THE MISSION

CYBER SECURITY

2024

12 AKTUELLE TRENDS IM BEREICH CYBERSECURITY

Innovative Lösungen für neue Bedrohungen

Inklusive Vorstellung der 5 Start-ups von THE MISSION Cyber Security 2024!

INHALT

THE MISSION
CYBER SECURITY

Besuchen Sie unsere Initiative THE MISSION auch online unter

https://www.handelsblatt.com/adv/the-mission/

Die digitale Transformation geht für die Unternehmen mit zahlreichen Vorteilen einher. Zugleich nimmt jedoch auch die Bedeutung des Themas Cybersicherheit zu. Denn mit der zunehmenden Digitalisierung steigt das Risiko von Cyberangriffen. Gerade im Zuge der Vernetzung sind immer mehr Bereiche und Systeme eines Unternehmens von außen erreichbar und damit angreifbar. Und sind Angreifer erst einmal irgendwo eingedrungen, können sie ebenfalls mehr Systeme im Unternehmen erreichen.

Im jüngsten Lagebericht zur IT-Sicherheit in Deutschland von 2023 weist das Bundesamt für Sicherheit in der Informationstechnik (BSI) darauf hin, dass täglich weltweit ungefähr 70 neue Schwachstellen in Softwareprodukten entdeckt werden. Gegenüber dem vorherigen Berichtszeitraum ist dies ein Anstieg um etwa 25 Prozent. Und mehr als 200 neue Schadprogramm-Varianten kommen im Durchschnitt weltweit täglich dazu. Diese Lücken und Programme können Angreifer für den Zugang zum Unternehmenssystem unter Umständen nutzen.

Aufgrund dieser enormen Bedeutung der Cybersicherheit gibt es seit diesem Jahr ein neues Programm als Teil der Initiative THE MISSION: Cyber Security. Dieser Report greift begleitend dazu zwölf Trends auf, die die aktuelle Entwicklung im Bereich Cybersicherheit und Cyberangriffe darstellen.

Zuvor erfolgt ein Blick auf den gegenwärtigen Status quo bei den Unternehmen mit Blick auf den Bereich Cybersecurity. Wie hoch ist das Aufkommen von Cyberangriffen? Was sind die größten Risiken? Wie sind die Unternehmen darauf vorbereitet? Welche Schäden sind mit den Angriffen verbunden?

Für die Unternehmen gibt es zahlreiche Ansätze zur Verbesserung der Abwehr von Cyberangriffen. Eine Rolle spielen dabei auch Partner wie Start-ups im Bereich Cybersicherheit. Fünf dieser jungen Unternehmen werden in der aktuellen THE MISSION Cyber Security gefördert. Kurzporträts dieser Start-ups sind ebenfalls im Report zu finden.

Der Status quo im Bereich Cybersecurity

Cyberangriffe sind zur größten Sorge der Unternehmen geworden

Unternehmensbefragung in Deutschland:
Was sind die bedrohlichsten Risiken für Ihren Betrieb?
> 1.000 befragte Unternehmen, Mehrfachnennungen möglich (max. drei Antworten), Nennungen in Prozent

Quelle: Gothaer

48 %
Cyberangriffe, Viren, Trojaner etc.

41 %
Menschliches Versagen

40 %
Betriebsausfall

31 %
Einbruch/Vandalismus

30 %
Brände/Explosionen

28 %
Ausfall I Zulieferer

19 %
Reputationsverlust durch schlechte Presse

11 %
Sturm/Hagel

9 %
Hochwasser

Und tatsächlich wächst der Schaden

Durch Cyberangriffe entstandene Schäden in Deutschland

Quelle: Bitkom

Viele Unternehmen sind noch nicht allzu gut vorbereitet

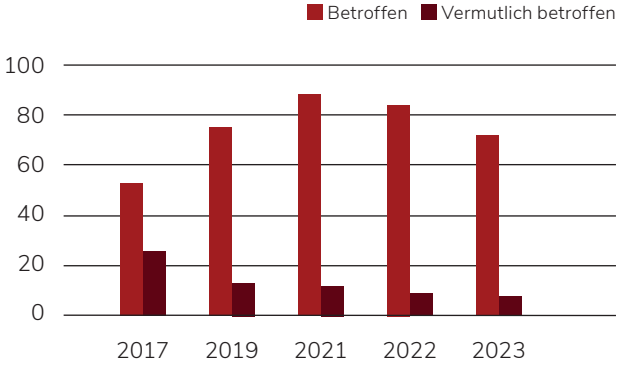
Cybersecurity-Readiness-Index

Quelle: Cisco

Das Risiko eines Angriffs ist hoch …

Datendiebstahl, Industriespionage und Sabotage in den Unternehmen
Anteil der Unternehmen, die in den letzten zwölf Monaten (2017/2019: 24 Monaten) davon (vermutlich) betroffen waren

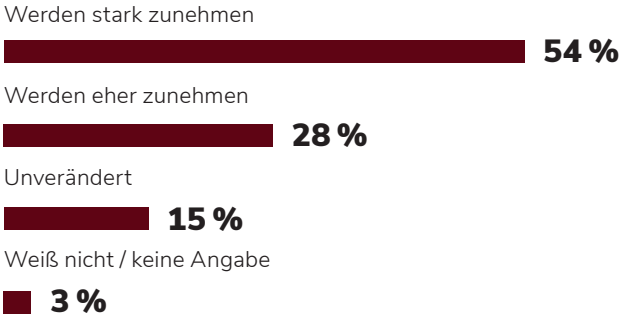
Quelle: Bitkom Research



… und dürfte weiter steigen

Wie wird sich die Anzahl der Cyberattacken in den nächsten zwölf Monaten im Vergleich zu den letzten zwölf Monaten voraussichtlich entwickeln?
Anteil der 2023 befragten Unternehmen

Quelle: Bitkom Research



Die Nachfrage nach Cybersecurity-Angeboten wird stark zunehmen

Deutschlands Cybersecurity-Markt
Volumen

Quellen: IDC, Bitkom

Die 5 Start-ups der THE MISSION CYBER SECURITY 2024

langlauf
SECURITY AUTOMATION

Automatisierte Erzeugung von Softwarestücklisten – auch ohne Quellcode

Die **Langlauf Security Automation GmbH** ist Spezialist für die automatisierte Erstellung von Softwarestücklisten (Software Bills of Materials, kurz SBOMs). Dank Langlauf können Unternehmen Regularien wie den Cyber Resilience Act (CRA) effizient erfüllen, ohne ihre Fachkräfte mit lästiger, stets wiederkehrender Arbeit zu belasten. Langlaufs Technologie wird als Selfservice bereitgestellt und lässt sich nahtlos in bestehende Prozesse und Pipelines integrieren. Da für die Erstellung von SBOMs kein Quellcode erforderlich ist, eignet sich die Lösung auch für zugelieferte Komponenten, Legacy- sowie verschiedenste andere Arten von Software, darunter Firmware, Embedded Images, virtuelle Maschinen, Container sowie Linux- und Windows-Anwendungen. Der Mehrwert der Lösung konnte in zahlreichen Projekten mit (M)DAX-Konzernen, der Cyberagentur (Gesellschafter BMVg) sowie durch die Auswahl für die hochdotierte BMBF-Initiative „StartUpSecure“ unter Beweis gestellt werden. Langlauf ist unabhängig, inhabergeführt und beschäftigt derzeit neun Mitarbeiter an den Standorten Lippstadt/Paderborn und deutschlandweit.

Kontakt: www.langlauf.io
Jan Stijohann, stijohann@langlauf.io

SANCTUARY

Sicherheit für eingebettete Systeme

SANCTUARY hat sich auf die Bereitstellung modernster Cybersicherheitslösungen für eingebettete Systeme spezialisiert. Gegründet im Jahr 2020, ist das Unternehmen heute hauptsächlich in der Industrieautomatisierungs- und Raumfahrtbranche aktiv. SANCTUARY entwickelt On-Device-Sicherheitslösungen für eingebettete Systeme unter Verwendung von Virtualisierung und hardwaregestütztem Trusted Computing, bietet aber auch Vertrauenstechnologien zwischen Geräten wie etwa eine robuste Public-Key-Infrastruktur (PKI) für schwierige Netzwerkbedingungen an.

Schließlich ermöglicht die OT-Asset Management-Lösung „SANCTUARY Insight“ umfassende Transparenz und Kontrolle über Steuerungen und Netzwerkgeräte in der Produktion (Operational Technology, OT). „SANCTUARY Insight“ verbindet nahtlos passive und aktive Erkennung und bietet einen beispiellosen Einblick in die gesamte OT-Landschaft. Dabei werden Detailinformationen über alle Geräte der Produktion gesammelt, von modernen Netzwerkgeräten bis hin zu in die Tage gekommenen SPSen, ohne die Betriebsabläufe zu stören.

Kontakt: www.sanctuary.dev
Emmanuel Stapf, emmanuel.stapf@sanctuary.dev

Priorisierung stärkt die OT-Resilienz

asvin Software ermöglicht das Priorisieren von Cybersicherheitsmaßnahmen und damit den deutlich effektiveren Einsatz von Ressourcen. Betreiber von Operational Technology (OT) erreichen damit trotz Regulierungsdruck (NIS2 oder CRA) und komplexen Herausforderungen ihre Resilienzziele.
Mit „Risk By Context"TM und „Device Security Booster"TM lassen sich Risiken exakt lokalisieren und deren Beseitigung erstklassig planen. Durch das Herstellen von Kontext-Bezügen zwischen sämtlichen Elementen der OT im Unternehmen und seinen Zulieferern sind sowohl offensichtlich, als auch bisher nicht erkannte Risikofaktoren darstellbar. Das erlaubt präzise Risikovorhersagen. Vor allem aber sind damit wertvolle Aussagen zur Priorisierung von Abwehrmaßnahmen möglich. Unternehmen brauchen so für den Schutz ihrer OT kein zusätzliches Fachpersonal und können ihre Cybervorkehrungen optimal planen. Beispiel Kosten für Rückrufaktionen durch eigen- oder fremdverschuldete Softwarefehler im Automobilbau: Wer in der Lage ist, erwartbare Risiken zu sehen, kann seine Rückstellungen minimieren. Entwickelt wurde die Risikoanalyse- und Priorisierungstechnologie am Autostandort Stuttgart und am renommierten MIT in Cambridge, MA, USA.

Kontakt: www.asvin.io
Gerhard Steininger, g.steininger@asvin.io

Cybersicherheit leicht gemacht

Diri hat eine einzigartige SaaS-Lösung entwickelt, die kleinen und mittleren Unternehmen hilft, proaktiv mit Cybersicherheit zu arbeiten. Die Lösung rationalisiert und erhöht die Qualität der Arbeit des Unternehmens mit Cyberrisiken und gibt dem Unternehmen eine gute Kontrolle und Übersicht über die Vermögenswerte, Risiken, Bedrohungen und Behandlungen des Unternehmens. Zusätzlich zum Risikomanagement für die Cybersicherheit bieten wir ein separates Datenschutzmodul an, und im Laufe des Jahres 2024 werden wir auch ein separates Compliance-Modul bereitstellen, damit Sie einfach überprüfen und melden können, ob Sie z. B. mit NIS2 konform sind.

In Kürze wird auch unser KI-Modul verfügbar sein, das das Unternehmen durch die Prozessschritte der Lösung unterstützt. Dies wird die Qualität und Effizienz weiter steigern, den Ressourcenverbrauch und den Bedarf an Fachwissen senken. Zusammen mit einer benutzerfreundlichen Oberfläche und einer kostengünstigen Preisgestaltung helfen wir Unternehmen, die Kontrolle über ihre Cybersicherheit zu übernehmen. Die Mitarbeiter werden zu Cybersheriffs im eigenen Unternehmen – und halten Angreifer in Schach.

Kontakt: www.diri.ai
Frøydis Barstad, froydis@diri.no
Gaute Wangen, gaute@diri.no

Die Zukunft des sicheren Speicherns

TF-Industries GmbH hat mit „Safe Storage" eine innovative Lösung für die Sicherheit von Back-up-Systemen entwickelt. Dieses System ist der weltweit erste physisch automatisierte Airgap. Das patentierte Schleusenverfahren erzeugt eine physische Trennung zwischen dem Produktivnetzwerk und dem Back-up bzw. Vault. So wird der Datenstrom kontrolliert und abgeschirmt, um die Daten vor Cyberbedrohungen zu schützen und die Integrität des Back-ups zu gewährleisten. Nach einer Entwicklungszeit von vier Jahren wurde im Januar 2024 nach erfolgreichem MVP die TF-Industries GmbH gegründet. Ansässig ist TF-Industries im Zentrum für IT-Sicherheit (ZITS) in Bochum. Seit der Gründung ist das Team kontinuierlich gewachsen und hat wichtige und essenzielle Partnerschaften geknüpft, um das Unternehmenswachstum zu fördern. Der „Safe Storage" wurde bereits erfolgreich bei den ersten Kunden implementiert. Das Unternehmen wurde zu den offiziell Top-drei-Start-ups in NRW gewählt.

Kontakt: www.tf-industries.com | Tobias Bümmerstede, buemmerstede@tf-industries.com

12 aktuelle Trends im Bereich Cybersecurity

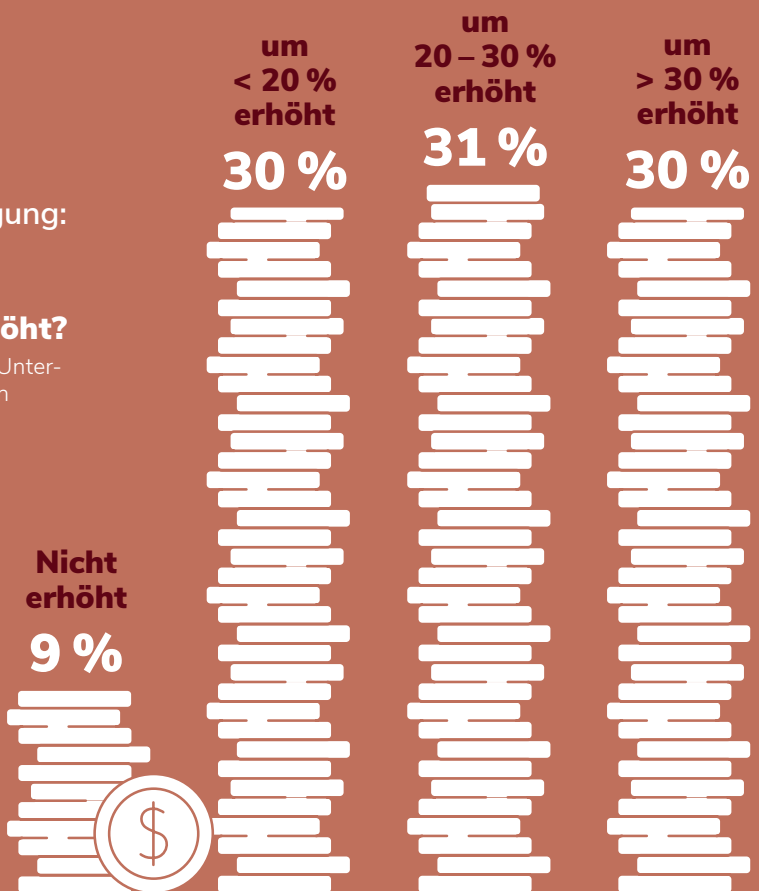
TREND #1

Unternehmen müssen investieren – und tun das auch

Globale Unternehmensbefragung:
Um wie viel haben Sie Ihre Cybersicherheitsbudgets in den letzten zwei Jahren erhöht?

Befragt wurden mehr als 8.000 befragte Unternehmen aus 30 unterschiedlichen Ländern

Quelle: Cisco



Wie sehr die Bedeutung des Themas Cybersecurity gewachsen ist, zeigt eine Auswertung von Google Trends. Demnach wird in der Suchmaschine inzwischen mehr als doppelt so häufig nach diesem Begriff gesucht wie noch im Jahr 2022 – und viermal häufiger als 2019. Aufgrund der vielen Berichte über erfolgreiche Cyberangriffe und milliardenschwere Schäden sehen die Unternehmen in Deutschland offenbar einen besonderen Handlungsbedarf, die eigene Resilienz zu verbessern.

Tatsächlich scheinen die Sorgen groß zu sein: Auf die Frage, ob sie die eigene geschäftliche Existenz durch Cyberangriffe gefährdet sehen, antworten inzwischen 52 Prozent der befragten Unternehmen mit Ja, wie eine Umfrage des Digitalverbands Bitkom zeigt. Noch im Jahr 2021 galt das lediglich für neun Prozent. Tatsächlich sehen viele in einem Mehr an Cybersicherheit aber nicht nur eine Herausforderung, sondern auch eine Chance: **In einer Unternehmensbefragung des TÜV-Verbands gaben 76 Prozent der Befragten an, ein hohes Niveau an Cybersecurity sei ein Wettbewerbsvorteil.** Wer die Daten der Kundschaft und der Partner wirksam schützen kann, gilt als vertrauenerweckend, so das Kalkül.

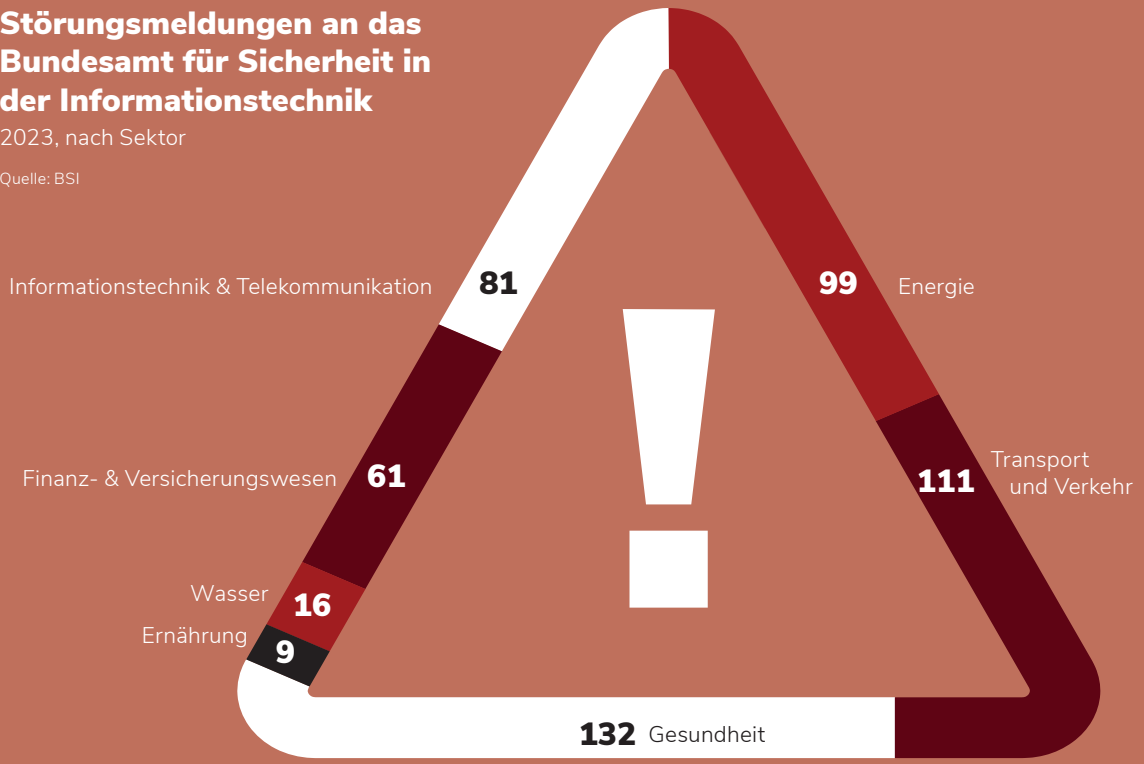
Zwar haben viele Unternehmen in der zurückliegenden Zeit schon größere Investitionen in die Sicherheitsstruktur vorgenommen – und beispielsweise ihre Schutzsoftware verbessert, Notfallpläne aufgestellt, das Back-up-Management optimiert sowie technische Stresstests oder Schulungen für die Belegschaft organisiert. So ist der Anteil des IT-Budgets, der in deutschen Firmen für Sicherheitsmaßnahmen aufgewendet wird, laut Bitkom zwischen 2022 und 2023 von neun auf 14 Prozent angestiegen. Allerdings gilt eine Mehrheit der Unternehmen hierzulande noch nicht wirklich als gut vorbereitet, wie eine Untersuchung des Telekommunikationskonzerns Cisco zeigt. Demnach wird die sogenannte Cybersecurity Readiness nur bei elf Prozent der Unternehmen als ausgereift (mature) und bei 33 Prozent als fortgeschritten (formative) bezeichnet. Bei der Analyse wurde geprüft, inwieweit bei Unternehmen bestimmte Sicherheitstechnologien bereits standardmäßig verwendet werden – wie etwa komplexe Authentifizierungsprozesse, Verschlüsselungstechniken, dezentrales und redundantes Speichern, KI-basierte Schwachstellenanalysen und Ähnliches. Wenig überraschend sind die Readiness-Werte bei größeren Unternehmen im Durchschnitt höher als bei kleinen.

Auch unter Unternehmen, die im Bereich der kritischen Infrastruktur (KRITIS) tätig sind, gibt es heute noch immer einige, deren Sicherungssysteme keine hohen Reifegrade erreichen, wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem Lagebericht kritisiert. Der Anteil der Unternehmen mit geringem Reifegrad liegt demnach je nach Analysefokus zwischen 27 und 39 Prozent. Das BSI mahnt daher zusätzliche Investitionen an.

Prognosen gehen davon aus, dass die Unternehmen ihre Investitionen in die Cybersicherheit weiter massiv ausweiten werden, nicht nur in Deutschland, sondern global. Laut Cisco plant jedes dritte Unternehmen weltweit im laufenden Jahr mit einem Budget-Plus von mehr als 30 Prozent. Und eine weitere Hälfte will zumindest zwischen zehn und 30 Prozent mehr ausgeben.

Betreiber kritischer Infrastrukturen:
Störungsmeldungen an das Bundesamt für Sicherheit in der Informationstechnik
2023, nach Sektor

Quelle: BSI



Gesetzliche Vorgaben für Unternehmen hinsichtlich Cybersecurity nehmen zu

Wie gravierend ein Cyberangriff ist, hängt auch damit zusammen, ob sich nur beim betroffenen Unternehmen Schäden materialisieren – oder ob andere Bereiche ebenfalls in Mitleidenschaft gezogen werden. Als besonders gefährlich werden Attacken angesehen, die jene Unternehmen ins Visier nehmen, die sogenannte kritische Infrastrukturen betreiben (KRITIS). Diese erbringen Leistungen, die für einen funktionierenden Alltag unerlässlich sind – und ohne die die Versorgung der Bevölkerung behindert oder die Sicherheit des Landes gefährdet wäre. Zu den neuralgischen Branchen werden unter anderem die Sektoren Energie, Transport und Verkehr, Gesundheit, Wasser, Ernährung oder auch das Finanz- und Versicherungswesen gezählt. Werden Unternehmen aus diesen Bereichen lahmgelegt, kann dies ein Land massiv schwächen. Gerade vor dem Hintergrund dessen, dass geopolitische Auseinandersetzungen künftig vermehrt in der Cyberwelt stattfinden dürften, wird die Schaffung von sicheren IT-Strukturen als Beitrag zur Landesverteidigung angesehen.

Die Europäische Union (EU) hat auf die wachsende Bedrohung reagiert, indem sie die Zusammenarbeit der Mitgliedsstaaten im Bereich der Cybersicherheit gestärkt hat. Vor allem aber soll ein einheitliches Schutzniveau für Unternehmen aus dem KRITIS-Bereich geschaffen werden. Dazu werden diese zu mehr Vorsichts- und Sicherheitsmaßnahmen verpflichtet. Die „Network and Information Security"-Richtlinie (NIS2) aus dem Jahr 2022, die derzeit von den Mitgliedstaaten in nationales Recht übertragen wird, hat die Vorgaben im Vergleich zur vorherigen Richtlinie aus dem Jahr 2016 stark ausgeweitet. So werden deutlich mehr Unternehmen unter die neuen Regelungen fallen, da diese bereits ab einer Belegschaft von mindestens 50 Arbeitskräften und einem Jahresumsatz von mindestens zehn Millionen Euro greifen. **Die Zahl der betroffenen Unternehmen wird allein für Deutschland auf mehr als 25.000 geschätzt.** Wichtig ist, dass diese nicht proaktiv darüber informiert werden, dass die neuen Regelungen auf sie zutreffen, sondern dieses selbst prüfen müssen.

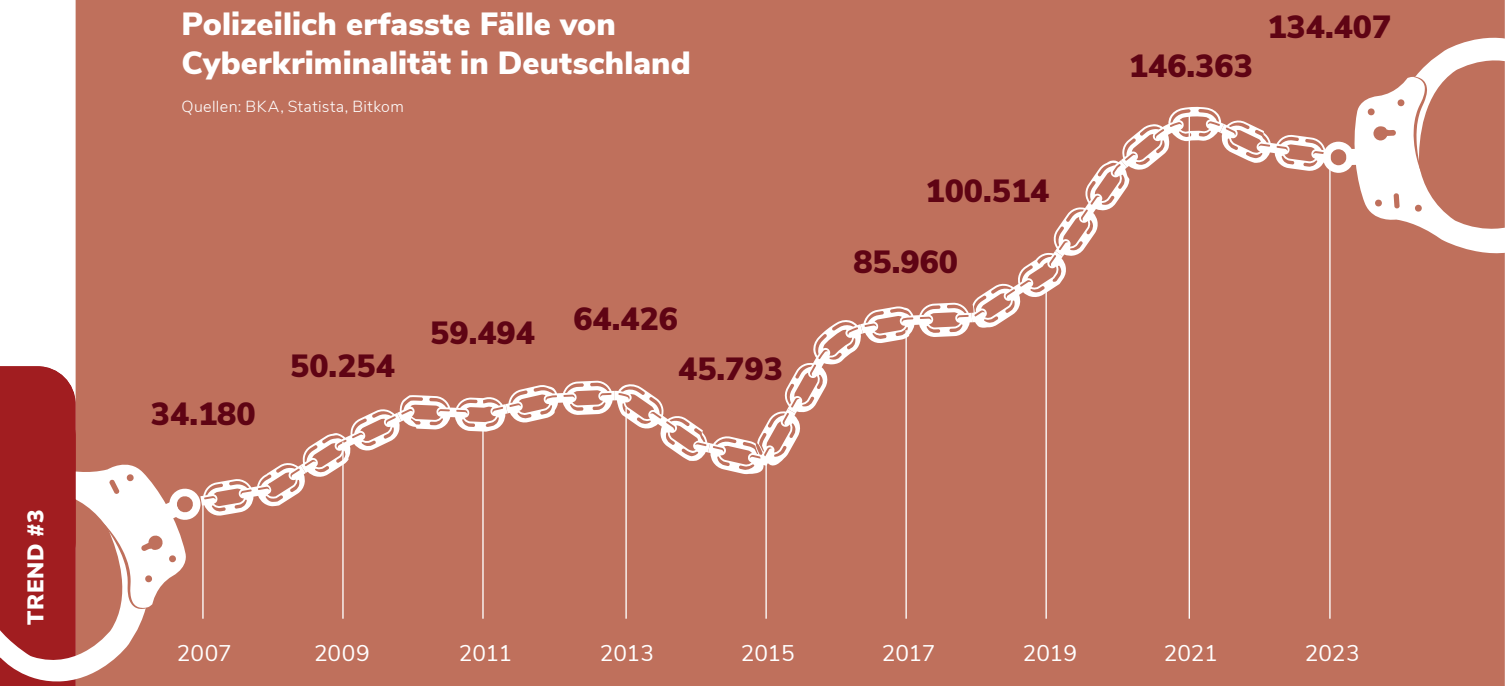
Unternehmen aus dem KRITIS-Bereich werden künftig verpflichtet sein, strengere Sicherheitsmaßnahmen umzusetzen, Krisen- und Notfallpläne vorzuhalten und ihre Risiken kontinuierlich und konsequent zu managen. Letzteres gilt dabei nicht nur für das eigene Unternehmen, sondern auch für die Lieferketten. Ferner müssen Mindeststandards eingehalten werden – etwa, indem die sogenannte Zwei-Faktor-Authentifizierung angewandt wird. Hinzu kommt die Pflicht, die eigenen Führungskräfte regelmäßig umfassend zu schulen. Und nicht zuletzt müssen Unternehmen, die Sicherheitsvorfälle erleben, diese an die zuständigen Behörden melden – und dies bereits innerhalb von 24 Stunden.

Um die neuen Vorgaben überwachen zu können, sollen die entsprechenden Behörden gestärkt werden. Auf EU-Ebene gilt dies für die Europäische Agentur für Cybersicherheit (ENISA), in Deutschland für das Bundesamt für Sicherheit in der Informationstechnik (BSI). Halten Unternehmen die Vorgaben nicht ein, können sie von den Behörden dazu gezwungen werden. **Auch Bußgelder sind möglich. Diese können bis zu zehn Millionen Euro betragen.**

TREND #3

Polizeilich erfasste Fälle von Cyberkriminalität in Deutschland

Quellen: BKA, Statista, Bitkom



Menschen und Unternehmen leiden immer stärker unter Cybercrime

Die Zahl der Cybercrime-Fälle, die das Bundeskriminalamt (BKA) in der Polizeilichen Kriminalstatistik (PKS) verzeichnet, ist enorm: Im Jahr 2023 waren es mehr als 130.000. **Mit knapp 32 Prozent ist die Aufklärungsquote in diesem Kriminalitätsfeld eher gering.** Obendrein geht das BKA davon aus, dass es neben dem sogenannten Hellfeld von polizeibekannten Fällen noch ein großes Dunkelfeld von nicht gemeldeten Fällen gibt.

Die Schäden, die durch Cyberkriminalität entstehen, sind unterschiedlich: Bei Privatpersonen können finanzielle Schäden entstehen, wenn Bankkonten gehackt oder Phishing-Angriffe nicht als solche erkannt werden. Im schlimmsten Falle kann auch die eigene Sicherheit betroffen sein, etwa wenn private Daten von Prominenten öffentlich werden. Auch Bloßstellungen sind denkbar – beispielsweise wenn medizinische Daten in die falschen Hände geraten.

Bei öffentlichen Einrichtungen gehört die Lahmlegung des Verwaltungsbetriebs zu den häufigsten Schäden: Dies bedeutete zuletzt beispielsweise, dass Behörden nicht erreichbar waren, Sozialleistungen zeitweise nicht ausgezahlt und Termine nicht vergeben werden konnten. Besonders gravierend waren die Schäden bei Cyberangriffen auf Kliniken: Hier konnten Datenbanken mit Patienteninformationen mitunter nicht mehr abgerufen werden – ein Missstand, der letztlich Menschenleben gefährden kann.

In der Unternehmenswelt sind die Schäden ebenfalls vielfältig: Wenn der eigene Betrieb aufgrund von lahmgelegten IT-Systemen pausieren muss, gehen Umsätze verloren. Wenn darüber hinaus Lieferverpflichtungen nicht eingehalten werden können, können Schadensersatzzahlungen folgen. Zu den Schäden zählt auch der Verlust immaterieller Werte – etwa in Form von Produktionsgeheimnissen oder Patenten.

Die Cybercrime-Schäden für die deutsche Wirtschaft beliefen sich 2023 auf 148 Milliarden Euro, 20 Milliarden mehr als im Vorjahr.

Nicht zuletzt leidet die Reputation von Unternehmen, die Opfer von Cyberangriffen werden. Schließlich beweisen sie, dass ihre Schutzsysteme nicht in ausreichendem Maße justiert waren – und dass sie mit den Daten der Kundschaft und der Geschäftspartner nicht sorgsam genug umgegangen sind.

Zu all dem gesellen sich später meist auch noch die Kosten für die Schadensbehebung: Daten müssen wiederhergestellt, Schutzsysteme verstärkt und Beratungsleistungen eingekauft werden. Auch Lösegelder – etwa für das Entschlüsseln von Daten nach Ransomeware-Angriffen – zählen zu den Schadenssummen. Allerdings ist der Anteil der Unternehmen, die auf Lösegeldforderungen eingehen und diese bezahlen, zuletzt massiv zurückgegangen, wie beispielsweise Zahlen des Cybersecurity-Beratungsunternehmens Coveware zeigen. **Demnach zahlen weltweit nur noch 29 Prozent der Unternehmen Lösegelder.** Die Gründe für die neue Standfestigkeit sind heterogen: Einerseits haben viele bessere Back-up-Strategien implementiert, sodass sie verschlüsselte Daten selbst wiederherstellen können. Zum anderen brechen die Angreifer oftmals ihre Versprechen – und können die Daten gar nicht mehr entschlüsseln. Oder sie verkaufen sie trotz anderslautender Versprechen weiter.

Einer Bitkom-Schätzung zufolge resultieren inzwischen 72 Prozent aller Schäden, die deutschen Unternehmen aufgrund von Diebstahl, Industriespionage oder Sabotage entstehen, aus Cyberattacken. Dies entsprach im Jahr 2023 einer Summe von 148 Milliarden Euro.

Die Wertschöpfungskette der Cyberkriminalität wird immer feingliedriger

Der Aufstieg des Internets hat die Arbeitsteilung in der Wirtschaft vereinfacht. Dabei geholfen haben beispielsweise digitale Handelsplattformen, auf denen nicht nur Waren, sondern auch spezialisierte Dienstleistungen angeboten werden können – ähnlich einem klassischen Schwarzen Brett, auf das aber weltweit zugegriffen werden kann. Unternehmen können sich auf diese Weise kurzfristig Hilfe buchen oder ganze Tätigkeiten auslagern. Heute ist es üblich, dass Unternehmen nicht mehr alle anfallenden Aufgaben selbst erledigen, sondern auf ein Ökosystem von Partnern zurückgreifen. Die Wertschöpfungsketten sind also länger geworden. Viele Unternehmen setzen dabei auf sogenannte As-a-Service-Modelle: Dabei wird Soft- und Hardware nicht mehr selbst gekauft und betrieben, sondern für monatliche Lizenzgebühren von externen Dienstleistern gemietet. Ein Beispiel hierfür ist das Cloud-Computing.

Auf die gleiche Weise hat allerdings auch das organisierte Verbrechen seine Strukturen professionalisiert und individualisiert. Kriminelle Organisationen müssen heute nicht mehr alle Schritte selbst beherrschen, die für Angriffe auf Behörden oder Unternehmen notwendig sind, sondern kaufen sich die notwendigen Dienstleistungen auf einem freien Markt ein. Dazu nutzen sie Plattformen im Darknet. Das Angebot an spezialisierten Dienstleistungen ist inzwischen sehr groß: Provider vermieten Server, von denen aus die Angriffe ausgeführt werden können. Programmierer:innen bieten an, Malware zu programmieren oder bestehende Programme weiter zu „veredeln“, beispielsweise indem sie deren Tarnung gegenüber Virenscannern optimieren.

Sogar die Angriffe selbst können an externe Dienstleister ausgelagert werden. Diese verschicken dann – in Auftragsarbeit – Phishing-Mails oder versuchen, Server lahmzulegen. Besonders ausgefeilt sind die Angebote im Bereich Ransomware-as-a-Service: Hier übernehmen Dienstleister nicht nur die Ausführung der Angriffe, sondern auch eine Art Kundenservice für die angegriffenen Unternehmen sowie die Zahlungsabwicklung für die Lösegelder inklusive der notwendigen Geldwäsche. Viele Akteure sind aufgebaut wie normale Unternehmen – und werben mitunter ganz offen um neue Arbeitskräfte oder für ihre Angebote.

Auch in der Unterwelt ist die Produktpalette groß: Unterschieden wird zwischen maßgeschneiderten Produkten, die einzeln programmiert werden, und günstigeren Standard-Toolkits, die per Baukastenprinzip für Angriffe genutzt werden können. **Einstiegsmodelle sind für wenige Hundert US-Dollar zu haben, spezialisierte Dienstleistungen kosten schnell hohe vierstellige Summen.**

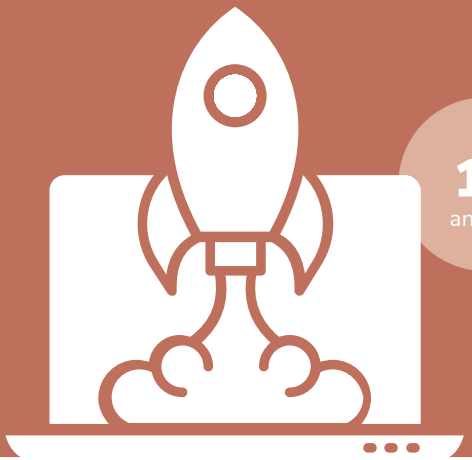
Die geschilderte Professionalisierung der Cybercrime-Strukturen hat dazu geführt, dass die Angriffe häufiger und die Schäden größer werden. Gleichzeitig professionalisieren die Staaten ihre Polizeiarbeit im Kampf gegen die Cyberkriminalität. In Deutschland beispielsweise haben die Bundesländer inzwischen Spezialeinheiten aufgebaut, die sich explizit mit der Internetkriminalität befassen. Da kriminelle Banden oftmals global und von für sie sicheren Standorten aus operieren, wird in der Polizeiarbeit meist der sogenannte Infrastrukturansatz verfolgt. Dabei werden nicht die einzelnen Tätergruppen ins Visier genommen, sondern Plattformen und andere Server, die die Kriminellen für ihre Arbeit brauchen – so etwa die großen Handelsplattformen im Darknet.

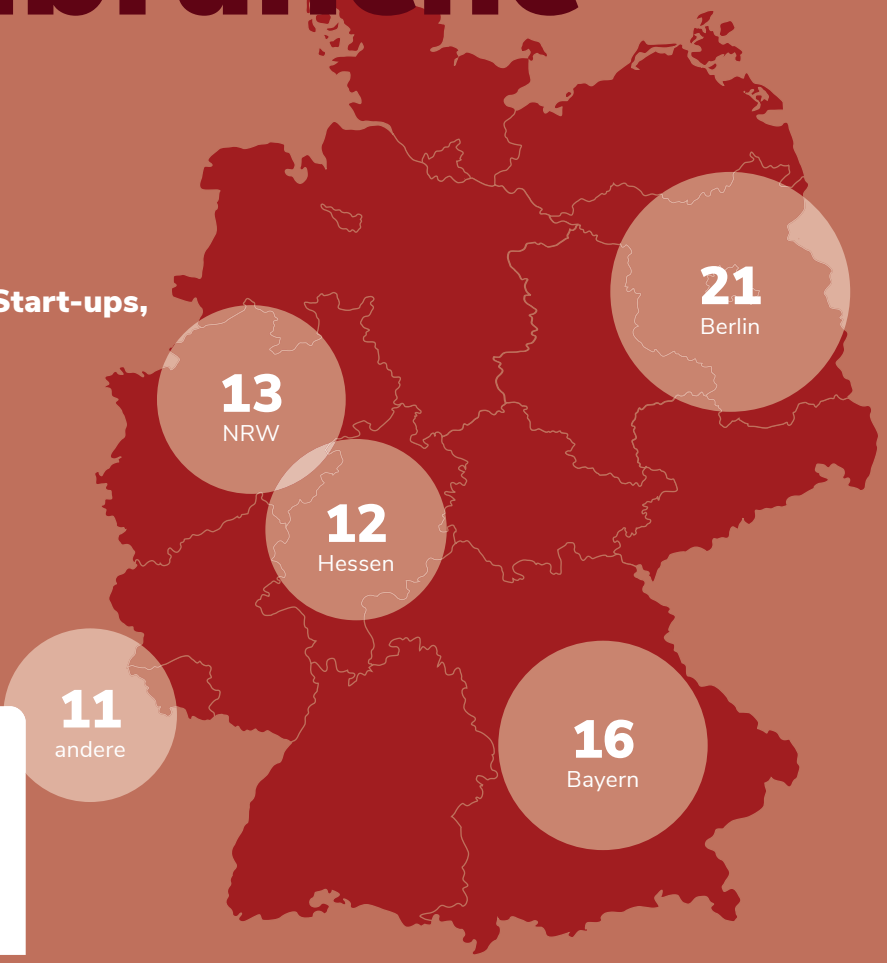
TREND #5

Cybersicherheit ist zur innovativen Boombranche geworden

Deutsche Cybersecurity-Start-ups, nach Bundesland

Quellen: Dealroom, eigene Auswertung





Wer in Internetsuchmaschinen nach Angeboten der Cybersicherheitsbranche sucht, dem fällt zunächst eines auf: Am Anfang der Trefferlisten findet sich stets eine hohe Zahl von gesponserten Links. Das zeigt, wie groß der Konkurrenzkampf in der digitalen Sicherheitsbranche ist – und wie groß die Nachfrage nach entsprechenden Dienstleistungen.

Tatsächlich ist der Bedarf in den zurückliegenden Jahren massiv gewachsen: Zum einen kommt es heute viel öfter zu Cyberangriffen, welche den betroffenen Unternehmen schwere Finanz- und Reputationsschäden bescheren können, wenn sie nicht abgewehrt werden. Zum anderen digitalisiert sich die Wirtschaftswelt zunehmend: Immer mehr Verwaltungs-, Steuerungs-, Kontroll- und Planungsaufgaben werden von Menschen an vernetzte Computer und Clouds übertragen. Dies erhöht die Menge an potenziell gefährdeten Strukturen, die geschützt werden müssen.

Aufgrund der vielfältigen Bedrohungen ist es heute deutlich komplexer geworden, die eigenen Systeme ausreichend gegen Gefahren abzuschirmen. Dementsprechend breit ist die Palette von Angeboten. Dazu zählen einerseits Softwarelösungen, die die firmeneigenen Datenbanken, Netzwerke, Clouds, Server und Kommunikationswege im Alltag schützen sollen. Hinzu kommen zahlreiche Dienstleistungen. Angeboten werden beispielsweise Schwachstellenanalysen und Penetrationstests, um potenzielle Einfallstore für Angriffe zu identifizieren und zu schließen, ebenso die Erstellung von Notfallplänen, die Schulung von Führungskräften und Belegschaften oder die Zertifizierung regulierungskonformer Maßnahmen. Im Fokus stehen auch Beratungsleistungen: Um im Schadensfall Spuren sichern und Daten wiederherstellen zu können, werden beispielsweise mobile forensische Expertenteams angeboten. **Tatsächlich zeigen Bitkom-Zahlen für das Jahr 2024, dass die Ausgaben der deutschen Unternehmen für Dienstleistungen im Bereich Cybersecurity mit 4,4 Milliarden Euro fast genauso hoch sind wie die für Sicherheitssoftware mit 5,2 Milliarden Euro.**

Da sich gerade kleine und mittelgroße Unternehmen meist keine eigene Abteilung für IT-Sicherheit leisten können und der Fachkräftemangel den Aufbau entsprechender Strukturen obendrein erschwert, kaufen viele Unternehmen Sicherheitsleistungen extern ein. Als führendes Bezahlmodell hat sich dabei das As-a-Service-Konzept durchgesetzt. Dabei wird Sicherheitssoftware nicht gekauft, sondern quasi gemietet, meist inklusive der entsprechenden Service- und Beratungsdienstleistungen.

Insgesamt ist der Markt für Cybersicherheit sehr heterogen – und geprägt von vielen spezialisierten Anbietern, die einzelne Teilbereiche abdecken. Dabei spielen auch Start-ups zunehmend eine Rolle, schließlich ist der Innovationsdruck in diesem Sektor angesichts der vielfältigen Bedrohungen hoch. Zwar hat auch Deutschland eine florierende Start-up-Szene, diese ist allerdings bei Weitem kleiner als die in den USA und in Israel, den beiden führenden Ländern.

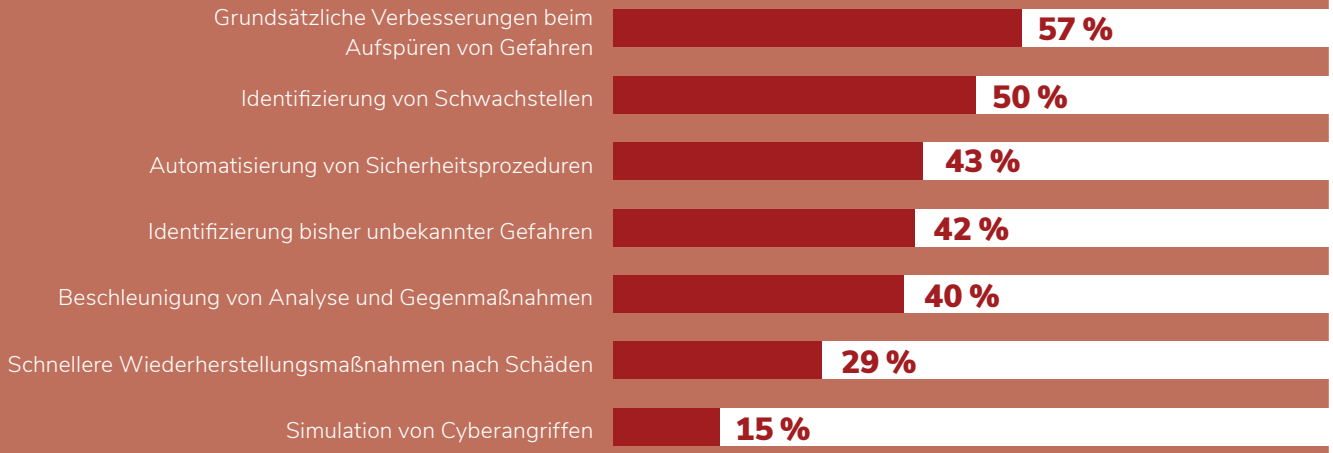
Da viele Unternehmen gerne Leistungen aus einer Hand kaufen und sich ihre Sicherheitsarchitektur nicht aus unterschiedlichen Angeboten zusammenbauen möchten, wird erwartet, dass sich der Markt für Cybersicherheit bald konsolidiert. Tatsächlich gab es weltweit zuletzt einige größere Übernahmen.

TREND #6

Künstliche Intelligenz wird die Cyberabwehr stärken ...

Globale Unternehmensbefragung:
Wie kann künstliche Intelligenz die Cybersicherheit stärken?
Ca. 1.800 befragte Unternehmen aus 15 Ländern, Mehrfachantworten möglich

Quelle: Darktrace



... aber leider auch die Cyberkriminalität

Künstliche Intelligenz (KI) macht IT-Systeme leistungsfähiger und effizienter. Aufgrund ihres enormen Potenzials wird sie zurecht zu den Leittechnologien gezählt, die unsere Zeit nachhaltig prägen und große wirtschaftliche Impulse erzeugen.

KI-Systeme, die eigenständig Lösungswege entwickeln können und denen man nicht mehr alle Einzelschritte per Wenn-dann-Befehl einprogrammieren muss, reduzieren den Arbeitsaufwand für die beteiligten Menschen enorm. Daher ist es nicht verwunderlich, dass KI bereits heute zur Stärkung der Cyberabwehr hinzugezogen wird. Die Einsatzgebiete sind vielfältig: So können KI-Anwendungen beispielsweise als permanenter Stresstest fungieren, der die firmeneigene IT auf Schwachstellen und Sicherheitslücken untersucht. Ferner können sie dabei helfen, Angriffe zu identifizieren, indem sie Anomalien in den verwendeten Codes aufspüren. Auch beim Ver- oder Entschlüsseln sensibler Daten sind KI-Systeme leistungsstarke Hilfsmittel, ebenso beim Wiederherstellen von Daten nach erfolgten Angriffen. Und nicht zuletzt kann die KI menschliches von künstlichem Verhalten unterscheiden. Dies ist beispielsweise bei der Phishing-Abwehr relevant, wenn es um die Frage geht, ob tatsächlich ein Mensch eine E-Mail formuliert hat oder ob es sich um einen Betrugsversuch handelt.

Schon heute basieren komplexe Sicherheitsarchitekturen zumindest zum Teil auf KI-Anwendungen. Und ihre Bedeutung wird stark wachsen, zeigen Prognosen. **So werden dem globalen Markt für KI-Anwendungen im Bereich der Cybersicherheit Zuwachsraten von 20 Prozent pro Jahr vorhergesagt.**

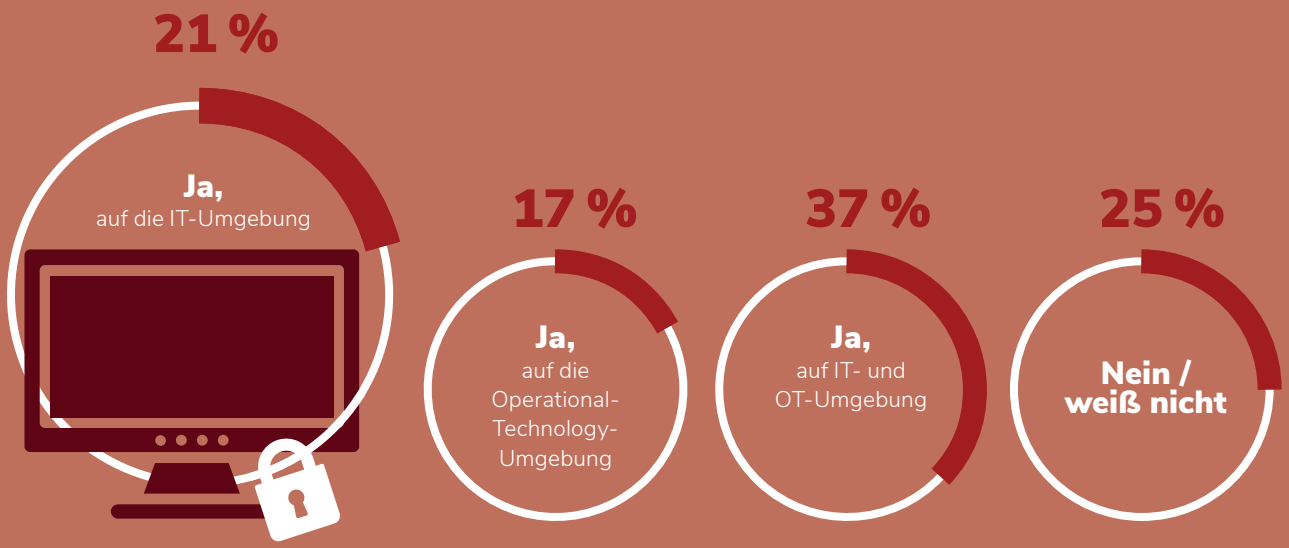
Doch genauso wie der Cybersecurity-Sektor mithilfe von KI aufrüstet, tut dies auch das organisierte Verbrechen. Tatsächlich ist es für potenzielle Kriminelle deutlich einfacher geworden, Angriffe zu starten. Mithilfe KI-basierter Chatbots und Übersetzungstools beispielsweise können in Sekundenschnelle Anschreiben in allen Sprachen formuliert werden. Programmieranwendungen erstellen mit wenigen Klicks eine individuelle Schadsoftware. Und auch das Auffinden von Schwachstellen und potenziellen Einfallstoren in den Systemen der anvisierten Unternehmen wird durch den Einsatz von KI deutlich vereinfacht. Inzwischen existieren im Darknet auch KI-basierte Chatbots, die eigens für die Zwecke der Cyberkriminellen trainiert wurden – wie etwa FraudGPT oder WormGPT.

Nicht zuletzt können auch die von den Unternehmen im Alltag verwendeten KI-Anwendungen ein Einfallstor für Angriffe sein. Beispielsweise können die Modelle mit gezielten Anfragen dazu gebracht werden, jene Daten zu reproduzieren und preiszugeben, mit denen sie einst trainiert wurden. Gerade wenn das System beim Training Zugriff auf sensible Firmendaten hatte, besteht hierin eine große Sicherheitsgefahr. Eine weiteres Einfallstor kann die Sprachsteuerung der Systeme sein: Viele KI-Modelle optimieren sich mithilfe der an sie gerichteten Anfragen. Wenn das System mit manipulativen Anfragen traktiert wird, besteht die Möglichkeit, die Funktionen des Systems gezielt zu verschieben, sodass diese unbemerkt zum Schaden des Unternehmens arbeiten.

Letztlich muss also attestiert werden, dass eine Art Waffengleichheit herrscht, wenn sich sowohl die Cybersicherheit als auch die -kriminalität mit KI-Anwendungen ausstattet. Beim daraus resultierenden Wettlauf wird es mehr und mehr darauf ankommen, wer der Gegenseite einen Schritt voraus ist.

Globale Befragung von Unternehmen aus dem Bereich kritische Infrastruktur:
Hat Ihr Unternehmen im vergangenen Jahr einen Ransomware-Angriff erlebt?
1.100 befragte Unternehmen aus dem Bereich kritische Infrastruktur

Quelle: Claroty



Auch bei Operational Technology wird Cybersecurity immer wichtiger

Unter den Branchen, die ihre Investitionen in die Cybersicherheit zuletzt besonders erhöht haben, steht die Industrie ganz vorn, wie eine Unternehmensbefragung des TÜV-Verbands zeigt. Diese Entwicklung ist nachvollziehbar, da die Folgen von Cyberangriffen in diesem Sektor besonders schwerwiegend sind. Während lahmgelegte Systeme in Dienstleistungsbranchen unschön sind, können sie für das verarbeitende Gewerbe existenzbedrohend sein. In Branchen wie der Stahl- oder der Chemieindustrie können Unterbrechungen sogar zur Zerstörung ganzer Produktionsanlagen führen.

Neben IT-Systemen, die Informationen verarbeiten und speichern, muss in der Industrie auch die Operational Technology (OT) geschützt werden. Diese ist dafür zuständig, physische Prozesse zu lenken – also beispielsweise Maschinen zu steuern. Auch Gebäudeautomatisierungssysteme zählen zur OT, ebenso Mess- und Überwachungsanlagen oder Transportsysteme wie etwa Fließbänder. Während IT und OT früher klar getrennt waren, sind beide Bereiche zunehmend zusammengewachsen. Maschinen werden durch Computer gesteuert und erfassen mittels Sensorik große Mengen an Daten, die in Echtzeit analysiert und zur Prozessoptimierung genutzt werden. Das „Internet der Dinge“ (IoT) hat OT vernetzt und globale Steuerung und Echtzeitanpassungen ermöglicht.

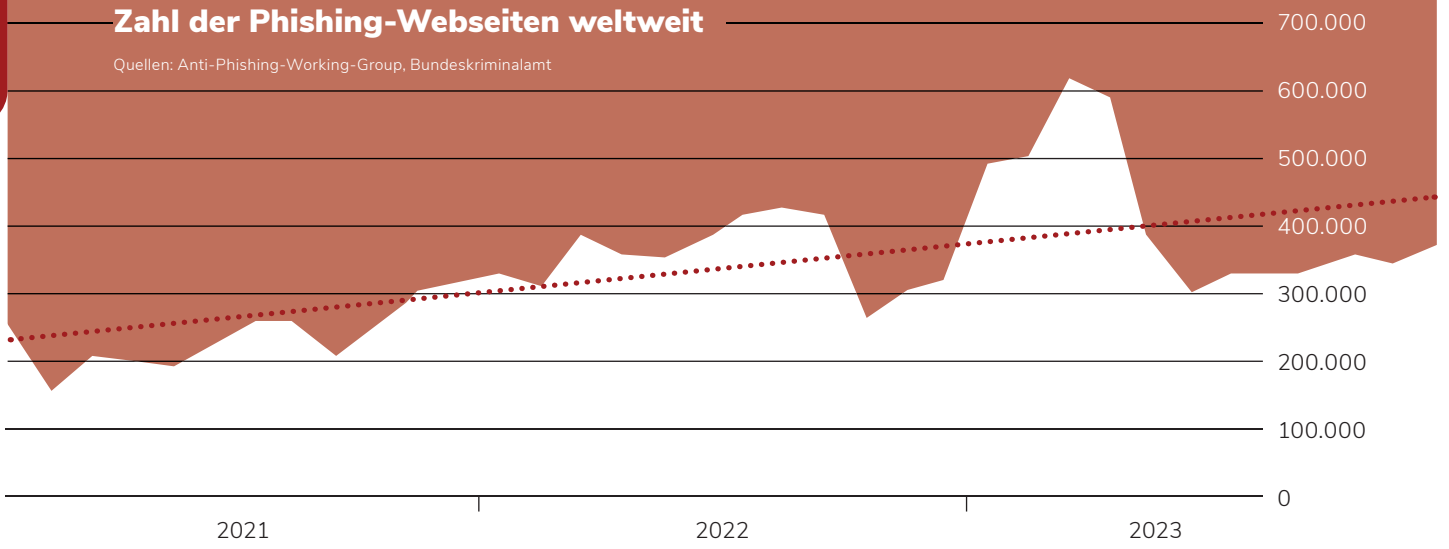
All dies hat enorme Effizienzvorteile gebracht: Produktionsprozesse können über den ganzen Globus hinweg gesteuert werden, und Anpassungen sind in Echtzeit möglich. Die Automation wird dadurch noch weiter verfeinert. Gleichzeitig aber entstehen Risiken, denn auch die OT ist jetzt über die Netzwerke von überallher angreifbar. Weil die Sicherung der OT-Systeme so komplex und aufwendig ist, gilt die IT in der Industrie meist als besser gesichert als die OT. Und das, obwohl dieser Bereich deutlich sensibler ist: Wird ein OT-Steuerungssystem per Cyberangriff manipuliert, kann dies dazu führen, dass unbrauchbare Produkte hergestellt werden. Im schlimmsten Falle kann es zu Unglücken in den Fabriken kommen, die Menschenleben gefährden.

Die Sicherung der OT gegen Cyberangriffe erfordert spezifische Maßnahmen und besonders gut qualifizierte Fachkräfte, die sowohl IT-Sicherheits- als auch Maschinenbaukenntnisse besitzen. Entsprechend groß ist der Fachkräftemangel in diesem Bereich. Zu den Schutzmaßnahmen, die ergriffen werden können, gehört die Segmentierung der Systeme in kleine, abtrennbare Zonen. Bei einem Angriff können auf diese Weise schnell „Wände“ eingezogen werden, die eine Gesamtinfizierung verhindern. Auch Zero-Trust-Strategien setzen sich zunehmend durch. Diese beschränken die Zugriffsrechte der Mitarbeitenden auf das Notwendigste und verlangen eine vollständige Authentifizierung bei jedem Zugriff.

Von zentraler Bedeutung sind auch Notfallpläne und Überwachungsroutinen. Der kontinuierliche Datenaustausch zwischen OT- und IT-Systemen sollte überwacht werden, um Anomalien frühzeitig zu erkennen. **Eine Befragung des Softwareunternehmens Fortinet unter 570 Unternehmen zeigt, dass etwa die Hälfte der größeren Unternehmen, die OT nutzen, bereits ein Operational Technology Security Operations Center (OT SOC) implementiert haben.** Diese Kontrollzentren sind permanent von Fachkräften besetzt und überwachen Sicherheitsbedrohungen in der Betriebstechnologie.

TREND #8

Faktor Mensch:
Kriminelle zielen zunehmend auf unvorsichtige Mitarbeitende



Angriffe zielen oft auf das schwächste Glied in der Kette. Schließlich ist dort ein Durchbruch am einfachsten. Cyberkriminelle gehen beim sogenannten Phishing genau so vor: Sie versuchen, unachtsame oder schlecht geschulte Mitarbeiter:innen zu Fehlern zu bewegen, um darüber einen Zugang zu wichtigen Daten oder Netzwerken zu bekommen. Der Faktor Mensch ist somit ein zentraler Eintrittsvektor für Kriminelle. **Die internationale Anti-Phishing-Working-Group (APWG) verzeichnet pro Monat rund 300.000 Phishing-Kampagnen weltweit. Die Zahl der pro Tag verschickten Phishing-Nachrichten wird sogar auf mehr als drei Milliarden geschätzt.** Einer Umfrage des TÜV-Verbands zufolge entfällt der mit Abstand größte Anteil der Cyberangriffe, die deutsche Unternehmen erleben, auf Phishing.

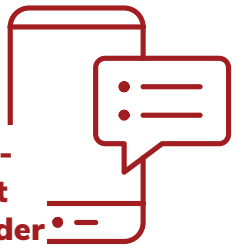
In den meisten Fällen erfolgt die Kontaktaufnahme dabei per E-Mail. Aber auch Angriffe per SMS, Voicemail oder Anruf kommen zunehmend vor. Laut APWG sind Sammlungen von Handynummern im Cybercrimebereich zu einem wertvollen Gut geworden, da sie als Angriffsweg begehrt sind.

Ziel der Phishing-Angriffe ist es, die Zielpersonen dazu zu bringen, Daten – wie Benutzernamen, Passwörter oder Kontodaten – preiszugeben oder sogar direkt Zahlungen zu tätigen. Dafür werden Anschreiben formuliert, die echt wirken und dringend klingen sollen – um die Zielperson zur Antwort zu motivieren. Dabei wird beispielsweise nach Ablageorten für Paketzustellungen gefragt oder darum gebeten, Rechnungen zu autorisieren. Es werden Software- oder Netzwerkfehler vorgetäuscht oder Links zu Voicemail-Downloads verschickt. Bei all dem versuchen die Angreifer:innen, authentisch zu wirken. Optisch und sprachlich wirken die Anfragen wie Mails von großen Konzernen – oder von anderen Abteilungen im eigenen Haus. Oftmals wird auch versucht, Informationen über das Zielunternehmen einzustreuen, um noch echter zu wirken. Zwar fielen viele Angriffsversuche in der Vergangenheit durch Rechtschreib- und Grammatikfehler auf. Die Möglichkeiten der künstlichen Intelligenz und ihrer Übersetzungs- und Formulierungstools aber werden dieses Phänomen voraussichtlich bald beenden.

Die Ziele, die die Kriminellen verfolgen, sind unterschiedlich. Es kann darum gehen, Gelder von Konten abzuzweigen oder schlichtweg zu erpressen. Auch Spionage kann ein Ziel sein, ebenso Vandalismus. Gelingt es, Zugangsdaten zu Systemen zu erbeuten, kann auf diesem Weg Schadsoftware unterschiedlichster Art installiert werden.

Mithilfe von effektiver Software-Schutzschirme können Unternehmen einen Großteil der eingehenden Phishing-Angriffe direkt herausfiltern und unschädlich machen. Dennoch gelingt es den Kriminellen oft genug, durch die Spamfilter zu schlüpfen. In diesem Fall kommt es darauf an, dass die Mitarbeiter:innen wachsam bleiben und lernen, falsche von echten Nachrichten zu unterscheiden. Die Unternehmen setzen hierbei zunehmend auf sogenannte Awareness-Schulungen – auch um eine Kultur der Verantwortungsübernahme zu etablieren. Einige firmeninterne Mailsysteme sind bereits mit Buttons ausgestattet, über die Mitarbeiter:innen verdächtig erscheinende Mails testen können.

Eine Herausforderung für die IT-Sicherheit ist der verstärkte Trend zur Arbeit im Homeoffice. Die Netzwerke dort sind schwerer zu schützen. Ebenso kann es vorkommen, dass Mitarbeiter:innen schlecht gesicherte Privatgeräte nutzen.



Kriminelle versenden Phishing-Nachrichten zunehmend direkt auf Mobiltelefone – per SMS oder über andere Messengerdienste. Der Wert der erbeuteten Handynummern steigt, zeigen Studien.

TREND #9

Die Maschen wandeln sich:

Neue Tricks werden entwickelt, alte fallengelassen

Unternehmensbefragung in Deutschland:
Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten zwölf Monate in Ihrem Unternehmen einen Schaden verursacht?
> 1.000 befragte Unternehmen in Deutschland

Quelle: Bitkom

	2021	2023
Distributed Denial of Service (DDoS)	27	12
Spoofing	20	14
Infizierung mit Schadsoftware bzw. Malware	31	28
Ransomware	18	23
Angriffe auf Passwörter	18	29
Phishing	18	31

Wirtschaftskriminelle und die, die sie bekämpfen, befinden sich stets in einem Wettlauf. Die Täter:innen entwickeln immer wieder neue Tricks und neue Maschen, mit denen sie ihre Opfer überrumpeln und die Ermittlungsbehörden abhängen können. Letztere versuchen, Schritt zu halten, indem sie kriminelle Aktionen antizipieren, Geschäftsmodelle zerstören und Opfer schulen.

Im Bereich der Cyberkriminalität ist es nicht anders. Auch im Internet tummeln sich kriminelle Banden, die die modernen Kommunikationswege für Betrug, Diebstahl, Erpressung, Spionage, politische Sabotage oder Ähnliches zu nutzen versuchen. Immer wenn neue Angebote und Technologien auf den Markt kommen, entstehen auch darauf abzielende kriminelle Aktivitäten. Mit dem Aufstieg des Onlinebankings rund um die Jahrtausendwende beispielsweise begannen auch die Versuche, auf illegalem Wege an die entsprechenden Zugangsdaten der Nutzer:innen zu gelangen.

Tatsächlich entstehen ständig neue Trends. Die klassischen Viren, die sich selbst verbreiten und wahllos Systeme lahmlegen, dabei aber eher dem Vandalismus und nicht dem Verbrechen mit kommerziellem Hintergrund zuzurechnen sind, stehen heutzutage nicht mehr so stark im Fokus. Andere Ansätze dagegen haben einen großen Aufstieg erlebt:

- **Malware:** Die bekannteste Form solcher Schadprogramme ist zurzeit die Ransomware. Entsprechende Programme dringen in das System eines Unternehmens ein und verschlüsseln dort Daten oder sperren Zugänge. Für die Beseitigung der Zerstörung wird ein Lösegeld gefordert, das in Form von Kryptowährungen über dunkle Kanäle zu zahlen ist. **Die Gesamtkosten, die betroffenen Unternehmen für die Behebung der Ransomware-Schäden im Schnitt entstehen, sind nach Angaben des Sicherheitsanbieters Sophos zwischen 2021 und 2024 um die Hälfte angestiegen.**

Allerdings nimmt der Anteil der Unternehmen, die tatsächlich Lösegelder zahlen, stark ab – ein Zeichen dafür, dass das Geschäftsmodell an seine Grenzen kommt. Andere Malware-Ansätze sind Trojaner oder Spyware. Entsprechende Programme sammeln Daten über die Nutzer:innen oder verschicken gezielt Daten aus deren Netzwerken.

- **Phishing:** Hierbei wird versucht, Personen zur Preisgabe sensibler Daten zu verleiten – wie Zugangsdaten zum Firmennetz, zum Bankkonto oder Ähnlichem. In der Regel gelingt dies durch Täuschung bei der Kontaktaufnahme und eine vermeintliche Eiligkeit: Dabei wird so getan, als komme eine E-Mail, ein Anruf oder eine SMS von Geschäftspartnern, von Vorgesetzten oder von großen Unternehmen. Oftmals werden einzelne Personen gezielt anvisiert, beispielsweise CEOs.

- **Distributed Denial of Service (DDoS):** Hier wird versucht, Server mit so vielen Anfragen zu traktieren, dass sie nicht mehr funktionsfähig sind. Oftmals werden dafür andere Server genutzt, auf denen zuvor entsprechende Bots eingepflanzt wurden. Der DDoS-Ansatz wird im Besonderen von politisch motivierten Cyberkriminellen genutzt und zielt dann oftmals auf die Webseiten von Behörden ab. Doch können damit auch kommerzielle Interessen verfolgt werden – etwa das Ausschalten von Konkurrenz oder das Erpressen von Lösegeldern.

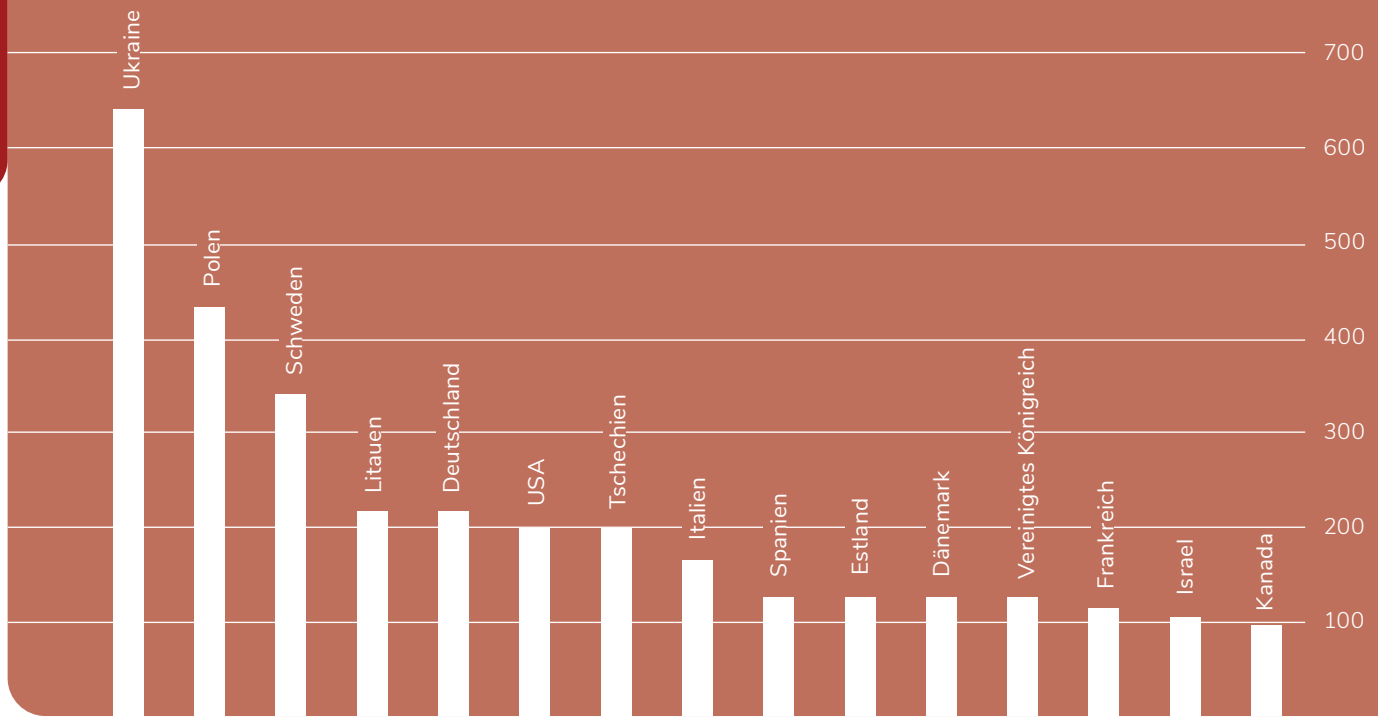
Zu beachten ist, dass oftmals unterschiedliche Ansätze miteinander kombiniert werden, um zum Ziel zu gelangen. Es wird erwartet, dass kriminelle Banden künftig verstärkt auf Deepfakes und biometrische Datenmanipulationen zurückgreifen werden – etwa, um sich Zugriffe zu verschaffen, die durch Fingerabdrücke oder Iriserkennung gesichert sind.

TREND #10

Geopolitische Streitigkeiten finden zunehmend im Internet statt

Zahl der Angriffe prorussischer Hacktivismus-Gruppen
2023

Quelle: Orange Security



Länder, die sich feindlich gegenüberstehen, führen oftmals eine Art Kalten Krieg. Sie bekämpfen sich zwar nicht mit Waffen auf einem Schlachtfeld. Auf anderen Feldern aber gibt es dennoch Auseinandersetzungen: Man versucht, den anderen mit Propagandaoffensiven zu diskreditieren – oder seine ökonomische Stärke mithilfe von Wirtschaftsspionage, Zöllen oder anderen Handelsbarrieren zu schwächen.

Heutzutage finden entsprechende Scharmützel zunehmend im Internet statt. Dabei ist oftmals von einer Cyberfront die Rede. Trollarmeen verbreiten dann Fake-News auf Social-Media-Plattformen, während Hackergruppen die IT-Infrastrukturen der Gegenseite angreifen – beispielsweise mithilfe von DDoS-Angriffen, die darauf abzielen, wichtige Server mit einer gezielten Flut von Anfragen zu überfordern und lahmzulegen. Oftmals sind die agierenden Gruppen zwar selbstständig und verfolgen eigene politische oder religiöse Ziele. Viele von ihnen werden aber zumindest mittelbar von staatlicher Seite gelenkt und sollen nur den Anschein erwecken, eigenständig zu sein. Die Gruppen verfügen meist über ein weltweites Netzwerk von Unterstützer:innen, die über Messengerdienste Instruktionen erhalten und somit dezentral Angriffe ausführen können.

Meist versuchen die Gruppen, wichtige Server gezielt mit Anfragen zu überfordern und lahmzulegen – etwa die von Behörden oder Energieunternehmen.

Auch wenn die Unternehmen nicht das eigentliche Ziel der Aktionen sind, entsteht der Schaden oftmals dennoch bei ihnen. Denn im Visier der DDoS-Attacken stehen nicht nur Behörden, sondern auch Banken und andere Finanzunternehmen sowie zentrale Wirtschaftszweige wie etwa die Autoindustrie. Auch Unternehmen, die unmittelbar oder mittelbar für wichtige Infrastrukturen zuständig sind, werden angegriffen – so etwa solche, die Energienetze betreiben, Strom herstellen oder auch Flughäfen. Dabei wird darauf abgezielt, das öffentliche Leben zumindest zeitweise zu behindern.

Ein starker Anstieg der Zahl politisch motivierter Fälle von Cyberkriminalität wurde zuletzt im Zuge des Krieges zwischen Israel und der Hamas festgestellt. Gerade Israel musste großflächig Cyberangriffe aus der ganzen Welt abwehren. Auch während der Weltklimakonferenz in Dubai kam es zu vermehrten Vorkommnissen. So wurden Webseiten von Umweltgruppen gezielt lahmgelegt.

Die größte Menge sogenannter Hacktivismus-Attacken stand zuletzt im Zusammenhang mit dem Krieg Russlands gegen die Ukraine. Gruppen, die mit Russland in Verbindung gebracht werden, zielten dabei vor allem auf jene westlichen Länder, die sich geografisch in der Nähe der Ukraine befinden und diese offen unterstützen, sei es mit Waffen oder mit Geld. Dazu zählen Polen, Schweden, Litauen, Deutschland und Tschechien. Die mit den Angriffen einhergehende Faketivism-Offensiven zielen darauf ab, die sozialen Medien mit falschen Nachrichten zu fluten, um so die öffentliche Meinung zu beeinflussen und die Regierungen von ihrem harten Kurs gegenüber Russland abzubringen. Die Machthaber in Moskau nutzen dabei aus, dass Regierungen in den demokratischen Ländern keine direkte Kontrolle über die Medienlandschaft und die sozialen Medien haben.

Eine Analyse des Unternehmens Orange Cyberdefense zeigt, dass Europa inzwischen zum entscheidenden Schauplatz der Hacktivismus-Scharmützel geworden ist. **Demnach finden 85 Prozent aller Attacken weltweit hier statt.**

Neue Bedrohungen, neue Versicherungen

Deutsche Versicherungen:
Bruttobeitragseinnahmen durch Cyberversicherungen

Quellen: Bafin, Gothaer

2020	2021	2022
287 Mio. €	**446 Mio. €**	**699 Mio. €**

Umfragen zeigen, dass deutsche Unternehmen in möglichen Cyberangriffen die größte Gefahr für den eigenen Betrieb sehen – weit vor Einbrüchen, Lieferkettenunterbrechungen, Bränden oder Naturkatastrophen. Vor diesem Hintergrund ist es wenig verwunderlich, dass sich die Unternehmen gegen Cyberrisiken schützen möchten. Dies tun sie nicht nur, indem sie in zusätzliche Sicherheitsmaßnahmen für ihre Systeme investieren und so die Wahrscheinlichkeit von Schadensfällen reduzieren, sondern auch, indem sie sich versichern, also indem sie das Ausmaß drohender Schäden reduzieren. Gerade für kleine und mittlere Unternehmen (KMU), die selbst keine große Abteilung für IT-Sicherheit aufbauen können, dürften entsprechende Angebote interessant sein.

Tatsächlich wächst der – noch recht junge – Markt für Cyberversicherungen derzeit kräftig. **Zwar haben einer Umfrage der Gothaer zufolge im Jahr 2024 erst 25 Prozent aller KMU in Deutschland eine entsprechende Cyberpolice abgeschlossen. Im Jahr 2021 waren es demnach allerdings nur 16 Prozent.** Daten aus einer Anbieterbefragung der Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin) zeigen, dass die Umsätze bei Cyberversicherungen zuletzt stark gestiegen sind. So betrugen die Bruttobeitragseinnahmen der deutschen Versicherer im Jahr 2022 fast 700 Millionen Euro, während es im Jahr 2020 nicht einmal 300 Millionen waren. Die Zahlen beziehen sich dabei auf das sogenannte Stand-alone-Geschäft, also auf Versicherungspolicen, die ausschließlich Cyberrisiken absichern. Umfassende Versicherungspakete, die darüber hinaus weitere Risiken abdecken, sind darin noch nicht berücksichtigt. Tatsächlich aber wird der Schutz vor Schäden aus cyberkriminellen Angriffen zunehmend in entsprechende Bündel integriert.

Die Leistungsspektren der abgeschlossenen Cyberversicherungen sind sehr heterogen – je nachdem, welche Schadenssummen abgedeckt wurden und welche Zusatzleistungen inkludiert sind. Zu den Bausteinen gehört beispielsweise die Erstattung von Kosten, die für die Wiederherstellung beschädigter Datenbanken oder bei Geschäftsunterbrechungen in Form von Umsatzausfällen anfallen. Mitunter werden auch Kosten abgesichert, die durch die Verletzung von Datenschutzregularien entstehen.

Nicht zuletzt enthalten viele Policen zudem Hilfs- und Beratungsangebote für den Schadensfall, etwa in Form forensisch oder juristisch geschulter Hilfsteams oder von PR-Expert:innen, die sich um Reputationsschäden kümmern. Bei all dem können sich die Leistungsspektren von Versicherungen und Cybersecurity-as-a-Service-Anbietern überschneiden. Allerdings kooperieren diese ohnehin schon oft, weil sie wechselseitig vom Know-how der anderen Seite profitieren.

Die Bafin-Befragung zeigt, dass das Geschäft mit Cyberversicherungen für die Assekuranzen bisher meist noch nicht auskömmlich war. Ein Grund dafür liegt in den recht hohen Aufwendungen, die den Anbietern infolge der wachsenden Cyberkriminalität bereits entstanden sind. Zum anderen sind die Angebote bisher kaum standardisiert, was einen erhöhten Verwaltungsaufwand bedeutet. Angesichts der Tatsache, dass die Bedarfe der Unternehmen hinsichtlich ihres Versicherungsschutzes sehr individuell ausfallen, wird sich daran nur bedingt etwas ändern. Zumindest im Bereich der Basisangebote für kleinere Unternehmen könnte es aber zu Standardisierungen kommen.

Auch kleine und mittlere Unternehmen versichern sich zunehmend gegen Cyberrisiken. Der Anteil liegt allerdings erst bei einem Viertel, zeigt eine Umfrage der Gothaer.

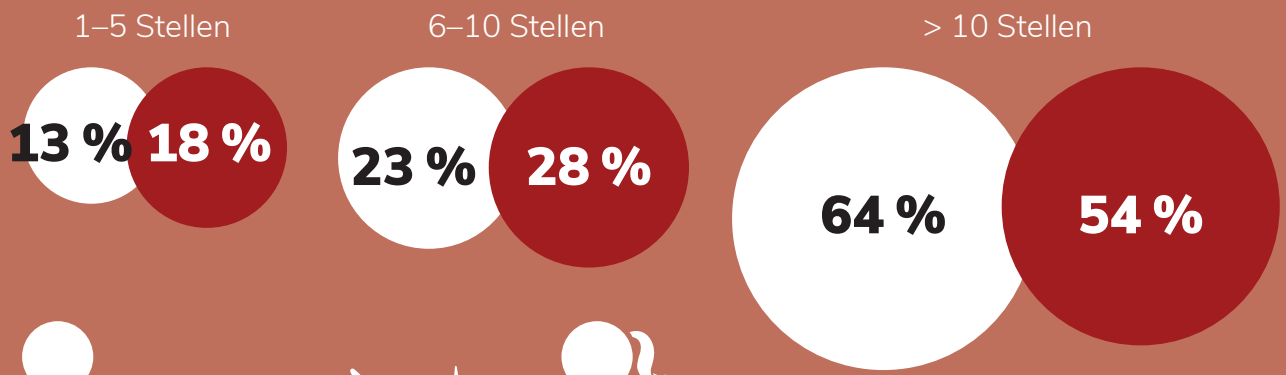
TREND #12

Der Fachkräftemangel im Bereich Cybersecurity wird zum Problem

Globale Unternehmensbefragung:
Wie viele unbesetzte Stellen haben Sie zurzeit im Bereich Cybersecurity?
> 8.000 befragte Unternehmen aus 30 unterschiedlichen Ländern

Quellen: Cisco, Bitkom

Großunternehmen (> 1.000 Mitarbeitende)
Mittelstand (250–1.000 Mitarbeitende)



Schon heute haben Unternehmen große Probleme, geeignete Fachkräfte für ihre IT-Abteilungen zu finden. Laut einer Bitkom-Umfrage unter rund 800 deutschen Unternehmen bleiben vier von zehn Stellen hierzulande länger als ein halbes Jahr unbesetzt. In der Summe geht der Verband davon aus, dass von knapp 1,3 Millionen IT-Stellen in Deutschland zurzeit zwölf Prozent unbesetzt sind, also rund 150.000. Bis 2040 könnte sich diese Lücke sogar vervierfachen.

Umfragen zeigen, dass der Fachkräftemangel ausgerechnet im Bereich der IT-Sicherheit am höchsten ist. Dies verwundert nicht, schließlich steigt die Zahl der Cyberangriffe und der damit verbundenen Schäden an. Gleichzeitig schreitet die Digitalisierung voran, weswegen es mehr und mehr Systeme gibt, die geschützt werden müssen. Vor allem die Finanz- und Versicherungsbranche klagt über Probleme bei der Stellenbesetzung, wie eine Umfrage des Softwareherstellers Sophos zeigt.

Ein Grund für den besonderen Mangel im Bereich der IT-Sicherheit ist die Komplexität der dazugehörigen Aufgaben. Es werden hier besonders gut ausgebildete Expert:innen gebraucht, doch genau die sind besonders rar. Zwar ist die Zahl der Studienabsolvent:innen im Fach Informatik hierzulande im zurückliegenden Jahrzehnt um nahezu die Hälfte angewachsen. Auch gibt es inzwischen zahlreiche berufsbegleitende Fortbildungen und Aufbaustudiengänge, die Quereinsteiger:innen den Weg in das Berufsfeld ermöglichen. Doch scheint das bei Weitem nicht zu reichen. Selbst bei den deutschen Bundesbehörden gelten rund 15 Prozent der Stellen im Bereich der Cybersicherheit als unbesetzt. Bei einer Umfrage des TÜV-Verbands unter rund 500 deutschen Unternehmen gab die Hälfte an, bei der IT-Sicherheit bereits auf externe Hilfe angewiesen zu sein. Auch dies ist ein Grund, warum die Branche für Sicherheitsdienstleistungen – oftmals unter dem Namen Cybersecurity-as-a-Service bekannt – ein hohes Wachstum verzeichnet.

Einer Bitkom-Schätzung zufolge wird die Zahl der Informatiker:innen in Deutschland im Jahr 2030 bei 1,2 Millionen liegen, die Zahl der Stellen aber bei 1,5 Millionen.

Die gezielte Anwerbung von Fachkräften aus dem Ausland kann helfen, die Lücke auf dem Arbeitsmarkt für IT-Sicherheit zu schließen. Allerdings werden entsprechende Expert:innen auf der ganzen Welt gesucht. Die Lücke auf dem globalen Arbeitsmarkt ist enorm: Schätzungen der Non-Profit-Organisation ISC2 zufolge arbeiteten im Jahr 2023 rund 5,5 Millionen Menschen weltweit im Bereich der Cybersicherheit. Im Vergleich zum Jahr 2019 stellt diese Zahl tatsächlich eine Verdopplung dar. Doch eigentlich müsste die Zahl der Jobs noch deutlich stärker steigen. Aber es fehlen die Bewerber:innen. ISC2 schätzt die Lücke zwischen Arbeitsangebot und -nachfrage inzwischen auf vier Millionen.

Der Mangel an Fachkräften führt dazu, dass die wenigen verfügbaren Fachkräfte hohe Gehälter aushandeln können. **Laut gehalt.de verdient fast jede vierte Sicherheitsfachkraft mehr als 100.000 Euro im Jahr.** Tatsächlich leiden viele Unternehmen bereits unter der großen Verhandlungsmacht der Kandidat:innen: Bei der Bitkom-Umfrage wurden zu hohe Gehaltsforderungen als Hauptgrund dafür genannt, warum Unternehmen ihre offenen Stellen nicht besetzen können.

IMPRESSUM

THE MISSION – Cyber Security ist ein Projekt in Zusammenarbeit mit:

Montan-Stiftung-Saar

SIEMENS energy

THALES
Building a future we can all trust

DUSSMANN GROUP

WSL Patent Marke Design

e:fs TechHub GmbH

Das **Handelsblatt Research Institute** (HRI) ist ein unabhängiges Forschungsinstitut unter dem Dach der Handelsblatt Media Group. Es schreibt im Auftrag von Kundinnen und Kunden wie Unternehmen, Finanzinvestoren, Verbänden, Stiftungen und staatlichen Stellen wissenschaftliche Studien. Dabei verbindet es die wissenschaftliche Kompetenz des 20-köpfigen Teams aus Ökonom:innen, Sozial- und Naturwissenschaftler:innen sowie Historiker:innen mit journalistischer Kompetenz in der Aufbereitung der Ergebnisse. Es arbeitet mit einem Netzwerk von Partner:innen sowie Spezialist:innen zusammen. Daneben bietet das Handelsblatt Research Institute Desk-Research, Wettbewerbsanalysen und Marktforschung an.

Konzept, Recherche und Gestaltung:
Handelsblatt GmbH
Handelsblatt Research Institute
Toulouser Allee 27, 40211 Düsseldorf
www.handelsblatt-research.com

Projektmanagement: Dr. Jan Kleibrink
Text: Dr. Hans Christian Müller
Layout: Christina Wiesen, Kristine Reimann
Redaktionsschluss: April 2024

Bilder: Envato, Flaticon, Freepik

THE MISSION ist eine Initiative von:

FUTURY BAIN & COMPANY SCHWARZ | LIDL Kaufland SCHWARZ Produktion prezero schwarz digits

Handelsblatt MEDIA GROUP SOLUTIONS