CYBER SECURITY REPORT 2023

SCHWARZ

LIDL

Kaufland

SCHWARZ Produktion

prezero

Vorwort

Cybersicherheit gehört auf jede Vorstandsagenda

Spionage, Sabotage, Desinformation, Datendiebstahl. Tagtäglich bedrohen Cyberkriminelle und staatliche Hacker Wirtschaft und Gesellschaft. Allein in Deutschland entsteht der Wirtschaft ein jährlicher Schaden von über 200 Milliarden Euro.

Ob Beeinflussung der öffentlichen Meinung, Diebstahl geistigen Eigentums oder Erpressung von Lösegeld – zumeist sind es nur wenige Schritte vom ersten Einbruchspunkt bis hin zur Kompromittierung hochsensibler Daten und Systeme. 11.000 Sicherheitslücken weisen Unternehmen im Durchschnitt entlang der üblichen Angriffspfade von Hackern auf; alle 39 Sekunden erfolgt irgendwo auf der Welt ein Cyberangriff.

Die fortschreitende Datennutzung und Vernetzung steigern die Komplexität und das Wachstum der Angriffsfläche exponentiell – sowohl in Politik und Verwaltung als auch in der Wirtschaft. Gleichzeitig sinken die moralischen Schwellen im Cyberraum. Krankenhäuser, Schulen oder Lebensmittelhändler, jeder kann jeden Tag zum Opfer werden. Konsequenzen spielen keine Rolle, Menschenleben werden bewusst riskiert. Durch die umfassende Digitalisierung unseres Lebens ist Cyberkriminalität, genauso wie der Klimawandel, zu einer der größten Herausforderungen unserer Zeit geworden.

Nur ein falscher Klick genügt. Beobachten und abwarten darf deshalb keine Antwort sein. Es gilt, keine Zeit mehr zu verlieren. Die Entwicklung proaktiver und nachhaltiger Cyberstrategien muss oberste Priorität haben.

Die Frage ist, was passiert, wenn etwas passiert. Für die Unternehmen der Schwarz Gruppe ist die Beantwortung dieser Frage von zentraler Bedeutung. Die dabei gewonnene Expertise teilen wir gerne und gezielt. Dieser Cyber Security Report gibt Einblicke in die Methoden aktueller Hackerangriffe, Hinweise zu typischen IT-Schwachstellen und der Exponiertheit von Führungskräften und Mitarbeitern im Internet wie auch konkrete Empfehlungen zur Optimierung. Zudem werden regulatorische Vorgaben und zukünftige Pflichten erläutert und deren Konsequenzen für das Management im Detail beleuchtet.

Die Sicherung unseres digitalen Ökosystems kann nur gelingen, wenn wir uns intensiv austauschen und gemeinsam Lösungen entwickeln. Noch schweigen viele Betroffene – oft aus falscher Scham oder weil Reputationsschäden befürchtet werden. Das spielt jedoch allein den Tätern in die Hände.

Lassen Sie uns unsere Erfahrungen und Erkenntnisse teilen, um es den Angreifern so schwer wie möglich zu machen. Die Abwehr von Cyberkriminalität erfordert den gemeinsamen Schulterschluss.

Handeln Sie jetzt. Setzen Sie Cybersicherheit ganz oben auf Ihre Agenda.

Gerd Chrzanowski
Komplementär der Schwarz Gruppe

Executive Summary

Cybersicherheit gehört – unabhängig von der fachlichen Expertise – auf jede Vorstands- und Aufsichtsratsagenda. Informationsaustausch und proaktives Handeln auf allen Ebenen sind entscheidend, um den immer aggressiver auftretenden kriminellen und staatlichen Akteuren entgegenzutreten. Das große Schweigen vieler Opfer spielt den Tätern in die Karten.

Dieser Bericht soll eine große Bandbreite an Einblicken und praktischen Handlungsempfehlungen für Führungskräfte – unabhängig von ihren Vorkenntnissen oder ihrem Aufgaben- und Entscheidungsspektrum – in Wirtschaft, Verwaltung und Politik ermöglichen. Dazu gehört die aktuelle Cybersicherheitslage im Kontext von Schäden, Wahrnehmung, Ökosystem der Cyberkriminellen, Personal oder Budget. Ebenfalls werden die Methoden der Angreifer beleuchtet. Es wird deutlich, warum Hacker immer in die Netzwerke von Organisationen gelangen können und wie sie dort trotz zahlreicher Schutzmaßnahmen ihre Ziele (Daten, Systeme) erreichen. Schließlich werden Gegenmaßnahmen für unterschiedliche Bedrohungen im Cyberraum für Organisationen, Führungskräfte und Mitarbeiter aufgezeigt, um vor die Welle der Cyberkriminalität zu gelangen.

Es wurden unterschiedliche Daten und Analysen für die Erstellung des Berichts kombiniert. Auf Basis von Expertenwissen wurde eine vergleichende Analyse nationaler und internationaler Berichte von Behörden, Wissenschaft und IT-Sicherheitsunternehmen, die bis März 2023 veröffentlicht wurden, vorgenommen. Ihre Schwerpunkte decken viele Themen, Methoden und Daten ab. Hierzu zählen auch Empfehlungen für präventive und reaktive Maßnahmen für die Cyberresilienz von Organisation sowie die praktische, nicht juristische Einordnung regulatorischer Trends.

Um die Dimensionen und die Bedeutung der externen Angriffsfläche zu verstehen, wurden im Februar 2023 insgesamt 213 in Deutschland verortete Organisationen aus dem öffentlichen Sektor und der Wirtschaft analysiert. Dies erfolgte automatisiert, nicht invasiv und anonymisiert im Aggregat für die sechs Gruppen. Der Fokus lag auf allen Unternehmen, welche in DAX (40), MDAX (50) und SDAX (70) gelistet sind. Zusätzlich wurden acht Handelsunternehmen, 35 Flughäfen und die zehn größten deutschen Städte nach Einwohnern untersucht. Zum Zeitpunkt der Veröffentlichung des Berichts können die Ergebnisse aufgrund der Dynamik des aus dem Internet erreichbaren digitalen Fußabdrucks jeder Organisation bereits wieder anders ausfallen.

Um das Vorgehen von Hackern nach dem Vordringen in eine Organisation besser zu verstehen, wurden anonymisierte Datensätze aus dem Jahr 2022 von XM Cyber anonymisiert und durch unabhängige Dritte analysiert.

Um das Ausmaß und die Gefährdungslage von offen verfügbaren Identitätsdaten im Surface, Deep und Dark Web zu verstehen, wurden Ende Februar 2023 in einer Stichprobe die Führungskräfte (CEO und weiterer Vorstand) und Unternehmensdomains (.com und .de) von zehn großen deutschen Unternehmen untersucht. Diese kamen aus den Branchen Handel, Pharma, Transport, Finanzdienstleistungen und Banken, Konsumgüter, Technologie, Automobil und Telekommunikation. Hierbei wurde eine Datensammlung mit über 124 Milliarden Datensätzen aus Cyberangriffen und Datenlecks der letzten 18 Jahre verwendet.

Nach Umfragen des Branchenverbands Bitkom waren im Jahr 2022 allein in Deutschland 84 Prozent der befragten Unternehmen von einem Cyberangriff betroffen. Auch wenn die geschätzten

Gesamtschäden in Deutschland leicht auf 203 Milliarden Euro zurückgegangen sein sollen, rechnet man weltweit mit einem Anstieg der durch Cyberangriffe entstandenen Kosten auf bis zu 20 Billionen Euro bis Ende 2030. Aufgrund der hohen Dunkelziffer an Fällen sind genaue Zahlen nicht verfügbar. Die Bandbreite an Kosten für Cyberangriffe reicht von 30.000 Euro bis weit über 25 Millionen Euro. Sind personenbezogene Daten von Kunden oder Mitarbeitern verschlüsselt worden, liegen Lösegeldforderungen bei etwa vier Millionen Euro. Die Nachwirkungen von Cyberangriffen können Organisationen über ein Jahr beschäftigen oder für Monate in ihren Aktivitäten einschränken. In der öffentlichen Verwaltung musste bereits selbst in Deutschland der Notstand für sechs Monate ausgerufen werden.

In 80 Prozent der Fälle werden Organisationen Opfer externer Akteure, vor allem aus Russland und China. Innentäter machen 20 Prozent der Fälle aus. Auf Untergrundforen und -marktplätzen lassen sich einfach Schadcodes und kostengünstig Benutzerkonten erwerben. Professionelle Dienstleistungen für alle Arten von Cyberangriffen sind auf Stundenbasis anmietbar. Erfolgsbasierte Umsatzbeteiligung zeichnet ebenfalls ein hochdynamisches Ökosystem im Hintergrund von Cyberakteuren aus, welches sich erfolgreich dem Zugriff von Strafverfolgungsbehörden entzieht.

Social Engineering gehört zu den ältesten und kontinuierlichsten Bedrohungen aus dem Cyberraum. Dies ist eine wesentliche Erkenntnis aus der vergleichenden Analyse. 82 Prozent der Sicherheitsvorfälle gehen auf menschliches Fehlverhalten zurück, wovon 60 Prozent das Resultat eines unaufmerksamen Klicks auf Anhänge oder Internetlinks in E-Mails sind.

Ransomware stellt nach Einschätzungen von BSI, ENISA und FBI weiterhin die größte Bedrohung für Organisationen dar. Ransomware zielt darauf ab, die Kontrolle über Vermögenswerte in Form von Daten und Systemen zu erlangen. Mittlerweile werden Opfer vierfach unter Druck gesetzt: 1. Man löscht die Kopien (Backups) und verschlüsselt alle Daten. 2. Man kopiert vor dem Verschlüsseln alle Daten und droht mit der Veröffentlichung im Darknet. 3. Man analysiert die Daten der Opfer und droht Kunden und Dienstleistern mit der Veröffentlichung. 4. Man kombiniert die Verschlüsselung mit Angriffen auf die Verfügbarkeit (Distributed Denial of Service [DDoS]) von Systemen durch eine Flut an Datenverkehr.

Letztere Angriffsmethode bleibt beliebt, kann teils Wochen oder Monate andauern und nimmt neue Dimensionen in Umfang und Volumen an, weil weltweit immer mehr IT-Komponenten für DDoS-Attacken missbraucht werden können. Ende 2022 wurde ein Angriff bekannt, bei dem eine Cloud-Umgebung von 10.000 Rechnern aus über zehn Ländern mit einer großen Anzahl an Anfragen (3,47 Terabits pro Sekunde) versucht wurde zu überlasten. Diese Datenmenge pro Sekunde entspricht einer Summe von 55,52 Regalkilometern Aktenordnern (8-cm-Ordner mit 250 A4-Seiten und durchschnittlich 2.000 Anschlägen).

Als eine immer größer werdende und damit ernstzunehmende Gefahr gelten Angriffe auf die Lieferkette oder sogenannte Supply-Chain-Attacken. Galten im Jahr 2020 noch unter ein Prozent der Angriffe Lieferketten, zeigen Analysen einen Anstieg zwischen 17 Prozent und 62 Prozent im Jahr 2022.

Mit der Digitalisierung und deren Harmonisierung mit Altsystemen wächst die Komplexität, was im Umkehrschluss auch das Risiko für Cyberattacken ansteigen lässt. Der digitale Fußabdruck von Organisationen, welcher vom Internet aus erreichbar ist, wächst und wandelt sich stetig. Börsennotierte Unternehmen, kritische Infrastrukturen wie Flughäfen oder die größten Städte in Deutschland zeigen sich im Bereich Anwendungs- und Netzwerksicherheit oder Nutzung neuster Verschlüsselungsprotokolle für die Kommunikation verwundbar. Die Bewertung ihrer Sicherheitssituation aufgrund verschiedener Kriterien fällt für die Mehrheit der 213 Organisationen gering und teils kritisch aus.

Mit verschwimmenden Grenzen zwischen außen und innen scheint der Fokus auf die Außengrenzen

einer Organisation nicht mehr zeitgemäß. Berücksichtigt man die Ergebnisse der externen Angriffsfläche, muss davon ausgegangen werden, dass die Angreifer immer einen Weg in Zielorganisationen finden. Im Durchschnitt haben Organisationen 11.000 interne Schwachstellen, die von Angreifern ausgenutzt werden können. In weniger als 20 Prozent der Fälle muss sich ein Hacker etwas anstrengen und benötigt mehr als vier Schritte zu sensiblen Daten. Schwachstellen sind eine Kombination aus nicht behobenen Software-Schwachstellen (fehlende Updates / Patching), Fehlkonfigurationen von IT-Systemen, falsch verwalteten Anmeldeinformationen oder unzureichend geschützten Ressourcen. 75 Prozent der Schwachstellen führen jedoch nicht zu kritischen Systemen. Dies sind weniger als zwei Prozent. IT- und IT-Sicherheitsteams könnten ihre Arbeit daher um 99,6 Prozent reduzieren, wenn sie sich auf die Härtung dieser Systeme konzentrieren würden. Sollten Organisationen die Härtung vernachlässigen und sich auf moderne Lösungen zur Angriffserkennung (EDR/XDR) verlassen, kann dies ein falsches Gefühl der Cybersicherheit vermitteln. Bei etwa 40 Prozent der untersuchten Organisationen waren derartige Lösungen bei weniger als 50 Prozent der IT-Infrastruktur im Einsatz. Gerade weil Daten von Mitarbeitern gestohlen werden können oder bereits unbemerkt gestohlen wurden, ist das Zugriffs- und Rechtemanagement für die IT besonders wichtig. 80 Prozent der untersuchten Organisationen sind hier verschiedenen Angriffsmethoden ausgesetzt.

Die Daten von 20 deutschen Vorständen und ihren Mitarbeitern von zehn Unternehmen sind mit über 1,2 Millionen Identitäten und 305.000 Passwörtern auch im Klartext oder mit schwachem Schutz im Surface, Deep und Dark Web auffindbar. Alle untersuchten Vorstände waren von mindestens einem Datenleck betroffen. Im Schnitt waren es 16, im Höchstfall 70. In zwei Fällen konnten Daten von sensiblen Seiten (zum Beispiel Glücksspiel, Dating, Erwachseneninhalte) gefunden werden. Zu den Daten auf sensiblen Seiten gehörten Klartextpasswörter, Social-Media-Profile, private Telefonnummern oder Privatadressen. Insgesamt konnten 115 Passwörter für alle Vorstände identifiziert werden. 70 Prozent davon lagen unverschlüsselt vor.

Neben der Erkenntnis und dem Problemverständnis für Gefahren zählen letztendlich nur die erfolgreichen Maßnahmen, um den möglichen Angreifern das Leben so schwer wie möglich zu machen. Entscheider sollten ihre Schwerpunkte in fünf Bereiche legen: 1. Entwicklung einer risikobasierten und proaktiven Cyberstrategie, 2. Schaffung und Pflege einer Sicherheitskultur, 3. Einbeziehung aller Prozesse einer Organisation, 4. Verbesserung der Fähigkeiten der Mitarbeiter, 5. Investitionen in geeignete Cybersicherheitstechnologien und -dienstleistungen.

Neben Erkenntnis und Problemverständnis werden zahlreiche Organisationen in den nächsten Jahren vor neue regulatorische Rahmenbedingungen gestellt. Gerade in der EU gibt es mit DORA, NIS 2 und CRA Gesetze bzw. Gesetzesvorhaben, die in den nächsten zwei bis fünf Jahren weitreichende Auswirkungen im Sinne der Datenschutz-Grundverordnung auf eine Vielzahl an Organisationen haben werden und für diese Einschnitte bedeuten. Vorgesehene Bußgelder bewegen sich bei zwei bis drei Prozent des weltweiten Jahresumsatzes und einem Minimum von sieben bis 20 Millionen Euro. Auch in den USA versucht der Gesetzgeber die Cybersicherheit durch neue Gesetze zu verbessern. Vorstände und Aufsichtsräte werden dabei mit in die Verantwortung genommen.

Führungskräfte können also nicht abwarten, sondern müssen handeln.

Inhalt

Vorwort 1

Executive Summary 3

1 Cybersicherheit auf einen Blick 9

2 Angriffsflächen einer digitalen Welt 25

3 Mit den Augen der Hacker – unsichtbare Angriffspfade 35

4 Risikofaktor Mensch – das Internet vergisst nie 49

5 Der Weg vor die Cyberkriminalitätswelle 59

6 Gesetzliche Cybersicherheits-anforderungen der Zukunft 77

Anhang 91

Unternehmen der Schwarz Gruppe im Überblick 93

Abkürzungsverzeichnis 101

Literaturverzeichnis 103

1 Cybersicherheit auf einen Blick

DIE TOP-BEDROHUNGEN

PHISHING

Social Engineering
Phishing/Spearfishing

60 % aller E-Mails sind Spam
70 % davon mit Phishing-Absichten

RANSOMWARE

1-fach = Verschlüsselung, Vernichtung von Backups
2-fach = zusätzlich: Kopie/Abzug, Veröffentlichung oder Verkauf der Daten
3-fach = plus: Betroffenen Dritten wie Kunden und Zulieferern wird mit Veröffentlichung gedroht.

SCHÄDEN DURCH CYBERANGRIFFE IN EURO

3-4 MILLIONEN EURO KOSTEN JE VORFALL

IM EINZELFALL AUCH MEHR ALS 250 MIO. EURO

€

In 94 % der Cyberangriffe ist unklar, ob Zahlungen erfolgt sind.
Bis zu 656 Mio. Euro Lösegeldzahlungen flossen 2021 in der EU. Colonial Pipeline zahlte 4,4 Mio. Euro.

WAS WIRD GESTOHLEN?

1. **E-Mails**
2. Kundendaten
3. Zugangsdaten
4. IP / geistiges Eigentum
5. Finanzdaten

DIE TOP-SCHWACHSTELLEN

Nach Software laut globaler Schwachstellendatenbank

1. **Google**
2. Microsoft
3. Adobe
4. IBM
5. Oracle

FACHKRÄFTEMANGEL

PERSONAL IN DER CYBERSICHERHEIT

Weltweit arbeiten 4,65 Mio., in Deutschland 464.000 Experten in der Cybersicherheit.

ES FEHLEN

3,4 Mio. WELTWEIT | **104 Tsd.** IN DEUTSCHLAND

CYBERNEWS

Alle 39 Sekunden ein Angriff • 23.000

Bedenklich: Angreifer wurden erst nach 270 Tagen bemerkt • 2022 wurde alle 20 Min. eine

Ransomware: Landkreis Anhalt-Bitterfeld ruft für 6 Monate den Katastrophenfall aus • Die

DSGVO

Datenschutzverletzungen können einen hohen finanziellen Schaden nach sich ziehen.

DDoS

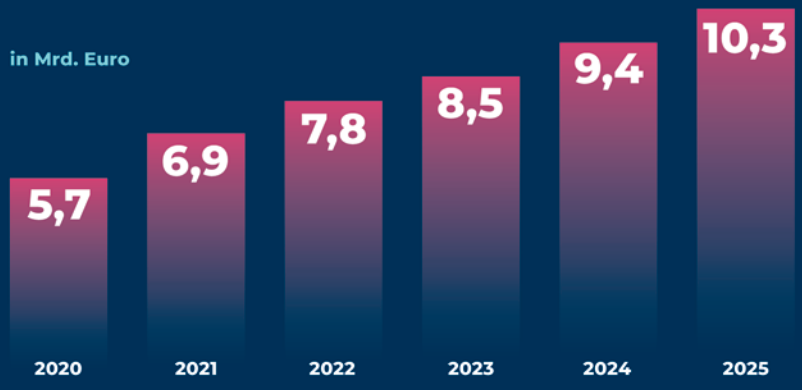
Server werden mit einer solch großen Anzahl von Anfragen bombardiert, dass diese zusammenbrechen.

SUPPLY-CHAIN-ANGRIFFE

Angreifer verschaffen sich über Drittanbieter oder Lieferanten Zugriff auf das Netzwerk eines Unternehmens.

CYBERBUDGET

NUR 5–11 % DES IT-BUDGETS FLIESSEN IN DIE CYBER-SICHERHEIT



DER DEUTSCHE MARKT FÜR IT-SICHERHEIT WÄCHST DERZEIT JÄHRLICH UM RUND 11 %

* Bitkom empfiehlt, mind. 20 % des Budgets für IT-Sicherheit einzuplanen. Entscheider von 80 % der Unternehmen mit Aufsichtsrat werden von diesem mit Fragen zur Cybersicherheit konfrontiert.

CYBERCRIME AS A SERVICE

DDoS	ab 9 EUR/Std.
Botnetz	ab 75 EUR/Monat
Phishing-Kampagne	ab 499 EUR/Monat
Keylogging-Kampagne	ab 180 EUR/Monat
Ransomware und RAT	ab 1.000 EUR/Monat
Malware Angriff	ab 40 EUR
Social Media Account	ab 9 EUR
Netflix Account	ab 90 Cent
Kreditkarten-Klon	ab 7 EUR
E-Mail mit Passwort	ab 60 Cent
Admin Account	500 – 140.000 Euro

Quellen: eigene Darstellung; https://www.visualcapitalist.com/cp/charted-the-dark-web-price-index-2022/ [4, 13, 14, 22, 29, 31, 36, 37, 51, 52, 54, 67, 71]

DDoS-Attacken pro Tag weltweit • 71 Mio. Anfragen pro S

Software-Schwachstelle festgestellt • Anstieg der kritischen Schwachstellen um 59 % • Beden

gesamte Verwaltung Costa Ricas durch Cyberangriff lahmgelegt • Ransomware: Landkreis ruf

1 Cybersicherheit auf einen Blick

1.1 Schäden und Auswirkungen: von Datendiebstahl über Erpressung bis hin zum Notstand

Nach Umfragen des Branchenverbands Bitkom waren im Jahr 2022 allein in Deutschland 84 Prozent der befragten Unternehmen von einem Cyberangriff betroffen. Weitere neun Prozent der Unternehmen gehen davon aus, sie glauben also, die Hacker sind schon in ihren IT-Systemen [4]. Weiter führen Untersuchungen der Allianz aus, dass 45 Prozent der Unternehmen Angst vor einem solchen Moment haben, der zu kostspieligen oder sogar zu existenzbedrohenden Betriebsunterbrechungen führen kann. Damit gelten Cybervorfälle aktuell als wichtigstes Geschäftsrisiko [2].

Dem gegenüber steht eine Befragung von 1.350 Unternehmen aus 13 Ländern, die zu 80 Prozent der Meinung sind, sich gut gegen die unterschiedlichen Akteure zu verteidigen. Lediglich bei staatlichen Angreifern aus Russland, China und Nordkorea sinkt das Selbstvertrauen auf 50 Prozent [60].

1.1.1 Allgemeine Schäden durch Cyberkriminalität

Cyberangriffe auf IT-Infrastrukturen von staatlichen Institutionen, Unternehmen oder Privatpersonen sind oft weitgehend mit Schäden und Auswirkungen verknüpft, die bei den Betroffenen mit einer Minderung oder einem Verlust von materiellen wie auch immateriellen Gütern verbunden sind. Aufgrund einer hohen Dunkelziffer an Vorfällen, die behördlich nicht erfasst werden können, sind genaue Statistiken in ihrer Gesamtheit nur schwer darstellbar. Die Allianz geht in einer Schätzung davon aus, dass der weltweite monetäre Schaden, welcher durch cyberkriminelle Akte entsteht, sich jährlich auf 1 Billion Euro beläuft. Dies entspricht ein Prozent des weltweiten Bruttoinlandsprodukts [2]. Andere Schätzungen gehen von weltweiten Schäden in Höhen von etwa acht Billionen Euro aus, die bis 2027 auf 10 bis 22 Billionen Euro steigen sollen [1], [41], [70]. Allein in Deutschland sind nach Angaben von Bitkom im Jahr 2022 rund 203 Milliarden Euro an Gesamtschäden durch Cyberattacken entstanden [4]. Das Ausmaß ist im Vergleich zu früheren Beobachtungen und insbesondere zum Rekordjahr 2021 leicht rückläufig [14].

Eine ähnliche Problematik ergibt sich für durchschnittliche Schäden bzw. Kosten je Vorfall. Ebenfalls tragen fehlende Definitionen und Kategorisierungen der Zwischenfälle dazu bei, indem sie die Vergleichbarkeit unterschiedlicher Schadensstatistiken erschweren. Daher sollten Berichte über Schäden aus Cyberangriffen generell eher für eine qualitative Beobachtung und eine unternehmensspezifische Trendbewertung verwendet werden.

Nach Angaben des Bundeskriminalamts (BKA) aus dem Jahr 2021 belaufen sich die gemittelten Kosten pro Vorfall auf rund 555.000 Euro. Dabei umfasst die Spannweite einen Bereich von 83.000 Euro bis 909.000 Euro [14].

Nach Untersuchungen der European Union Agency for Cybersecurity (ENISA) betragen die Kosten zur Wiederherstellung der Betriebsfähigkeit nach einem Cyberangriff im Mittel 200.000 Euro [35].

Die direkten Kosten aus einem schwerwiegenden Sicherheitsvorfall sind erheblich höher und werden im Durchschnitt auf 369.000 Euro geschätzt. Dabei ist hier eine große Streuung um den Mittelwert besonders bemerkenswert, da diese eine Bandbreite zwischen rund 30.000 Euro und 2 Millionen Euro umfasst [35]. Die große Bandbreite entsteht dadurch, dass Unternehmen je nach Branche und Unternehmensgröße unterschiedlich stark betroffen sind. Nach Ergebnissen der Allianz sind bei kleinen und mittleren Unternehmen (KMUs) tendenziell höhere Schäden zu verzeichnen [2]. Aber auch Großkonzerne werden durch Cyberkriminalität stark in Mitleidenschaft gezogen. In einer aktuellen sektorübergreifenden Umfrage der Munich RE haben mehr als 70 Prozent der befragten Unternehmen angegeben, dass sie bereits Opfer eines Betruges, einer Erpressung oder von Datendiebstahl geworden sind [65]. Für die Finanzbranche, das Gesundheitswesen, den Energie- sowie Transportsektor liegen die Kosten innerhalb von Europa mit mehr als 400.000 Euro pro entstandenem Schaden deutlich über dem Durchschnitt. Geringere monetäre Auswirkungen haben dagegen der Bereich E-Commerce oder die Telekommunikationsbranche zu verzeichnen [35].

Neben den direkten finanziellen Schäden können zusätzlich Folgeschäden durch Cyberangriffe entstehen. Diese nachgelagerten Schäden entstehen dabei durch etwaige betriebliche Unterbrechungen der Geschäftstätigkeiten sowie die daraus folgenden Umsatzeinbußen [28]. In Umfragen werden insbesondere die Unterbrechungen bei deutschen Unternehmen zunehmend als existenzbedrohend wahrgenommen [4]. Der drohende Verlust von Kundenvertrauen oder potenzielle Reputationsschäden aus Cyberangriffen lassen sich dagegen nur schwer monetär bemessen [28]. Erste Studien zeigen jedoch, dass Unternehmen mit Fokus auf Konsumenten am ehesten einen Reputationsverlust erleiden [59]. Bei börsennotierten Unternehmen kann ein schwerwiegender Cyberangriff zu Börsenkursverlusten (Kursverlust von im Durchschnitt 3,5 Prozent) führen, da mit einem langfristig entgangenen Gewinn für das Unternehmen bzw. Aktionäre gerechnet werden muss [3].

1.1.2 Schäden durch Datendiebstahl

Bei Schäden durch den Abfluss von Daten, Informationen oder Wissen entstehen mögliche finanzielle Schäden bei einem angegriffenen Unternehmen primär durch den entgangenen Gewinn. Gleichzeitig können aber auch die Rechte Dritter durch den Abfluss von Daten oder Wissen verletzt werden. In diesem Fall können weitere Schäden durch Schadenersatzansprüche entstehen. Analog zur vorangegangenen Argumentation lassen sich durch diese Faktoren entstehende Schäden jedoch nur schwer quantifizieren. Um Einblicke in diese sehr diffuse Lage zu erhalten, können Fallstudien Abhilfe schaffen.

So wurde bei einer aktuellen Untersuchung der ENISA von 623 ausgewählten Sicherheitsvorfällen im Berichtszeitraum festgestellt, dass bei rund 46 Prozent der Fälle ein belegbarer Datenabfluss stattgefunden hat, bei dem insgesamt ein Volumen von 136 Terabyte an Informationen illegitim entwendet wurde. Dabei kann nur für 30 Prozent der gestohlenen Daten eine Aussage über den Inhalt getätigt werden. Die Untersuchung zeigt weiter, dass 41,7 Prozent der gestohlenen Daten nicht personenbezogen gewesen sind [31]. Die Ergebnisse verdeutlichen, dass von den Angreifern bevorzugt Daten entwendet werden, die sich negativ auf die betroffenen Unternehmen auswirken können. Die gestohlenen Daten enthalten zu 19 Prozent Finanzinformationen, wie Abteilungsbudgets, Quittungen, Einkommenserklärungen oder Jahresabschlüsse, und zu 24 Prozent Geschäftsinformationen, wie Produktionsdaten, Verwaltungsdokumente, Rechtsakten, Handelsregistrierungen oder Geheimhaltungsvereinbarungen [31].

Laut Bitkom wurden in Deutschland im Jahr 2022 bei den befragten Unternehmen verstärkt Daten zu E-Mails (68 Prozent), Kundendaten (45 Prozent), unkritische Geschäftsdaten (38 Prozent), Zugangsdaten zu Cloud-Diensten (32 Prozent), kritische Geschäftsdaten (28 Prozent), Mitarbeiterdaten (25 Prozent), Daten zu geistigem Eigentum (18 Prozent) und Finanzdaten (14 Prozent) im Zuge von Cyberangriffen gestohlen [4]. Dagegen zeigen Untersuchungen von Verizon, dass Angreifer zu 40 Prozent auf Zugangsdaten, zu 40 Prozent auf Personendaten und nur zu zehn Prozent auf Finanzdaten ab-

zielen [74].

Die Studien verdeutlichen insgesamt, welche Werte in Form von Daten bzw. Informationen aus staatlichen Institutionen, Unternehmen oder von Privatpersonen exfiltriert werden und worauf es Cyberkriminelle entweder gezielt oder in der Breite abgesehen haben. Im Unternehmenskontext entstand dadurch für das Jahr 2022 ein Schaden von 41,5 Milliarden Euro in Bezug auf den Verlust von Wettbewerbsvorteilen [4]. Hinsichtlich Betriebsspionage belaufen sich Schäden auf mehr als 21 Milliarden Euro [17].

Nach Untersuchungen der ENISA enthielten rund 58 Prozent der gestohlenen Daten personenbezogene Daten nach der Datenschutz-Grundverordnung (DSGVO) [31]. Dabei spielen die Rechte Dritter, im regulatorischen Sinne, eine erhebliche Rolle bei der Bemessung des Schadensausmaßes durch Datendiebstähle aus Cyberangriffen. Nach aktuellen Analysen von IBM für das Jahr 2022 betragen die durchschnittlichen Kosten für eine Datenschutzverletzung aus Datenabflüssen 4,05 Millionen Euro und erreichten damit ein Allzeithoch, was einen Anstieg von 13 Prozent im Vergleich zum Jahr 2020 bedeutet.

Im Zusammenhang mit der Corona-Pandemie und der wachsenden Telearbeit sollte auch Erwähnung finden, dass sich die Kosten durch eine Datenschutzverletzung signifikant erhöhen können. Hier muss im Vergleich zum klassischen Arbeitsmodell mit einem Anstieg von 565.000 Euro bis zu 942.000 Euro bei Schäden aus einer Datenschutzverletzung gerechnet werden.

Bemerkenswert ist zudem, dass eine Datenschutzverletzung im Falle von gestohlenen oder kompromittierten Anmeldedaten im Mittel 243 Tage vorliegt, bis sie tatsächlich erkannt wird. Weitere 84 Tage vergehen im Durchschnitt, bis sie eingedämmt bzw. behoben wird. Bei der geografischen Betrachtung der Kosten durch Datenschutzverletzungen von IBM zeigt sich weiter, dass die höchsten Kosten mit 8,9 Millionen Euro in den USA verzeichnet werden. Für Deutschland liegen die durchschnittlichen Schäden bei 4,57 Millionen Euro [54].

1.1.3 Schäden durch Erpressung

Um einen direkten finanziellen Profit aus einer Cyberattacke zu erzielen, kommen klassische Methoden wie Löse- oder Schweigegelderpressungen zur Anwendung. Dabei stehen insbesondere umsatzstarke Unternehmen im besonderen Fokus der Angreifer, da hier die größten Gewinne zu erwarten sind (sogenannte Big-Game-Hunting) [13]. Nach einer Analyse aus dem Jahr 2022 von der ENISA sind monatlich mehr als zehn Terabyte an Daten von Cybererpressungen betroffen [31]. Die jährlichen Schäden durch Erpressung nehmen rasant zu und lagen im Jahr 2022 für Europa bei 24,3 Milliarden Euro [14]. Für Deutschland wird für das Jahr 2022 ein Gesamtschaden durch Erpressung von 10,7 Milliarden Euro aufgeführt [4]. Im Jahr 2019 lagen die Schäden noch bei 5,3 Milliarden Euro und haben sich mehr als verdoppelt [14]. Glaubt man Prognosen, so muss für das Jahr 2030 sogar mit weltweiten Schäden aus Erpressung von bis zu 250 Milliarden Euro ausgegangen werden [64].

Im Mittel liegen die Kosten für solche Erpressungsdelikte aktuell bei rund 540.000 Euro in Europa. Sie können aber auch deutlich höher ausfallen. Der größte zu beobachtende Schaden in diesem Zusammenhang lag bei 1 Millionen Euro [35]. Vom BKA werden die durchschnittlichen Schäden für eine Erpressung mit nur ca. 193.000 Euro für das Jahr 2022 angegeben [14]. Werden bei der Erpressung personenbezogene Daten benutzt, dann liegen die durchschnittlichen Schäden laut IBM sogar bei 4,28 Millionen Euro [54]. Erpressungsfälle, bei denen Daten mit Personenbezug eine Rolle spielen, sind zudem im Berichtszeitraum um elf Prozent angewachsen. Dadurch steigen entstehende Schäden um ein Vielfaches [31], [54].

Bei einer Erpressung entsteht ein Hauptschaden durch die Zahlung eines Lösegeldes. Nach den Analysen von ENISA konnte in 94,2 Prozent der Fälle nicht bestimmt werden, ob ein Lösegeld gezahlt wurde, da diese Informationen nicht gern preisgegeben werden [31]. Nach den Untersuchungen von BKA und Europol konnte aber festgestellt werden, dass im Jahr 2021 insgesamt Lösegeldzahlungen zwischen 376 Millionen Euro und 565 Millionen Euro in Form von Kryptowährungen geleistet wurden [14], [36]. Die Steigerungsraten von gezahlten Löse-

geldzahlern betrugen seit 2019 bis zu 300 Prozent [36]. Bei einem Betrugsversuch per E-Mail, einem sogenannte Business E-Mail Compromise (BEC) bzw. CEO-Betrug, entsteht durchschnittlich ein Schaden von ca. 74.500 Euro [40].

Dass Löse- bzw. Schweigegelderpressungen eskalieren können, zeigen zwei bemerkenswerte Cyberangriffe in Deutschland und Costa Rica, bei denen den staatlichen Institutionen ein erhebliches Volumen an schützenswerten Informationen durch cyberkriminelle Gruppierungen entwendet und auf den Opfersystemen verschlüsselt wurden. Die Landeskreisverwaltung von Anhalt-Bitterfeld in Sachsen-Anhalt war im Juli 2021 davon so stark betroffen, dass infolge der Beeinträchtigung der Katastrophenfall für länger als sechs Monate ausgerufen werden musste [14].

Der zweite Fall in Costa Rica zeigt, dass die Auswirkungen ein gesamtes Land treffen können. Die Auswirkungen der Cyberattacke waren in diesem Fall so schwerwiegend, dass der neu gewählte costaricanische Präsident, Rodrigo Chaves Robles, dazu gezwungen wurde, am Tag seines Amtsantritts den nationalen Notstand auszurufen. Insgesamt waren hier mindestens 27 behördliche Einrichtungen betroffen – darunter das Finanz- und das Arbeitsministerium des Landes. Nach Angaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) war damit erstmals ein Land gesamtstaatlich von einer Cyberattacke betroffen [13]. Die „Conti Ransomwaregang“ verlangte bis zu 20 Millionen US-Dollar in Kryptowährung.

1.2 Ökosystem und Brandbeschleuniger für Cyberkriminalität

Bei Cyberangriffen können die Täter bzw. Angreifer durch das Internet im Verborgenen agieren. Um Cyberangriffe besser zu verstehen und abwehren zu können, ist es für Unternehmen und Institutionen wie auch Privatpersonen essenziell, den Gegner zu kennen und seine Absichten zu verstehen. Zu 80 Prozent handelt es sich bei Cybervorfällen um externe Angreifer und nur zu 20 Prozent um interne Täter – wobei die größten Schäden von internen Tätern angerichtet werden [74].

Täter bzw. Tätergruppen waren im Jahr 2022 wie folgt charakterisiert: 51 Prozent organisierte Banden, 38 Prozent Hacker, 36 Prozent ehemalige Beschäftigte (unabsichtlich), 14 Prozent konkurrierende Firmen und sechs Prozent ausländische Nachrichtendienste. Bei der Herkunft der Täter lässt sich für das Jahr 2022 insgesamt ein geografischer Trend Richtung Osten verzeichnen, da Russland mit 36 Prozent (+13 Prozent zu 2021) und China mit 43 Prozent (+ 13 Prozent) bereits den Hauptanteil abdecken [4].

1.2.1 Cyberkriminalität als Dienstleistung

Hürden bzw. Hindernisse, um cyberkriminelle Aktivitäten durchzuführen, sind offenbar nicht hoch genug. Auf Untergrundforen und -marktplätzen lassen sich vergleichsweise einfach und preiswert Schadcodes erwerben oder ganze Infrastrukturen als Dienste anmieten, um großangelegte Erpressungs- und Betrugskampagnen mit speziellen Schadprogrammen und trickreichen E-Mails zu realisieren [22], [25], [26], [55]. Diese unter dem Sammelbegriff Cybercrime as a Service (CaaS) bekannten Angebote aus dem Untergrund bieten hohe monetäre Anreize bzw. Renditen, um kriminell aktiv zu werden. Im Berichtszeitraum wird dies durch eine große Vielfalt von Cyberangriffen deutlich.

Es zeigt sich ein Trend, dass die Angriffe von den Tätern deutlich an Facettenreichtum gewinnen, raffiniert kombiniert und kontinuierlich weiterentwickelt werden [14], [33].

Ein Trend, der zum Wachstum beiträgt, sind sogenannte Affiliate-Programme, bei denen CaaS-Anbieter eine Gewinnbeteiligung versprechen, sollte der Schadcode von Partnern erfolgreich bei einem Angriff angewendet werden [63]. Neben der Motivation, Partner in solchen Beteiligungsprogrammen zu werden, ist dieses Geschäftsmodell in Bezug auf die Arbeitsteilung besonders förderlich, da sich CaaS-Anbieter darauf konzentrieren können, ihre schadhaften Produkte zu verbessern und zu verfeinern. Partner wiederum streben an, den größtmöglichen Erfolg durch den Einsatz von CaaS-Produkten zu erzielen [63].

Im Zusammenhang mit cyberkriminellen Aktivitäten dürfen außerdem spezielle Dienste, Werkzeuge und Technologien nicht unerwähnt bleiben, die Bedrohungsakteuren beispielsweise dazu verhelfen, hinterlassene Fußabdrücke zu verwischen und täterseitige Eintrittsbarrieren weiter zu minimieren. Zu den beliebtesten ausgenutzten legitimen Techniken zählen nach Angaben von Europol u.a. Dienste mit einer starken Ende-zu-Ende-Verschlüsselung, wie Messaging-Anwendungen, Anonymisierungsdienste, Kryptowährungssysteme und virtuelle private Netzwerke (VPNs). In eine Grauzone fallen dabei Dienste, die häufig in Ländern mit sehr strengen Datenschutzgesetzen angeboten werden oder strategisch in solchen platziert werden. Außerdem werden Dienste aus Ländern angeboten, die nicht mit internationalen Strafverfolgungsbehörden zusammenarbeiten – darunter Bulletproof-Hoster, betrügerische Kryptowährungsbörsen und VPNs, in denen eine Nachverfolgung nicht möglich ist. Sie werden analog zum CaaS-Prinzip aktiv im Untergrund beworben [36].

Mit den CaaS-Geschäftsmodellen und genügend zur Verfügung stehenden Verschleierungsstrategien entsteht ein sehr lukratives und hochdynamisches Ökosystem, um organisierte Cyberkriminalität zu betreiben. Dieses Phänomen darf unter keinen Umständen unterschätzt werden und ist nach Erkenntnissen von Europol ein übergreifender Treiber in allen Teilbereichen der Cyberkriminalität. Es erlaubt nicht nur Akteuren mit geringem technischem Kenntnisstand kriminell erfolgreich zu sein, sondern macht auch Operationen professioneller Bedrohungsakteure effizienter [36].

1.2.2 Das Umfeld als Brandbeschleuniger

Neben CaaS als treibender Kraft tragen auch das globale Umfeld und cyberkriminelle Akteure zur akuten Bedrohungslandschaft bei. So führen viele Unternehmen aufgrund des digitalen Wandels umfangreiche Umstrukturierungsmaßnahmen ihrer IT-Landschaft (Informationstechnologie-Landschaft) durch. Dadurch vergrößern sich der digitale Fußabdruck und die Angriffsfläche, wie in Kapitel 2 und 3 deutlich wird.

Mit der Einführung neuer Technologien und deren Harmonisierung mit Altsystemen wächst die Komplexität, was im Umkehrschluss auch das Risiko für Cyberattacken ansteigen lässt [43], [44], [49], [75]. In einem ähnlichen Zusammenhang spielt ebenfalls die im Berichtszeitraum noch anhaltende pandemische Lage, ausgelöst durch COVID-19, eine entscheidende Rolle. Durch die Pandemie haben das hybride Arbeiten und die cloudbasierte Abwicklung von Geschäftsabläufen zugenommen und führen zu neuen Sicherheitsproblemen [35], [36].

Dieser Umstand wird durch Cyberkriminelle opportunistisch ausgenutzt, indem beispielsweise in Erpressungswellen mit Angriffen auf die Unternehmensinfrastruktur gedroht wird [13] oder gezielt Protokolle attackiert werden, deren Nutzung während der Pandemie zum Alltag wurden [36]. Europol wie auch das BKA meldet im selben Kontext vermehrt durchgeführte Betrugskampagnen [14], [36].

Ebenso richten sich Angriffe gegen Staat und Verwaltung. Allein in Deutschland werden täglich Angriffe auf Regierungsnetze, beispielsweise durch gezielte Attacken auf die Bundesverwaltung, aus dem Internet durchgeführt [13]. Das BKA berichtet zusätzlich von einer steigenden Anzahl von Angriffen auf die kritische Infrastruktur (KRITIS) [14]. Explizit politisch motivierte Ziele werden spätestens mit der Störung von demokratischen Prozessen durch staatliche und nichtstaatliche Akteure deutlich. Mit der Absicht, politische Wahlen im Vorfeld zu beeinflussen, wurden in der jüngeren Vergangenheit beispielsweise in Frankreich und im Vereinigten Königreich teils schützenswerte Informationen zuerst durch Cyberattacken gestohlen und später veröffentlicht [13].

Eine weitere Form der hybriden Bedrohung, bei der aktiv illegitime Einflussnahme auf Staaten betrieben wird, um diesen zu schaden oder sie zu destabilisieren, hält der geopolitische Konflikt bzw. Krieg zwischen der Ukraine und Russland vor Augen. Er zeigt, dass Cyberangriffe Einzug in die strategische Kriegsführung halten. Spezielle Cyberattacken zielen darauf ab, die Funktionsfähigkeit angegriffener Einrichtungen zu beeinträchtigen, aber auch das Vertrauen der Öffentlichkeit in die Führung des Landes zu untergraben, Angst, Unsicherheit und Zweifel zu streuen und Desinformationskampagnen zu erleichtern [33], [69]. Ebenfalls lässt sich seit Beginn des Ukraine-Krieges eine Mobilmachung von sogenannte IT-Armeen feststellen [22]. Es findet eine verstärkte Solidarisierung von hacktivistischen oder anderen Gruppierungen auf beiden Seiten der kriegerischen Auseinandersetzung statt. Hacktivisten sind Gruppierungen, die aus politischen oder anderen Zwecken hacken.

Im Berichtszeitraum ziehen durchgeführte Operationen auch gewisse Kollateralschäden für andere Staaten mit sich, so dass insbesondere im Cyberraum für Deutschland und andere europäische Staaten sich die Bedrohungslage zunehmend verschärft [13].

1.3 Modi Operandi der Angreifer

Cyberkriminalität schürt berechtigte Sorgen und Ängste vor der zunehmenden Bedrohung durch Cyberangriffe. Nach aktuellen Umfragen berichten 91 Prozent der Unternehmen, dass sie bereits von mindestens einem Sicherheitsvorfall betroffen waren [28]. Im Folgenden werden zusätzlich zu den genannten Schäden die korrespondierenden aktuellen Trends und Methoden der Bedrohungsakteure beleuchtet, die besonders bezeichnend für den Berichtszeitraum sind. Dabei werden auch das cyberkriminelle Ökosystem und das globale Umfeld gleichermaßen mit einbezogen. Die untere Tabelle liefert hierfür einen ersten Orientierungspunkt. In diesem Zusammenhang beschreibt der Angriffsvektor eine bestimmte Kombination aus Techniken und Methoden, die der Angreifer nutzt, um seine Ziele zu erreichen.

Schäden	Mögliche Angriffsmethoden
Datendiebstahl/-abfluss	Ransomware, Malware, Phishing, Social Engineering, Spam, Supply-Chain-Angriffe
Erpressung	Distributed Denial of Service, Ransomware, Supply-Chain-Angriffe
Betrug	Phishing, Social Engineering, Spam
Betriebsunterbrechungen	Distributed Denial of Service,, Malware, Ransomware, Supply-Chain-Angriffe

Zuordnung von Schäden und möglichen Angriffsvektoren bzw. -methoden

1.3.1 Social Engineering immer noch das profane Einfallstor

Social Engineering gehört zu den ältesten und zugleich zu den aktuellen Bedrohungen aus dem Cyberraum. Dies ist eine wesentliche Erkenntnis aus der vergleichenden Analyse.

Es umfasst verschiedenste Aktivitäten, die versuchen über den Faktor Mensch neue Angriffswege zu eröffnen. Mit Manipulationstechniken sollen Opfer dazu gebracht werden, sensible Informationen preiszugeben oder sich falsch zu verhalten. So wird beim Phishing dazu verleitet, angehängte Dateien aus betrügerischen E-Mails zu öffnen, bösartige Websites zu besuchen und Zugang zu firmeninternen Systemen zu gewähren. Beim sogenannte Finance Phishing zielt der Angreifer beispielsweise darauf ab, an die Einwahldaten des Online-Bankings seines Opfers zu gelangen. Social Engineering tritt neben Spam und Phishing über verschiedenste Medien, auch als Betrugstechnik wie Investment Fraud und CEO Fraud (auch als „whaling“ bezeichnet) auf [33].

Nach behördlichen Einschätzungen gehören angewendete Techniken des Social Engineering zu den größten Bedrohungen [13], [14], [36], [33]. Dies ist nicht weiter verwunderlich, da 82 Prozent der Sicherheitsvorfälle, bei denen eine unautorisierte Offenlegung schützenswerter Informationen tatsächlich erfolgte, auf menschliches Fehlverhalten zurückzuführen sind, über 60 Prozent davon durch Phishing [36], [74].

Durch den massenweisen Abgriff von sensiblen Daten können, beispielsweise über den Verkauf auf Untergrundmarktplätzen, weitere Straftaten und erhebliche Schäden folgen [14]. Berichten zufolge werden gestohlene Zugangsdaten (zum Beispiel durch Infostealer Malware; siehe Kapitel 4) häufig dazu verwendet, um über unternehmensinterne E-Mail-Adressen weitere Informationen über potenzielle Opfer auszuspionieren. Diese Informationen können anschließend dazu genutzt werden, um beispielsweise bei einer der finanziell erfolgreichsten Arten der Cyberkriminalität, BEC-Angriffen, realistische Vorwände zu nutzen, um Vertrauen bei Opfern aufzubauen [33]. Bei der wohl verbreitetsten Social-Engineering-Aktivität, dem Spam, lag die Quote aller eingehenden E-Mails laut dem BSI im Berichtszeitraum bei durchschnittlich 58 Prozent. Bei rund 70 Prozent der Spam-Nachrichten handelte es sich um tatsächliche Angriffe. Bemerkenswert war eine Spam-Welle mit erpresserischem Hintergrund im Dezember 2021 und Februar 2022, die auf Netze des Bundes gerichtet war [13].

Phishing gilt als größter Haupteintrittsvektor für Schadprogramme und tritt neben seiner bekanntesten Form, der E-Mail, ebenfalls über täuschend echt wirkende Fake-Webseiten, SMS, Telefonie oder in den sozialen Medien auf [14], [33]. Obwohl mit 2,9 Prozent nur ein geringer Anteil der Angestellten durch Phishing-E-Mails getäuscht wird, ist dies über die massenweise Erreichbarkeit von E-Mail-Postfächern immer noch ein für den Angreifer lohnendes Geschäft [74]. Phishing-Nachrichten nehmen zusätzlich häufig Bezug auf gesellschaftliche Ereignisse. Durch knappe Zeitfristen und die Androhung von Geldstrafen wird eine Angstkulisse beim Empfänger aufgebaut und dessen Unsicherheit bewusst ausgenutzt.

Die am häufigsten imitierten Absender von Spam-Nachrichten waren 2021 u.a. sehr bekannte Unternehmen aus der Logistikbranche und Software-Branche sowie Suchmaschinenanbieter und Messenger-Dienste. Seit der Corona-Pandemie konnte laut Erkenntnissen der Anti Phishing Working Group ein fortwährend starker Anstieg der Phishing-Zahlen beobachtet werden [14]. Der Finanzsektor war hierbei im Jahr 2021 weltweit am stärksten betroffen. Doch auch im Gesundheitswesen, bei Verwaltungen und Dienstleistern konnte dieser Anstieg verzeichnet werden [14]. Die Auswirkungen des Ukraine-Krieges zeigten sich im Finance Phishing in Fälschungen des Corporate Designs von Banken und dem Versenden von Spam-E-Mails zur angeblichen Überprüfung von Sanktionen [13].

Neben den geringen Kosten für die Anmietung einer Phishing-Service-Infrastruktur, welche nach Angaben des BKA bei nur rund 94 Euro im Monat beginnen, verursacht die zunehmende Automatisierung weiter neue Gefahren [14]. Die Angreifer können neben einem Dienstleistungsmodell wie Phishing as a Service (PaaS) zusätzlich auf vorgefertigte Werkzeuge und Dienste zur Einrichtung einer Social-Engineering-Kampagne, mitsamt einer zugehörigen Phishing-Website, zurückgreifen. Mo-

derne Phishing-Werkzeuge sind laut Einschätzung eines bekannten Software-Konzerns so ausgefeilt, dass sie in Bezug auf Rechtschreibung, Grammatik und Bildinhalte als legitim beim Empfänger bzw. potenziellen Opfer wahrgenommen werden. Teilweise werden erlangte Daten nicht nur an die eigentlichen Angreifer, sondern zusätzlich an die Inhaber solcher Dienste weitergeleitet und dadurch verschärft sich die Bedrohungslage weiter [33]. Mit dem Einzug von Künstlicher Intelligenz (KI) bei Social Engineering lassen sich zunehmend kriminelle Nutzungen beobachten. Derzeitige Entwicklungen für KI-Sprachmodelle bergen hinsichtlich der fortlaufenden Automation neue Gefahren. So lassen sich insbesondere kurze automatisch generierte Texte kaum von denen eines Menschen unterscheiden [13].

1.3.2 Das Schweizer Taschenmesser: Ransomware, Malware & Co.

Malicious Software (Malware) ist ein Überbegriff für schadhaften Programmcode, welcher nicht autorisierte Prozesse auf einem infizierten System ausführt (Remote Code Execution (RCE)) und sich dadurch negativ auf dessen Vertraulichkeit, Integrität und Verfügbarkeit auswirkt. Darunter fallen u.a. auch Programme wie Viren, Würmer, Spyware oder auch Ransomware [33]. Infolge der Brisanz von Ransomware wird im weiteren Verlauf insbesondere auf diese eingegangen.

Ransomware ist nach Einschätzungen von BSI, ENISA und FBI die größte Cyberbedrohung im Berichtszeitraum [13], [33], [38]. Sie zielt darauf ab, die Kontrolle über Vermögenswerte in Form von Daten zu erlangen. Dies gelingt unter Anwendung von Verschlüsselungstechniken, so dass Betroffene nicht mehr auf ihre Daten zugreifen können. Anschließend werden sie von der Malware zu Lösegeldzahlungen aufgefordert, um die Verfügbarkeit ihrer Daten mit dem auf der Angreiferseite vorhandenen Entschlüsselungsschlüssel wieder herzustellen. Angriffe durch Ransomware beschränken sich aber nicht nur auf die reine Verschlüsslung der Daten. Seit einigen Jahren nimmt, neben der allgemein zunehmenden Anzahl an Ransomware-Vorfällen, auch die Gefahr durch zusätzliche Strategien – die sogenannte Double bzw. Triple Extortion – zu [13].

Hierbei kooperieren oft unterschiedliche Angreifer oder nutzen Ransomware as a Service (RaaS) bzw. Ransomware-Affiliate-Programme, um Opfer nach dem Verschlüsselungsschritt obendrein unter Druck zu setzen.

Bei der Double Extortion wird mit der Veröffentlichung bzw. dem Verkauf der Daten gedroht. Nach aktuellen Erkenntnissen machen diese Drohung 47 Prozent der Angreifer tatsächlich wahr [31], was auch durch weitere Beobachtungen bestätigt ist [25].

Eine weitere Eskalationsstufe ist die Triple Extortion, bei der eine weitere Androhung von Angriffen auf die Verfügbarkeit der Opfersysteme ausgesprochen wird und welche im Berichtszeitraum an erhöhter Relevanz gewinnt [14], [33].

Insgesamt kann Ransomware als die Hauptbedrohung für Staat, Wirtschaft und Gesellschaft verstanden werden [13], [2]. Dabei lässt sich im Falle der Wirtschaft keine konkrete Zielgruppe identifizieren. Organisationen jeglicher Größe sind von Ransomware-Angriffen betroffen [65]. Die Angreifer visieren jeden Sektor an und machen hier keinen Unterschied zwischen Industrie, Behörden oder beispielsweise dem Gesundheitsbereich [31]. In Fällen, in denen es zu einem bestätigten Verlust von Daten gekommen ist, nimmt die Nutzung von Ransomware immer weiter zu [74].

Rund 28 Prozent der Unternehmen, welche Informationen über Vorfälle veröffentlicht haben, waren von Ransomware-Attacken betroffen [35], [65]. Hier zeigt sich ein eindeutiger Trend. Waren 2019 noch unter fünf Prozent der Unternehmen betroffen, steigt diese Zahl von Angriffen bis in den Berichtszeitraum stetig an [74]. Dabei sind meist nur Fälle bekannt, in denen die Opfer weder Schweigegeld noch Lösegeld bezahlt haben. Aufgrund einer hohen Dunkelziffer nicht gemeldeter Fälle kann davon ausgegangen werden, dass der Anteil an tatsächlichen Ransomware-Angriffen höher einzuschätzen ist [13].

Durch die zunehmenden Abhängigkeiten von Lieferketten erhöht sich die Gefahr durch Ransomware weiter. Wird ein Unternehmen in der Lieferkette getroffen, kann dies zum Problem im gesamten Geschäftsablauf führen. Mit RaaS und einschlägigen Affiliate-Programmen bietet das Untergrundökosystem den Angreifern alle Tools, die benötigt werden, um IT-Systeme von Opfern erfolgreich anzugreifen. Durch diese Professionalisierung werden die Angriffe gezielter auf lohnende Ziele durchgeführt. Dies spiegelt sich auch in den Forderungen der Angreifer wider. Nach Angaben von Europol sind sie in den letzten Jahren im Durchschnitt um 170 Prozent gestiegen [36]. Die Kosten für das Beschaffen von gängigen Ransomware-Programmen liegen in einer Bandbreite von 550 Euro bis 1200 Euro [57].

Nach BSI-Berichten spielt Ransomware außerdem eine erhebliche Rolle in der geopolitischen Auseinandersetzung zwischen Russland und der Ukraine. In den ersten Tagen des Krieges wurden vermehrt Wiper-Attacken beobachtet, mit dem Ziel, ukrainischen Banken massiv zu schaden.

Als eine spezielle Unterart der Ransomware dient ein Wiper nicht dem Zweck, Löse- oder Schweigegelder zu erpressen. Im Gegensatz zu Ransomware ist bei einem Wiper technisch nicht vorgesehen, die Daten wieder zu entschlüsseln, und hier sind diese Daten unwiederbringlich verloren. Dementsprechend bieten Wiper eine solide Grundlage, Daten-Infrastrukturen zu zerstören. Indizien zur Nutzung von Wipern finden sich außerdem bei dem Versuch, ein ukrainisches Umspannwerk zu attackieren. Zum einen sollte eine Wiper-Instanz die Betreiber dabei behindern, die Kontrolle über das Umspannwerk zurückzugewinnen. Zum anderen sollten weitere Instanzen wiederum spezielle Server-Systeme schädigen. Insgesamt verlief diese Attacke nicht nach Plan, denn sie konnte vorzeitig erkannt werden, bevor Teile der Energieversorgung des Landes hätten ausfallen können [13]. Dass Wiper-Techniken bzw. übliche Ransomware darüber hinaus sehr effektiv sind, zeigt der Angriff auf Costa Rica, welcher im Frühjahr 2022 in einem Katastrophenfall mündete.

1.3.3 Vermehrte Angriffe auf die Verfügbarkeit

Neben der Platzierung von Ransomware auf Endpunkten (zum Beispiel Laptops, Desktop PC) durch die Ausnutzung von Systemschwachstellen, Fehlkonfigurationen oder Techniken des Social Engineering als bewährte Infiltrationsstrategien gehört auch Distributed Denial of Service (DDoS) zu den beliebtesten und zugleich verheerendsten Angriffsmethoden. Sie sind deshalb so verheerend, weil sie das Ziel haben, die Verfügbarkeit von Netzwerk- und Computersystemen durch eine Flut von Datenverkehr zielgerichtet zu „überfordern“. So sind bei einer solchen Attacke betroffene Systeme gar nicht oder nur noch eingeschränkt operativ nutzbar.

Mit genügend krimineller Energie ergeben sich dadurch wiederum entscheidende Handlungsoptionen, die im Berichtszeitraum ein bisher ungekanntes Ausmaß angenommen haben. Damit das Potenzial dieser Angriffe allerdings zum Tragen kommt, bedarf es einer gewissen Systematik. In den meisten Fällen ist für einen Angriff eine Vielzahl von Computerressourcen erforderlich, damit genügend Datenvolumen und Bandbreite generiert werden können, um effektiv ein anvisiertes Zielsystem zu attackieren. Hierfür machen sich Angreifer in der Regel im Vorfeld sogenannte Botnetze zu Nutze. In ihrer Gesamtheit bestehen sie aus vielen einzelnen kompromittierten Computersystemen, die im Kollektiv die nötige „Schlagkraft“ für einen DDoS-Angriff aufweisen und bequem nach dem CaaS-Prinzip von Angreifern angemietet werden können. Nach aktuellen Recherchen des BKA werden auf Untergrundmarktplätzen, in Abhängigkeit von der Größe, Botnetz-Infrastrukturen bereits zwischen 75 Euro und 1400 Euro pro Monat angeboten [14].

Solche vorbereiteten Infrastrukturen, gepaart mit einer verhältnismäßig niedrigen Preisschwelle, begünstigen die vermehrte Nutzung von DDoS durch Cyberkriminelle. Für das Jahr 2021 konnte durch unterschiedliche Mitigationsdienstleister ein bezeichnender Anstieg von DDoS-Angriffen in Deutschland beobachtet werden. Einer dieser Quellen zufolge lag der Zuwachs sogar bei 41 Prozent im Vergleich zum Vorjahr [13]. Dies machte sich u.a. durch eine signifikante Häufung von Vor-

fällen in Relation zu Ransomware bemerkbar, um die Erfolgschancen von Erpressungskampagnen sukzessive zu steigern. Aber auch solche Erpressungswellen, die nicht so raffiniert sind und ausschließlich DDoS-Techniken nutzen, sind prävalent. Beide unter dem Begriff Ransom Denial of Service (RDoS) zusammenfassbaren Maschen der Cyberkriminellen richten sich nach Berichten von Europol vornehmlich gegen Internetdiensteanbieter, KMUs und Finanzinstitute [33].

Nach Untersuchungen des Financial Services Information Sharing and Analysis Center (FS-ISAC) gehört RDoS sogar zu den drei relevantesten Bedrohungen für den gesamten Finanzsektor [40]. So wurden insgesamt im Netz des größten deutschen Telekommunikationsanbieters durchschnittlich 2335 DDoS-Angriffe im Monat für das Jahr 2021 beobachtet, wobei der längste Angriff 82 Tage andauerte [14]. Darüber hinaus lassen sich in der Häufigkeitsverteilung aktueller und vergangener Statistiken saisonal Auffälligkeiten erkennen. Vor allem vor und während umsatzstarker Zeiträume im E-Commerce (vgl. Black Friday, Weihnachtsgeschäft etc.) steigt die Anzahl an Vorfällen markant an [13], [14]. Allein in der E-Commerce-Aktionswoche „Cyber-Week“ hat sich im Jahr 2021 die Anzahl an DDoS-Vorfällen nach Angaben des BSI im direkten Vergleich zum Vorjahr verdoppelt [13].

Mit diesem sich manifestierenden Trend erreichten DDoS-Angriffe auch neue Rekordzahlen, gemessen an ihren Bandbreiten und Anfrageraten. Sie sind in Bezug auf den Berichtszeitraum und frühere Beobachtungen beispiellos [13], [14]. So konnten im August 2021 bei einem Versuch, die Verfügbarkeit eines Cloud-Dienstes zu beeinträchtigen, Spitzenwerte von 2,4 Terabits pro Sekunde aufgezeichnet werden [62]. Nach Angaben des Dienstleisters stammte der Angriff aus ca. 70.000 Quellen in unterschiedlichen Ländern und erreichte innerhalb weniger Sekunden die gesamte Schlagkraft. Damit lag dieser skizzierte Vorfall beim 3,5-Fachen der vom BSI berichteten durchschnittlichen Bandbreite für solche Attacken in Deutschland und war doppelt so hoch wie der Rekord aus dem Jahr 2021 [13]. Im Zusammenhang mit diesem bemerkenswerten Vorfall muss ebenfalls Erwähnung finden, dass Cloud-Plattformen seit der Corona-Pandemie insgesamt populäre Ziele für DDoS-Angriffe sind. Sie erweitern die Angriffsfläche und erhöhen die Wahrscheinlichkeit für Organisationen und Unternehmen, Opfer eines DDoS-Angriffs zu werden. Im Zuge der Übergangszeit zu Online-Technologien während der Pandemie waren besonders die Telekommunikationsbranche, das Finanzwesen, die Computerspiele-Industrie, der E-Commerce und das Gesundheitswesen davon betroffen [33].

Zusätzlich haben nicht finanziell motivierte Cyberkriminelle zu der skizzierten neuen Qualität von Angriffen auf die Verfügbarkeit beigetragen. Auch politisch motivierte Aktivitäten entwickeln sich im Berichtszeitraum eher zur Norm als zur Ausnahme. Im Jahr 2021 wurden eine Reihe von Zwischenfällen bekannt, bei denen Behörden und Organisationen unterschiedlicher Länder angegriffen wurden. Im Zusammenhang mit der Bundestagswahl wurde die Website des Bundeswahlleiters attackiert. Zudem hat der zugespitzte geopolitische Konflikt bzw. Krieg zwischen Russland und der Ukraine bis jetzt offenbart, dass Angriffe auf die Verfügbarkeit eine zentrale Rolle in der modernen Kriegsführung spielen können. Gerade zu Beginn des Krieges wurden im Februar 2022 von Russland koordinierte DDoS-Attacken gegen ukrainische Regierungs- und Finanzinstitutionen beobachtet.

Mit zunehmenden Landgewinnen auf russischer Seite wurde zusätzlich physische Einflussnahme auf die Verfügbarkeit der Internet-Infrastruktur betrieben, so dass ukrainischer Datenverkehr über russische Netze umgeleitet werden konnte. Auf diese Weise war Russland in der Lage, systematisch Zugänge zu sozialen Medien zu blockieren, die Weitergabe von Informationen zu unterbinden und Überwachungsmaßnahmen für bestimmte geografische Bereiche innerhalb der Ukraine zu platzieren. Außerdem stört Russland aktiv Mobilfunknetze, um die ukrainische Bevölkerung dazu zu zwingen, russische Dienste zu nutzen. Seitdem sucht die Ukraine nach Möglichkeiten, den Betrieb dieser KRITIS aufrechtzuhalten. Eine eingesetzte Alternative ist das Ausweichen auf Satelliten-Internetsysteme. Aktive Zensierung betreibt Russland in diesem Zusammenhang auch gegen das eigene Volk [33]. Mit weiterem Verlaufe des Kriegs konnten darüber hinaus vermehrt Aktivitäten durch Hacktivismus insbesondere in Verbindung mit DDoS verzeichnet werden. Proukrainische Gruppierungen attackieren dabei gezielt russische Systeme oder Unternehmen mit enger Beziehung zu Russland.

Dabei gab es auch Kollateralschäden mit Auswirkungen auf Deutschland, als ein deutscher KRITIS-Betreiber, der Teil eines russischen Ölkonzerns ist, zum Ziel wurde [13]. Prorussische Gruppierungen wie Killnet attackierten im Gegenzug deutsche Rüstungsunternehmen, Behörden oder Flughäfen, nachdem die positive politische Entscheidung für die Lieferung von Leopard-Panzern in die Ukraine erfolgt war.

1.3.4 Einblicke in russische Computer Networked Operations

Verärgert über den Krieg in der Ukraine, wurden tausende interne Dokumente des russischen IT-Sicherheitsunternehmens NTC Vulkan aus den Jahren 2016-2021 an den Journalisten Hannes Munzinger der Süddeutschen Zeitung gesendet [29]. An der Auswertung waren elf Medienhäuser aus acht Ländern beteiligt. Die Unterlagen („Vulkan Files“) geben Einblicke in die offensiven Cyberfähigkeiten für Computer Network Operations (CNO) der russischen Föderation.

Gegründet wurde das russische Unternehmen NTC Vulkan von Anton Markov und Alexander Irzhavsky; beide sind Absolventen der Militärakademie in St. Petersburg. Markov ist ehemaliger Kapitän, Irzhavsky ein Major der russischen Armee. Mit mehr als 120 Mitarbeitern, von denen die Hälfte Softwareentwickler sind, wurden sie schnell erfolgreich. Zu den Kunden zählten Aeroflot, Sberbank oder die russische Eisenbahn [73]. Ab 2011 erhielt NTC Vulkan Aufträge für die drei russischen Geheimdienste: der Militärnachrichtendienst GRU, der Auslandsnachrichtendienst SWR und der Inlandsgeheimdienst FSB. Dazu gehören die Entwicklung der Produkte Scan-V, Amezit und Crystal-2V.

Scan-V durchsucht das Internet nach bekannten Schwachstellen und speichert diese Daten, um sie für zukünftige Cyberangriffe nutzen zu können [29]. Siehe hierzu auch die Ergebnisse der digitalen Angriffsfläche deutscher Organisationen in Wirtschaft und öffentlichen Sektor in Kapitel 2.

Amezit ist eine Lösung zur Kontrolle des Nutzerverhaltens im Internet [68] im Sinne der Telekommunikationsüberwachung (TKÜ). Darüber hinaus erlaubt es die Erstellung gefälschter Social-Media-Konten für Desinformationskampagnen [29].

Crystal2V ist ein Trainingsprogramm für offensive Cyberoperationen der Mitarbeiter von Militär und Geheimdienst [73].

NTC Vulkan arbeitete eng mit der staatsnahen Hackergruppe Sandworm (auch bekannt als „Einheit 74455“) zusammen [68]. Sandworm führte erfolgreiche CNO Kampagnen gegen zahlreiche Ziele in der Ukraine und die olympischen Spiele in Südkorea durch. Sandworm ist vor allem für die Malware NotPetya [77] [78] bekannt, welche weltweit Schaden von über 10 Milliarden Euro angerichtet haben soll.

Ehemalige Softwareentwickler von NTC Vulkan leben mittlerweile in Deutschland, Irland und anderen EU-Ländern. Laut den Ermittlungen von „Der Spiegel“, arbeiten ungefähr 90 ehemalige NTC-Vulkan Mitarbeiter, in diversen Unternehmen in der EU, unter anderem bei AWS und Siemens [68]. Dabei stellt sich die Frage, welche Interessen diese Softwareentwickler inzwischen verfolgen, sprich ob sie ein Sicherheitsrisiko („Double pay roll“) darstellen.

1.3.5 Lieferketten im Visier der Angreifer

Als eine immer größer werdende und damit ernstzunehmende Gefahr gelten Angriffe auf die Lieferkette oder sogenannte Supply-Chain-Attacken [13], [14], [33], [51], [66]. Galten im Jahr 2020 noch unter ein Prozent der Angriffe Lieferketten, liegt dieser Anteil im Berichtszeitraum, abhängig von unterschiedlichen Berichten, nun deutlich höher. Betrachtete Analysen zeigen einen Anstieg bei Angriffen auf die Lieferketten zwischen 17 Prozent und 62 Prozent [33], [75], [74].

Bei solchen Attacken werden „schwache Glieder" bzw. Schwachstellen in der Lieferkette eines Unternehmers gezielt angegriffen, um u.a. über Umwege das eigentliche Zielsystem zu erreichen, so dass Profit für den Angreifer entsteht. Damit setzen Cyberkriminelle genau an dem Vertrauen an, welches Unternehmen ihren Kunden, Lieferanten oder Drittanbietern entgegenbringen.

Als Beispiel soll an dieser Stelle die Finanzbranche angeführt werden. Durch starke Abhängigkeiten in Unternehmensstrukturen zu Anbietern und Lieferanten besteht für sie ein erhebliches Risiko, Opfer eines Lieferkettenangriffs zu werden. Zwar sind Finanzinstitute auf Basis starker Regulierung häufig besser abgesichert, aber mehrere öffentlichkeitswirksame Vorfälle bei Drittanbietern haben gezeigt, dass auch sie von solchen neuartigen Attacken beeinträchtigt werden können [40]. Viele dieser und weiterer Lieferkettenvorfälle wurden mit Ransomware-Angriffen verknüpft, womit Cyberkriminelle mit einer einzigen Kompromittierung ihren Aktionsradius sukzessive erweitern konnten [33].

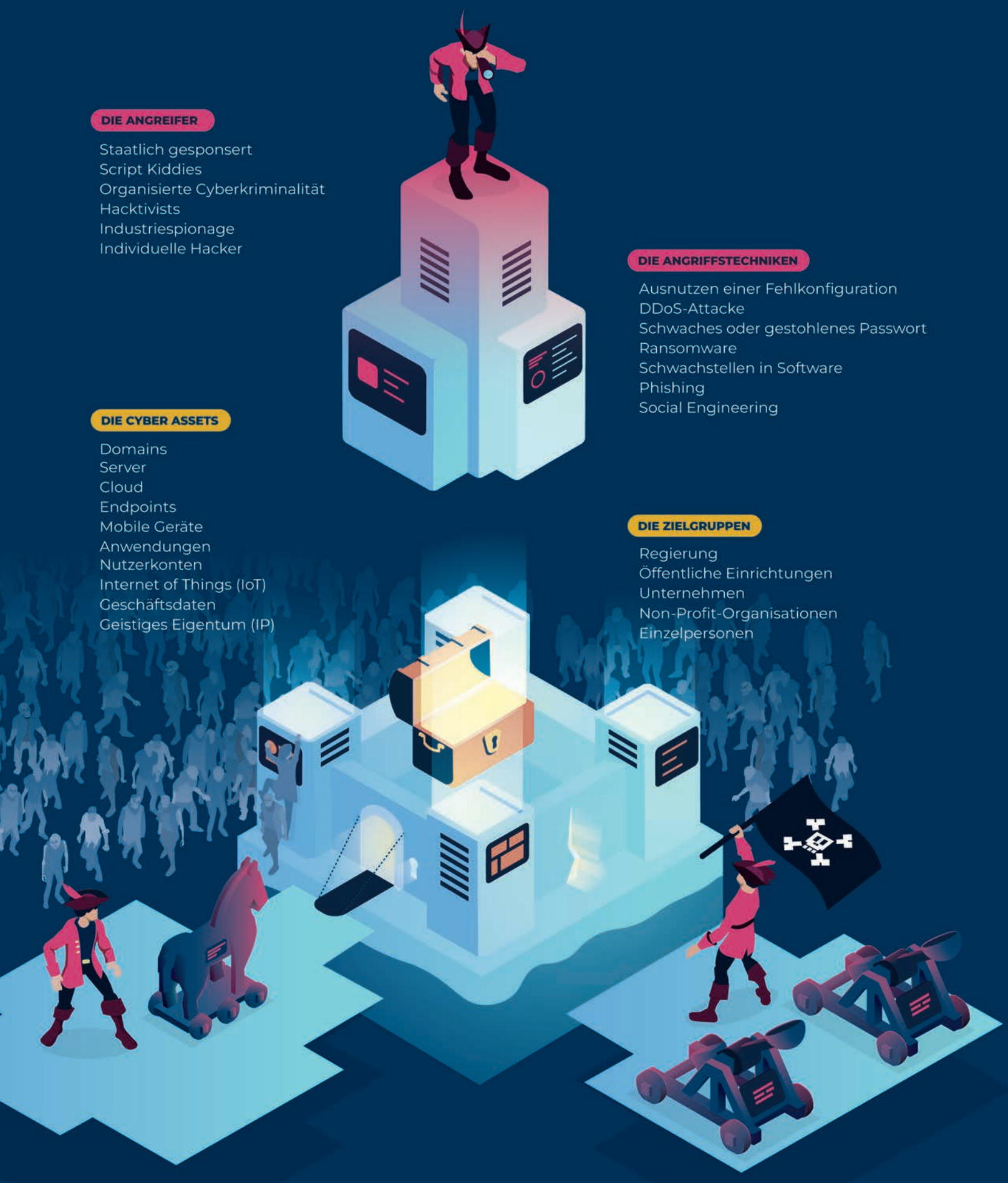
Der wohl prominenteste Lieferkettenangriff war der 2020 verübte Angriff auf ein Software-Produkt für Server-Management (Solarwinds), bei dem eine Hintertür (Backdoor) etabliert werden konnte. Über diese konnten die Angreifer über die Softwareentwicklung in Osteuropa Kontrolle über Systeme erlangen. Nach einem Update des Herstellers konnte diese Backdoor auf Systeme von bis zu 18.000 Kunden gelangen und einen Schaden bei einer Vielzahl von Großunternehmen und US-Regierungseinrichtungen anrichten [40].

Dass Schwachstellen auf fast jedem Weg in ein Unternehmen gelangen können, zeigt eine im Jahr 2021 entdeckte Schwachstelle in Log4j, einer freien Programmbibliothek zur Protokollierung, die standardmäßig in vielen Systemen Verwendung findet. Nach Schätzungen war die Schwachstelle der Öffentlichkeit acht Jahre nicht bekannt und auf hunderten Millionen Geräten weltweit zu finden [58]. Sie wurde von mehreren staatlich finanzierten und weiteren organisierten Akteuren massiv ausgenutzt, bevor sie Ende des Jahres 2021 geschlossen wurde [25].

Ähnlich können öffentliche Clouds für Unternehmen zum Problem werden, sofern sie Vorlagenprofile Dritter nutzen, um eine persönliche Umgebung für sich in der Cloud zu errichten [22], [25], [26], [33], [41], [44]. Dies wird durch die Analysen in Kapitel 3 unterstrichen.

2 Angriffsflächen einer digitalen Welt

CYBERANGRIFFE
ANGRIFFSFLÄCHEN EINER DIGITALEN WELT



DIE ANGREIFER

Staatlich gesponsert
Script Kiddies
Organisierte Cyberkriminalität
Hacktivists
Industriespionage
Individuelle Hacker

DIE ANGRIFFSTECHNIKEN

Ausnutzen einer Fehlkonfiguration
DDoS-Attacke
Schwaches oder gestohlenes Passwort
Ransomware
Schwachstellen in Software
Phishing
Social Engineering

DIE CYBER ASSETS

Domains
Server
Cloud
Endpoints
Mobile Geräte
Anwendungen
Nutzerkonten
Internet of Things (IoT)
Geschäftsdaten
Geistiges Eigentum (IP)

DIE ZIELGRUPPEN

Regierung
Öffentliche Einrichtungen
Unternehmen
Non-Profit-Organisationen
Einzelpersonen

ANWENDUNGSSICHERHEIT

Mindestens eine hochkritische Schwachstelle [1]

HÄNDLER

STÄDTE

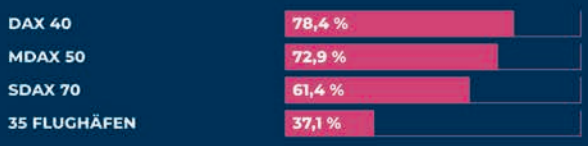
100%

ALLER 8 UNTERSUCHTEN HANDELSUNTERNEHMEN

90%

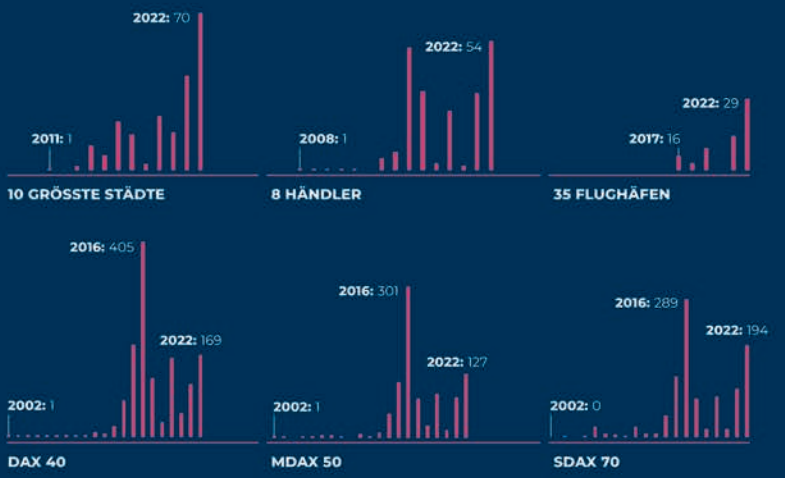
DER 10 GRÖSSTEN STÄDTE DEUTSCHLANDS

wiesen mind. eine Schwachstelle in ihren Anwendungen auf.



KRITISCHE SCHWACHSTELLEN

Anzahl der nicht adressierten Schwachstellen nach dem Jahr ihrer Veröffentlichung



DNS-KONFIGURATION

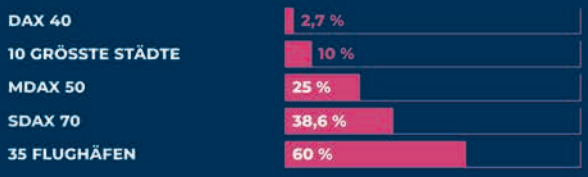
SPF-Eintrag [2] in Mailserver-Konfiguration

HÄNDLER

0%

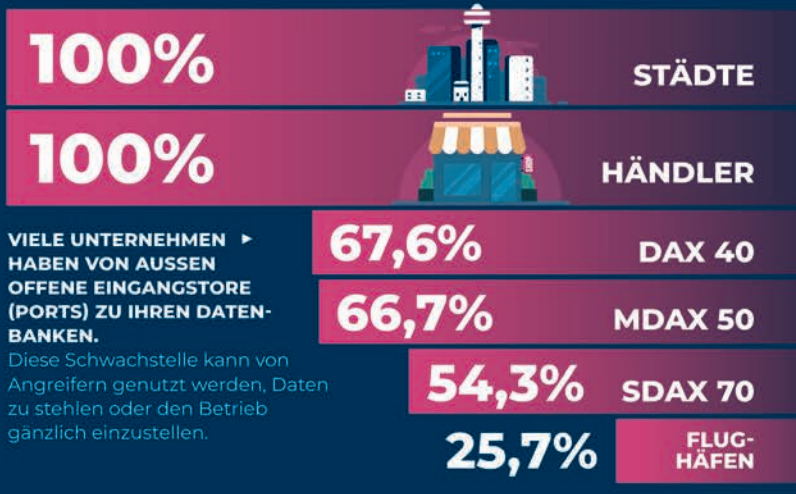
◄ **KEINES DER UNTERSUCHTEN HANDELSUNTERNEHMEN HATTE EINEN SPF-EINTRAG [2] FÜR E-MAILS KONFIGURIERT.**

Der SPF-Eintrag [2] ist eine wichtige technische Maßnahme, um zu verhindern, dass Dritte Ihre E-Mail-Identität kapern und für Cyberkriminalität nutzen (z.B. Phishing-Kampagnen).



NETZWERKSICHERHEIT

Erreichbarkeit von Datenbanken über das Internet

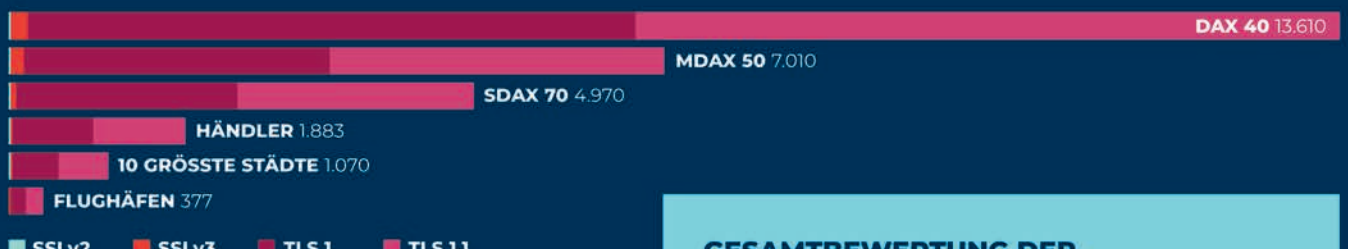


VIELE UNTERNEHMEN HABEN VON AUSSEN OFFENE EINGANGSTORE (PORTS) ZU IHREN DATENBANKEN. ►

Diese Schwachstelle kann von Angreifern genutzt werden, Daten zu stehlen oder den Betrieb gänzlich einzustellen.

ANZAHL VERALTETER VERSCHLÜSSELUNGSPROTOKOLLE

Ist der Datenfluss zwischen Mitarbeitern, Kunden und Partnern vor dem Zugriff Dritter geschützt?



▲ **ES WIRD DEUTLICH, DASS INSGESAMT EINE STARK VERBREITETE NUTZUNG VERALTETER VERSCHLÜSSELUNGSPROTOKOLLE VORHERRSCHT.**

Diese Protokolle sind bekannt dafür, dass sie von Cyberkriminellen ausgenutzt werden können, um an sensitive Daten zu gelangen.

GESAMTBEWERTUNG DER ANGRIFFSFLÄCHE

Der Höchstwert liegt bei 100 und basiert auf der Kritikalität der Ergebnisse in den einzelnen Bewertungskategorien.

80 PUNKTE GELTEN ALS GUTES ERGEBNIS

1) Schwachstelle mit einem Common-Vulnerability-Scoring-System-(CVSS-)Wert von größer 7

2) SPF: Sender Policy Framework; Standardmethode zur E-Mail-Authentifizierung

Quelle: eigene Darstellung; LocateRisk

2 Angriffsflächen einer digitalen Welt

Alle Organisationen – egal ob Politik, Verwaltung, Wirtschaft oder Non-Profit-Organisation – haben heute einen komplexen digitalen Fußabdruck. Dieser ist durch das Internet von überall erreichbar und wird von Angreifern als ein zentraler Angriffsvektor genutzt. Fortschreitende Datennutzung, Vernetzung und Digitalisierung lassen ihn wachsen. Die kontinuierliche Veränderung ist sein Wesen. Die Grenzen zwischen dem Innen und Außen verschwimmen, man spricht von hybriden Umgebungen. Gleichzeitig sinken Kontrolle und Kapazitäten zur Absicherung durch die Verantwortlichen in Organisationen.

Die vorgenommene Analyse der Firmen in DAX (40), MDAX (50), SDAX (70), von acht Handelsunternehmen sowie von 35 Flughäfen und den zehn größten Städten unterstreicht dies eindrücklich. Viele große und bekannte Organisationen haben erheblichen Nachholbedarf, um ihren digitalen Fußabdruck zu schützen oder zu verringern, so dass die Grundsätze von Vertraulichkeit, Integrität und Verfügbarkeit gewahrt bleiben. Organisationen müssen ihre externe Angriffsfläche kontinuierlich bewerten und überwachen, um potenzielle Schwachstellen zu beseitigen.

Der digitale Fußabdruck einer Organisation beschränkt sich nicht mehr nur auf die Informationstechnologie (IT) in Firmenzentrale und Rechenzentrum sowie operative Technologie (OT) in Produktionsanlagen. Organisationen haben eine Vielzahl an Geschäftsbereichen, Standorten, globalen Aktivitäten, Dienstleistern, eingesetzter Hardware und Software, Partnern, Interaktionen mit Kunden und neuen Arbeitsstrukturen bzw. -formen. Cloud-Dienste, Fernwartungszugänge oder IoT-Geräte kommunizieren mit dem Internet. Moderne Webanwendungen setzen sich aus diversen Schnittstellen und Komponenten zusammen, die einen großen Funktionsumfang bieten [51], [66]. Vielfach wird dieser nicht benötigt, führt aber unbemerkt zu einer größeren Angriffsfläche. Im Bereich der Produktion sind heute OT-Systeme und Lösungen im Einsatz, die sehr lange Soft- und Hardwarelebenszyklen aufweisen [43], [46]. Sie wurden mit dem Ziel von Zuverlässigkeit, Funktionalität und Sicherheit (Safety) entwickelt – nicht jedoch Cybersicherheit. Die Gesamtheit des durch externe Akteure identifizierbaren und erreichbaren digitalen Fußabdrucks bezeichnet man als externe Angriffsfläche (External Attack Surface).

Prinzipiell sollte eine Kompromittierung externer Systeme und Netze nicht zur Kompromittierung interner Systeme führen [48]. Bei zahlreichen Angriffen werden jedoch nicht mehr Burggraben und Burgmauer (Perimeter) überwunden. Es werden gezielt Mitarbeiter privat angegriffen, um dann über deren legitime Zugangsdaten und Vertrauenswürdigkeiten an die meist zahlreich vorhandenen Systeme mit Außenanbindung zu gelangen, zum Beispiel VPN, Extranet Portal oder Exchange Online.

Zu den gängigen Strategien zur Verwaltung einer externen Angriffsfläche gehören die Implementierung von Sicherheitskontrollen wie Firewalls, Intrusion-Detection-Systemen und Zugangskontrollen sowie die Überwachung des Netzwerkverkehrs und des Benutzerverhaltens auf Anzeichen verdächtiger Aktivitäten. Regelmäßige Schwachstellenbewertungen und Penetrationstests können ebenfalls dazu beitragen, Schwachstellen in der externen Angriffsfläche eines Unternehmens zu identifizieren und zu beseitigen. Darüber hinaus müssen die Mitarbeiter in sicheren Surf- und E-Mail-Praktiken geschult werden, um das Risiko von Phishing-Angriffen und anderen Social Engineering-Techniken zu minimieren (siehe auch Kapitel 3).

Letztendlich besteht das Ziel der Verwaltung einer externen Angriffsfläche darin, das Risiko zu verringern, dass ein externer Angreifer unbefugten Zugriff auf das Netzwerk oder die Daten eines Unternehmens erlangt. Durch die sorgfältige Überwachung und Sicherung der nach außen gerichteten Systeme und Dienste kann eine Organisation ihre Anfälligkeit für externe Angriffe minimieren und die Vertraulichkeit, Integrität und Verfügbarkeit ihrer wichtigen Systeme und Daten gewährleisten.

2.1 Anwendungen

In dieser Kategorie wurde geprüft, ob die genutzte Software zum Beispiel (Microsoft Exchange Server, WordPress, Apache-Webserver etc.) veröffentlichte Sicherheitslücken (CVE) aufgrund von fehlenden Updates aufweist. Anwendungssicherheit ist einer der komplexesten und umfangreichsten Punkte im Bereich IT-Sicherheit. In der Überprüfung wurde fokussiert die von den Unternehmen im Webbereich verwendete Software wie bspw. WordPress, OpenSSL, Apache-Webserver und PHP auf fehlende Updates untersucht. Webanwendungen gehören heutzutage zum alltäglichen Leben dazu und werden in vielen Bereichen eingesetzt. Wird eine Sicherheitslücke einer verwendeten Webanwendung ausgenutzt, ist dies für den Betroffenen oftmals nicht direkt erkennbar. Selbst bei ausgereifter Software können Sicherheitslücken immer wieder auftreten.

Einige Sicherheitslücken in Anwendungen sind beispielsweise SQL Injections, Cross-Site Scripting, Remote Code Executions und Buffer Overflows. Manchmal können auch mehrere Schwachstellen gleichzeitig in einer Software vorkommen und ausgenutzt werden.

Die Gefahren solcher Schwachstellen sind vielfältig. SQL Injections betreffen beispielsweise Datenbanken. So können Unbefugte Datensätze in der Datenbank löschen, manipulieren oder sensible Daten aus der Datenbank auslesen. Dadurch können wichtige Daten gelöscht oder Kundendaten an Unbefugte gelangen.

Angriffe durch Cross-Site Scripting betten gefährliche Programmcodes in eine eigentlich sichere Umgebung ein. Es wird häufig für Phishing-Angriffe verwendet. Durch Phishing geraten Nutzerdaten und Kennwort für die betreffende Anwendung an Unbefugte. Unbefugte können sich dann Zugriff zur betroffenen Anwendung verschaffen und sich als die Person ausgeben, deren Daten gestohlen wurden.

Zuletzt erlauben Remote Code Executions das Ausführen von Schadcode auf den Unternehmensservern. Hierdurch ist es möglich, Anwendungen zu manipulieren und tiefer in das Netzwerk vorzudringen. Der Schaden für die betroffene Organisation kann damit sehr groß sein. Es können nicht nur Daten verloren gehen, sondern Unbefugte können sich beispielsweise als Mitarbeiter einer Organisation ausgeben und so Kontakt mit Kunden aufnehmen (siehe auch Kapitel 3).

Das **Common Vulnerability Scoring System (CVSS)** versucht, die Kritikalität einer Schwachstelle darzustellen, und ist der internationale De-facto-Standard. Die Bewertung von Schwachstellen erfolgt bei CVSS anhand verschiedener Metriken. Aus diesen errechnet sich ein Schweregrad von 0.0 bis 10.0. Zur Bewertung der Konsequenzen eines erfolgreichen Angriffs durch die Ausnutzung einer CVSS ist entscheidend, inwieweit die Schutzziele Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability) beeinträchtigt werden.

Für die Untersuchung mussten eine oder mehrere Schwachstellen mit einem CVSS-Wert von 7.0–8.9 (hoch) oder höher identifiziert werden.

	Mindestens eine Schwachstelle mit CVSS 7.0	Keine Schwachstelle mit CVSS 7.0
Die 10 größten Städte	90 Prozent	10 Prozent
8 Händler	100 Prozent	0 Prozent
35 Flughäfen	37,1 Prozent	62,9 Prozent
DAX 40	78,4 Prozent	21,6 Prozent
MDAX 50	72,9 Prozent	27,1 Prozent
SDAX 70	61,4 Prozent	38,6 Prozent

Identifizierte Schwachstellen im Bereich Anwendungen

2.2 Netzwerk

Steht in Ihrem Netzwerk die Zugbrücke unten, das Tor und die Fenster unbeabsichtigt offen? In dieser Kategorie wird geprüft, ob es offene Zugänge zu kritischen Diensten und Systemen wie Datenbank- und Datei-Servern gibt. Durch ein verwundbares Netzwerk können beispielsweise vertrauliche Daten an Unbefugte geraten oder Daten innerhalb des Netzwerks von außen verändert werden.

Einen solchen Zugang zum Netzwerk können Unbefugte durch die Ports bekommen. Ein Port bildet gemeinsam mit der IP-Adresse die Adresse einer Anwendung im Internet. Über diesen Port kann die Anwendung dann kommunizieren. Ein Port muss offen sein, damit die Anwendung kommunizieren kann. Da offene Ports von außen (aus dem Internet) und damit auch für Unbefugte erreichbar sind, sollten nur Ports geöffnet sein, bei denen es notwendig ist. Neben einem kompletten Schließen des Ports lässt sich der Zugriff auch auf einzelne IP-Adressen limitieren, somit können beispielsweise anstatt des kompletten Internets nur noch Standorte des eigenen Unternehmens mit dem Port kommunizieren. Oftmals werden Ports auch unabsichtlich geöffnet oder nach dem Öffnen nicht wieder geschlossen.

Kritische Ports sind ein bevorzugtes Ziel von Angreifern, da sie ihnen Zugang zu weiteren Systemen und sensiblen Daten verschaffen. Beim Angriff auf eine französische Hotelkette wurden ein Terabyte an Buchungsinformationen, Kreditkartendetails sowie Zugangsdaten von Kunden auf diese Weise gestohlen.

	Erreichbare Datenbanken	Keine erreichbaren Datenbanken
Die 10 größten Städte	100 Prozent	0 Prozent
8 Händler	100 Prozent	0 Prozent
35 Flughäfen	25,7 Prozent	74,3 Prozent
DAX 40	67,6 Prozent	32,4 Prozent
MDAX 50	66,7 Prozent	33,3 Prozent
SDAX 70	54,3 Prozent	45,7 Prozent

Netzwerksicherheit – offene Datenbanken und Ports

2.3 Verschlüsselung

Ist der Datenverkehr zwischen Ihren Mitarbeitern und Kunden oder Partnern vor dem Zugriff durch Dritte abgesichert? Kryptographische Verfahren tragen maßgeblich zur Sicherheit im Internet bei. Sie sind mathematische Verfahren, welche die Schutzziele Vertraulichkeit, Integrität und Authentizität erfüllen.

Unsichere Übertragung sensibler Inhalte im Netz macht Datendiebstahl einfach und gefährdet Unternehmen samt Lieferketten. Jede Website, die Besucherdaten abfragt, ist verpflichtet ein gültiges SSL-Zertifikat zu führen. Bei fehlender SSL-Verschlüsselung drohen Verschlechterung des Google-Rankings und Abmahnung.

In der externen Analyse wurde die Verschlüsselungsqualität der Datenverbindungen bewertet. Dabei werden auch Gültigkeit und Version der Sicherheitszertifikate (zum Beispiel SSLv3, TLS 1.0) sowie deren korrekte Implementierung überprüft.

Bei der Analyse wurden zahlreiche veraltete Verschlüsselungsmethoden identifiziert, die nicht mehr als sicher gelten. Hierbei handelt es sich um SSLv2, SSLv3, TLS 1 und TLS 1.1. Trotz der bekannten Sicherheitsrisiken setzen immer noch einige Organisationen auf diese veralteten Verfahren, wie in der beigefügten Tabelle zu sehen ist. Es ist wichtig, dass Organisationen ihre Verschlüsselungsverfahren auf aktuellem Stand halten, um so Daten und Netzwerke vor potenziellen Angriffen zu schützen. So können Angreifer, welche Zugriff auf den Netzwerkverkehr haben, diesen aufbrechen, um Daten zu stehlen oder den Netzwerkverkehr zu manipulieren. Zudem ist es Angreifern auch möglich, den Netzwerkverkehr aufzuzeichnen, um diesen dann ein paar Jahre später mit der verbesserter Rechenleistung aufzubrechen. Dies kann zum Abfluss von Forschungsdaten, zu Datenschutzverletzungen und Image-Schäden führen. Unternehmen sollten daher sicherstellen, dass sie die neuesten Verschlüsselungsstandards (Aktuell TLS 1.2 oder TLS 1.3) verwenden, und ihre Sicherheitsrichtlinien regelmäßig aktualisieren, um sich gegen ständig wachsende Cyberbedrohungen zu schützen.

	Veraltete Verschlüsselungsmethoden	Moderne Verschlüsselungsmethoden
Die 10 größten Städte	100 Prozent	0 Prozent
8 Händler	100 Prozent	0 Prozent
35 Flughäfen	74,3 Prozent	25,7 Prozent
DAX 40	100 Prozent	0 Prozent
MDAX 50	97,9 Prozent	2,1 Prozent
SDAX 70	95,7 Prozent	4,3 Prozent

Eingesetzte Verschlüsselungsmethoden

	SSLv2	SSLv3	TLS 1	TLS 1.1
Die 10 größten Städte	2	29	505	535
8 Händler	5	31	876	971
35 Flughäfen	0	7	175	195
DAX 40	4	205	6503	6898
MDAX 50	6	158	3275	3571
SDAX 70	3	72	2366	2529

Anzahl veralteter Verschlüsselungsmethoden

2.4 Bewertung der gesamten Sicherheit

Ein hoher Wert für die externe Sicherheitssituation steht für eine aufgeräumte externe Angriffsfläche, und somit für eine niedrigere Wahrscheinlichkeit eines Cybervorfalls. Der Wert hat im besten Fall einen Wert von 100, im schlechtesten Fall einen Wert von 0. Ein Wert von über 80 ist gut, ein Wert von unter 65 schlecht. Bei sicherheitsrelevanten Funden werden, je nach Kritikalität, Punkte abgezogen. Neben dem stetigen Patchen von Sicherheitslücken hilft es, seine Angriffsfläche zu verkleinern und hierdurch den Gesamtwert zu verbessern.

Die Bewertungen der Kritikalität basieren auf branchenüblichen und öffentlich verfügbaren Standards, wie zum Beispiel NIST CIS (National Institute of Standards & Technology sowie das Center for Internet Security), BSI (Bundesamt für Sicherheit in der Informationstechnik) oder OWASP (Open Web Application Security Project) und vielen mehr. Die Analysen berücksichtigen die Vorgaben der DSGVO.

	80 Prozent – 100 Prozent	**0 Prozent – 79 Prozent**
Die 10 größten Städte	0 Prozent	100 Prozent
8 Händler	0 Prozent	100 Prozent
35 Flughäfen	57,1 Prozent	42,9 Prozent
DAX 40	40,5 Prozent	59,5 Prozent
MDAX 50	27,1 Prozent	72,9 Prozent
SDAX 70	41,4 Prozent	58,6 Prozent

Ganzheitliche Bewertung der externen Sicherheitssituation

2.5 Maßnahmen zum Schutz der externen Angriffsfläche

Organisationen können verschiedene Maßnahmen ergreifen, um ihre externe Angriffsfläche zu schützen:

a. Analysieren Sie regelmäßig und möglichst ganzheitlich Ihre externe Angriffsfläche, um Ihre Risikosituation sowie die Maßnahmenpriorisierung neu zu bewerten.

b. Kontinuierliche externe Schwachstellenanalysen und Penetrationstests identifizieren potenzielle Schwachstellen, bevor sie ausgenutzt werden können.

c. Einsatz von Firewalls, Intrusion-Detection-and-Prevention-Systemen (IPS/IDS) und Web Application Firewalls (WAF). Sie helfen, unbefugten Zugriff zu verhindern sowie bösartigen Datenverkehr zu erkennen und zu blockieren.

d. Regelmäßige Patches für Systeme und Anwendungen können Angreifer daran hindern, bekannte Schwachstellen in veralteter Software auszunutzen.

e. Verwenden Sie starke Authentifizierungs-Mechanismen (Multi-Faktor-Authentifizierung; komplexe Passwörter).

f. Sensibilisieren Sie Mitarbeiter für Cybersicherheit am Heimarbeitsplatz.

3 Mit den Augen der Hacker – unsichtbare Angriffspfade

SCHWACHSTELLENMANAGEMENT
AUF DEN RICHTIGEN FOKUS KOMMT ES AN

99,6 %

Sicherheitsteams können ihren täglichen Aufwand zur Systemhärtung um 99,6 % reduzieren, würden sie sich auf 2 % der wichtigsten Schwachstellen konzentrieren.

IDENTITÄTSDIEBSTAHL
Der Angreifer gibt sich als Mitarbeiter aus, um unbemerkt an Daten zu gelangen.

90 % DER BEKANNTEN SCHWACHSTELLEN WERDEN MONATLICH NICHT ADRESSIERT.

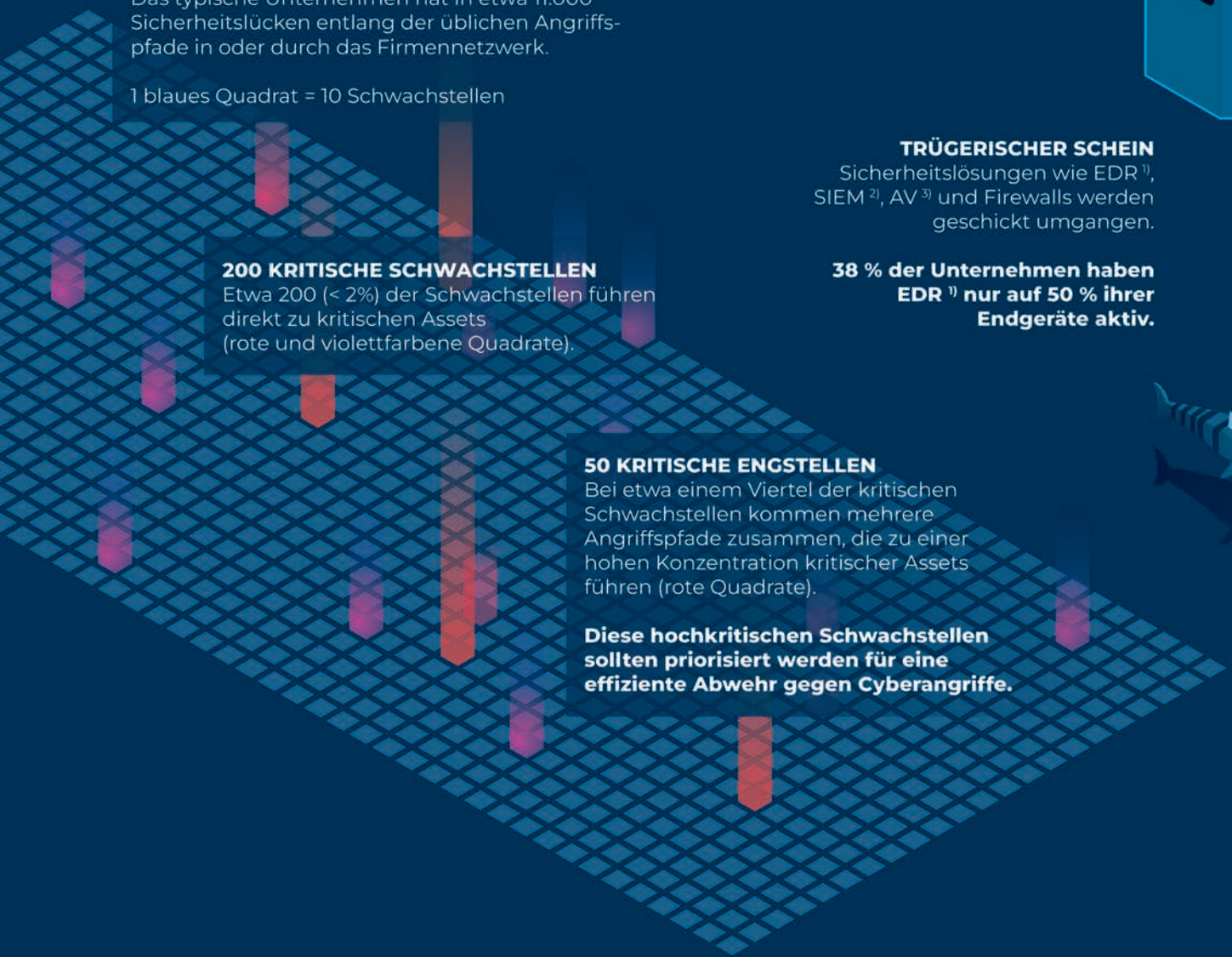
11.000 SICHERHEITSLÜCKEN
Das typische Unternehmen hat in etwa 11.000 Sicherheitslücken entlang der üblichen Angriffspfade in oder durch das Firmennetzwerk.

1 blaues Quadrat = 10 Schwachstellen

TRÜGERISCHER SCHEIN
Sicherheitslösungen wie EDR [1], SIEM [2], AV [3] und Firewalls werden geschickt umgangen.

38 % der Unternehmen haben EDR [1] nur auf 50 % ihrer Endgeräte aktiv.

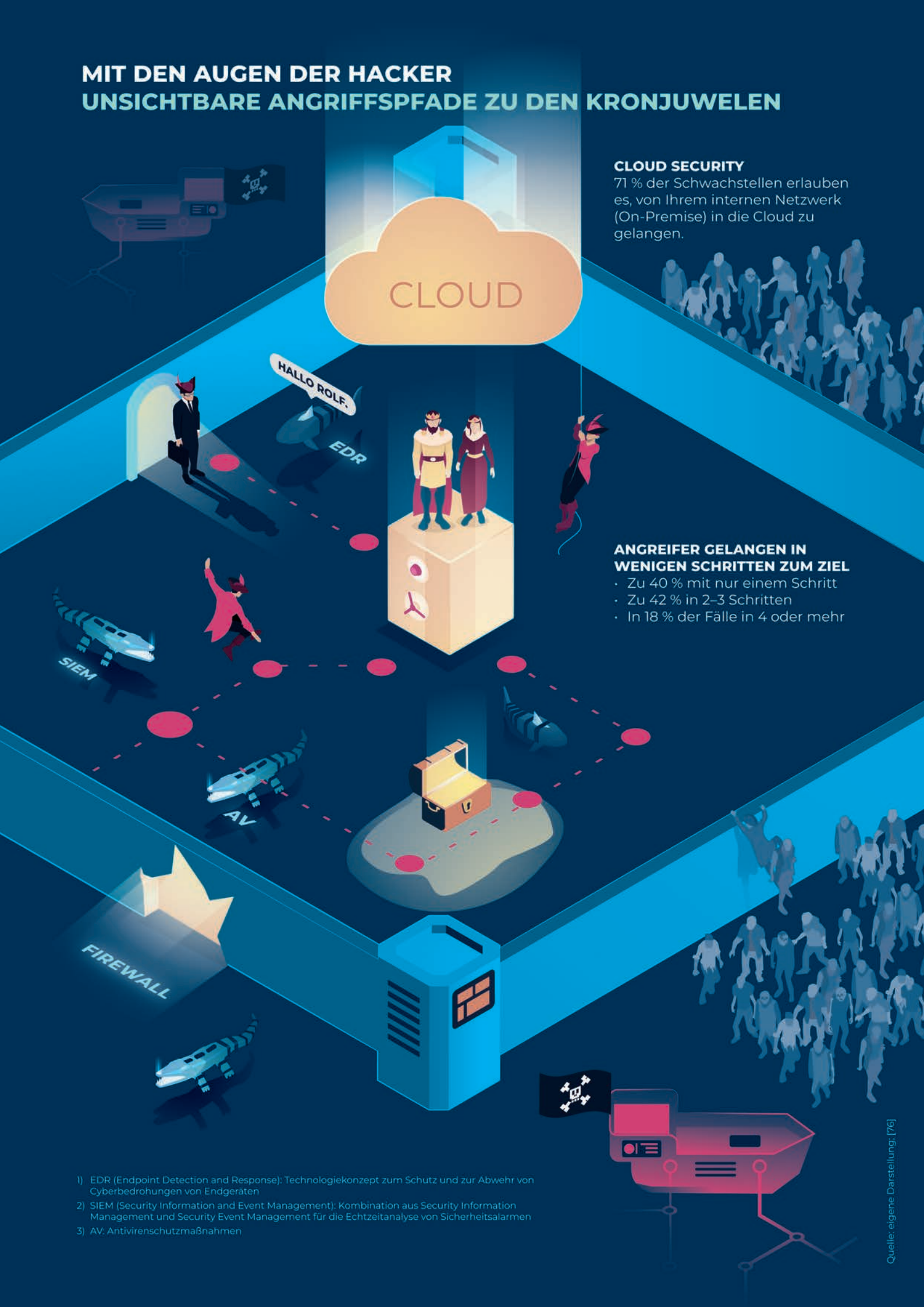
200 KRITISCHE SCHWACHSTELLEN
Etwa 200 (< 2%) der Schwachstellen führen direkt zu kritischen Assets (rote und violettfarbene Quadrate).



50 KRITISCHE ENGSTELLEN
Bei etwa einem Viertel der kritischen Schwachstellen kommen mehrere Angriffspfade zusammen, die zu einer hohen Konzentration kritischer Assets führen (rote Quadrate).

Diese hochkritischen Schwachstellen sollten priorisiert werden für eine effiziente Abwehr gegen Cyberangriffe.

MIT DEN AUGEN DER HACKER
UNSICHTBARE ANGRIFFSPFADE ZU DEN KRONJUWELEN



CLOUD SECURITY
71 % der Schwachstellen erlauben es, von Ihrem internen Netzwerk (On-Premise) in die Cloud zu gelangen.

ANGREIFER GELANGEN IN WENIGEN SCHRITTEN ZUM ZIEL
- Zu 40 % mit nur einem Schritt
- Zu 42 % in 2–3 Schritten
- In 18 % der Fälle in 4 oder mehr

1) EDR (Endpoint Detection and Response): Technologiekonzept zum Schutz und zur Abwehr von Cyberbedrohungen von Endgeräten
2) SIEM (Security Information and Event Management): Kombination aus Security Information Management und Security Event Management für die Echtzeitanalyse von Sicherheitsalarmen
3) AV: Antivirenschutzmaßnahmen

Quelle: eigene Darstellung; [76]

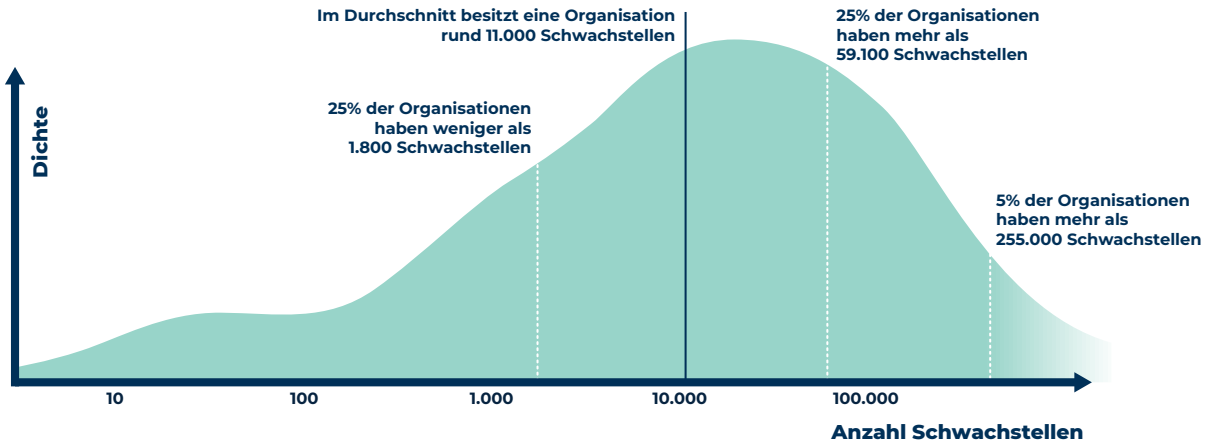
3 Mit den Augen der Hacker – unsichtbare Angriffspfade

Viele Organisationen haben sich jahrelang darum gekümmert ihre Burgmauern zu erhöhen und zu verstärken. Mit verschwimmenden Grenzen zwischen außen und innen ist das kein geeigneter Ansatz mehr. Es muss davon ausgegangen werden, dass die Angreifer bereits hinter den Burgmauern sind und man die Königin und den König, also die kritischsten Systeme und Daten, einer Organisation schützt.

Um dies besser zu verstehen, wurden Datensätze von XM Cyber exportiert, anonymisiert, überprüft und analysiert [76]. Dabei wurden zehntausende von Angriffspfaden aus dem Jahr 2022 in die Bewertung mit einbezogen und über 60 Millionen Schwachstellen aufgedeckt, die über 10 Millionen kritische IT-Systeme betreffen.

Die Härtung heutiger, sich ständig ändernder IT-Umgebungen gleicht einer Sisyphusarbeit. Sicherheitslücken tauchen auf, IT-Sicherheitsteams schalten so viele wie möglich so schnell wie möglich aus, und währenddessen tauchen immer wieder neue Probleme auf. Allerdings schaffen Organisationen nur, etwa zehn Prozent aller Schwachstellen in einem Monat zu adressieren. Manche Schwachstellen werden erst ein Jahr nach Veröffentlichung oder später adressiert.

Im Durchschnitt haben alle hier untersuchten Organisationen 11.000 Schwachstellen, die Angreifer nutzen könnten, um kritische Systeme zu kompromittieren – und einige (fünf Prozent) Organisationen kämpfen mit mehr als dem 20-Fachen an Schwachstellen. Dazu gehören nicht behobene Schwachstellen über das Patch Management, Fehlkonfigurationen von IT-Systemen, falsch verwaltete Anmeldeinformationen, unzureichend geschützte Ressourcen und eine Vielzahl anderer Sicherheitsprobleme.



Quelle: [76]

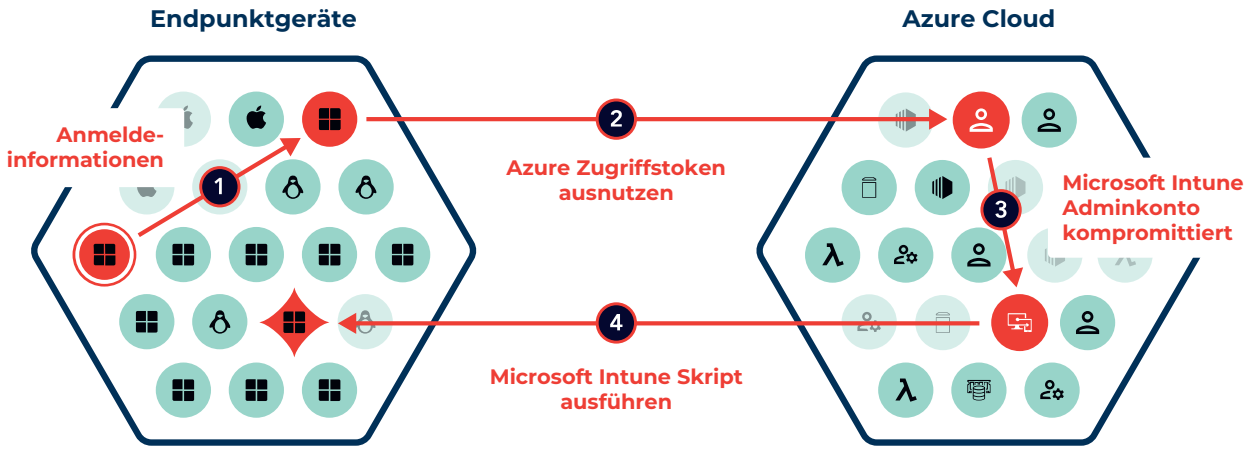
Verteilung von Schwachstellen über alle untersuchten Organisationen

Viele Schwachstellen (ca. 75 Prozent) führen jedoch nicht zu den kritischen Systemen einer Organisation. In der Cloud gilt diese Erkenntnis für 96 Prozent und in lokalen IT-Umgebungen für 61 Prozent der Systeme. Auch wenn Angreifer im Schnitt etwa 39 verschiedene Angriffsmethoden ausnutzen können, führen drei von vier Angriffspfaden in eine Sackgasse. Im Schwachstellenmanagement von Organisationen wird heute jedoch meist alles als „kritisch“ eingestuft. Entsprechend besteht die tägliche Herausforderung darin, Risiken bewusst zu ignorieren, zu vertagen oder zu priorisieren. Er gleicht also nicht der Suche der Nadel im Heuhaufen, sondern eher der Suche nach der Nadel im Nadelhaufen. Die Frage ist also, ob der heutige Ansatz zeitgemäß und effizient ist.

Die Infografik zeigt die Anzahl an Schwachstellen eines typischen IT-Systems in der Höhe von 11.000. Ein Quadrant entspricht zehn Schwachstellen. Der Großteil der der Schwachstellen (Grau) repräsentiert eine Sackgasse oder führt zu einer Sackgasse. Nur etwa zwei Prozent der Schwachstellen (ca. 200) stellen die zentralen Vektoren (Rot, Lila) dar, über die Angreifer zu den sensitiven Zielsystemen gelangen. Einer von vier Vektoren (Rot) setzt dabei zehn Prozent oder mehr kritische Systeme den Angreifern aus. Liegt der Fokus nur auf diesen Systemen, können IT und IT-Sicherheitsteams ihre Arbeit um 99,6 Prozent reduzieren.

Sind Angreifer einmal hinter die Burgmauern gelangt, suchen sie den Weg des geringsten Widerstands, um an kritische Systeme zu gelangen. Davon können sie im Schnitt mindestens 90 Prozent erreichen hinzu kommen auch 71 Prozent der Cloud-Systeme – sie benötigen dafür nur wenige Schritte und Angriffstechniken. In 82 Prozent der Fälle sind es weniger als drei Schritte (Systeme zum Beispiel PC oder Server). 92 Prozent der Systeme, die bei den großen Hyperscalern AWS, Google oder Azure lagern, können in nur einem Schritt aus dem Netzwerk einer Organisation (On-Premise / On-Prem) kompromittiert werden. Zwischen den Anbietern gibt es keinen Unterschied. Hinzu kommt, dass 48 Prozent der untersuchten Organisationen Cloudangebote nutzen, die vom Internet (externe Angriffsfläche) erreichbar sind.

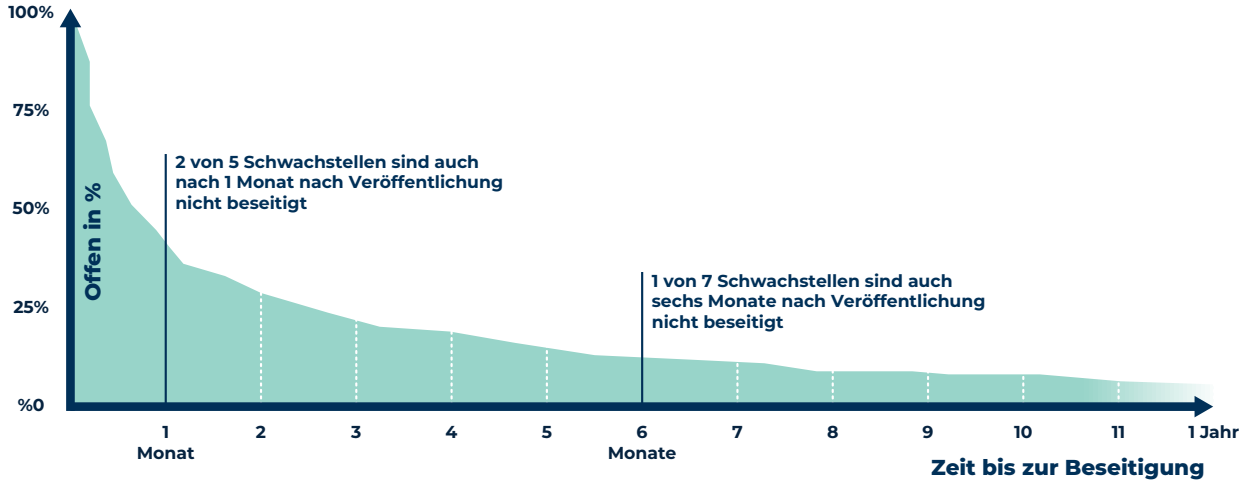
Das nachfolgende Beispiel verdeutlicht das Vorgehen eines Angreifers, welcher zahlreiche Techniken kombiniert, um an das gesamte Netzwerk und kritische Daten zu gelangen. Hierbei hat der Angreifer die Kontrolle über einen beliebigen Computer eines Mitarbeiters übernommen. Der Angreifer wird meistens versuchen sich in mehreren Rechnern einzunisten, um alternative Einfallstore zu haben. Vielfach wird dies dadurch vereinfacht, dass ein Nutzer auf mehreren Rechnern vorhanden ist. Nachdem Anmeldeinformationen und -berechtigungen ausgenutzt wurden, bewegt sich der Angreifer in die Cloud weiter (hier Microsoft Azure) und sammelt Azure Zugriffstokens (via Multifaktorauthentifizierung (MFA)). Nach weiterer Erforschung der IT Umgebung, wurden die Berechtigungen erhöht um ein Microsoft Intune Administratorkonto zu kompromittieren. Intune ist eine Mobile Device Management Lösung. Mit diesem Schritt hat der Angreifer eine mächtige und vertrauenswürdige Identität erlangt, um sich flexibel Code auf Rechnern im ganzen Netzwerk einer Organisation aufzuspielen. Dabei startete der Angreifer mit einer geringen Berechtigung und bewegte sich zwischen On-Premise und Cloud lateral hin und her.



Quelle: [76]

Angriffspfadbeispiel

Selten müssen Angreifer komplexe Angriffstechniken verwenden oder neuste Schwachstellen ausnutzen. Stattdessen können sie die gleiche Methode auf verschiedenen Pfaden und Computern oder Servern innerhalb eines Netzwerks verwenden. Es ist wichtig zu verstehen, dass bekannte Schwachstellen wie zum Beispiel Log4j oder PrintNightmare nur einen Angriffsvektor darstellen. Angreifer müssen auch nicht auf die neusten Schwachstellen zurückgreifen. Die Untersuchung hat gezeigt, dass sechs Jahre alte Schwachstellen (zum Beispiel UltraVNC, aCropalypse) heute noch für Angriffspfade in Organisationen verantwortlich sind, weil es sehr lange dauert diese zu beseitigen.



Quelle: [76]

Wie lange Schwachstellen in IT Umgebungen unadressiert bleiben

Im Vergleich zu allen Angriffstechniken und Schwachstellen, ist das Active Directory für 82 Prozent der Schwachstellen bei den untersuchten Organisationen verantwortlich. Das Active Directory ist ein Verzeichnisdienst, der Windows-Netzwerke verwaltet. Die zugehörige Datenbank beinhaltet Informationen zu jeglichen Objekten, die sich im Netzwerk befinden: Benutzer, Computer, Drucker, freigegebene Ordner.

Derzeit ersetzen viele Organisationen ihre Antivirussoftware durch weiterentwickelte Lösungen zur Angriffserkennung, welche als Endpoint Detection and Response (EDR) bezeichnet werden. Der Einsatz dieser Lösungen kann jedoch zu einem falschen Gefühl der Cybersicherheit führen. EDR-Systeme können umgangen oder für Angriffe manipuliert werden (zum Beispiel Datenlöschung). Auch laufen diese Lösungen nicht immer stabil auf manchen IT-Systemen, so dass sie nicht überall im Einsatz sind. In der vorliegenden Analyse, sind bei 38 Prozent der Organisationen die EDR-Systeme auf weniger als 50 Prozent der IT-Infrastruktur im Einsatz, das betrifft insbesondere Linux- und Mac-Systeme. Auch wenn EDR generell verbreitet ist, konnten trotzdem Angriffspfade in Systemen mit hohem EDR-Einsatz identifiziert werden. Nur eine von zehn Organisationen haben ihre EDR-Systeme im vollen Umfang auf mindestens 90 Prozent der IT Umgebung im Einsatz.

Gerade weil Daten von Mitarbeitern gestohlen werden können, ist das Zugriffs- und Rechtemanagement für die IT besonders wichtig. 80 Prozent der untersuchten Organisationen sind hier verschiedenen Angriffsmethoden ausgesetzt. 22 Prozent der Organisationen geben mindestens 50 Prozent ihrer Nutzerpopulation erhöhte Zugriffs- und Verwaltungsrechte. In 76 Prozent der Organisationen finden sich Nutzer mit sehr hohen Administrationsrechten auf zahlreichen Rechnern hinterlegt. Etwa zehn Prozent können mehr als 100 Computer oder Server verwalten. Die Untersuchung lässt den Schluss zu, dass 26 Prozent der Organisationen diese Nutzer unbemerkt über ein „Golden Image“ (d.h. ein Standard IT Setup für ein Notebook oder eine virtuelle Maschine auf einem Server) verbreiten.

	Organizations	Exposures	Critical Assets	Choke Points
PrintNightmare (CVE-2021-34527)	54,2%	0,5%	2,8%	3,3%
Text4Shell	42,7%	0,0%	2,6%	0,1%
UltraVNC (CVE-2019-8277)	18,8%	0,1%	0,2%	0,6%
Log4j	33,3%	0,0%	2,6%	0,1%
DejaBlue	28,1%	0,0%	0,5%	0,0%
EternalBlue (CVE-2017-0144)	18,8%	0,0%	0,2%	0,0%
Follina - Microsoft office (CVE-2022-30190)	25,0%	0,0%	0,0%	0,1%
SMBGhost (CVE-2020-0796)	16,7%	0,0%	0,5%	0,0%
aPAColypse (CVE-2017-11907)	18,8%	0,0%	0,0%	0,0%
Spring4Shell - CVE-2022-22965	20,8%	0,0%	0,7%	0,0%
BlueKeep (CVE-2019-0708)	17,7%	0,0%	0,1%	0,0%
LNK Exploits	21,9%	0,0%	0,0%	0,0%
ProxyNotShell RCE (CVE-2022-41040, CVE-2022-41082)	13,5%	0,0%	0,4%	0,0%
NoPac (CVE-2021-42278, CVE-2021-42287)	8,3%	0,0%	0,3%	0,0%

Top Schwachstellen - Angriffspfadanalyse

Quelle: [76]

	Organizations	Exposures	Critical Assets	Choke Points
Network Reachability	81,2%	7,9%	7,4%	17,8%
Reset User Password	76,0%	18,8%	3,2%	3,5%
Credential Dump	80,2%	2,7%	7,3%	4,3%
Domain Credentials	75,0%	2,7%	7,0%	15,7%
Resource-Based Constrained Delegation	76,0%	8,5%	3,6%	7,9%
Add Logon Script	76,0%	18,7%	2,8%	3,8%
Add Members to Group	77,1%	14,8%	2,1%	0,5%
Local Credentials	75,0%	0,6%	2,8%	4,7%
Member Of Group	72,9%	6,7%	2,9%	0,4%
Taint Shared Content	76,0%	5,6%	2,5%	1,8%
Credentials Relay	58,3%	0,4%	3,1%	4,2%
Proxy Spoofing	81,2%	0,3%	0,1%	2,1%
RDP Credential Usage	60,4%	0,9%	1,6%	7,5%
Microsoft SQL Credentials Usage	70,8%	0,1%	4,4%	0,7%
PrintNightmare (CVE-2021-34527)	55,2%	0,5%	2,8%	3,3%
Add ACE to OU	66,7%	0,9%	2,9%	0,0%

Top Angriffsmethoden - On-Prem Umgebung

Quelle: [76]

	Organizations	Exposures	Critical Assets	Choke Points
AWS IAM Add Policy Privilege Escalation	19,8%	0,2%	2,5%	3,1%
AWS Update Role Impersonation Policy	19,8%	0,1%	2,5%	2,5%
AWS EC2 (AttachVolume, DetachVolume) Take Over	19,8%	0,1%	2,1%	1,1%
AWS Modify EC2 Instance User Data	18,8%	0,1%	2,1%	1,1%
AWS Create User Access Key	18,8%	0,0%	2,0%	0,6%
AWS Update Lambda Code	18,8%	0,0%	1,4%	0,6%
AWS Update Login Profile	17,7%	0,0%	1,9%	0,6%
AWS Over-privileged AWS EC2 Instance Creation	19,8%	0,0%	2,0%	0,3%
AWS S3 Bucket Read Data	19,8%	0,1%	0,6%	0,0%
AWS S3 Bucket Write Data	18,8%	0,1%	0,6%	0,0%
AWS Over-privileged AWS Lambda Function Creation	17,7%	0,0%	1,7%	0,4%
AWS EC2 Role Compromise	20,8%	0,0%	1,4%	0,2%
AWS EBS Share Volume Snapshot	17,7%	0,1%	0,1%	0,0%
AWS Lambda Change Function Role	17,7%	0,0%	1,2%	0,4%
AWS EC2 Change Machine Role	17,7%	0,0%	1,5%	0,3%
AWS Add User To Group	16,7%	0,0%	1,5%	0,4%
AWS EC2 SSM SendCommand takeover	12,5%	0,0%	1,5%	0,4%

Top Angriffsmethoden - AWS Umgebung

Quelle: [76]

	Organizations	Exposures	Critical Assets	Choke Points
Azure Member Of Group	30,2%	1,0%	23,0%	0,2%
Azure Run Command On VM	28,1%	0,3%	20,6%	0,1%
Azure Run Command On VM Using VM Extensions	28,1%	0,3%	16,6%	0,1%
Azure Application Owner Can Compromise the Application Service Principals	31,2%	0,2%	2,6%	0,2%
Azure Add Role Assignment	30,2%	0,0%	38,4%	0,3%
Azure Tables Compromise	24,0%	1,2%	9,9%	0,0%
Azure Graph Role Compromise	29,2%	0,0%	35,4%	0,0%
Azure Read Blobs	17,7%	0,9%	9,1%	0,0%
Azure Group Member of Group	22,9%	0,1%	1,5%	0,0%
Azure Queues Compromise	16,7%	0,3%	3,0%	0,0%
Azure Reset Application Credentials	1,0%	0,1%	0,0%	0,2%
Azure Resource Attached Identity Compromise	22,9%	0,0%	18,9%	0,0%
Azure Applications Can Add Passwords to Other Applications	14,6%	0,1%	0,3%	0,1%
Microsoft Intune - Execute Script	9,4%	0,0%	0,8%	0,1%
Azure Upload Blobs	16,7%	0,3%	1,8%	0,0%
Read OneDrive Files using Azure Applications	26,0%	0,0%	0,0%	0,0%
Azure Application Can Read E-Mails	24,0%	0,0%	0,0%	0,0%
Azure Automation Account Compromise	19,8%	0,0%	3,8%	0,0%
Azure Key Vaults Compromise	24,0%	0,1%	0,4%	0,0%
Azure List Functions publish XML keys in Azure Site	21,9%	0,1%	1,0%	0,0%
Azure Automation Account Application Compromise	8,3%	0,0%	3,8%	0,0%

Top Angriffsmethoden - Azure Umgebung

Quelle: [76]

	Exposures	Critical Assets	Choke Points
GCP Create Service Account Key	0.0%	1.2%	0.3%
GCP Service Account From Resource	0.0%	1.2%	0.1%
GCP Compromise Linux VM	0.1%	0.8%	0.2%
GCP Allows Signing of Arbitrary Payloads	0.0%	1.1%	0.0%
GCP Create VM with Specified Service Account	0.0%	1.0%	0.2%
GCP Create Function with Specified Service Account	0.0%	0.9%	0.2%
GCP Set a Project IAM Policy	0.0%	1.7%	0.1%
GCP Read BigQuery	0.1%	0.9%	0.0%
GCP Set Storage IAM Policy	0.0%	0.4%	0.3%
GCP Read Data From Bucket	0.1%	0.5%	0.0%
GCP Member Of Group	0.0%	1.2%	0.0%
GCP Request Service Account Token	0.0%	1.1%	0.0%
GCP Access Token Stealer	0.0%	0.1%	0.0%
GCP Set a Folder IAM Policy	0.0%	1.5%	0.0%
GCP Write Data To Bucket	0.1%	0.4%	0.0%
GCP Compromise Function	0.0%	0.1%	0.0%
GCP Write BigQuery	0.1%	0.9%	0.0%
GCP Set an Organization IAM Policy	0.0%	1.2%	0.0%
GCP Set Service Account IAM Policy	0.0%	0.9%	0.2%
GCP Request Service Account Token By Implicit Delegation	0.0%	1.1%	0.0%
GCP Signing Well-Formed JWT	0.0%	1.1%	0.0%

Top Angriffsmethoden - GCP Umgebung

Quelle: [76]

4 Risikofaktor Mensch – das Internet vergisst nie

RISIKOFAKTOR MENSCH

DAS INDIVIDUELLE DIGITALE RISIKOPROFIL EINES EINZIGEN DAX-CEO

Analysiert wurden die durch Datenlecks öffentlich gewordenen persönlichen Daten von nur einem CEO eines deutschen DAX-Unternehmens.

DAS INTERNET VERGISST NICHTS

ANALYSE VON DATENLECKS IN 10 GROSSEN DEUTSCHEN UNTERNEHMEN

10 UNTERNEHMEN = **20** DOMAINS

11.807 GESAMTANZAHL DER DATENLECKS

1.239.112 BETROFFENE IDENTITÄTEN

472.689 EINDEUTIGE MERKMALE

305.678 PASSWÖRTER

933.434 PERSONENBEZOGENE DATENSÄTZE

STICHPROBE: 20 CEOS GROSSER DEUTSCHER UNTERNEHMEN

Bezogen auf öffentlich zugängliche persönliche Daten

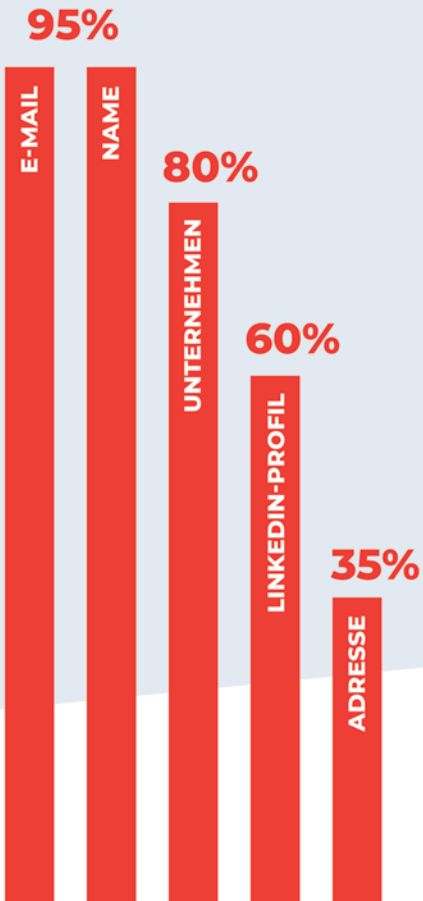
16 DURCHSCHNITTLICHE ANZAHL AN SCHWACH-STELLEN PRO CEO

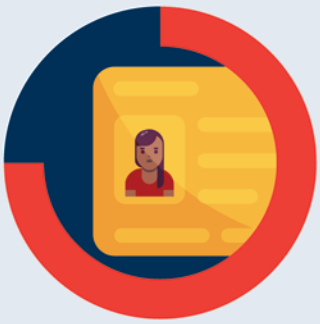
70 GEMESSENER HÖCHST-WERT EINER PERSON

20/20 JEDER EINZELNE CEO WAR VON DATENLECKS BETROFFEN

Quelle: eigene Darstellung; [24]

WELCHE INFOS SIND AM HÄUFIGSTEN BETROFFEN?





75%

VORFÄLLE BEZOGEN AUF PERSÖNLICHE DATEN

25 % NUR E-MAIL UND PASSWORT

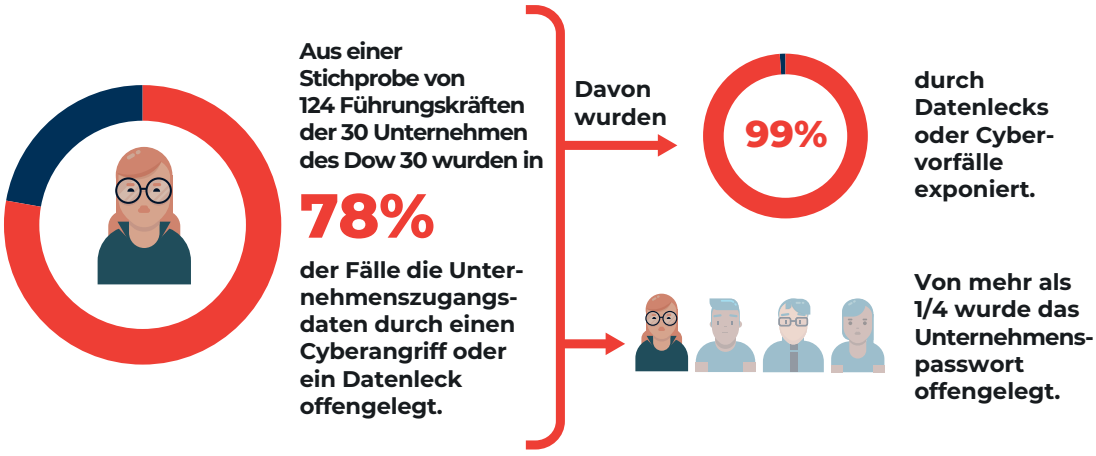
19/20

19 VON 20 DER ANALYSIERTEN „.DE“- ODER „.COM“-DOMAINS GABEN PASSWÖRTER VON MITARBEITERN ODER FÜH-RUNGSKRÄFTEN IM KLARTEXT PREIS.

4 Risikofaktor Mensch – das Internet vergisst nie

Der Mensch bleibt weiterhin die entscheidende Schwachstelle in über 80 Prozent der Fälle von Cyberangriffen – egal ob bei gestohlenen Zugangsdaten, Phishing, Ransomware, Innentätern oder sonstigem menschlichem Versagen. Die böswillige Nutzung personenbezogener Daten aus offenen Quellen oder Datenlecks stellt ein erhebliches Risikopotenzial für Organisationen dar. Führungskräfte stehen besonders häufig im Visier.

In einer Analyse von Unternehmen, die im amerikanischen Dow-30-Aktienindex gelistet sind, wurden seit 2018 über 13.000 Cybervorfälle oder Datenabflüsse registriert. Diese beinhalten über 11,3 Millionen Datensätze mit unternehmensinternen Zugangsdaten von Mitarbeitern und Führungskräften. Bei einer Stichprobe von 124 Führungskräften dieser Unternehmen konnten in 78 Prozent der Fälle Zugangsdaten (Passwörter, Benutzername) gefunden werden.



Quelle: eigene Darstellung; [24]

Analyse der digitalen Exponiertheit von Führungskräften von Unternehmen im Dow-30-Aktienindex

4.1 Wie exponiert sind deutsche Führungskräfte?

Um das Ausmaß und die Gefährdungslage von offen verfügbaren Identitätsdaten im Surface, Deep und Dark Web zu verstehen, wurden Ende Februar 2023 in einer Stichprobe die Führungskräfte (CEO und weiterer Vorstand) und Unternehmensdomains (.com und .de) von zehn großen deutschen Unternehmen untersucht. Diese kamen aus den Branchen Handel, Pharma, Transport, Finanzdienstleistungen und Banken, Konsumgüter, Technologie, Automobil und Telekommunikation.

Hierbei wurde auf die weltweit größte kommerzielle Sammlung von Datensätzen aus Cyberangriffen und Datenabflüssen der letzten 18 Jahre bis heute der Firma Constella Intelligence zurückgegriffen. Sie umfasst mehr als 124 Milliarden Datensätze und mehr als 180 Milliarden kuratierte Identitätsattribute aus 125 Ländern in 53 Sprachen. Darunter fallen auch Daten aus Foren und Chats, in denen derartige personenbezogene Daten für Cyberangriffe wie Phishing, Account Takeover (ATO), hybride Desinformationskampagnen oder Ransomware gehandelt werden.

Alle untersuchten Vorstände waren von mindestens einem Datenleck betroffen. Im Schnitt waren es 16, im Höchstfall 70. Zu den auffindbaren Daten gehörten Telefonnummern, private oder IP-Adressen. In zwei Fällen konnten Daten von sensiblen Seiten (zum Beispiel Glückspiel, Dating, Erwachseneninhalte) gefunden werden. Zu den Daten auf sensiblen Seiten gehörten Klartextpasswörter, Social-Media-Profile, private Telefonnummern oder Privatadressen.

Bei 13 von 20 Führungskräften waren mindestens einmal Passwörter im Klartext auffindbar. Insgesamt konnten 115 Passwörter über alle Vorstände identifiziert werden. 70 Prozent davon lagen unverschlüsselt vor.

4.2 Wie exponiert sind die Mitarbeiter von zehn deutschen Unternehmen?

Insgesamt wurden 1.239.112 Identitäten aus 11.807 Datenlecks identifiziert. Darunter 305.678 Passwörter und 933.434 Datensätze mit persönlich identifizierbaren Informationen, welche Unternehmensidentitäten von „.com“- und „.de“-Domains zuzuordnen sind. Es ist davon auszugehen, dass die überwiegende Mehrheit dieser exponierten Datensätze unentdeckt geblieben ist und die betroffenen Personen oder Unternehmen sich dieser Sache nicht bewusst sind.

In 104 Fällen wurden Unternehmensdaten (zum Beispiel E-Mail) für Dating-, Erwachsenen-, Glücksspiel- oder andere heikle und kritische Websites verwendet. 1.690 Datensätze betrafen neun der zehn analysierten Unternehmen.

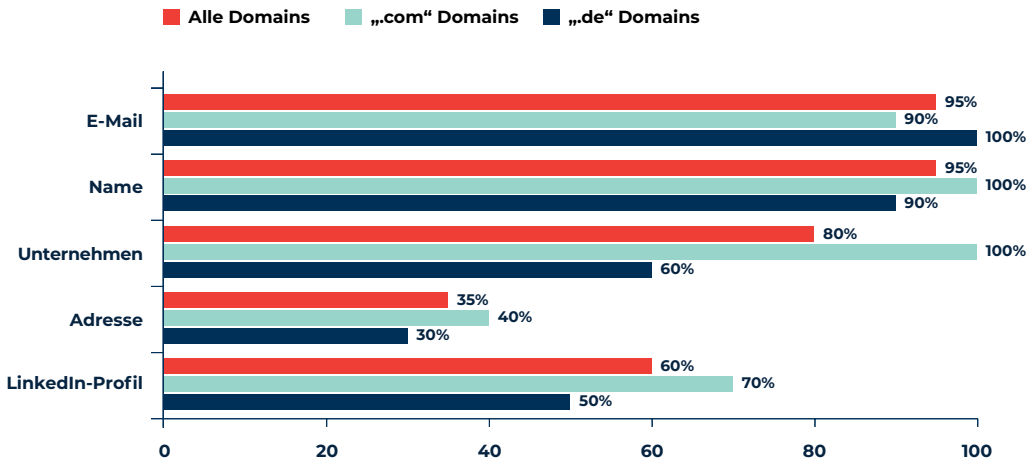
Daneben konnten 36.272 Nutzer (keine Mitarbeiter) bei 17 von 20 Domains und 346 Gefährdungen Dritter durch Infostealer identifiziert werden. Unter diesen Nutzern könnten sich Mitarbeiter mit privilegierten Zugangsrechten im IT-Umfeld befinden. Sie müssen keine Führungskräfte sein, um als ein interessantes Ziel für Cyberkriminelle zu gelten. Es war noch nie so einfach, die eigenen Zugangsrechte als Insider zu monetarisieren. Als Beispiel sei auf die Ransomware-Gruppe LAPSUS$ verwiesen, die auf ihrem Telegram-Kanal nachfolgende Werbung für die Anwerbung von Insidern mit zentralen Rollen in Technologieunternehmen veröffentlicht hat. Angebote reichen von einigen 1.000 Euro bis 20.000 Euro pro Woche bis hin zu mehr als 1 Million Euro in Kryptowährung. Laut einer Umfrage in den USA berichteten 65 Prozent der IT-Verantwortlichen, mit derartigen Angeboten konfrontiert worden zu sein.

4.3 Sensible Mitarbeiterdaten, die am häufigsten gefunden wurden

Einmal erfasst, werden personenbezogene Daten häufig auf Marktplätzen im Deep oder Dark Web verkauft oder für alle Nutzer platziert. Der einfache Zugang zu diesen personenbezogenen Daten bietet Cyberkriminellen die nötigen Ressourcen für ein breites Spektrum von Angriffen. Mit vertrauenswürdigen Mitarbeiteridentitäten können moderne interne Cybersicherheitssysteme umgangen werden.

Für den Großteil der zehn deutschen Unternehmen konnten mehrere Attribute für einen personenbezogenen Datensatz identifiziert werden. Generell sind dies E-Mails, Namen und Adressen, aber auch Passwörter.

Für 19 von 20 Internetdomains der zehn deutschen Unternehmen wurden Passwörter für ihre Mitarbeiter im Klartext offengelegt. Darüber hinaus waren andere Passwörter nur mit „schwachen" Algorithmen wie SHA1 oder MD5 geschützt. Ein mit MD5 geschütztes Passwort mit einer Länge von acht Zeichen (Zahlen, Groß- und Kleinbuchstaben, Symbole) kann mit heutigen Technologien in etwa acht Stunden herausgefunden werden. Daher sollten Passwörter im besten Fall länger als 15 Zeichen sein.



Quelle: eigene Darstellung; [24]

Rangliste der häufigsten offengelegten Attribute je Firmendomain

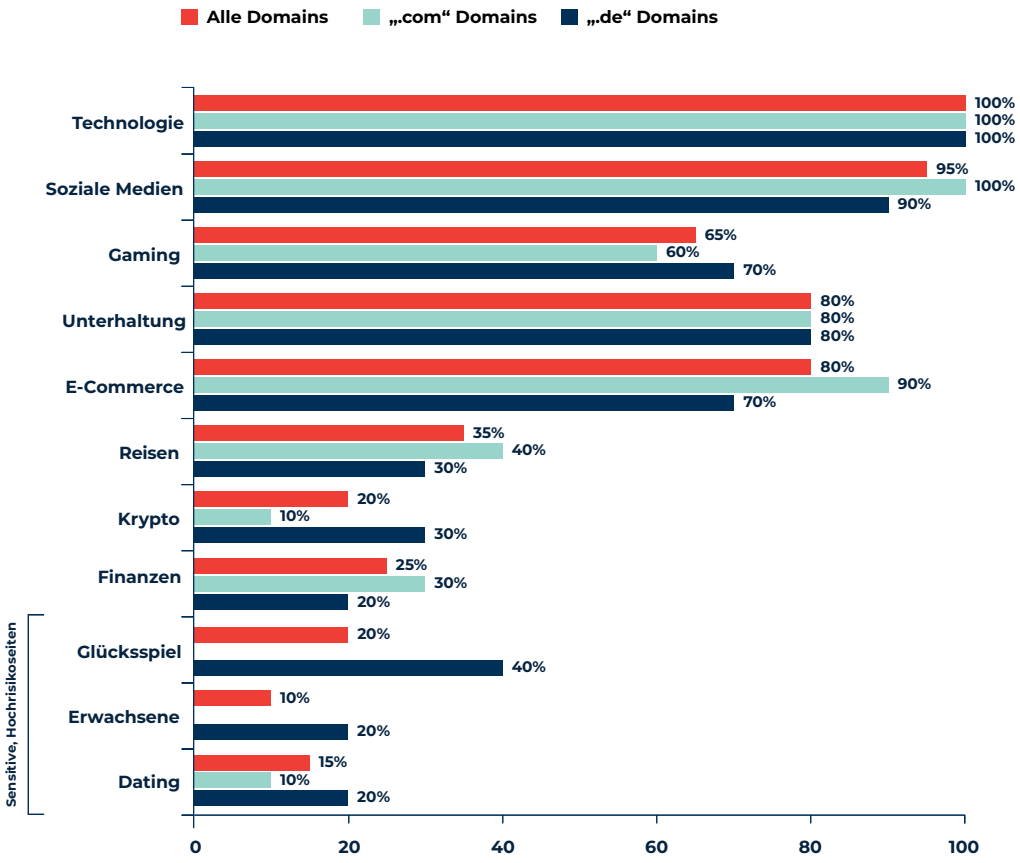
4.4 Wo die Daten der Mitarbeiter am häufigsten exponiert wurden

Jegliche Verwendung von Mitarbeiter- und Firmendaten auf anderen Websites stellt ein Risiko dar. Sie deutet zudem auf fehlende Wahrnehmung der Personen für die Gefahren für sich, ihre Familien und ihr Unternehmen hin.

Für die untersuchten Unternehmen und ihre Mitarbeiter stammten personenbezogene Daten meist aus Cyberangriffen oder Datenlecks aus den Bereichen Technologie (100 Prozent), Social Media (95 Prozent), Unterhaltung (80 Prozent), E-Commerce (80 Prozent) und Gaming (65 Prozent) und Reisen (35 Prozent) sowie Kryptowährung, Erwachseneninhalte, Dating und Glückspiel mit jeweils 20 Prozent.

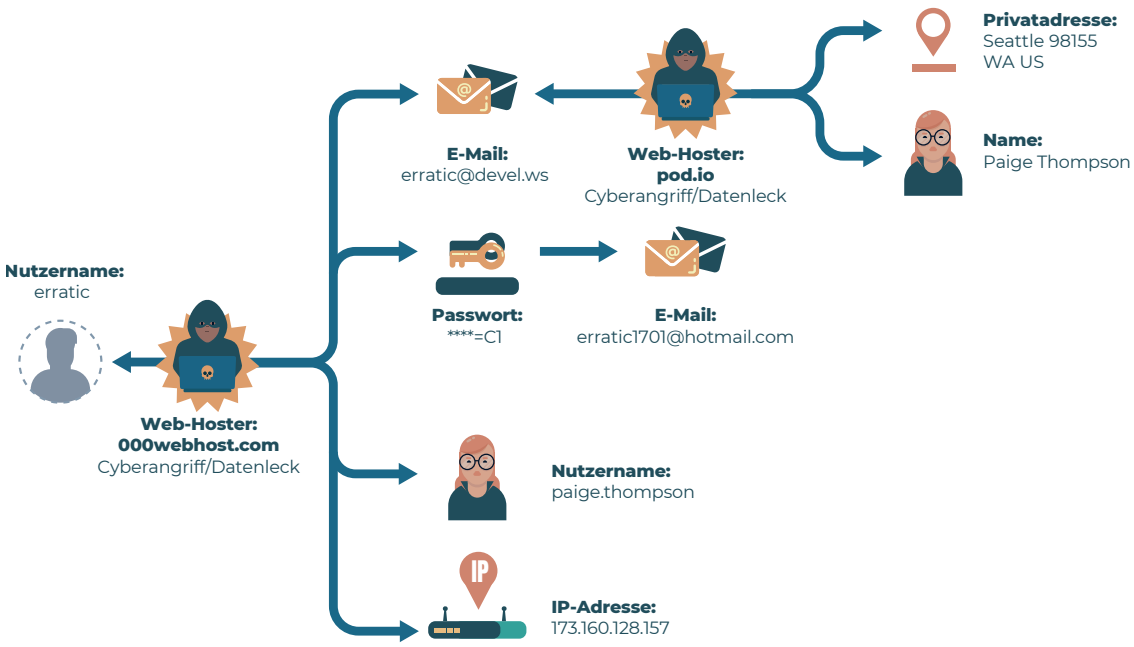
4.5 Risiko Infostealer-Schadprogramme

In Foren im Deep und Dark Web wird zunehmend über Information-Stealer-(Infostealer-)Schadsoftware gesprochen und das Interesse dürfte weiter zunehmen. Die Software ist darauf ausgelegt, über einen möglichst langen Zeitraum unbemerkt personenbezogene Daten zu erkennen, zu sammeln und an eine fremde Quelle zu senden. Dazu zählen Cookie-Daten, Benutzernamen oder Passwörter. Die geringen Kosten und die Verfügbarkeit als Malware-as-a-Service-Angebot bietet Cyberkriminellen eine attraktive niedrigschwellige Möglichkeit für den Einsatz in Operationen.



Quelle: eigene Darstellung; [24]

Von welchen Cyberangriffen und Datenpannen die Mitarbeiter- und Führungskräftedaten stammen



Quelle: eigene Darstellung; [24]

Feststellung einer Identität aus Datenabflüssen verschiedener Angriffe

Insgesamt konnten 36.272 kompromittierte Nutzer (keine Mitarbeiter, aber zum Beispiel ein Kunde mit seiner privaten E-Mail-Adresse) für 17 von 20 Internetdomains (85 Prozent) der deutschen Unternehmen identifiziert werden. Die Anmeldedaten von 284 Mitarbeitern waren ebenfalls von Infostealern betroffen. Darüber hinaus gibt es 346 Fälle bei Mitarbeitern mit ihren Anmeldedaten, die Aktivitäten Dritter Cyberrisiken aussetzen (zum Beispiel einen E-Commerce-Anbieter).

4.6 Warum das Internet nicht vergisst

Auch wenn die Datenschutz-Grundverordnung ein „Recht auf Auskunft" und ein „Recht auf Vergessenwerden" beinhaltet, muss man verstehen, dass große Teile des Internets gar nichts vergessen. Gerade wer seit Jahren privat und geschäftlich mit verschiedensten Organisationen rund um den Globus interagiert, hinterlässt einen stetig wachsenden digitalen Fußabdruck. Dabei ist es unmöglich, alle Cyberangriffe und Datenlecks mit persönlichem Bezug mitzubekommen. Dies kann auch Cyberkriminellen zum Verhängnis werden.

Paige Thompson hackte 2019 die amerikanische Bank Capital One, wodurch ein Schaden von 250 Millionen US-Dollar entstand und über 100 Millionen Menschen betroffen waren. Paige Thompson nutze das Alias „Erratic" und stellte den erfolgreichen Hack in einem Darknetforum vor. Weitere Informationen zu ihrer Identität waren nicht bekannt. Was Paige Thompson allerdings nicht wusste: Sie hatte Ihr Alias für Anmeldedaten für einen Webhosting-Anbieter (000webhost.com) verwendet. Die gesamten Daten des Anbieters wurden nach einem erfolgreichen Cyberangriff von einer anderen Hackergruppe bereits 2015 im Darknet veröffentlicht. Folgende personenbezogenen Daten waren dort einsehbar:

000webhost.com
Nutzername: paige.thompson
E-Mail: erratic@devel.ws
IP-Adresse: 173.160.128.157
Passwort: ****=C1

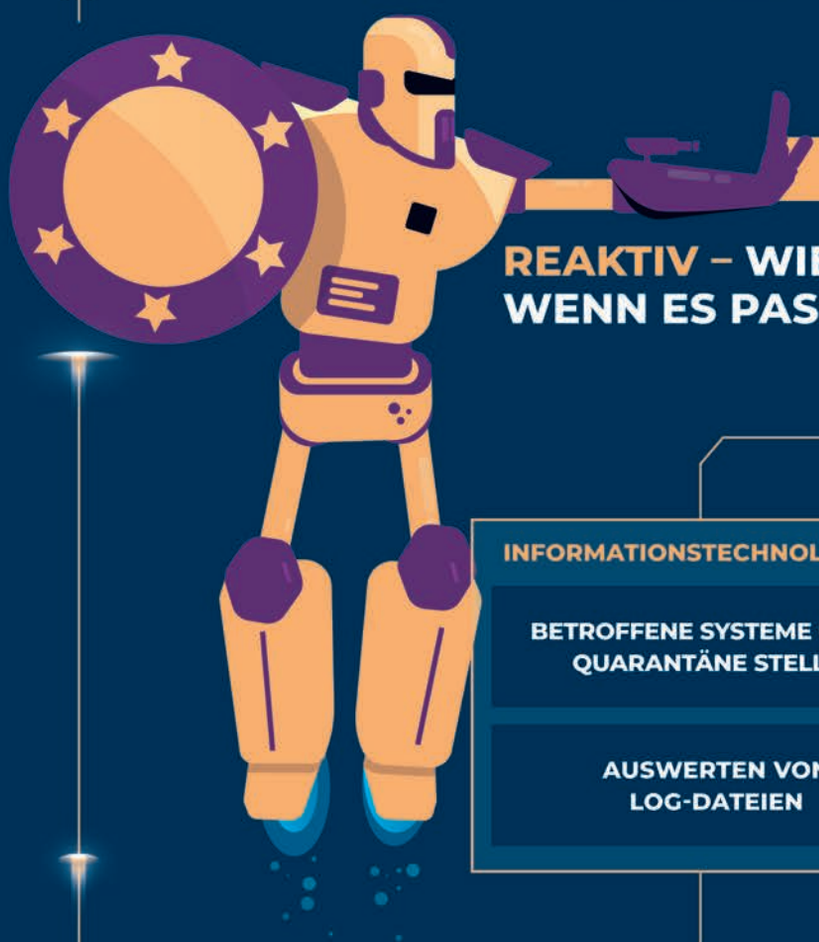
Die E-Mail-Adresse und das gleiche Passwort waren auch in anderen Datenabflüssen nach erfolgreichen Hacks auffindbar. Durch die Verknüpfung aller Daten und weiterer Recherchearbeiten der Strafverfolgungsbehörden konnte Paige Thompson eindeutig identifiziert und 2022 verurteilt werden.

5 Der Weg vor die Cyberkriminalitätswelle

CYBERANGRIFF-CHECKLISTE
EMPFEHLUNGEN ZUM UMGANG MIT CYBERANGRIFFEN

PRÄVENTIV – WAS IST VOR DEM ANGRIFF ZU TUN?

- ☐ **RISIKOBASIERTE UND PROAKTIVE CYBERSTRATEGIE**
  Schwachstellen und Risiken verstehen, bevor Maßnahmen und Prioritäten festgelegt werden.
- ☐ **REGELMÄSSIGES SECURITY-AWARENESS-TRAINING DER MITARBEITER**
  Förderung des Bewusstseins zum Erkennen von Angriffen.
- ☐ **NETZWERKSEGMENTIERUNG**
  Isolierung der Alt-/Legacy-Systeme ohne mögliche Sicherheitsupdates von anderen Systemen innerhalb des Netzwerks.
- ☐ **ZENTRALES MONITORING VON NETZWERKEN**
  Regelmäßige Überprüfung von Log-Daten, die Aktivitäten innerhalb des Netzwerks festhalten.
- ☐ **KRITISCHE SYSTEME KENNEN**
  Ein IT-Asset-Management schafft den Überblick über alle IT-Systeme und hilft dabei, Updates zu priorisieren.
- ☐ **RISIKOMANAGEMENT VON DRITTPARTEIEN**
  Ransomware kann auch über Dienstleister in das eigene Unternehmen gelangen.
- ☐ **PATCH- UND EXPOSURE-MANAGEMENT**
  Fördert die schnelle Installation von Sicherheitsupdates, um Lücken frühestmöglich zu schließen.
- ☐ **TRENNUNG VON ADMIN- UND NUTZERKONTEN**
  Etablierung von einer strikten Trennung zwischen Administratorenkonten mit hohen Privilegien und normalen Nutzerkonten.
- ☐ **NOTFALLPLAN FÜR ZWISCHENFÄLLE**
  Dokumentation aller Verfahren zu Kommunikation, Reaktion und Einbindung von Sicherheitsbehörden.
- ☐ **KONTROLLIERTER ZUGRIFF VON AUSSEN**
  Aufbau eines Identitäts- oder Berechtigungs- und Zugangsmanagements (mehrstufig MFA).
- ☐ **ERSTELLEN VON BACKUPS**
  Vorbeugung gegenüber Schäden mit Hilfe einer klaren, redundanten und umgesetzten Backup-Strategie – sowohl online wie offline.
- ☐ **E-MAIL-FILTERUNG**
  Installation von Spam-Detektoren und Blockierung von auffälligen Servern.
- ☐ **ANGEMESSENES IT-SICHERHEITSBUDGET**
  Empfehlung: mind. 20% des IT-Budgets



TRAINIERE REGELMÄSSIG

REAKTIV – WIE VERHÄLT MAN SICH, WENN ES PASSIERT IST?

ANGRIFFE FESTSTELLEN

INFORMATIONSTECHNOLOGIE (IT)

- **BETROFFENE SYSTEME UNTER QUARANTÄNE STELLEN**
- **ANALYSE DES NETZWERKVERKEHRS**
- **AUSWERTEN VON LOG-DATEIEN**
- **BACKUPS ÜBERPRÜFEN**

SCHLIESSEN DER LÜCKEN UND WIEDERHERSTELLEN DER SYSTEME

Quellen: eigene Darstellung; [8, 12, 16, 19, 20, 35, 59]

DISTRIBUTED DENIAL OF SERVICE (DDoS)
CHECKLISTE ZUM SCHUTZ GEGEN DDoS-ANGRIFFE

- ☐ **DDoS-REAKTIONS-STRATEGIE**
  Für die Entwicklung wird empfohlen, einen Plan A und B zu erstellen.
- ☐ **DDoS-RESILIENTE IT-STRUKTUR**
  Ziel hierbei ist es, den technischen Aufwand für Angreifer zu erhöhen.
- ☐ **AUFBAU VON REAKTIONS-TEAMS MIT EXPERTISE**
  Sicherstellung der Verfügbarkeit durch ein Team aus erfahrenen Mitarbeitern.
- ☐ **POTENZIELLE ZIELE IDENTIFIZIEREN**
  Sicherstellung der Verfügbarkeit der Systeme und Geschäftsprozesse.
- ☐ **VERANTWORTLICHKEITEN FÜR SYSTEME KLÄREN**
  Identifizierung der personellen Zuständigkeiten der ermittelten Ziele.
- ☐ **PLAN ZUR AUFRECHTERHALTUNG DES GESCHÄFTSBETRIEBS**
  Definieren von alternativen Handlungen bei Unterbrechung.
- ☐ **NETZWERKSEGMENTIERUNG UND LASTAUSGLEICH**
  Segmentierung nach Art und Nutzung der Dienste.
- ☐ **PATCH-MANAGEMENT**
  Beseitigen von bekannten Schwachstellen durch Einspielen von Patches und Nutzung von Exposure-Management-Lösungen.
- ☐ **DDoS-RESILIENT BY DESIGN FÜR IoT-GERÄTE**
  Resilientes Design für die Sicherheit und Verfügbarkeit von Komponenten im Bereich IoT.
- ☐ **KRITISCHE SYSTEME ZU DRITTANBIETERN AUSLAGERN**
  Es ist ratsam, besonders gefährdete Systeme zu Dienstleistern auszulagern.
- ☐ **LEISTUNGSGRENZEN DER SYSTEME DEFINIEREN**
  Festlegen von Schwellenwerten, bei denen Abwehrmaßnahmen erfolgen müssen.
- ☐ **PROAKTIVE ANALYSE UND MONITORING**
  Hilft dabei, Auffälligkeiten im Netzwerk frühestmöglich zu erkennen.

FÜR DEN ERNSTFALL

DIE WELLE WIRD STÄRKER

In den letzten Jahren hat sich die Maximalkraft der DDoS-Wellen dramatisch erhöht.

DER BISLANG HÖCHSTE GEMESSENE DDoS-ANGRIFF LAG BEI 3,2 TB/s

ORGANISATION

- **WEDER VERHANDELN NOCH BEZAHLEN**
- **MELDEN VON CYBERANGRIFF (AN SICHERHEITSBEHÖRDEN)**
- **KRISENKOMMUNIKATION AUFSETZEN**
- **NOTFALLMANAGEMENT STARTEN**

LESSONS LEARNED – IN DIE ZUKUNFT INVESTIEREN

5 Der Weg vor die Cyberkriminalitätswelle

Neben der Erkenntnis und dem Problemverständnis zählen letztendlich nur die erfolgreichen Maßnahmen, um den möglichen Angreifern das Leben so schwer wie möglich zu machen. Da ein Großteil der Unternehmen im Berichtszeitraum bereits schmerzliche Erfahrungen mit Cyberangriffen sammeln musste, rückt das Thema Cybersicherheit zunehmend in den Fokus von Entscheidern [2], [21], [27], [28], [75]. So sind – zusammengenommen – das Bewusstsein und die Besorgnis über Risiken bei Führungskräften stark von 16 Prozent auf 27 Prozent bei den Befragten angestiegen [75].

Für die Zukunft und die anstehenden Herausforderungen steht daher das erfolgreiche Umsetzen von Maßnahmen, sowohl für Unternehmen mit niedrigem als auch für solche mit hohem Reifegrad in Bezug auf Cybersicherheit, an erster Stelle. Die Ergebnisse von besser abgesicherten Unternehmen zeigen, dass konsequent umgesetzte Maßnahmen sich insgesamt positiv auf die Cybersicherheit auswirken [28].

5.1 Allgemeine Maßnahmen und Budgets

Zur Verminderung von Schäden oder Beeinträchtigungen durch erfolgreiche Cyberangriffe lassen sich die effektiven Maßnahmen wie folgt einteilen [23], [28], [75]:

1. Entwicklung einer risikobasierten und proaktiven Cyberstrategie
2. Schaffung und Pflegen einer Sicherheitskultur
3. Einbeziehung aller Prozesse einer Organisation
4. Verbesserungen der Fähigkeiten von Mitarbeitern
5. Investition in die geeignetsten Cybersicherheitstechnologien und -dienstleistungen

Wegen der erheblichen Auswirkungen auf Unternehmen, heutige wie auch zukünftige Cyberbedrohungen mit sich bringen, sollte jedes Unternehmen eine risikobasierte und proaktive Cyberstrategie entwickeln und umsetzen [28]. In die Entwicklung sollten die zukünftigen Herausforderungen der nächsten drei bis fünf Jahre mit einfließen [35]. Hierbei müssen die Unternehmensleitung und die Führungskräfte eng zusammenarbeiten, damit der Schutzbedarf von Vermögenswerten und Prozessen mit den Gefahren und Investitionsentscheidungen solide abgestimmt werden können, um eine cyberresiliente IT-Architektur zu erreichen [75]. Die Prüfung und der Abgleich der Strategie sollten jährlich an die aktuellen Herausforderungen angepasst werden [28].

Obwohl der Einsatz von Technologien bei Cyberangriffen und deren Abwehr den größten Einflussfaktor besitzt, spielt eine Cybersicherheitskultur im Unternehmen eine sehr wichtige Rolle bei der Umsetzung von Maßnahmen. Diese Maßnahme liegt die Erkenntnis zu Grunde, dass der Mensch oder besser der Endnutzer ein entscheidendes Glied in der Kette zur Verhinderung von Sicherheitsverletzungen ist [25]. Für das Etablieren einer funktionierenden Sicherheitskultur sollten demnach das Bewusstsein und die Sensibilisierung für Cybersicherheit bei allen Mitarbeitern eines Unternehmens gestärkt werden, um die Cyberresilienz in einem Unternehmen maßgeblich zu verbessern. Die Etablierung der Sicherheitskultur sollte im Unternehmen in der höchsten Führungsebene verankert sein und auch Aufsichtsräte mit einschließen [23], [75].

Zur erfolgreichen Umsetzung einer Cyberstrategie sollte diese vorhandene Betriebsabläufe in einem Unternehmen ausreichend berücksichtigen. Außerdem zeigen Ergebnisse bei Unternehmen mit hohem Reifegrad in Bezug auf Cybersicherheit, dass das Einbinden der gesamten Organisation und von Prozessen zu besseren Ergebnissen führt. In diesem Zusammenhang ist ein wichtiger Aspekt die klare Festlegung von Verantwortlichkeiten [28]. Die höchsten Führungskräfte für Cybersicher-

heit sollten auch direkt an den CEO berichten [27], [28], [52], [53]. Die Festlegung und die Nutzung von einheitlichen Leistungsindikatoren im gesamten Unternehmen helfen bei der Bewertung von Maßnahmen [75].

Die robuste Planung von Umsetzungsmaßnahmen zur Prävention, Erkennung und Untersuchung sowie die Erstellung von auf das Unternehmen angepassten Reaktionsplänen spielen eine wichtige Rolle. Zur Erzielung einer ausreichenden Cybersicherheit sollte von allen Beteiligten bei der Etablierung von Prozessen immer der Aspekt beachtet werden, dass die Schnelligkeit der Reaktion auf einen Angriff einen entscheidenden Faktor für den Erfolg oder Misserfolg eines Angreifers mit hoher Professionalität hat [25], [75].

Für die Umsetzung von Maßnahmen werden gut ausgebildete und erfahrene Mitarbeiter benötigt. Dabei besteht die größte Herausforderung bei einem Großteil von Unternehmen (bis 47 Prozent) bereits darin, dass bereits ein Mangel an qualifizierten Cybersicherheitsfachkräften besteht [28], [39], [52], [53]. Daher sollten Unternehmen verstärkt auf die Talentakquise wie auch auf die Ausbildung von bestehenden Mitarbeitern setzen, um die Lücke an Kompetenz schnell zu schließen [28]. Nach Untersuchungen von IBM können die Kosten bzw. Schäden durch ein kompetentes Reaktionsteam im Durchschnitt um ca. 13 Prozent gesenkt werden [54]. Bei der Erkennung von neuartigen Angriffen werden auch in Zukunft eine Kombination aus Technologie und erfahrenen Fachkräften notwendig sein, um die raffiniertesten Bedrohungen zu erkennen und abzuwehren [75].

Bei der Etablierung von Techniken oder Technologien für die Cybersicherheit gilt der Grundsatz, je länger der „Weg“ oder je größer der Aufwand für mögliche Angreifer ist, desto geringer ist die Wahrscheinlichkeit eines erfolgreichen Angriffs mit Daten- bzw. Informationsabflüssen [74]. Außerdem sollte als Grundregel die Angriffsfläche für mögliche Angreifer bei IT-Systemen und eingesetzter Software minimal gehalten werden [13], [44]. Bei der technischen Umsetzung sollten Unternehmen auf eine sogenannte Zero-Trust-Architektur setzen und Technologien danach auswählen. Bei der Zero-Trust-Architektur wird eine Authentifizierung für alle Aktionen, Benutzer und Geräte angestrebt, um insgesamt eine cyberresiliente IT-Architektur zu etablieren [48]. Außerdem wird bei der Zero-Trust-Architektur das Prinzip der geringstmöglichen Berechtigungen (nach risikobasierten adaptiven Richtlinien) für Nutzer oder Systeme angewendet, um die Daten besonders zu schützen [28], [48].

Für die Umsetzung einer Cyberstrategie muss für die Beschaffung das notwendige Budget eingeplant werden. Die Ausgaben für IT-Technologien variieren im Jahr 2022 je nach Branche sehr stark und liegen zwischen zwei Prozent (Industrieprodukte) und 18 Prozent (Software-Entwicklung) des Gesamtumsatzes [71]. Im Durchschnitt über alle Branchen werden ca. zwischen drei Prozent und fünf Prozent des Gesamtumsatzes für IT-Sicherheit ausgegeben. Für das Jahr 2023 wird ein gemitteltes Wachstum der IT-Budgets in Deutschland von neun Prozent erwartet [4].

Nach einer Untersuchung der ENISA variieren die Ausgaben für Cybersicherheit stark je nach Branche und liegen in einem Bereich von fünf Prozent des gesamten IT-Budgets im Energiesektor bis zehn Prozent bei digitalen Infrastrukturen [35]. Im Jahr 2022 beträgt der Markt für IT-Sicherheit bzw. Cybersicherheit in Deutschland 7,8 Milliarden Euro. Nach einer Schätzung der Bitkom soll der Markt für IT-Sicherheit in Deutschland jährlich um bis zu zehn Prozent wachsen [5]. Weltweit wird ein durchschnittliches Wachstum von elf Prozent pro Jahr prognostiziert [42]. McKinsey schätzt, dass der weltweite Markt bei 1–2 Billionen Euro liegt, davon jedoch erst 150 Milliarden Euro realisiert sind [1]. Für einzelne Cybersicherheitstechnologien werden von der ENISA noch größere Wachstumszahlen erwartet und diese liegen zwischen 16 Prozent (für Cyber Threat ntelligence) und 22 Prozent (für Applikationssicherheit, Cloud-Sicherheit, Data Privacy) [35].

5.2 Maßnahmen gegen Social Engineering

Zu den wichtigsten und wirksamsten Maßnahmen gegen Social Engineering zählen:

1. regelmäßige Awareness-Schulungen durchführen und vertiefend auf die Funktion des Arbeitnehmers abstimmen

2. Etablierung und regelmäßige Anpassung eines Reaktionsplans

3. ständige Überwachung unternehmensähnlicher Ressourcen/Domains sowie des digitalen Fußabdrucks des Unternehmens mittels Recherchen auf nach frei verfügbaren Quellen

4. Überwachung des E-Mail-Verkehrs mit Hilfe von Regeln und Filtern

Um ein Sicherheitsbewusstsein gegenüber Social Engineering zu erzeugen und zukünftigem Fehlverhalten vorzubeugen, sollten regelmäßige Schulungen für Mitarbeiter durchgeführt werden. Mit regelmäßigen Schulungen kann insbesondere auf aktuelle Trends und Methoden des Social Engineerings eingegangen werden. Mitarbeiter sollten dabei mit den in ihrer Funktion am häufigsten auftretenden Betrugs- und Manipulationsversuchen vertraut gemacht werden [33]. Dadurch würden, beispielsweise durch Finance Phishing, viel weniger Mitarbeiter zum Opfer werden, wenn bekannt wäre, dass Banken in Deutschland unter keinen Umständen per E-Mail dazu auffordern, Zugangsdaten einzugeben oder Links in E-Mails anzuklicken [13]. Untersuchungen bestätigen, dass diese Schulungen sehr wirksam sind. Die Ergebnisse zeigen, dass sich die Schulungen auf 90 Prozent der Teilnehmer mit technischem Hintergrund und sich auf 70 Prozent der Teilnehmer ohne technischen Hintergrund positiv auswirken [74]. Für Schulungen kann auf aktuelle behördliche Informationen wie solche des BSI [11] oder der Cybersecurity and Infrastructure Security Agency (CISA) [18] zurückgegriffen werden.

Um bei einem Angriff oder einem Vorfall angemessen und schnell reagieren zu können, wird von Experten empfohlen einen auf das Unternehmen angepassten Reaktionsplan für Social Engineering zu entwickeln. Mit der Etablierung und regelmäßigen Aktualisierungen von Reaktionsplänen zu Phishing-Vorfällen kann im Falle eines Angriffs schnell und effizient gehandelt werden. Damit ist es möglich, diese Angriffe abzuwenden oder schadensbegrenzende Maßnahmen einzuleiten [33].

Da der Angreifer bei Social Engineering massiv darauf angewiesen ist, das Vertrauen oder die Beziehung zu seinem potenziellen Opfer über Informationen aufzubauen, ist es für Unternehmen oder Privatpersonen besonders wichtig, darüber Kenntnis zu haben, welche Informationen für den Angreifer verfügbar (sogenannte Open Source Intelligence [OSINT]) sind. Über die Ernennung einer Person, welche regelmäßig OSINT-Recherchen zur eigenen Organisation betreibt, ist es möglich, den digitalen Fußabdruck des Unternehmens zu überwachen. Außerdem können dadurch frühzeitig Erkenntnisse über Datenschutzverletzungen und die Veröffentlichung von sensiblen Daten in kriminellen Foren erlangt werden [33].

Damit Angriffe durch die Nutzung von Social Engineering ihre potenziellen Opfer gar nicht erst erreichen, sollten moderne Technologien zum Filtern und Analysieren von E-Mail-Nachrichten eingesetzt werden. Erkenntnisse über neue Social-Engineering-Aktivitäten können u.a. mit Hilfe von Filtermaßnahmen für die Verhinderung eines Eindringens in die eigenen Unternehmensnetzwerke verwendet werden [33]. Diese Maßnahmen umfassen neben einer E-Mail-Filterung auch Webfilter, welche den Zugang zu Phishing-Websites und das Nachladen von Malware unterbinden. Unternehmen sollten den Empfang und das Versenden von Dateianhängen unbedingt bei der Filterung miteinbeziehen. So kann sichergestellt werden, dass den Nutzer auch von scheinbar vertrauenswürdigen Absendern kein Schadcode erreicht [13]. Über das Verbot von potenziell gefährlichen Dateitypen und die ausschließliche Bereitstellung von Software aus einer geprüften und sicheren Quelle kann das Schutzmaß weiter erhöht werden. Zudem sollten Berechtigungen für Nutzer und Programme regelmäßig überprüft und angepasst werden [33].

5.3 Maßnahmen gegen Ransomware

Zu den wichtigsten und wirksamsten Maßnahmen gegen Ransomware zählen:

1. Bewusstsein gegenüber Ransomware-Bedrohungen schaffen
2. resiliente IT-Infrastruktur durch Netzwerksegmentierung herstellen
3. Schwachstellen in der IT-Infrastruktur kontinuierlich entdecken und wirksam beseitigen
4. Entwicklung eines Reaktionsplans und Überwachung der IT-Infrastruktur
5. regelmäßige Erstellung von mehrfach redundanten Sicherungen von besonders gefährdeten Informationen bzw. Daten
6. Melden der Ransomware-Angriffe und Strafanzeige erstatten

5.3.1 Prävention

5.3.1.1 Organisatorisch

Risikobasierte und proaktive Cyberstrategie

Vor der Festlegung von Maßnahmen und Prioritäten müssen Sie Ihre Organisation inklusive aller möglichen Kunden- und Lieferkettenbeziehungen verstehen. Diese Untersuchung sollte durch externe Experten begleitet werden und eine Risiko- und Schwachstellenanalyse von Organisation, Prozessen und Technik miteinander verknüpfen. Nur so können Sie eine für sich passende Cybersicherheitsstrategie entwickeln.

Resiliente IT-Infrastruktur durch Netzwerksegmentierung

Durch die strategische oder proaktive Herstellung einer resilienten Internet-Infrastruktur kann der Aufwand zum Eindringen in das System massiv erhöht und damit die Wahrscheinlichkeit einer Detektion von Angriffen gesteigert werden. Bei der proaktiven Konzeption des Netzwerkes kann auf bewährte Praktiken wie Netzwerksegmentierung, aktuelle Patches, regelmäßige Backups und ein angemessenes Identitäts- oder Berechtigungs- und Zugangsmanagement, vorzugsweise mit Multi-Faktor-Authentifizierung (MFA), zurückgegriffen werden [33], [31]. Durch den Einsatz von aktuellen Technologien wie Endpoint Detection and Response und Extended Detection Response, sowie der Verwendung von aktuellen Signaturen wird das Risiko für einen Ransomware-Angriff minimiert [33].

Cybersicherheitskultur und Ransomware-Awareness-Training

Da das Einfallstor von Ransomware in IT-Systeme sehr oft über die Schwachstelle „Mensch“ durch die Anwendung verschiedenster Social-Engineering-Techniken verläuft, ist es besonders wichtig, das Bewusstsein zum Erkennen von Angriffen bei den Nutzern durch wirksame Schulungen zu stärken. Der Austausch und die Zusammenarbeit mit anderen Cybersicherheitsexperten und nationalen Computer-Emergency-Response-Teams und die Nutzung von verfügbaren Tools für den Austausch von Malware-Informationen können zur Verbesserung der Cyberresilienz beitragen [33].

Reaktionsplan für Ransomware-Attacken

Um für einen möglichen Angriff auch organisatorisch vorbereitet zu sein, empfiehlt es sich, einen Reaktionsplan für Zwischenfälle zu erstellen, zu pflegen und zu üben. In diesem Plan sollten alle Kommunikationsabläufe, alle Reaktions- und Benachrichtigungsverfahren dokumentiert sein [33], [31], [8], [37]. Für den Umgang mit Vorfällen kann man sich an umfassenden Checklisten beispielsweise von der CISA [19] orientieren.

Versicherung abschließen

Über eine Cyber-Versicherung können die finanziellen Auswirkungen im Falle eines Ransomware-Angriffs geschmälert werden. Es sollten regelmäßige Risikoanalysen durchgeführt werden, aufgrund deren überlegt werden kann, ob eine Cyber-Versicherung einen Vorteil bringen würde [31]. Ebenfalls ist es wichtig, das Versicherungsunternehmen mit Vorfallsszenarien zu konfrontieren, um festzustellen, ob die Versicherung in typischen Fällen den Schaden übernimmt.

Kritische Systeme kennen und härten

Durch das IT-Assest Management und die Einführung eines Exposure Managements hat die IT-Abteilung einen Überblick über alle IT-Systeme sowie deren Hard- und Software-Version. Hiermit ist es möglich, kritische Systeme und Handlungsbedarfe im Netzwerk zu identifizieren und Updates zu priorisieren [8].

Regelmäßige Übungen durchführen

Regelmäßige Übungen helfen nicht nur im Notfall, sondern können die Mitarbeiter auch schon im Voraus für das Thema sensibilisieren. Durch Übungen werden Notfallpläne wie zum Beispiel das Wiederaufsetzen von Systemen nicht nur theoretisch durchgespielt, sondern auch praktisch geübt. Hierdurch können die theoretischen Pläne durch praktische Erfahrungen ergänzt werden, wie die Zeit, die benötigt wird, den Notfallplan umzusetzen [8].

Sicherstellen, dass Dritte bewährte Praxis anwenden

Ransomware kann auch über Dienstleister in das eigene Unternehmen gelangen. Deshalb sollte nicht nur auf das Risikomanagement und Cyberresilienz des eigenen Unternehmens, sondern auch auf angemessene Sicherheitsmaßnahmen von anderen Unternehmen geachtet werden, die in direkter oder indirekter Beziehung zum eigenen Unternehmen stehen (vgl. Lieferkette) [19].

5.3.1.2 Technisch

Eingeschränkter und kontrollierter Zugriff von außen

Um Zugriff auf die IT-Infrastruktur von außen sicher zu gewährleisten, bedarf es eines angemessenen Identitäts- oder Berechtigungs- und Zugangsmanagements. So sollten Zugang für externe Verbindungen nur für bekannte IP-Adressen via VPN erlaubt werden – vorzugsweise mit Multi-Faktor-Authentifizierung [33], [31], [8].

Netzwerksegmentierung

Es ist gängige Praxis, Altsysteme (vgl. Legacy-Systeme) zu betreiben, die keine Sicherheitsupdates erfahren können. Damit diese dennoch sicher im operativen Umfeld genutzt werden können, ist es notwendig, sie von anderen Systemen innerhalb des Netzwerks angemessen zu trennen bzw. zu isolieren [8].

Patch-Management

Ein Einfallstor für Malware und insbesondere Ransomware sind Sicherheitslücken in Browsern und deren Plugins. Durch ein konsequentes Patch-Management können Sicherheitsupdates von Herstellern solcher Produkte schnell installiert werden, um Lücken frühestmöglich zu schließen, bevor diese von Angreifern ausgenutzt werden können [13], [33].

Erstellung von Backups

Nach einem erfolgreichen Ransomware-Angriff kann die Wiederherstellung der Betriebsfähigkeit nur durch eine klare, redundante und vollständig umgesetzte Backup-Strategie gewährleistet werden [13]. Ebenfalls besteht die Möglichkeit, die Daten ggf. wieder zu entschlüsseln, da beispielsweise von Europol [37] Werkzeuge zur Entschlüsselung für weit verbreitete Ransomware-Instanzen existieren. Die Anwendung der 3-2-1-Regel (drei Kopien, zwei verschiedene Speichermedien, eine Kopie außerhalb) und die Verschlüsselung von Datensicherungen schützen diese vor dem Angreifer. Die Zugänge zu betroffenen Systemen sollten ebenfalls bis zur Behebung stillgelegt werden [31].

Zentrales Monitoring von Netzwerken

Log-Daten, welche Aktivitäten innerhalb des Netzwerks festhalten, sollten regelmäßig überprüft werden. So kann proaktiv eine potenzielle Ausbreitung in weitere Bereiche des Netzwerks unterbunden werden. Dies Bedarf einer Logging-Policy, die idealerweise mittels eines zentralen Servers Logs manipulationssicher speichert. Existiert eine solche Policy noch nicht, muss dies unbedingt nachgeholt werden. Das Monitoring kann durch Security-Information-and-Event-Management- (SIEM-) bzw. Angriffserkennungssysteme automatisiert ergänzt werden [8]. Zudem ist die Minimierung von Reaktionszeiten von enormer Bedeutung, denn die Zeit, die Angreifer zur Verbreitung von Ransomware innerhalb eines Unternehmens benötigen, ist sehr kurz [25].

Trennung von Administratoren- und Nutzerkonten

Es muss eine strikte Trennung zwischen Administratorenkonten mit hohen Privilegien und normalen Nutzerkonten etabliert werden. So haben es Angreifer schwerer, ein Konto mit erhöhten Berechtigungen zu kompromittieren, da es nicht für gewöhnliche Bürotätigkeiten (u.a. E-Mail-Verkehr, Browsing) Anwendung findet. Grundsätzlich gilt das Prinzip, dass Konten immer nur mit den geringsten Privilegien erstellt werden (vgl. Principle of Least Privilege) [31], [8].

Absicherung des Perimeters

Angriffe auf eine IT-Infrastruktur finden häufig auf über das Internet erreichbare Systeme statt. Zur regelmäßigen Überprüfung, ob Schwachstellen auf diesen Systemen von außen ausgenutzt werden können, helfen Penetrationstests. So kann auch die Härtung des jeweiligen Systems überprüft werden. Ähnliche Vorgehensweisen lassen sich auch für interne Systeme überlegen [8], [19].

Verschlüsselung von personenbezogenen Daten
Daten mit Personenbezug sollten DSGVO-konform verschlüsselt werden. So können sie nicht ohne weiteres von Cyberkriminellen ausgenutzt werden [31].

Blockierung des Zugriffs auf bösartige Infrastrukturen
Ransomware benötigt häufig Zugriff auf externe Command-and-Control-Server. Können solche Verbindungen aus dem internen Netzwerk heraus unterbunden werden, so sind Angreifer in ihrem Handlungsspielraum stark begrenzt. Eine Verbindungskontrolle bzw. -beschränkung kann hier entsprechend Abhilfe schaffen. Hierfür gibt es frei verfügbare DNS- oder Malware-Filterungsdienste, die dabei unterstützen können [8].

Einschränken von Makros
Trotz aller Maßnahmen besteht das Potenzial, dass Malware bzw. Ransomware die IT-Infrastruktur erreicht. Hier sollte verhindert werden, dass Schadcode aktiv auf dem System ausgeführt werden kann, indem Scripting und Makros deaktiviert werden. In Abhängigkeit vom jeweiligen Betriebssystem lässt sich dies über Gruppenrichtlinien oder andere technische Mechanismen erwirken [8], [19].

E-Mail-Filterung
Durch Mechanismen wie Spam-Detektoren am E-Mail-Gateway und die Blockierung von auffälligen Servern können bösartige E-Mails und Anhänge sicher erkannt und gefiltert werden. Zusätzlich können Anhänge mittels Sandboxing in einer isolierten Umgebung geprüft werden [8].

Backups überprüfen
Bevor eine Wiederherstellung durchgeführt wird, sollte sichergestellt werden, dass das Backup nicht bereits von der Ransomware infiziert wurde. Durch Verwendung von Backup-Kopien oder Write-Blockern wird beim Einspielen des Backups sichergestellt, dass eine Infektion nicht auf die Sicherungskopie übergreift [8].

Auswerten von Log-Dateien
Zuvor erfasste Log-Dateien können bei der Analyse und Aufklärung eines Sicherheitsvorfalls unterstützen. Sie können Aufschluss darüber geben, welche Systeme oder Segmente betroffen sind. Darüber hinaus können sie wichtige Hinweise über den tatsächlichen Infektionsweg der Ransomware geben [8].

5.3.2 Reaktion

5.3.2.1 Organisatorisch

Melden von Ransomware-Attacken
Das Melden eines Ransomware-Angriffes und das Erstatten einer Strafanzeige zeigen ebenfalls Wirkung, denn hier zeigen Ergebnisse des FS-ISAC, dass Angreifer ihren Betrieb einstellen, wenn sie den Druck der Strafverfolgungsbehörden verspüren. [40]. Die Kollaboration mit den zuständigen Behörden stellt ebenfalls ein wirksames und sehr wichtiges Werkzeug gegen Ransomware da. Nur dadurch können eine polizeiliche Prävention und Strafverfolgung erfolgreich sein. Zudem können Behörden eine unterstützende Funktion bieten, indem sie auf das korrekte Verhalten bei einem Vorfall hinweisen [14], [31].

Weder verhandeln noch bezahlen
Behörden wie das BSI oder Europol raten grundsätzlich davon ab, das geforderte Löse- oder Schweigegeld zu zahlen oder mit den Angreifern zu verhandeln, da keine Garantie besteht, dass die Schlüssel herausgegeben werden [13], [31]. Außerdem ermutigt man die Angreifer durch eine erfolgreiche Zahlung zu weiteren Straftaten [31]. Auf den Seiten von Europol [37] und der CISA [19] werden auch detaillierte Handlungsempfehlungen bei einem erfolgreichen Ransomware-Angriff aufgeführt.

Aus der Vergangenheit lernen
Aus Angriffen lassen sich Erkenntnisse über Schwachpunkte und Fehlverhalten ziehen. Sie sollten in die bisherige Reaktionsstrategie und Awareness-Trainings mit eingebaut werden, um künftige Vorfälle besser zu unterbinden bzw. auf sie reagieren zu können [8].

5.3.2.2 Technisch

Betroffene Systeme unter Quarantäne stellen
Isolierung von durch Ransomware befallenen Systemen innerhalb der IT-Infrastruktur hilft dabei, die Verbreitung der Ransomware im Netzwerk einzudämmen [31].

Betroffene Systeme versuchen zu entschlüsseln
Von offiziellen Stellen werden Werkzeuge frei zur Verfügung gestellt, um von Ransomware verschlüsselte Daten wieder zu entschlüsseln. Eines dieser Werkzeuge ist das von Europol zur Verfügung gestellte No-More-Ransom-Projekt, welches für 162 Ransomware-Varianten Schlüssel für die Entschlüsselung von infizierten Daten bereitstellt [31].

5.4 Maßnahmen gegen Angriffe auf die Verfügbarkeit

Zu den wichtigsten und wirksamsten Maßnahmen gegen DDoS-Bedrohungen zählen:

1. Schulung und Festlegung einer Reaktionsstrategie für den Umgang mit DDoS
2. IT-Infrastruktur DDoS-resilienter auslegen
3. Nutzung von Mitigationsdienstleistern für gezielte DDoS-Abwehr
4. Melden von DDoS-Attacken
5. vorbereitet sein auf zukünftige DDoS-Attacken

5.4.1 Prävention

5.4.1.1 Organisatorisch

DDoS-Reaktionsstrategie
Besonders Unternehmen mit mittlerer oder niedriger Cyberresilienz sollten den Ausbau einer Reaktionsstrategie verstärkt angehen, da diese Unternehmen signifikant mehr Angriffe zu verzeichnen haben. Für die Entwicklung einer Strategie zur Wiederherstellung der Betriebsfähigkeit wird von BSI und ENISA empfohlen einen Plan A und B zu erstellen [33], [28], [12].

Beauftragung von DDoS-Mitigationsdienstleistern
Durch die Nutzung von spezieller Software oder Mitigationsdienstleistern können DDoS-Angriffe durch Maßnahmen wie Protokollkonformität oder durch Anwendung von Filterung für die Quell- und Zieladressen abgeschwächt werden. Das BSI bietet eine Liste von geprüften Mitigationsdienstleistern sowie eine Sammlung von Sofortmaßnahmen für die Abwehr von DDoS-Angriffen an [12], [10]. Hierbei

ist es besonders wichtig, den Umfang der Dienstleistungen zu verstehen, um Limitierungen sowie Lücken aufzudecken und mitigieren zu können [33], [20].

Aufbau von Reaktionsteams mit angemessener Expertise
Um während DDoS-Angriffen die Verfügbarkeit der Systeme und der Geschäftsprozesse sicherzustellen, ist es wichtig, ein Team aus erfahrenen Mitarbeitern mit entsprechendem Wissen zu bilden. Das Team sollte bereits proaktiv vor Angriffen gebildet werden und aus Mitarbeitern des IT-Betriebs und des IT-Sicherheitsteams, dem IT-Sicherheitsbeauftragten sowie dem Presse- und Öffentlichkeitsteam bestehen. Nur so ist es möglich, schnellstmöglich auf einen Angriff zu reagieren, damit Kunden und Vertragspartner über die Einschränkung schnell informiert werden [33], [12].

Potenzielle Ziele identifizieren
Es sollten alle möglichen Ziele für DDoS-Angriffe im Unternehmen identifiziert und bewertet werden. Ziele können unter anderem Webserver, Mailserver, DNS-Server oder VPNs sein. Bei der Bewertung der Ziele sollten Schwachpunkte bzw. Engstellen des Netzwerks identifiziert werden und eine Priorisierung zur Absicherung erstellt werden [33], [9], [20].

Verantwortlichkeiten für Systeme klären
Um im Falle eines Angriffs die Koordination und somit die Einleitung von Abwehrmaßnahmen zu erleichtern, sollten im Vorfeld die personellen Zuständigkeiten der ermittelten Ziele sowie deren Rollen identifiziert und festgehalten werden [9].

Plan zur Aufrechterhaltung des Geschäftsbetriebs erstellen
Über einen Plan zur Aufrechterhaltung des Geschäftsbetriebs lassen sich alternative Wege, beispielsweise für die Kommunikation, definieren, welche im Falle eines Ausfalls Anwendung finden. Dadurch kann die Unterbrechung des Geschäftsablaufs und somit auch die dadurch entstehenden Kosten erheblich reduziert werden [33], [20].

Mitarbeiterschulungen und Übungen zur Vorbereitung auf DDoS-Angriffe
Damit verantwortliche Mitarbeiter stets gut auf aktuelle Angriffsmethoden und Abläufe bei einem Zwischenfall vorbereitet sind, ist es essenziell, das notwendige Wissen in Schulungen zu vermitteln und die Abläufe in Übungen durchzuspielen. Dieses Wissen kann zudem dazu beitragen, Lücken aufzudecken und Härtungsmaßnahmen durchzuführen [33], [9], [20].

5.4.1.2 Technisch

DDoS-resiliente IT-Struktur
Die Infrastruktur kann durch spezifische Maßnahmen resilienter bzw. härter gegenüber DDoS-Attacken ausgelegt werden. Das Hauptziel dieser Härtung besteht insgesamt darin, den technischen Aufwand und demnach die Angriffskosten für einen Angreifer insgesamt massiv zu erhöhen, so dass die Attacke für den Angreifer zu teuer wird und er von einer Fortsetzung absieht [33].

Netzwerksegmentierung und Lastausgleich
Durch die Anwendung von Netzwerksegmentierung nach Art und Nutzung der Dienste sowie durch die Absicherung der Netzwerkinfrastruktur mittels Proxy-Lösungen, Loadbalancing und Einbindung des genutzten Internet-Service-Providers (ISP) bei den vorbeugenden technischen Maßnahmen lässt sich die Widerstandsfähigkeit der eigenen IT-Systeme erhöhen [9].

Patch Management
Durch die Aktualisierung von Webservern und das schnelle Beseitigen von bekannten Schwachstellen durch Einspielen von Patches im Rahmen eines ganzheitlichen Exposure Managements kann der Aufwand für Angreifer deutlich erhöht werden [33].

DDoS-resilient by Design für IoT
Die Angreifer haben das Interesse, die Verfügbarkeit von Komponenten zu beschränken sowie den Betrieb anderer Netze oder Systeme massiv zu stören oder aber auch das Potenzial, die Sicherheit

der Nutzer zu gefährden. Unternehmen sollten sich frühzeitig mit diesem Thema befassen und hier bereits bei der Installation von neuen Systemen im Bereich des Internet of Things (IoT) auf ein resilientes Design und entsprechende Konfiguration achten [33].

Nach den aktuellen Untersuchungen der ENISA verlagern sich DDoS-Angriffe verstärkt in Richtung Mobilfunknetze und dem Internet of Things (IoT). Hier bieten Sensoren und Geräte ein geeignetes Ziel für DDoS-Angriffe, da diese Systeme nur über begrenzte Ressourcen verfügen und daher oft schlecht geschützt sind.

Verlagerung kritischer Systeme zu Drittanbietern
Bei besonders gefährdeten Systemen wie beispielsweise Webseiten ist es ratsam, diese zu Dienstleistern auszulagern, welche über eine bessere Infrastruktur verfügen, um Angriffe abzuwehren und Leistungsspitzen abzufedern. Neben einer höheren Verfügbarkeit und höheren Kosten auf der Seite des Angreifers können so auch die Kollateralschäden minimiert werden [33], [9].

Leistungsgrenzen der Systeme definieren
Über wohldefinierte Leistungsgrenzen der Systeme lassen sich Schwellwerte festlegen, ab welchen vorkommenden Lasten eine genauere Beobachtung und ab wann gezielte Abwehrmaßnahmen vonnöten sind. Dabei sind insbesondere auch Netzwerk-Knotenpunkte wie Paketfilter, Switches und Router mit einzubeziehen, da sie oftmals das schwächste Glied der Kette bilden [9].

Analysemittel bereitstellen
Benötigte Programme und Logs, welche nach und während eines Angriffes zur Analyse vonnöten sind, müssen zuvor installiert und konfiguriert werden, um im Ernstfall schnellstmögliche effektive Gegenmaßnahmen einzuleiten [9].

Proaktives Monitoring
Mit Hilfe einer proaktiven Überwachung des Netzwerks kann eine Baseline gebildet werden. Diese hilft im Anschluss Auffälligkeiten im Netzwerk, welche auf einen Angriff hindeuten, frühestmöglich zu erkennen. Beim Erstellen der Baseline ist es wichtig, sowohl Tage mit gewöhnlicher als auch solche mit besonders hoher Auslastung mit einzubeziehen, um das System nicht zu sensibel gegenüber gewöhnlichen Lastspitzen zu machen [33], [20].

5.4.2 Reaktion

5.4.2.1 Organisatorisch

Melden von DDoS-Angriffen
Nicht nur Verantwortliche im Unternehmen und Mitigationsdienstleister sollten informiert werden, um schnellstmöglich auf die Geschehnisse reagieren zu können. Auch die vom Ausfall Betroffenen und die Öffentlichkeit sollte schnellstmöglich darüber in Kenntnis gesetzt werden. Deshalb ist es ratsam, die dafür nötigen Informationen aufzubereiten. Internet-Service-Provider (ISP) können nicht nur unterstützende Funktionen haben, sondern gegebenenfalls auch Klarheit darüber schaffen, ob Ihr Unternehmen Ziel des Angriffs ist oder nur zu den Kollateralschäden zählt. Bei größeren DDoS-Angriffen bittet das BSI darum, den Angriff auch anonymisiert zu melden, um die aktuelle IT-Bedrohungslage in Deutschland analysieren zu können [12], [20]. Das BSI empfiehlt zudem bei größeren DDoS-Angriffen Strafanzeige bei der Polizei zu erstatten [12].

Rechtliche Konsequenzen ziehen

Es sollte das eigene Justiziariat oder der zuständige Anwalt eingeschaltet werden und Strafanzeige bei der örtlichen Polizei gestellt werden [12].

Aus Geschehenem lernen

Aus dem Angriff lassen sich Erkenntnisse über Angreifer, Schwachpunkte und Mitigationsstrategien ziehen. Sie sollten in die bisherige Reaktionsstrategie mit eingebaut werden, um künftige Vorfälle besser zu unterbinden bzw. deren Auswirkungen abzuschwächen [20].

5.4.2.2 Technisch

Angriff feststellen

Wenn eine Ressource oder ein Service ausfällt, geschieht dies oftmals nicht durch böswilliges Einwirken Dritter. Jedoch sollte im Falle eines Angriffs dieser schnellstmöglich identifiziert werden. Über die Auslastung der Hardware und des Netzwerkes lässt sich kurzfristig eine erste Einordnung der Situation tätigen [20].

Protokollierung und Analyse des Netzwerkverkehrs

Über die Protokollierung und Analyse des Netzwerkverkehrs ist es nicht nur möglich, die angegriffenen Ziele sowie die dafür verwendete Methode zu bestimmen, sondern auch, Details über den Angreifer und dessen Abwehr zu erfahren. Diese Informationen sind zudem bei einer Meldung des Angriffs von entscheidender Bedeutung [12], [20].

Filterung von Netzwerkverkehrsdaten

Über die Anwendung von Filtern auf Quell- und Zieladressen der Angreifer sowie den Inhalt der eingehenden Netzwerkdaten ist es möglich, den Angriff abzuschwächen. So kann zwar nicht immer die angegriffene Ressource verfügbar gehalten werden, jedoch ist es dadurch möglich, die Chance auf Kollateralschäden zu vermindern [12].

Überwachung von Systemen, die nicht direkt von einem Angriff betroffen sind

Auch Systeme, welche bisher vom Angriff verschont geblieben sind, sollten genauer beobachtet werden. Dies kann nicht nur den Hinweis auf eine mögliche Infektion oder folgende Angriffswellen liefern. Angreifer haben in der Vergangenheit DDoS-Attacken genutzt, um Opfer von ihrem eigentlichen Ziel abzulenken [20].

5.5 Maßnahmen gegen Lieferkettenangriffe

Zu den wichtigsten und wirksamsten Maßnahmen gegen Supply-Chain-Angriffe zählen:

1. Analyse, Identifizierung und Management von Risiken in der Lieferkette
2. Schulung von Mitarbeitern im Umgang mit Supply-Chain-Angriffen
3. ganzheitliche Betrachtung und kontinuierliche Verbesserung der Cyberresilienz bezüglich der Lieferketten
4. Aufbau und Nutzung von Systemen für ein Schwachstellen- und Patch-Management für die gesamte Lieferkette

Um Angriffe auf die Lieferkette zu vermeiden oder die Schäden auf ein akzeptables Maß zu reduzieren, ist es notwendig, ein sogenannte Third-Party-Risks-Management (TRM) oder auch Cyber-Supply-Chain-Risk-Management (C-SCRM) einzuführen [35]. Dazu sollten zu Beginn alle Glieder der Kette (u.a. Lieferanten, Drittanbieter) ermittelt und dokumentiert werden. Anschließend sind die jeweiligen Risiken in Bezug auf die Auswirkungen auf die Geschäftskontinuität insbesondere bei Cyberangriffen nach festgelegten und einheitlichen Kriterien zu bewerten. Bei der Bestimmung von möglichen Bedrohungen sollten die aktuellen Trends berücksichtigt werden [33], [32]. Nach Vorhersagen durch das FS-ISAC werden zunehmende Angriffe durch staatliche Akteure vorhergesagt und es wird insgesamt von einer wachsenden Anzahl von Angriffen auf Lieferketten in der Zukunft ausgegangen

[33], [74], [75], [40]. In einzelnen Branchen wie der Finanzwirtschaft wird TRM bzw. C-SCRM direkt regulatorischen Anforderungen unterliegen [40].

Für die Umsetzung und Anwendung eines Risikomanagementsystems für Lieferkettenangriffe sind kompetente Mitarbeiter essenziell. Mit dem Thema sollten alle an der Lieferkette beteiligten Mitarbeiter frühzeitig durch Training und Sensibilisierungskampagnen vertraut gemacht werden, um Angriffe frühzeitig zu identifizieren [33]. Dabei ist insbesondere der Aspekt zu beachten, dass zwischen dem Bekanntwerden einer Schwachstelle und deren Schließung ein großer Zeitraum liegen kann, den Angreifer zu ihren Gunsten ausnutzen können [32].

Zur Verbesserung der Cyberresilienz gegenüber Lieferkettenangriffen sollten umfassende Maßnahmen bei Unternehmen und deren Zulieferern konsequent und fortlaufend umgesetzt werden. Dazu sollten alle Komponenten einer Infrastruktur für den Entwurf, die Entwicklung, die Herstellung und die Lieferung von Produkten angemessen und kontinuierlich gegen Eingriffe von Angriffen nach den gängigen Praktiken der Cybersicherheit abgesichert werden. Die Entwicklungsprozesse sollten so umgesetzt werden, dass Eingriffe schnell identifiziert werden können. Die Entwicklungs- und Produktionssysteme sollten in getrennte Netzwerksegmente unterteilt werden, um die Wege für Angreifer zu verlängern und zu erschweren. Die Zugänge für Dienstanbieter zum eigenen System sollten durch die Verwendung von verschlüsselter Kommunikation und einer MFA sehr streng reglementiert und limitiert sein [32]. Für weitere technische Maßnahmen kann auf Empfehlungen des BSI [7], der ENISA [32], [33] oder der CISA [16], [17], [15] zurückgegriffen werden.

Mit dem Aufbau und der kontinuierlichen Durchführung eines Schwachstellen-Managements für die Lieferkette sollten bewährte Methoden für die Überwachung und Bewertung von Schwachstellen angewendet werden. Dabei müssen insbesondere die Schwachstellen von verwendeten Komponenten von Drittanbietern berücksichtigt werden. Die Beseitigung von Schwachstellen sollte durch einen Prozess, der das Patch-Management umsetzt, etabliert werden. Dabei sollten u.a. eine Überprüfung und ein Testen von Patches durchgeführt werden, um sicherzustellen, dass die betrieblichen, sicherheitstechnischen, rechtlichen und Cybersicherheitsanforderungen erfüllt werden [32], [33]. Weitere Empfehlungen für die Umsetzung von geeigneten Maßnahmen für ein Schwachstellen- und Patch-Management können Empfehlungen von der ENISA [32], [33] entnommen werden.

5.6 Cybersicherheit als Investment

Das Erzielen einer angepassten bzw. angemessenen Cyberresilienz stellt heute eine große Herausforderung dar, um den kontinuierlichen Betrieb des Unternehmens zu sichern [13], [27], [75]. Gleichzeitig zeigen Untersuchungen, dass Kunden heute Cybersicherheit als Selbstverständlichkeit ansehen und nicht bereit sind dafür „extra“ zu bezahlen [28].

Vor dem Hintergrund der erheblichen Auswirkungen von Cyberangriffen und einer hohen kundenseitigen Erwartungshaltung bezüglich der Cybersicherheit besteht die Notwendigkeit einer risikobasierten, nachhaltigen und proaktiven Cyberstrategie [28]. Diese kann als Kombination aus guter Präventionsarbeit mit der Möglichkeit, auf Cyberattacken angemessen zu reagieren, angesehen werden. Proaktiv bedeutet in der Planung und Umsetzung nicht erst auf eine entsprechende Regulatorik zu warten [75]. Zukünftig werden hierbei in Umfang, Größe und Komplexität zentralisierte Ansätze nicht mehr erfolgreich sein, da Verantwortliche für die Cybersicherheit zunehmend in verschiedenen Teilen von Unternehmen eingesetzt werden sollten, um Entscheidungen mit Sicherheitsbezug zu dezentralisieren [35]. Dazu ist es essenziell, dass der notwendige „Freiraum“ (Ressourcen, Ideen, Zeit) durch die verantwortlichen Führungskräfte bereitgestellt wird, damit eine effektive Cyberstrategie und ein effektives Risikomanagement entwickelt werden können [75]. Daher ist es notwendig, in Programme zur Änderung des Sicherheitsverhaltens und der Sicherheitskultur für Führungskräfte im Bereich Sicherheit und Risikomanagement zu investieren, damit sich neue Denkweisen durchsetzen und neue Sicherheitsverhaltensweisen in Unternehmen umgesetzt und gelebt werden können [35].

Letztlich müssen die Verantwortlichen für den Cyberbereich Sicherheitsfragen so darstellen, dass die Führungskräfte sie verstehen und danach handeln können. Führungskräfte müssen ihrerseits mehr Verantwortung für operative Cyberanforderungen übernehmen, um die Cyberfähigkeiten ihres Unternehmens insgesamt zu verbessern [75]. Die Untersuchung von Deloitte listet auf, welche Fragen sich Führungskräfte in hochentwickelten Unternehmen beim Thema Cybersicherheit stellen, um die richtige Strategie oder die richtigen Maßnahmen daraus abzuleiten [28]:

- Verfügen wir über die richtige Technologie und das richtige Partner-Ökosystem – und wie können wir ein wachsendes, komplexes Netzwerk von Drittparteien steuern?
- Investieren wir auf die richtige Art und Weise und in die richtigen Bereiche – und verfügen wir über den richtigen Rahmen, um zu verstehen, wie und wo Cybersicherheitsmaßnahmen im gesamten Unternehmen einen Mehrwert schaffen?
- Verfügen wir über den richtigen Bewertungsrahmen, um zu verstehen, wie und wo Cybersicherheitsmaßnahmen im gesamten Unternehmen einen Mehrwert schaffen?

Die Umsetzung einer Cyberresilienz kann u.a. nur durch die Etablierung einer sicherheitsorientierten Kultur erreicht werden, bei der eine gemeinsame Sprache auf der Grundlage von Kennzahlen existiert, so dass Informationen über die Cybersicherheit in Messwerte übersetzt werden, die für Vorstandsmitglieder und das gesamte Unternehmen von Bedeutung sind [75]. Bei besonders erfolgreichen Unternehmen sind Cybersicherheit und deren Umsetzung unter Einbezug der Geschäftsführung oder des Vorstandes in die gesamte Organisation integriert [28].

Für den operationellen Betrieb von Unternehmen sind IT-Systeme unerlässlich und werden aus betriebswirtschaftlicher Betrachtung als Betriebskosten geführt. Für diese Kosten kann auf der Basis der zu erwartenden Umsätze bzw. Gewinne ein sogenannte Return on Investment (ROI) berechnet werden und als Rentabilitätskennzahl für die Entscheidungsfindung über Investitionen dienen. Bei der Berechnung einer Rentabilitätskennzahl für

die Kosten von Ausgaben für die Cybersicherheit lässt sich diese Betrachtung rein quantitativ nur schwer durchführen, da sich die positiven monetären Ergebnisse nur sehr schwer bestimmen lassen. Ebenfalls sorgen die Ausgaben nicht automatisch für Ergebnisse, die zu einer sofortigen und messbaren Amortisation beitragen.

Nach der Untersuchung des World Economic Forum werden die Kosten für IT-Sicherheit vom Großteil der Geschäftsführer und IT-Verantwortlichen als einer der Schlüsselfaktoren für das eigene Geschäft angesehen. Für eine Abwägung von geeigneten Maßnahmen im Bereich der IT-Sicherheit ist eine objektive Bewertung notwendig. Es wird insgesamt empfohlen, eine behutsame Risikobewertung vor der Einführung neuer IT-Technologien durchzuführen, um die Risiken durch mögliche Cyberattacken gegen den Nutzen abzuwägen [75]. Nach Angaben der ENISA sollte die Rentabilitätsberechnung für die IT-Sicherheitsausgaben auf Basis des sogenannte Return on Security Investment (ROSI) durchgeführt werden. Bei der Berechnung des ROSI wird bestimmt, wie viel potenzieller Verlust oder Schaden durch einen Sicherheitsvorfall mit einer Investition in IT-Sicherheit vermindert werden kann. Darüber hinaus können mit dieser Berechnungsmethode verschiedene Ausgaben für Cybersicherheit und deren Wirksamkeit verglichen werden [34].

Neben der quantitativen Betrachtung der Ausgaben für IT-Sicherheit zeigen verschiedene Untersuchungen indirekte und langfristige positive Effekte für Unternehmen, die sich beispielsweise nicht mittels ROSI abbilden lassen. Nach einer Untersuchung von Deloitte konnten durch umgesetzte Maßnahmen zur Erhöhung der Cyberresilienz positive Effekte u.a. bei der Markenreputation, Umsatzsteigerung, einer verbesserten betrieblichen Stabilität der Lieferkette, bei der Rekrutierung und Bindung von Talenten, der langfristigen Nachhaltigkeit und einem verbesserten Kundenvertrauen erzielt werden [28].

6 Gesetzliche Cybersicherheitsanforderungen der Zukunft

EU NETWORK INFORMATION SECURITY DIRECTIVE 2.0 2022/2555

ZIELGRUPPE: BETREIBER VON WESENTLICHEN UND WICHTIGEN EINRICHTUNGEN (KRITISCHE INFRASTRUKTUREN), DIE IN DER EU TÄTIG SIND.

2023

NIS 2
Seit 16. Jan. 2023 in Kraft. Bis 17. Okt. 2024 in nationales Recht; vorauss. durch IT-Sicherheitsgesetz 3.0 in Deutschland

CRA
(Datum noch nicht bekannt)

SEC 206(4)-9 UND RIN3235-AM89
Für April 2023 erwartet

DORA
Seit 16. Jan. 2023 in Kraft; geht bis 17. Jan. 2025 in nationales Recht über

ANFORDERUNGEN UND PFLICHTEN NIS 2 (MASSNAHMEN)

- Erstellen von IT-Sicherheitsregeln und -prozessen
- Notfallmanagement
- Angriffserkennung (IDS/IPS, SIEM, E/XDR, Logs)
- Sichere Beschaffung
- Regelmäßige Trainings (Hygiene)
- Verschlüsselung
- Identitäts- und Zugangsmanagement
- Schwachstellenmanagement, Penetrationstests
- Meldung innerhalb von 24 Std. an Behörde
- Zertifizierung

STRAFEN

DSGVO
Bis 20 Mio. Euro oder bis 4 % des globalen Umsatzes

NIS
Bis 10 Mio. Euro oder bis 2 % des globalen Umsatzes

ITSIG
2,0 bis 20 Mio. Euro

CRA
Bis 15 Mio. Euro oder bis 2,5 % des globalen Umsatzes

PCI DSS
5.000 – 100.000 Euro pro Monat

HISTORISCHE STRAFEN

746 Mio. EUR (DSGVO)

405 Mio. EUR (DSGVO)

225 Mio. EUR (DSGVO)

265 Mio. EUR (DSGVO)

35 Mio. EUR (DSGVO)

EU CYBER RESILIENCE ACT (2022/0272/COD)

ZIELGRUPPE: HERSTELLER, DISTRIBUTOREN, HÄNDLER VON SOFTWARE UND HARDWARE MIT „DIGITALEN ELEMENTEN“

ZIELE

Sicherheit
von Software und vernetzten Produkten erhöhen

Einheitliche Standards
zur Bewertung von Hardware- und Software-Produkten

Transparenz
über Sicherheit von Produkten erhöhen

Cyberresilienz
von Unternehmen und Gesellschaft erhöhen

ANFORDERUNGEN

1. Planung, Design, Entwicklung, Produktion und Lieferung erfolgt nach Security by Design und Datenschutz-Prinzipien
2. Software Bill of Materials (SBOM)
3. Stückliste für Software-Code
4. Dokumentation der Technik und Risikobewertung
5. Minimum 5 Jahre Support mit Software-Updates
6. Kontinuierliche Schwachstellenüberprüfung
7. Definierter Prozess für Schwachstellenbehebung und Meldestelle für Nutzer
8. Meldung von Schwachstellen und Vorfällen innerhalb von 24 Std. an Behörden

SEC 206(4)-9 UND RIN3235-AM89

- Regelmäßige Information zu Cybersecurity-Maßnahmen, Strategien
- Existenz eines Cybersicherheits-Programms
- Nutzung Dienstleister für Schwachstellen und Risikoanalyse
- Third Party Cyber Risk
- Maßnahmen zur Prävention, Erkennung, Minimierung und Wiederherstellung
- Benennung eines CISO
- Vorstand und Aufsichtsrat: Cybersecurity-Expertise und -Oversight
- Cybersicherheitsvorfälle innerhalb von 72 Std. melden
- Reporting aller bisherigen Vorfälle, die nicht an die Öffentlichkeit berichtet wurden

BIS 2030 WIRD ES 25 MILLIARDEN VERNETZTE PRODUKTE AUF DER WELT GEBEN.

Quelle: eigene Darstellung; offizielle Quellen von EU und SEC, www.csoonline.com

6 Gesetzliche Cybersicherheitsanforderungen der Zukunft

Network and Information Security 2[1] (NIS 2): EU-Richtlinie zur Steigerung des allgemeinen Cybersicherheitsniveaus

HINTERGRUND DER REGULATORIK

- Ungeachtet der Erfolge der im Jahr 2016 erlassenen EU-weiten Rechtsvorschrift zur Cybersicherheit (NIS-Richtlinie, vgl. IT-Sicherheitsgesetz 2.0 in Deutschland) ergeben sich inhärente Mängel, die ein wirksames Vorgehen gegen aktuelle und neue Herausforderungen zur Gewährleistung der Cybersicherheit verhindern.

- Essenzielle Sektoren mit wirtschaftlicher und gesellschaftlicher Bedeutung sind durch die NIS-Richtlinie nicht abgedeckt und ihr eingeräumter Ermessensspielraum führt in Teilen zu einer fehlgeleiteten Umsetzung seitens der EU-Mitgliedsstaaten in nationales Recht (u.a. uneinheitliche Einteilung von Sektoren und Auslegung beim Risikomanagement in unterschiedlichen Mitgliedsstaaten).

- NIS 2 behebt die inhärenten Mängel und löst die NIS-Richtlinie vollumfänglich ab.

GEGENSTAND DER REGULATORIK

Der gesetzliche Anwendungsbereich der NIS-2-Richtlinie erstreckt sich auf Dienste von Einrichtungen deren Verlust oder Unterbrechung direkte oder indirekte Auswirkungen hat und entscheidend für das wirtschaftliche und soziale Leben in der EU sind. NIS 2 erweitert den Geltungsbereich der NIS-Richtlinie eindeutig in nachfolgende Einrichtungen aus dem privaten und öffentlichen Bereich, die in der EU tätig sind:

- Wesentliche Einrichtungen
  - Energie (Elektrizität, Fernwärme und -kälte, Öl, Gas, Wasserstoff)
  - Verkehr (Luft-, Schienen-, Schifffahrts- und Straßenverkehr)
  - Bankenwesen und Finanzmarktinfrastrukturen
  - Gesundheitswesen
  - Trink- und Abwasserversorgung
  - Digitale Infrastruktur (u.a. Anbieter von Internet-Austauschpunkten, DNS-Diensteanbieter, Anbieter von Cloud-Computing-Diensten)
  - Verwaltung von Informations- und Kommunikationstechnologien (IKT)
  - Öffentliche Verwaltung
  - Weltraum (Bodeninfrastruktur)

- Wichtige Einrichtungen
  - Post- und Kurierdienste
  - Abfallbewirtschaftung
  - Herstellung, Produktion und Vertrieb von chemischen Stoffen
  - Herstellung, Verarbeitung und Vertrieb von Lebensmitteln
  - Verarbeitendes Gewerbe und Herstellung von Waren (u.a. medizinische Geräte, Elektrogeräte, Computer, Kraftfahrzeuge, Anhänger und Sattelanhänger)
  - Anbieter digitaler Dienste (u.a. Online-Marktplätze, Online-Suchmaschinen, soziale Netzwerke)
  - Forschungseinrichtungen

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&from=EN

ZIELSETZUNG DER REGULATORIK

- Angesichts des schnellen digitalen Wandels und der fortschreitenden Vernetzung sind inhaltliche Vertiefungen und Ergänzungen der Anforderungen an die Cybersicherheit notwendig. Nur durch diese angepassten Vorschriften lässt sich ein angemessenes Schutzniveau für Netz- und Informationssysteme bezüglich aktueller und zukünftiger Cyberbedrohungen erreichen.

- Eine Ausweitung der strengeren Anforderungen auf weitere Sektoren ist zwingend erforderlich, um flächendeckend kritische Bereiche in der EU vor Cyberangriffen und etwaigen Sicherheitsvorfällen zu schützen.

ZEITLICHER RAHMEN

- Vorlage des Entwurfs: 16. Dezember 2020

- Inkrafttreten: 16. Januar 2023

- Umsetzung durch EU-Mitgliedsstaaten: 17. Oktober 2024 (voraussichtlich durch IT-Sicherheitsgesetz 3.0 in Deutschland)

ADRESSATEN

Betreiber von wesentlichen und wichtigen Einrichtungen, die in der EU tätig sind. Kleinst- und Kleinunternehmen (unter 50 Beschäftigte und unter 10 Millionen Euro Umsatz), welche auch zu diesen Einrichtungen zählen, sind von der NIS-2-Richtlinie ausgeschlossen.

ANFORDERUNGEN AN ADRESSATEN

- **einheitliches und erweitertes Risikomanagement**
  Einrichtungen, die als wesentlich oder wichtig eingestuft werden, müssen einen gefährdungsübergreifenden Ansatz mit einem vorgegebenen Mindestumfang zur Minimierung der Risiken wählen. Dies ist eine essenzielle Änderung, denn in der NIS-Richtlinie wurden die Regeln von den nationalen Behörden festgelegt, was zu erheblichen Unterschieden zwischen den Ländern und zu Komplikationen für Einrichtungen führte, die in mehreren Mitgliedstaaten tätig sind. Die wichtigsten Mindestanforderungen sind dabei ein Sicherheitskonzept, eine Risikoanalyse sowie eine Bewertung auf Wirksamkeit eingeleiteter Risikomaßnahmen für die Cybersicherheit. In diesem Zusammenhang gilt es, auch das Risiko, welches von unmittelbaren Anbietern oder Diensteanbietern in der Lieferkette ausgeht, miteinzuschließen. Zudem müssen Maßnahmen ergriffen werden, die im Falle eines Sicherheitsvorfalls den Betrieb aufrechterhalten, wie ein angemessenes Backup-Management, Strategien zur Wiederherstellung und ein Krisenmanagement. Letzteres ist enorm wichtig, um neuen Meldepflichten zu genügen.

- **Verschärfung der Meldepflicht**
  Bei einem Sicherheitsvorfall besteht Meldepflicht gegenüber dem zuständigen nationalen Computer-Security-Incident-Response-Team (CSIRT), welches durch den jeweiligen EU-Mitgliedsstaat zu etablieren ist. Bei erheblichen Vorfällen, die Auswirkungen auf die weitere Bereitstellung des Dienstes haben, ist die zuständige Behörde direkt zu informieren. Zusätzlich unterliegt die Meldepflicht einem mehrstufigen Prozess: (i) Frühwarnung (innerhalb von 24 Stunden), (ii) Meldung (innerhalb von 72 Stunden) und (iii) Abschlussbericht (nach einem Monat).

- **Verpflichtung zur Zertifizierung**
  Darüber hinaus können einige wichtige und wesentliche Einrichtungen verpflichtet werden, IKT-Produkte, -Dienstleistungen und -Verfahren für bestimmte Tätigkeiten zu zertifizieren.

ESSENZIELLE IMPLIKATIONEN DURCH ANFORDERUNGEN

Angesichts der Ausweitung des Geltungsbereichs durch NIS 2 wird eine rasche Umsetzung der Richtlinie zu einer Herausforderung. Viele Einrichtungen sind nicht in der Lage ,die geforderten Maßnahmen zeitnah umzusetzen, obwohl sie in den Geltungsbereich der NIS-2-Richtlinie fallen.

SANKTIONEN

Verstoßen Adressaten gegen die Pflichten der NIS-2-Richtlinie, drohen Bußgelder, die in Abhängigkeit von der Klassifikation der Einrichtung verhängt werden können:

- Für wesentliche Einrichtungen können Strafen in Höhe von mindesten 10 Millionen Euro oder zwei Prozent des gesamten weltweiten Jahresumsatzes aus dem vorangegangenen Geschäftsjahr ausgesprochen werden – je nachdem, welcher Betrag der höhere ist.

- Für wichtige Einrichtungen können Strafen in Höhe von mindesten 7 Millionen Euro oder 1,4 Prozent des gesamten weltweiten Jahresumsatzes aus dem vorangegangenen Geschäftsjahr ausgesprochen werden – je nachdem, welcher Betrag der höhere ist.

Cyber Resilienz Act[1] (CRA): EU-Gesetzesentwurf über Cyberresilienz von Produkten mit digitalen Elementen

HINTERGRUND DER REGULATORIK

- Eng verknüpft mit immer neuer Technologie und der Platzierung dieser in neuen Produkten ist das zunehmende Risiko, Opfer von Cyberattacken zu werden, welche offene Sicherheitslücken in den Produkten ausnutzen.

- Auftretende Sicherheitsvorfälle, ausgelöst durch solche unsicheren Produkte, können aufgrund ihrer Vernetzung Organisationen oder ganze Lieferketten beeinträchtigen. Ferner können sie sich rasant auf dem Binnenmarkt und darüber hinaus ausweiten, was zu schwerwiegenden wirtschaftlichen und sozialen Störungen in der EU führen kann.

- Für die meisten Produkte, welche auf dem EU-Binnenmarkt in Verkehr gebracht werden, gibt es derzeit keine Rechtsvorschriften, die explizit auf deren Cybersicherheit abzielen.

GEGENSTAND DER REGULATORIK

- Hardware- und Software-Produkte mit digitalen Elementen. Damit sind all solche Produkte und deren Datenfernverarbeitungslösungen, einschließlich Software- oder Hardware-Komponenten, gemeint, die getrennt in Verkehr gebracht werden sollen.

- Konkrete Beispiele für Hardware- und Software-Produkte mit digitalen Elementen sind u.a.:
  - Fitnesstracker, intelligente Lautsprecher mit ausgelagerter Analysefunktionalität (Cloud, Web-Applikationen)
  - Foto- und Textverarbeitung
  - Passwortmanager
  - Systeme für Absicherung und Netzwerkmanagement (u.a. Router, Firewalls, Angriffserkennungssysteme)
  - Software für Fernzugriff
  - Mikrocontroller und Central Processing Units (CPUs)
  - Hypervisoren und Container-Runtime-Systeme
  - Chipkarten bzw. -leser

[1] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

ZIELSETZUNG DER REGULATORIK

- **Security by Design und darüber hinaus**
  Sicherstellung, dass in der EU in Verkehr gebrachte Produkte mit digitalen Elementen eine minimale Angriffsfläche für cyberkriminelle Akteure darstellen und dass Hersteller über den gesamten Lebenszyklus (Planungs-, Entwurfs-, Entwicklungs-, Produktions-, Liefer- und Wartungsphase) für die Cybersicherheit ihrer Produkte verantwortlich bleiben. Dadurch wird das Sicherheitsniveau für Produkte mit digitalen Elementen insgesamt auf eine neue Ebene angehoben.

- **Transparenz für Nutzer**
  Es wird Transparenz für gewerbliche Anwender und Verbraucher geschaffen, da oft ein unzureichendes Verständnis von Schwachstellen und der Zugang zu Informationen fehlt, um Produkte mit angemessenen Cybersicherheitsvorkehrungen auszuwählen und sicher verwenden zu können.

ZEITLICHER RAHMEN

- Vorlage des Entwurfs: 15. September 2022
- Inkrafttreten: noch nicht bekannt
- Umsetzung durch EU-Mitgliedsstaaten: noch nicht bekannt, aber spätestens 24 Monate nach dem Inkrafttreten (Meldepflicht besteht bereits nach zwölf Monaten)

ADRESSATEN

Die Regulatorik gilt vornehmlich für Hersteller, aber auch Importeure und Distributoren von Hardware- und Software-Produkten mit digitalen Elementen mit der Absicht, sie auf dem EU-Binnenmarkt in Verkehr zu bringen.

ANFORDERUNGEN AN ADRESSATEN

1. **Security by Design**
   Hersteller müssen geeignete Maßnahmen bereits während der Planungsphase ergreifen, die die Auslieferung eines sicheren Produkts mit digitalen Elementen gewährleisten. So müssen u.a. geeignete Kontrollmechanismen etabliert werden, die vor unbefugten Zugriffen schützen. Bei der Verarbeitung von Daten ist darauf zu achten, dass Verschlüsselungsmechanismen eingesetzt werden und nur die Daten, die für das Funktionieren des Produkts unbedingt erforderlich sind, ausgetauscht werden (vgl. Minimalprinzip). Auch ist bei der Auslieferung eine sichere Konfiguration als Standard-Einstellung vorzusehen, die via Reset-Funktionalität jederzeit wieder erreicht werden kann. Produkte mit Schwachstellen dürfen gar nicht in Verkehr gebracht werden. Hierfür bedarf es einer Bewertung der Cybersicherheitsrisiken, welche bereits sehr früh in die Produktentwicklung einfließen muss.

2. **Bewertung der Cybersicherheitsrisiken**
   Produkte mit digitalen Elementen werden so konzipiert, entwickelt und hergestellt, dass sie entsprechend ihren Risiken ein angemessenes Cybersicherheitsniveau gewährleisten. Hierzu bedarf es einer Inventarisierung aller Cybersicherheitsrisiken und deren Bewertung. Im Rahmen dieses kontinuierlichen Prozesses muss auch eine sogenannte Software Bill of Material (SBOM) erstellt werden, welche alle Abhängigkeiten von anderen Bibliotheken, Anwendungen und Diensten offenlegt. Auf dieser Basis können Analysen über Schwachstellen systematisch durch den Hersteller erfolgen. Zudem gibt die SBOM Aufschluss über die gesamte Lieferkette und deren Risiken in Bezug auf das Produkt.

3. **Meldepflicht für aktiv ausgenutzte Schwachstellen und Vorfälle**
   Hersteller müssen binnen 24 Stunden erkannte Sicherheitslücken oder Vorfälle der zuständigen Behörde melden. Bei Sicherheitsvorfällen müssen auch die Nutzer der Produkte informiert werden und über mögliche Mitigationsstrategien unterrichtet werden. Wird eine Sicherheitslücke außerhalb des Handlungsbereichs des Herstellers bekannt, so muss diese dem jeweiligen Lieferanten oder Drittanbieter in der Lieferkette gemeldet werden.

4. **Bereitstellung von Sicherheitsupdates**
   Nach Inverkehrbringung müssen Maßnahmen ergriffen werden, um etwaige Schwachstellen für die erwartete Produktlebensdauer oder fünf Jahre (je nachdem, welcher Zeitraum kürzer ist) zu beheben. Dies schließt auch proaktive Tests und Überprüfungen des Produkts mit ein.

5. **Gebrauchsanweisung und technische Dokumentation**
   Bevor ein Produkt mit digitalen Elementen in Verkehr gebracht wird, stellt der Hersteller sicher eine Gebrauchsanweisung und eine technische Dokumentation anzufertigen, welche zur Verfügung gestellt wird. Die Gebrauchsanweisung enthält dabei für Nutzer verständliche Hinweise zur sicheren Nutzung während des gesamten Lebenszyklus des Produkts. Die technische Dokumentation beinhaltet eine umfassende Beschreibung sowie Details zur Konzeption, Entwicklung und Herstellung des Produkts und zu festgelegten Verfahren zur Behandlung von Schwachstellen. Darunter fällt ebenfalls die SBOM und die Bewertung der Cybersicherheitsrisiken.

6. **Konformitätsbewertung**
   Hersteller müssen grundsätzlich darlegen, dass ihre Produkte die auferlegten Anforderungen vor der Inverkehrbringung erfüllen. Für Produkte mit erhöhtem Risiko (u.a. Betriebssysteme, industrielle Firewalls, CPUs) findet die Bewertung auf Konformität durch eine unabhängige dritte Instanz statt.

ESSENZIELLE IMPLIKATIONEN DURCH ANFORDERUNGEN

- **frühzeitiger Handlungsbedarf, um EU-Konformität zu erreichen**
  Auch wenn noch nicht bekannt ist, wann der Gesetzentwurf in Kraft tritt, müssen insbesondere Hersteller von Produkten mit digitalen Inhalten aufgrund teilweise langer Entwicklungszyklen sich bereits jetzt mit den Anforderungen des CRA auseinandersetzen.

- **erhebliche Aufwände durch Neugestaltung etablierter Prozesse**
  Aufgrund der neuen Anforderungen an Hersteller, Importeure und Distributoren von Hardware- und Software-Produkten mit digitalen Elementen ist mit erheblichen Mehraufwänden zu rechnen. Nicht nur müssen bestehende Prozesse nach den Prinzipien der Security by Design neu ausgerichtet werden und die gesamte Lieferkette für die Risikobewertung in Betracht gezogen werden. Ebenfalls muss die sehr strenge Meldepflicht und ein angemessenes Schwachstellen- bzw. Patch-Management etabliert werden und mit Lieferanten und Drittanbietern koordiniert sein.

SANKTIONEN

Verstoßen Adressaten gegen die Pflichten des CRA, drohen Bußgelder. Die nationalen Behörden sind befugt, Geldbußen bis zu 15 Millionen Euro oder 2,5 Prozent des gesamten weltweiten Jahresumsatzes aus dem vorangegangenen Geschäftsjahr zu verhängen – je nachdem, welcher Betrag höher ist.

DORA[1]

HINTERGRUND DER REGULATORIK

Der EU-Finanzsektor ist seit vielen Jahren durch einen einheitlichen Rechtsrahmen reguliert. Jedoch umfasst dieser kaum Regelungen zu den operativen Risiken im Zusammenhang mit Informations- und Kommunikationstechnologien (IKT). Durch die zunehmende Abhängigkeit von Finanzunternehmen und IKT-Drittanbietern wachsen die Risiken für die Betriebsstabilität und Leistungsfähigkeit insbesondere vor dem Hintergrund drohender Cyberattacken oder sonstiger IKT-Störungen. Mit dem Digital Operational Resilience Act (DORA), welcher am 16. Januar 2023 in Kraft getreten ist, erlässt die EU neue Vorschriften zur Stärkung der IKT-Sicherheit im Finanzwesen und schließt damit offene Flanken im bisherigen Rechtsrahmen. Die EU-Mitgliedsstaaten müssen diese Richtlinie bis zum 17. Januar 2025 in nationales Recht umsetzen.

ADRESSATEN

Unter DORA fallen nahezu alle Finanzunternehmen in den Mitgliedsstaaten der EU wie Kredit- und Zahlungsinstitute, E-Geld-Institute, Wertpapierhändler, Anbieter von Krypto-Dienstleistungen, Verwaltungsgesellschaften, Handelsplätze, Versicherungsunternehmen und -vermittler, Ratingagenturen oder Wirtschaftsprüfungsgesellschaften. Darüber hinaus sind ebenso IKT-Drittdienstleister wie digitale Dienste und Datendienste, Cloud- und Software-Anbieter, Datenanalysedienste oder Rechenzentren betroffen.

ANFORDERUNGEN AN ADRESSATEN

Die Anforderungen an die Adressaten der Regulierung lassen sich in die folgenden vier obligatorischen Kernthemenbereiche einteilen: (i) IKT-Risikomanagement, (ii) Meldung von IKT-bezogenen Vorfällen, (iii) Prüfung der digitalen Betriebsstabilität, (iv) Steuerung des Risikos durch IKT-Drittanbieter. Allerdings ist zu erwähnen, dass DORA Pflichten aus bereits bestehenden Vorschriften miteinbezieht (u.a. MaRisk/BAIT, MaGo/VAIT oder KaMaRisk/KAIT). Essenzielle Abweichungen oder Ergänzungen können pro Kernthemenbereich zusammengefasst werden. In Bezug auf (i) erweitern sich die Pflichten für das Management hinsichtlich Genehmigungs-, Überwachungs- und Überprüfungshandlungen. Dies schließt auch regelmäßige Schulungen zu IKT-Risiken ein. IKT-Systeme müssen zudem zum Schutz kontinuierlich überwacht und Reaktions- und Wiederherstellungsmaßnahmen erarbeitet werden. Zu (ii) besteht eine Meldepflicht inklusive eines Frühwarnsystems für alle IKT-bezogenen Vorfälle. Nach Erkennen eines Vorfalls besteht eine detaillierte Aufzeichnungspflicht. Für schwere Vorfälle müssen vorlagenbasierte Berichte an zuständige Behörden, Dienstnutzer und Kunden übermittelt werden. Hinsichtlich (iii) stellt ein umfassendes Programm die Prüfung der digitalen Betriebsstabilität sicher, welche IKT-Instrumente, -Systeme und -Prozesse gleichermaßen abdeckt. Im Turnus von drei Jahren müssen darüber hinaus erweiterte bedrohungsorientierte Penetrationstests durchführen werden. Bezüglich (iv) muss ein Register von IKT-Drittdienstleistern erstellt werden. Ebenso muss eine Risikoanalyse für die Inanspruchnahme von IKT-Drittdienstleistern erfolgen. Insbesondere gilt dies auch für unterbeauftragte Anbieter.

SANKTIONEN

Bei Verstößen kann die federführende Aufsichtsbehörde Geldstrafen von bis zu einem Prozent des durchschnittlichen weltweiten Tagesumsatzes aussprechen.

[1] https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/738197/EPRS_ATA(2022)738197_DE.pdf

SEC CYBERSECURITY RULE 206(4)-9[1]

HINTERGRUND DER REGULATORIK

Im Kontext der steigenden Bedrohungslage von Cyberangriffen veröffentlichte die US-Börsenaufsichtsbehörde Securities and Exchange Commission (SEC) am 9. Februar 2022 den neuen Regelwerksentwurf: SEC Cybersecurity Rule 206(4)-9. Mit diesem Entwurf soll ein umfassender regulatorischer Rahmen aufgespannt werden, der Cybersicherheitsrisiken für den Finanzsektor eindämmt. In diesem Zusammenhang soll das Vertrauen der Anleger in die operative Widerstandsfähigkeit von Anlageberatern und -fonds sowie die Sicherheit ihrer Anlagen gestärkt werden. So sollen Dienstleister befähigt werden auf Sicherheitsvorfälle angemessen und wirksam zu reagieren. Gleichzeitig sollen Auswirkungen minimiert werden, so dass sich Dienstleister schnell von einem Vorfall erholen können. Zum aktuellen Zeitpunkt ist noch ungewiss, wann das Regelwerk in Kraft treten soll.

ADRESSATEN

SEC Cybersecurity Rule 206(4)-9 richtet sich an Anlageberater und Investmentgesellschaften, welche bei der SEC registriert sind. Auch werden sogenannte Closed-End-Unternehmen von dem Rechtsrahmen erfasst, die sich dafür entschieden haben, nach dem Investment Company Act als Business Development Company behandelt zu werden.

ANFORDERUNGEN AN ADRESSATEN

In seiner aktuellen Form sieht SEC Cybersecurity Rule 206(4)-9 sehr weitreichende und detailreiche Anforderungen vor, die beispiellos für den Finanzsektor sind. Im Wesentlichen lassen sie sich auf drei Kernthemenbereiche reduzieren: (i) Richtlinien und Verfahren zum Cybersicherheitsrisikomanagement, (ii) Berichterstattung für erhebliche Sicherheitsvorfälle und (iii) Offenlegung von Cyberrisiken und Vorfällen. Zu (i) müssen registrierte Anlageberater und Investmentgesellschaften u.a. eine Bestandsaufnahme für Informationssysteme und etwaige Datenflüsse durchführen. Auf dieser Basis gibt eine Risikoanalyse Aufschluss über die aktuelle Bedrohungslage. Risikobewertungen müssen schriftlich erfolgen. In Bezug auf (ii) müssen erhebliche Sicherheitsvorfälle innerhalb von 48 Stunden an die SEC gemeldet werden. Die zu meldenden Informationen sind sehr umfangreich und erstrecken sich ebenfalls auf betroffene Investmentgesellschaften. Letztlich mit (iii) müssen gegenüber Anlegern und anderen Marktteilnehmern Cybersicherheitsrisiken unabhängig davon, ob das Unternehmen von diesen bereits betroffen war, offengelegt werden. Auch müssen alle konkreten Sicherheitsvorfälle der letzten zwei Geschäftsjahre, die zu einer Schädigung des Unternehmens oder seiner Kunden geführt hat, veröffentlicht werden.

SANKTIONEN

Geldbußen bzw. Sanktionen gegen Verstöße von SEC Cybersecurity Rule 206(4)-9 konnten bei den Recherchearbeiten nicht ermittelt werden.

[1] https://www.sec.gov/rules/proposed/2022/33-11028.pdf

SEC RIN3235 AM89[1]

HINTERGRUND DER REGULATORIK

Im Fokus stehen börsennotierte Unternehmen, die bereits der Meldepflicht des Securities Exchange Act von 1934 unterliegen. Grund für den Regelungsentwurf ist, dass Cybersicherheitsvorfälle ein zunehmendes Risiko für alle gesellschaftlichen Bereiche darstellen und es kaum Transparenz über den Zustand der Cybersicherheit in den börsennotierten Unternehmen gibt. Angriffe können nicht nur schwerwiegende Auswirkungen auf einzelne Unternehmen haben, sondern auch auf die gesamte Wirtschaft (Stichwort Lieferketten), die kritische Infrastruktur und in besonders schweren Fällen auch auf die nationale Sicherheit.

Ziel der angestrebten Vorschriften ist die Etablierung eines einheitlichen Berichtswesens über die Cybersicherheitssituation der Unternehmen sowie auch Erhöhung des Cybersicherheitswissens bei C-Level und Aufsichtsrat.

ADRESSATEN

Der SEC RIN3235 AM89 Entwurf richtet sich an alle Unternehmen, die dem Securities Exchange Act von 1934 unterliegen. Dabei handelt es sich um börsennotierte Unternehmen mit Sitz in den Vereinigten Staaten. Jedoch wird momentan ermittelt, ob kleinere Unternehmen von dieser Regelung ausgenommen werden sollten oder für sie Sonderregeln gelten.

ANFORDERUNGEN AN ADRESSATEN

Jegliche Cybersicherheitsvorfälle müssen innerhalb von vier Werktagen gemeldet werden. Darüber hinaus verpflichten sich Unternehmen, kontinuierlich über die Auswirkungen und Maßnahmen nach Cyberangriffen zu berichten.

Außerdem werden Angaben zur allgemeinen Cyber-Strategie und dem Risikomanagement von Unternehmen verlangt – insbesondere Angaben dazu, wie mit Cybersicherheitsrisiken umgegangen wird, welche Rolle die Geschäftsleitung spielt und welche Vorstandsmitglieder oder Aufsichtsräte Cybersecurity-Fachkenntnisse besitzen.

Alle Angaben und Meldungen müssen in der Inline Extensible Business Reporting Language (Inline XBRL) dargestellt werden.

SANKTIONEN

Im Entwurf sind derzeit keine konkreten Sanktionen definiert für den Fall, dass Unternehmen der Meldepflicht nicht nachkommen.

[1] https://www.sec.gov/rules/proposed/2022/33-11038.pdf

Anhang

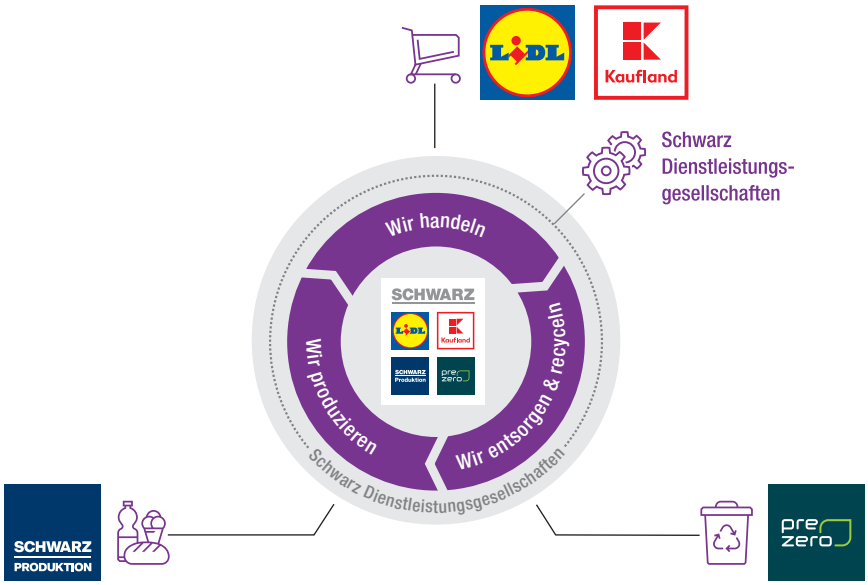
Unternehmen der Schwarz Gruppe im Überblick

575	13.700	32	6,8	154,1
Tausend Beschäftigte weltweit	**Filialen**	**Ländern aktiv**	**Milliarden Filialkunden bei Lidl und Kaufland**	**Milliarden Euro Jahresumsatz[1] im Geschäftsjahr 2022**

Unternehmen der Schwarz Gruppe im Porträt

Mit über 575.000 Mitarbeitern in 32 Ländern ist die Schwarz Gruppe eine der weltweit führenden Handelsgruppen. Beheimatet im baden-württembergischen Neckarsulm, bilden die beiden Handelssparten Lidl und Kaufland die Säulen im Lebensmitteleinzelhandel. Darüber hinaus ist die Schwarz Produktion in der Lebensmittelherstellung und PreZero im Bereich der Umweltdienstleistungen aktiv. Damit deckt die Schwarz Gruppe als eine der wenigen Handelsgruppen den ganzen Wertschöpfungskreis ab – von der Produktion über den Handel bis hin zu Entsorgung und Recycling. Unterstützung erfahren sämtliche Gesellschaften der Schwarz Gruppe durch verschiedene Dienstleistungsgesellschaften im In- und Ausland. Neben der Erbringung von Verwaltungsdienstleistungen fallen hierunter zum Beispiel auch die Beschaffung von Nichthandelsware oder der Betrieb des Fuhrparks.

[1] Nettoumsatz im Geschäftsjahr 2022 (beinhaltet sämtliche handelsrechtlichen Umsätze inkl. sonstiger Erlöse).



Vielfalt ist unsere Stärke

Sparten

Handel (Lidl/Kaufland)

Die Landesgesellschaften der Lidl Gruppe betreiben den Lebensmitteleinzelhandel im Discountbereich. Der Frische-Discounter beschäftigt insgesamt rund 380.000 Mitarbeiter und betreibt in derzeit 31 Ländern rund 12.200 Filialen und über 200 Warenverteil- und Logistikzentren. Zudem ist Lidl in Asien mit Mitarbeitern vertreten. Das Sortiment von Lidl umfasst durchschnittlich 3.600 Artikel. Im Geschäftsjahr 2022 erzielte Lidl einen Umsatz von 114,8 Milliarden Euro.

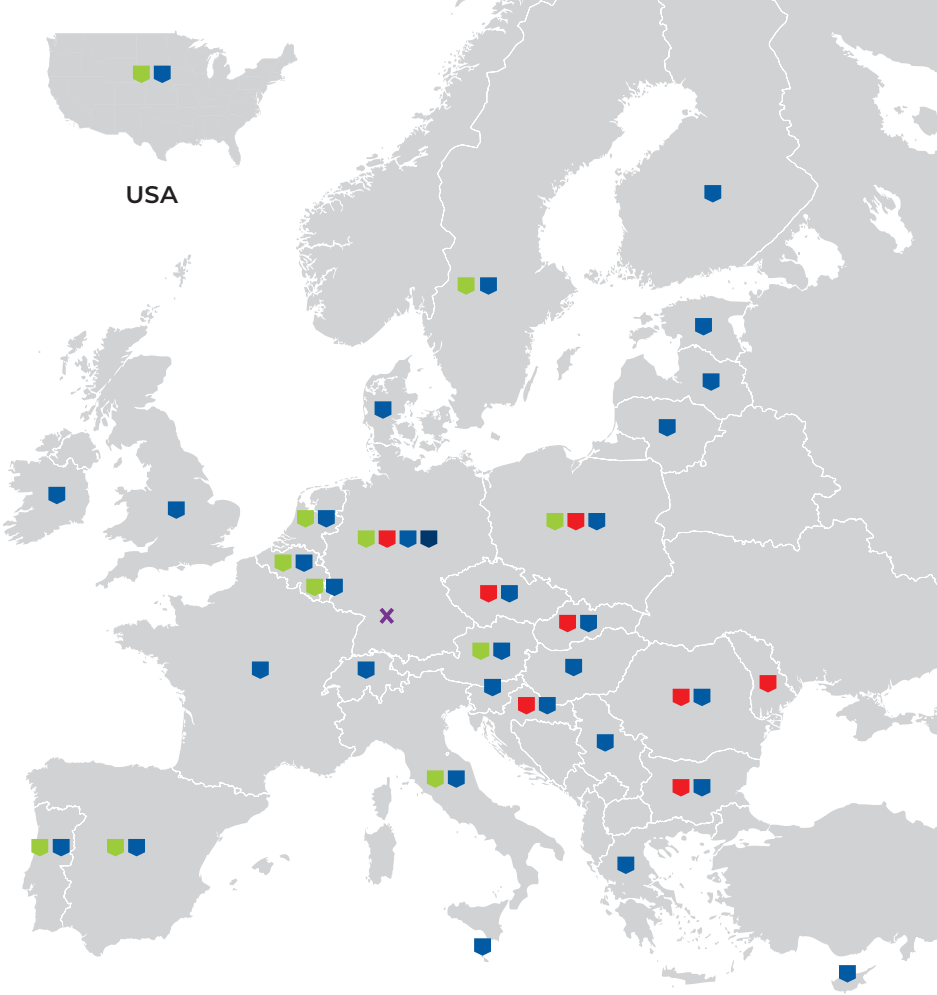
Die Landesgesellschaften der Kaufland Gruppe betreiben den Lebensmitteleinzelhandel auf der Großfläche – mit rund 1.500 Märkten sowie über 150.000 Beschäftigten in acht europäischen Ländern. Mit durchschnittlich 30.000 Artikeln in Deutschland und 17.000 in den anderen Ländern bietet das Unternehmen ein umfangreiches Sortiment an Lebensmitteln und Waren für den täglichen Bedarf. Daneben betreibt Kaufland fünf Fleischwerke, die Fleisch- und Wurstwaren für die Filialen produzieren. Im Geschäftsjahr 2022 erzielte Kaufland einen Umsatz von 31,8 Milliarden Euro.

Auf dem Weg nach morgen – Verantwortung übernehmen

Verantwortlich zu handeln ist Lidls Weg, das Qualitätsversprechen jeden Tag aufs Neue zu erfüllen und sich damit für die Zukunft sicher aufzustellen. Dieses Verständnis setzt Lidl im Rahmen von sechs strategischen Fokusthemen in die Praxis um: „Klima schützen“, „Ressourcen schonen“, „Biodiversität achten“, „Fair handeln“, „Gesundheit fördern“ und „Dialog führen“.

Machen macht den Unterschied

Der Vollsortimenter Kaufland achtet auf eine nachhaltige Gestaltung des Sortiments und setzt sich für verantwortungsvolle Produktionsbedingungen sowie eine artgerechte Haltung von Tieren ein. Zudem trägt Kaufland zu einem umfassenden Umwelt-, Klima- und Artenschutz bei.



- Lidl
- Kaufland
- PreZero
- Schwarz Produktion

Stand: Juni 2022

Standorte der Unternehmen der Schwarz Gruppe weltweit

Recycling (PreZero)

Die PreZero Gruppe ist ein international tätiger Umweltdienstleister in Europa und Nordamerika. An mehr als 475 Standorten übernimmt PreZero mit über 30.000 Beschäftigten und 66 Sortier- und Recyclinganlagen die Entsorgung von Abfällen sowie die Sortierung, Aufbereitung und das Recycling von rund 15 Millionen Tonnen Wertstoffen pro Jahr. Ergänzt wird das Portfolio um das Wertstoff- und Umweltmanagement innerhalb der Unternehmen der Schwarz Gruppe von der Marke GreenCycle sowie nachhaltige Faser- und Papierprodukte von OutNature und digitale Palettenlösungen von PreTurn. Im Geschäftsjahr 2022 erzielte PreZero einen Umsatz von 3,9 Milliarden Euro.

Rund

15

Millionen Tonnen Wertstoffe pro Jahr werden entsorgt und recycelt.

Neues Denken für ein sauberes Morgen

PreZero setzt sich für eine saubere Zukunft ein, in der ein effizienter und vollständig geschlossener Wertstoffkreislauf unsere Umwelt schützt und nachhaltig Werte schafft. Der eigene Anspruch lautet: Wir wollen Ressourcen schonen und die Menge des Abfalls, der nicht wiederverwertet werden kann, gegen null reduzieren.

Produktion (Schwarz Produktion)

Die Unternehmen der Schwarz Produktion stellen mit ihren rund 5.500 Beschäftigten an 20 Produktions-, Verwaltungs- und Dienstleistungsstandorten deutschlandweit hochwertige Lebensmittel sowie nachhaltige Verpackungen und Materialien für die Handelsunternehmen Lidl und Kaufland her. An insgesamt 12 Standorten werden Getränke, Schokolade, Eis, Backwaren, Nüsse und Trockenfrüchte, Kaffee, Teigwaren und Papier produziert. An drei weiteren Standorten betreibt die Schwarz Produktion Kunststoff- und Recyclingwerke. Diese sind dabei zentraler Bestandteil eines einzigartigen und nachhaltigen PET-Wertstoffkreislaufes.

Heute liefern und an morgen denken

Die Unternehmen der Schwarz Produktion engagieren sich aus der Überzeugung heraus, dass nachhaltiges Wirtschaften und Unternehmenserfolg Hand in Hand gehen. Um ihrer Verantwortung gerecht zu werden, haben die Unternehmen der Schwarz Produktion Nachhaltigkeit als einen ihrer sieben Unternehmenswerte definiert und damit fest in ihrer Unternehmensphilosophie verankert.

Unsere Dienstleister für die Sparten

Unterstützung erfahren sämtliche Unternehmensbereiche der Gruppe durch die Schwarz Dienstleistungsgesellschaften mit administrativen (Controlling, Finanzen, Personal usw.) und operativen (Beschaffung, Immobilien, IT usw.) Services. So bündeln wir unsere Kräfte, nutzen Synergiepotenziale und agieren effizient und nachhaltig.

Mit Vielfalt global Verantwortung leben

Als internationale Unternehmensgruppe haben die Unternehmen der Schwarz Gruppe an vielen Stellen Einfluss auf Gesellschaft und Umwelt. Kaum eine Unternehmensgruppe ist so vielfältig und deckt den gesamten Kreislauf ab. Die damit einhergehende Verantwortung nehmen die Unternehmen der Schwarz Gruppe sehr ernst und orientieren ihr Handeln an einer gemeinsam erarbeiteten Nachhaltigkeitsvision, fußend auf den vier Fokusthemen Menschen, Produktqualität, Kreislaufsysteme und Ökosysteme.

Digitalisierung

Die Digitalisierung ist ein entscheidender Erfolgsfaktor für die Unternehmen der Schwarz Gruppe. Ein wichtiger Teil davon ist die umfangreiche Omnichannel-Strategie: Die Handelssparten Lidl und Kaufland verknüpfen das stationäre Geschäft optimal mit der Onlinewelt. Wichtige Bausteine dafür sind der Lidl-Onlineshop, der Kaufland-Online-Marktplatz und die Loyalty-Programme Lidl Plus und K-Card. Auf dem Online-Marktplatz von Kaufland bieten mehr als 10.000 Händler über 45 Millionen Produkte an. Lidl Onlineshops sind bereits in sieben Ländern verfügbar – in Belgien, Deutschland, den Niederlanden, Polen, der Slowakei, Spanien und Tschechien. Damit verlängern die Handelssparten der Schwarz Gruppe das Regal des stationären Geschäfts um ein Vielfaches und schaffen zukunftsträchtige Synergien zwischen stationärem und Online-Handel. Der gesamte Online-Umsatz der Unternehmen der Schwarz Gruppe belief sich 2022 auf 1,9 Milliarden Euro.

	**17**	**Produktionsstätten**
	**70**	**Sortier- und Recyclingwerke**
	**251**	**Lager**
	**13.700**	**Filialen**

Zahlen im Überblick

Darüber hinaus entwickeln die Unternehmen der Schwarz Gruppe neue Trends und Geschäftsfelder in einer digitalen Welt, um ihre Position zukunftsfähig zu gestalten und stetig auszubauen. Dabei steht die Cloud als Basistechnologie besonders im Fokus. Mit STACKIT, der digitalen Marke der Schwarz IT, werden seit März 2022 Cloud- und Colocation-Services auch für Kunden außerhalb der Schwarz Gruppe angeboten. Der Leistungsumfang der STACKIT Cloud ist bedarfsorientiert ausgerichtet, individuell anpassbar und lässt sich für Organisationen ohne vorhandene Digitallösungen bis hin zu solchen mit etablierten, jedoch isolierten und abgeschnittenen IT-Landschaften gleichermaßen einfach implementieren. Das Angebot erlaubt dabei einen individuellen und direkten Einstieg in die Cloud. Seit dem Aufbau der Cloud-Plattform 2018 wurde STACKIT kontinuierlich zu einem attraktiven Geschäftsmodell ausgebaut. Hierbei legt die Schwarz IT als Betreiber von STACKIT größten Wert auf Datensicherheit und Datenschutz. Die Rechenzentren der Schwarz IT in Deutschland und Österreich unterliegen somit vollständig dem europäischen Recht sowie der Datenschutz-Grundverordnung (DSGVO).

Im Bereich der Lebensmittelproduktion trieb die Schwarz Produktion im Geschäftsjahr 2021 den Bau der ersten Kaffeerösterei im nordrhein-westfälischen Rheine voran. In nur 18 Monaten gelang es der Schwarz Produktion, ein hochmodernes Werk zu errichten, das im Kalenderjahr 2022 die Belieferung der europäischen Filialen von Lidl und Kaufland mit Kaffeeprodukten startete. Mehr als 80 Mitarbeiter werden in Rheine jährlich über 50.000 Tonnen Filterkaffee und ganze Bohnen der Marken Bellarom (Lidl) und K-Classic (Kaufland) herstellen. Mit der erfolgreichen Integration des Eiswerks in Waldfeucht-Haaren (Kreis Heinsberg, Nordrhein-Westfalen) erweiterte die Schwarz Produktion im Jahr 2021 zudem die eigene Eisproduktion. Bereits seit 2017 produziert die zur Schwarz Produktion gehörende Bon Gelati im benachbarten Übach-Palenberg mit 340 Mitarbeitern Eiscreme in höchster Qualität für die Lidl Filialen in Europa. Unter dem Namen „Bon Gelati Haaren“ werden nun von weiteren 200 Mitarbeitern qualitativ hochwertige Eisprodukte für Lidl und Kaufland hergestellt.

Werteorientierte Unternehmensführung

Die Gesellschaft, die Wirtschaft und der Handel stehen vor weitreichenden Veränderungen. Die Unternehmen der Schwarz Gruppe haben dabei die Möglichkeit und die Verantwortung, die stattfindende Transformation nachhaltig zu gestalten und dabei die globalen Herausforderungen fest im Blick zu behalten. Ihre tägliche Arbeit hat zahlreiche Berührungspunkte mit den drängendsten Fragen dieser Zeit. Um Klimawandel, Ressourcenknappheit oder Menschenrechtsverletzungen zu begegnen, ist Zusammenhalt gefragt. Denn nur gemeinsam, in Zusammenarbeit über alle Unternehmen und Ebenen hinweg – vom Angestellten bis ins Top-Management – wird es gelingen, langfristige und wirksame Veränderungen zu erzielen und so zu einer nachhaltigen Entwicklung beizutragen.

Eine vertrauensvolle Zusammenarbeit basiert darauf, andere Meinungen zu hören, sich auszutauschen und nach der besten Lösung zu streben. Deshalb gehört der echte Dialog mit den Stakeholdern zur werteorientierten Unternehmensführung der Unternehmen der Schwarz Gruppe. Aber auch eine gemeinsame Wertvorstellung prägt unser nachhaltiges Handeln. Nur wer aus Überzeugung das Richtige tut, wird als fairer Partner wahrgenommen. Deshalb ist ein transparentes Handeln des Managements essenziell. Es ist die gesellschaftliche Verantwortung der Unternehmen der Schwarz Gruppe, integer zu handeln und Korruption und unlauteren Geschäftsmethoden aktiv entgegenzuwirken. Stakeholder werden bei Kontroll- und Beschwerdemechanismen mit eingebunden, um rechtliche Rahmenbedingungen und interne Richtlinien einzuhalten. Das Thema verantwortungsvolle Geschäftspraktiken beinhaltet zudem die Digitalisierung von Geschäftsprozessen sowie die Einhaltung von Datenschutz und -sicherheitsvorgaben. Darüber hinaus gehören langjährige und faire Geschäftsbeziehungen, Kooperationen in Produktionsländern sowie die Förderung von Infrastrukturprojekten im Sinne eines gesellschaftlichen Engagements dazu.

Abkürzungsverzeichnis

APT	Advanced Persistence Threat (Begriff für komplexen Cyberangriff)
ATO	Account Takeover
AWS	Amazon Web Services
BCM	Business Continuity Management
BEC	Business E-Mail Compromise
BKA	Bundeskriminalamt
BSI	Bundesamt für Sicherheit in der Informationstechnik
CaaS	Cybercrime as a Service
CEO	Chief Executive Officer
CERT	Computer-Emergency-Response-Team
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
COVID-19	Coronavirus-Krankheit
CPU	Central Processing Unit (Prozessor für Computer)
CRA	Cyber Resilience Act
C-SCRM	Cyber-Supply-Chain-Risk-Management
CSIRTs	Computer-Security-Incident-Response-Teams
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DNS	Domain Name System
DORA	Digital Operational Resilience Act
DR	Disaster Recovery
DSA	Digital Service Act
DSGVO	Datenschutz-Grundverordnung
DSP	Digital Service Provider
EDR	Endpoint Detection and Response
ENISA	European Union Agency for Cybersecurity
EU	Europäische Union
Euro	Euro (Währung)
FS-ISAC	Financial Services Information Sharing and Analysis Center
GCP	Google Cloud Platform
IDS	Intrusion Detection System
IKT	Informations- und Kommunikations-technologien
IoT	Internet of Things
IPS	Intrusion Prevention System
ISP	Internet Service Provider
IT	Informationstechnologie
ITISG	IT-Sicherheitsgesetz (Deutschland)
KaMaRisk/ KAIT	Mindestanforderung an das Risikomanagement von Kapital-verwaltungsgesellschaften/ Kapitalverwaltungsaufsichtliche Anforderungen an die IT
KI	Künstliche Intelligenz
KMU	Kleine und mittlere Unternehmen
KRITIS	Kritische Infrastruktur(en)
MaGo/ VAIT	Mindestanforderungen an die Geschäftsorganisation / Versicherungs-aufsichtliche Anforderungen an die IT
Malware	Malicious Software
MaRisk/ BAIT	Mindestanforderungen an das Risikomanagement der Banken / Bankenaufsichtliche Anforderungen an die IT
MFA	Multi-Faktor-Authentifizierung
NIS	Network and Information Security Directive
OES	Operators of Essential Services
OSINT	Open Source Intelligence
OT	Operational Technology
PaaS	Phishing as a Service
PCI-DSS	Payment Card Industry Data Security Standard
RaaS	Ransomware as a Service
RDoS	Ransom Denial of Service
ROI	Return on Investment
ROSI	Return-on-Security Investment
SBOM	Software Bill of Materials (Stückliste für Software-Code)
SEC	Securities and Exchange Commission
SIEM	Security Incident and-Event Management
SQL	Structured Query Language (Datenbanksprache)
SSL	Secure Socket Layer (Übertragungsprotokoll)
TLS	Transport Layer Security (Übertragungsprotokoll)
TRM	Third-Party-Risks-Management
US	United States
USD	US-Dollar (Währung)
VPN	Virtuelles privates Netzwerk

Literaturverzeichnis

[1] Aiyer, B.; Caso, J.; Russel, P.; Sorel, M., „New survey reveales $2 trillion market opportunity for cybersecurity technology and service providers“, McKinsey, 2022

[2] Allianz, “Allianz Risk Barometer”, 2023.

[3] Bischoff, P., “How data breaches affect stock market prices”, comparitech, 2021. Online https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/.

[4] Bitkom e.V., “Wirtschaftsschutz 2022”, 2022.

[5] Bitkom e.V., “7,8 Milliarden Euro: Markt für IT-Sicherheit wächst 2022 um 13 Prozent”, 25. Oktober 2022. [Online]. https://www.bitkom.org/Presse/Presseinformation/IT-Sicherheit-waechst-2022.

[6] BNP Media, “The Security Benchmark Report 2022”, 2022.

[7] BSI, “Industrial Control System Security Top 10 Bedrohungen und Gegenmaßnahmen 2022”, 2022.

[8] BSI, “Maßnahmenkatalog Ransomware”, 2022.

[9] BSI, “Prävention von DDoS-Angriffen”, 2018.

[10] BSI, “Qualifizierte DDoS-Mitigation Dienstleister im Sinne § 3 BSIG”, 2022.

[11] BSI, “Social Engineering”, [Online]. https://www.bsi.bund.de/dok/11312692.

[12] Bundesamt für Sicherheit in der Informationstechnik, “Abwehr von DDoS-Angriffen”, 2018.

[13] Bundesamt für Sicherheit in der Informationstechnik, “Die Lage der IT-Sicherheit in Deutschland 2022”, 2022.

[14] Bundeskriminalamt, “Cybercrime Bundeslagebild 2021”, 2022.

[15] CISA, “ICT Supply Chain Resource Library”, 2022.

[16] CISA, “Implementing Number Matching in MFA Applications”, 2022.

[17] CISA, “Implementing Phishing-Resistant MFA”, 2022.

[18] CISA, “Phishing” 2022.

[19] CISA, “Ransomware Guide”, 2022. [Online]. https://www.cisa.gov/stopransomware/ransomware-guide.

[20] CISA, “Understanding and Responding to Distributed Denial-of-Service Attacks”, 2022.

[21] CISCO, “Security Outcomes Report: Achieving Security Resilience”, Volume 3, 2022.

[22] Clearsky Cybersecurity, “2022 Annual Report”, 2023.

[23] CLTC, “Cyber Oversight Effectiveness Development: A new approach for boards of directors”, UC Berkley, 2021.

[24] Constella Intelligence (2022) “Identity Breach Report”

[25] CrowdStrike “2022 Global Threat Report”, 2022.

[26] CrowdStrike, “2023 Global Threat Report”, 2023.

[27] Deloitte, “2021 Global Future of Cyber Survey”, 2021.

[28] Deloitte, “2023 Global Future of Cyber Survey”, 2022.

[29] Der Spiegel, „»Vulkan Files« Enthüllungen: Das sind Putins Geheimpläne für den Cyberkrieg“, 31. März 2023. [Online] https://www.spiegel.de/politik/deutschland/vulkan-files-enthuellungen-wie-putins-cybersoldaten-den-krieg-ins-internet-tragen-a-bb241ad9-a9c3-422e-af57-ffe59986a1d8.

[30] Der Spiegel, „So liefen die »Vulkan Files«-Recherchen - Woher die Daten stammen, wie sie überprüft wurden, was sie verraten“, 30. März 2023, [Online] https://www.spiegel.de/netzwelt/web/vulkan-files-so-liefen-die-recherchen-zu-putins-krieg-im-netz-a-8ba012dd-4d73-40fd-9731-73ea157a16b1

[31] ENISA, “ENISA Threat Landscape for Ransomware Attacks”, 2022.

[32] ENISA, “ENISA Threat Landscape for Supply Chain Attacks”, 2021.

[33] ENISA, “ENISA Threat Landscape 2022”, 2022.

[34] ENISA, “Introduction to Return on Security Investment”, 2012.

[35] ENISA, “NIS Investments”, 2022.

[36] Europol, “Internet Organised Crime Threat Assessment (IOCTA)”, 2021.

[37] Europol, “No More Ransom”, 2023. [Online]. https://www.nomoreransom.org/de/index.html.

[38] FBI, “Internet Crime Report 2022”, Internet Crime Complaint Center, 2023.

[39] Fortinet, “2022 Cybersecurity Skills Gap”, 2022.

[40] FS-ISAC, “Navigating Cyber 2022”, 2022.

[41] Gartner, “Cyber Risk Primer for 2023”, 2023.

[42] Gartner, “Forecast: Information Security and Risk Management, Worldwide, 2020-2026, 4Q22 Update“, 2022.

[43] Gartner, “Infrastructure Security Primer for 2023”, 2023.

[44] Gartner, “Innovation Insight for Attack Surface Managemnt”, 2022.

[45] Gartner, “IT Key Metrics Data 2023: IT Security Measures – Analysis”, 2022.

[46] Gartner, “Predicts 2023: Cyber-Physical Systems Security – Beyond Asset Discovery”, 2022.

[47] Gartner, “Predicts 2023: Enterprises must expand from threat to exposure management”, 2022.

[48] Gartner, “Predicts 2023: Zero Trust moves past marketing hype into reality”, 2022.

[49] Gartner, “Top Trends in Cybersecurity 2022”, 2022.

[50] Gartner, “2023 Planning Guide for Security”, 2022.

[51] Google, “Securing Software Supply Chains”, Perspectives on Security, Volume One, 2022.

[52] Heidrick & Struggles, “Global Chief Information Security Officer (CISO) Survey”, 2021

[53] Heidrick & Struggles, “Global Chief Information Security Officer (CISO) Survey”, 2022

[54] IBM, “Cost of a data breach 2022 Report”, 2022.

[55] INTEL 471, “Year in Review 2022”, 2023.

[56] ISC2, “Cybersecurity Workforce Study”, 2022.

[57] Kaur, D., “Ransomware-as-a-service? There’s a marketplace on the dark web for it”, T_HQ technology and business, 4. August 2022. [Online]. https://techhq.com/2022/08/ransomware-as-a-service-dark-web/.

[58] Luber, S., “Was ist Log4Shell (Log4j-Schwachstelle)?”, 3. November 2022. [Online]. https://www.security-insider.de/was-ist-log4shell-log4j-schwachstelle-a-6e6873adc74e25e845e027ac024303c8/.

[59] Makridis, C.A., “Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018”, Journal of Cybersecurity, 7, 1, 1-8, 2021.

[60] Mandiant, “Global Perspectives on Threat Intelligence”, 2023.

[61] Mandiant, “Ransomware Protection and Containment Strategy”, 2022.

[62] Microsoft, “Microst Azure – Blog”, 11. Oktober 2021. [Online]. https://azure.microsoft.com/en-us/blog/business-as-usual-for-azure-customers-despite-24-tbps-ddos-attack/. [Zugriff am 02 2023].

[63] Midler, M. „Ransomware as a Service (RaaS) Threats“, Carnegie Mellon University, 2020. [Online] https://doi.org/10.1184/R1/13050170.v2.

[64] Morgan, S., “Top 10 Cybersecurity Predictions and Statistics For 2023”, 10. Dezember 2022. [Online]. https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/.

[65] Munich RE, “Munich RE Global Cyber Risk and Insurance Survey 2022”, 2022.

[66] Paulus, A., Rupp, C., “Government’s Role in Increasing Software Supply Chain Security”, Stiftung Neue Verantwortung, 2023.

[67] Reddie, A.; Krishnan, P., “Moving Left and Right: Cybersecurity Processes and Outcomes in M&A Due Diligence”, Center for Long-Term Cybersecurity, UC Berkley, 2022.

[68] Reuters, „Siemens investigating report employee worked for Russian hacking firm“, 31. März 2023, [Online] https://www.reuters.com/technology/siemens-investigating-report-employee-worked-russian-hacking-firm-2023-03-31/

[69] Siegert, J., “Notizen aus Moskau: Hybrider Krieg!?”, 2016. [Online]. https://www.bpb.de/themen/europa/russland-analysen/nr-314/225679/notizen-aus-moskau-hybrider-krieg/.

[70] Statista, “Cybersecurity Outlook”, 2022.

[71] Statista, “IT spending as share of company revenue in 2022 by Industry”, 2022. [Online]. https://www.statista.com/statistics/1105798/it-spending-share-revenue-by-industry/.

[72] The White House, “National Cybersecurity Strategy”, 2023.

[73] The Guardian, „Vulkan files‘ leak reveals Putin’s global and domestic cyberwarfare tactics“, 30. März 2023, [Online] https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics.

[74] Verizon, “Data Breach Investigations Report (DBIR) 2022”, 2022.

[75] World Economic Forum, “Global Cybersecurity Outlook 2023”, 2023.

[76] XM Cyber; Cyentia Institute, „Navigating the Paths of Risk - The State of Exposure Management in 2023“, 2023.

[77] ZDF, „Putins digitales Waffenarsenal: „Vulkan Files“: Russland plant den Cyberkrieg“ 30. März 2023, [Online] https://www.zdf.de/nachrichten/digitales/vulkan-files-cyberangriff-hacker-ukraine-krieg-russland-100.html.

[78] ZDF, „Russische Firma für Cyberwaffen: Was steckt hinter den „Vulkan Files“?“, 30. März 2023, [Online] https://www.zdf.de/nachrichten/digitales/vulkan-files-leak-daten-faq-ukraine-krieg-russland-100.html

Impressum

Herausgeber

Schwarz Digital GmbH & Co. KG
Stiftsbergstraße 1
74172 Neckarsulm

Sitz: Neckarsulm
Amtsgericht Stuttgart: HRA 735957
USt-IdNr.: DE325553482

E-Mail: csc@cyberconference.schwarz
https://cyberconference.schwarz/

Die Zusammenfassung der bestehenden und geplanten Regulatorik im Cybersecurity Kontext stellt keine Rechtsberatung dar und erhebt keinen Anspruch der Vollständigkeit. Sie dient dazu den Lesern einen Überblick zu verschaffen.

Die Schwarz Digital GmbH & Co. KG wird vertreten durch die Schwarz Digital Beteiligungs-GmbH mit Sitz in Neckarsulm, eingetragen im Handelsregister des Amtsgerichts Stuttgart unter HRB 769509, die ihrerseits gemeinsam durch zwei gesamtvertretungsberechtigte Geschäftsführer, u.a. Rolf Schumann und Robert Jozic vertreten wird.