzichten kleinere Betriebe weitgehend darauf.

Ein wesentlicher Faktor ist der Ressourcenzugang. Größere Unternehmen verfügen über die finanziellen Mittel, externe Expertise zu nutzen, während kleinere Betriebe die Anforderungen intern bewältigen müssen. Besonders Unternehmen der kritischen Infrastruktur setzen überdurchschnittlich häufig auf externe Beratung: 58 Prozent von ihnen nutzen Berater, verglichen mit nur 13 Prozent der nicht KRITIS-betroffenen Unternehmen.

Neue regulatorische Vorgaben stoßen oft zunächst auf Zurückhaltung – verstärkt durch fehlende nationale Gesetzesübersetzungen. Viele Unternehmen zeigen sich in dieser frühen Phase optimistisch, doch mit der Konkretisierung der Anforderungen könnte diese Einschätzung nachlassen.

Die Botschaft ist klar: NIS-2 wird die Cybersecurity-Landschaft nachhaltig verändern. Besonders kleinere Unternehmen und solche, die bisher nicht unter spezifische Cybersicherheitsanforderungen fielen, müssen aktiv werden, um die neuen Vorgaben zu erfüllen. Gleichzeitig zeigt sich, dass Unternehmen mit umfangreicheren Ressourcen frühzeitig Maßnahmen ergreifen, während kleinere Betriebe oft abwarten.

Die Richtlinie bringt jedoch nicht nur Herausforderungen, sondern auch Chancen. Wer sich frühzeitig mit den Vorgaben auseinandersetzt, stärkt nicht nur die Compliance, sondern verbessert auch die eigene Resilienz gegenüber Cyberbedrohungen – ein entscheidender Wettbewerbsvorteil in einer zunehmend digitalisierten Geschäftswelt.

2.3 CYBERSECURITY IN DER LIEFERKETTE

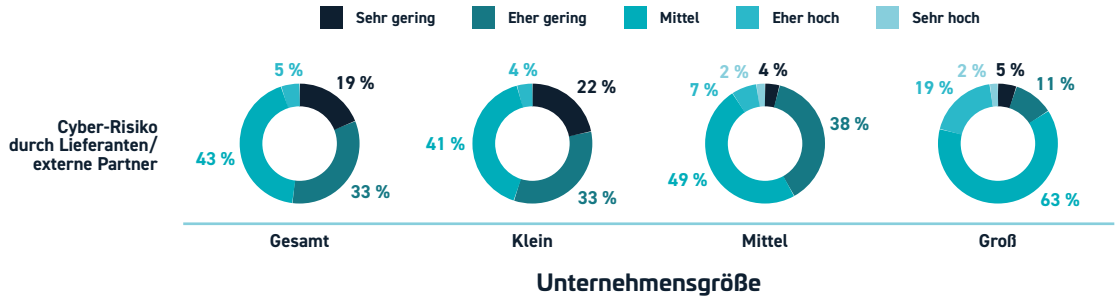
Die Absicherung von Lieferketten gewinnt angesichts zunehmender Cyberbedrohungen an Bedeutung. Dennoch zeigt sich ein starkes Gefälle in der Wahrnehmung und Umsetzung entsprechender Sicherheitsmaßnahmen. Im Durchschnitt sehen über die Hälfte (52 Prozent) der befragten Unternehmen kein Cyber-Risiko durch ihre Lieferanten oder externen Partner (siehe Abbildung 15). Damit liegen die Ergebnisse über denen der Bitkom-Studie zum Wirtschaftsschutz, die zeigt, dass 37 Prozent der dort befragten Unternehmen angeben, in ihren Organisationen fehle es an ausreichendem Bewusstsein für diese Risiken [30]. Besonders auffällig: Kleinere Unternehmen neigen häufiger als große Unternehmen dazu, Cyberrisiken in ihrer Lieferkette zu unterschätzen oder gar auszuschließen. Fünfundfünzig Prozent der kleinen Unternehmen stufen das Risiko als „eher gering" oder „sehr gering" ein, während größere Unternehmen tendenziell vorsichtiger sind und zu 84 Prozent das Risiko als mindestens „mittel" bewerten. Ein möglicher Grund dafür könnte sein, dass kleine Unternehmen häufig als Teil einer größeren Lieferkette agieren, statt selbst Hauptakteur zu sein. Zudem fehlen ihnen oft die personellen und finanziellen Ressourcen für umfassende Risikoanalysen.

Ein weltweiter Vergleich zeigt eine andere Perspektive: In der WEF-Befragung in 57 Ländern betrachten 54 Prozent der großen Unternehmen die Sicherheit der Lieferkette als größte Herausforderung für ihre Cyberresilienz. Besonders problematisch wird die zunehmende Komplexität und mangelnde Transparenz in den Lieferketten gesehen. Schwachstellen in von Dritten bereitgestellter Software sowie sich ausbreitende Cyberangriffe im gesamten Ökosystem gelten dabei als zentrale Risiken [6].

Die Ergebnisse der Bitkom-Studie zum Wirtschaftsschutz 2024 zeigen wiederum, dass die Bedrohungen durch Angriffe auf Zulieferer real sind. 13 Prozent der befragten Unternehmen wissen sicher, dass ihre Zulieferer in den letzten zwölf Monaten Opfer von Datendiebstahl, Industriespionage oder Sabotage wurden. Weitere 13 Prozent vermuten einen solchen Vorfall. 44 Prozent der betroffenen Unternehmen mussten dadurch einen signifikanten Geschäftsausfall verzeichnen [92].

Die unterschiedliche Wahrnehmung von Risiken zeigt sich auch in den Sicherheitsanforderungen an Lieferanten. Während nur 16 Prozent der kleinen Unternehmen verbindliche Cybersecurity-Anforderungen für alle ihre Lieferanten festgelegt haben, steigt dieser Anteil auf 23 Prozent bei mittleren Unternehmen und 40 Prozent bei großen Unternehmen. KRITIS-Unternehmen liegen mit 49 Prozent nochmals darüber.

Zusätzlich setzen viele Unternehmen Sicherheitsvorgaben für ausgewählte Lieferanten um. Insgesamt 41 Prozent der befragten Unternehmen formulieren solche



Quelle: [255]

Abbildung 15: Einschätzung des Cyber-Risikos durch Lieferanten und externe Partner (in %)

Anforderungen nur für bestimmte Zulieferer. Besonders deutlich zeigt sich dies in großen Unternehmen: 85 Prozent setzen entweder für alle (40 Prozent) oder für einige (45 Prozent) ihrer Lieferanten Sicherheitsanforderungen durch.

Mittlere Unternehmen zeigen eine gemischte Herangehensweise. Achtzehn Prozent der Unternehmen haben aktuell keine verbindlichen Anforderungen, planen aber deren Einführung, während 15 Prozent dies derzeit nicht vorsehen. Kleine Unternehmen gehen mit dem Thema uneinheitlich um. 56 Prozent von ihnen haben bereits Cybersecurity-Anforderungen für ihre Lieferanten definiert – 16 Prozent für alle, 40 Prozent für einige. Gleichzeitig zeigt sich jedoch, dass 34 Prozent der kleinen Unternehmen keine Pläne zur Einführung entsprechender Maßnahmen haben.

Die Überprüfung von Cybersecurity-Maßnahmen wie der Einhaltung von Sicherheitsstandards bei Lieferanten zeigt ebenso erhebliche Unterschiede zwischen den Unternehmen. Während 80 Prozent der großen Unternehmen ihre Lieferanten regelmäßig oder gelegentlich überprüfen, liegt dieser Anteil über alle Unternehmensgrößen hinweg bei nur 49 Prozent. Ein Drittel der Unternehmen verzichtet vollständig auf eine Überprüfung. Besonders aktiv sind Unternehmen aus dem Finanz- und Versicherungswesen sowie aus der Energieversorgung: 79 Prozent dieser Unternehmen bewerten die Sicherheitsmaßnahmen ihrer Lieferanten. Im Gegensatz dazu sind Unternehmen aus der Handels- und Konsumgüterbranche mit nur elf Prozent am seltensten in der Überprüfung aktiv.

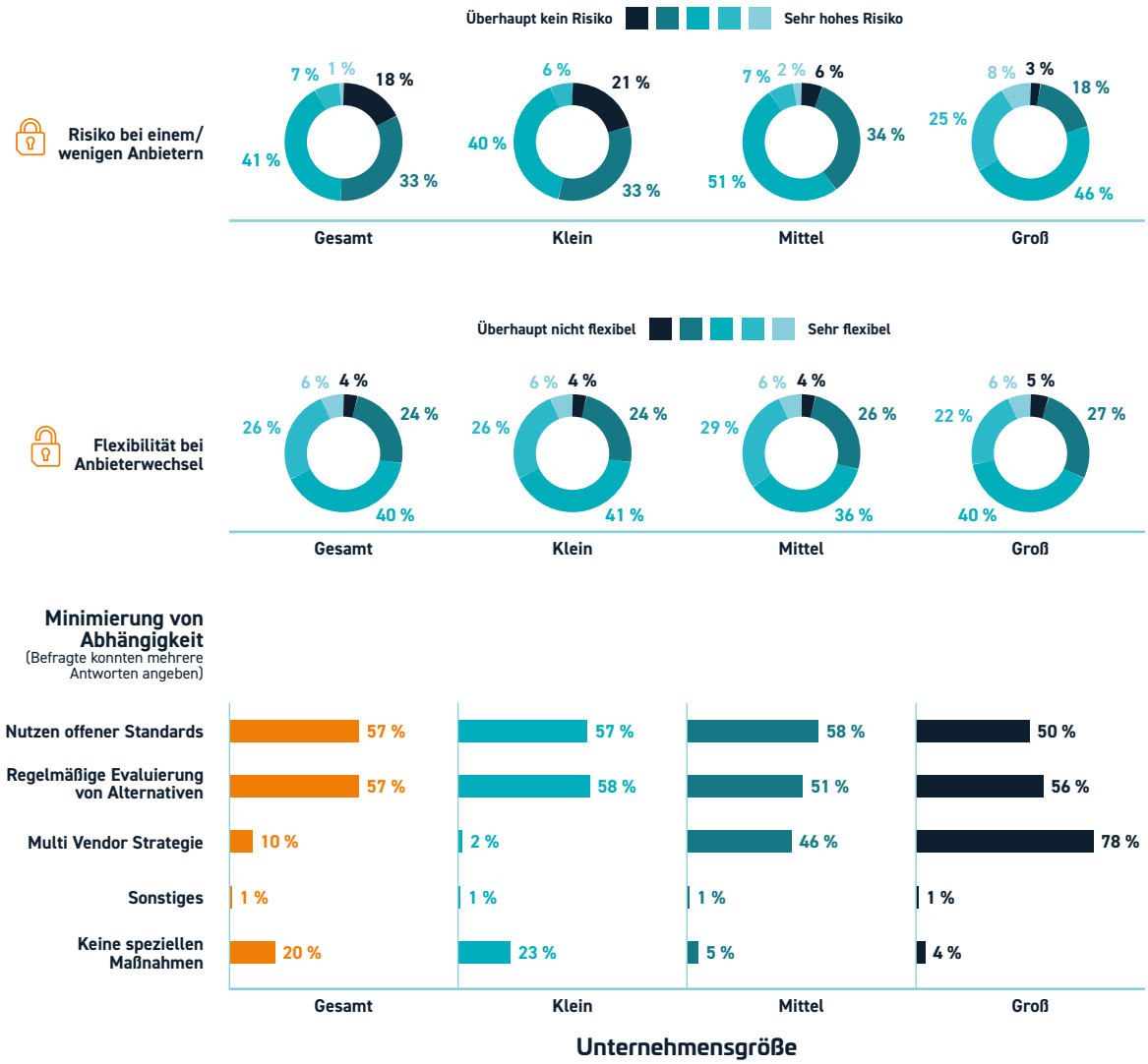
Der Anteil der Unternehmen, die ihre Lieferanten regelmäßig auf Cybersecurity-Standards prüfen, liegt mit 13 Prozent knapp unter dem in der Bitkom-Studie zum Wirtschaftsschutz ermittelten Wert von 19 Prozent [30]. Allerdings zeigt sich ein positiver Trend: 36 Prozent der Unternehmen – unabhängig von ihrer Größe – führen zumindest gelegentliche Prüfungen durch. Kleine und mittlere Unternehmen liegen hier nahezu gleichauf: 36 Prozent der kleinen und 35 Prozent der mittleren Unternehmen überprüfen ihre Lieferanten gelegentlich. Deutliche Unterschiede gibt es jedoch bei regelmäßigen Überprüfungen. Während nur zehn Prozent der kleinen Unternehmen ihre Lieferanten regelmäßig prüfen, steigt dieser Anteil bei mittleren Unternehmen auf 26 Prozent und bei großen Unternehmen auf 43 Prozent. Dies deutet darauf hin, dass mit steigender Unternehmensgröße nicht nur das Bewusstsein für Risiken zunimmt, sondern auch die Ressourcen zur Umsetzung systematischer Überprüfungen vorhanden sind.

Unternehmen, die zumindest anlassbezogen die Cybersecurity-Maßnahmen ihrer Lieferanten überprüfen, wurden auch zur Häufigkeit ihrer Audits und Assessments befragt. Dazu zählen beispielsweise Sicherheitsüberprüfungen durch interne oder externe Auditoren oder Penetrationstests. 70 Prozent der großen Unternehmen auditieren ihre Lieferkette mindestens einmal jährlich oder häufiger. Über alle Unternehmensgrößen hinweg führen 29 Prozent der Unternehmen ihre Audits jährlich oder häufiger durch, 24 Prozent alle zwei Jahre, während 16 Prozent seltenere Intervalle angeben. Insgesamt verzichten etwa 30 Prozent der Unternehmen gänzlich auf regelmäßige Audits ihrer Lieferkette. Besonders kleine Unternehmen führen seltener Audits oder Assessments durch – mehr als ein Drittel verzichtet vollständig darauf.

Ein deutlicher Branchenunterschied zeigt sich ebenfalls: Unternehmen aus dem Finanz- und Versicherungswesen (83 Prozent) sowie aus der Energie- und Versorgungsbranche (82 Prozent) auditieren ihre Lieferanten mindestens alle zwei Jahre oder häufiger. Im Gegensatz dazu liegt der Anteil in der Handels- und Konsumgüterbranche mit nur 14 Prozent auf dem niedrigsten Niveau.

2.4 IT-ANBIETERSTRATEGIEN UND DAS RISIKO VON VENDOR-LOCK-INS

Cybersecurityprodukte sind ein zentraler Baustein jeder Sicherheitsstrategie. Sie dienen dazu, Cyberangriffe abzuwehren und die digitale Resilienz zu stärken. Doch die Wahl der richtigen Anbieter hat weitreichende Folgen. Ein Vendor-Lock-in – die starke Abhängigkeit von einem einzelnen Anbieter – kann Flexibilität einschränken, Kos-



Quelle: [255]

Abbildung 16: Vendor-Lock-in in der Cybersecurity: Risiko, Flexibilität und Gegenmaßnahmen (in %)

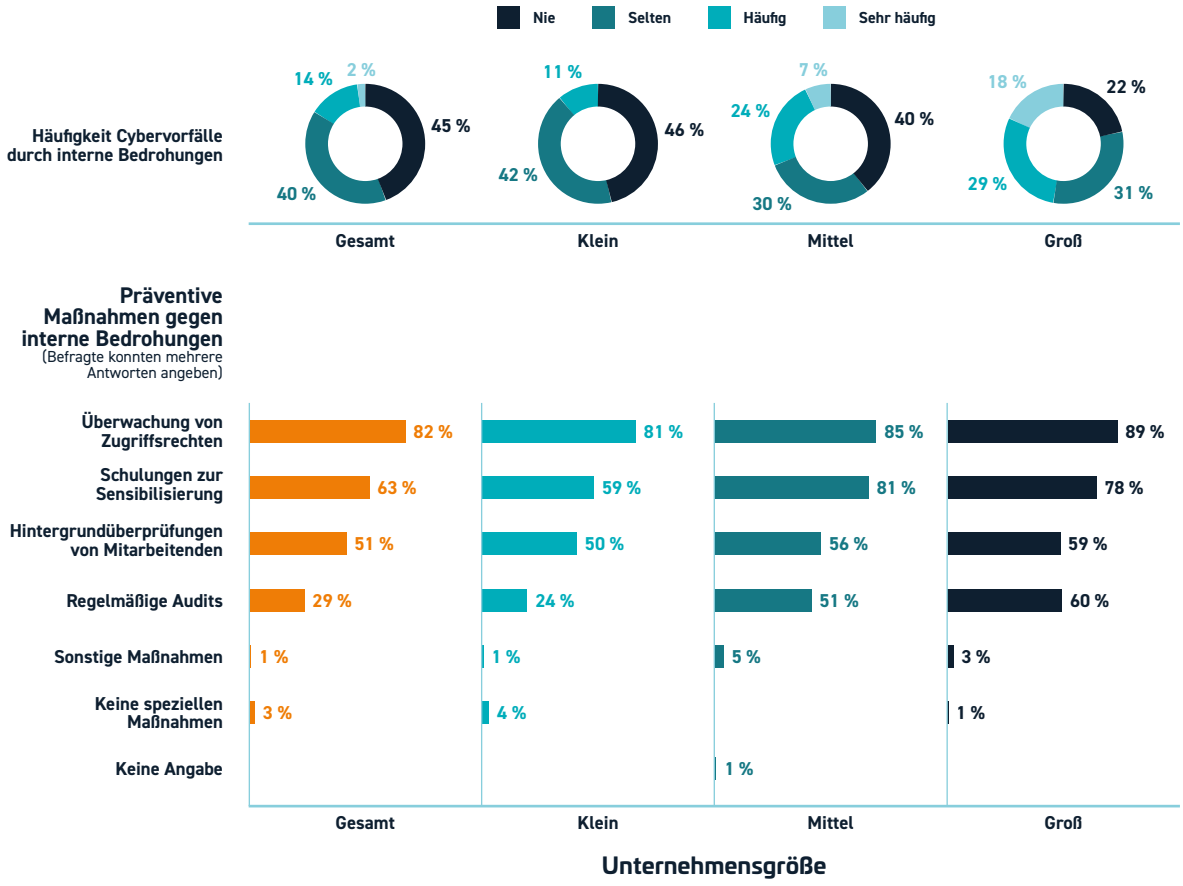
ten erhöhen und die Anpassung an neue Bedrohungen erschweren. Besonders in der Cybersecurity stellt dies eine Herausforderung dar: Fehlende Kompatibilität zwischen Anbietern und hohe Wechselkosten erschweren es Unternehmen, schnell auf neue Bedrohungen zu reagieren oder innovative Lösungen zu integrieren.

Die vorliegenden Erhebungen zeigen eine riesige Diskrepanz zwischen kleinen und großen Unternehmen in ihrer Anbieterstrategie. Während kleine Unternehmen fast ausschließlich auf Komplettlösungen eines einzelnen Anbieters setzen (93 Prozent), nutzen 88 Prozent der großen Unternehmen mehrere Anbieter. Je größer das Unternehmen, desto geringer ist die Abhängigkeit von einem einzigen Anbieter. Mittlere Unternehmen sind nahezu gleich verteilt: 49 Prozent setzen auf einen einzelnen Anbieter, 50 Prozent nutzen mehrere Anbieter.

Auch die Wahrnehmung der damit verbundenen Risiken unterscheidet sich deutlich (siehe Abbildung 16). Nur sechs Prozent der kleinen Unternehmen sehen in der Konzentration auf ein oder wenige Produkte ein hohes Risiko und liegen damit knapp unter dem Durchschnitt (acht Prozent), während dieser Anteil bei großen Unternehmen 33 Prozent beträgt.

Um die Risiken eines Vendor-Lock-ins zu reduzieren, setzen Unternehmen verschiedene Maßnahmen ein. Mehr als 50 Prozent der befragten Unternehmen – unabhängig von ihrer Größe – nutzen offene Standards oder evaluieren regelmäßig alternative Anbieter. Dies sind wichtige Maßnahmen, um langfristige Bindungen an einzelne Anbieter zu vermeiden (siehe Abbildung 16).

Die Sicherheitsprobleme bei CrowdStrike im Juli 2024 haben gezeigt, dass Unternehmen mit einer Multi-Vendor-Strategie schneller auf alternative Systeme umstel-



Quelle: [255]

Abbildung 17: Häufigkeit von Cybervorfällen durch interne Bedrohungen und in den letzten 12 Monaten und präventive Sicherheitsmaßnahmen (in %)

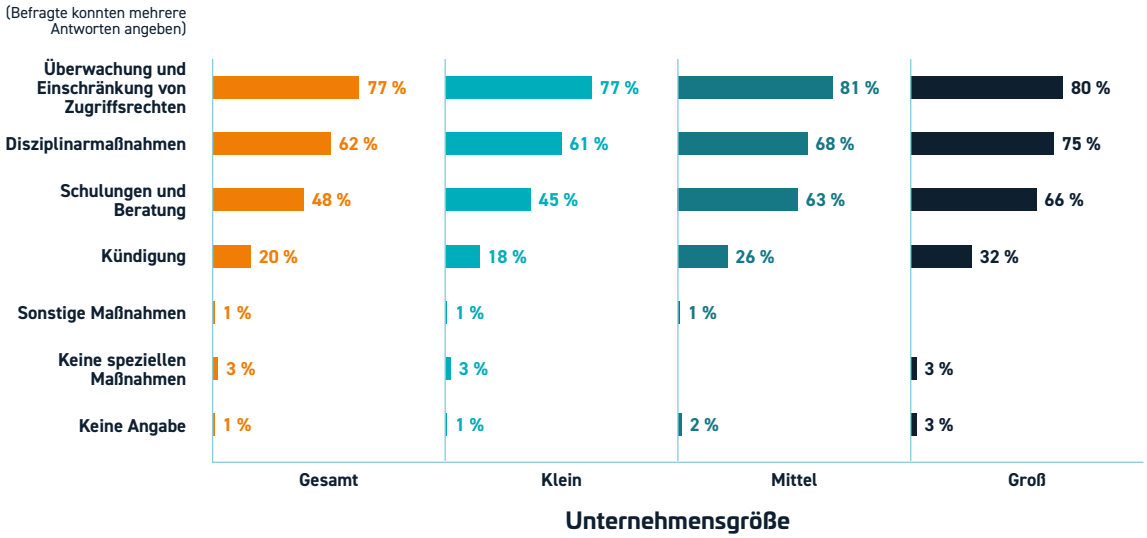
len konnten, während stark abhängige Unternehmen mit längeren Ausfallzeiten konfrontiert waren. Allerdings bleibt die tatsächliche Umsetzung einer Multi-Vendor-Strategie herausfordernd. Aktiv verfolgen 78 Prozent der großen Unternehmen eine Multi-Vendor-Strategie, um Abhängigkeiten gezielt zu reduzieren. Dies bedeutet, dass sie nicht nur mehrere Anbieter nutzen, sondern ihre IT-Infrastruktur gezielt so gestalten, dass Abhängigkeiten reduziert werden. Bei kleinen Unternehmen ist diese Strategie weniger verbreitet (zwei Prozent), da die Verwaltung mehrerer Anbieter erhebliche personelle und finanzielle Ressourcen erfordert.

Unabhängig von den getroffenen Maßnahmen bleibt die tatsächliche Umsetzung einer flexiblen Anbieterstrategie für viele Unternehmen eine Herausforderung. Nur 32 Prozent der Unternehmen sehen sich in der Lage, ihre Anbieter flexibel zu wechseln (siehe Abbildung 16). Dies zeigt, dass die Nutzung mehrerer Anbieter oder die Einführung offener Standards allein nicht automatisch zu einer hohen Anpassungsfähigkeit führt.

2.5 INTERNE RISIKEN

Interne Bedrohungen stellen ein ernstzunehmendes und oft unterschätztes Risiko für Unternehmen jeder Größe dar. Obwohl sie häufig als Teil des akzeptierten Risikoprofils betrachtet werden, gehören sie zu den schwierigsten Herausforderungen im Bereich der Cybersecurity. Besonders alarmierend sind die aktuellen Zahlen der Bitkom-Studie zum Wirtschaftsschutz: 27 Prozent der Cyberangriffe gehen auf vorsätzlich handelnde (ehemalige) Mitarbeiter zurück, während 23 Prozent unbeabsichtigt durch aktuelle oder ehemalige Beschäftigte verursacht werden [30]. Ein Blick auf internationale Einschätzungen zeigt eine abweichende Wahrnehmung. Im Global Cybersecurity Outlook 2025 des WEF nannten lediglich sieben Prozent der Befragten böswillige Insider als ihre größte Cybersecurity-Bedrohung – im Vergleich zu anderen Risiken rangiert dieses Thema weltweit weit unten auf der Prioritätenliste [6].

Die Zahlen der Bitkom-Studie decken sich mit den Ergebnissen unserer aktuellen Umfrage. Während 45 Prozent der Unternehmen in den letzten zwölf Monaten keine internen Bedrohungen registriert haben, geben 40 Prozent an, solche Vorfälle zumindest selten erlebt zu ha-



Quelle: [255]

Abbildung 18: Umgang mit Mitarbeitenden, die als potenzielle interne Bedrohung gelten (in %)

ben. Betrachtet man die Häufigkeit solcher Bedrohungen nach Unternehmensgröße, zeigt sich ein klares Muster: In kleinen Unternehmen berichten elf Prozent von häufigen Vorfällen, weniger als ein Prozent von sehr häufigen. In mittleren Betrieben steigt der Anteil auf 24 Prozent häufige und sieben Prozent sehr häufige Vorfälle. Großunternehmen sind mit 29 Prozent häufigen und 18 Prozent sehr häufigen Vorfällen am stärksten gefährdet (siehe Abbildung 17).

Die Daten verdeutlichen, dass sich interne Bedrohungen mit wachsender Unternehmensgröße verstärken. Während die Bitkom-Studie das grundsätzliche Risiko durch interne Akteure aufzeigt, machen die aktuellen Zahlen deutlich, dass insbesondere große Unternehmen betroffen sind. Kleinere Betriebe mögen seltener Ziel interner Angriffe sein, doch auch sie sind nicht immun.

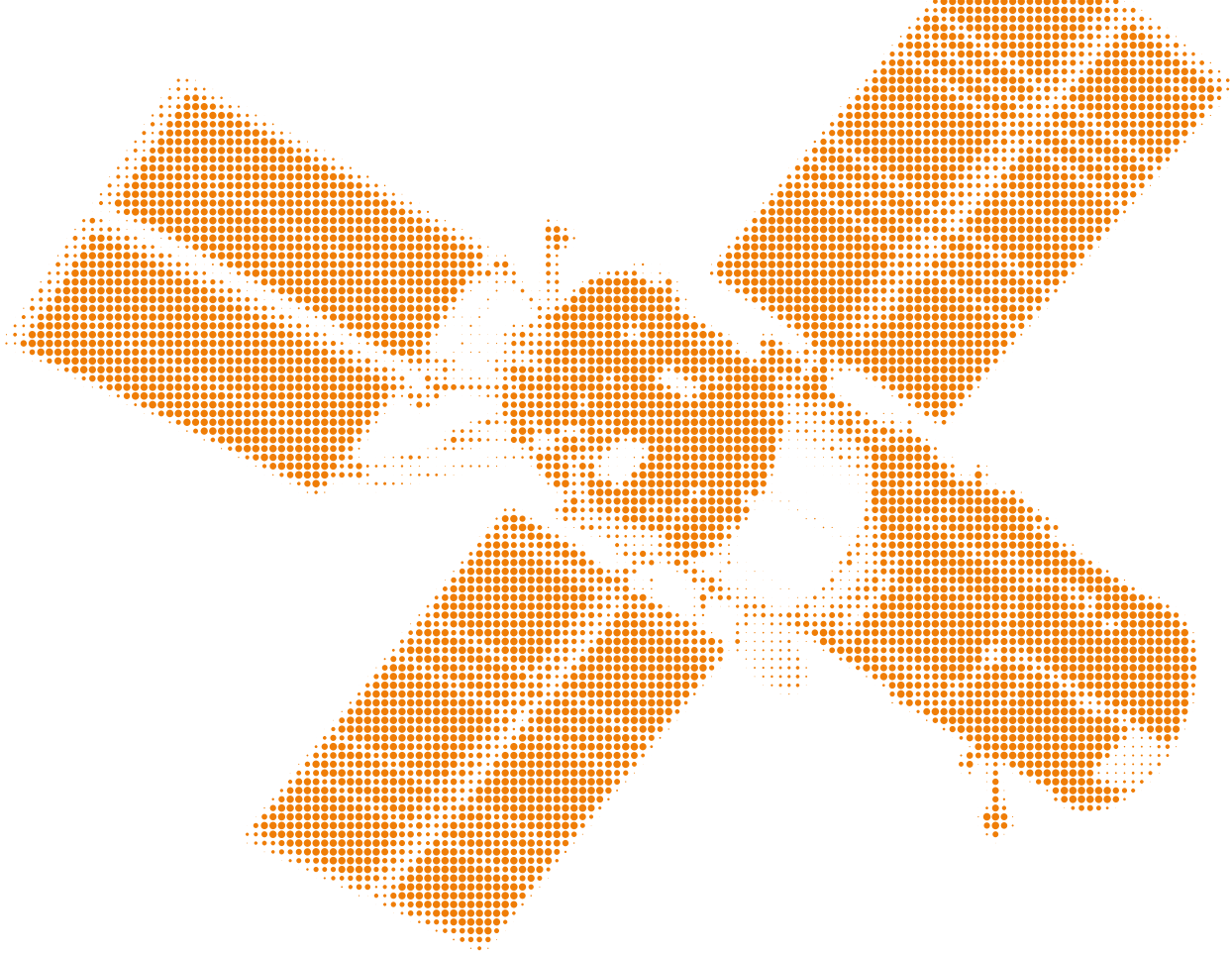
Um interne Bedrohungen zu bewältigen, setzen Unternehmen in erster Linie auf technische Maßnahmen, die Vertraulichkeit, Integrität und Verfügbarkeit sensibler Daten sicherstellen sollen (siehe Abbildung 17). Besonders verbreitet ist die Kontrolle von Zugriffsrechten: 82 Prozent der Befragten geben an, den Zugriff auf Systeme und Daten streng zu überwachen und einzuschränken. Auch präventive Maßnahmen wie Hintergrundüberprüfungen von Mitarbeitenden sind mit 51 Prozent weit verbreitet.

Bei Schulungen zur Sensibilisierung zeigen sich deutliche Unterschiede nach Unternehmensgröße. Während 81 Prozent der mittleren Unternehmen solche Schulungen regelmäßig durchführen, sind es bei großen Unternehmen 78 Prozent und bei kleinen lediglich 59 Prozent. Trotz der höheren Ressourcen größerer Unternehmen fällt ihr Engagement in diesem Bereich nicht wesentlich höher aus als bei mittleren Unternehmen.

Ein vergleichbares Muster zeigt sich bei regelmäßigen Audits als Maßnahme der Gefahrenmitigation interner Bedrohungen. Ihr Anteil steigt mit zunehmender Unternehmensgröße an: 24 Prozent der kleinen Unternehmen setzen darauf, während der Anteil bei mittleren Unternehmen auf 51 Prozent und in großen Unternehmen auf 60 Prozent ansteigt. Dies weist darauf hin, dass größere Organisationen stärker auf strukturierte Kontrollmechanismen setzen, während kleinere Unternehmen solche Maßnahmen seltener implementieren.

Die Mehrheit der Unternehmen schätzt ihre IT-Infrastruktur im Hinblick auf interne Bedrohungen als gut oder besser ein. Sechzig Prozent der Befragten sind der Ansicht, dass ihre Sicherheitslage angemessen ist. Unterschiede zwischen den Unternehmensgrößen sind dabei erkennbar: Kleine Unternehmen bewerten ihre Sicherheitsmaßnahmen zu 58 Prozent positiv, mittlere zu 70 Prozent und große zu 86 Prozent.

Beim Umgang mit Mitarbeitenden, die eine potenzielle internen Bedrohung darstellen könnten, setzen 77 Prozent der Unternehmen auf die Überwachung und Einschränkung von Zugriffsrechten (siehe Abbildung 18). Dieses Vorgehen ist über alle Unternehmensgrößen hinweg weit verbreitet: Kleine Unternehmen geben dies zu



77 Prozent an, mittlere zu 81 Prozent und große zu 80 Prozent. Disziplinarmaßnahmen werden von 62 Prozent der Unternehmen ergriffen, wobei ihr Einsatz mit zunehmender Unternehmensgröße ansteigt – von 61 Prozent bei kleinen Unternehmen über 68 Prozent bei mittleren bis zu 75 Prozent bei großen Unternehmen. Schulungen und Beratungsangebote werden insgesamt seltener genutzt. Während 45 Prozent der kleinen Unternehmen darauf setzen, sind es bei mittleren 63 Prozent und bei großen 66 Prozent.

Ein deutlicher Unterschied zeigt sich bei der Kündigungspraxis. Während nur 18 Prozent der kleinen Unternehmen diesen Schritt wählen, steigt der Anteil bei mittleren Unternehmen auf 26 Prozent und bei großen auf 32 Prozent. Größere Unternehmen scheinen somit entschlossener, sich von potenziell risikobehafteten Mitarbeitenden zu trennen. Dies könnte darauf hindeuten, dass in kleineren Strukturen persönlichere Bindungen und flachere Hierarchien eine Rolle spielen, die den Umgang mit internen Bedrohungen beeinflussen.

2.6 CYBERSECURITY IM WELTRAUM

Satellitenkommunikation ist ein unverzichtbarer Bestandteil moderner digitaler Infrastrukturen. Sie ermöglicht globale Datenübertragung, Navigation und Kommunikation – oft unbemerkt, aber essenziell für zahlreiche Branchen. Gleichzeitig wächst die Abhängigkeit von diesen Technologien, wodurch sie zunehmend ins Visier von Cyberangriffen geraten. Dennoch bleibt das Risikobewusstsein vieler Unternehmen gering.

Die vorliegenden Erhebungen zeigen eine deutliche Diskrepanz zwischen Nutzung und Sicherheitsbewusstsein. Während 59 Prozent der Befragten das Risiko für Cyberangriffe auf Satelliten als gering oder nicht existent einstufen, erkennen lediglich 13 Prozent eine erhöhte Bedrohung. Insbesondere kleine und mittlere Unternehmen unterschätzen die Gefahr: Rund 60 Prozent dieser Unternehmen stufen das Risiko als niedrig ein. Im Gegensatz dazu zeigen größere Unternehmen ein stärkeres Risikobewusstsein – 70 Prozent bewerten die Bedrohung als „mittel" bis „hoch", fünf Prozent sogar als „sehr hoch". Besonders ausgeprägt ist diese Einschätzung in der Energie- und Versorgungsbranche, wo 35 Prozent der Unternehmen das Risiko als „hoch" einstufen.

Dass Satellitenkommunikation auf globaler Ebene bislang kaum als sicherheitskritischer Faktor wahrgenommen wird, zeigt auch der Global Cybersecurity Outlook 2025 des WEF. Lediglich zwei Prozent der befragten Unternehmen sehen Satellitentechnologien als einen der maßgeblichen Einflussfaktoren für die Cybersicherheitslage in den kommenden zwölf Monaten [6].

In der vorliegenden Untersuchung spiegelt sich diese Wahrnehmung direkt in den getroffenen Schutzmaßnahmen wider. Während 32 Prozent der großen Unternehmen umfassende Sicherheitsmaßnahmen implementiert haben, sind es bei kleinen und mittleren Betrieben im

Durchschnitt nur sieben Prozent. Je größer das Unternehmen, desto gezielter werden Investitionen in die Absicherung der Satellitenkommunikation getätigt. Besonders in der Energie- und Versorgungsbranche zeigt sich dieser Trend: 67 Prozent der Unternehmen haben zumindest grundlegende Sicherheitsvorkehrungen getroffen, zwölf Prozent setzen sogar auf umfassende Schutzmechanismen.

Auffällig ist, dass ein Drittel der befragten Unternehmen das Thema Sicherheit in der Satellitenkommunikation als nicht relevant betrachtet. Dabei gewinnt diese Infrastruktur strategisch zunehmend an Bedeutung. Die fortschreitende Digitalisierung und Globalisierung machen Satellitenkommunikation zu einem unverzichtbaren Faktor in Unternehmensnetzwerken, Lieferketten und industriellen Prozessen. Unternehmen, die sich frühzeitig mit den damit verbundenen Risiken auseinandersetzen, stärken nicht nur die eigene Sicherheitsstrategie, sondern sichern langfristig ihren Geschäftsbetrieb.

2.7 FAZIT

Die Ergebnisse der vorliegenden Erhebungen verdeutlichen, dass Cybersecuritystrategien maßgeblich von der Unternehmensgröße und den verfügbaren Ressourcen abhängen. Große Unternehmen sind in nahezu allen sicherheitsrelevanten Bereichen besser aufgestellt. Sie verfügen über umfangreichere IT-Ressourcen, setzen verstärkt auf Cloud-Hyperscaler und investieren gezielt in Cybersecurity, Security Operations Center (SOCs) sowie Penetrationstests. Zudem führen sie häufiger Lieferketten-Audits durch, beschäftigen Datenschutzbeauftragte und greifen verstärkt auf externe Spezialisten zurück, beispielsweise zur Umsetzung regulatorischer Anforderungen wie NIS-2. Ein weiteres wesentliches Merkmal großer Unternehmen ist die geringere Abhängigkeit von einzelnen Anbietern: Durch eine Multi-Vendor-Strategie senken sie gezielt das Risiko eines Vendor-Lock-ins.

In einem Bereich zeigt sich hingegen kaum ein Unterschied zwischen großen und mittleren Unternehmen: Bei der Bekämpfung interner Bedrohungen durch aktuelle oder ehemalige Mitarbeitende setzen beide Gruppen in ähnlicher Intensität auf Schulungen, Audits und disziplinarische Maßnahmen.

Besonders auffällig ist der Rückstand der Branche Handel und Konsumgüter. Unternehmen in diesem Sektor verfügen häufig über weniger IT- und Cybersecurity-Ressourcen, verzichten überdurchschnittlich oft auf Datenschutzbeauftragte und führen seltener Penetrationstests sowie Lieferketten-Audits durch. Diese Defizite erhöhen die Verwundbarkeit gegenüber Cyberangriffen und regulatorischen Anforderungen.

Ein positives Signal kommt hingegen von KRITIS-Unternehmen. Banken, Versicherungen, Unternehmen aus dem Gesundheitswesen sowie aus der Energie- und Versorgungsbranche sind deutlich besser aufgestellt als nicht-kritische Unternehmen. Sie investieren gezielt in Cybersecurity und nehmen ihre gesellschaftliche und wirtschaftliche Verantwortung ernst.

Insgesamt zeigt sich eine wachsende Bereitschaft zur Investition in IT-Sicherheit. Trotz wirtschaftlicher Herausforderungen, regulatorischem Druck und internen Risiken setzen Unternehmen verstärkt auf den Ausbau ihrer Sicherheitsmaßnahmen – ein wichtiger Schritt für die langfristige Resilienz der deutschen Wirtschaft.

KAPITEL 3

GRENZENLOS BEDROHT
CYBERGEFAHREN VOM MEERESGRUND BIS INS WELTALL

GEO
36.000 km

20.500 km

MEO

5.000 km

1.200 km

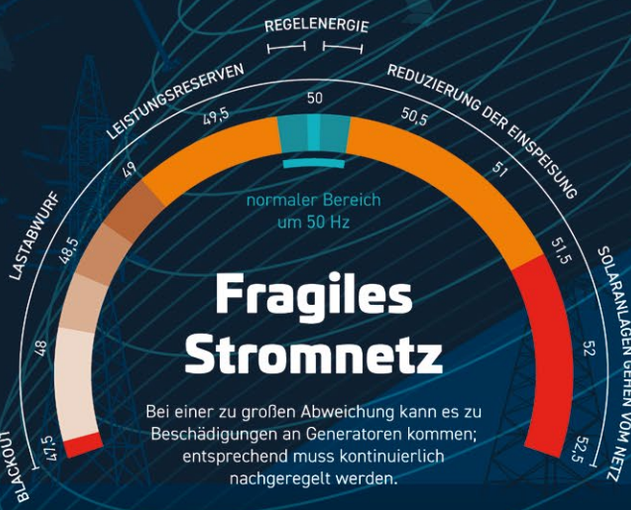
LEO

500 km

00 m ü NN

- 1.000 m

Ein GPS III Satellit neuester Bauart, mit erhöhter Genauigkeit und verbessertem Schutz gegen Jamming.



Fragiles Stromnetz

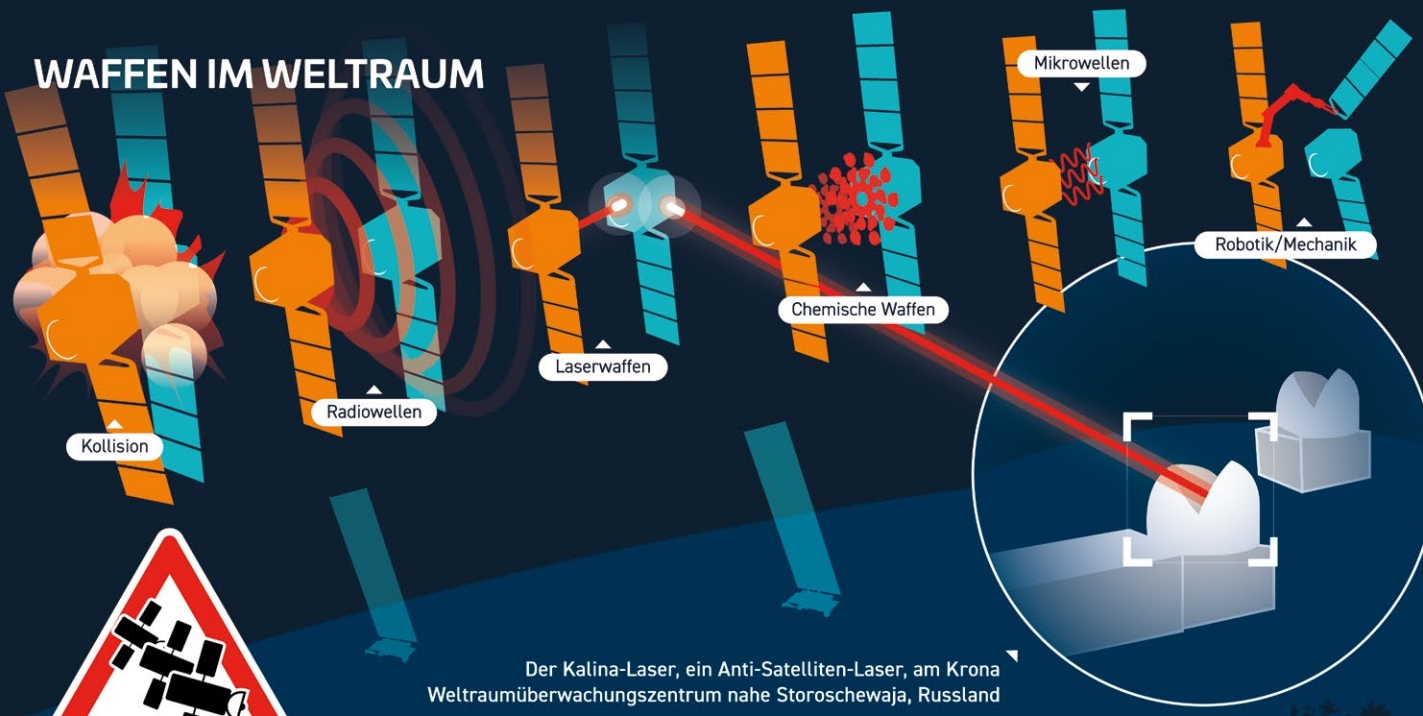
Bei einer zu großen Abweichung kann es zu Beschädigungen an Generatoren kommen; entsprechend muss kontinuierlich nachgeregelt werden.

Torpedos

Ferngesteuerte Unterwasserfahrzeuge

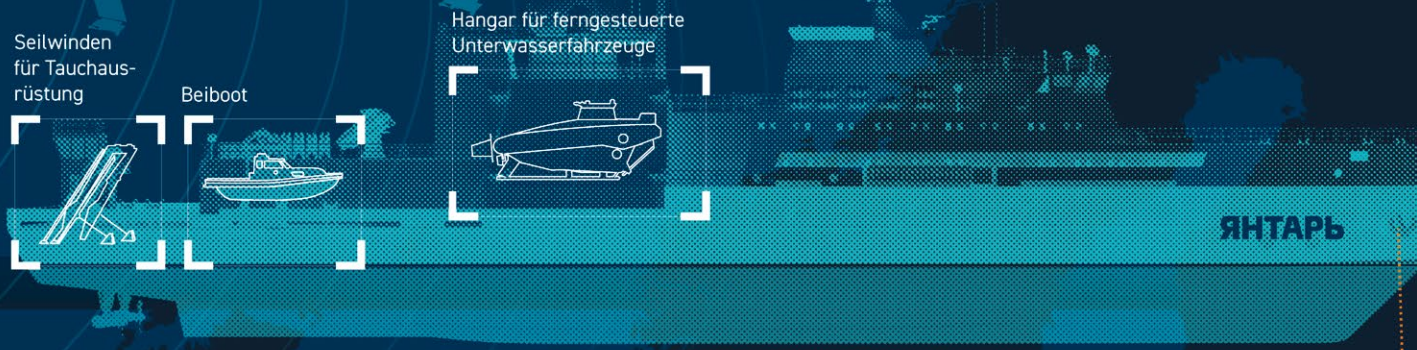
Anker wird absichtlich über den Meeresboden gezogen, um Kabel zu beschädigen.

WAFFEN IM WELTRAUM



Der Kalina-Laser, ein Anti-Satelliten-Laser, am Krona Weltraumüberwachungszentrum nahe Storoschewaja, Russland

Mehr als 13.000 Satelliten kreisten bis November 2024 um die Erde.



Unterseekabel mit Anbindung an Deutschland

Atlantic Crossing 1	14.301 km
IOEMA	1.600 km
C-Lion1	1.172 km
Elektra-GlobalConnect 1	44 km
Fehmarn Bält	20 km
Germany-Denmark 3	n.a.
GlobalConnect-KPN	43 km
Aurora	n.a.

Am 25. Dezember 2024 wurde das Stromkabel EstLink 2 zwischen Finnland und Estland mutmaßlich durch den russischen Tanker Eagle S beschädigt.

Am 26. Januar 2025 wurde ein Datenkabel zwischen Schweden und Lettland durch den Frachter Vezhen beschädigt.

Am 15. Februar 2022 verweilte die Fortuna rund 12 Stunden lang über einer Ölpipeline.

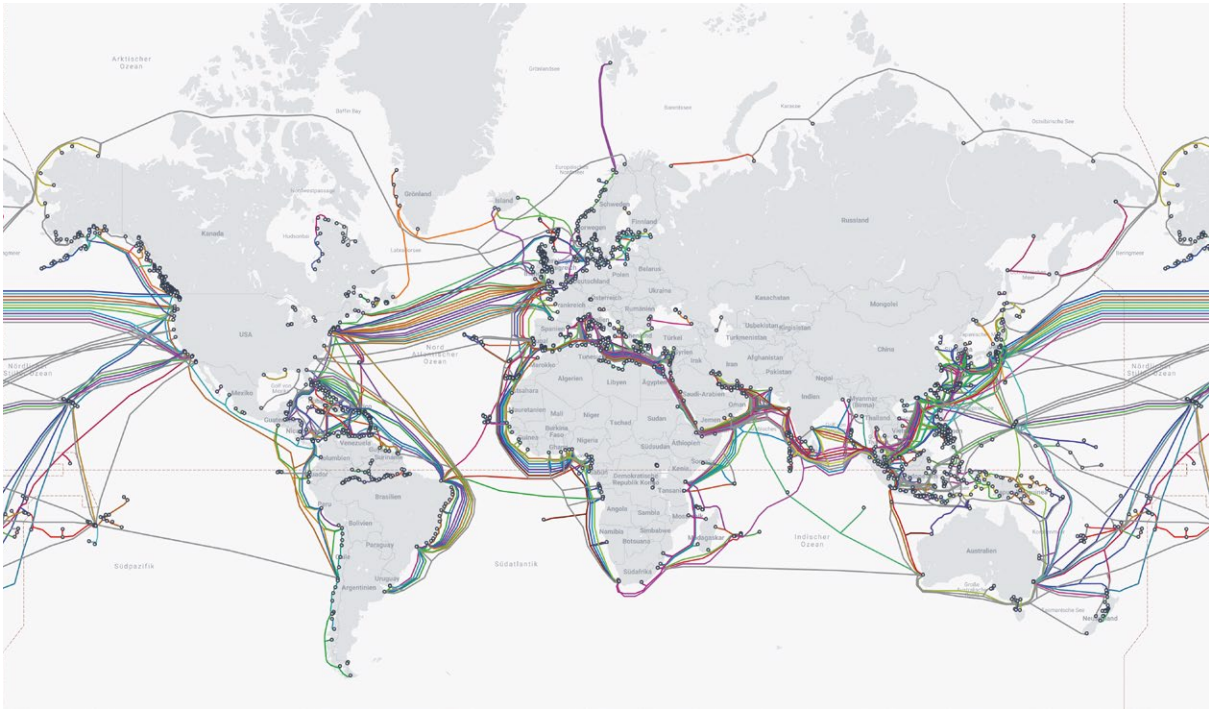
Quellen: [86], [119], [155], [279], [286], [297], [305], [321], eigene Darstellung

3 GRENZENLOS BEDROHT – CYBERGEFAHREN VOM MEERESGRUND BIS INS WELTALL

In den unwirklichen Lebensbedingungen tief auf dem Meeresgrund spannen sich die Nervenadern des Informationszeitalters. In Kürze wird die Zahl der aktiven Glasfaser-Tiefseekabel auf über 600 ansteigen (siehe Abbildung 19), um mit dem zunehmenden Bedarf nach schnellen Übertragungskapazitäten weltweit Schritt zu halten.

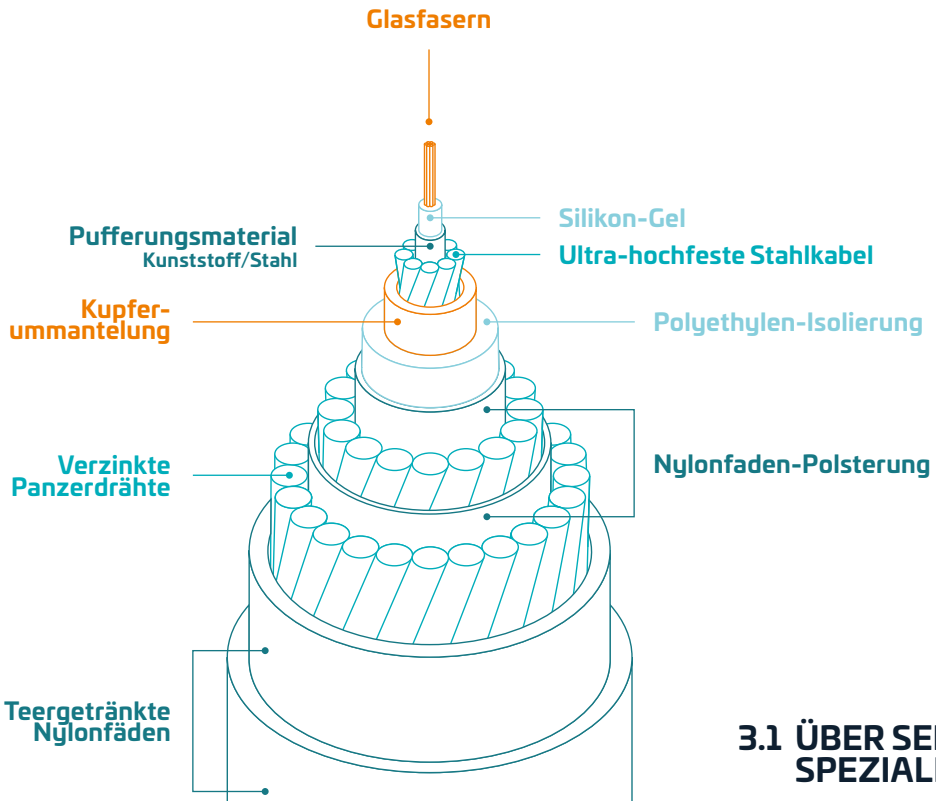
Im Jahr 2024 wurden geschätzt sechs Zettabyte in den kabelbasierten Netzen und weitere 1,3 Zettabyte in den Mobilfunknetzen [150] übertragen. Um diese Dimensionen zu verdeutlichen: sechs Zettabyte würden drei Milliarden der handelsüblichen und heutzutage weit verbreiteten externen Festplatten mit einer Kapazität von jeweils zwei Terabyte füllen. Würde man diese Datenmenge auf Papier drucken, würde der resultierende Stapel circa sechs Billionen Kilometer hoch sein, fast 40-mal die Entfernung zwischen Erde und Sonne. Die unzähligen Transaktionen und Wirtschaftsaktivitäten, die in diesen Datenströmen enthalten sind, hatten bereits 2016 einen geschätzten Wert von täglich über zehn Billionen US-Dollar [104].

Bereits ein kurzer Ausfall dieser Verbindungen hat sofort enorme wirtschaftliche Verluste zur Folge. Durch eine sechsstündige Nichterreichbarkeit von Facebook entgingen Meta beispielsweise 100 Millionen US-Dollar an Werbeeinnahmen. Wissenschaftliche Studien haben weiterhin ergeben, dass ein Anstieg der Wahrscheinlichkeit einer Internetabschaltung um einen Prozentpunkt statistisch signifikant mit einem Rückgang des Pro-Kopf-Bruttoinlandprodukts um durchschnittlich 15,6 Prozentpunkte korreliert und dass jeder zusätzliche Tag einer Internetabschaltung im Durchschnitt 86,58 US-Dollar pro Person kostet [281].



Quelle: [290]

Abbildung 19: Weltweite Seekabel



Quelle: [291]

Abbildung 20: Aufbau eines Seekabels

3.1 ÜBER SEEKABEL UND SPEZIALFAHRZEUGE

Die mehr als 1,5 Millionen Kilometer Glasfaserkabel ermöglichen es beispielsweise auch, dass der Zugriff auf eine Webseite in den USA von Deutschland aus nur 60 Millisekunden dauert. Durch diese Leistungsfähigkeit hat sich das Internet nicht nur zum Rückgrat unserer täglichen Kommunikation entwickelt, sondern ist die Basis für Handel und Finanzwesen, und auch immer mehr Steuerungs- und Überwachungsaufgaben, beispielsweise in kritischen Infrastrukturen (KRITIS), werden darüber betrieben.

Aufgrund der rauen Meeresbedingungen müssen die Seekabel enorm belastbar sein. Die durchschnittliche Tiefe des Atlantiks beträgt zum Beispiel 3.293 Meter. Durch diese Wassersäule wirkt auf jeden Quadratzentimeter eine Kraft von fast 330 Kilogramm. Da in dieser Tiefe Seekabel typischerweise nicht eingegraben, sondern lediglich auf den Grund gelegt werden, müssen sie darüber hinaus auch gegen Einflüsse wie Seebeben und seismische Aktivitäten gewappnet sein. Die empfindlichen Fasern sind daher durch einen mehrschichtigen Aufbau geschützt, der nicht nur Stahldrähte zur Stabilisierung, sondern unter anderem auch eine Kupferummantelung enthält, welche auch der Stromversorgung des Seekabels dient (siehe Abbildung 20).

Warum ein Kabel eine Stromversorgung für sich selbst benötigt, wird schnell offensichtlich. Zwar gibt es für Seekabel spezielle Lichtwellenleitertypen, die einen besonders geringen Signalverlust haben und somit sehr weite Strecken überbrücken können. Die circa 5.500 Kilometer zwischen der Ostküste der Vereinigten Staaten und den Atlantikküsten Europas sind dann aber doch etwas zu

weit. Das längste in Betrieb befindliche Seekabel ist noch immer die seit 1999 aktive Verbindung SEA-ME-WE 3 (South-East Asia – Middle East – Western Europe 3) mit einer Länge von insgesamt 39.000 Kilometern. Um die Signale zuverlässig über solche Distanzen zu bekommen, ist eine entsprechende Verstärkung erforderlich. Beim ersten transatlantischen Glasfaserkabel, dem von 1988 bis 2002 genutzten TAT-8, wurden hierfür noch Photodioden und Halbleiterverstärker genutzt. Im Jahr 1996 kamen hierfür bei der TAT-12/13-Verbindung jedoch erstmals quantenmechanische Prinzipien zum Einsatz: Eine Dotierung der Glasfasern mit der seltenen Erde Erbium ermöglicht es, die transportierten Signale durch die Zuführung von sogenanntem Pumplicht auf rein optischem Wege zu verstärken. Um diese im Schnitt alle 70 Kilometer eingebrachten Verstärker zu versorgen, werden die Seekabel mit einer Betriebsspannung von typischerweise 10.000 Volt versorgt [182].

Auch wenn sich solche Pumpen grundsätzlich ohne digitale Schaltkreise betreiben lassen, werden für eine kontinuierliche Leistungsüberwachung und zur Nachsteuerung der Verstärkung Überwachungen und Mikroprozessoren benötigt, um die Betriebstemperatur in optimalen Bereichen zu halten und Störungen wie beispielsweise Verbindungsfehler zügig aufzuspüren.

Solche Fehler treten trotz des äußerst stabilen Aufbaus der Kabel regelmäßig auf. Allerdings sind die Ursachen meist nicht natürlicher Art: Analysen zeigen, dass über 70 Prozent der Vorfälle im Unterwasserbereich unbeabsichtigt, aber menschlichen Ursprungs sind. Oftmals sind Schleppnetze von Fischerbooten, Anker oder Infrastrukturmaßnahmen, wie Baggerarbeiten an Häfen, Auslöser für die durchschnittlich knapp 150 Kabelunterbrechungen weltweit pro Jahr [67].

Um die Seekabel vor solchen Unfällen bestmöglich zu schützen, sind ihre Positionen und Wege auch keineswegs geheim, sondern insbesondere bei Verlegung auf dem Meeresgrund ohne Eingrabung öffentlich verfügbar und beispielsweise in Seekarten verzeichnet. Trotzdem verursacht die Fischerei mit ihren Netzen 38 Prozent aller Schäden [291], Schiffsanker sind für jedes vierte beschädigte Kabel verantwortlich. Weitere elf Prozent aller Zwischenfälle werden auf andere Weise von Menschen verursacht [302]. Genau diese Transparenz erhöht aber auch die Anfälligkeit für potentielle Angreifer, zumal die Zufälligkeit mancher Vorfälle und Beschädigungen ziemlich unglaubwürdig erscheint – umso mehr, wenn sich solche Ereignisse häufen.

Gerade dies war Ende letzten Jahres der Fall. Bereits im Oktober 2023 hatte das chinesische und unter der Flagge von Hongkong fahrende Containerschiff „Newnew Polar Bear“ die Datenlinks zwischen Schweden und Estland (EE-S 1) und eine der Finnland-Estland-Verbindungen sowie die Balticconnector-Gaspipeline in der Ostsee beschädigt, aber in jüngerer Zeit folgte noch viel mehr. So wurde am 17. November 2024 zunächst die Datenverbindung BCS East-West Interlink zwischen Litauen und Schweden unterbrochen und nur wenige Stunden später, am frühen Morgen des 18. Novembers, der Datenlink C-Lion1 zwischen Finnland und Deutschland. Als Verursacher wurde der chinesische Frachter „Yi Peng 3“ im Auftrag Russlands vermutet. Da die Beschädigungen jedoch in internationalen Gewässern erfolgten und somit der Flaggenstaat China für die Ermittlungen zuständig und die Ostseeanrainer reine Beobachter waren, verliefen diese im Meeressande.

Die Beschädigung eines weiteren Datenkabels zwischen Finnland und Schweden am 3. Dezember 2024 wurde im Verlauf der Ermittlungen als Unfall im Rahmen von Baumaßnahmen identifiziert, aber bereits am ersten Weihnachtsfeiertag 2024 kam es zu einer Unterbrechung des 650-Megawatt-Stromkabels Estlink 2. Schnell wurde der Verdacht erhärtet, dass es sich in diesem Fall erneut um einen bewussten Sabotageakt handelte. Die finnischen Behörden reagierten schnell und hielten den unter Verdacht stehenden Tanker „Eagle S“, welcher der russischen Schattenflotte zugeordnet wird, fest und leiteten eine Untersuchung des Vorfalls ein. Nicht nur in der Ostsee ist es unruhig: So wurde am 3. Januar 2025 ein wichtiges Datenkabel des Trans-Pacific Express-Kabelsystems, das Taiwan mit der Westküste der Vereinigten Staaten verbindet, durch das chinesische Frachtschiff „Shunxing 39“ beschädigt. Auch wenn der Nachweis einer Sabotageabsicht in solchen Fällen nicht ganz einfach ist, unterstrich der schwedische Minister für Zivilschutz

mit Blick auf die Yi Peng 3-Ermittlungen, dass man es durchaus merken sollte, wenn man seinen Anker 150 Kilometer weit hinter sich herzieht [194].

Stromkabel sind zudem üblicherweise im Seeboden vergraben, um sie zum einen vor ebensolchen Unfällen besser zu schützen, und zum anderen auch aufgrund von Umweltauflagen. Zur Verringerung möglicher Konsequenzen für Meeresflora und -fauna wird zum Beispiel für die Küstenmeere der Nordsee gefordert, dass die Temperaturerhöhung in 20 cm Tiefe unterhalb der Oberfläche maximal 2° Kelvin betragen darf. Dafür müssen die Kabel mittels Einspülung oder der Nutzung von Seefräsen mindestens ein bis 1,5 Meter tief verlegt werden [40]. Das Seekabel 2Africa soll sogar bis zu drei Meter tief versenkt werden.

Allerdings gehen die Gefahren nicht nur von versehentlich oder bewusst nachgeschleppten Ankern aus. Russland hat verschiedene Spezialschiffe und Unterseeboote, welche explizit für solche Aufklärungs- und Sabotageaktionen ausgelegt sind. Einige davon wurden in den letzten Jahren immer wieder dabei beobachtet, wie sie sich oft über Stunden oder gar Tage in Bereichen von Windparks oder Seekabeln aufhielten, wie beispielsweise die „Yantar". Querstrahlruder und spezielle Antriebspods ermöglichen dem Schiff, stationär über einem Punkt zu verbleiben. In seinen Hangars führt es mehrer Mini-Unterseeboote sowie verschiedene ferngesteuerte Unterwasserfahrzeuge (Remoted Operated Vehicle, ROV) mit. Diese sind unter anderem mit Greifarmen für Arbeiten am Meeresgrund ausgestattet und können vermutlich Glasfaserkabel nicht nur zerschneiden, sondern auch Geräte zum Abhören (sog. Taps) einbringen [280].

Die Tauchausstattung kann allerdings nicht nur über Wasser, sondern auch weit unauffälliger und schwieriger zu entdecken mit Spezial-Unterseebooten verbracht werden. Erwähnenswert ist beispielsweise das Projekt 1910 Kashalot, von dem zwei U-Boote gebaut und 1986 beziehungsweise 1991 in Dienst gestellt wurden und mittlerweile zur sogenannten Hauptverwaltung Tiefseeforschung (GUGI) des russischen Verteidigungsministeriums gehören. Mittels spezieller Triebwerke können auch die Kashalot-U-Boote dicht über dem Meeresboden schweben und erreichen durch ihre Titanhülle eine außergewöhnlich hohe maximale Tauchtiefe von geschätzten 1.000 Metern. Zum Vergleich: Für die U-Boote der U.S. Navy werden je nach Klasse maximale Tauchtiefen von 240 bis 490 Meter vermutet.

Insgesamt betreibt GUGI mehr als 50 Schiffe und U-Boote, die zu Aufklärungs- und Sabotagezwecken am Meeresboden eingesetzt werden können.

Vor dem Hintergrund der gehäuften Vorfälle im Ostseeraum hat die NATO im Januar 2025 die Operation „Baltic Sentry" gestartet, welche durch den Einsatz von Fregatten, Überwachungsflugzeugen und Seedrohnen vor weiteren Aktionen gegen die kritischen Infrastrukturen in der Ostsee abschrecken soll [210]. Weiterhin wurde das Projekt HEIST (Hybrid space-submarine architecture Ensuring InfoSec of Telecommunications) initiiert. Dessen Ziel ist es, Schäden an Seekabeln innerhalb kürzester Zeit bis auf einen Meter genau zu lokalisieren und den Datenverkehr im Falle eines Vorfalls unmittelbar umzuleiten [101].

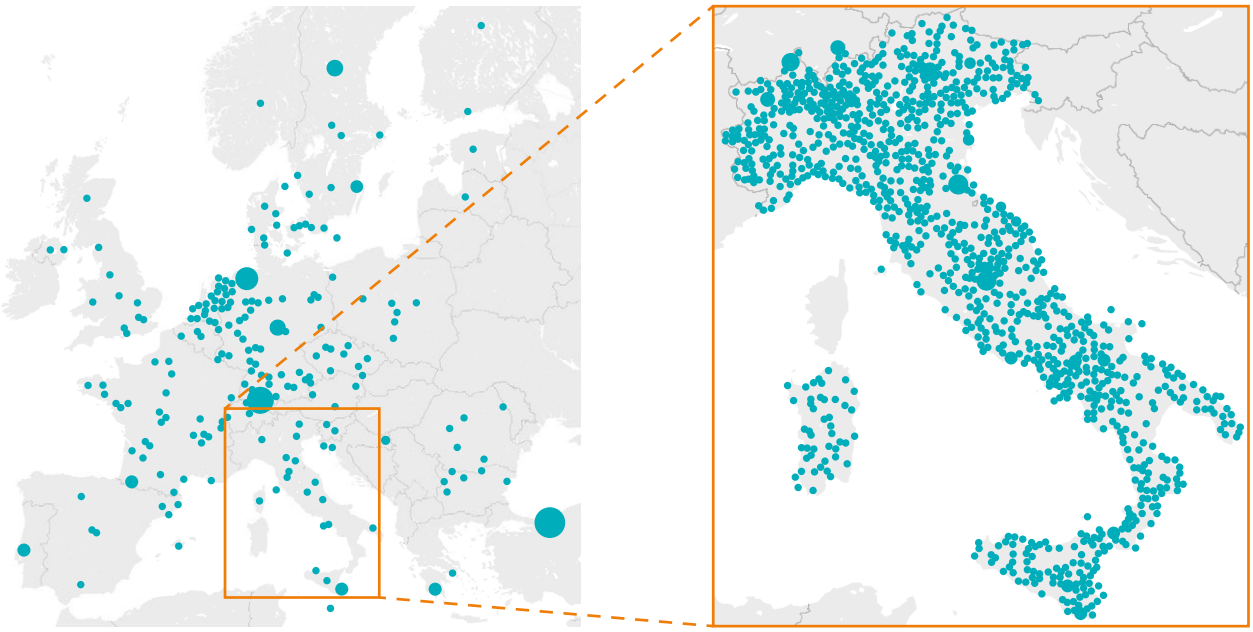
Künftig werden solche Abhängigkeiten noch weiter zunehmen, beispielsweise durch Projekte wie die geplante „Greece-Egypt Electrical Interconnection" (GREGY Interconnector), die ab 2031 den zu 75 Prozent in ägyptischen Windparks mit einer Leistung von 9,5 Gigawatt erzeugten Strom nach Griechenland und Europa transportieren soll [75]. Verschiedene weitere Offshore-Windparks und Verbindungen sind in Planung. Sabotagekapazitäten wie die Kashalot-Boote erhöhen somit das Risiko hybrider Aktivitäten, die als Unfälle getarnt werden können und oftmals schwer attribuierbar sind [39]. Die bisherigen Beschädigungen konnten aufgrund der Redundanzen der weltweiten Datenverbindungen aufgefangen werden, ebenso hatten auch die Vorfälle bei Stromkabeln durch die übergreifende Vernetzung des Europäischen Verbundsystems (EV) keine größeren Auswirkungen. Mittels 39 Übertragungsnetzbetreibern versorgt das EV fast 600 Millionen Menschen mit Strom, die eine hohe Versorgungsstabilität gewohnt sind.

3.2 MODERNE BLUTADERN: DAS EUROPÄISCHE VERBUNDSYSTEM

Das Szenario eines großflächigen und mehrtägigen Stromausfalls ist schon lange keine Fiktion mehr. Zu kleineren und kürzeren Strom- oder Internetausfällen kommt es immer wieder. Die häufigsten Ursachen sind auch hier Umwelteinflüsse, Kaskadeneffekte aufgrund technischer Fehler oder menschliches Versagen (siehe Abbildung 21). Weitflächige Ausfälle wie am 21. Juni 2024, bei dem es zu einem umfassenden Blackout in Südosteuropa kam und Albanien, Bosnien und Herzegowina, Montenegro und Kroatien betroffen waren, sind bisher jedoch noch die Ausnahme.

Reparaturen an beschädigten Seekabeln können Monate dauern. Das EV wird mit N+1 Redundanz betrieben, was bedeutet, dass es auch funktionsfähig bleibt, wenn eine Komponente ausfällt – dies gilt auch für Stromleitungen.

Fallen Leitungen jedoch längerfristig aus, haben die Netzbetreiber weniger Optionen, um die N+1 Redundanz sicherzustellen. Somit kann das Risiko steigen, dass beispielsweise bewusst lokal herbeigeführte (weitere) Störungen weitflächige Effekte nach sich ziehen. Sind die in den letzten Monaten häufiger zu beobachtenden Vorfälle bei Internet- und Stromverbindungen somit als systematisches Austesten sowohl der Effekte und Resilienzen in den jeweiligen Netzen als auch der Reaktionen der westlichen Nationen sowie ihrer Prozesse und Geschwindigkeiten zu bewerten? Es gilt, auf jeden Fall vorbereitet zu sein.



Quelle: [269]

Abbildung 21: Analyse von Blackouts, weitflächig in Europa und lokal in Italien

Hierbei darf nicht vergessen werden, dass die Stromversorgung, welche Grundlage für nahezu alle Bereiche unserer modernen Gesellschaft ist, selbst ein äußerst komplexes System darstellt, das kontinuierlich überwacht und nachgeregelt werden muss.

Aufgrund des Klimawandels und des entsprechend neuen und sich weiter adaptierenden Erzeugungsmixes werden die Verbundsysteme zunehmend unter kritischen Bedingungen betrieben [269]. Nicht in allen Ländern ist die Infrastruktur auf den weiteren Übergang zu erneuerbaren Energien bereits hinreichend vorbereitet [139]. Hierdurch entstehen auch neue Cybergefahren, die zunächst nicht ganz offensichtlich sind.

Damit die Stromversorgung stabil funktioniert, müssen sich Stromerzeugung und -verbrauch permanent die Waage halten. Ein Indikator, ob zu viel oder zu wenig Strom erzeugt beziehungsweise verbraucht wird, ist die Netzfrequenz. Die europäische Stromversorgung basiert auf Wechselstrom mit 50 Hertz. Wird mehr Strom erzeugt als verbraucht, steigt die Frequenz; wird zu wenig erzeugt, sinkt sie. Bei einer zu großen Abweichung kann es beispielsweise zur Beschädigung von Generatoren kommen, entsprechend muss kontinuierlich nachgeregelt werden.

Sinkt die Frequenz, aktivieren die Energieversorger zunächst Reserven, um den Mehrbedarf zu decken. Reicht dies nicht aus, kommt es zum Lastabwurf – einzelne Bereiche werden kontrolliert von der Stromversorgung getrennt. Reicht auch dies nicht aus, erfolgt bei Frequenzen unter 47,5 Hertz die Trennung der Kraftwerke vom Netz, damit diese nicht beschädigt werden: ein Blackout. Im Falle einer steigenden Frequenz muss dahingegen die Stromproduktion reduziert werden, allerdings geht dies bei Großkraftwerken nicht abrupt, sondern kann einige Minuten dauern.

Einfacher handzuhaben sind beispielsweise Photovoltaikanlagen (PV-Anlagen), weshalb bis 2012 gebaute Anlagen die Einspeisung ab einer Frequenz von 50,2 Hertz abrupt einstellen. Da der Ausbau der Photovoltaik mittlerweile jedoch sehr umfassend ist – für 2025 wird mit einer Gesamtkapazität von 328 Gigawatt in Europa gerechnet – könnte es durch einen plötzlichen Wegfall dieser Systeme wiederum zu einer Unterversorgung kommen und damit die Gefahr eines Blackouts entstehen. Neuere Anlagen drosseln daher zunächst die Einspeisung und schalten erst bei 51,5 Hertz ab.

Da ständig Schwankungen im Stromnetz auftreten, müssen diese auch kontinuierlich ausgeglichen werden, beispielsweise durch die Schwungmasse der Generatoren in Kraftwerken, die sogenannte Momentanreserve. Erneuerbare Energiequellen liefern jedoch keine Momentanreserve, sodass die Stabilität zunehmend durch intelligente Steuerungen, Leistungselektronik und Batteriespeicher gewährleistet werden muss: ein komplexes System, in dem ein hohes Maß an Cybersecurity zwingend erforderlich ist. Im Gegensatz zu Netz- und Kraftwerksbetreibern unterliegen private PV-Anlagen aber kaum Regularien.

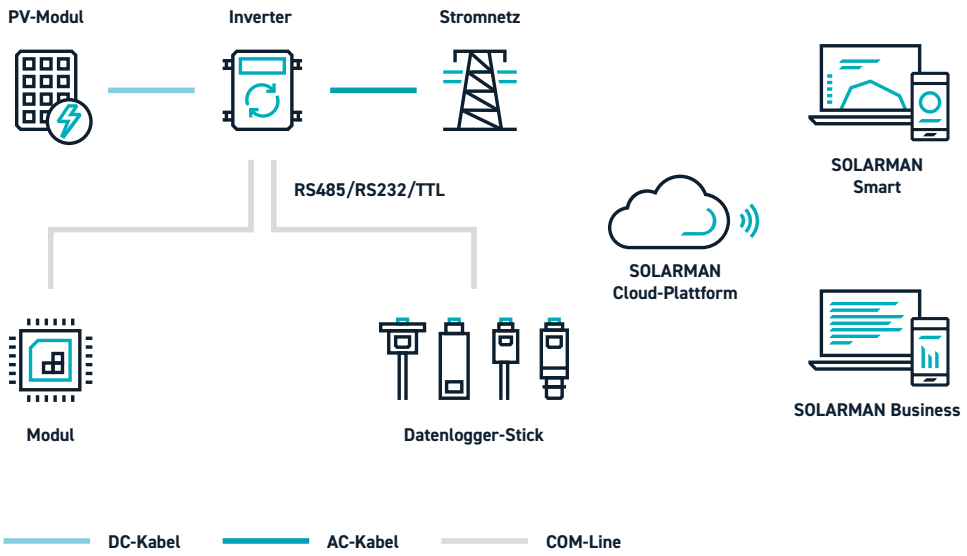
Dies wirkt sich unmittelbar auf die Cybersecurity aus. Wie in vielen anderen Bereichen auch hat der intensive Wettbewerb über die Jahre zu einer Verlagerung der Produktionsstätten und Lieferketten geführt. Beispielsweise ist es Peking mit seiner 2015 gestarteten „Made in China 2025"-Initiative (MIC2025) und massiven Subventionen von mehreren Milliarden US-Dollar gelungen, umfassende Kapazitäten aufzubauen und eine dominante Position einzunehmen. 85 Prozent der PV-Module werden mittlerweile in China hergestellt.

3.3 GRENZENLOSE ABHÄNGIGKEITEN

Oftmals sind hier Geschwindigkeit der Vermarktung und Preis die ausschlaggebenden Faktoren, während die Cybersecurity leidet. Dies wurde im Bereich der Inverter, die den von PV-Modulen erzeugten Gleichstrom in den Wechselstrom der lokalen Versorgungsnetze wandeln, als Problem erkannt (siehe Abbildung 22). So wurden beispielsweise erhebliche Schwachstellen in den PV-Überwachungsplattformen von Solarman und Deye festgestellt, die einem Angreifer eine Manipulation der Invertereinstellungen ermöglichen konnten [173]. Mittels eines geeigneten, koordinierten Angriffs auf eine Vielzahl betroffener Anlagen hätte so ein Blackout ausgelöst werden können.

Während hier die Schwachstellen rechtzeitig gemeldet und Patchs bereitgestellt wurden, kam es in Japan zu einem Vorfall, bei dem Angreifer 800 PV-Anlagen mittels der Ausnutzung einer bekannten Schwachstelle übernahmen. Die gekaperten Systeme wurden zur Verbreitung des Mirai-Botnetzes genutzt, nicht für einen Angriff auf das Stromnetz – aber dies hätte auch das Ziel sein können [37].

Die Gefahr geht aber nicht nur von den Schwachstellen der Inverter aus. Daher gibt es auch kein entspanntes Zurücklehnen, falls die eigenen PV-Anlagen aufgrund ihrer Konfiguration oder Firewalls nicht aus dem Internet erreichbar sein sollten: Viele der heute verbauten Anlagen werden auf der Basis von Cloud-Diensten überwacht und gesteuert – und die laufen häufig in chinesischen Rechenzentren. Die hierdurch faktisch extern kontrollierte Gesamtkapazität beläuft sich auf viele Gigawatt, sehr viel höher als die im EV verfügbare Notstromkapazität. Wer diese Cloud kontrolliert, kann einen Blackout auch ganz ohne U-Boote und Kabelschneider herbeiführen.



Quelle: [173]

Abbildung 22: Photovoltaiksysteme können bei Vorhandensein von Schwachstellen ein Risiko für die Stabilität der Versorgungsnetze darstellen

Dies ist kein Einzelfall. Durch die jahrzehntelange Kosten- und Effizienzoptimierung und Verlagerung von Produktionsstätten und Versorgungsketten sind nahezu alle Bereiche der IT betroffen. Dabei sind nicht nur das oftmals fahrlässige Sicherheitsniveau oder die in China betriebenen Clouds das Problem. Vielmehr ist es einem cleveren und strategisch denkenden Akteur möglich, erheblichen Einfluss auf den Cyberraum auszuüben und in den Systemen potentiell künftiger Konfliktparteien frühzeitig und zuverlässig Hintertüren einzubauen.

Auch wenn es im Bereich von Hardwaremanipulationen nur wenige öffentlich bekannte Beispiele gibt, die zudem gemein haben, dass sie von allen Beteiligten vehement abgestritten wurden, so liegen Potenzial und Gefährdung auf der Hand: Die Diskussion im Falle des Microsemi ProASIC3-Chips, ob es sich bei einer undokumentierten Funktionalität zum Zugriff auf den gesamten Chip um Debugging-Funktionalitäten oder eine Hintertür handelte, verdeutlicht die Herausforderungen in diesem Bereich. Zum einen ist der Nachweis einer Manipulation extrem schwierig, zum anderen lassen sich zumindest geschickte Hintertüren glaubhaft abstreiten. Die Möglichkeiten im Rahmen der globalen und komplex verzweigten Versorgungsketten, wie sie durch die Explosionen manipulierter Pager und Walkie-Talkies der Hisbollah offensichtlich wurden, verschärfen die Situation zusätzlich.

Die Anstrengungen vieler Länder, die eigenen Produktionskapazitäten zu erhöhen, Lieferketten sicherer zu machen und Abhängigkeiten zu reduzieren, sind daher leicht nachvollziehbar. Zur Umkehrung des Trends der stark geschrumpften eigenen Produktionskapazitäten und vor dem Hintergrund der zunehmenden Auswirkungen auf die Sicherheit hat beispielsweise das Weiße Haus im Jahr 2022 den „Creating Helpful Incentives to Produce Semiconductors for America Act“ (CHIPS for America Act) verabschiedet. Das Gesetzespaket stellt 52 Milliarden US-Dollar Fördermittel für die heimische Halbleiterproduktion bereit – von Forschung und Entwicklung bis zur Sicherheit der zugehörigen Lieferketten. Das Programm hat mittlerweile zu Investionen in mehrere dutzend Firmen von knapp 400 Milliarden US-Dollar geführt. So entstehen derzeit unter anderem 73 neue Halbleiterwerke beziehungsweise werden bestehende erweitert. Auf diese Weise wollen die Vereinigten Staaten bis 2032 wieder eine Produktion von 30 Prozent der Weltmarktkapazität erreichen, nachdem diese mittlerweile auf unter zehn Prozent zurückgegangen ist.

Europa fällt es schwerer, seine Rolle in der Halbleiterfertigung zu verbessern. Dies liegt nicht allein an den zweistelligen Milliardenbeträgen, die ein modernes Werk kostet, oder den notwendigen Fachkräften für den Betrieb. Die Herausforderung liegt eher im weiteren Ökosystem, in dem weniger Grundlagen vorhanden sind als beispielsweise in den Vereinigten Staaten. Auch deshalb mag der EU Chips Act, der mit 43 Milliarden Euro ausgestattet zumindest annähernd an den CHIPS for America Act heranreicht, derzeit noch nicht das gleiche Momentum erzeugen, und es bleibt abzuwarten, ob das Ziel der EU eines globalen Marktanteils von 20 Prozent bis 2030 zu erreichen ist.

Dies ist aber nicht die einzige Baustelle, wo aufgeholt werden muss. Im Gegenteil, der größte Schaden und die meisten Herausforderungen entstehen zunächst weiterhin durch Cyberkriminalität und die sich schnell weiterentwickelnden, professionellen Angreifergruppen (Advanced Persistent Threats, APTs).

3.4 SOPHISTIZIERUNG DER ANGREIFER

Die heutige – und kontinuierlich zunehmende – Komplexität der weltweiten IT-Systeme und Netze birgt viele Risiken. Die dem chinesischen Staat zugerechnete Angreifergruppe Salt Typhoon (Advanced Persistent Threat, APT-40) hat Ende 2024 beispielsweise für umfassende Schlagzeilen gesorgt, da sie in der Lage war, tief in die Netze mehrerer US-Telekommunikationsanbieter einzudringen und unter anderem Gespräche von Donald Trump und weiteren politischen Persönlichkeiten abzuhören. Entgegen der ursprünglichen Annahme, dass die Angriffe Systemen galten, welche für Abhörmöglichkeiten (sogenannte „Lawful Interception“) durch US-Behörden nach entsprechenden richterlichen Anordnungen speziell hierfür installiert waren, zeigte sich die Opera-

tion sehr viel breiter angelegt und lief bereits über viele Monate oder gar Jahre.

Das Beunruhigende daran ist, dass es trotz Erkennung der Angreifer nicht möglich war, diese komplett aus den Netzen zu entfernen, und – was noch schwerwiegender ist – der genaue Status der andauernden Sicherheitsverletzungen nicht identifiziert werden konnte. Dies führte sogar dazu, dass die sonst eher skeptisch auf Verschlüsselung schauenden US-Behörden Empfehlungen herausgaben, Kommunikation per Ende-zu-Ende Verschlüsselung abzusichern [81]. Die Dimension scheint jedenfalls immens. Die entwendeten Metadaten können China beispielsweise helfen, Schlüsselpersonen aus Politik und Industrie zu identifizieren.

Jedoch selbst wenn aufgezeichnete Gespräche und VTCs keine vertraulichen oder brisanten Inhalte gehabt haben sollten, ist die Sorge über darauf basierende, durch generative künstliche Intelligenz (Generative AI, GAI) erzeugte Deep Fakes nun groß. Durch die rasante Weiterentwicklung der Technologie wird die Unterscheidung selbst mit maschineller Unterstützung und bei guten Trainingsdaten immer schwieriger.

Auch wenn die berichteten Vorfälle bisher „nur" die Vereinigten Staaten betroffen haben, zeigen die Formulierungen der mächtigen Five-Eyes-Allianz (FVEY) der Geheimdienste von Australien, Kanada, Neuseeland, dem Vereinigten Königreich und den Vereinigten Staaten die Brisanz des Vorfalls. Zwar hat das Vereinigte Königreich die gemeinsame Warnung der anderen vier Mitglieder nicht unterschrieben, die nebulösen Formulierungen der australischen Dienste lassen jedoch erkennen, dass vermutlich nicht nur Systeme in den USA betroffen waren.

Dies wäre auch wenig überraschend, denn es gibt nur eine begrenzte Anzahl an Herstellern von entsprechendem Equipment, und die international agierenden Telekommunikationsdienstleister werden in verschiedenen Ländern recht ähnliche Strukturen in ihren Netzen und Systemen betreiben. Sollten Länder von einer so massiven Spionageoperation daher tatsächlich nicht betroffen sein, obwohl sie erwartungsgemäß zum Aufklärungsfokus Chinas gehören, dann dürfte dies eher Kapazitätsgründe aufseiten der Angreifer haben – die angesichts der geeigneten Nutzung von KI, insbesondere aber auch der erheblichen Ressourcen Chinas in diesem Bereich heutzutage eher zweitrangig sein dürften.

Neben den umfassenden staatlichen und staatsnahen Elementen existiert dort eine blühende Industrie, die Hacking und die Durchführung ganzer Cyberoperationen als Dienstleistung anbietet: Die i-Soon-Leaks haben hierzu wichtige Erkenntnisse geliefert. Anfang 2024 wurden umfassende Dokumente des chinesischen Cybersecurity-Unternehmens von einer anonymen Quelle veröffentlicht. Die enthaltenen Präsentationen und Listen zu buchbaren Cyberoperationen zeigen, wie das Unternehmen mit den chinesischen Nachrichtendiensten und Institutionen auf industriellem Niveau zusammengearbeitet hat [55].

Bedenkt man beispielsweise die bereits umfassenden Aktivitäten der im Ukrainekrieg auf beiden Seiten agierenden Cybergruppen, ist es nicht unwahrscheinlich, dass einige Staaten bei der Durchführung illegaler oder im Graubereich anzusiedelnder Operationen zunehmend auf solche Elemente zurückgreifen, die es ihnen ermöglichen, die Verantwortlichkeit beziehungsweise Urheberschaft abzustreiten. Schon jetzt lassen sich die Herausforderungen, die mit der zunehmenden Professionalisierung und Privatisierung von Cyberoperationen für die Cyberabwehr einhergehen, an konkreten Beispielen verdeutlichen, wie ein Blick auf Operational Relay Box (ORBs) und Schutzsysteme wie Firewalls zeigt.

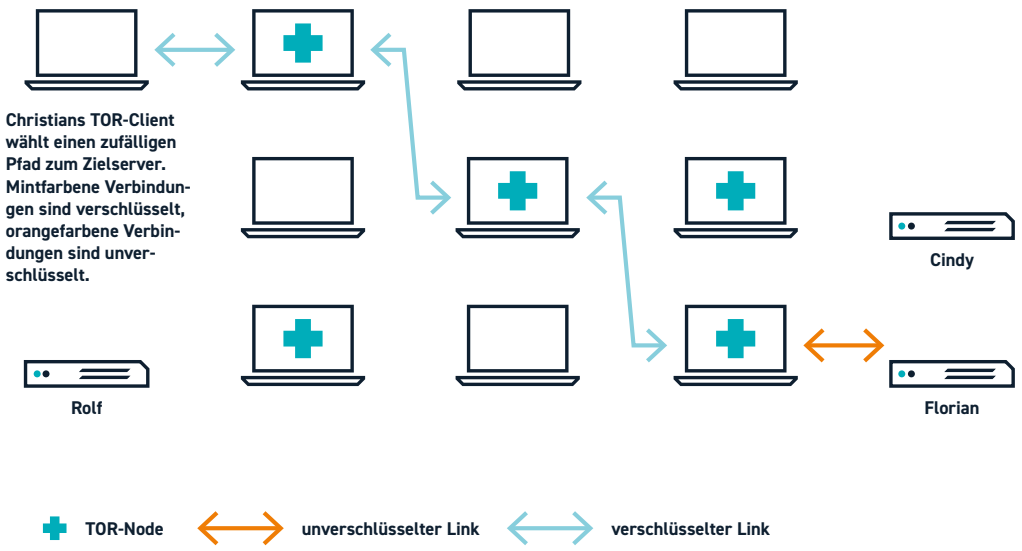
3.5 ÜBER KATZ- UND MAUSSPIELE

Mit ORBs haben die Möglichkeiten der Angreifer, Spuren zu verwischen, erheblich zugenommen. Bisher kamen vor allem Proxyserver, die lediglich Datenverkehr unter Nutzung ihrer eigenen IP-Adresse weiterleiten (Pseudonymisierung), sowie Virtual Private Networks (VPNs) zum Einsatz. In beiden Fällen sieht ein Beobachter nicht die Adresse des eigentlichen Urhebers einer Verbindung, sondern nur eine des zwischengeschalteten Dienstes. Da allerdings alle erforderlichen Informationen auf den Proxy-Servern beziehungsweise VPN-Knoten vorliegen, genügt zur Identifizierung eines Nutzers ein entsprechender Zugriff auf den jeweiligen Server.

Eine echte Anonymisierung ist durch „The Onion Router" (TOR) möglich. Unter Nutzung einer zusätzlichen, aber sehr einfach anzuwendenden Software kann Datenverkehr mehrschichtig verschlüsselt und über mehrere Instanzen weitergeleitet werden. Jeder Knoten der Verbindung kennt jeweils nur das vorherige und nächste System in der Kette. Die eigentliche Nachricht ist vergleichbar mit Briefwahlunterlagen, die in mehreren (verschlüsselten) Umschlägen verpackt sind. Jeder Knoten kann immer nur einen davon öffnen und leitet den Rest weiter. Daher hat niemand in der Kette außer der Absender selbst die Information über sowohl den Urheber als auch das finale Ziel der Kommunikation (siehe Abbildung 23).

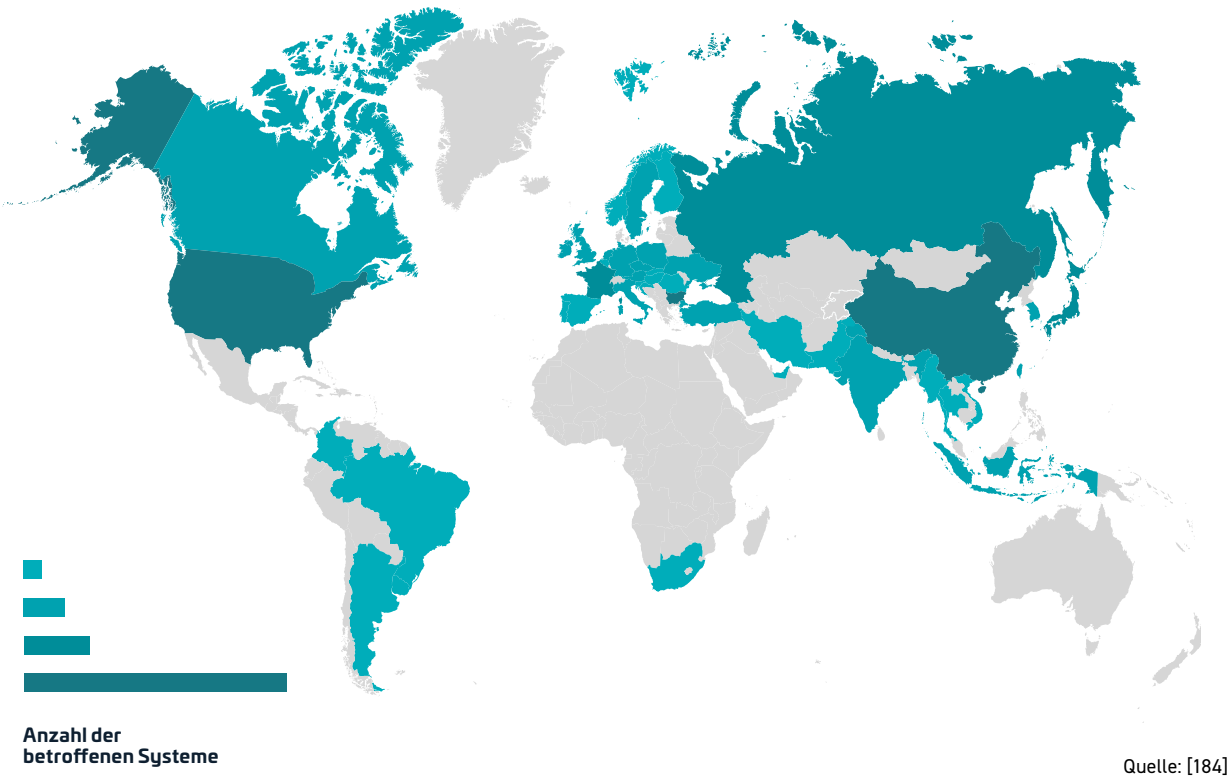
Allerdings gibt es sowohl gegen die Pseudo- als auch die Anonymisierung von Absenderadressen Verteidigungsmöglichkeiten. Im Internet finden sich zahlreiche Seiten, welche die weltweit verfügbaren Proxyserver nahezu auf Minutenbasis aktualisiert auflisten, sodass die entsprechenden Adressen geblockt werden können.

Auch das TOR-Netz kann außen vor gehalten werden: Die Anzahl sogenannter „Exit-Nodes", also der Rechner, die ihre IP-Adresse bereitstellen, um Datenverkehr in ihrem



Quelle: [292]

Abbildung 23: Funktionsweise von TOR



Quelle: [184]

Abbildung 24: Übersicht über die Verteilung von IP-Adressen eines ORB-Netzes

Namen ins Internet weiterzuleiten, ist sehr begrenzt und hat sich über viele Jahre kaum vergrößert – was aus rechtlichen Gründen und abhängig von den Haftungsregularien der jeweiligen Länder nicht überrascht. Nachdem es über lange Zeit circa 1.000 entsprechende Rechner gab, hat sich der Wert mittlerweile auf rund 2.300 Knoten eingependelt – eine im digitalen Zeitalter kurze, einfach zu verarbeitende Liste und gemessen an den derzeit knapp 30 Milliarden vernetzten Geräten nahezu vernachlässigbar.

Da die Information über die Adressen der im TOR-Netz teilnehmenden Rechner aus funktionalen Gründen zudem frei verfügbar ist, gibt es auch hier jederzeit aktuelle Listen, welche somit auch ein Blocken der TOR-Knoten einfach ermöglichen. Im Bereich der Proxy-Server sind die möglichen Adressbereiche deutlich dynamischer und das Feld potenzieller IP-Adressen ist sehr viel größer, grundsätzlich ist die Erstellung und Verwaltung von Deny-Listen, um entsprechende Kommunikationspartner zu blockieren, aber nicht viel komplexer.

Was ein professioneller Angreifer zum Verwischen seiner Spuren also tatsächlich benötigt, ist eine unauffällige IP-Adresse, die weder auf ihn zurückzuführen ist noch geblockt ist oder einfach automatisiert geblockt werden kann. Genau hier kommen die zuvor erwähnten ORBs ins Spiel.

Ein ORB ist Teil eines Netzes zum Weiterleiten von Datenverkehr im Internet. Im Gegensatz zu Proxy-Servern oder Teilnehmern in TOR erfolgt dies jedoch ohne Wissen der Besitzer der jeweiligen Geräte. Hierfür bringen Angreifer schlecht abgesicherte IoT-Systeme, Home-Router und WLAN-Geräte von Privathaushalten oder Unternehmen unter ihre Kontrolle und fügen sie den ORB-Netzen hinzu. Auch wenn sich die Sicherheitssituation bei Home-Routern und ähnlichen Systemen in den letzten Jahren verbessert hat, sind Schwachstellen und schlechtes Patch-Management noch immer verbreitet und auch von Haus aus eingebaute Hintertüren lassen so manchen Hersteller in einem schlechten Licht erscheinen. Wer echter Profi ist, belässt es aber auch nicht bei der Erlangung des Zugangs – er schließt die Schwachstelle nach Möglichkeit hinter sich, um potenzielle weitere Angriffe durch andere Parteien zu verhindern.

Nun sind solche ORBs nichts Neues – schon aus den Snowden-Dokumenten 2013 war ersichtlich, dass die FVEY-Gemeinschaft auf jährlicher Basis anfällige Rechner identifiziert, übernommen und zu einem entsprechenden Netz zusammengestellt hat. In diesem Kontext tauchte der Begriff ORB erstmals auf. Was sich in jüngerer Zeit jedoch geändert hat, sind Dimension, Geschwindigkeit und Einstiegshürden. Was früher wenigen mächtigen Nachrichtendiensten vorbehalten war, lässt sich heute für wenig Geld in der „Cybercrime as a Service"-Ökonomie (CaaS) erwerben. Die Aktualisierung der Mitglieder eines ORB-Netzes ist nun bei weitem nicht mehr auf einen jährlichen Rhythmus fixiert, sondern nachfrageabhängig. Von China ausgehende Cyberoperationen greifen zunehmend auf solche kommerziellen ORB-Netze zurück (siehe Abbildung 24). Da deren Knoten teilweise weniger als 31 Tage aktiv sind, wird die Verteidigung

gegen darüber geleitete Angriffe entsprechend schwieriger, denn die ORBs finden sich in keinen Listen.

Für die Detektion bedeutet dies, dass IP-Adressen als Erkennungsmerkmal eines Angreifers oder Quelle bösartiger Aktionen eine immer geringere Rolle spielen und als Indicator of Compromise (IOC) noch mehr an Wert verlieren.

Verschärft wird dies noch, wenn ORB-Betreiber nicht einmal mehr verwundbare Geräte suchen und übernehmen müssen, sondern dieser Dienst durch dubiose Firmen gleich eingebaut wird. Ein Hersteller von Firmware für Smartphones, also von tief im System sitzenden Programmen, welche die Kommunikation und Steuerung zwischen Betriebssystem und verbauten Hardwarekomponenten ermöglichen, hatte zusätzliche und nicht dokumentierte Funktionalitäten integriert. Darunter befand sich ein versteckter Proxy-Zugang. Diese vermietete der Anbieter in Form von 15-minütigen Zugriffsmöglichkeiten, bei denen die betroffenen Smartphones ohne Wissen ihrer Besitzerinnen und Besitzer den Datenverkehr von Dritten unter der eigenen IP-Adresse weiterleiteten. Motivation des Herstellers war wohl, dass die Erträge aus dem Verkauf der Firmware nicht mehr rentabel genug waren, weshalb auf diese Weise eine zusätzliche Einkommensquelle geschaffen wurde. Auch wenn nur eine überschaubare Anzahl an Smartphonebesitzern in Asien betroffen waren, unterstreicht der Fall die Risiken der weltweiten IT-Lieferketten.

3.6 ALLTÄGLICHER „CYBERWAR“

Selbst wenn ein Gerät von einem vertrauenswürdigen Hersteller stammt und die Lieferkette kontrolliert ist, gilt es wachsam zu bleiben. Gerade sicherheitsrelevante Komponenten wie Firewalls oder Systeme zur Einbruchserkennung sind interessante Ziele für Angreifer – beherrscht man sie, kann man mühelos weiter in die dahinterliegenden Netze vordringen. Hierzu zählten in den letzten Monaten Firewalls der Firmen Fortinet, Palo Alto Networks, Zyxel, SonicWall oder CISCO.

Das britische Cybersecurity-Unternehmen Sophos stellte jüngst eindrucksvoll dar, wie intensiv Cyberoperationen mittlerweile ausgetragen werden. Über fünf Jahre hinweg wurden vom Unternehmen angebotene Firewalls in der Operation „Pacific Rim“ durch chinesische Angreifer attackiert [186]. Was mit einer Infiltration und Ausspähung einer Niederlassung in Indien begann, entwickelte sich zunächst zu einer Masseninfizierung von Zehntausenden von Firewalls weltweit, welche dann als Teile von ORB-Netzen zur Verfügung gestellt wurden. Im weiteren Verlauf folgten dann auch verschiedene zielgerichtete und besser verborgene Angriffe, beispielsweise gegen Versorger im Bereich Kernenergie, militärische Einrichtungen, Telekommunikationsanbieter, Nachrichtendienste und den Flughafen einer nicht näher genannten Hauptstadt.

Die Hartnäckigkeit der Angreifer führte dazu, dass Sophos in einer aufwändigen Operation die Firewalls, auf denen die Angriffe zunächst entwickelt und getestet wurden, aufspürte. In die Geräte brachte Sophos anschließend selbst Implantate ein, um die Aktionen der Eindringlinge zu beobachten. Schließlich erlangte Sophos auch Zugriff auf die in Entwicklung befindliche Schadsoftware. Auf dieser Basis gelang es, die jahrelange Aktion auf ein konkretes Netzwerk von Sicherheitsforschern im chinesischen Chengdu zurückzuführen. Der detaillierte Bericht mahnt vor einem immer aggressiveren und kreativeren Vorgehen der Cyberakteure – und betont die Verantwortung von Hardware- und Softwareherstellern zur Transparenz. Immer noch hüllen sich viele Herstellerunternehmen nach schwerwiegenden Sicherheitsvorfällen in Schweigen. Gerade bei Cybersecurity-Produkten kann dies drastische Folgen für die Benutzer oder deren Kunden haben.

Die ohnehin bereits erhebliche Angriffsoberfläche könnte sich durch neue Dienste und eine Vielzahl weiterer Systeme, insbesondere im IoT-Bereich, jedoch noch massiv vergrößern. Die rasante technologische Weiterentwicklung eröffnet immer neue Möglichkeiten, die ganze Lebensbereiche grundlegend verändern können. Viele Bereiche haben ein bei weitem noch nicht ausgeschöpftes Optimierungspotenzial, welches mit Blick auf Herausforderungen wie den Klimawandel und die Not-

Quelle: [288]

Abbildung 25: Neue Möglichkeiten mit 5G im Agrarsektor

wendigkeit der Reduzierung des CO2-Fußabdrucks aktiviert werden muss. So lassen sich beispielsweise in der Logistik durch optimierte Routen und die Nutzung von prädiktiver Instandhaltung erhebliche Einsparungen erzielen, indem Instandhaltungen nicht routinemäßig, sondern nur bei erkanntem Bedarf erfolgen. Auch wenn solche Ansätze nicht neu, sondern bereits seit den 90er Jahren im Einsatz sind, ermöglicht das IoT mit einer Vielzahl neuer Sensorik sowie KI-gestützter Auswertung der umfassenden Datenmengen (Big Data) eine nie dagewesene Genauigkeit, tiefe Systemeinblicke und zahllose neue Anwendungsfälle.

3.7 ENTWICKLUNG DER IT-LAND(WIRT)SCHAFT

Ein gutes Beispiel für solche Entwicklungen ist der Agrarsektor, wo durch die Digitalisierung ein erhebliches Optimierungspotenzial entsteht (Neue Möglichkeiten mit 5G im Agrarsektor siehe Abbildung 25). Die durch umfassende IoT-Sensorik gewonnenen Daten können dort unter anderem helfen, Bodenbedingungen und die Entwicklung des Wetters kontinuierlich zu analysieren, den Gesundheitszustand von Pflanzen zu überwachen und darauf basierend eine optimale Zufuhr von Wasser, Düngemitteln und Pestiziden zu gewährleisten, welche wiederum durch punktgenaue Navigation und Steuerung der entsprechenden Maschinen nur in der absolut notwendigen Menge und mit einem Minimum an menschlichen Arbeitskräften zum Einsatz kommen. Der Landmaschinen-Riese John Deere hat zum Beispiel eine Technologie namens ExactShot eingeführt, bei der ein Sensor genau registriert, wann jeder einzelne Samen in die Erde eingebracht wird, woraufhin eine kleine Menge von Dünger direkt auf den Samen gesprüht wird, anstatt den gesamten Boden zu düngen. Dies könnte weitflächig eingesetzt alleine in den Vereinigten Staaten jährlich 352 Millionen Liter Dünger einsparen [84].

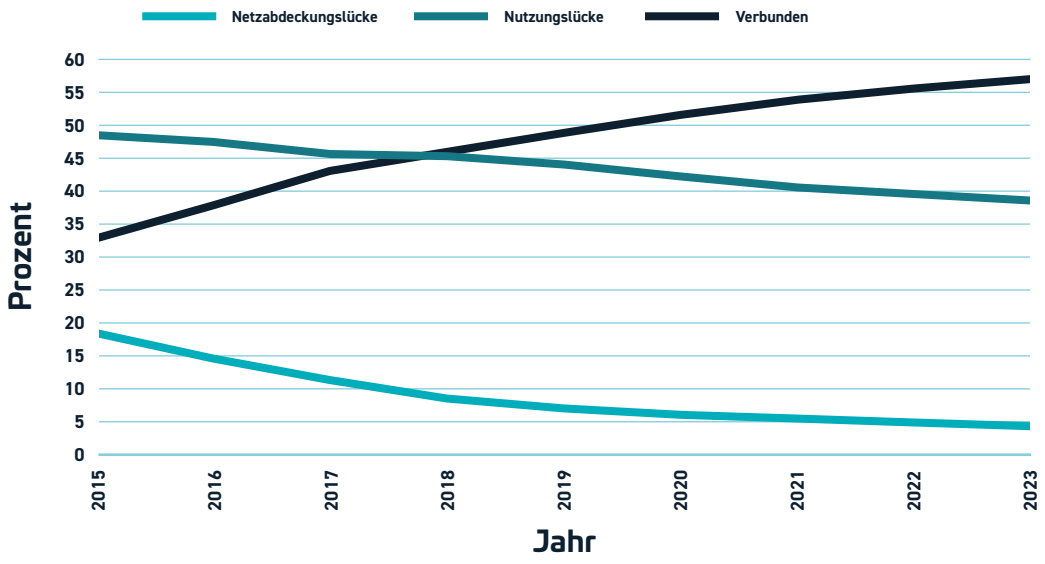
Mit entsprechender Sensorik und Datenauswertung versehen können neben der Reduzierung von Düngemitteln und Wasserbedarf Ernten auch zum bestmöglichen Zeitpunkt initiiert oder Pflanzenkrankheiten frühzeitig erkannt werden. Das Zusammenspiel von Bodensensorik, Drohnen, automatisierten Maschinen und deren Konnektivität ist dabei elementar. Die Kehrseite: Hersteller versuchen immer wieder, ihre Marktstellung zu sichern und auszubauen, beispielsweise durch die Einschränkung von Interoperabilität (sogenanntes Vendor-Lock-in) oder die Sperrung des Zugriffs auf Funktionalitäten und die Innereien ihrer Systeme. John Deere wurde beispielsweise für Praktiken kritisiert, Reparaturmöglichkeiten durch Dritte mittels proprietärer Fehlercodes sowie die Koppelung der Maschinenteile an die Fahrgestellnummer (VIN) der Traktoren zu verhindern. Auch ermöglicht der jederzeitige Fernzugriff durch den Hersteller Maßnahmen wie die Deaktivierung eines Systems. Dies dürfte bei Maschinen der Fall gewesen sein, die während der russischen Besetzung von Melitopol Anfang 2022 durch die Angreifer gestohlen wurden [179]. Während dieses Beispiel positiv bewertet werden kann, ist die Bedeutung einer sicheren Implementierung solcher Funktionalitäten

und der entsprechenden Zugriffswege jedoch essenziell. So machte bereits im Jahr 2010 in den Medien ein Vorfall die Runde, bei dem ein Hacker eine Flotte mit mehr als 100 Fahrzeugen gesperrt hatte, indem er ein System hackte, welches eigentlich nur die Nutzung von Fahrzeugen bei säumiger Zahlung unterbinden sollte [235]. In diesem Zusammenhang sei auch an das Datenleck bei Volkswagen in der AWS Cloud erinnert, wodurch exakte Nutzerprofile inklusive Bewegungsverhalten von über 600.000 Kunden mit Fahrzeugen erstellbar waren [169].

3.8 VORAUSSETZUNG KONNEKTIVITÄT

Zunächst bedarf es für die Realisierung solcher neuer Anwendungsfelder jedoch einer zuverlässigen und weitflächigen Verfügbarkeit von Netzverbindungen. Genau dies stellte gerade im ländlichen Raum bisher immer wieder eine Herausforderung dar. Nach Angaben der GSM Association [123] sind mittlerweile 96 Prozent der Weltbevölkerung mit mobilem Breitband versorgt, und 57 Prozent der Weltbevölkerung, knapp 4,6 Milliarden Menschen, nutzen bereits mobiles Internet auf eigenen Geräten (siehe Abbildung 26).

Ermöglicht wird dies durch eine komplexe Infrastruktur von knapp 1.400 Telekommunikationsanbietern, die weltweit über schätzungsweise sieben Millionen Funkmasten Mobilfunknetze verschiedener Standards von 2G bis 5G ausstrahlen. Während 80 Prozent der genutzten Smartphones bereits 4G oder 5G unterstützen, ermöglichen frühere Generationen den Zugang für ältere Geräte



Quelle: [123]

Abbildung 26: Entwicklung der Abdeckung und Nutzung zellularer Netze

– oftmals sind dies aber nicht mehr die Telefone in den Händen der Nutzerinnen und Nutzer, sondern betreffen Dienste, die eher im Hintergrund arbeiten: So basieren beispielsweise noch verschiedene Notrufsysteme auf 2G. Da nun auch in den europäischen Ländern zunehmend die Abschaltung der alten Netzgenerationen vorangetrieben wird, kann der Druck auf die Notruftaste im Fahrstuhl bald im Nichts enden, wenn nicht rechtzeitig umgerüstet wird.

Dies mag zunächst zwar bedauerlich klingen, ist aber längst überfällig, denn europäische Länder hinken hier hinterher: Australien hatte das Ende seiner 2G-Infrastruktur bereits im Jahr 2016 eingeleitet und 2018 abgeschlossen. Dies ist nicht nur aus Sicht der Freigabe und Neuzuteilung der entsprechenden Frequenzen für neuere Netzgenerationen sinnvoll, sondern auch unter Sicherheitsaspekten. Dabei spielt nicht nur das Alter eine Rolle (2G ist eine Entwicklung aus den 1980er Jahren), sondern das Sicherheitsmodell ist aus heutiger Sicht schlichtweg unzureichend: So muss sich in 2G-Netzen zwar das Mobiltelefon gegenüber dem Provider-Netz authentisieren, nicht jedoch das Netz – und somit der Funkturm vor Ort – gegenüber dem Mobiltelefon. Deshalb ist es auch so einfach, bösartige Funkzellen in 2G einzubringen und Verbindungen zu übernehmen.

Es ist also mehr als an der Zeit, die alten und unsicheren Systeme abzuschalten, denn sie erhöhen auch in den Infrastrukturen der Telekommunikationsdienstleister die Angriffsfläche, beispielsweise durch noch in Nutzung befindliche alte Protokolle und Sicherheitsgefälle zwischen verschiedenen Netzgenerationen – ein insgesamt hochkomplexes Gesamtsystem.

Trotzdem ist dieses nicht in der Lage, alle Winkel auf der Erde zu erreichen. Dass 96 Prozent der Weltbevölkerung abgedeckt sind, liegt vor allem an den großen Ballungszentren, während im ländlichen Raum immer noch unterversorgte Bereiche existieren. Aber auch hier ist bereits eine Lösung verfügbar, und neue Technologien könnten mit rasanter Geschwindigkeit für einen Lückenschluss sorgen.

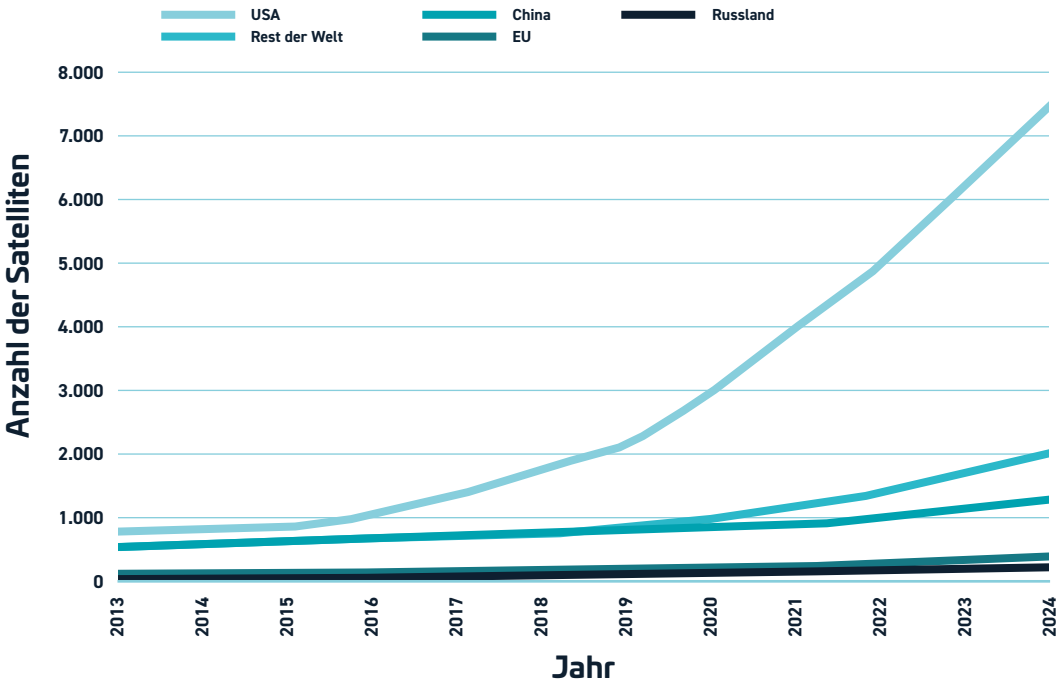
Das 3GPP-Konsortium (The 3rd Generation Partnership Project), der Verbund von Standardisierungsorganisationen, der unter anderem die LTE und 5G-Technologien spezifiziert hat, legte auch die Grundlagen für die Einführung von „Massive IoT", also Netzen mit einer sehr hohen Anzahl von Geräten, die typischerweise einfach strukturiert sind, wenig Energie verbrauchen und relativ preiswert sind [123]. Die zugehörigen Standards für schmalbandiges IoT (Narrowband IoT, NB-IoT) und „LTE-M" (Long-Term Evolution Machine Type Communications) koexistieren mit den heutigen 5G-Standards – und können nicht nur von den terrestrischen, zellularen Mobilfunknetzen (Terrestrial Network, TN) ausgestrahlt werden, sondern auch von Satelliten (Non-Terrestrial Network, NTN).

Die ersten entsprechend spezialisierten 5G-Schmalband-IoT-Himmelskörper sind bereits in ihren Umlaufbahnen und werden künftig eine weltweite, lückenlose Abdeckung und Anbindung von IoT-Geräten ermöglichen. Praktisch bedeutet dies, dass ein IoT-Gerät über die Funkmasten eines Mobilfunknetzes kommuniziert, wenn diese in entsprechender Nähe sind. Ist dies nicht der Fall, kann es seine Daten über speziell hierfür vorgesehene Satelliten senden – und somit beispielsweise die beschriebenen IoT-Szenarien in der Landwirtschaft ermöglichen, jederzeit und an jedem Punkt der Erde.

3.9 CYBER IM WELTRAUM

Durch die neuen technologischen Möglichkeiten erleben die Weltrauminfrastrukturen in den letzten Jahren eine explosionsartige Entwicklung, beispielsweise im Bereich schneller Internetzugänge.

Früher standen Kommunikationssatelliten hauptsächlich im geostationären Orbit (Geostationary Earth Orbit, GEO) in einer Höhe von knapp 36.000 Kilometern fest über einem Punkt der Erde. Der Vorteil ist, dass sich mit einer geringen Anzahl von Satelliten große Bereiche der Erdoberfläche abdecken lassen. Aufgrund der großen Distanz haben diese allerdings lange Signallaufzeiten und durch die hohe Anzahl gleichzeitiger Verbindungen relativ geringe Datenübertragungsraten.



Quelle: eigene Darstellung

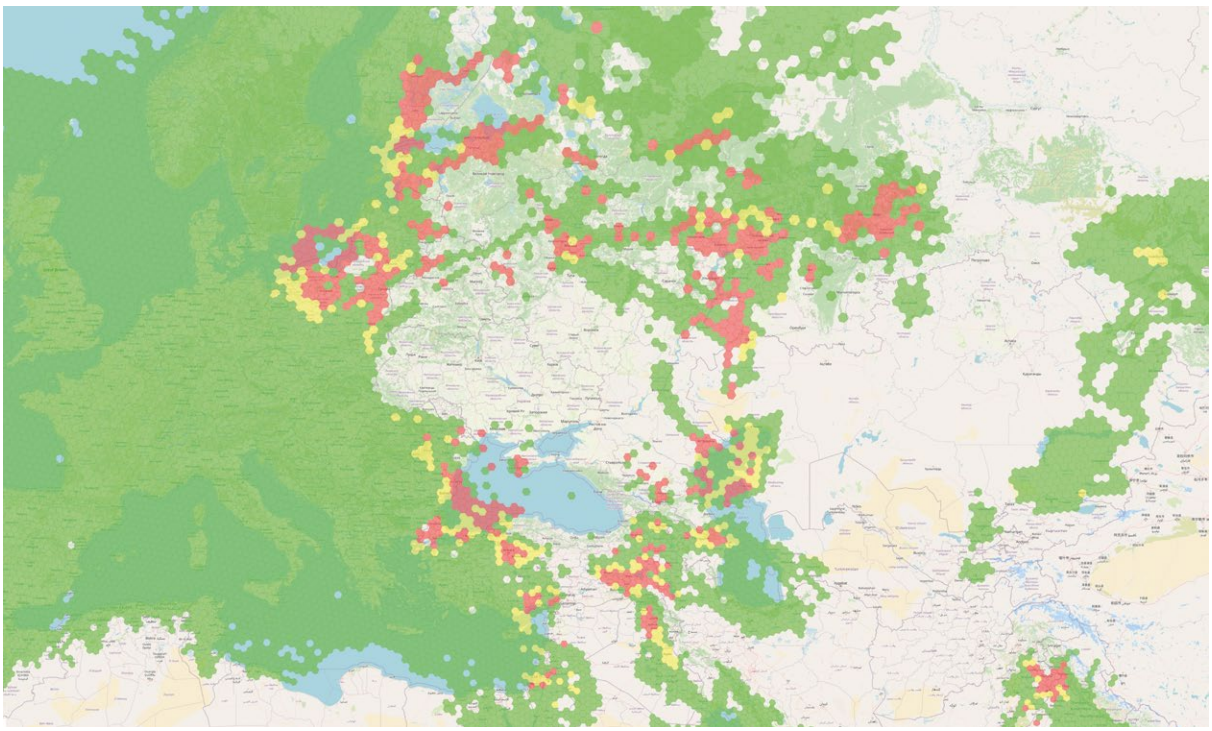
Abbildung 27: Entwicklung der Anzahl an Satelliten nach Nationen

Im mittleren Erdorbit (Medium Earth Orbit, MEO) finden sich hauptsächlich Satelliten von Navigationssystemen, wie beispielsweise das Global Positioning System (GPS). Die Höhe und Satellitenbahnen ermöglichen es, dass von jedem Punkt der Erde jederzeit mindestens vier Satelliten zu sehen sind, was für eine genaue Positionsbestimmung erforderlich ist. Satelliten in der erdnahen Umlaufbahn (Low Earth Orbit, LEO) fliegen dahingegen relativ nah über der Erdoberfläche. Dies erfordert für eine globale Abdeckung eine sehr hohe Anzahl an Satelliten. Dementsprechend war dieser Bereich früher Erdbeobachtungs- und Aufklärungssatelliten vorbehalten, welche je nach genauer Höhe ein bis drei Tage für eine Abdeckung der gesamten Erdoberfläche benötigen. Durch die hohen Kosten blieb die Zahl an Systemen jedoch begrenzt. Gerade beim Aufbau der ersten satellitenbasierten, kommerziellen Telekommunikationssysteme in den 80er und 90er Jahren mussten mehrere Unternehmen, wie beispielsweise Iridium und Globalstar, Insolvenz anmelden [183], [230]. Durch Investoren und Umstrukturierungen konnten diese Anbieter jedoch später den Betrieb wieder aufnehmen.

Durch die Wiederverwendung von Raketen und entsprechend günstigere Verbringung sowie die gesunkenen Produktionskosten für neue Satelliten wurde leistungsfähigen Megakonstellationen im LEO der Weg eröffnet. Die Starlink-Satelliten befinden sich beispielsweise in einer Höhe von 550 Kilometern. Die Laufzeit des Signals beträgt hier nur etwa 25 Millisekunden, während es bei einem geostationären Satelliten aufgrund seiner Höhe 500–600 Millisekunden Verzögerung gibt – für viele Dienste im Internet heutzutage nicht mehr akzeptabel. Die niedrigen Umlaufbahnen und relativ kleinen abzudeckenden Flächen pro Satellit ermöglichen weiterhin hohe Datenraten. Diese Leistungsparameter haben dafür gesorgt, dass sich Starlink nicht nur in abgelegenen Regionen als zuverlässiger und schneller Internet-Zugangspunkt erwiesen hat, sondern auch neue Möglichkeiten für Flugzeuge und Schiffe weltweit bietet oder beispielsweise im Ukraine-Krieg eine bedeutende Rolle spielt.

Die potenziellen Anwendungsfälle und wirtschaftlichen Perspektiven treiben die Weiterentwicklung des Bereichs rasant voran. Eine Reihe weiterer Megakonstellationen steht bereits in den Startlöchern. Während Starlink derzeit mit über 6.900 Satelliten den Orbit mit Abstand dominiert [240], hat OneWeb bereits deutlich über 600 Satelliten in Umlaufbahnen, und Projekte wie Chinas Qianfan mit geplanten über 15.000 Satelliten oder Amazons Projekt Kuiper mit 3.236 Satelliten werden dafür sorgen, dass es voll am Himmel wird (siehe Abbildung 27). Auch die EU hat jüngst 10 Milliarden Euro für das Projekt „Infrastructure for Resilience, Interconnectivity and Security by Satellite“ (IRIS^2) beschlossen, um Europa bis 2030 mit einer sicheren, autonomen Kommunikationsmöglichkeit via 290 Satelliten zu versorgen [93].

Was mit herkömmlichen TN aufgrund des hohen erforderlichen Aufwands und der damit verbundenen Kosten nicht komplett erreicht werden konnte – eine 100-prozentige, weltweite Netzabdeckung – wird durch die neuen Satellitensysteme im LEO Realität.



Quelle: [329]

Abbildung 28: Störung von GPS-Signalen

Während dies viele neue Anwendungsfälle, wie am Beispiel der Landwirtschaft bereits angerissen, ermöglicht, entstehen auch neue Herausforderungen. Nachdem sich Starlink als wichtiges System für die Ukraine im Kampf gegen die russischen Invasoren entwickelt hatte, kündigte Moskau an, dass es dieses als legitimes militärisches Ziel betrachten kann. Bisherige Aktivitäten des Kreml beschränkten sich jedoch auf Störmaßnahmen mit elektronischen Systemen wie Tobol oder Tirada-2, denn Russland verwendet selbst – mittels illegal erworbener Terminals – Starlink. Darüber hinaus birgt ein umfassender Angriff auf die Satelliten eines amerikanischen Anbieters ein erhebliches Eskalationspotenzial.

Störmaßnahmen gegen Satellitensignale sind nichts Neues und können manchmal ganz unscheinbare Ursachen haben. Im Falle eines Lkw-Fahrers in Newark, USA, nutzte dieser schon im Jahr 2013 einen GPS-Störsender, um ein System der Firma auszuhebeln, welches die Routen der Fahrzeuge in Echtzeit mitverfolgte – vielleicht, um die eine oder andere ungesehene Pause machen zu können. Allerdings führten seine Wege auch wiederholt zum internationalen Flughafen Newark Liberty, wo es zu Beeinträchtigungen des Flugverkehrs aufgrund des Störsenders kam. Die Ursache wurde entdeckt und der Fahrer zu einer Geldstrafe von knapp 32.000 US-Dollar verurteilt – und von seiner Firma entlassen [93].

Waren solche Störungen früher Einzelfälle, kommt es durch die veränderte geopolitische Situation mit ihren zahlreichen Krisenherden und Kriegen mittlerweile zu permanenten und weiträumigen Beeinflussungen. Spätestens seit Beginn des Ukraine-Kriegs mit der russischen Invasion im Februar 2022 gehört das Stören entsprechender Signale zum Alltag, sowohl in den Kriegsgebieten als auch in anderen gefährdeten Regionen mit kritischer Infrastruktur.

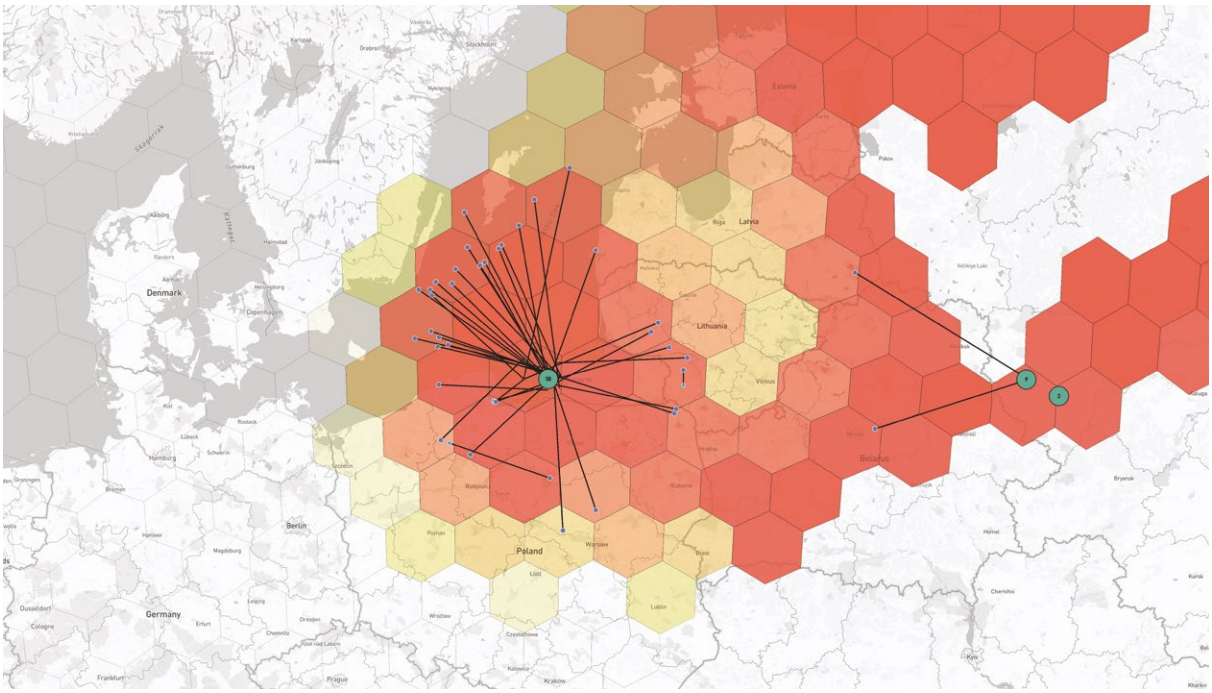
Ziel der Störversuche ist es, Drohnen und Lenkflugkörper, die von der Satellitennavigation abhängen, zu verwirren und an den eigentlichen Zielen vorbeizulenken. Schätzungen gehen davon aus, dass im Ukraine-Krieg 75 Prozent der Drohnen beider Seiten mittels solcher elektronischen Störmaßnahmen ausgeschaltet werden. Dies wirkt sich auch auf andere Bereiche wie die zivile Luftfahrt aus. So kam es bereits mehrfach zu Einschränkungen des Flugverkehrs im Ostseeraum. Finnair hatte zum Beispiel seine Flüge nach Tartu Anfang 2024 für einen Monat aufgrund der vermutlich von Russland ausgehenden, massiven GPS-Störungen im Ostseeraum ausgesetzt [244]. Webseiten wie GPSJAM geben einen Überblick über die aktuelle Situation und stellen auch historische Daten bereit (siehe Abbildung 28), die einem die heutige Dimension solcher Aktivitäten vor Augen führen.

Gefährlicher als reines Stören von Signalen ist deren Manipulation, das sogenannte Spoofing. In diesem Fall „verschwindet" das Signal nicht einfach beziehungsweise kann von einem Empfänger nicht genutzt werden, weil es von einem anderen, stärkeren Signal überlagert wird. Stattdessen wird ein korrekt aussehendes Signal (wiederum stärker als das Originalsignal) erzeugt, sodass der Empfänger nur dieses „sieht" und verarbeitet,

was sich dann beispielsweise in einer falschen GPS-Position widerspiegeln kann. Ist der Versatz nur klein, kann dies zunächst völlig unauffällig sein, beispielsweise in engen Fahrwassern, aber schnell katastrophale Folgen haben. In diesem Kontext sei an die Folgen für Seefahrt und weltweite Wirtschaft erinnert, nachdem das Containerschiff „Ever Given“ im März 2021 sechs Tage den Suezkanal blockierte. Der Vorfall war zwar keinem Cyberangriff auf die Positions- oder Steuerungssysteme des Schiffes, sondern starken Winden, geschuldet, aber die Möglichkeiten für einen bösartigen Akteur liegen auf der Hand.

Auch ohne gezielten Angriff auf ein bestimmtes Fahrzeug stellen die umfassenden Aktivitäten und betroffenen Gebiete mittlerweile eine Gefährdung für die zivile Luftfahrt dar: Im letzten Jahr wurde ein Anstieg von Spoofing um 500 Prozent beobachtet. Während im ersten Halbjahr 2024 knapp 300 Flüge pro Tag fehlerhafte Positionen durch ihre GPS-Systeme erhalten hatten, wuchs diese Zahl im zweiten Halbjahr auf knapp 1.500 pro Tag an. Konkret wirkt sich dies so aus, dass im Cockpit eine fehlerhafte Position angezeigt wird, welche möglicherweise nicht auffällt. Nur wenn die Piloten rechtzeitig Informationen über GPS-Störungen in einem Gebiet haben und deren Verarbeitung im System aktivieren, können fehlerhafte Positionsanzeigen verhindert werden.

Die tägliche Betroffenheit und somit Gefährdung der zivilen Luftfahrt wird mit einem Blick auf entsprechende Tracking-Seiten offensichtlich: Während die blauen Punkte die tatsächlichen Positionen der Flugzeuge anzeigen,



Quelle: [261]

Abbildung 29: Beispiel von GPS-Spoofing der zivilen Luftfahrt im Januar 2025

werden ihren Systemen Positionen im grün markierten Bereich vorgetäuscht – am 11. Januar 2025 hatten beispielsweise mindestens 58 Flüge rund um Kaliningrad fehlerhafte Positionen (siehe Abbildung 29).

Kritisch ist, dass hiervon auch besonders sicherheitsrelevante Systeme wie zum Beispiel das Bodenannäherungswarnsystem (Ground Proximity Warning System, GPWS) betroffen sind. Dazu kommt, dass bei mindestens einem Flugzeugtyp verschiedene Systeme der Bordelektronik identifiziert wurden, die nach einem Spoofing-Angriff nicht mehr in einen korrekten Betriebszustand übergehen, selbst wenn die Störung beendet ist [220] – so auch das GPWS.

Hierdurch kann es im weiteren Flug zu einer erheblichen Zahl von Fehlermeldungen des Systems kommen und somit auch zu dem als Alarmmüdigkeit (Alert Fatigue) bekannten Effekt: Durch die überwältigende Anzahl von Fehlalarmen stellt sich schnell eine Desensibilisierung ein. Sollte dann tatsächlich ein echter Alarm darunter sein, wird diesem keine Beachtung mehr geschenkt, da er nur ein weiterer von vielen Fehlalarmen zu sein scheint – mit in einem solchen Szenario möglicherweise tödlichen Konsequenzen. Die Elektronik vieler der circa 200.000 Flugzeuge, welche täglich weltweit unterwegs sind, scheint dafür jedenfalls alles andere als vorbereitet zu sein. In einem Fall wurde berichtet, dass ein Flugzeug nach einem Spoofing-bedingten großen Sprung der Systemzeit in die Zukunft für mehrere Wochen zur Instandsetzung aus dem Verkehr gezogen werden musste [199]. Zwar waren die Piloten in der Lage, die Maschine sicher zu landen, die Systeme konnten anschließend jedoch nur durch Neuaufsetzen in einen korrekten Zustand zurückgebracht werden.

Durch die zunehmenden Abhängigkeiten vom Weltraumsegment verschärft sich diese Situation noch weiter. So haben beispielsweise kleinere Flughäfen begonnen, ältere Instrumentenlandesysteme (ILS) aufgrund ihrer hohen Betriebskosten stillzulegen und durch „Localizer Performance with Vertical Guidance“ (LPV) zu ersetzen – letzteres ist ein GPS-basierter Anflug. Sind die GPS-basierten System an Bord des Flugzeugs gestört, bietet ILS eine sichere, unabhängige Technologie, um auch unter schlechten Wetterbedingungen und ohne Sicht sicher landen zu können. Steht nur noch LPV zur Verfügung, hat die Besatzung in solchen Situationen ein echtes Problem.

Die aus Sicherheitsgründen hohen Auflagen in der Luftfahrt erschweren allerdings auch ein zeitnahes Schließen eventuell erkannter Schwachstellen in IT-Systemen eines Flugzeugs. Die erforderlichen Tests und Rezertifizierungen können Monate und länger dauern – es empfiehlt sich also, redundante Technologien wie ILS auch weiterhin möglichst umfassend beizubehalten. Eine Umfrage im letzten Jahr ergab, dass knapp 70 Prozent der Aircrews die Auswirkungen von GPS-Spoofing auf die Flugsicherheit als sehr hoch oder extrem bewerten [220]. Nicht nur die Luftfahrt ist durch Signalmanipulationen gefährdet: Dies zeigen beispielsweise Beobachtungen verfälschter Schiffspositionen im Hafen von Schanghai aus dem Jahr 2019.

Vor dem Hintergrund der massiven Aktivitäten gegen Dienste wie GPS ist auch die Besorgnis über die russischen Aktivitäten rund um den Satelliten COSMOS 2553, der am 5. Februar 2022 in eine sehr ungewöhnliche Umlaufbahn geschossen wurde, nachzuvollziehen. Dieser befindet sich in einem sogenannten Friedhofsorbit, in dem sich aufgrund der dortigen sehr hohen Strahlungswerte üblicherweise keine aktiven Satelliten befinden, sondern lediglich einige schon lange außer Dienst befindliche Altsysteme.

Laut Moskau soll es sich bei COSMOS 2553 um die Erprobung neuer Systeme unter hoher Strahlenbelastung handeln, während die NASA das System als möglichen Radaraufklärungssatelliten in ihr Archiv aufgenommen hat. Washington hat jedoch seine Besorgnis kommuniziert, dass der Satellit der Erprobung von Technologien dienen könnte, um einen Atomsprengkopf im Orbit zu platzieren [131].

Die erhebliche Wirkung, die eine Atomdetonation in solchen Höhen hätte, wurde von den USA beim Projekt Starfish Prime bereits im Jahr 1962 untersucht. Während der elektromagnetische Impuls der in einer Höhe von 400 Kilometern über dem Pazifik gezündeten Wasserstoffbombe mit einer Sprengkraft von 1,4 Megatonnen sogar noch

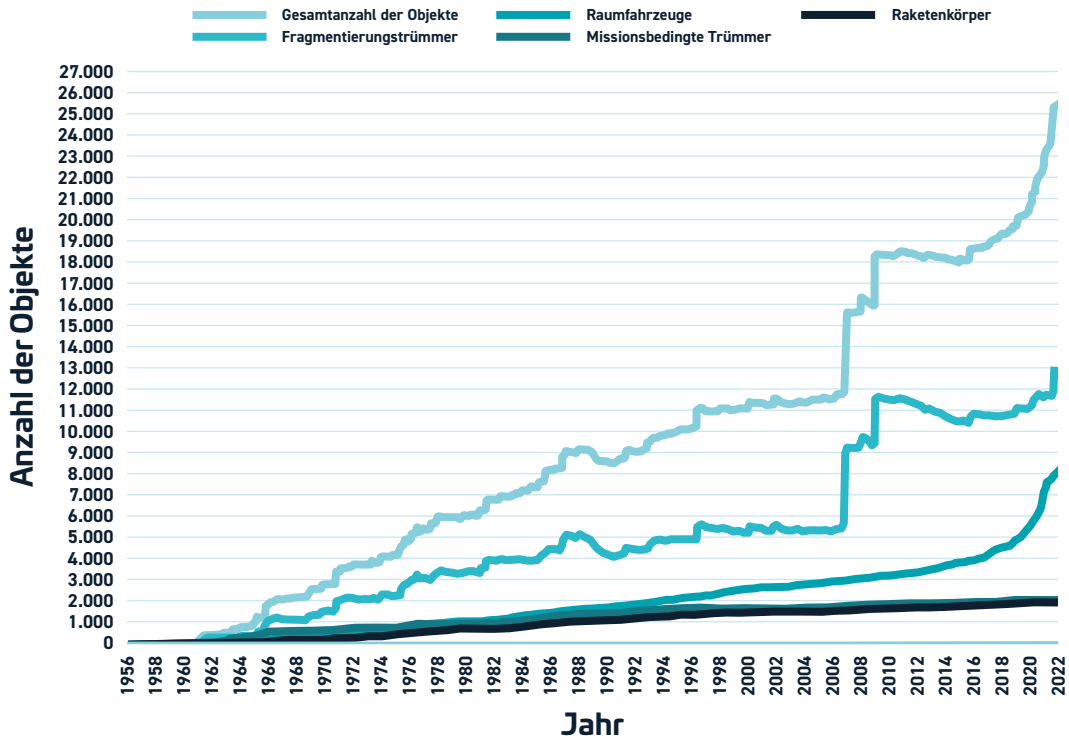
Infrastruktur auf Hawaii zerstörte, beeinflusste die durch die Explosion erhöhte Strahlung im Orbit mehrere Satelliten und sorgte auch nach Monaten noch für Ausfälle, sodass ein Drittel der damals (vergleichsweise äußerst geringen Anzahl von) aktiven Satelliten zerstört wurde. Die sehr viel intensiveren Effekte als von der Wissenschaft erwartet führten schließlich zur Unterzeichnung des Weltraumvertrags von 1967, welcher die Platzierung von Nuklearwaffen im Weltall verbietet.

Auch wenn ein solches Szenario ziemlich unwahrscheinlich ist, kann es vor dem Hintergrund der heutigen geopolitischen Spannungen nicht mehr vollständig ausgeschlossen werden. In vielen Bereichen, wie Militär, Aufklärung aber auch Wirtschaft, haben die USA und zahlreiche weitere Nationen weitaus größere Abhängigkeiten von den künstlichen Erdtrabanten als Russland. Ein entsprechender Angriff hätte daher insbesondere auf die westlichen Nationen ungeheure Auswirkungen. Die Nichtverfügbarkeit der globalen Satellitennavigationssysteme (Global Navigation Satellite Systems, GNSS), allen voran GPS, hätte, wie bereits durch die zuvor beschriebenen Störungen erkennbar, massive Auswirkungen auf die Luft- und Seefahrt, aber auch auf die Logistik an Land. Ebenso wären zahlreiche Waffensysteme wie beispielsweise GPS-gelenkte Präzisionsmunition nur noch bedingt und stellenweise gar nicht einsetzbar – ein Grund für die massiven Störmaßnahmen in der Ukraine und in Russland. Die Forderungen amerikanischer Think Tanks, insbesondere die für die Führung und Kontrolle der nuklearen Fähigkeiten wichtigen Satelliten im LEO gegen entsprechende EMP- und Strahlungsgefährdungen zu schützen, liegt daher auf der Hand [17].

Die genaue Position ist jedoch nicht die einzige Größe, die aus den Signalen der Navigationssatelliten durch Trilateration errechnet werden kann [127]: Ein maßgeblicher Aspekt ist die Zeit.

Navigationssatelliten senden Signale, die zum einen Informationen über die Position des Satelliten im Orbit und zum anderen einen Zeitstempel der hochpräzisen internen Atomuhren, über die jeder dieser Satelliten verfügt, enthalten. Hat ein Empfänger mehrere Satelliten im Blick, kann er aus diesen Daten seine eigene Position errechnen, aber auch die eigene interne und sehr viel weniger genaue Uhr mit den hochgenauen Atomuhren synchronisieren. Da dieser Vorgang fortlaufend erfolgt, kann eine Präzision auf 100 Milliardstel Sekunden genau erreicht werden [203], ohne dafür selbst teure, hochgenaue Atomuhren haben zu müssen. Diese extreme Genauigkeit hat zu einer massiven Abhängigkeit in vielen Bereichen geführt. Beispielsweise werden im Finanzhandel und an den Börsen die Uhren interner Systeme mit der GPS-Zeit synchronisiert, um Zeitstempel für Transaktionen zu erstellen. Die hochgenaue Zeit dient der Synchronisation der Basisstationen – sozusagen der Funkmasten – der Mobilfunkanbieter; Energieversorgungsunternehmen nutzen sie sowohl zur Synchronisation in Kraft- und Umspannwerken als auch zur schnellen Erkennung von Fehlern im Stromnetz. Auch die Uhren von Routern, also der Systeme, die den Datenverkehr im Internet weiterleiten, werden unter anderem mittels der Satellitenzeit synchronisiert. Neben solchen elementaren Beispielen aus den kritischen Infrastrukturen kommt die GPS-Zeit aber noch in vielen anderen Bereichen zum Einsatz, etwa zur schnellen und genauen Lokalisierung von seismischen Aktivitäten – die Liste ist nahezu endlos. Wie sich der Ausfall der hochgenauen Zeit in den jeweiligen Bereichen auswirkt, wie schnell sich eine Zeitabweichung auf Betriebsabläufe auswirken könnte, ist von der jeweiligen Anwendung abhängig, aber in der Breite auch kaum vorhersehbar. Zu komplex sind die Abhängigkeiten. Klar ist jedoch, dass ein breitbandiger Ausfall unserer heutigen Satellitensysteme drastische Konsequenzen in allen Lebensbereichen hätte, das Herbeiführen einer Atomdetonation im Orbit also nur als Ultima Ratio in einem existenziellen Krieg zu erwarten wäre, in dem eine Partei nichts mehr zu verlieren hat.

Auch wenn es nicht zum Super-GAU im Weltall kommen mag, steht eines fest: Der Konkurrenzkampf im Orbit nimmt stetig zu. Ob Kommunikationssatelliten, speziell für Massive IoT entwickelte Konstellationen, Frühwarnsysteme, welche auf Infrarotbasis weltweit Raketenstarts orten können, oder Aufklärungssatelliten mit optischen oder Radarsensoren – die Vielfalt und Möglichkeiten nehmen immer weiter zu. Zwar sind militärische Aufklärungssatelliten nichts Neues, wenn auch wenige Details darüber bekannt sind. Einen Einblick in die hohe



Quelle: [73]

Abbildung 30: Anstieg Debris und der Effekt von ASAT-Tests

Leistungsfähigkeit der US-Systeme hat aber ein Tweet von Donald Trump auf der Plattform X gegeben. Darin veröffentlichte er eine Aufnahme, die Analysten zufolge vom Satelliten USA 224 stammt. Anhand der Position des Satelliten zum Zeitpunkt der Aufnahme sowie deren Beschaffenheit und Details gehen Experten von einer Auflösung von zehn Zentimetern oder besser aus. Vor diesem Hintergrund überrascht es daher nicht, dass mehrere Nationen schon längere Zeit Systeme in Entwicklung haben, um solche hochgenauen Einblicke aus dem Himmel zu verhindern [36].

Versuche mit Anti-Satellitenwaffen (ASAT) begannen bereits in den späten 1950er Jahren, zunächst durch die USA. Während zu Beginn Flugzeuge entsprechende Flugkörper hoch genug verbringen mussten und diese dann gegen Satelliten gestartet wurden, können moderne Systeme wie die Standard Missile 3 (SM3) der US-Streitkräfte auch vom Boden und von See gegen Satelliten eingesetzt werden. Neben den Vereinigten Staaten haben auch China im Jahr 2007, Indien im Jahr 2019 und Russland im November 2021 erfolgreich ASAT erprobt [247]. Diese Tests ernteten mehrfach intensive internationale Kritik, da bei der Zerstörung der Satelliten häufig unzählige kleine Weltraumschrottteilchen, der sogenannte Debris, entstehen und diese sich mitunter über Jahre oder Jahrzehnte in den Umlaufbahnen halten, bis sie letztendlich absinken und verglühen. Die letzten Teile des von den Vereinigten Staaten 1985 mit einer ASAT zerstörten Solwind Satelliten traten beispielsweise 19 Jahre später in die Erdatmosphäre ein. Der chinesische ASAT-Test mit der Zerstörung von Fengyun-1C im Jahr 2007 erzeugte knapp 3.400 größere Teile, von denen viele noch in Umlaufbahnen sind.

Durch die hohen Geschwindigkeiten und somit Energien beim Zusammenstoß im Orbit können auch kleine Teilchen erheblichen Schaden verursachen. Objekte größer als 5 Millimeter können bei Kollision eine Mission schnell beenden beziehungsweise die Systeme komplett zerstören, während es selbst bei Objekten kleiner als ein Millimeter zu Einschränkungen und Fehlern nach einer Kollision kommen kann.

Mittlerweile sind bereits mehr als 29.000 Objekte mit einer Größe von über zehn Zentimetern, stellenweise bis hin zu mehreren Metern, im Orbit, weiterhin schätzungsweise 670.000 Objekte mit Größen zwischen einem und zehn Zentimetern sowie über 170 Millionen Objekte, die zwischen einem Millimeter und einem Zentimeter groß sind. Gerade die ASAT-Tests haben hier jeweils zu großen Sprüngen an Weltraumschrott und Splitterteilen geführt (siehe Abbildung 30).

Auch durch die stark gestiegene Zahl von Raketenstarts und neuer Systeme wird es immer voller im Orbit. Mit einer zunehmenden Anzahl von Objekten steigt entsprechend auch die Gefahr, dass es durch zufällige Kollisionen und die dadurch jeweils entstehenden Trümmerteilen zu einem kaskadierenden Effekt, dem sogenannten Kessler-Syndrom, kommt und in der Folge mehr und mehr funktionsfähige Systeme beschädigt oder zerstört werden, sodass im schlimmsten Fall fast die gesamte Weltrauminfrastruktur ausfallen könnte. Deshalb gibt es verschie-

dene Programme, die den Debris aus den Umlaufbahnen entfernen sollen, wie zum Beispiel das Projekt „Active Debris Removal/In-Orbit Servicing“ (ADRIOS) der europäischen Weltraumagentur ESA [94], [233].

Da Debris nicht differenziert, gefährdet die immer höhere Zahl der Schrottteilchen jegliche funktionsfähige Systeme unabhängig von deren Nationalität. Der Einsatz von kinetischen ASAT-Waffen sollte daher für die meisten Nationen zunehmend unattraktiv werden. Aber nicht nur deshalb. Die ursprünglichen ASAT-Systeme, welche eine kinetische Zerstörung des Ziels avisieren, stammen aus einer Zeit, in der der Orbit relativ leer war und es nur wenige militärische Hochwertsysteme gab, die normalerweise jahrzehntelang im Einsatz waren. So war es durchaus realistisch, die Aufklärungsfähigkeiten des Gegners durch Zerstörung einer entsprechend kleinen Anzahl von Systemen zu stoppen.

Die Kommerzialisierung der Raumfahrt, die rapide technologische Weiterentwicklung und der Erfolg verschiedener Privatunternehmen haben diese Situation jedoch grundlegend verändert. Auch wenn beispielsweise Spitzenauflösungen von unter zehn Zentimetern bei der optischen Aufklärung noch immer einzelnen Militärs vorbehalten sind, so liegt dies eher an staatlichen Regulierungen als den technischen Möglichkeiten. So verbietet die US-Regierung beispielsweise, dass Privatunternehmen Satellitenbilder mit Auflösungen von unter 25 Zentimetern anfertigen und schränkt auch die Nutzung der Frequenzbänder ein. Dass dies trotzdem zu einer neuen Situation geführt hat, zeigen Dienste wie Maxar, dessen Satellitenbilder unter anderem auch durch verschiedene Analysen der Situation in der Ukraine bekannt wurden.

Durch solche neuen Angebote auf dem Markt ist es heutzutage möglich, hochdetaillierte Bilder mit Auflösungen von bis zu 30 Zentimetern, die für wichtige Gebiete der Erde bis zu 15-mal täglich aktualisiert werden, zu kaufen. Hiermit ist nicht nur ein früheres Alleinstellungsmerkmal von Staaten gefallen, sondern die neuen Aufklärungsflotten privater Unternehmen ermöglichen noch viel mehr: eine nahezu Echtzeit-Überwachung der Erdoberfläche, welche immer weiter ausgebaut wird. So lassen sich schon heute mit den aus einer hohen Anzahl relativ einfacher Satelliten erfassten Daten Dienstleistungen wie KI-basierte Analysen von Veränderungen über die Zeit oder auch die Verfolgung von Objekten wie Schiffen beauftragen, während sich die geringe Anzahl äußerst leistungsfähiger militärischer Satelliten typischerweise auf bestimmte Regionen fokussieren muss und die Wiederbesuchsraten geringer sein können.

Den Vereinigten Staaten wurde aufgrund der immensen Möglichkeiten neuer Megakonstellationen schnell klar, dass sie diese auch militärisch nutzen müssen, um ihren technologischen Vorsprung zu halten. Entsprechend wurde mit der Verbringung eines als „Proliferated Architecture“ bezeichneten neuen Aufklärungssystems begonnen, das aus einer Vielzahl kleinerer Satelliten besteht. Auch wenn wenig darüber bekannt ist, scheint es sich bei den bisher mit den Missionen NROL-146, NROL-186, NROL-113, NROL-167 und NROL-126 verbrachten Systemen um Starshield-Satelliten zu handeln, welche auf den Starlink-Internetsatelliten basieren, aber um eine Aufklärungskomponente erweitert sind [317].

Dies ist auch der Grund, warum klassische kinetische ASAT-Waffen an Wert verlieren: Durch die Verteilung der Sensorik auf eine Vielzahl kleinerer Plattformen im LEO wäre auch ein entsprechend umfassender Einsatz von ASAT-Waffen erforderlich, immer mit der Gefahr ungewollter und undifferenzierter Kaskadierung und somit auch der Gefährdung der eigenen Systeme des Angreifers. Gleichzeitig schreiten die durch den zivilen Sektor geschaffenen neuen Möglichkeiten so schnell voran, dass dies eine Herausforderung für Militärs werden kann.

Ein Beispiel ist die Copernicus Sentinel-1-Mission der Europäischen Weltraumorganisation. Das Paar der Sentinel-1-Satelliten, die 2014 und 2016 in Dienst gegangen sind (Sentinel-1B ist im Dezember 2021 ausgefallen und wird durch den im Dezember 2024 in den Orbit verbrachten Sentinel-1C ersetzt, zwischenzeitlich hat nur Sentinel-1A Daten geliefert), hat Radarsysteme an Bord, welche unabhängig von der Tages- und Nachtzeit sowie den Wetterbedingungen Bilder der Erdoberfläche generieren. Dafür werden von den Satelliten kontinuierlich Mikrowellenimpulse mit einer Frequenz von 5,4 Gigahertz ausgestrahlt, die von der Erdoberfläche reflektiert

werden (deshalb auch der Name Sentinel-1 C-Synthetic Aperture Radar, Sentinel-1 C-SAR, da die 5,4-Gigahertz-Frequenz im sogenannten C-Band liegt). Auf Basis der Änderungen des empfangenen reflektierten Signals sowie der Kenntnis über die Position und Bewegung der Satelliten lässt sich letztendlich ein sehr genaues, zweidimensionales Bild generieren [95].

Was dabei jedoch immer passieren kann, ist eine Störung des Signals auf seinem Weg zur Erde oder zurück zu den Satelliten. Insbesondere wenn Systeme am Boden im gleichen Frequenzbereich aktiv sind, kann es zu Interferenzen, also einer ungewünschten Überlagerung von Signalen, kommen, was sich in Fehlern in der Bildgenerierung widerspiegeln kann.

Befinden sich auf dem Boden Radaranlagen, die im gleichen Frequenzbereich wie die Sentinel-1-Satelliten arbeiten, kommt es zu markanten Fehlern im Bild. Auf dieser Basis konnten beispielsweise Patriot-Systeme in Israel identifiziert werden, oder Übungen von Fregatten der russischen Admiral Gorshkov-Klasse, deren Flaggschiff erst 2019 in Dienst gestellt wurde.

Vor dem Hintergrund dieser zunächst überraschenden Fähigkeiten von Sentinel-1 C-SAR war eine Aufnahme von besonderem Interesse, in der es zu besonders intensiven Interferenzen kam. Aufgrund der besonders ausgeprägten Störung gehen verschiedene Analysten davon aus, dass es sich um einen bewussten Test Russlands handelte, die Aufklärung des Satelliten zu stören. Da allerdings auch das im C-Band operierende russische Luftraumüberwachungsradar 96L6 in der Ukraine zum Einsatz kommt, gibt es auch Interpretationen, dass es sich um eine hierdurch verursachte, zufällige Störung handelte.

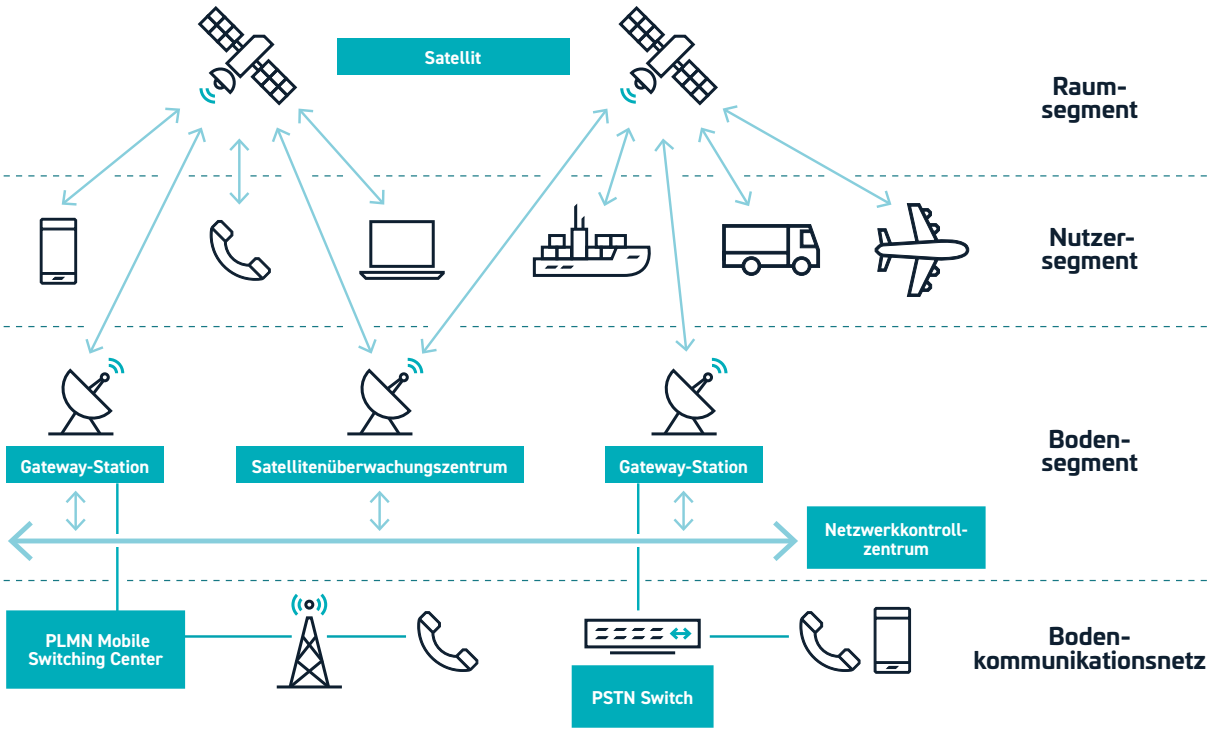
Diese Entwicklungen verdeutlichen aber auch die aus militärischer Sicht zwingende Notwendigkeit, Fähigkeiten zum Schutz vor gegnerischer Aufklärung zu entwickeln. Entsprechend arbeiten verschiedene Nationen an Systemen zum temporären Blenden bis hin zum permanenten Zerstören von Sensorik gegnerischer Aufklärungsplattformen und haben diese stellenweise auch schon in Betrieb genommen. Ein Beispiel für solche Aktivitäten ist das Korla-Versuchsgelände in Xinjiang in China, wo neben Anti-Satelliten-Lasern vermutlich auch Versuche zur Widerstandsfähigkeit von elektronischer Ausrüstung gegen elektromagnetische Impulse (EMP), wie sie auch bei Atomexplosionen in großen Höhen entstehen, durchgeführt werden, oder der Kalina-Laser am russischen Weltraumüberwachungszentrum Krona.

Neben den zuvor beschriebenen kinetischen Möglichkeiten und Lasern gibt es aber noch diverse andere Ansätze weltraumbasierter Waffensysteme, beispielsweise auf Basis von Jamming, hochenergetischen Mikrowellen, dem Versprühen bestimmter Chemikalien oder dem mechanischen Einwirken nach Annäherung.

So finden sich zunehmend Satelliten, die beispielsweise mit Greifarmen ausgestattet sind, so wie der chinesische Shijian-21, der einen ausgedienten Satelliten auf einen höheren Friedhofsorbit anhob. Ein derartiges Manöver ist bei den hohen Geschwindigkeiten der Satelliten von über 28.000 km/h in der Erdumlaufbahn nicht trivial. Während in diesem Fall Weltraummüll aufgeräumt wurde, könnten solche Fähigkeiten im Zweifelsfall auch gegen Satelliten anderer Nationen eingesetzt werden: So konnten Manöver festgestellt werden, bei denen chinesische und russische Satelliten in die Nähe zu anderen Satelliten gebracht wurden und diese beobachteten und sogar verfolgten. Im Mai 2024 hatte Russland beispielsweise COSMOS 2576, einen sogenannten Inspektionssatelliten, in der Nähe eines US-Aufklärungssatelliten positioniert.

Die Dual-Use-Problematik, also die Eigenschaft von Systemen, sowohl zivil als auch militärisch eingesetzt werden zu können, ist hier – wie allgemein im Cyberbereich – inhärent und kann mit Blick auf die besondere Sensitivität der Systeme im Orbit für viele Nationen sehr bedrohlich wirken. Ein derzeit in Erforschung befindliches System zur schnellen Beseitigung von Debris auf Basis mehrerer weltraumgestützter Laser ist ein perfektes Beispiel.

Wie in vielen Bereichen der Weltraumsysteme ist aber auch dieses Spiel keines mehr, welches exklusiv von einigen wenigen Staaten dominiert wird. Neue Start-ups mit dem Potential, den weiteren Verlauf im Orbit nachhal-



Quelle: [320]

Abbildung 31: Architektur von Satellitensystemen.
Längst sind alle Bereiche Cyberbedrohungen ausgesetzt

tig zu beeinflussen, drängen mit innovativen Ideen und neuen Ansätzen ins Feld. So hat zum Beispiel das Start-up GuardianSat eine Förderung zur Erforschung neuer Technologien zum Schutz von Satelliten erhalten. Die Defense Advanced Research Projects Agency (DARPA), eine Forschungseinrichtung des Pentagon, aus deren Projekten nicht nur das Internet, GPS und teflonbeschichtete Pfannen hervorgegangen sind, hat die Notwendigkeit der Einbeziehung innovativer Start-ups als Voraussetzung, technologisch führend zu bleiben, längst erkannt – dies gilt insbesondere auch für den zivilen Raumfahrtsektor [307].

Angesichts der hohen Abhängigkeiten und der weiter schnell zunehmenden Bedeutung der Satelliten im Weltall, des Strebens mehrerer Nationen nach Dominanz sowie der ambitionierten Aktionen und Pläne nebst der neuen Vorreiterrolle von Privatunternehmen ist zumindest eines klar: Es wird ungemütlich werden, vor allem im Cyberraum.

Dabei darf insbesondere nicht vergessen werden, dass die künstlichen Himmelskörper nicht isoliert betrachtet werden dürfen – sie sind Teile eines komplexen Gesamtsystems (Architektur von Satellitensystemen siehe Abbildung 31). Während frühere Satellitengenerationen, beispielsweise für Fernsehübertragung, sehr einfach konzipiert und prinzipiell nur Relaiselemente waren, die ein von der Bodenstation kommendes Signal aufgenommen, verstärkt und wieder abgestrahlt haben, wurden im Laufe der Zeit immer mehr Funktionalitäten realisiert.

Neben hochkomplexen militärischen Aufklärungssatelliten, preisgünstigen, relativ kleinen, aber hochentwickelten Kommunikationssatelliten, etwa im Starlink-Verbund oder in den bildgebenden Aufklärungsflotten von Privatunternehmen wie Maxar, BlackSky und Planet, sind immer mehr Systeme im Himmel anzutreffen. Mit Satellite Computing, der Verarbeitung von Daten direkt im Orbit, um neue Anwendungsfälle zu eröffnen, wird dies noch weiter zunehmen, und auch die Komplexität der Systeme weiter steigen. Dadurch wird auch die Cybersecurity aller beteiligten Komponenten immer kritischer, von den IT-lastigen Satelliten und dem Schutz ihrer Signale, über die Bodenstationen zur Steuerung bis zu den Verbindungselementen in andere Netze und Systeme.

Während früher eher die bodengebundenen Teile Gefahr liefen, Ziel eines Angreifers zu werden, hat die schnelle Weiterentwicklung des Raumsegments und insbesondere die zu Beginn geringen Cybersecurity-Maßnahmen sowie sinkende technische Einstiegshürden den Angriff auf Satelliten attraktiv gemacht. Um dem entgegenzuwirken und die Sicherheit der Systeme ins Visier zu nehmen, hat die U.S. Air Force im Jahr 2020 den sogenannten Hack-a-Sat-Wettbewerb ins Leben gerufen. Dort bekommen Hacker verschiedene Aufgaben gestellt, die Ergebnisse sollen in die Entwicklung sicherer Systeme einfließen.

Dass noch immer ein großer Nachholbedarf bezüglich Sicherheit im Bereich der Satellitensysteme besteht, haben spätestens die Auswirkungen des Russland zugerechneten Cyberangriffs auf ViaSats KA-SAT-System

zu Beginn der Ukraine-Invasion gezeigt, bei dem neben mehreren tausend Kunden in der Ukraine unter anderem auch über 5.800 Windkrafträder von Enercon in Deutschland betroffen waren. Mittels eines bösartigen Softwareupdates und einer Wiper-Software war es den Angreifern gelungen, die Firmware der Satellitenmodems zu löschen und diese somit unbrauchbar zu machen – ein gar nicht mal sehr sophistizierter, aber durchaus wirkungsvoller Angriff.

3.10 GRENZENLOS BEDROHT

Der Streifzug vom Meeresboden bis ins Weltall offenbart die Komplexität der heutigen sich schnell entwickelnden Situation mit ihren unzähligen Faktoren und Abhängigkeiten. Cyberbedrohungen lauern an allen Ecken und Enden. Von Cyberkriminalität bis zu staatlich gesteuerten Cyberoperationen entwickeln die Akteure ihre Verfahren kontinuierlich weiter, um unerkannt im Cyberraum zu agieren. Die empfindlichen Energieversorgungsnetze und die leicht angreifbaren Nervenbahnen der weltweiten Kommunikation, selbst abhängig von IT, stehen durch die gestiegenen geopolitischen Spannungen vor besonderen Herausforderungen. Durch die über Jahrzehnte immer stärker gewordenen Abhängigkeiten und globale, äußerst komplexe Versorgungsketten ist es sophistizierten Akteuren ein Leichtes, durch den Cyberraum Effekte mit katastrophaler Auswirkung im realen Umfeld zu initiieren.

Noch ist der Wettlauf aber nicht verloren. Viele Initiativen gehen grundlegende Mängel an, von den Forderungen nach sicheren Auslieferungszuständen ohne Leer- oder Trivialpasswörter bei neuen IT-Komponenten bis zu den Förderungen zum Aufbau lokaler Halbleiterkapazitäten und der Entwicklung eines europäischen Hochleistungsprozessors auf Basis der offenen RISC-V-Prozessorarchitektur. Entscheidend ist, die Souveränität Europas in allen Bereichen, von der Hardware bis zur Software, zu erhöhen. In der Praxis mangelt es bis dato nicht an guten Ideen und geeigneten Programmen. Vielmehr ist die Ausschöpfung der vorhandenen Möglichkeiten und deren ernsthafte Umsetzung das Problem. Solange Produktauswahl nicht auf Sicherheitserwägungen, sondern Lobbyismus, mangelndem Systemverständnis und Angst vor Änderungen erfolgt, wird sich nichts verbessern und ein Super-GAU nur eine Frage der Zeit sein.

KAPITEL 4

PRODUKTCHAOS
HERAUSFORDERUNG DER CYBERSECURITY-LÖSUNGSLANDSCHAFT

3.500
Anbieter weltweit einschl. Startups

bis zu 6
Produkte pro Anbieter

bis zu 336
aktive Produkte in größeren Unternehmen

EUR
5,8 Mrd.
Ausgaben in Deutschland für Cybersecurity-Lösungen

Komponenten der Cybersecurity-Landschaft und ihre Aufgaben

Minimum	Firewall (FW)	REAKTIV	AUSSEN	INNEN	ZERO-TRUST ARCHITEKTUR DURCHGEHEND EMPFOHLEN	Schützt Ihre Systemen vor externen Netzwerkzugriffen
	IPS / IDS					Erkennt und schützt Ihr Netzwerk vor vordefinierten Attacken
	SIEM					Aggregiert Sicherheitsinformationen aus verschiedenen Quellen zur Echtzeitauswertung
	VM / EASM / CTEM	PRÄV.				Kontinuierliches Schwachstellenmanagement (XM Cyber)
	Verschlüsselung					Notwendig, um den nötigen Schutzbedarf von abgelegten und transferierten Daten zu ermöglichen
	Backup					Wiederherstellung von Daten & Systemen z.B. nach einem Ransomware-Vorfall
Erweitert	Anti-Virus	REAKTIV				Schutz von Endgeräten vor Schadsoftware
	IAM					Management von Benutzern und deren Berechtigungen (z.B. System- und Datenzugriffe)
	SOAR					Verwalten von Sicherheitsvorfällen
	OT / IoT Security					Schützt Ihre Produktionsanlagen und vernetzten Geräte
	NDR / EDR / XDR / MDR	PRÄVENTIV	AUSSEN			Erweiterter und aktiver Schutz von Endgeräten
	GRC / CCM					Management von Risiken und Compliance-Anforderungen
	WAF					Die Web Application Firewall (WAF) Schützt Ihre Webanwendungen vor Attacken
	CTI					Informationen über Bedrohungen und Bedrohungsakteure
	Cloud Security					Scannt und meldet Fehlkonfigurationen in Ihren Cloud-Instanzen

64 %

aller Sicherheits-Teams sagen aus, dass die vorhandenen Produkte nicht optimal interoperabel sind. **Dies führt zu Ineffizienz und potenziellen Sicherheitslücken.**

Handlungsempfehlungen für Käufer

1. Problem- und Bedarfsanalyse

- eigene Risiken, Bedarfe und Probleme verstehen
- Portfolioanalysen der bestehenden Systemlandschaft
- Möglichkeiten und Einschränkungen berücksichtigen

2. Ersten Überblick verschaffen

- Marktüberblick der Produkttypen
- Harmonisierung mit eigenen Assets
- Vertriebsstrategien hinterfragen

3. Vorauswahl treffen

- Vorauswahl einiger Lösungen
- gute Steuerung der Präqualifizierung

4. Vorabtests

- umfassende und gewissenhafte Prüfung der Vorauswahl durch kompetentes Personal
- Berücksichtigung von Zertifizierungen / Standards
- enge Kooperation mit Anbietern zwecks Bewertung der Wirksamkeit
- Gespräche mit Referenzkunden oder dem eigenen Netzwerk zu Erfahrungen im Umgang mit der Cybersecurity-Lösung führen

5. Finale Auswahl

- „Best of Breed"-Ansatz nicht allein aufgrund technischer Kriterien
- bedarfs-, nutzungs- und zielgruppenorientierte finale Auswahl
- auf Usability für Zielgruppe achten
- Anforderungskatalog für Anbieter erstellen
- Sicherheit der Lösungen als Vertragsbestandteil

Quellen: [5], [7], [15], [16], [28], [38], [91], [116], [118], [128], [140], [141], [205], [218], [239], [273], [309], [330], eigene Darstellung

4 PRODUKTCHAOS – HERAUSFORDERUNG DER CYBERSECURITY-LÖSUNGSLANDSCHAFT

4.1 DIE PRODUKTLANDSCHAFT DER CYBERSECURITY VON HEUTE

Neben organisatorischen Sicherheitsmaßnahmen basiert die Cybersecurity von Organisationen maßgeblich auf einer Vielzahl von Software- und Hardwarelösungen. Diese übernehmen zentrale Aufgaben wie die Prävention und Reaktion auf Cyberangriffe oder den Datenschutz. Regulatorische Anforderungen zwingen verschiedenste Branchen zur Implementierung spezifischer Technologien, wie Angriffserkennungssysteme, Datenverschlüsselung oder Schwachstellenmanagement, etwa im Rahmen des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG) [218]. Laut dem IT-Sicherheitsbeauftragen eines Energiekonzerns, „hilft NIS-2 dabei, dass selbst Administratoren den Vorstand von der Wichtigkeit der IT-Sicherheit überzeugen können und dann das Budget zur Umsetzung (...) zur Verfügung gestellt bekommen." Es scheint jedoch keinen Einfluss auf die Lösungsanbieter zu haben, denn „die Tools beinhalten das, von dem die Anbieter denken, dass sie es brauchen, um es verkaufen zu können."

Cybersecurity-Lösungen können vor allem dort unterstützen, wo menschliche Fähigkeiten an ihre Grenzen stoßen. Sie arbeiten in der Regel effizienter, konsistenter und sind in der Lage, weitaus größere Datenmengen in für Menschen nicht erreichbarer Geschwindigkeit zu verarbeiten, zu automatisieren und zu bewerten. Mitarbeitende können ihre Zeit für strategisch wichtigere Aufgaben einsetzen und ihre Produktivität steigern. In einigen Fällen können Produkte auch außerhalb der Cybersecurity eingesetzt werden (z. B. Big Data Analytics & Business Intelligence).

Entscheidungsträger stehen vor der Herausforderung, die „richtigen" Technologien zu identifizieren und im Rahmen der verfügbaren Budgets zu kombinieren, um eine wirkungsvolle Absicherung gegen Cyberbedrohungen zu gewährleisten. 80 Prozent der Entscheider berichten zudem davon, ihre Cybersecurityausgaben zu kürzen [141].

In den letzten 25 Jahren ist die Zahl der Cybersecurity-Anbieter mit der Digitalisierung und der dadurch wachsenden Angriffsfläche dynamisch gewachsen. Aktuellen Schätzungen zufolge gibt es weltweit mehr als 3.500 Anbieter, einschließlich Start-ups [15], [118]. Viele Produkte stellen hochspezialisierte Einzellösungen dar, die auch zum Einfallstor für Angreifern werden können (Software-Lieferkette) oder Konflikte mit anderen IT-/IT-Security Lösungen herbeiführen können [77], [83], [124], [158], [205], [254], [275]. Die von Fehlern des Falcon Sensors im Sommer 2024 betroffene Fluggesellschaft Delta Air Lines machte CrowdStrike für Ausfallschäden in Höhe von 500 Millionen US-Dollar verantwortlich [105]. Laut einer Umfrage geben 64 Prozent aller Sicherheitsteams an, dass ihre vorhandenen Produkte nicht reibungslos zusammenarbeiten, was sowohl zu Ineffizienz als auch zu potenziellen Sicherheitslücken führt [205].

In einigen Produktkategorien lassen sich weltweit 200 Anbieter identifizieren. Mehr und mehr Anbieter versuchen ein Themenfeld oder ganze Themenfelder durch integrierte „All-in-One" / „Suite" / Plattform-Lösungen abzudecken. Eine Lösung für alles gibt es bis heute nicht, auch wenn die Marketingabteilung und Paketierungsangebote mancher Hersteller das Gegenteil vermitteln wollen. Darüber hinaus gehört es zur Norm, Fähigkeiten oder Technologiepartnerschaften anzukündigen, die erst mit großem Zeitverzug in Produkte integriert werden. Grundsätzlich bergen „All-in-One"-Lösungen für Organisationen immer das Risiko eines Vendor-Lock-ins [128].

Organisationen setzen daher eine Vielzahl von Lösungen ein. Studien weisen eine Bandbreite von bis zu 83 eingesetzten Produkten von 29 Anbietern pro Unternehmen bis hin zu beeindruckenden 336 verschiedenen Produkten von 57 Anbietern auf [16], [118], [141], [309]. Die Ausgaben für Cybersecurity-Lösungen in Deutschland beliefen sich im Jahr 2024 auf 5,8 Milliarden Euro [28]. Weltweit wird der Markt für Cybersecurity bis 2029 auf ein Volumen von 247 bis 292 Milliarden USD anwachsen, mit jährlichen Wachstumsraten zwischen acht Prozent [273] und 17 Prozent [116], abhängig von der jeweiligen Region.

Kapitel 1 und die Schwarz Cybersecurity Reports aus den Jahren 2023 und 2024 machen deutlich, dass die Schäden durch Cyberangriffe weltweit steigen. Wie ist das möglich, wenn Organisationen neben Menschen und Prozessen, massiv in Cybersecurity-Lösungen investieren?

4.2 CYBERSECURITY-LÖSUNGEN: EIN ÜBERBLICK

Welche Lösungen für den Schutz der Organisation gewählt werden sollten, hängt maßgeblich von der Größe der Organisation, den regulatorischen Anforderungen, dem Risikoprofil und den verfügbaren Ressourcen ab. Eine grundlegende Sicherheitsausstattung muss Netzwerke, Daten und Endgeräte präventiv und reaktiv schützen.

Firewalls bieten als erste Verteidigungslinie gegen Cyberangriffe Schutz vor unautorisierten Zugriffen auf Netzwerke, indem sie den ein- und ausgehenden Datenverkehr überwachen, steuern und Bedrohungen blockieren. Früher eigenständige Lösungen, gehören **Intrusion Detection- und Intrusion Prevention-Systeme (IDS/IPS)** heute zu den essenziellen Bestandteilen moderner Firewalls und sorgen für einen umfassenderen Schutz. Während klassische Firewalls Datenpakete anhand statischer Regeln blockieren, ermöglichen IDS/IPS eine tiefgehende Prüfung der Inhalte sowie die Erkennung von Verhaltensmustern und Anomalien. IDS überwachen Netzwerke auf verdächtige Aktivitäten, protokollieren diese und lösen Warnmeldungen aus, während IPS-Angriffe in Echtzeit verhindern, beispielsweise durch die Sperrung verdächtiger Internet Protocol (IP)-Adressen, die als eindeutige Kennung für Geräte in Netzwerken dienen. Moderne Firewalls gibt es als virtuelle und physische Maschinen. Sie nutzen große Bedrohungsdatenbanken, machen tiefgehende Analysen des Datenverkehrs und setzen auf maschinelles Lernen.

Ergänzend dazu bieten **Web Application Firewalls (WAF)** gezielten Schutz für Organisationen, deren Online-Dienste besonderen Sicherheitsanforderungen unterliegen. WAFs überwachen den HTTP(S)-Datenverkehr – also die Kommunikation zwischen Endgeräten und Webseiten – und schützen sowohl Webanwendungen als auch Application Programming Interfaces (APIs), die die Kommunikation zwischen verschiedenen Programmen und Systemen ermöglichen, vor einer Vielzahl von Angriffen.

Zur Verbindung oder Trennung von Netzen unterschiedlicher Kritikalität oder Geheimhaltungsstufen, kommen neben Firewalls bei Industrieanlagen oder Militär und Geheimdiensten, unidirektionalen **Datendioden** oder bi-direktionalen **Security Gateways / High Assurance Guards** zum Einsatz.

Data Loss/Leakage Prevention (DLP)-Lösungen verhindern den unbefugten Zugriff auf sensible Daten sowie deren Weitergabe (z. B. per E-Mail oder Fileshare). DLP überwacht Daten am Speicherort, in Verwendung oder bei der Übertragung.

Security Information and Event Management (SIEM)-Systeme aggregieren und korrelieren Informationen aus verschiedensten Quellen wie Firewalls, Netzwerk, Applikationen (z. B. SAP) oder Endgeräten in Echtzeit. Dadurch sollen automatisiert komplexe Angriffe erkannt und ein ganzheitliches Lagebild erzeugt werden. Alarmmeldungen, Berichte oder Fallmanagement unterstützen die Sicherheitsverantwortlichen bei der Identifikation und Behebung von Sicherheitsvorfällen. Trotz des finanziellen und personellen Aufwands können SIEM-Systeme auch für kleinere Organisationen wertvoll sein. Unter den über 85 Anbietern weltweit, gibt es entsprechende Produkte für die unterschiedlichsten Organisationsgrößen.

Jeder PC sollte heute mindestens über **Anti-Virus-Programme** verfügen. Ein gut verwaltetes **Identity & Access Management (IAM)** regelt Zugriffsmöglichkeiten und Rechte aller Anwender und somit auch sensible Informationen. Ebenso wichtig sind **Backuplösungen und Wiederherstellungsprozesse**, die Datenverluste minimieren und die Geschäftskontinuität sichern. Fehlende Softwareupdates, -schwachstellen oder Fehlkonfigurationen erlauben Hackern erfolgreich ihr Werk zu vollenden. Patchmanagement Software und Schwachstellen-Scanner machen einen Abgleich zwischen Systemständen und bekannten Schwachstellen oder verfügbaren Softwareupdates zum Zweck der Prävention. **Continuous Threat Exposure Management (CTEM)**-Plattformen, erweitern diesen Ansatz und kombinieren ihn mit der kontinuierlichen Simulation von Angriffen auf alle internen und externen Systeme einer Organisation, Visualisierung von Angriffspfaden oder einer Priorisierung der Systemhärtungsmaßnahmen.

Lösungen wie **Network Detection and Response (NDR)**, **Endpoint Detection and Response (EDR)**, **Extended Detection and Response (XDR)** und **Managed Detection and Response (MDR)** überwachen Endgeräte und Server auf Bedrohungen und führen automatisiert entsprechende Gegenmaßnahmen aus. Sie stellen die nächste Stufe von Anti Virus-Software da und es ist eine zunehmende Konvergenz mit SIEM zu beobachten, da immer mehr Daten von verschiedenen Quellen integriert und analysiert werden. Im Unterschied zu anderen Detektionssystemen wie IDS/IPS sollen sie auch komplexere Angriffe, etwa Advanced Persistent Threats (APTs) oder Zero-Days, erkennen. Auch Bedrohungen durch Innentäter, die aus den eigenen Reihen einer Organisation stammen, können identifiziert werden. Organisationen können aus über 110 Anbietern wählen.

Das volle Potenzial von Cybersecurity-Lösungen, die Daten aus verschiedenen Quellen aggregieren, entfaltet sich durch den Einsatz oder die Integration einer **Security Orchestration Automation and Response (SOAR)**-Plattform. Diese automatisiert Routineaufgaben, etwa das Isolieren von Benutzerkonten oder das Sperren von Passwörtern bei verdächtigen Login-Versuchen, und erhöht so die Effizienz und Geschwindigkeit der Reaktion auf Sicherheitsvorfälle.

GRC (Governance, Risiko Management und Compliance)- und **CCM (Continuous Controls Monitoring)-Lösungen** unterstützen Organisationen dabei, Richtlinien, Prozesse, Risiken und regulatorische Anforderungen (z. B. PCI-DSS, ISO 27001, BSI-IT-Grundschutz, NIST) zu verwalten sowie deren Einhaltung kontinuierlich zu überwachen. In der Vergangenheit erforderten derartige Lösungen sehr viel manuelle Eingaben und kontinuierliche Bearbeitung, um sie im Einklang mit den Veränderungen von IT-Umgebung und -Organisation zu halten. Heute können viele Sicherheitsanforderungen für IT-Systeme automatisch durch entsprechende Datenquellen überwacht werden.

Zusätzlich wirken **Cyber Threat Intelligence (CTI)**-Plattformen präventiv, indem sie Daten zu Cyberbedrohungen aus diversen Quellen sammeln, analysieren und korrelieren. Diese Informationen werden gezielt an Teams oder andere Sicherheitslösungen, wie beispielsweise SIEM-Systeme, weitergeleitet, um frühzeitige Warnungen und effektivere Abwehrmaßnahmen zu ermöglichen.

4.3 CYBERSECURITY-MARKT UND MARKTVERSAGEN

Einige Cybersecurity-Produkte wie Firewalls oder Anti-Virus-Lösungen sind seit Jahrzehnten etabliert und werden kontinuierlich weiterentwickelt. Andere Lösungen wie SIEM, SOAR, CTEM oder OT-Security entstanden erst in den letzten 15 Jahren. Im Bereich von Cloudsecurity gibt es Anbieter, die in weniger als zwei Jahren über 100 Millionen Euro an jährlichem Umsatzvolumen (Annual Recurring Revenue (ARR)) erreichten.

Die Expansion des Marktes für Cybersecurity-Produkte spiegelt die zunehmende Notwendigkeit wider, der wandelnden Bedrohungslage in einer digitalen Welt in den Bereichen Prävention, Detektion und Reaktion entgegenzutreten. Jede neue Technologie, Arbeitspraxis oder Partnerschaft wie auch jedes neue Geschäftsmodell bringt potenzielle Angriffsvektoren für Angreifer oder Geschäftsmöglichkeiten für Cybersecurity-Abieter mit sich.

Heute erfüllt kein Cybersecurity-Produkt die Kundenanforderungen an Automatisierung, Preisgestaltung, Serviceleistungen oder Integration in das gesamte Lösungsportfolio einer Organisation [3]. Die Bewertung von Cybersecurity-Produkten wird häufig als frustrierend empfunden: „Es ist ein Labyrinth. Wenn man sich heute auf dem Cybersecurity-Markt umschaut, kann man sich für eine lange Zeit verirren. Jeder hat eine Lösung für ein Problem, das wir noch gar nicht identifiziert und bewertet haben.“, so ein CISO aus dem Energiesektor, welcher im Rahmen des Artikels interviewt wurde. Zudem können Entscheidungen unter hohem Zeitdruck erfolgen—gerade nach Vorfällen.

Auf dem Cybersecurity-Markt gibt es regen Wettbewerb in sämtlichen Produktkategorien. Die Größe des Marktes und neue Bedrohungsszenarien führen kontinuierlich zum Eintritt weiterer Anbieter. So wurden im Jahr 2024 über 14 Milliarden Euro in Cybersecurity-Firmen inves-

tiert. Entwickler von Cloud Security (Cloud Native Application Protection (CNAPP))-Lösungen lagen dabei auf dem ersten Rang. Cybersecurity-Lösungen müssen KI als integralen Bestandteil integrieren, um selbst agiler zu werden und Innovationskraft zu signalisieren [7]. Parallel dazu findet eine Konsolidierung durch die führenden Anbieter statt, die eine Plattformstrategie verfolgen und ihr Portfolio durch Zukäufe von „Features" erweitern müssen. Die nahtlose Integration neuer Technologien und ihrer Teams stellt auch für die großen Anbieter eine Herausforderung dar [219]. Der Wert der M&A-Transaktionen überstieg 40 Mrd. Euro [239]. Die Verkaufszyklen variieren zwischen Produktkategorien und Branchen. Vom Erstkontakt bis zum Abschluss können bis zu drei Jahre vergehen.

Eine Studie aus dem Jahr 2020 argumentiert, dass der Cybersecurity-Markt dysfunktional im Sinne der „Lemons"-Theorie des Nobelpreisträgers George A. Akerlof sei [5], [140]. Ein im Rahmen des Artikels interviewter IT-Leiter eines deutschen Maschinenbauers merkt analog an: „95 Prozent des Marktes sind Bullshit. Eine der größten Herausforderungen für uns ist es, die Spreu vom Weizen zu trennen."

Produkte innerhalb einer Kategorie unterscheiden sich in Qualität, Sicherheitsarchitektur, Souveränitäts- oder Datenschutzanforderungen. Zudem konkurrieren sie mit Lösungen anderer Produktkategorien aufgrund von Funktionsüberlappungen. Produktqualität wird durch unterschiedlichste Maßnahmen durch die Anbieter signalisiert: Marketing, Informationsmärkte (z. B. Gartner, IDC), Reputation (Referenzkunden, Fachexpertise des Personals), Standards und Siegel (z. B. Security Made in Germany, NIST, BSI Grundschutz), Zertifizierungen (z. B. CC EAL4+, ISO 27001), Zulassungen (z. B. VS-NfD, GEHEIM), Garantieerklärungen (z. B. Kombination Produkt mit Cyberversicherung) oder kostenlose Probezeiträume (z. B.: Try & Buy-Angebote). Dennoch können Kunden nur unter großem Aufwand, Expertise und nach einer gewissen Zeit, Qualitätsunterschiede, Nutzen oder Alternativen identifizieren. Viele Organisationen investieren mehr in Cybersecurity-Produkte, als tatsächlich erforderlich wäre, nutzen jedoch deren volles Potenzial nicht aus [118]. Funktionen oder die Lösungen bleiben oft minimal oder ungenutzt, was die Effektivität der gesamten Cybersecurity-Strategie erheblich einschränkt [177].

Preise von Cybersecurity-Produkten geben wenig Rückschlüsse über ihren Nutzen und werden meist frei durch die Anbieter gesetzt. Sie berücksichtigen dabei eine Vielzahl an Faktoren (Preisgefüge innerhalb der Produktkategorie, Zielkunden, Zielmärkte) sowie generelle Rabatte und Margen für die Vertriebskanäle in der Preisfestsetzung. Distributoren und Wiederverkäufer, wie z. B. Systemintegratoren oder MSSP, können, je nachdem ob sie nur einen Kauf abwickeln oder signifikantes Neugeschäft generieren, gemeinsam bis zu 40 Prozent Rabatt auf den Listenpreis erhalten. Die Preise variieren stark zwischen den Lösungen. Häufig werden Basisversionen von Software kostenlos („Freemium Ansatz") oder zu attraktiven Einstiegspreisen angeboten, die jedoch die tatsächlichen Anforderungen der Kunden oft nicht abdecken. Nach der Anschaffung sind dann Ergänzungen („Add-ons") erforderlich, um die Funktionalität zu erweitern.

So sind Anti-Virus oder EDR-Lösungen von ein bis 30 Euro pro Endgerät beziehungsweise Asset [140] vergleichsweise erschwinglich, insbesondere bei Großunternehmen, die von Mengenrabatten profitieren. Auch Firewalls gibt es bereits ab 100 Euro, sie können jedoch auch über eine Million Euro kosten. SIEM-Systeme gibt es auch als kostenlose Open-Source Version. Dagegen können die jährlichen Kosten für etablierte SIEM-Lösungen für mittelgroße Organisationen fünf bis sechsstellige Beträge pro Jahr aufwenden – einschließlich Implementierung, Wartung und Schulungen [38]. Anbieter gemanagter Cybersecurity-Services (MSSP) verlangen typischerweise Paketpreise, die sich an der Anzahl der Systeme und inkludierten Dienstleistungen sowie dem Service-Level (z. B. 24x7, Reaktionszeit) orientieren [289]. Hier wird meist mit Preisen unterhalb von zehn Euro je Endgerät gerechnet.

Auch wenn der Markt von Informationsasymmetrien geprägt ist, gibt es keine Anzeichen von Marktversagen bei dem das Risiko der Nachfrager, eine qualitativ geringere Lösung zu wählen, das Angebot von qualitativ hochwertigeren Lösungen verringert.

4.4 WICHTIGE SCHRITTE VOR DEM ERWERB VON CYBERSECURITY-LÖSUNGEN

Um eine fundierte Kaufentscheidung zu treffen, müssen Entscheider eine Vielzahl von Fragen beantworten:

- Welche Risiken bestehen für die eigene Organisation und wie sind sie zu priorisieren?
- Wie ist meine externe und interne IT- und Cybersecurity-Situation?
- Welche Lösungen sind verfügbar, und welche tatsächlich notwendig?
- Woran wird der Erfolg des Produkts bemessen?
- Wie kann der interne Betrieb oder die externe Steuerung und der maximale Nutzen sichergestellt werden?
- Ist es zwingend notwendig, die Lösung intern zu betreiben?
- Welche Mindestanforderungen müssen erfüllt werden?
- Sind die Produkte skalierbar? Haben Sie die Fähigkeit, sich dem Wachstum einer Organisation anzupassen?
- Welche Preis- und Lizenzmodelltrends gibt es für die avisierte Produktkategorie?
- Sind die Folgekosten erfasst?
- Welche Betreibermodelle gibt es für die Produktkategorie?
- Ist die Expertise für die Bewertung der Lösung während des Beschaffungsprozesses inklusive Proof of Concept/Value (POV/C) in der Organisation vorhanden oder sollte sie extern eingekauft werden?
- Welche Erfahrungen haben vergleichbare Organisationen mit Anbietern gemacht?
- Welche Anforderungen haben die Arbeitnehmervertreter?
- Wie lassen sich die geplanten Investitionen mit dem Budget in Einklang bringen?
- Ist es sinnvoller, auf einen einzigen Anbieter oder verschiedene „Best-of-Breed"-Lösungen zu setzen?

Jede dieser Fragen bringt zusätzliche Herausforderungen mit sich. Eine der größten besteht darin, geeignete Entscheidungskriterien zu definieren. Ohne detaillierte Risiko- und Schutzbedarfsanalysen sollten Organisationen keine Entscheidung über eine technische Lösung treffen. Auch die Frage, ob das erforderliche Wissen und die Kapazitäten für Betrieb und Integration in die bestehende IT- Landschaft und den IT-Sicherheitsansatz vorhanden sind, muss immer beantwortet sein. Gibt es hier Defizite, besteht die Gefahr, dass sich Organisationen in falscher Sicherheit wiegen [160]. Nicht umsonst sagt man: „A Fool with a Tool is just a Fool", denn das Ziel ist nicht das Produkt, sondern die Problemlösung und Verbesserung der Cybersecurity.

Dieses strukturierte Vorgehen wird jedoch häufig zu Gunsten einer schnellen Entscheidung vernachlässigt.

In einigen Fällen kann es vorkommen, dass das Budget nicht ausreicht oder keine kommerziell verfügbaren Lösungen existieren, um die spezifischen Risiken und Bedrohungen einer Organisation zu adressieren und angemessen zu mindern. In solchen Situationen ist es entscheidend, alternative Ansätze zur Sicherstellung der Cybersecurity zu verfolgen und die Kontrolle zu behalten:

- Kombination verschiedener, etablierter Lösungen
- Kontinuierliche Systemhärtung und -prüfung auf alle Typen von Schwachstellen

4.5 DIE ANBIETERPERSPEKTIVE

Abseits offensichtlicher Marketingmethoden bedienen sich Anbieter häufiger Strategien, die auf psychologische Mechanismen und Emotionen abzielen:

Die FUD-Strategie (Fear, Uncertainty, Doubt) zählt zu den ältesten und etabliertesten Ansätzen im Marketing. Bereits vor Jahrzehnten wurde sie im IT-Bereich kritisch beleuchtet und teilweise für die Monopolstellung einiger großer Technologiekonzerne mitverantwortlich gemacht [227]. Während diese Methode früher dazu diente, Misstrauen gegenüber Wettbewerbern zu schüren, wird sie im heutigen Cybersecurity-Markt vor allem genutzt, um die Dringlichkeit des Kaufs von Produkten über Angst zu betonen. Dazu zählt etwa die Nennung von Statistiken zur Anzahl an Malware, Angriffen, Schwachstellen oder den finanziellen Folgen von Cyberangriffen. Studien belegen, dass Angst und Stress die rationale Urteils- und Entscheidungsfähigkeit beeinträchtigen und Alternativen oft nicht ausreichend bedacht werden [70], [154], [270]. Das menschliche Bestreben, unangenehme Gefühle und drohende Verluste zu vermeiden, wird gezielt ausgenutzt [102]. Dieser Ansatz wird unter IT-Sicherheitsexperten zunehmend offen und kritisch diskutiert.

Mit der FUD-Strategie verbundene Ansätze setzen häufig auf eine Dringlichkeit. Diese Strategie nutzt aus, dass potenzielle Kunden unter Zeitdruck weniger rationale Vergleiche anstellen und schnellere Entscheidungen treffen. Der Stress wird durch die komplexe Materie und eine Überflutung an Informationen oft noch verstärkt [229].

Im harten Wettbewerb reicht es nicht, die eigenen Produkte zu bewerben. Anbieter schüren gezielt Zweifel an Konkurrenzprodukten. Dieser Ansatz wurde beispielsweise von Microsoft in der langjährigen Kampagne gegen Linux eingesetzt, um Unsicherheiten hinsichtlich der Qualität anderer Anbieter zu erzeugen [122], [308]. Eine weitere verbreitete Methode ist das Verfassen gefälschter Bewertungen (Fake Reviews). Schätzungen zufolge sind bis zu 43 Prozent aller Bewertungen auf großen Plattformen manipuliert, sowohl positiv als auch negativ [330].

Ein weiteres Mittel ist die Darstellung eines Produkts als umfassende Lösung („All-in-One"). Dabei wird das psychologische Prinzip des geringsten Aufwands ausgenutzt: Angesichts der Komplexität neigen Menschen dazu, einfache Lösungen zu bevorzugen [33].

4.6 HERAUSFORDERUNGEN VENDOR-LOCK-INS

Anbietergebundene, maßgeschneiderte Lösungen und proprietäre Formate können zwar innerhalb einer Unternehmenslandschaft effizient funktionieren, schränken jedoch die Flexibilität und Innovationsfähigkeit bei der Auswahl anderer Lösungen erheblich ein. Ein Wechsel des Anbieters erfordert oft eine kostspielige und komplexe Migration der bestehenden Systeme in neue Lösungen.

Die bereits beschriebenen Inkompatibilitäten bei der Implementierung anderer Produkte erschweren zusätzlich den Arbeitsalltag in diversifizierten Systemen. In der Praxis führt dies häufig dazu, dass Organisationen gezwungen sind, auf weitere Produkte und Dienstleistungen desselben Anbieters zurückzugreifen. Diese Abhängigkeit verschärft wiederum operative Herausforderungen. So werden (hohe) Preissteigerungen seitens der Anbieter wahrscheinlicher, insbesondere wenn diese davon ausgehen können, dass ihren Kunden keine echten Alternativen zur Verfügung stehen.

Darüber hinaus kann es vorkommen, dass Anbieter ihre Produkte nicht konsequent weiterentwickeln, um neue Technologien zu unterstützen oder steigenden Anforderungen gerecht zu werden. Dies hemmt nicht nur Innovationspotenziale, sondern kann auch dazu führen, dass sich neue Angriffsvektoren ergeben. In solchen Fällen fühlen sich vor allem kleinere Unternehmen den großen Anbietern auf dem Cybersecurity-Markt ausgeliefert. Ein Informationssicherheitsbeauftragter (ISB) eines kommunalen Energieversorgers beschreibt dies so: „Das Problem ist, wir können nicht viel ausrichten. Wir können auf Schwachstellen hinweisen, das interessiert die Lieferanten aber nicht."

4.7 HANDLUNGSEMPFEHLUNGEN FÜR ANBIETER

Bei der Entwicklung von Cybersecurity-Lösungen sollten Anbieter eine Reihe zentraler Aspekte berücksichtigen, um die Qualität ihrer Produkte zu steigern und die Kundenzufriedenheit erhöhen.

- Entwickler sollten **Security-by-Design** und **Security-by-Default** als grundlegende Prinzipien in den gesamten Entwicklungsprozess integrieren. Diese Ansätze gewährleisten, dass Sicherheitsmechanismen von Anfang an berücksichtigt werden und standardmäßig aktiviert sind, was künftig als Qualitätsmerkmal auf dem Markt entscheidend sein wird [7], [91].

- Der **Shift-Left-Security-Ansatz** sollte konsequent umgesetzt werden, indem Sicherheitsüberprüfungen und -maßnahmen so früh wie möglich in die Entwicklungsphase einfließen. Dies erfordert klare Definitionen von Sicherheitsanforderungen, regelmäßige Schulungen der Entwicklungsteams sowie die Bereitstellung zusätzlicher personeller Ressourcen, etwa durch spezialisierte Software-Architekten oder Sicherheitsverantwortliche innerhalb der Teams.

- Anbieter sollten ihre Lösungen oder Organisation von **unabhängigen Stellen zertifizieren lassen**, um die tatsächliche Wirksamkeit ihrer Lösungen für Kunden nachvollziehbar zu machen.

- Die Benutzerfreundlichkeit sollte sich durch ein durchdachtes **UX/UI-Design**, intuitive Benutzeroberflächen sowie konsistente Terminologien und Symbole im Sinne der täglichen Arbeit von IT-Sicherheitsmitarbeitern auszeichnen. Die enge Zusammenarbeit mit Kunden ist entscheidend, z. B. Advisory Boards.

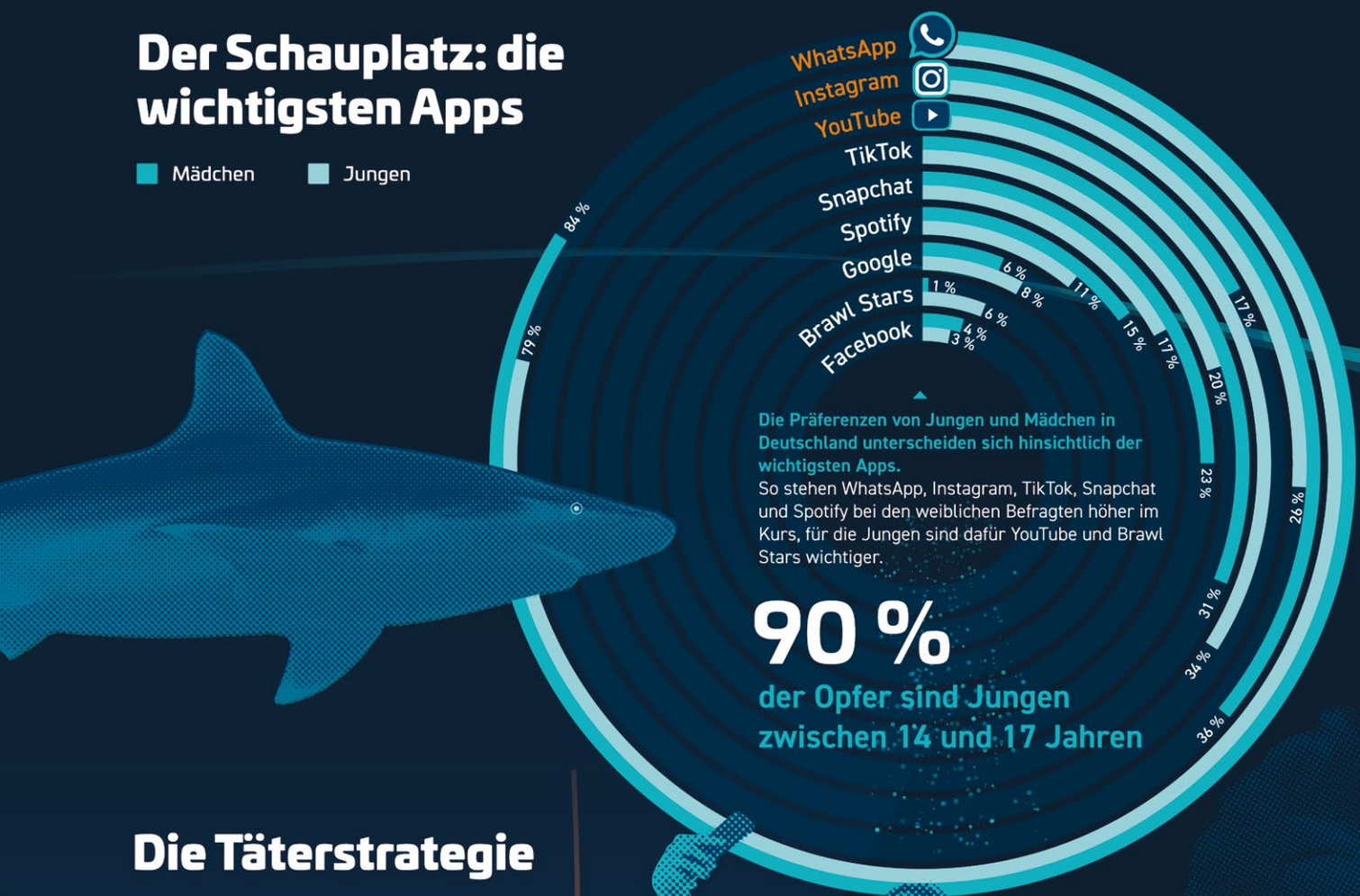
- Produkte müssen sich in bestehende IT-Security Lösungsportfolios nahtlos integrieren und eine hohe Kompatibilität mit den Produkten anderer Anbieter aufweisen. Dazu gehören auch standardisierte Formate wie das **Common Event Format (CEF)** oder das **Log Event Extended Format (LEEF)**, welches gerade in der **OT-Security** wichtig ist.

Abschließend lässt sich festhalten, dass die Verbesserung der Cybersecurity-Lösungslandschaft nur durch eine enge und transparente Zusammenarbeit aller Beteiligten erreicht werden kann. Nur durch diese kollektive Anstrengung wird es möglich sein, eine resilientere und sichere digitale Zukunft zu gestalten.

KAPITEL 5

VERTRAUENSMISSBRAUCH
DIE UNTERSCHÄTZTE GEFAHR VON SEXTORTION

Der Schauplatz: die wichtigsten Apps

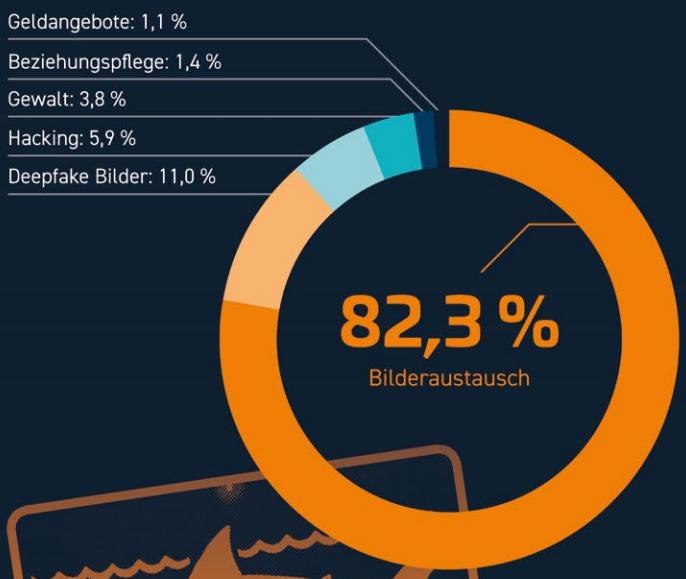


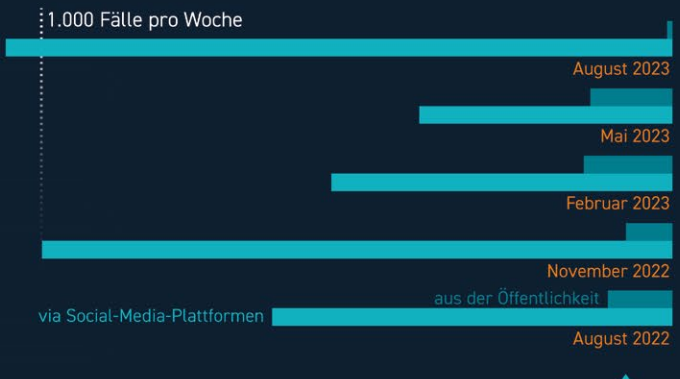
Die Präferenzen von Jungen und Mädchen in Deutschland unterscheiden sich hinsichtlich der wichtigsten Apps.
So stehen WhatsApp, Instagram, TikTok, Snapchat und Spotify bei den weiblichen Befragten höher im Kurs, für die Jungen sind dafür YouTube und Brawl Stars wichtiger.

90 %
der Opfer sind Jungen zwischen 14 und 17 Jahren

Die Täterstrategie

Wie Täter an die intimen Inhalte gelangen





Dem National Center for Missing & Eploited Children (NCMEC) sind von 08/2022 bis 08/2023 im Durchschnitt 812 Sextortionfälle pro Woche gemeldet worden.

Weltweit hat sich die Gesamtzahl im Jahr 2023 mit 26.718 Fällen im Vergleich zu 10.731 Fällen im Vorjahr mehr als verdoppelt.

27 %

der Opfer, die eine Zahlung tätigten, erhielten weitere Forderungen.

Prävention

Warnsignale erkennen

Aufklärung & Awareness

Offene Gespräche

Technologische Schutzmaßnahmen

Schadensbegrenzung

Wenn Betroffene dennoch Opfer von Sextortion werden, sind bestimmte Schritte entscheidend ▾

Quellen: [23], [43], [59], [78], [68], [130], [176], [190], [295], [231], [243], [294], [295], [296], [306], [318], [324], eigene Darstellung

5 VERTRAUENSMISSBRAUCH – DIE UNTERSCHÄTZTE GEFAHR VON SEXTORTION

Es gibt Momente, die dein Leben in ein Vorher und Nachher teilen – und manchmal passieren sie so leise, dass du es erst merkst, wenn es zu spät ist.

TAG 1 – DIE NACHRICHT, DIE ALLES VERÄNDERT

Es war ein gewöhnlicher Dienstagabend im Herbst. Es war dunkel und der Regen klopfte an mein Fenster. Ich saß an meinem Schreibtisch, mein Heft vor mir, und starrte auf die Matheaufgaben für Zehntklässler, die ich längst hätte lösen sollen. Mein Handy vibrierte. Es war nicht ungewöhnlich – ich bekam ständig Nachrichten während, ich andere Dinge tat. Aber diese Nachricht war anders.

Hi 🙂. Ist das Profil von Max?
Ich glaub, ich kenn dich von irgendwo.

Ich starrte auf den Text. Wer war das? Es war eine dieser Nachrichten, die sofort neugierig machten – und die man schwer ignorieren konnte.

Ja, das bin ich. Wer bist du?

Die Antwort kam, bevor ich mich wieder auf meine Matheaufgabe konzentrieren konnte.

Ich bin Lena. Sorry, falls ich störe!
Ich hab dein Bild in einer Gruppe gesehen. Du siehst echt nett aus.

Nett – dieses Wort hatte schon lange niemand mehr benutzt, um mich zu beschreiben. Obwohl, war nett nicht die Schwester von sch...? Mein Herz klopfte ein bisschen schneller.

Danke … ähm, in welcher Gruppe war das?

Oh, ich weiß nicht mehr. Egal.
Du hast einfach etwas Besonderes. 😊

Sie hatte ein Profilbild, das mich neugierig machte. Es zeigte ein hübsches Mädchen, dessen Augen mich direkt durch den Bildschirm anzusehen schienen. Ich wusste, dass ich vorsichtig sein sollte. Aber sie wirkte echt. Nicht wie diese offensichtlichen Bots und KI-generierten Mädchen, die mit einer wirren Mischung aus Emojis und absurden Angeboten die Nachrichten überfluteten.

Ach so, okay. Danke, glaub ich. 😅

Haha, du bist süß, wenn du nervös bist.

TAG 2 – DIE ROUTINE DER NACHRICHTEN

Lena wurde schnell ein fester Bestandteil meines Tages. Jede freie Minute checkte ich mein Handy, gespannt, ob sie geschrieben hatte. Unsere Chats wurden länger, persönlicher. Sie erzählte mir, dass sie in der Nähe wohnte, aber erst vor Kurzem hergezogen sei und niemanden kenne. Sie schickte Bilder – nichts Auffälliges, aber genug, um zu zeigen, dass sie da war, dass sie echt war.

Und ich? Ich fing an, mich auf ihre Nachrichten zu freuen. Es war, als hätte ich eine Freundin gefunden, jemanden, der mich verstand, der sich wirklich für mich interessierte.

Es war ein seltsames Gefühl. Lena schrieb fast jeden Tag. Immer freundlich, immer neugierig. Sie fragte nach meinen Hobbys, nach meiner Schule, nach dem, was ich gern in meiner Freizeit tat. Sie wusste, wann sie interessiert klingen musste und wann sie ein Kompliment einstreuen sollte.

„Du bist bestimmt mega gut im Zeichnen“, schrieb sie eines Abends, nachdem ich ihr erzählt hatte, dass ich manchmal Skizzen mache. Es fühlte sich gut an, so etwas zu lesen. Ein bisschen wie Bestätigung von jemandem, der mich verstehen wollte.

Lena: **„Schickst du mir mal eins deiner Bilder? Ich wette, du bist ein kleiner Künstler!“**

Ich: **„Ähm, die sind echt nicht so besonders …“**

Lena: **„Ach komm schon. Vertrau mir. Ich würde das niemals jemandem zeigen, wenn du nicht willst.“**

Also schickte ich eines. Ein kleines, unscheinbares Bild, das ich vor Monaten gezeichnet hatte. Lena lobte es überschwänglich. Sie schrieb, wie talentiert ich sei, wie sie mich beneiden würde. Und obwohl ich wusste, dass es übertrieben war, fühlte ich mich gut. Am Abend, während ich mit ihr schrieb, kam meine Mutter ins Zimmer.

„Max, bist du fertig mit den Hausaufgaben?“ Sie blieb in der Tür stehen, die Arme verschränkt.

„Fast“, murmelte ich, ohne vom Handy aufzusehen.

„Mit wem schreibst du denn die ganze Zeit?“, fragte sie neugierig. „Nur mit einem Freund“, log ich.

Ich fühlte, wie mein Gesicht heiß wurde. Es war das erste Mal, dass ich Lena verschwieg, und ich verstand nicht, warum.

TAG 4 – DIE ERSTE GRENZÜBERSCHREITUNG

Unsere Chats wurden schnell vertraut. Lena war immer freundlich und interessiert und begann, persönlicher zu werden. Ihre Fragen waren so geschickt gestellt, dass ich kaum bemerkte, wie viel ich von mir preisgab. Und doch schaffte sie es, dass ich mich sicher fühlte. Der Bruch kam schleichend. Vielleicht hätte ich ihn früher erkennen müssen. Aber in dem Moment, als Lena zum ersten Mal eine persönliche Frage stellte, die sich anders anfühlte, ignorierte ich das Gefühl in meinem Bauch.

Eines Abends fragte sie:

Lena: **„Max, ich hab ein Bild gemacht. Willst du’s sehen? 😉“**

Ich: **„Ähm, klar!“**

Das Bild, das sie schickte, war harmlos. Sie trug ein T-Shirt, saß auf ihrem Bett, ein schüchterner Blick in ihren Augen. Aber etwas daran fühlte sich anders an – als würde sie auf etwas warten.

Ich spürte, wie mein Magen sich zusammenzog.

Lena: **„Findest du mich hübsch?“**

Ich: **„OMG, total.“**

Lena: **„Jetzt du. Zeig mir, wie du gerade aussiehst. 😊“**

Ich zögerte. „Warum eigentlich nicht?“ dachte ich. Ein harmloses Bild konnte doch nicht schaden. Also machte ich ein Selfie und schickte es. Vielleicht würden wir uns bald sehen? Lena antwortete sofort.

Lena: **„Wow, du siehst so gut aus. Echt, ich glaube, ich hab noch nie jemanden wie dich kennengelernt.“**

Ich spürte, wie ich rot wurde, und mein Herz klopfte ein bisschen schneller. War ich verliebt? Ihr Lob fühlte sich an wie eine warme Decke an einem kalten Tag.

TAG 7 – DER ERSTE FEHLER

Die Nachrichten von Lena waren wie ein Sog. Jedes Mal wollte sie mehr – und ich auch. Sie bekam es von mir. Aus einem Bild wurden zwei, dann drei. Sie war immer so nett, so bewundernd, dass ich nicht bemerkte, wie tief ich schon drinsteckte. Eines Abends, als ich eigentlich schlafen sollte, schrieb sie wieder.

Lena: **„Ich hab noch ein Bild, aber es ist ein bisschen … naja, mutig. Willst du’s sehen?“**

Ich: **„ … “**

Das Bild war anders als die bisherigen. Es war ein Bild, das mich nervös machte und gleichzeitig erregte. Anders als die Bilder von Mädels aus einer Anzeigenkampagne für eine bekannte Unterwäschemarke, die mir Freunde neulich auf dem Schulhof gezeigt hatten. Sie sahen sexy aus, aber sie bedeuteten mir nichts. Lena dagegen schon. Ich spürte, wie mein Körper heiß wurde und mein Herz raste.

Lena: **„Jetzt du. Sei mutig.**
Du vertraust mir doch, oder?“

Ich fühlte kurz einen Stich in meiner Brust, ein leises Flüstern, das mir sagte, dass etwas nicht stimmte. Aber ich ignorierte es. Ich wollte sie nicht enttäuschen und ich wollte irgendwie auch mehr von ihr.

TAG 10 – DIE DROHUNG

Die Nachricht kam nachmittags, als ich an einem normalen Tag von der Schule nach Hause kam. Lena und ich schrieben uns mittlerweile über eine Woche lang und hatten immer wieder intimste Bilder, Videos und Wünsche ausgetauscht.

Lena: **„Ich hab alles gespeichert, Max. Die Bilder, die Videos. Wenn du mir nicht 300 Euro zahlst, schicke ich es an alle. Deine Freunde. Deine Eltern.“**

Mir wurde übel. Ich fühlte, wie mein Herz in meiner Brust raste, während meine Hände kalt wurden. Ich hatte keine Worte. Meine Hände zitterten, während ich zurückschrieb.

Ich: **„Bitte, mach das nicht. Ich hab das Geld nicht!“**

Lena: **„Dann besorg es. Du hast 24 Stunden.**
Sonst ruiniere ich Dein Leben.“

TAG 11 – DIE ZAHLUNG

Ich konnte nicht schlafen, nicht denken. Jede Nachricht, die ich erhielt, ließ mein Herz schneller schlagen. Die Drohungen wurden härter, die Forderungen drängender. Schließlich gab ich nach.

Ich nahm mein Handy und überwies mein gesamtes Geld per App. Geburtstagsgeschenke, Weihnachtsgeld, Zeitung austragen – alles weg.

Lena: **„Gut. Zahlung erhalten.**
Du bist ein braver Junge.“

Ich starrte auf den Bildschirm, spürte, wie Erleichterung durch mich strömte. Es war vorbei!

Doch am nächsten Tag kam die nächste Nachricht.

Lena: **„Ich brauche mehr. 500 Euro.**
Danach ist Schluss. Versprochen.“

Ich war fassungslos. Panik stieg in mir auf. Ich wusste nicht, wie ich da wieder rauskommen sollte.

TAG 12 – DER ZUSAMMENBRUCH

Ich saß in meinem Zimmer, die Tür abgeschlossen, mein Handy in der Hand. An Konzentration in der Schule war nicht zu denken. Schlafen war kaum möglich. Ich hatte ständig Kopfschmerzen. Meine Fingernägel hatte ich mir abgekaut. Es war, als ob ich neben mir stand ohne jegliche Kontrolle über mein Leben. Jede neue Nachricht war ein Schlag in meinen Magen. Ich hatte nichts mehr zu geben. Mein Geld war weg, meine Hoffnung auch.

Meine Eltern merkten, dass etwas nicht stimmte. „Max, was ist los mit dir? Du bist so still in letzter Zeit", sagte mein Vater beim Abendessen. „Nichts", murmelte ich und stocherte in meinem Essen.

Meine Mutter legte eine Hand auf meinen Arm. „Du weißt, dass du mit uns reden kannst, oder?"

Meine innere Stimme glich meinem Ich aus Kindergartenzeiten und schrie: „Helft mir, Mama und Papa!" Aber sie hörten mich nicht. Ich schämte mich unendlich. Für meine Dummheit. Für die Bilder meines nackten Körpers. Für die Videos von meinem Körper und die geheimen Wünschen in den Chats zwischen Lena und mir.

In dieser Nacht saß ich alleine auf meinem Bett und starrte in die Dunkelheit.

Alles raste, mein Atem stockte und die innere Leere übermannte mich.

Ich wollte und konnte nicht mehr auf dieser Welt sein.

Es gab nur einen Ausweg aus diesem Horrorfilm.

Morgen würde ich dem ein Ende bereiten.

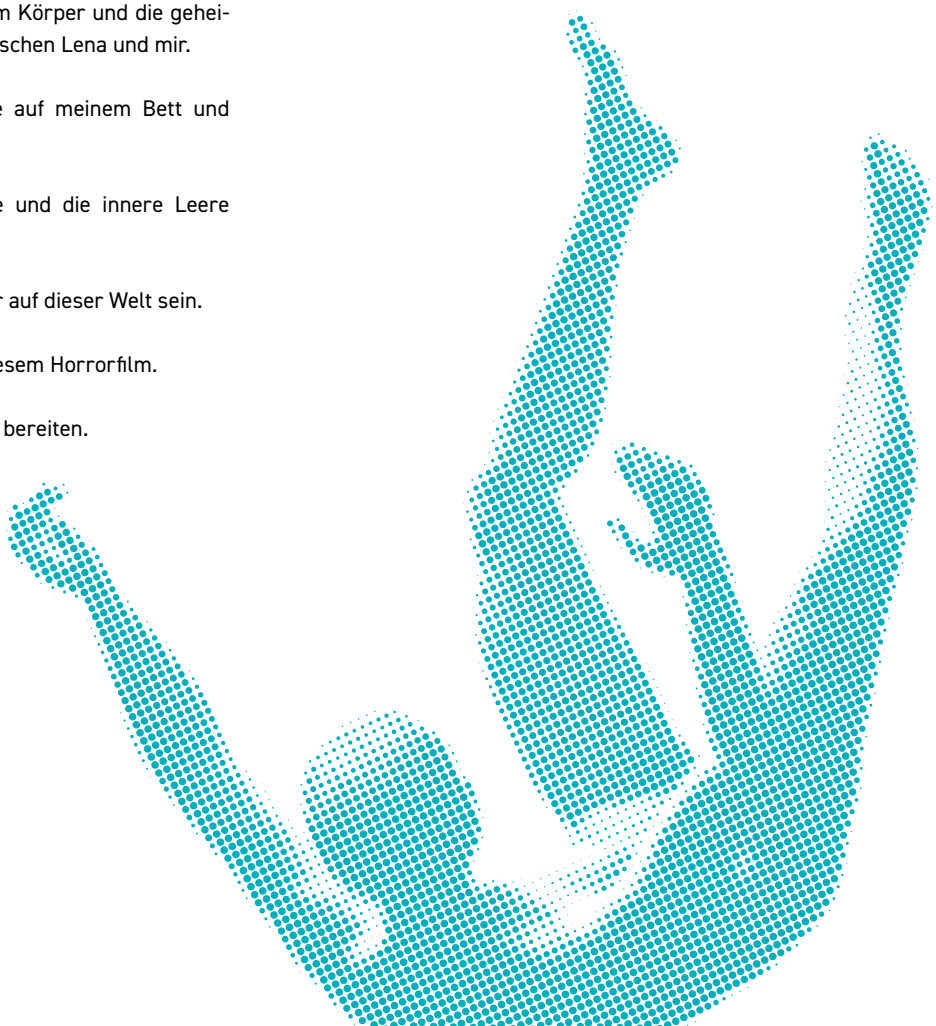
Dann schlief ich erschöpft ein.

EPILOG

Max hatte Glück. Anstatt sich sein Leben zu nehmen, suchte er doch am nächsten Tag ein Gespräch mit seinen Eltern und konnte seinen Albtraum beenden. Seine Geschichte zeigt eindrücklich, wie gefährlich Sextortion sein kann und wie schwer es für Betroffene ist, sich aus dem Netz der Täter zu befreien. Doch nicht alle Opfer finden einen Ausweg. Viele erleiden langfristige psychische und finanzielle Schäden, oft mit tragischen Konsequenzen.

Dem 17-jährigen Jordan DeMay aus dem U.S. Bundesstaat Michigan kann dagegen niemand mehr helfen. Er nahm sich im März 2022 in weniger als sechs Stunden nach der ersten Kontaktaufnahme durch die Täter sein Leben.

Sextortion ist längst nicht mehr ein Einzelfall, sondern ein weltweites Phänomen, das immer mehr Menschen betrifft – besonders Jugendliche. Um diese Bedrohung umfassend zu verstehen, lohnt es sich, einen genauen Blick auf ihre Mechanismen, Auswirkungen und Hintergründe zu werfen.



5.1 WAS IST SEXTORTION?

Sextortion, eine Kombination aus den englischen Wörtern „Sex“ und „Extortion“ (Erpressung), beschreibt eine Form der digitalen Erpressung, bei der psychologische Manipulation mit dem gezielten Einsatz moderner Technologien verbunden wird. Täter drohen, intime Bilder oder Videos sowie Chats der Betroffenen zu veröffentlichen, um Opfer zur Herausgabe weiterer intimer Inhalte, Geldzahlungen oder anderer Zugeständnisse zu zwingen [132], [215], [224], [231], [236], [294]. Besonders problematisch ist, dass sowohl tatsächliche als auch mithilfe von Deepfake-Technologie erstellte kompromittierende Inhalte den psychologischen Druck auf die Opfer erheblich erhöhen. Die täuschend echten Manipulationen lassen Drohungen glaubwürdig erscheinen und verstärken die Angst vor sozialer Bloßstellung [100]. Ein bezeichnendes Merkmal von Sextortion ist die Geschwindigkeit, mit der diese Fälle eskalieren können: Mitunter dauert es nur wenige Stunden von der ersten Kontaktaufnahme bis zur Erpressung [296], [324].

Die Digitalisierung hat die Art und Weise, wie Menschen kommunizieren, grundlegend verändert. Soziale Medien, Messaging-Dienste und andere digitale Plattformen sind heute neben Smartphones fester Bestandteil des Alltags. Insbesondere Jugendliche nutzen diese Plattformen intensiv, teilen persönliche Inhalte und pflegen soziale Kontakte im digitalen Raum. Seit der COVID-19-Pandemie hat sich der Trend zur Verlagerung sozialer Interaktionen ins Digitale weiter verstärkt [23]. Dieses veränderte Kommunikationsverhalten schafft jedoch auch Angriffsflächen für Sextortion, Cybermobbing oder Rache-Pornos („Revenge Porn“).

Sextortion unterscheidet sich von anderen Formen der Online-Kriminalität durch den explizit sexuellen Kontext. Während beispielsweise Phishing darauf abzielt, Zugang zu sensiblen Daten zu erlangen, und Love Scam emotionale Manipulation zur finanziellen Bereicherung nutzt, steht bei Sextortion die gezielte Ausnutzung intimer Inhalte im Vordergrund [294]. Eine Abgrenzung zum Phänomen Cybermobbing ist jedoch schwierig, da sich die Mechanismen und Auswirkungen teilweise überschneiden. Cybermobbing umfasst wiederholte digitale Schikanen über digitale Kanäle, oft geprägt durch die Anonymität der Täter und eine breite Öffentlichkeit [213], [253]. Im Gegensatz dazu richten sich Sextortion-Täter gezielt mit sexualisierten Angriffen an die emotionale und soziale Verwundbarkeit ihrer Opfer [133], [224].

Die weltweite Zunahme von Sextortion-Fällen ist alarmierend. 2023 wurden über 26.700 Fälle gemeldet – ein deutlicher Anstieg gegenüber den 10.700 Fällen im Jahr 2022 [130]. Zwischen Oktober 2022 und März 2023 registrierten FBI und Homeland Security mehr als 13.000 Berichte über finanzielle sexuelle Erpressung von Kindern, mit mindestens 12.600 betroffenen Opfern und 20 dokumentierten Suiziden [324], [325]. Zudem berichtete die Internet Watch Foundation (IWF), dass allein in den ersten sechs Monaten des Jahres 2023 mehr Fälle gemeldet wurden als im gesamten Jahr 2022 [151].

Fehlende Erfassung in der Kriminalstatistik

Sextortion ist, ähnlich wie Cybermobbing, in vielen Datenerhebungen weltweit noch nicht als eigenständiges Phänomen etabliert. Cybermobbing wurde beispielsweise erst 2018 in die globalen Erhebungen der World Health Organization (WHO) aufgenommen. Sextortion ist in Umfragen oft schwer abgrenzbar, obwohl bereits Daten zu verwandten Taten wie dem Erhalten oder Versenden von Bildern ohne Erlaubnis existieren [106]. Eine hohe Dunkelziffer verschärft die Problematik zusätzlich.

In Deutschland fehlt es weiterhin an präzisen Zahlen, da Sextortion in der polizeilichen Kriminalstatistik (PKS) nicht als eigenständiger Deliktbereich ausgewiesen wird [59]. Zudem berücksichtigt die PKS in der Regel nur Taten, bei denen die Täter ihren Standort im Inland haben. Delikte, die aus dem Ausland heraus begangen werden, bleiben meist unberücksichtigt [59]. Diese Erfassungslücken erschweren es, ein klares Bild des tatsächlichen Ausmaßes zu gewinnen. Trotz dieser Einschränkungen gilt Sextortion als eine der größten internetbasierten Bedrohungen [43]. Die Anpassung der Statistik wäre leicht umsetzbar. Laut einer Umfrage der Deutschen Presse-Agentur wurden 2023 bundesweit mehr als 2.000 Fälle erfasst. Ermittler gehen auch für 2024 von einer hohen Zahl solcher Delikte aus, insbesondere im Zusammenhang mit einem Anstieg von Taten, die aus dem Ausland begangen werden [278].

Einige Bundesländer meldeten für 2024 gegensätzliche Trends in ihren Statistiken: In Hessen stiegen die registrierten Fälle von Sextortion von einem niedrigen dreistelligen Bereich im Vorjahr auf einen mittleren dreistelligen Bereich bis Dezember 2024 [278], [323]. Dagegen verzeichnete das Landeskriminalamt Baden-Württemberg einen Rückgang der Zahlen in der PKS von 308 Fällen im Jahr 2022 auf 102 Fälle 2023 [176],

[323]. Diese Veränderung ist jedoch auf eine bereinigte Datenerfassung zurückzuführen, die zwischen Inlands- und Auslandstaten unterscheidet. Die Zahlen spiegeln daher nicht das tatsächliche Ausmaß des Phänomens wider [59], [176].

Im Jahr 2024 gaben sieben Prozent der Personen, die Opfer von Straftaten im Internet geworden waren, an, von Cybermobbing betroffen gewesen zu sein – ein Wert, der im Vergleich zu 2023 unverändert blieb. Bei Sextortion berichteten vier Prozent der Befragten über entsprechende Vorfälle, was einem Rückgang im Vergleich zu sieben Prozent im Jahr 2023 entspricht. Ein ähnlicher Trend zeigte sich bei Love Scamming, dessen Anteil von acht Prozent im Jahr 2023 auf sechs Prozent im Jahr 2024 sank. Zudem gingen die Berichte über Vorfälle mit Deepfake-Inhalten im selben Zeitraum von vier Prozent auf drei Prozent zurück [232]. Diese Rückgänge lassen sich jedoch unter anderem auf die zunehmende Verlagerung der Täteraktivitäten ins Ausland zurückzuführen, wodurch sie nicht in den nationalen Statistiken erfasst werden.

Viele Betroffene erstatten keine Anzeige, sei es aus Scham, Angst oder Unkenntnis über rechtliche Schutzmöglichkeiten [133], [224]. Studien weisen darauf hin, dass viele Opfer niemandem von ihren Erfahrungen berichten und nicht mal ein Fünftel Anzeige erstattet [259], [318], [333], was sowohl die Aufklärung als auch die Strafverfolgung erschwert.

5.2 TÄTERSTRATEGIEN UND VORGEHENSWEISEN

Sextortion wird zunehmend von professionellen, transnationalen Netzwerken durchgeführt, die gezielt psychologische und technologische Mittel einsetzen, um Opfer zu manipulieren. Viele dieser Täter operieren aus Ländern wie Nigeria, der Elfenbeinküste, Indien oder den Philippinen. In einigen Fällen wurden in diesen Ländern organisierte Gruppen entdeckt, die Opfer weltweit kontaktieren und gezielt manipulieren [100], [326]. Allein in Indien werden täglich schätzungsweise 500 Fälle von Sextortion gemeldet, von denen jedoch nur ein Bruchteil offiziell angezeigt wird [334].

Diese Gruppen nutzen verschlüsselte Plattformen und setzen zunehmend KI-gestützte Technologien wie Deepfakes ein, um täuschend echte Inhalte zu erzeugen. Daneben stehen Tätern auch standardisierte Skripts zur Verfügung, die in kriminellen Netzwerken kursieren und gezielt für Sextortion-Angriffe eingesetzt werden. Berichte zeigen, dass Opfer häufig identische Drohnachrichten erhalten, die seit 2021 öffentlich zugänglich sind und weiterhin aktiv verwendet werden [241]. Zudem fordern sie Zahlungen in schwer rückverfolgbaren Kryptowährungen, um ihre Identität und ihre Aktivitäten zu verschleiern [59], [100], [152], [222], [306], [326], [334]. Neben Kryptowährungen nutzen Sextortion-Täter zunehmend alternative Finanzplattformen wie Etsy, Amazon, PayPal und Selar.co, um Geld zu waschen oder ihre Identität zu verschleiern. Darüber hinaus erleichtern anonyme Online-Foren und Messenger-Gruppen den Austausch von Erpressungstaktiken, wodurch Täter effektiver vorgehen und Strafverfolgung erschwert wird [9].

Beispielsweise verbreiten extremistische Online-Communitys wie die „Manosphere“ und „Incels“ gezielt Inhalte, die Sextortion als Mittel der Machtausübung legitimieren. In einschlägigen Foren und auf Plattformen wie Telegram tauschen Täter Manipulations- und Erpressungstechniken aus. Diese Gruppen verstärken die Vorstellung, dass Frauen für männliches Leid verantwortlich seien, und nutzen digitale Räume zur Ideologisierung und Professionalisierung von Tätermethoden [9]. Dies zeigt, dass digitale Gewalt nicht isoliert betrachtet werden kann, sondern Täter Teil eines größeren Ökosystems sein können.

Neben organisierten kriminellen Netzwerken zählen auch Einzelpersonen aus dem sozialen Umfeld der Opfer – wie (Ex-)Partner, Freunde oder Familienangehörige – zu den Tätern von Sextortion. Ihre Motivationen reichen von emotionalen Beweggründen wie Eifersucht bis hin zu finanziellen Interessen oder dem Wunsch nach Kontrolle. Häufig tritt Sextortion in Verbindung mit Gewalt in intimen Beziehungen auf, sei es durch Drohungen, emotionalen Druck oder digitalen Missbrauch. Täter nutzen

in diesen Fällen digitale Plattformen, um Macht über das Opfer auszuüben und ihre Drohungen zu untermauern [224], [295], [332].

Sextortion folgt einem klaren Muster, welches in mehrere Phasen unterteilt werden kann:

1. **Kontaktaufnahme:**
   Täter suchen gezielt nach potenziellen Opfern auf Plattformen wie Instagram, Snapchat oder TikTok, die bei Jugendlichen zum Teilen persönlicher Inhalte besonders beliebt sind. Mithilfe gefälschter Profile oder synthetischer Identitäten, die oft gestohlene Bilder oder Identitätsdaten enthalten, geben sie sich als Gleichaltrige oder romantisch interessierte Personen aus, um das Vertrauen der Opfer zu gewinnen [294], [306]. Häufig wird die Kommunikation schnell auf verschlüsselte Messenger-Dienste oder E-Mail verlagert, um eine Nachverfolgung oder mögliche Sperrung auf Social-Media-Plattformen zu vermeiden [243], [294], [306], [318].

   Zu den typischen Methoden der Täter zählen:

   - Die Verwendung mehrerer Identitäten oder die Vortäuschung eines anderen Geschlechts, um Nähe zu schaffen: Zusätzliche Profile verstärken unter anderem die Glaubwürdigkeit der Täter, während vorgetäuschte Rollen gezielt romantisches Interesse oder Vertrauen auslösen sollen.

   - Der gezielte Zugriff auf öffentliche Social-Media-Profile, um persönliche Informationen wie Freundeslisten und Vorlieben zu sammeln.

   - Heimliches Aufzeichnen von Nachrichten oder Videochats, um später Druck auszuüben [306].

2. **Vertrauensaufbau:**
   Im nächsten Schritt versuchen Täter, eine emotionale Bindung zum Opfer aufzubauen. Sie zeigen sich einfühlsam, interessieren sich scheinbar für persönliche Probleme und Vorlieben der Betroffenen und sammeln gezielt Informationen, die sie später als Druckmittel nutzen können. Jugendliche sind besonders anfällig für diese Manipulation, da sie häufig geschmeichelt sind und die Risiken unterschätzen [243], [294].

   Eine häufig eingesetzte Strategie besteht darin, über Online-Dating-Plattformen Vertrauen zu gewinnen. Viele Opfer verlassen sich darauf, die Vertrauenswürdigkeit ihres Gegenübers anhand des Kommunikationsverhaltens oder der Profilgestaltung zu beurteilen. Untersuchungen zeigen jedoch, dass diese vermeintlichen Hinweise leicht manipuliert oder gefälscht werden können, was den Tätern die Täuschung erleichtert [294].

   Diese gezielte Täuschung durch emotionale Manipulation und falsche Signale erschwert es den Betroffenen, die wahren Absichten der Täter rechtzeitig zu erkennen, was das Risiko erheblich erhöht [243], [294].

3. **Erpressung:**
   Sobald intime Inhalte geteilt wurden, beginnt die eigentliche Erpressung. Die Täter drohen mit der Veröffentlichung der Inhalte, falls die Opfer ihren Forderungen nicht nachkommen. Diese umfassen oft die Herausgabe weiterer intimer Inhalte, finanzielle Zahlungen oder andere Zugeständnisse [318]. Täter setzen auf massiven emotionalen Druck, indem sie Aussagen wie „Ich dachte, du liebst mich“ nutzen, um Schuldgefühle zu erzeugen. Die Drohung, soziale Bloßstellung herbeizuführen, verstärkt die Angstzustände der Opfer erheblich. Besonders perfide ist, dass Täter in extremen Fällen sogar mit Selbstverletzung oder Suizid drohen [306].

   Ein besonders problematisches Merkmal solcher Angriffe ist ihre Dynamik: In 27 Prozent der Fälle folgen auf die erste Erpressung weitere Forderungen, wodurch die Opfer in eine Spirale geraten, aus der sie

sich kaum befreien können [295]. Selbst wenn die Opfer versuchen, den Kontakt abzubrechen, nehmen die Täter häufig erneut Verbindung auf – oft über alternative Plattformen oder weitere gefälschte Identitäten. Diese Taktik verstärkt das Gefühl der Ausweglosigkeit und sorgt dafür, dass die Opfer sich zunehmend isoliert und unter der Kontrolle der Täter fühlen [295].

In vielen Fällen dient das kompromittierende Material lediglich als Mittel, um die Opfer unter Druck zu setzen. Laut Berichten geben 70 Prozent der Betroffenen, die nicht zahlen, an, dass ihre Bilder letztlich nicht veröffentlicht wurden [68]. Dies verdeutlicht, dass die Drohung häufig lediglich darauf abzielt, die Opfer gefügig zu machen, ohne dass tatsächlich eine Veröffentlichung geplant ist.

Täterstrategien sind vielfältig und variieren je nach Ziel und Situation:

- **Gezielte Manipulation (Social Engineering):**
  Täter nutzen psychologische Tricks wie Social Engineering, um das Vertrauen ihrer Opfer zu gewinnen. Dies schließt empathisches Verhalten und gezielte Fragen ein, die eine emotionale Abhängigkeit schaffen sollen. Über Wochen oder Monate hinweg werden intime Informationen gesammelt, die später als Druckmittel dienen [243], [294].

- **Automatisierte Angriffe:**
  Neben individuellen Ansätzen setzen Täter auch auf automatisierte Kampagnen. Häufig kommen generische Phishing-Mails zum Einsatz, in denen beispielsweise behauptet wird, die Webcam des Opfers sei gehackt worden und man hätte Bilder oder Videos von sexuellen Handlungen. Solche Drohungen sind oft frei erfunden, zielen jedoch auf die Angst der Opfer ab. Bezahlungen werden meist in Kryptowährungen wie Bitcoin gefordert, da diese schwer rückverfolgbar sind [100], [222].

- **Einsatz von Deepfake-Technologie:**
  Die Verbreitung von Deepfake-Technologie hat die Methoden von Sextortion-Tätern auf ein neues Niveau gehoben. Täter erstellen täuschend echte Bilder oder Videos aus den öffentlichen oder geteilten Daten ihrer Opfer, die sie in kompromittierenden Situationen zeigen. Derzeitigen Erkenntnissen zufolge bestehen etwa elf Prozent der Materialien aus Fälschung [295]. Zusätzlich werden solche Fälschungen in extremistischen Online-Foren verbreitet, um Opfer gezielt zu isolieren und weiter unter Druck zu setzen [9]. Diese Inhalte wirken oft so authentisch, dass sie von den Betroffenen selten hinterfragt werden. Laut Europol steigt die Nutzung rasant. Diese technologischen Fortschritte verstärken den psychologischen Druck auf die Opfer erheblich, da die Täuschung kaum erkennbar ist [46], [100].

- **Weitere Methoden:**
  Täter setzen gezielt auf falsche Versprechungen, beispielsweise Modelverträge, Geld oder Online-Spielgutscheine, um Opfer zu locken beziehungsweise dazu zu bringen, ein Foto von sich zu senden [306]. Auch der Einsatz von Chatbots, die menschliche Kommunikation simulieren, wird zunehmend beobachtet [324].

Neben den Phasen eines Angriffs und den verschiedenen Strategien lassen sich zwei Hauptvarianten von Sextortion unterscheiden [174]:

1. **Kontaktbasierte Sextortion:**
   Wie mehrheitlich beschrieben, kontaktieren und manipulieren Täter ihre Opfer direkt über soziale Medien oder Messenger-Dienste, um kompromittierende Inhalte zu erhalten. Diese Inhalte werden anschließend als Druckmittel verwendet, um weitere Forderungen zu stellen [174].

2. **Datenleck-basierte Sextortion:**
   Nicht zu unterschätzen ist jedoch auch die Gefahr, dass Täter durch Sicherheitslücken oder Datenlecks an persönliche Informationen wie Passwörter gelangen. Häufig behaupten sie, kompromittierende Inhalte zu besitzen, die jedoch gar nicht existieren [162], [174], [222].

5.3 WER IST BETROFFEN? ZIELGRUPPEN UND RISIKOFAKTOREN

Sextortion betrifft Menschen aller Altersgruppen und sozialer Hintergründe rund um die Welt, wobei bestimmte Gruppen besonders gefährdet sind [112]. Jugendliche gehören zu den am häufigsten betroffenen Zielgruppen [78], [215].

Unterschiede zwischen den Geschlechtern sind deutlich erkennbar. Jungen und Männer werden häufiger Opfer sexueller Erpressung, da Täter gezielt kompromittierende Inhalte nutzen, um finanzielle oder andere Forderungen durchzusetzen. Mädchen und Frauen hingegen werden verstärkt Opfer sexueller Belästigung oder der nicht einvernehmlichen Verbreitung intimer Bilder oder Videos (Revenge Porn), insbesondere durch ehemalige Partner [78], [215].

Studien zeigen, dass männliche Teenager zwischen 14 und 17 Jahren überdurchschnittlich häufig Opfer von Sextortion werden [68], [78], [215], [231], [295], [306], [326]. Täter nutzen gezielt die emotionale Unsicherheit und den oft leichtsinnigen Umgang Jugendlicher mit digitalen Medien, um Vertrauen aufzubauen und intime Inhalte zu erpressen [294].

Wenn das Geschlecht bekannt ist, sind 98 Prozent der Betroffenen männlich, wobei 38 Prozent unter 18 Jahre alt sind [68]. Täter manipulieren Jungen oft, indem sie sich als junge Frauen ausgeben und über soziale Netzwerke oder Online-Spiele den Kontakt aufnehmen [324], [326]. Jungen fühlen sich oft sicherer als Mädchen, zwischen realen und gefälschten Inhalten im Internet unterscheiden zu können, was sie jedoch anfälliger für gezielte Manipulation macht [211]. Außerdem neigen sie dazu, Passwörter weniger sorgfältig zu nutzen, kommunizieren häufiger mit Fremden online und bewegen sich in Communities, in denen Missbrauch wie Sextortion verbreitet ist, beispielsweise in Online-Spielen oder bestimmten sozialen Netzwerken [113], [190], [211], [287]. Ein hohes Bedürfnis nach sozialer Anerkennung, mangelnde digitale Bildung und die unkritische Nutzung sozialer Netzwerke erhöhen die Anfälligkeit für Sextortion zusätzlich [318], [324].

Teenager im Alter von 14 bis 18 Jahren nutzen soziale Netzwerke und Messenger besonders intensiv, was sie durch Sexting oder unbedachtes Teilen persönlicher Inhalte gefährdet [190], [318]. Jugendliche verbringen bis zu sechs Stunden online, wobei Plattformen wie Instagram, Snapchat, TikTok und Brawl Stars, ein Online-Game mit Chatfunktion, besonders intensiv genutzt werden [27], [190]. Die Plattformen bieten Tätern einfache Zugänge zu ihren Opfern, da Jugendliche oft persönliche Inhalte teilen, ohne sich der Risiken bewusst zu sein. Zudem trägt eine unzureichende elterliche Kontrolle oder fehlende Aufklärung über digitale Risiken erheblich dazu bei, dass Jugendliche leicht zu Opfern werden [98].

Auch Erwachsene geraten ins Visier von Sextortion-Tätern. Besonders gefährdet scheinen Männer zwischen 30 und 50 Jahren zu sein, da sie häufig über finanzielle Mittel, eine exponierte gesellschaftliche Stellung und familiäre Verpflichtungen verfügen, die sie erpressbar machen [132]. Bei erwachsenen (männlichen) Opfern greifen Täter oft auf Phishing-Mails zurück, in denen sie behaupten, die Webcam des Opfers gehackt zu haben, oder nutzen Dating-Plattformen wie Tinder oder Bumble, um Vertrauen zu gewinnen und intime Inhalte zu erschleichen. Frauen, insbesondere Influencerinnen, sind ebenfalls zunehmend Opfer von Sextortion, oft in Verbindung mit Cyberstalking [112].

5.4 PSYCHOLOGISCHE UND GESELLSCHAFTLICHE AUSWIRKUNGEN

Sextortion hat tiefgreifende psychologische und soziale Auswirkungen, die vielschichtig sind und häufig weit über den akuten Stressmoment hinausgehen. Für Jugendliche sind sie besonders schwerwiegend, da diese Altersgruppe oft noch nicht über die emotionale Reife und die Ressourcen verfügt, um mit derartigen Bedrohungen umzugehen. Schulische und familiäre Unterstützung sowie politische Maßnahmen zur Förderung digitaler Kompetenzen sind daher von entscheidender Bedeutung [27].

Studien zu Cybermobbing haben gezeigt, dass die Anonymität der Täter das Machtungleichgewicht zwischen Täter und Opfer vergrößert und dadurch Gefühle von Unsicherheit und Hilflosigkeit bei den Betroffenen intensiviert. Diese Anonymität und die Unklarheit darüber, wer hinter den Drohungen steht, spielen auch bei Sextortion eine zentrale Rolle und untergraben das Vertrauen in digitale Räume nachhaltig [213], [316]. Zudem verstärkt die potenziell große Reichweite digitaler Plattformen die Angst, der sozialen Bloßstellung zu entkommen [213].

Sextortion führt bei den Opfern zu weit mehr als den Gefühlen von Scham, Angst und Selbstzweifeln. Besonders belastend ist der sogenannte „double hit" [327] – ein „doppelter Schlag" für die Betroffenen: Neben finanziellen Verlusten erleben sie häufig den emotionalen Bruch einer als wertvoll empfundenen Beziehung. Studien zeigen, dass dieser emotionale Verlust und die damit verbundene Enttäuschung oft schwerer wiegt als der finanzielle Schaden [327]. Viele Opfer suchen die Schuld an ihrer Situation bei sich selbst, vor allem wenn sie intime Inhalte freiwillig geteilt haben. Besonders belastend ist, dass Täter ihre Opfer gelegentlich zu ungewollten sexuellen Handlungen zwingen [133], [327]. Diese Scham und Selbstvorwürfe hindern die Betroffenen oft daran, sich anderen anzuvertrauen oder Hilfe zu suchen. Studien zeigen, dass viele Betroffene sich vollständig aus ihrem sozialen Umfeld zurückziehen, was langfristig zu zusätzlichen psychischen und sozialen Problemen führt [112], [318]. Viele Opfer berichten zudem von Schlaflosigkeit, sozialer Isolation und Paranoia, da sie ständig die Veröffentlichung der kompromittierenden Inhalte fürchten. Diese Belastungen können in extremen Fällen zu Suizidgedanken führen [112], [207], [214], [224], [318], [332], [333].

In besonders schweren Fällen kann es zu Selbstverletzungen und Suizid kommen [27]. Auch Cybermobbing/-bullying kann derart drastische Konsequenzen für Teenager und Kinder ab zehn Jahren haben, weil es die Wahrscheinlichkeit, an Suizid zu denken, drastisch erhöht. Studien zeigen, dass 16 Prozent der Jugendlichen Erfahrungen mit digitaler Gewalt gemacht haben [27]. Tendenz steigend. Dies verdeutlicht die Dringlichkeit, präventive Maßnahmen zu ergreifen, um digitale Kompetenzen zu fördern und Jugendliche besser vor solchen Bedrohungen zu schützen.

Der Fall Jordan DeMay oder Amanda Todd[1] zeigt die verheerenden Auswirkungen von Sextortion und Cybermobbing. Die 15-Jährige Kanadierin beging am 10. Oktober 2012 nach zwei gescheiterten Versuchen, Suizid im Haus ihrer Eltern, nachdem sie seit 2010 Drohungen und Bloßstellungen im Internet ausgesetzt war. Auch mehrere Schul- und Ortswechsel halfen nicht. Ihr Peiniger Aydin Coban aus den Niederlanden sitzt seit 2017 im Gefängnis für weitere Erpressungen von Männern und Frauen aus den USA, Kanada und Großbritannien. Dieses Beispiel zeigt, wie eng Sextortion mit anderen Formen digitaler und physischer Gewalt verknüpft ist und welche schwerwiegenden Konsequenzen solche Delikte haben können. Zudem zeigt es, wie Sextortion das Leben der Opfer und ihres sozialen Umfelds für immer beeinträchtigen kann [112], [318], [333]. Auch gesamtgesellschaftlich sind die Auswirkungen spürbar. Sie manifestieren sich in Form sinkender Bildungsabschlüsse, gesundheitlicher Probleme und eines gesteigerten Bedarfs an therapeutischen Maßnahmen [21], [163].

5.5 RECHTLICHE RAHMENBEDINGUNGEN UND POLIZEILICHE ERMITTLUNGEN

Sextortion ist kein klar definierter Straftatbestand im deutschen Recht. Stattdessen greifen mehrere Paragrafen des Strafgesetzbuchs (StGB), je nach Kontext und Art der Tat. Dabei reicht das Spektrum von Erpressung über sexuelle Nötigung bis hin zur Verbreitung kinderpornografischer Inhalte.

- **§ 253 StGB (Erpressung):** Wenn Täter mit der Veröffentlichung intimer Inhalte drohen, um Zahlungen oder andere Forderungen durchzusetzen [59], [137].

- **§ 238 StGB (Nachstellung):** Bei wiederholten Drohungen oder langanhaltendem Druck auf das Opfer greift dieser Paragraf, der Stalking kriminalisiert [59].

1 https://www.amandatoddlegacy.org

- **§ 184b und § 184c StGB (Verbreitung kinder- und jugendpornografischer Inhalte):** Diese Paragrafen finden Anwendung, wenn Minderjährige betroffen sind oder intime Bilder von Jugendlichen als Druckmittel genutzt werden [59], [137], [231].

- **§ 176b StGB (Sexueller Missbrauch von Kindern):** Intime Aufnahmen, die durch Sexting entstehen, können in Sextortion-Szenarien ebenfalls strafbar sein und als Missbrauch gewertet werden, wenn sie als Druckmittel verwendet werden [59], [231].

Internationale Vergleiche zeigen, dass Sextortion auch in anderen Ländern nicht immer ein eigenständiger rechtlicher Begriff ist. In den USA etwa wird Sextortion ebenfalls nicht als spezifischer Straftatbestand geführt, sondern unter bestehenden Gesetzen wie Erpressung oder Kinderpornografie erfasst [333].

Die Strafverfolgung von Sextortion ist mit erheblichen Herausforderungen verbunden, da Täter gezielt digitale Technologien nutzen, um ihre Identität zu verschleiern und Ermittlungen zu erschweren.

Ein weiteres zentrales Problem ist die geringe Anzeigebereitschaft der Betroffenen. Studien zeigen, dass jeweils maximal ein Fünftel der Befragten Anzeige erstattet [259], [318], [333]. Auch die Befürchtung, nicht ernst genommen zu werden, spielt hier eine Rolle. Diese Zurückhaltung führt zu einer hohen Dunkelziffer und erschwert die systematische Bekämpfung des Phänomens.

Trotz der bestehenden Herausforderungen verzeichnen deutsche und internationale Strafverfolgungsbehörden Fortschritte in der Bekämpfung von Sextortion. Innovative Ermittlungsansätze und internationale Kooperationen spielen dabei eine zentrale Rolle:

- **Nachverfolgung von Kryptowährungen:** Die Analyse von Geldströmen hat sich als zentrale forensische Methode in der Cyberkriminalitätsbekämpfung etabliert. Spezialisierte Softwarelösungen (z. B. Chainalysis) ermöglichen es, Zahlungsflüsse zu untersuchen und verdächtige Transaktionen zurückzuverfolgen, um kriminelle Netzwerke zu identifizieren [99], [222].

- **Internationale Zusammenarbeit:** Kooperationen mit Europol und Interpol ermöglichen grenzüberschreitende Ermittlungen und die Zerschlagung globaler Netzwerke. So führte eine internationale Polizeimaßnahme zur Aufdeckung eines transnationalen Sextortion-Rings, der mindestens 47.000 US-Dollar von Opfern erpresste [152].

- **Sensibilisierung der Plattformen:** Soziale Netzwerke und Kommunikationsdienste werden zunehmend in die Präventionsarbeit eingebunden. Plattformbetreiber wie Instagram und WhatsApp werden dazu angehalten, verdächtige Aktivitäten zu melden und Mechanismen zur Früherkennung zu entwickeln [241].

Die Kombination aus technologischen, rechtlichen und kooperativen Ansätzen unterstreicht die Vielschichtigkeit der Bekämpfung von Sextortion. Dennoch bleibt es eine zentrale Herausforderung, sowohl die Täter als auch die verwendeten digitalen Infrastrukturen effektiv zu adressieren.

5.6 PRÄVENTION UND INTERVENTION: STRATEGIEN GEGEN SEXTORTION

Die Prävention von Sextortion ist essenziell, um die Zahl der Fälle zu reduzieren. Bildung, technologische Schutzmaßnahmen und gesellschaftliches Engagement spielen hierbei eine zentrale Rolle. Ein erster Schritt besteht darin, Warnsignale frühzeitig zu erkennen.

Warnsignale lassen sich sowohl im Verhalten der Betroffenen als auch im Online-Verhalten erkennen. Häufig ziehen sich Opfer plötzlich aus sozialen Aktivitäten zurück, zeigen Angst vor Benachrichtigungen oder Nachrichten, verstecken ihr Smartphone oder ihren Computer oder leiden unter Schlafstörungen und Appetitverlust. Online zeigen sich Risiken oft durch Freundschaftsanfragen von Unbekannten oder durch plötzliche intime oder persönliche Fragen [306].

Bildung und Aufklärung sind Schlüsselmaßnahmen, um Jugendliche und Erwachsene über die Gefahren digitaler Erpressung zu informieren. Schulen sollten Informationen über Präventionsmaßnahmen anbieten, um einen sicheren Umgang mit sozialen Netzwerken und persönlichen Daten zu vermitteln. Eltern sollten regelmäßig Gespräche mit ihren Kindern führen, um ihnen potenzielle Gefahren aufzuzeigen und ihnen zu vermitteln, dass sie bei Problemen immer Unterstützung finden können. Diese Gespräche sollten ohne Vorwürfe geführt werden und den Fokus darauf legen, dass jeder Mensch Opfer von Sextortion werden kann – unabhängig von Alter, Geschlecht oder Verhalten [58], [103], [231], [306].

Zudem tragen technologische Schutzmaßnahmen dazu bei, Sextortion zu verhindern. Plattformen wie Instagram und WhatsApp haben Sicherheitsmechanismen wie Zwei-Faktor-Authentifizierung und automatische Erkennung verdächtiger Aktivitäten eingeführt. Die Nutzung sicherer, schwer zu erratender Passwörter sowie die Vorsicht vor verdächtigen Links in E-Mails sind ebenfalls wichtige Maßnahmen. Auch die regelmäßige Überprüfung und Anpassung von Privatsphäre-Einstellungen auf Social-Media-Plattformen schützt. Zudem minimieren regelmäßig aktualisierte Betriebssysteme und Virenschutzprogramme die Risiken durch Schadsoftware wie Infostealer. Auch die kontinuierliche Absicherung der digitalen Identität durch entsprechende Überwachungsdienste auf Datenlecks im Deep-, Dark- und Surfaceweb hilft bei der Prävention. Das Abdecken von Webcams, wenn sie nicht genutzt werden, reduziert zusätzlich die Gefahr unbefugter Aufnahmen [231], [306].

Ein zentraler Aspekt der Prävention ist das sichere Verhalten im digitalen Raum. Wir sollten darauf achten, keine Freundschaftsanfragen von Unbekannten anzunehmen und genau überlegen, was wir mit der Welt teilen.

Wenn Betroffene dennoch Opfer von Sextortion werden, sind bestimmte Schritte entscheidend:

- **Keiner Forderung nachkommen:** Es sollten keinerlei Geldzahlungen oder andere Forderungen wie das Senden von (weiteren) Bildern oder Videos getätigt werden [231], [306].
- **Ruhe bewahren und Unterstützung suchen:** Eine wertfreie Haltung von Unterstützenden wie Eltern, Freunden oder Beratungsstellen ist entscheidend. Beratungsangebote wie der Weiße Ring bieten schnelle und professionelle Hilfe.
- **Beweise sichern:** Alle relevanten Inhalte wie Chatverläufe oder Nachrichten sollten gesichert werden, beispielsweise durch Screenshots [306].
- **Kontakt abbrechen:** Täter sollten blockiert und weitere Nachrichten ignoriert werden [231].
- **Rechtliche Schritte einleiten:** Eine schnelle Anzeige bei den Zentralen Ansprechstellen der Polizeien für Internetkriminalität (Zentrale Ansprechstellen Cybercrime (ZAC)) und die Meldung an Plattformbetreiber sind essenziell, um möglicherweise bereits veröffentlichte Inhalte entfernen zu lassen.

Langfristige Prävention erfordert jedoch auch gesellschaftliches Engagement auf allen Ebenen. Tabus rund um sexuelle Inhalte müssen aufgebrochen werden, damit Betroffene sich ohne Angst vor Verurteilungen frühzeitig Hilfe suchen können. Gleichzeitig ist es entscheidend, dass psychologische und rechtliche Unterstützung leicht zugänglich ist.

Die enge Zusammenarbeit zwischen Politik, Bildungseinrichtungen und (Technologie-)Unternehmen ist unerlässlich, um Betroffene zu schützen und gegen diese Form der Kriminalität vorzugehen.

Sextortion ist eine ernste Bedrohung, die durch gezielte Prävention, technologische Innovationen und gesellschaftliches Handeln bekämpft werden kann. Nur durch eine gemeinsame Anstrengung von Bildungseinrichtungen, Strafverfolgungsbehörden und der Gesellschaft als Ganzes können Angriffe – vor allem auch gegen die Vulnerabelsten unserer Gesellschaft – verhindert und Betroffene nachhaltig geschützt werden.

ANHANG

ÜBER DIE SCHWARZ GRUPPE UND SCHWARZ DIGITS

Die Schwarz Gruppe ist eine international führende Handelsgruppe mit rund 13.900 Filialen und 575.000 Mitarbeitern in 32 Ländern. Im Geschäftsjahr 2023 erwirtschafteten die Unternehmen der Schwarz Gruppe einen Gesamtumsatz von 167,2 Milliarden Euro. Mit ihrem einzigartigen Ökosystem decken sie den gesamten Wertschöpfungskreis ab: von der Produktion über den Handel bis hin zu Recycling und Digitalisierung. Sie schaffen Lösungen, die das Leben von Milliarden Menschen heute und in Zukunft nachhaltiger, gesünder und sicherer machen – sie handeln voraus. Lidl und Kaufland bilden die Säulen im Lebensmitteleinzelhandel und sind ein fester Bestandteil im Alltag von 7,2 Milliarden Kunden. Viele Eigenmarkenprodukte und nachhaltige Verpackungen in deren Regalen kommen direkt von der Schwarz Produktion. Der Umweltdienstleister PreZero fördert mit seinem Wertstoffmanagement eine funktionierende Kreislaufwirtschaft und investiert so in eine saubere Zukunft. Schwarz Digits bietet als IT- und Digitalsparte überzeugende digitale Produkte und Services an, die den hohen deutschen Datenschutzstandards entsprechen und garantiert so größtmögliche digitale Souveränität. Als partnerschaftliche Dienstleister unterstützen Schwarz Corporate Solutions die Unternehmen der Schwarz Gruppe bei allen Themen von Verwaltung über Personal bis hin zu operativen Tätigkeiten.

Schwarz Digits ist die IT- und Digitalsparte der Schwarz Gruppe und bietet überzeugende digitale Produkte und Services an, die den hohen deutschen Datenschutzstandards entsprechen. Mit dem Anspruch größtmöglicher digitaler Souveränität stellt Schwarz Digits die IT-Infrastruktur und Lösungen für das umfangreiche Ökosystem der Unternehmen der Schwarz Gruppe bereit und entwickelt dieses zukunftsfähig weiter. Darüber hinaus schafft Schwarz Digits optimale Bedingungen für die Entwicklung richtungsweisender Innovationen für Endkunden, Unternehmen und Organisationen der öffentlichen Hand. Zu Schwarz Digits gehören 7.500 Mitarbeiter der Marken Schwarz IT, Schwarz Digital, STACKIT, XM Cyber, Lidl e-commerce, Kaufland e-commerce, Schwarz Media und mmmake.

DEFINITIONEN UND ABKÜRZUNGSVERZEICHNIS

DEFINITIONEN

Advanced Persistent Threat (APT)	Ein „Advanced Persistent Threat“ ist eine fortgeschrittene und anhaltende Bedrohung durch hochqualifizierte Cyberkriminelle.
Backdoor	Eine „Backdoor“ (dt. Hintertür) ist ein heimlicher unbefugter Zugang zu einer Zielumgebung oder einem Zielsystem.
Bot/Botnetz	Ein „Bot“ ist ein fernsteuerbares Schadprogramm, welches auf einem System installiert ist. Mit „Botnetz“ ist ein Systemverbund von Bots gemeint, welcher über C2-Kanäle gesteuert werden kann. Die kompromittierten Systeme können auf Anweisung hin zusätzliche bösartige Nutzlasten herunterladen oder gestohlene Daten zurück zum Angreifer leiten.
Command-and-Control (C2)	„Command-and-Control“ beschreibt eine Client/Server-Infrastruktur oder eine Menge von Techniken, mit denen ein Angreifer kompromittierte Computersysteme ansprechen oder steuern kann, die vorher beispielsweise in ein Botnetz integriert wurden. C2 besteht im Allgemeinen aus heimlichen Kommunikationskanälen zwischen Zielsystemen und einer Plattform, die der Angreifer kontrolliert.
Common Vulnerabilities and Exposure (CVE)	„Common Vulnerabilities and Exposure“ ist ein eindeutiges Identifikations- und Bennenungssytem für bekannte Sicherheitslücken in Software, das von einer unabhängigen Organisation vergeben wird.
Cybercrime-as-a-Service (Caas)	„Crime-as-a-Service“ ist die Bereitstellung von Cyberkriminalität als Dienstleistung, z.B. durch das Anbieten von Malware oder Hacking-Tools.
DevOps	„DevOps“ (Kofferwort entstanden aus Development und Operations) ist eine Arbeitsmethode, die die Zusammenarbeit zwischen Software-Entwicklung (Development) und IT-Betrieb (Operations) verbessert, um Software schneller, zuverlässiger und mit höherer Qualität auszuliefern.
DevSecOps	„DevSecOps“ (Kofferwort entstanden aus Development, Security und Operations) ist ein Ansatz, der die Sicherheit (Security) von Anwendungen bereits frühzeitig im Entwicklungsprozess (Development) berücksichtigt, indem Sicherheitsmaßnahmen in die Arbeitsabläufe von Entwicklern und IT-Betriebs-Teams (Operations) integriert werden.
(Distributed) Denial-of-Service	Ein „Denial-of-Service“-Angriff (DoS-Angriff) richtet sich gegen die Verfügbarkeit von Diensten, Systemen oder Netzwerken, um diese zu stören bzw. zu sabotieren. Erfolgt ein solcher Angriff durch mehrere parallele Systeme, wird er als Distributed DoS (DDoS) (dt. verteilter DoS) bezeichnet.
Malware-as-a-Service	„Malware-as-a-Service“ ist ein Geschäftsmodell, bei dem Cyberkriminelle Schadsoftware gegen eine Gebühr an andere Kriminelle vermieten oder verkaufen.
Managed Security Service Provider	Ein „Managed Security Service Provider“ ist ein Unternehmen, an das Cyber- bzw. IT-Sicherheitsdienstleistungen ausgelagert werden.
Man-in-the-Middle	Als „Man-in-the-Middle“ wird eine Technik bezeichnet, in der sich ein Angreifer zwischen das Opfer und einen legitimen Dienst stellt. Über diesen Mechanismus können auch Maßnahmen wie MFA überwunden werden.
Multifaktor-Authentifizierung	Bei der „Multifaktor-Authentifizierung“ erfolgt beim Zugriff auf ein System die Bestätigung der Identität des Nutzers mithilfe multipler Authentifizierungsfaktoren aus verschiedenen Kategorien (Überprüfung der biometrischen Merkmale, Wissensabfrage oder Besitznachweiserbringung).
One-Time Password (OTP)	„One-Time Password“ bezeichnet ein einmalig gültiges Passwort, das zur erhöhten Sicherheit bei Online-Transaktionen oder beim Zugriff auf sensible Daten verwendet wird.

Phishing	„Phishing“ leitet sich aus dem englischen „Password Fishing“ ab. Cyberkriminelle versuchen mittels Phishing, über gefälschte Webseiten, E-Mails oder sonstige Nachrichten an die persönlichen Daten potenzieller Opfer zu gelangen oder sie dazu verleiten, bösartige Aktionen durchführen zu lassen.
Ransomware	„Ransomware“ ist ein Schadprogramm, welches auf Systemen Dateien verschlüsselt. Angreifer nutzen es, um Lösegeld zu erpressen. Im Gegenzug wird versprochen, den Entschlüsselungsschlüssel auszuhändigen.
Ransomware-as-a-Service (Raas)	Bei „Ransomware-as-a-Service“ wird eine Ransomware oder sonstige Angebote rund um einen Ransomware-Angriff als Dienstleistung zur Verfügung gestellt. RaaS ist eine Unterkategorie von CaaS.
Schadprogramm/Malware	Ein „Schadprogramm“ bzw. ein „Schadcode“ ist eine Software – oder ein Teil davon –, die entwickelt wurde, um unerwünschte schädliche Funktionen auf einem System auszuführen. In englischer Sprache sind Schadprogramme unter dem Begriff „Malicious Software“ (Malware) geläufig.
Session-Hijacking	„Session-Hijacking“ ist eine Methode, bei der Cyberkriminelle die aktive Sitzung eines anderen Benutzers übernehmen und unbefugt auf dessen Konten oder Daten zugreifen können.
Security Information and Event Management	Ein „Security Information and Event Management“, ist ein System zur Sammlung, Analyse und Überwachung von Sicherheitsereignissen in einer IT-Infrastruktur, um Bedrohungen frühzeitig zu erkennen und abzuwehren.
Security Operations Centre	Ein „Security Operations Center“ ist eine zentrale Stelle in einer Organisation, die die IT-Sicherheit überwacht und auf Sicherheitsvorfälle reagiert.
Social Engineering	Beim „Social Engineering“ nutzen Cyberkriminelle vermeintlich menschliche Schwächen wie Angst, Neugier oder blinden Gehorsam aus, um ihre Opfer dazu zu verleiten, eigenständig sensible Informationen preiszugeben, Schutzmaßnahmen zu umgehen oder schädliche Programme zu installieren.
Spear-Phishing	Das „Spear-Phishing“ ist eine gezielte Form von Phishing, bei der Angreifer spezifisiche Informationen über ihre Opfer sammeln, um personalisierte und überzeugende E-Mails zu versenden, die Schadsoftware enthalten oder auf gefälschte Webseiten verweisen.
Threat Intelligence	„Threat Intelligence“ ist die Sammlung, Analyse und Interpretation von Informationen über potenzielle Bedrohungen, die ein Unternehmen oder eine Organisation angreifen könnten, wie z.B. Cyberangriffe, Spionage oder Sabotage.
The Onion Router (TOR)	„The Onion Router“ ist ein Netzwerk, das den anonymen und verschlüsselten Austausch von Daten über das Internet ermöglicht, indem es den Datenverkehr über mehrere miteinander verbundene Computer leitet.
Vishing	Das „Vishing“ ist eine Form des Phishings, bei der Angreifer versuchen, Opfer telefonisch zu täuschen und sie zur Preisgabe vertraulicher Informationen zu bewegen.
Whaling	Das „Whaling“ ist eine Form des Spear-Phishings, die sich speziell gegen hochrangige Führungskräfte richtet.
Zero-Day-Exploit/ Zero-Day-Schwachstelle	Schwachstellen in einem System oder einer Software können von Angreifern ausgenutzt werden. Ein „Exploit“ ist der Hebel, ein Codefragment, um die Schwachstelle technisch auszunutzen. „Zero-Days“ sind besondere Schwachstellen, denn weder Hersteller noch Betreiber des Systems oder der Software haben Kenntnis davon.

ABKÜRZUNGSVERZEICHNIS

ADRIOS	Active Debris Removal In-Orbit Servicing
AI	Artificial Intelligence
AitM	Adversary-in-the-Middle
API	Application Programming Interface
APT	Advanced Persistent Threat
ARR	Annual Recurring Revenue
ASAT	Antisatellitenwaffe
ASIC	Application-Specific Integrated Circuit
BKA	Bundeskriminalamt
BSI	Bundesamt für Sicherheit in der Informationstechnik
BYOD	Bring Your Own Device
CaaS	Cybercrime-as-a-Service
CATI	Computer Assisted Telephone Interview
CCM	Continuous Controls Monitoring
CEO	Chief Executive Officer
ChatGPT	Chat Generative Pre-Trained Transformer
CISA	Cybersecurity and Infrastructure Security Agency
CI/CD	Continous Integration/ Continuous Delivery
CNAPP	Cloud Native Application Protection
COVID	Coronavirus
CRA	Cyber Resilience Act
CSA	Cloud Services Appliance
CTEM	Continuous Threat Exposure Management
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DARPA	Defense Advanced Research Projects Agency
(D)DoS	(Distributed) Denial-of-Service
DHCP	Dynamic Host Configuration Protocol
DLP	Data Leakage Prevention
DoD	U.S. Department of Defense
DSGVO	Datenschutz-Grundverordnung
EDR	Endpoint Detection and Response
EMP	Elektromagnetischer Impuls
ENISA	European Network and Information Security Agency
ESA	European Space Agency
EU	Europäische Union
EUIBA	European Union Institutions, Bodies and Agencies
EV	Europäische Verbundsysteme
FBI	Federal Bureau of Investigation
FIDO	Fast Identity Online
FLOP	False Load Output Prediction
FUD	Fear, Uncertainty, Doubt
FVEY	Five Eyes
GAU	Größter anzunehmender Unfall
GB	Gigabyte
GBP	Great Britain Pound
GDP	Gross Domestic Product
G(en)AI	Generative AI
GEO	Geostationary Earth Orbit
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GPWS	Ground Proximity Warning System
GRC	Governance, Risikomanagement und Compliance
GRU	Russischer Militärgeheimdienst
GSM(A)	Global System for Mobile Communications (Association)
GUGI	Hauptverwaltung Tiefseeforschung des russischen Verteidigungsministeriums
IAM	Identity and Access Management
IBM	International Business Machines Corporation
IDS	Intrusion Detection Systeme
IHK	Industrie- und Handelskammer
IKT	Informations- und Kommunikations-technologien

ILS	Instrument Landing System
IO	Information Operations
IOC	Indicator of Compromise
IOCTA	Internet Organised Crime Threat Assessment
IoT	Internet of Things
IP	Internet Protocol
IR	Incident Response
IRIS²	Infrastructure for Resilience, Interconnectivity and Security by Satellite
ISO	International Standards Organization
IT	Informationstechnologie
IT-SiG	IT-Sicherheitsgesetz
IWF	Internet Watch Foundation
JIT	Just in Time
KI	Künstliche Intelligenz
KMU	kleine und mittlere Unternehmen
KRITIS	Kritische Infrastruktur(en)
LEEF	Log Event Extended Format
LEO	Low Earth Orbit
LKA	Landeskriminalamt
LLM	Large Language Model, großes Sprachmodell
LPV	Localizer Performance with Vertical Guidance
LTE(-M)	Long Term Evolution (for Machines)
MDR	Managed Detection and Response
MEO	Medium Earth Orbit
MFA	Multifaktor-Authentifizierung
Mio.	Million
MitM	Man-in-the-Middle
ML	Machine Learning
Mrd.	Milliarde
MSSP	Managed Security Service Provider
MTTD	Mean Time to Detect
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NDR	Network Detection and Response
NHS	National Health Services
NIS	Network and Information Security Directive
NIS2UmsuCG	NIS2-Umsetzungs- und Cybersicherheits-stärkungsgesetz
NTN	Non-Terrestrial Networks
OMB	U.S. Office of Management and Budget
ORB	Operational Relay Box
OSS	Open Source Software
OT	Operational Technology
OTP	One-Time-Password
PAN	Palo Alto Networks
PKS	Polizeiliche Kriminalstatistik
PoC	Proof of Concept
PoV	Proof of Value
PSIRT	Product Security Incident Response Team
PV	Photovoltaik
RaaS	Ransomware-as-a-Service
ROV	Remotely Operated Vehicle
SCA	Source Code Analysis
SCSR24	Schwarz Cybersecurity Report 2024
SDLC	Software Development Lifecycle
SIEM	Security Information and Event Management
SLAP	Speculative Load Address Prediction
SOAR	Security Orchestration Automation and Responses
SOC	Security Operations Centre
SQL	Structured Query Language
SSCS	Software Supply Chain Security
SSH(D)	Secure Shell (Daemon)
SSRF	Server Side Request Forgery
StGB	Strafgesetzbuch
TLPT	Threat-Led Penetration Testing
TN	Terrestrial Network
TOR	The Onion Router
UI	User Interface

USD	US-Dollar
UX	User Experience
VIN	Vehicle Identification Number
VPN	Virtuelles privates Netzwerk
VTC	Video Teleconference
WAF	Web Application Firewall
WHO	World Health Organisation
XDR	Extended Detection and Response
XML	Extensible Markup Language
ZAC	Zentrale Ansprechstellen Cybercrime der Polizeien
ZDE	Zero-Day-Exploit
ZIT	Zentralstelle zur Bekämpfung der Internetkriminalität

LITERATURVERZEICHNIS

[1] Aggarwal, R. (2025). "Who was DeepSeek?", Januar.

[2] Agora Strategy (o. J.). "How Geopolitics Changes the Global Cyber Threat Landscape".

[3] Aiyer, B., Caso, J., Russel, P. & Sorel, M. (2022). "New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers", McKinsey & Company.

[4] Akamai (2024). "Alles, was Sie über die XZ Utils Backdoor wissen müssen", 01. April.

[5] Akerlof, G. A., (1970). "The Market for Lemons: Quality and the Market Mechanism", The Quarterly Journal of Economics, 84(3), pp.488-500

[6] Akshay, J., Moschetta, G., Winslow, E. (2025). "Global Cybersecurity Outlook 2025", World Economic Forum.

[7] Ali, R. (2021). "Looking to the future of the cyber security landscape", Network Security 3, 8-10.

[8] Alspach, K. (2024). "CISA Breached Via Ivanti VPN Vulnerabilities: Report', CRN, 08. März.

[9] Alto Intelligence (2024). "Blame the Women. Incels, loneliness and new security threats emerging from the digital sphere".

[10] America's Cyber Defense Agency (2024). "Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways", CISA, 29. Februar.

[11] Andrea, D. M. (2024). "Cybersecurity Outlook for 2025: The Shifting Threat Landscape", KLR, 21. November.

[12] Anti-Phishing Working Group (APWG) (2024). "Phishing Activity Trends Report 3rd Quarter 2024", 14. Oktober.

[13] Antoniuk, D. (2025). "Slovakia registry cyberattack disrupts land, agriculture services", The Record, 10 Januar.

[14] Apostle, J., Harrison, A., Kawkabani, R., Hewitt, H. & Hardan, O. (2024). "NIS2: Where do European Countries Stand on Implementing Cybersecurity Strategies?", Orrick.

[15] Apple, C. (2024). "ACT closes its first year with 3,500+ cybersecurity tools and several new high-risk communities", Global Cyber Alliance, 17. Dezember.

[16] Ariganello, J. (2022). "More is Less: The Challenge of Utilizing Multiple Security Tools", Anomali, 13. April.

[17] Atlantic Council (2025). "Scowcroft Center for Strategy and Security".

[18] AWS (2024). "Was ist SDLC (Software Development Lifecycle)?".

[19] Axon, L., Bouckaert, J., Creese, S., Akshay, J. & Saunders, J. (2025). "Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards", World Economic Forum.

[20] Ayenson, M., Forte, E., Mager, M., Bousseaden, S., Groenewoud, R., Nakajima, A., DeJesus, T., Ibarra, J., Pease, A., Donaher, C., Kerr, D., Uhlmann, J., Erkailo, T., King, J., VanNice, A., Faouzi, A, Suryanarayana, S. & Wilhoit, C. (2024). "Elastic Security Labs Global Threat Report 2024", Elastic Security Labs.

[21] Baams, L., Talmage, C. A. & Russell, S. T. (2017). "Economic costs of bias-based bullying" School psychology quarterly, in: APA PsycNet, 32(3), S. 422.

[22] Banco Santander, S. A. (2024). "Statement", 14. Mai.

[23] Barlett, C. P., Simmers, M. M., Roth, B. et al. (2021). "Comparing cyberbullying prevalence and process before and during the COVID-19 pandemic", in: J Soc Psychol, 15. Juni, 161(4): S. 408–418.

[24] Beiersmann, S. (2024). "Tunnelvision: Exploit umgeht VPN-Verschlüsselung", ZDnet, 08. Mai.

[25] Beuth, P. (2024). "Nicht nur die CDU wurde über Check-Point-Schwachstelle gehackt", Spiegel Netzwelt, 13. Juni.

[26] Beuth, P., Flüpke, Hoppenstedt, M., Kreil, M., Rosenbach, M. & Wilkin, R. (2024). "Wir wissen, wo dein Auto steht", Der Spiegel, 27. Dezember.

[27] Bhatnagar, B. & Hancock, J. (2024). "One in six school-aged children experiences cyberbullying, finds new WHO/ Europe study", WHO, 27. März.

[28] Bitkom (2024). "Erstmals mehr als 10 Milliarden Euro für Deutschlands Cybersicherheit", 23. Oktober.

[29] Bitkom (2024). “Social Engineering: Wenn der Hacker sich als Kollege ausgibt”, 11. Oktober.

[30] Bitkom (2024). “Wirtschaftsschutz 2024”, 28. August.

[31] Böhm, M. (2023). “FBI erzielt Erfolge gegen berüchtigte Hackergruppe”, Spiegel Netzwelt, 20. Dezember.

[32] Born, G. (2024). “Neue Warnung vor Schwachstelle CVE-2024-3400 in Palo Alto Networks Firewalls”, Born City, 27. April.

[33] Bracha, H. S. (2014). “Freeze, flight, fight, fright, faint: Adaptationist perspectives on the acute stress response spectrum”, CNS Spectrums 9(9), 679-685.

[34] Bradley, T. (2024). “Illuminating The Dark Corners Of Cyber Defense With Identity”, Forbes, 17. September.

[35] British Library (2023). “Cyber Incident Update: Information & FAQ's”.

[36] Brumfiel, G. (2019). “Trump Tweets Sensitive Surveillance Image Of Iran”, NPR.

[37] Brumfield, C. (2024). “Hijack of monitoring devices highlights cyber threat to solar power infrastructure”, CSO Online.

[38] Buchanan Technologies (2024). “Manged SIEM Pricing & Costs”.

[39] Bueger, C. & Liebetrau, T. (2023). “Critical maritime infrastructure protection: What's the trouble? Marine Policy,”, 155, p.105772.

[40] Bundesamt für Naturschutz (2021). “Seekabel”.

[41] BSI (o. J.). “Die Kryptografie hinter Passkey”.

[42] BSI. (o. J.). “Social Engineering – der Mensch als Schwachstelle”.

[43] BSI (2023). “Die Lage der IT-Sicherheit in Deutschland 2023”, 02. November.

[44] BSI (2024). “Aktive Crime-Gruppen in Deutschland”, 22. November.

[45] BSI (2024). “CyMon – der Cybersicherheitsmonitor”.

[46] BSI (2024). “Die Lage der IT-Sicherheit in Deutschland 2024”, 12. November.

[47] BSI (2024). “Einfluss von KI auf die Cyberbedrohungslandschaft”, 30. April, pp.4,10.

[48] BSI (2024). “Fehlerhaftes Update von Crowdstrike Falcon”, 19. Juli.

[49] BSI (2024). “Ivanti Cloud Services Appliance Schwachstellen werden aktiv ausgenutzt”, 20. September.

[50] BSI (2024). “Kritische Backdoor in XZ für Linux”, 03. April. CSW-Nr. 2024-223608-1132, Version 1.1.1.

[51] BSI (2024). “Umsetzung der NIS-2-Richtlinie für die regulierte Wirtschaft”, 24. Juli.

[52] BSI (2024). “Zero-Day Schwachstellen bei CyberAngriffen auf verschiedene Ivanti-Produkte genutzt”, 01. März.

[53] BSI (2024). “Version 1.4: Zero-Day Schwachstellen bei Cyber-Angriffen auf verschiedene Ivanti-Produkte genutzt”, 01. März.

[54] BSI (2025). “Wahlen in Deutschland 2025”.

[55] Bundesamt für Verfassungsschutz (BfV) (2024). “BfV Cyber Insight – The i-Soon-Leaks: Industrialization of Cyber Espionage”, Bundesamt für Verfassungsschutz – Counter Intelligence.

[56] Bundesamt für Verfassungsschutz (BfV) (2024). “Gefährdung der Bundestagswahl durch unzulässige ausländische Einflussnahme”.

[57] Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) (2024). “Cyberversicherungen: hohe Nachfrage – und hohe Risiken?”, 07. Februar.

[58] BKA (2022). “Sextortion: Das Bundeskriminalamt warnt vor sexueller Erpressung im Internet“, 21. Oktober.

[59] BKA (2023). “Polizeiliche Kriminalstatistik Bundesrepublik Deutschland. Straftatenkatalog 2023. V 1.0”.

[60] BKA (2024). “Bundeslagebild Cybercrime 2023”, 13. Mai., pp.17,24.

[61] BKA (2024). “Cybercrime: Festnahmen in Hessen und Rheinland-Pfalz – Erneuter Schlag gegen Underground Economy im Internet”, 01. November.

[62] BKA (2024). “Durchsuchungen bei mutmaßlichen Anführern der Online-Gruppierung ‚New World Order‘”, 03. September.

[63] BKA (2024). “Erfolgreicher Schlag gegen die Infrastruktur von digitalen Geldwäschern der Underground Economy”, 19. September.

[64] BKA (2024). “Operation ‚Endgame‘: Bundeskriminalamt und internationalen Partnern gelingt bisher größter Schlag gegen weltweite Cybercrime”, 30. Mai.

[65] BKA (2024). "Operation ‚Power OFF': weltweiter Schlag gegen Cybercrime-Infrastruktur", 11. Dezember.

[66] BKA (2025). "Internationale Operation Talent: Abschaltung von nulled.to und cracked.io".

[67] Business Wire (2024). "Message from the International Cable Protection Committee: Recent Events Involving Submarine Cables in the Red Sea".

[68] Canadian Centre for Child Protection (C3P) (2022). "An Analysis of Financial Sextortion Victim Posts".

[69] CASIO Computer Co., Ltd. (2024). "Casio issues apology and notice concerning personal information leak due to unauthorized access to server", 18. Oktober.

[70] Chanel, O. & Chichilnisky, G. (2009). "The influence of fear in decisions: Experimental evidence". Journal of Risk and Uncertainty 39, 271-298.

[71] Check Point Team (2024). "2025 Cyber Security Predictions – The Rise of AI-Driven Attacks, Quantum Threats, and Social Media Exploitation", 28. Oktober.

[72] Clark, H. (2024). "What is the Software Development Life Cycle (SDLC)?", The Product Manager, 29. Oktober.

[73] Colvin, T., Karcz, J. & Wusk, G. (2023). "Office of Technology, Policy, and Strategy Cost and Benefit Analysis of Orbital Debris Remediation", NASA Office of Technology, Policy, and Strategy.

[74] Constantin, L. (2024) "Top 7 zero-day exploitation trends of 2024", CSO Online, 23. Dezember.

[75] Copelouzos Group (2024). "'GREGY' Interconnector – Copelouzos Group".

[76] Coveware (2024). "Quarterly Report".

[77] Creaplus (2023). "Too many solutions can make your organization less secure".

[78] Cross, C., Holt, K. & Holt, T. J. (2023). "To pay or not to pay: An exploratory analysis of sextortion in the context of romance fraud", in: Criminology & Criminal Justice, 11. Februar, 0(0).

[79] CrowdStrike (2024). "Technical Details: Falcon Content Update for Windows Hosts", CrowdStrike Executive Viewpoint, 20. Juli.

[80] Cybersecurity and Infrastructure Security Agency (CISA) (2023). "Zero Trust Maturity Model – Version 2.0", Cybersecurity Division.

[81] Cybersecurity and Infrastructure Security Agency (CISA) (2024). "Mobile Communications Best Practice Guidance | CISA".

[82] Cybersecurity and Infrastructure Security Agency (CISA) (2024). "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure", 07. Februar.

[83] Datensicherheit.de (2020). "Software: 76% der Anwendungen mit mindestens einer Sicherheitslücke".

[84] Deere & Company (2023). "Deere Debuts New Planting Technology & Electric Excavator During CES 2023".

[85] Deloitte (2024). "Global Future of Cyber Survey 2024", 22. Oktober.

[86] Deutschlandfunk (2025). "Sabotage in der Ostsee. Was steckt hinter der Zerstörung der Unterseekabel?", 20. Januar.

[87] Di Battista, A., Grayling S., Játiva, X., Leopold, T., Li, R., Sharma, S. & Zahidi, S. (2025). "World Economic Forum Future of Jobs Report 2025", World Economic Forum.

[88] Dr. Datenschutz (2024). "Kritische Linux XZ-Backdoor bedroht digitale Infrastruktur", 19. April.

[89] Drive Lock (2024). "Cyberangriffe auf OT: Warum Unternehmen dringend in OT-Sicherheit investieren müssen", 24. April.

[90] Epp, S. (2024). "KI-Angriffe mit KI-Abwehr schlagen", Security Insider, 19. September.

[91] Eschlberger, S., Vereno, D., Polanec, K. & Neureiter, C. (2024). "Introducing Cybersecurity Toolbox: A modelling framework for smart grid security".

[92] Europäische Union (2022). "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)".

[93] European Commission (2024). "IRIS2 | Secure Connectivity – European Commission", defence-industry-space.ec.europa.eu.

[94] European Space Agency (2024). "Active Debris Removal".

[95] European Space Agency (2024). "Sentinel-1B Successfully Passivated – Sentinel Online", Sentinel Online.

[96] European Union Agency for Cybersecurity (ENISA) (2024). "ENISA Threat Landscape 2024", 19. September., pp.7-8,13-14,26,28,46,50-51,53,78-80,83.

[97] European Union Agency for Cybersecurity (ENISA) (2024). "Foresight Cybersecurity Threats for 2030 – Update".

[98] European Union Agency for Law Enforcement Cooperation (Europol) (2017). "Online sexual coercion and extortion as a form of crime affecting children Law enforcement perspective", 19. Juni.

[99] European Union Agency for Law Enforcement Cooperation (Europol) (2022). "Facing reality? Law enforcement and the challenge of deepfakes, an observatory report from the Europol Innovation Lab", 28. April.

[100] European Union Agency for Law Enforcement Cooperation (Europol) (2024). "Internet Organised Crime Threat Assessment 2024", 22. Juli., p.10,12,24.

[101] Falco, G. (2024). "Hybrid Space-Submarine Architecture Ensuring Infosec of Telecommunications (HEIST)".

[102] FasterCapital (o. J.). "Angstmarketing Die Psychologie der Angst Ihre Auswirkungen auf Geschaeft und Marketing verstehen".

[103] Federal Bureau of Investigation (FBI) (o. J.). "Sextortion".

[104] Federal Communications Commission (2016). "STATEMENT OF COMMISSIONER JESSICA ROSENWORCEL".

[105] Financial Times (2024). "Delta Airlines sues CrowdStrike over $500mn losses from flight cancellations", 17. Januar.

[106] Fischer, S. M. & Bilz, L. (2024). "Mobbing und Cybermobbing an Schulen in Deutschland: Ergebnisse der HBSC-Studie 2022 und Trends von 2009/10 bis 2022", in: Journal of Health Monitoring, S. 46–67.

[107] Flügge, A. (o. J.). "Die Komplexität von Softwaresystemen", Object Systems.

[108] Frankfurter Allgemeine Zeitung (2024). "40 Jahre Haft wegen Verrat von CIA-Hackerprogrammen", 02. Februar.

[109] Fraunhofer-Institut für Entwurfstechnik Mechatronik IEM (2024). "Cyber Resilience Act: Drei Sofortmaßnahmen für Unternehmen", 11. Oktober.

[110] Fraunhofer-Institut für System- und Innovationsforschung ISI, im Auftrag von TA-SWISS Stiftung für Technologiefolgen-Abschätzung (2024). "Deepfakes und manipulierte Realitäten", 18. Juni.

[111] Fuest, B. (2024). "Und dann fällt dem Microsoft-Mitarbeiter eine halbe Sekunde Verzögerung auf", Welt, 12. April.

[112] Gámez-Guadix, M., Mateos-Pérez, E., Wachs, S., Wright, M., Martínez, J. & Íncera, D. (2022). "Assessing image-based sexual abuse: Measurement, prevalence, and temporal stability of sextortion and nonconsensual sexting ('revenge porn') among adolescents", in: Journal of Adolescence, 94(5), S. 789–799.

[113] Gámez-Guadix, M., Sorrel, M. A. & Martínez-Bacaicoa, J. (2023). "Technology-facilitated sexual violence perpetration and victimization among adolescents: A network analysis", in: Sexuality research and social policy, 20(3), S. 1000-1012.

[114] Gartner (2022). "Gartner Identifies Top Security and Risk Management Trends for 2022", 07. März.

[115] Gartner (2024). "Gartner Forecasts Global Information Security Spending to Grow 15% in 2025", Gartner, 28. August.

[116] Gartner (2024). "Information Security Spending: What does the future hold?", 27. November.

[117] Generalstaatsanwaltschaft Karlsruhe (2025). "Anklage gegen mutmaßlichen Cybererpresser der Württembergischen Staatstheater Stuttgart".

[118] Gillin, P. (2024). "Cybersecurity tool sprawl is out of control – and it's only going to get worse", SiliconeANGLE, 5 August.

[119] Govan, C. (2023). "Unlocking Satellite Connectivity: IoT's Reign of Coverage", floLIVE.

[120] Grealy, A. (2024). "KI-gestützte Cybersicherheit: Prognosen für das Jahr 2025", Armis, 16. Dezember.

[121] Greenberg, A. (2024). "Emerging Threats: Cybersecurity Forecast 2025", Google Cloud, 13. November.

[122] Greene, T.C. (2002). "MS Struggles to discredit Linux", The Register, 2. Januar.

[123] GSM Association (2024). "Massive IoT | Internet of Things | GSMA", Massive IoT.

[124] Hansen, S. (2023). "Cybersecurity Paradox: How too many solutions makes you less secure", Cryptomathic, 02. Juni.

[125] Haufe (2024). "Cyber Resilience in Deutschland: Ein alarmierender Bericht", 14. November.

[126] Hays (2024). "Global Cyber Security Report 2024 – Beyond Traditional Cyber Talent".

[127] Hayward, L. (2023). "Global Navigation Satellite System (GNSS) and Satellite Navigation Explained", Advanced Navigation.

[128] Hase, M. (2019). "Definition. Was ist Vendor Lock-in?", 20.September.

[129] Heise online (2024). "CDU-Angriff: Lücke in Check Point Gateway soll Einfallstor gewesen sein", 03. Juni.

[130] Henderson Vaughan, E. (2024). "NCMEC Releases New Sextortion Data", in: NCMEC, 15. April.

[131] Hennigan, W.J. (2024). "What One Russian Satellite Tells Us About the Future of Nuclear Warfare. The New York Times", 5. Dezember.

[132] Henry, N. & Umbach, R. (2024). "Sextortion: Prevalence and correlates in 10 countries", in: Computers in Human Behavior, Volume: 158.

[133] Henry, N., McGlynn, C., Flynn, A., Johnson, K., Powell, A. & Scott, A. J. (2020). "Image-based sexual abuse: A study on the causes and consequences of non-consensual nude or sexual imagery", in: Routledge, 11. Juni.

[134] Herder, C. (2024). "CISA Takedown of Ivanti Systems Is a Wake-up Call", Dark Reading, 09. Juli.

[135] Hiscox (2024). "Hiscoy Cyber Readiness Report 2024".

[136] Holtermann, F. (2025). "DeepSeek könnte heimlich OpenAI-Daten abgeschöpft haben", Handelsblatt, 29. Januar.

[137] Horten, B., Steffan, C., Weinand, M. & Brettel, H. (2024). "Kriminologischer Beitrag: Sextortion – Intime Aufnahmen als Druckmittel.", in: Journal Club, 21. Juni.

[138] Hotarek, F. (2023). "Die Identitätssicherheit als Basis von Zero Trust", it-daily.net, 13. August.

[139] Hradický, J. M., Strauszová, K. & Strapeková, O. (2024). "GLOBSEC Grid Transition Index 2024", GLOBSEC Grid Transition Index 2024.

[140] Hubback, J. (2020). "Research Report: Cybersecurity Technology Efficacy. Is cybersecurity the new 'market for lemons'?".

[141] Hughes, M. & Temsamami, K. (2025). "Capturing the cybersecurity dividend" IBM Institute for Business Value.

[142] IBM Corporation (o. J.). "Was ist Cyber-Resilienz?".

[143] IBM Corporation (2024). "IBM Security X-Force Threat Intelligence Index 2024".

[144] IBM Corporation (2024). "Cost of a Data Breach Report 2024".

[145] Information Systems Audit and Control Association (ISACA) (2024). "State of Cybersecurity 2024", 01. Oktober, pp.31-32.

[146] Insikt Group (2024). "H1 2024: Malware and Vulnerability Trends Report", Recorded Future, 10. September.

[147] Intel 471 (2024). "The 471 Cyber Threat Report 2024", 06. Mai.

[148] International Committee of the Red Cross (o. J.). "Cyber and information operations".

[149] International Monetary Fund (IMF) (2025). "GDP, current prices in billions of US dollars".

[150] International Telecommunication Union Development Sector (2024). "Measuring digital development – Facts and Figures 2024", ITU Publications.

[151] Internet Watch Foundation (IWF) (2023). "Hotline reports 'shocking' rise in the sextortion of boys", 18. September.

[152] INTERPOL (2022). "Asia: Sextortion ring dismantled by Police", 05. September.

[153] IT-Sicherheit (2024). "Mehr Widerstandsfähigkeit für OT-Systeme", 03. Juli.

[154] Janis, I.L. (1982). "Decisionmaking under stress", In Goldberger, L., Breznitz, S. (eds.) Handbook of stress. New York: Free Press, pp. 69-87.

[155] Jaschinsky, M. (2025). "Aktuelle Netzfrequenz (47,5-52,5Hz) – Netzfrequenz.info", NETZFREQUENZ.

[156] Jaye Tillson, J. (2024). "The Crumbling Castle", Cyber Defense Magazine, 02. Februar.

[157] Joos, T. (2024). "Die Gefahren von Schatten-IT", IP Insider, 08. Mai.

[158] Kern, M., Landauer, M., Skopik, F. & Weippl, E. (2024). "A logging maturity and decision model for the selection of intrusion detection cyber security solutions". Computers & Security 141, 103844.

[159] Kim, J., van Schaik, S., Genkin, D. & Yarom, Y. (2023). "iLeakage: Browser-based Timerless Speculative Execution Attacks on Apple Devices".

[160] Klein, D. (2021). "Relying on firewalls? Here`s why you'll be hacked", Network Security 1, 9-12.

[161] Knop, D. (2024). "Kritische Fortinet-Sicherheitslücke wird angegriffen", Heise Online, 10. Oktober.

[162] Koch, M.-C. (2024). "Sextortion-Fälle in den USA: Kriminelle schicken Bilder von der Umgebung mit", in heise, 05. September.

[163] Kochenderfer-Ladd, B., Ladd, G. W. & Thibault, S. A. (2021). "School bullying and peer victimization: Its role in students' academic achievement" in: P. K. Smith & J. O. Norman (Eds.), The Wiley Blackwell handbook of bullying: A comprehensive and international review of research and intervention (pp. 619–638), 15. März.

[164] Koopman, E. (2024). "Remote Code Execution on Ivanti Products Found in the Wild", CliftonLarsonAllen, 19. Februar.

[165] Kovacs, E. (2024). "Casio Confirms Data Breach as Ransomware Group Leaks Files", Security Week, 14. Oktober.

[166] KPMG (2024). “Control System Cybersecurity Annual Report 2024”.

[167] KPMG (2024). “KPMG Cybersecurity Survey 2024”, 13. Mai.

[168] Krämer, M.J. (2024). “XZ Utils-Vorfall: Open Source als Software Supply Chain-Falle”, ZDNet, 09. April.

[169] Kreil, M. & Flüpke (2024). “Wir wissen wo dein Auto steht”, Media.ccc.de.

[170] Kuhlenkamp, F. (2024). “Angriffe auf die deutsche Wirtschaft nehmen zu”, Bitkom, 28. August.

[171] Kuhlenkamp, F. (2024). “Erstmals mehr als 10 Milliarden Euro für Deutschlands Cybersicherheit ”, Bitkom, 23. Oktober.

[172] Labašová, D., Dančo, M. (2025). “Ransomware attack on Slovakia’s real estate register causes nationwide outage of all services and databases containing information on immovable property rights”, Kinstellar.

[173] Lakshmanan, R. (2024). “Researchers Uncover Vulnerabilities in Solarman and Deye Solar Systems”, The Hacker News.

[174] Landeskriminalamt Nordrhein-Westphalen (LKA NRW) (2020). “Erpressungsversuche via E-Mail. Präventionshinweise für Betroffene”.

[175] Landtag von Baden-Württemberg (2024). “Schlag gegen mutmaßliche Cybererpresser – hoher Schaden”, 10. Oktober.

[176] Landtag von Baden-Württemberg (2024). “Sextortion: Erpressungen mit Nacktaufnahmen nehmen zu”, 27. Mai.

[177] Ledesma, J. (2023). “Why Aren’t Cybersecurity Tools Living up to the Hype?”, Bitdefender.

[178] Lenaerts-Bergmans, B. (2023). “Angriffsvektoren: Was sie sind und wie sie ausgenutzt werden”, CrowdStrike, 07. Dezember.

[179] Lister, T. & Fylyppov, O. (2022). “Russians plunder $5M farm vehicles from Ukraine - to find they’ve been remotely disabled”, CNN.

[180] Luber, S. & Schmitz, P. (2021). “Was ist Endpoint Detection and Response (EDR)?”, Security Insider, 05.05.2021.

[181] Lyngaas, S. (2024). “Cyberattack forces major US health care network to divert ambulances from hospitals”, CNN, 10. Mai.

[182] Maloney, D. (2023). “Under The Sea: Optical Repeaters For Submarine Cables”, Hackaday.

[183] manager magazin (2002). “Globalstar: Jäher Absturz”.

[184] Mandiant (2024). “IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders”, Google Cloud Blog.

[185] McAfee, LLC (2024). “RockYou2024: das größte Kennwort-Datenleck in der Geschichte”, 12. Juli.

[186] McKerchar, R. (2024). “Pacific Rim: Inside the Counter-Offensive — The TTPs Used to Neutralize China-Based Threats”, Sophos News.

[187] Mäurer, D.K. (2024). “Bedeutender Schlag gegen die Cybercrime-Szene”, Tagesschau, 30. Mai.

[188] Malwarebytes Inc. (2024). “ThreatDown 2024 State of Ransomware”, 20. August.

[189] Manuel, R. (2024). “Pro-Russia Hackers Attack Japanese Liberal Democratic Party Website”. The Defence Post, 18. Oktober.

[190] Medienpädagogischer Forschungsverband Südwest (2024): “JIM-Studie 2024 – Jugend, Information, Medien”.

[191] Metz, C. (2024). “OpenAI’s internal AI details stolen in 2023 breach, NYT reports”, Reuters, 5. Juli.

[192] Microsoft Corporation (2024). “Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard”, 19. Januar.

[193] Microsoft Corporation (2024). “Microsoft Digital Defense Report 2024”.

[194] Minchin, J. (2025). “Eagle S could have cut more cables, says Finnish police”, Lloyd’s List.

[195] Moody, R. (2025). “Ransomware roundup: 2024 end-of-year report”, Comparitech Ltd., 09. Januar.

[196] Moreno. E (2024). “Ist Ihr Unternehmen wirklich gegen Cyberangriffe versichert?”, Chemie Technik, 18. März.

[197] Morgan, E. (2024). “Eroding Global Stability: The Cybersecurity Strategies Of China, Russia, North Korea, And Iran”, Irregular Warfare, 01. August.

[198] Müller, Dr. D. (2024). “KI befeuert Cyber-Angriffstechniken”, IT-Business, 16. Februar.

[199] Munro, K. (2024). “GPS Spoofing: It’s About Time, Not Just Position”, PenTestPartners.

[200] Mutzbauer, J. (2024). “Phishing-Attacke: Deutschlandweiter Hackerangriff auf IHK-Unternehmen”, CSO online, 18. März.

[201] Naraine, R. (2024). “Ivanti CEO Vows Cybersecurity Makeover After Zero-Day Blitz”, Security Week, 04. April.

[202] National Audit Office (2025). “Cyber threat to UK government is severe and advancing quickly, spending watchdog finds”.

[203] National Coordination Office for Space-Based Positioning, Navigation, and Timing (2023). "GPS.gov: Timing Applications", Gps.gov.

[204] Nawrocki, M. (2024). "DDoS Attacks Against Japan", NetScout, 17. Oktober.

[205] Netgate (2024). "The Top Cybersecurity Statistics for 2024".

[206] NHS England London (2024). "Update on cyber incident: clinical impact in South East London – Friday 14 June 2024".

[207] Nilsson M. G., Tzani-Pepelasis C., Ioannou M. & Lester D. (2019). "Understanding the link between Sextortion and suicide", in: International Journal of Cyber Criminol 13(1):55–69.

[208] Norddeutscher Rundfunk (NDR) (2024). "Cyberangriff auf Landesbehörden in MV: Internetseiten lahmgelegt", 24. Mai.

[209] North Atlantic Treaty Organization (NATO) (2024). "Cyber defence", 30. Juli.

[210] North Atlantic Treaty Organization (NATO) (2025). "NATO launches 'Baltic Sentry' to increase critical infrastructure security".

[211] Office of Communications (Ofcom) (2024). "Children and Parents. Media Use and Attitudes Report", 19. April.

[212] O'Flaherty, K. (2024). "CrowdStrike Reveals What Happened, Why—And What's Changed", Forbes, 07. August.

[213] O'Higgins Norman, J. (2020). "Tackling bullying from the inside out: Shifting paradigms in bullying research and interventions", in: Internation Journal of Bullying Preventition 2(3):161–169.

[214] O'Malley, R. L. (2023). "Short-term and long-term impacts of financial Sextortion on victim's mental well-being", in: Journal of Interpers Violence 38(13–14):8563–8592.

[215] O'Malley, R. L. & Holt, K. M. (2022). "Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime", in: Journal of interpersonal violence, 37(1-2), 258-283.

[216] Österreichische Rundfunk (ORF) (2024). "Cyberangriffe auf ÖVP und SPÖ", 23. September.

[217] Ohm, M., Plate, H. Sykosch, A. & Meier, M. (2020). "Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks".

[218] OpenKRITIS (2024). "NIS2-Umsetzungsgesetz: Neuerungen für die Cybersicherheit in Deutschland".

[219] OpenVPN (2023). "Navigating Cybersecurity: Choosing Between All-In-One Platforms and Point Solutions".

[220] OPSGROUP Team (2024). "GPS Spoofing: Final Report of the GPS Spoofing WorkGroup", GPS Spoofing: Final Report.

[221] OPSWAT (2024). "Was ist OT Security?", 02. Juli.

[222] Paquet-Clouston, M., Romiti, M., Haslhofer, B. & Charvat, T. (2019). "Spams meet cryptocurrencies: Sextortion in the bitcoin ecosystem", in: ACM Digital Library, S. 76-88.

[223] Parasoft (2023). "Aufbau von Resilienz in der Softwareentwicklung: Zurück zu den Grundlagen", 18. Dezember.

[224] Patchin, J. W. & Hinduja, S. (2020). "Sextortion among adolescents: 'Results from a national survey of U.S. youth.'", in: Sexual Abuse: A Journal of Research and Treatment, 32(1), 30–54.

[225] Patnaik, A. (2024). "Rising Tide of Software Supply Chain Attacks: An Urgent Problem", DarkReading, 12. September.

[226] Petrosyan, A. (2024). "Estimated cost of cybercrime worldwide 2018-2029", Statista, 30. Juli (Data for 2025).

[227] Pfaffenberger, B. (2000). "The rhetoric of dread: Fear, uncertainty, and doubt (FUD) in information technology marketing". Knowledge, Technology & Policy 13, 78-92.

[228] Pfliegl, K. (2024). "CrowdStrike: Das waren die Folgen für deutsche Unternehmen", Digital Business, 20. September.

[229] Phillips-Wren, G. & Adya. M. (2020). "Decision making under stress: the role of information overload, time pressure, complexity, and uncertainty", Journal of Decision Systems 29, 213-225.

[230] Pluta, W. (2008). "Iridium-Insolvenzverfahren beendet", Golem.de.

[231] Polizeiliche Kriminalprävention (o. J.). "Sextortion. Vom harmlosen Flirt zur organisierten Erpressung".

[232] Polizeiliche Kriminalprävention der Länder (ProPK) & Bundesamt für Sicherheit in der Informationstechnik (BSI) (2024). "Cybersicherheitsmonitor 2024: Kurzbericht zur Befragung zur Cybersicherheit".

[233] Portuguese Space Agency (2020). "ADRIOS (Active Debris Removal/ In-Orbit Servicing)", Portugal Space Agency.

[234] Poudel, S. S. (2024). "XZ Utils Backdoor: Sicherheitslücke in der Software-Supply-Chain", It-Sicherheit, 17. April.

[235] Poulsen, K. (2010). "Hacker Disables More Than 100 Cars Remotely", Wired.

[236] Powell, A. & Henry, N. (2019). "Technology-facilitated sexual violence victimization: Results from an online survey of Australian adults", in: Journal of Interpersonal Violence, Volume: 34(17), S.3637–3665.

[237] PricewaterhouseCoopers GmbH (PwC) (2024). "Cybersecurity + geopolitical conflict: What boards and CEOs should know and act upon", 15. Januar.

[238] PricewaterhouseCoopers GmbH (PwC) (2024). "Digital Trust Insights 2025".

[239] Privette, M. (2025). "The State of the Cybersecurity Market in 2024".

[240] Pultarova, T. & Howell, E. (2025). "Starlink: SpaceX's satellite internet project", Space.com.

[241] Raffile, P., Goldenberg, A., McCann, C. & Finkelstein, J. (2024). "A digital pandemic: uncovering the role of 'yahoo boys' in the surge of social media-enabled financial sextortion targeting minors", in: NCRI, 30. Januar.

[242] Rathert, T. (2024). "State of Ransomware 2024: 500 Prozent höhere Lösegeldzahlungen", connect, 06. Mai.

[243] Ray, A. & Henry, N. (2025). "Sextortion: A Scoping Review. Trauma, Violence, & Abuse", in: Sage Journmals Volume: 26(1), 138-155.

[244] Reuters Staff (2024). "Finnair pauses some Estonia flights due to GPS interference. Reuters", 29. April.

[245] Ribeiro, A. (2024). "Growing convergence of geopolitics and cyber warfare continue to threaten OT and ICS environments in 2024", 18. Februar.

[246] Rojoef, M. (2024). "Pro-Russia Hackers Attack Japanese Liberal Democratic Party Website", The Defense Post, 18. Oktober.

[247] Roman, N. (2024). "Global Status Of Anti-Satellite (ASAT) Weaponry And Testing | ACE", The Alliance for Citizen Engagement.

[248] Rundfunk Berlin-Brandenburg (RBB) (2024). "AfD Brandenburg meldet Hackerangriff auf Internetseite", 29. August.

[249] Rupp, C. (2024). "Navigating the EU Cybersecurity Policy Ecosystem", interface, 27. Juni.

[250] Scarfone, K. (2024). "Die größten OT-Bedrohungen und Security-Herausforderungen", Computer Weekly, 30. August.

[251] Schirrmacher, D. (2024). "Nach mehreren IT-Security-Vorfällen: Ivanti gelobt in offenem Brief Besserung", Heise Online, 08. April.

[252] Schubert, F. (2024). "Sicherheitslücken in Ivanti Connect Secure VPN", Leipziger Zeitung, 02. Dezember.

[253] Schultze-Krumbholz, A., Höher, J., Fiebig, J. et al. (2014). "Wie definieren Jugendliche in Deutschland Cybermobbing? Eine Fokusgruppenstudie unter Jugendlichen einer deutschen Großstadt", in: Praxis der Kinderpsychologie und Kinderpsychiatrie, 63 (2014) 5, S. 361-378.

[254] Schwartz, K.D. (2024). "Can you have too many security tools?", CIO, 29. August.

[255] Schwarz Digits (2024). "Eine quantitative Befragung der Unternehmen in Deutschland zum Thema Cybersecurity".

[256] Seaton, W. & Pandit, K. (2024). "New VPN Risk Report: 56% of Enterprises Attacked via VPN Vulnerabilities", Zscaler, 07. Mai.

[257] Security Insider (2024). "Internationale Ermittler zerschlagen ‚schädlichste Hackergruppe der Welt'", Security Insider, 21. Februar.

[258] Singh, N. (2024). "Palo Alto Networks Surveys the State of OT Security", Palo Alto, 20. März.

[259] SINUS (2023). "Ergebnisse einer Repräsentativ-Umfrage unter Jugendlichen 2023/2023".

[260] Skadden (2024). "Navigating the New Cybersecurity Landscape: Key Implications of the EU's NIS 2 Directive", 11. Oktober.

[261] SkAI Data Services and Zurich University of Applied Sciences – Centre for Aviation (2024). "Live GPS Spoofing and Jamming Tracker".

[262] Snider, S. (2024). "Snowflake Denies Responsibility for Ticketmaster, Santander Breaches", Information Week, 03. Juni.

[263] Sokolov, D. (2024). "Zerodays bei Ivanti aktiv genutzt: Connect Secure und Policy Secure sinds nicht", Heise Online, 10. Januar.

[264] Sonatype (2024). "10th Annual State of the Software Supply Chain".

[265] Sophos Ltd. (2024). "Sophos 2024 Threat Report: Cybercrime on Main Street", März.

[266] Spanien aktuell (2025). "Rekordsumme: Ransomware-Opfer zahlen 2024 fast 460 Millionen US-Dollar", 01. Januar.

[267] Splunk (2024). "State of Security: The Race to Harness AI".

[268] Stadt Aschaffenburg (2024). "Hackerangriff: Rathaus am Montag wieder geöffnet", 15. November.

[269] Stankovski, A., Gjorgiev, B., Locher, L. & Sansavini, G. (2023). "Power Blackouts in Europe: Analyses, Key insights, and Recommendations from Empirical Evidence", Joule, 7(11), pp.2468–2484.

[270] Starcke, K. & Brand, M. (2012). "Decision making under stress: A selective review. Neuroscience & Biobehavioral Reviews", 36(4), 1228-1248.

[271] Stary, V. (2024). "Kaspersky stellt Cybersecurity-Trends für 2025 vor", Netzwoche, 19. November.

[272] Statista (2022). "Estimated costs of cybercrime globally 2016-2027".

[273] Statista (2024). "Cybersecurity – Worldwide".

[274] Statista (2024). "Estimated cost of cybercrime worldwide 2018-2029".

[275] Statista (2024). "Number of common IT security vulnerabilities and exposures (CVEs) worldwide from 2009 to 2024 YTD".

[276] Stöckel, M. (2025). "Datenleck bei KI-Startup: Chatverläufe von DeepSeek frei zugänglich im Netz", Golem.de, 30. Januar.

[277] Subbotin, A. (2024). "CrowdStrike-Ausfall: Globaler IT-Stillstand und Workaround", Byte Snipers, 19. Juli.

[278] Süddeutsche Zeitung (2024). "Sextortion: Vom Flirt zur Erpressung", 29. Oktober.

[279] Sutton, H.I. (o. J.). "H I Sutton – Covert Shores".

[280] Sutton, H.I. (2020). "How Russian Spy Submarines Can Interfere With Undersea Internet Cables", Forbes, 19. August.

[281] Tagat, A., Phokeer, A. & Kreitem, H. (2024). "Net Loss: an Econometric Method to Measure the Impact of Internet Shutdowns", ACM Journal on Computing and Sustainable Societies, 2(2).

[282] Tagesschau (2024). "Die schleichende Gefahr vor der Europawahl", 31. Mai.

[283] Tagesschau (2024). "Konzerktkarten-Verkäufer Ticketmaster – 560 Millionen Kunden von Hackerangriff betroffen", 01. Juni.

[284] Tagesschau (2024). "Schwerer Cyberangriff auf die CDU", 01. Juni.

[285] Tagesschau (2024). "Verfassungsschutz warnt vor Beeinflussung der Wahl", 29. November.

[286] Tagesschau (2025). "Schweden geht nicht mehr von Sabotage aus", 03. Februar.

[287] Tak, S. & Catsambis, S. (2023). "Video games for boys and chatting for girls?: Gender, screen time activities and academic achievement in high school", in: ifip Educ Inf Technol 28, 15415–15443.

[288] Tang, Y., Dananjayan, S., Hou, C., Guo, Q., Luo, S. & He, Y. (2021). "A Survey on the 5G Network and Its Impact on agriculture: Challenges and Opportunities", Computers and Electronics in Agriculture, 180, p.105895.

[289] Taylor, R. (2024). "Managed IT Services Pricing: What to expect in 2024", Cybercommand, 26. Juli.

[290] TeleGeography (2019). "Submarine Cable Map".

[291] TeleGeography (2022). "Submarine Cable FAQs".

[292] The Tor Project, Inc (2019). "Tor Project: Overview".

[293] The White House (2021). "Executive Order on Improving the Nation's Cybersecurity", The White House, Briefing Room, 12. Mai.

[294] Thiel, C. (2020). "Liebesschwindel im Cyberspace", in: Rüdiger B (Hrsg) Cyberkriminologie. Kriminologie für das digitale Zeitalter. Springer VS, Wiesbaden, S 241–267, 01. April.

[295] Thorn & National Center for Missing and Exploited Children (NCMEC) (2024). "Trends in Financial Sextortion: An investigation of sextortion reports in NCMEC CyberTipline data", 24. Juni.

[296] Tidy, J. (2024). "Dead in 6 hours. How Nigerian sextortion scammers targeted my son", in: BBC, 09. Juni.

[297] Tokmetzis, D. (2024). "Almost 200 Russian Ships Suspected of Spying in the North Sea", Follow the Money – Platform for Investigative Journalism.

[298] Toulas, B. (2024). "Cisco warns of large-scale brute-force attacks against VPN services", Bleeping Computer, 16. April.

[299] Toulas, B. (2025). "New Apple CPU side-channel attacks steal data from browsers", BleepingComputer, 28. Januar.

[300] Trevino, A. (2024). "Acht häufige Angriffsvektoren, die Unternehmen kennen müssen", Keeper Security, 04. April.

[301] Trio Team (2024). "Die Bedeutung der XZ-Backdoor-Bedrohung verstehen: Ein verdeckter Einbruch in Open-Source-Software", 20. Oktober.

[302] TÜV NORD GROUP #explore (2020). "Tiefseekabel als Datenautobahn".

[303] TÜV Rheinland (2024). "Supply-Chain-Attacken".

[304] United Nations (2024). "United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes".

[305] United States Air Force Public Affairs (2018). "First GPS III Satellite Successfully Launched".

[306] United States Immigration and Customs Enforcement (ICE) (2024). "Sextortion".

[307] U.S. General Services Administration (2025). "SAM.gov", Sam.gov.

[308] Vaughan-Nichols, S.J. (2020). "How Microsoft went from Linux is a cancer to Microsoft Loves Linux", InsiderPro (archiviert), 11. Oktober.

[309] Vellante, D. & Bradley, E. (2024). "Breaking Analysis: Security budgets are growing but so is vendor sprawl", theCUBEResearch, 27. April.

[310] Verbraucherzentrale (2024). "Umfrage: Account gehackt – das erwarten Betroffene von den Unternehmen", 13. November.

[311] Verizon, (2024). "Data Breach Investigations Report 2024", 11. Juli.

[312] Vicens, A.J. (2024). "Low-level cybercriminals are pouncing on CrowdStrike-connected outage", Cyberscoop, 23. Juli.

[313] Vicens, A.J. (2024). "US adds 9th telcom to list of companies hacked by Chinese-backed Salt Typhoon cyberespionage", Reuters, 27. Dezember.

[314] Volpenhein, S. (2024). "Ascension was hacked after worker mistakenly downloaded malicious file Unclear how many patients' data exposed", Milwaukee Journal Sentinel, 13. Juni.

[315] V. Samson, F. (2024). "Nach XZ-Backdoor: Open-Source-Software als Risiko oder strategischer Vorteil?", Heise Online, 20. April.

[316] Waasdorp, T. E. & Bradshaw, C. P. (2015). "The overlap between cyberbullying and traditional bullying", in: Journal of adolescent health, 56(5), 483-488.

[317] Wall, M. (2024). "SpaceX launches 6th batch of next-gen US spy satellites from California (video)", Space.com.

[318] Walsh, W. A. & Tener, D. (2022). "If you don't send me five other pictures I am going to post the photo online: A qualitative analysis of experiences of survivors of sextortion", in: Journal of child sexual abuse, 31(4), 447-465.

[319] Walther, E. (2024). "Die Geopolitik hat Einzug in unsere Netze gehalten: Einblicke in den Cyber Underground", Handelsblatt Live, 26. Juli.

[320] Wang, Q., Li, W., Yu, Z., Imran, M., Ansari, S., Sambo, Y., Wu, L., Li, Q. & Zhu, T. (2023). "An Overview of Emergency Communication Networks", Remote Sensing, 15(6), pp.1595–1595.

[321] Weishaupt, J. (2019). "Competing in Space: Space-Based Weapons", 31. Oktober, Defense Visual Information Distribution Service.

[322] Weissmann, P. (2024). "NIS2 Umsetzungsgesetz", OpenKritis.

[323] Welter, I. (2024). "Der Kampf gegen Erpressung mit Nacktbildern", in: zdfheute, 17. August.

[324] WeProtect Global Alliance (2024a). "A web of deceit. Financial sexual extortion of children and young people. Briefing Paper".

[325] WeProtect Global Alliance (2024b). "Tackling the rising incidence of financial sexual extortion, Takeaways from a cross-sector innovation forum", in: PA-consulting.

[326] Whitehurst, L. (2022). "FBI: Steep climb in teens targeted by online 'sextortion'", in: AP News, 19. Dezember.

[327] Whitty, M. T. & Buchanan, T. (2016). "The online dating romance scam: The psychological impact on victims-both financial and non-financial", in: Criminology & Criminal Justice, 16(2), 176–194.

[328] WirtschaftsWoche (2024). "CrowdStrike-Panne legte 8,5 Millionen Windows-Geräte lahm", 21. Juli.

[329] Wiseman, J. (2022). "GPSJam GPS/GNSS Interference Map", gpsjam.org.

[330] Wisernotify (2025). "15 Fake Review Statistics You Can't Ignore (2025)".

[331] Wittenberg, K. (2024). "Sicherheitsexperten schlagen Alarm: Globale Welle von Hackerangriffen auf VPN-Dienste", Chip, 19. April.

[332] Wolak, J. & Finkelhor, D. (2016). "Sextortion: Keys findings from an online survey of 1631 victims", in: Crime Against Children Research Center & Thorn.

[333] Wolak, J., Finkelhor, D., Walsh, W. & Treitman, L. (2018). "Sextortion of minors: Characteristics and dynamics", in: Journal of Adolescent Health, 62(1), 72–79.

[334] Yadav, Y. (2022). “India becoming sextortion capital of the world?”, in: The Times of India, 09. März.

[335] ZDF heute (2024). “Bitkom: Mehr Cyberangriffe aus dem Ausland”, 13. Mai.

[336] ZDF heute (2024). “Wahlbeeinflussung in Rumänien: Experte: Demokratien vor Desinformation schützen”, 07. Dezember.

[337] Zeit online (2024). “Cyberangriff auf überregionalen Krankenhausbetreiber”, 14. Oktober.

ZEITREISE CYBER-BEDROHUNGEN

2010 2013

Staatliche Hackergruppe

Kriminelle Hackergruppe

Hacktivismus

Weltweiter Schaden durch Cyberangriffe (geschätzt) [1]

Die hier vorgestellten Fälle sind lediglich ein Auszug und bei Weitem nicht vollständig.

Der ehemalige NSA-Mitarbeiter Edward Snowden gibt Dokumente an Journalisten weiter. Diese legen die weltweiten Massenüberwachungsprogramme der Geheimdienste von USA und dem Vereinigten Königreich offen und führen zu einer öffentlichen **Debatte über die Grenzen von staatlicher Überwachung.**

Edward Snowden Leaks

Yahoo! Daten-diebstahl

Stuxnet-Wurm

FIN7

DOUBLE DRAGON

LAZARUS-GRUPPE SEIT 2009

COZY BEAR SEIT 2008

Target Daten-diebstahl

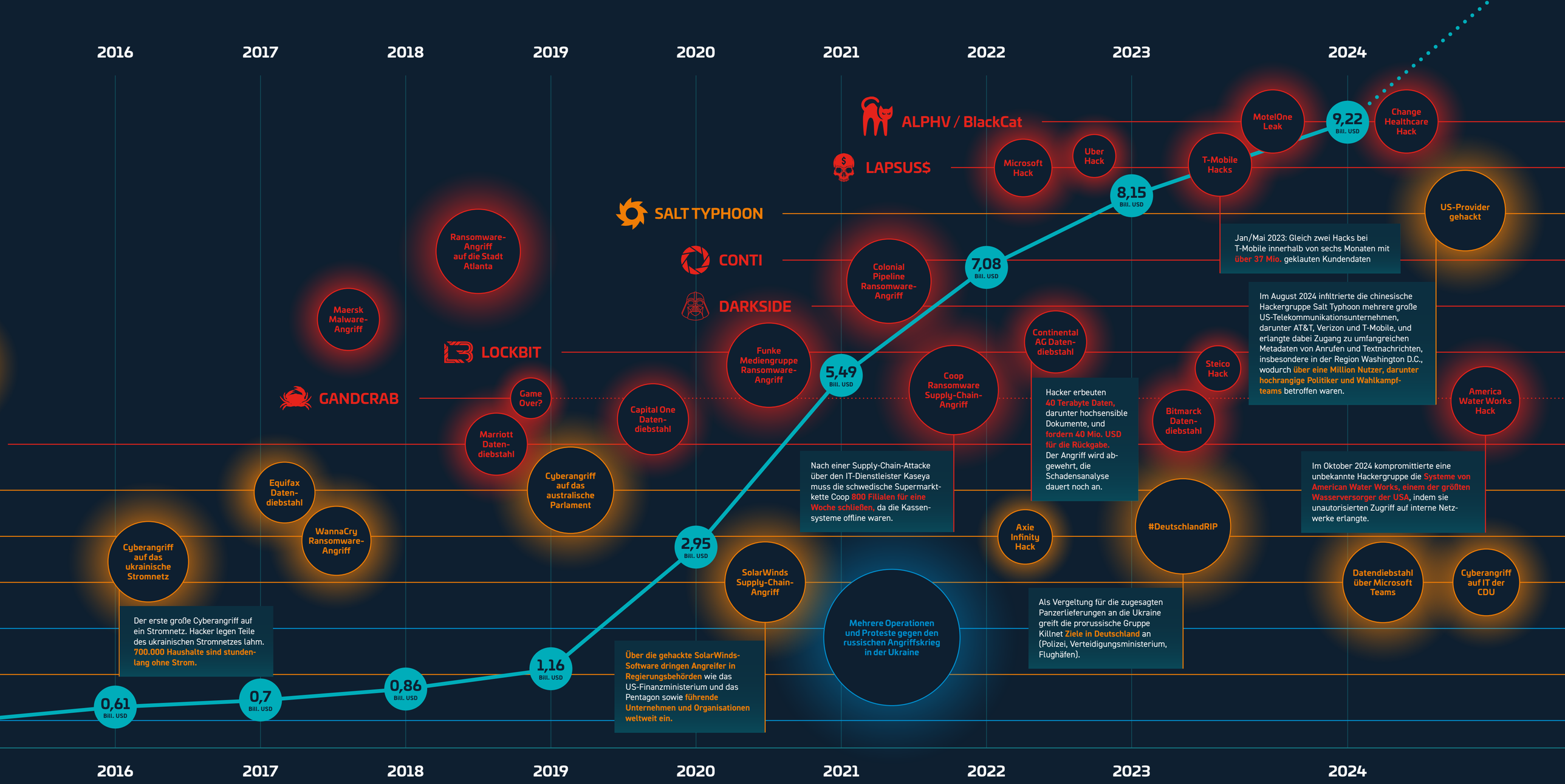
ANONYMOUS SEIT 2003

Operation Payback

EQUATION GROUP SEIT 2001

CULT OF THE DEAD COW SEIT 1984

2010 2013



1 Quellen: [272], [274], eigene Darstellung

IMPRESSUM

HERAUSGEBER

Schwarz Digits KG
Stiftsbergstr. 1
74172 Neckarsulm
Deutschland

Sitz: Neckarsulm
Registergericht: Stuttgart HRA 737212
USt-IdNr.: DE335467503

E-Mail: info@schwarz-digits.de
Website: www.schwarz-digits.de

Wissenschaftliche Leitung: Dr. Alexander Schellong

Autoren: Dr. Henrike Helmer, PD Dr. Robert Koch,
Dr. Patricia Köpfer, Dr. Alexander Schellong, Tolga Yilmaz

Design: André Renvert, Lukas Breitkreutz (infotectures)

Die Schwarz Digits KG wird vertreten durch die Ny-Stiftung mit Sitz in Dresden, Landesdirektion Sachsen, AZ 20-2245/589, die ihrerseits gemeinsam durch zwei gesamtvertretungsberechtigte Vorstände, u. a. Christian Müller und Rolf Schumann vertreten wird.