sosafe

Human Risk Review 2023

Die europäische Cyber-Bedrohungslage:
Experteneinblicke und Strategien

> Wir müssen Cyber Security näher an die Menschen bringen, Security Awareness in alle Lebensbereiche ausweiten und weiter stärken, und Cyber und Business als ineinander verwobene Themenbereiche verstehen.

Dr. Niklas Hellemann
CEO SoSafe

Editorial

Eigentlich muss man es nicht noch einmal betonen und doch war es nie treffender als heute: Die Cyber-Bedrohungslage ist angespannt und das Innovationstempo zieht weiter massiv an.

Was wir in den vergangenen Jahren und vor allem 2022 beobachtet haben, war auf vielen Ebenen eine Entwicklung im Schnelldurchlauf: Globale Krisen, geopolitische Herausforderungen und technologische Disruption haben unsere Welt instabiler gemacht – und zudem eine größere Angriffsfläche und neue Möglichkeiten für Cyberkriminelle geschaffen, ihre Methoden und Geschäftsmodelle weiter zu professionalisieren. Gleichzeitig haben technologische Entwicklungen wie "Large-Language-Modelle" die Demokratisierung der Cyberkriminalität vorangetrieben und sie für die breite Masse zugänglich gemacht. Das Ergebnis: Wir sehen uns heute einer endlosen

Menge an potenziellen Angreifenden gegenübergestellt, die über die nötigen Tools verfügen, um nicht nur die Reichweite, sondern auch die Erfolgschancen ihrer Cyberattacken zu maximieren.

Wir bei SoSafe warnen bereits seit Jahren davor, dass Cyberkriminelle in naher Zukunft ausgefeilte KI-basierte Taktiken wie Deepfake-Phishing oder Voice-Cloning für groß angelegte Angriffe einsetzen könnten. Mit dem Aufkommen öffentlich zugänglicher generativer KI-Tools wird dieses Szenario nun immer konkreter. In einer kleinen Studie fanden wir kürzlich heraus, dass Phishing-Mails mit ChatGPT bereits 40 Prozent schneller erstellt werden können – ein Vorgeschmack darauf, wie Cyberkriminelle ihr Geschäft weiter skalieren werden.

Ich denke, wir sind uns alle einig, dass Informationssicherheit kein Bereich ist, in dem wir irgendwann stehen bleiben können. Sicherheitsmaßnahmen müssen ständig weiterentwickelt und angepasst werden. Die Einführung neuer Technologien zum Schutz vor innovativen Angriffsmethoden ist eine Seite der Medaille. Doch wenn wir uns einer Sache sicher sein können, dann, dass Cyberkriminelle unaufhörlich (und oft mit Erfolg) nach Wegen suchen werden, selbst die fortschrittlichsten technologischen Schutzbarrieren zu durchbrechen. Dabei sind sie sich nur allzu bewusst, dass ihre größten Erfolgschancen in der emotionalen Manipulation der Menschen hinter der Technik liegen – wie die großen Datenschutzverstöße bei Uber und Reddit erst vor kurzem bewiesen haben. Social Engineering ist und bleibt ein Dauerbrenner. Die gute Nachricht ist aber, dass wir dieses Sicherheitsrisiko mit den richtigen Maßnahmen effektiv reduzieren können.

Wenig überraschend hat bei den für diesen Report befragten Organisationen deshalb Awareness-Building im Bereich Informationssicherheit oberste Priorität. Ob sie jedoch die nötigen Ressourcen in ihre Sicherheitskultur investieren können, wird maßgeblich von einem Faktor beeinflusst: inwieweit sich die oberste Führungsetage der Cyberrisiken bewusst ist. In gewisser Hinsicht ist genau das einer der Gründe, weshalb wir unseren jährlichen Human Risk Review veröffentlichen. Wir sind überzeugt, dass unsere Daten einen neuen Blickwinkel auf die Thematik ermöglichen. Wir teilen im Report Einblicke aus erster Hand zu aktuellen Cybercrime-Taktiken und der Rolle, die der Faktor Mensch dabei spielt. So möchten wir Organisationen nützliche Ressourcen an die Hand geben, die ihnen helfen, den Dialog rund um Security und Awareness anzustoßen.

Eine detaillierte Analyse unserer Plattform-Daten, Einblicke aus einer umfangreichen Studie unter europäischen Sicherheitsexpertinnen und -experten und Gespräche mit Security-Führungskräften verschiedener Branchen – alles führt uns zum selben Ergebnis: Wir müssen Cyber Security näher an die Menschen bringen, Security Awareness in alle Lebensbereiche ausweiten und weiter stärken, und Cyber und Business als ineinander verwobene Themenbereiche verstehen. Nur so können wir uns dem Miliarden-Problem Cybercrime stellen. So rasant wie sich die Cyber-Bedrohungslage weiterentwickelt, so rasant müssen wir uns den neuen Gegebenheiten anpassen.

Dr. Niklas Hellemann
CEO SoSafe

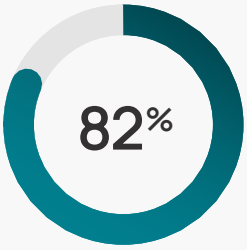
Inhalte

Executive Summary

Die Cyber-Bedrohungslage ist angespannt.

Jede 2.

Organisation wurde in den vergangenen 3 Jahren Opfer einer erfolgreichen Cyberattacke.



der Organisationen gehen nicht von einer Entspannung der Lage im kommenden Jahr aus.

> Wir leben im Zeitalter der Digitalisierung. Nahezu alles ist mit allem verknüpft – also kann auch alles gehackt werden.

Dr. Katrin Suder
Strategieexpertin (digitale Technologien, Wirtschaft & Politik)

Die **Top 3** erfolgreichsten Angriffstaktiken

1. Malware
2. Phishing
3. Ransomware

Die **Top 3** Zielabteilungen bei Angriffen

1. IT
2. Finance
3. Security

Und Cybercrime boomt – einige der Gründe dafür:

3 von 4

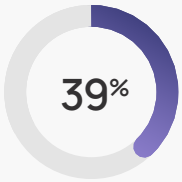
Sicherheitsverantwortlichen sagen, dass sich das Cyberrisiko ihrer Organisation aufgrund von **Geopolitik**, **KI** und **Remote Work** erhöht hat.

> Das zugrunde liegende Problem, das wir derzeit in der Cyber-Security-Industrie überall beobachten können: Burnout. Wir haben zu viele Daten, zu viele Fälle, aber nicht genug Zeit.

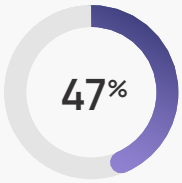
Stéphane Duguin
CEO CyberPeace Institute

8 von 10

Sicherheitsverantwortlichen sagen, dass die Sicherheit ihrer Organisation **zunehmend von der Sicherheit ihrer Partner und Lieferanten abhängt**.



Im Falle einer Ransomware-Attacke haben **ein Drittel aller Unternehmen** das Lösegeld gezahlt.



Bei kleineren Unternehmen war es sogar **fast die Hälfte**.

Die „Dry-Powder-Hypothese“ im Bereich Cybercrime

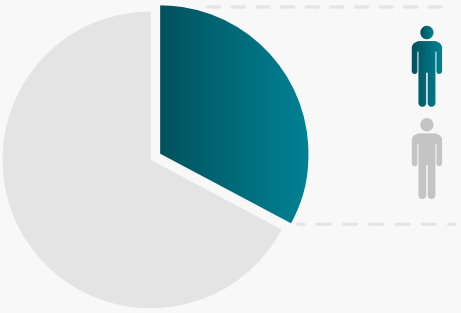
> Fortschrittliche Technologien wie Voice-Cloning stehen Cyberkriminellen bereits seit geraumer Zeit zur Verfügung. Trotzdem kam es bisher nicht zu breit angelegten Social-Engineering-Angriffen dieser Art. Eine Erklärung dafür: Simplere Methoden führen noch immer zum Erfolg. In Anbetracht der Datenlecks von Large Language Models und des rasanten Fortschritts im Bereich generativer KI wird sich das aber mit hoher Wahrscheinlichkeit bald ändern.

Dr. Niklas Hellemann
CEO SoSafe

80 % der Security-Verantwortlichen nehmen Social Engineering und Phishing als große Gefahr für ihre Organisation wahr:

Jeder 3.

User klickt auf schädliche Inhalte in Phishing-Mails, und



jeder 2.

User davon gibt sensible Informationen weiter.

In einer sich verschärfenden Cybercrime-Lage sind Social-Engineering-Techniken, die

negative Emotionen

hervorrufen, immer erfolgreicher.

> Schadhafte E-Mails erreichen uns in immer kürzeren Intervallen und die einzelnen Wellen werden wesentlich heftiger.

Sascha Czech
CSO Uniklinikum Münster

> Im Homeoffice sind viele User weniger fokussiert – es ist eine lockerere Umgebung. Man mischt vielleicht private Aktivitäten zwischen den Arbeitsalltag. Das führt zu Unaufmerksamkeit.

Dr. Stefan Lüders
Computer Security Officer CERN

Digital Natives
klicken mit einer

↗ 65 %

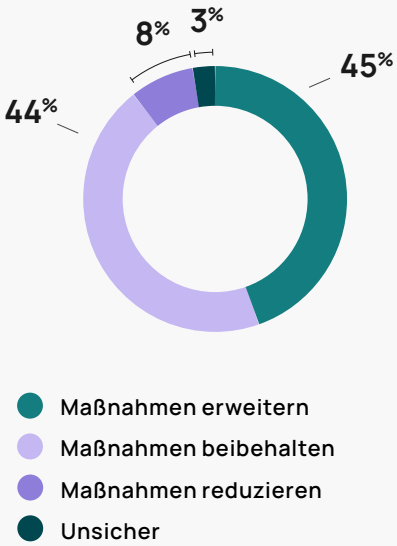
höheren Wahrscheinlichkeit auf Phishing-Mails als ältere User.

Ausblick: Wie gut sind Organisationen vorbereitet?

> Oft höre ich das Lebensmotto heraus: Es ist noch immer gut gegangen. Wenn es dann aber doch zu einem Angriff kommt, wird das mitunter sehr teuer.

Thomas Tschersich
CSO Deutsche Telekom

9 von 10 Organisationen planen, ihre Awareness-Maßnahmen im kommenden Jahr beizubehalten oder zu erweitern.



Die **Top 3** Security-Prioritäten in Organisationen

1. Die Security Awareness der Mitarbeitenden erhöhen
2. Identity und Access Management verbessern
3. Hybride Arbeitsmodelle besser absichern

> Alles das, was ich durch Awareness von Mitarbeitern abdecken kann, macht mich als Unternehmen resilienter. Ich spare so Geld, Zeit und natürlich auch Nerven und Risiko.

Thomas Schumacher
Managing Director Accenture Security

Die **effektivsten Hebel** zur Steigerung der Security Awareness laut Sicherheitsverantwortlichen:

1. Awareness-Maßnahmen via Kommunikationstools
2. Personalisierte Lernmöglichkeiten
3. Customization des Awareness-Programms

Methodik und Datenquellen

Umfrage unter Sicherheitsverantwortlichen

Für diese Umfrage zum Stand der Cybersicherheit in Organisationen haben wir uns mit dem in London ansässigen unabhängigen Marktforschungsunternehmen Censuswide zusammengetan. Dabei befragten wir im Februar 2023 mehr als 1.000 Sicherheitsexpertinnen und -experten aus sechs europäischen Ländern (Großbritannien, Deutschland, Österreich, Schweiz, Frankreich und Niederlande). Die Größe der Organisationen aus verschiedensten Branchen reichte von zehn bis über 5.000 Mitarbeitende.

Daten der SoSafe-Plattform

Mit dem Ziel, verschiedene Social-Engineering-Taktiken zu untersuchen, analysierten wir anonymisiert mehr als 8,4 Millionen Phishing-Simulationsmails von 3.000 Kundenorganisationen der SoSafe Awareness-Plattform. Dadurch erhielten wir exklusive Einblicke zum menschlichen Risiko in Organisationen und zum Erfolg verschiedener Angriffsmethoden.

Phish Test

Im Rahmen dieser Studie zum allgemeinen Phishing-Bewusstsein wurden 2022 über 9.000 Phishing-Simulationsmails an angemeldete User geschickt. Dabei erhielten die Teilnehmenden innerhalb von einer Woche drei realitätsnah simulierte Phishing-Mails (mit einem moderaten Komplexitätsgrad) mit dem Ziel, die vermeintlich schädlichen E-Mails zu erkennen. Teilnehmende, die auf eine E-Mail klickten, wurden zu kontextbezogenen Lerninhalten weitergeleitet.

Cybercrime ist das Geschäftsrisiko Nr. 1 – das hat der Faktor Mensch damit zu tun

Geschäftsrisiko
Nr. 1

Cybergefahren sind das Top-Risiko für Unternehmen.

Quelle: Allianz Risk Barometer 2023 [1]

4,35 Mio.
USD

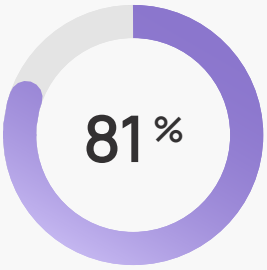
Durchschnittliche Gesamtkosten eines Datenschutzverstoßes.

Quelle: IBM Kosten eines Datenschutzverstoßes 2022 [2]

Sicherheitsverantwortliche sind sich einig: Cyberkriminalität gehört zu den größten Risiken für Organisationen weltweit. Seit Jahren führen uns Berichte wie das Allianz Risk Barometer oder der IBM-Report „Kosten eines Datenschutzverstoßes" die schockierenden Folgen vor Augen, die mangelnde Sicherheitsvorkehrungen haben können – nicht nur aus finanzieller Sicht, sondern auch für den Ruf der Organisationen. Geopolitische Herausforderungen, künstliche Intelligenz und Fachkräftemangel in der IT – aktuelle Entwicklungen tragen dazu bei, dass sich die Cybercrime-Lage weiter zuspitzt. Hinzu kommt, dass Cyberkriminelle immer ausgefeiltere Betrugsmaschen entwickeln und diese stetig an neue technologische und gesellschaftliche Entwicklungen anpassen. Das stellt Organisationen beim Aufsetzen ihrer Security-Strategien und bei der Wahl der richtigen Ansätze und Tools vor große Herausforderungen.

Jede 2.

Organisation wurde in den vergangenen 3 Jahren Opfer eines erfolgreichen Cyberangriffs, jede 3. sogar mehr als einmal. 64 % der betroffenen Organisationen beurteilen ihr Risiko für einen erneuten Angriff als hoch.



der Sicherheitsbeauftragten bewerten Phishing und die emotionale Manipulation von Mitarbeitenden als großes Sicherheitsrisiko für ihre Organisation.

Die Aussichten für die kommenden Monate und Jahre scheinen nicht rosig. Die für diesen Report befragten Sicherheitsexpertinnen und -experten waren sich mehrheitlich einig: **82 Prozent erwarten in den nächsten Monaten keine Entspannung der Sicherheitslage**.

Der gemeinsame Nenner

Trotz der Komplexität der Cyber-Bedrohungslage lässt sich ein roter Faden in all den Entwicklungen erkennen: der Faktor Mensch. Die technischen Schutzmaßnahmen können noch so effektiv sein – sie können uns nicht vor der emotionalen Manipulation durch Social Engineering bewahren. Phishing – als Paradebeispiel für Social Engineering – steht auf der Liste der erfolgreichsten Cyber-Angriffsstrategien auf Rang zwei. Ähnlich gefährlich im Hinblick auf ihr Risikopotential sind Sicherheitsbeauftragten zufolge nur Schadsoftware und Ransomware, die ebenfalls häufig mit einer Art menschlicher Interaktion beginnen, zum Beispiel wenn Mitarbeitende unwissentlich Zugangsdaten preisgeben.

Da es ein kosteneffektiver und einfacher Weg in die Unternehmenssysteme ist, entwickeln Angreifende ständig neue, innovative Social-Engineering-Strategien. Die gute Nachricht: Organisationen können den Faktor Mensch als Teil ihrer Sicherheitsstrategie proaktiv stärken und Risiken so effektiv reduzieren.

Der Mensch als erste und letzte Verteidigungslinie

Wenn Organisationen Cyberkriminelle mit ihren eigenen Methoden schlagen und menschliche Verhaltensmuster sowie verhaltenspsychologische Erkenntnisse zu ihrem eigenen Vorteil nutzen, können sie ihre Mitarbeitenden zu ihrer „menschlichen Firewall“ machen.

1 **Allianz (2023).** Allianz Risk Barometer.

2 **IBM (2022).** Kosten eines Datenschutzverstoßes 2022. Ein millionenschwerer Wettlauf um Erkennung und Reaktion.

3 **Heise (2023).** Sicherheitsvorfall bei Reddit: Angreifer erlangten Zugriff auf interne Systeme.

Alles das, was ich durch Awareness von Mitarbeitern abdecken kann, macht mich als Unternehmen resilienter. Ich spare so Geld, Zeit und natürlich auch Nerven und Risiko.

Thomas Schumacher
Managing Director Accenture Security

Der Phishing-Angriff auf Reddit[3] veranschaulichte das nur zu gut. Anfang 2023 erlitt das Unternehmen einen Datenschutzverstoß, bei dem die Angreifenden Zugriff auf interne Dokumente und Quellcode erlangten. Darauf folgte jedoch ein Paradebeispiel für eine starke Sicherheitskultur und achtsame Mitarbeitende: Der Angriff wurde von der Person, die die schädliche Phishing-Mail geklickt hatte, sofort erkannt und dem internen Sicherheitsteam gemeldet. Dieses konnte den Zugriff der Cyberkriminellen auf weitere Daten rechtzeitig verhindern und somit weitreichendere Folgen vermeiden.

Um uns vor Cyberkriminellen zu schützen, müssen wir also menschliche Verhaltensmuster verstehen und in den Fokus rücken. In diesem Report nehmen wir die Lage im Bereich Cybersicherheit und Awareness unter die Lupe, mit besonderem Fokus auf Europa. Zudem beleuchten wir, wie Organisationen verhaltenswissenschaftliche Erkenntnisse in der heutigen komplexen Bedrohungslage zu ihrem Schutz nutzen können. Die Einblicke basieren auf zahlreichen Daten sowie den Meinungen von Expertinnen und Experten aus verschiedenen Branchen, die mit uns teilen, welche Top-Prioritäten sie im Bereich Informationssicherheit heute setzen.

Wir leben im Zeitalter der Digitalisierung. Nahezu alles ist mit allem verknüpft – also kann auch alles gehackt werden.

Dr. Katrin Suder
Strategieexpertin (digitale Technologien, Wirtschaft & Politik)

Dr. Katrin Suder ist eine der renommiertesten Strategieexpertinnen an der Schnittstelle von digitalen Technologien, Wirtschaft und Politik. Sie berät verschiedene Unternehmen, darunter DAX-Konzerne und große US-Unternehmen. Die promovierte Physikerin und Neuroinformatikerin mit einem Doktor im Fachgebiet der Künstlichen Intelligenz verfügt über langjährige Erfahrung in Politik und Wirtschaft: Bis 2021 leitete sie den Digitalrat der Bundesregierung von Angela Merkel. Von 2014 bis 2018 war sie Staatssekretärin im Bundesverteidigungsministerium. Bei McKinsey arbeitete sie 14 Jahre lang, zuletzt als Director. Sie hat Mandate in deutschen und internationalen Aufsichtsräten, unter anderem im Board von Cloudflare.

Auf unserer Human Firewall Conference haben Sie gesagt: Wenn es eine Sache gibt, die Sie nachts wachhält, dann sind es Cyberbedrohungen. Warum?

Cyber ist eine gefährliche militärische, aber auch eine sehr effektive und kostengünstige kriminelle Waffe, denn Angreifende bleiben mit ihren Cyberangriffen meist unentdeckt. Eine Attribution ist nicht unmöglich, aber extrem aufwändig. Sie sind außerdem verhältnismäßig günstig, wenn man sie militärisch beispielsweise mit einem Kampfjet vergleicht. Außerdem gibt es ein niedriges "Eigenrisko" – niemand muss aufgrund der Distanz sein Leben riskieren. Und trotzdem können Cyberangriffe potenziell verheerende Auswirkungen haben. Als ich im Verteidigungsministerium tätig war, hat sich die Frage der Sicherheit immer mehr in den Cyberraum verlagert – deshalb haben wir der Verteidigungsstrategie mit Cyber eine neue Dimension hinzugefügt. Bei meiner Arbeit mit Unternehmen gehören Cybervorfälle heute zu den größten Business-Risiken. Unternehmen werden laufend gehackt. Die Frage ist nicht mehr, ob Du gehackt wirst, sondern wann - und vor allem: wie schnell Du reagierst und wie Du damit umgehst.

Die geopolitische Lage wird zunehmend instabil und fragmentiert. Wie wirkt sich das auch auf Gefahren im Cyberraum aus?

Cyber ist ein geopolitisches Machtinstrument und gleichzeitig ein neuer Angriffsvektor geworden, den Staaten für Ihre Interessen einsetzen. Unsere neue Weltordnung führt dazu, dass es immer weniger ordnungspolitische Kräfte gibt, dafür immer mehr nationale Interessen. Das können Spionage-Interessen oder Aggressor-Bestrebungen sein. Mit einem Investment in

Cyber investieren Staaten letztlich in eine Waffentechnologie und können mit einem kleinen Investment für verheerende Auswirkungen sorgen. Und dabei geht es nicht nur um Daten und Geld, sondern teilweise auch um Menschenleben.

Ist der akute Anstieg an Cyberangriffen in der aktuellen Lage ausschließlich (geo-)politisch motiviert?

Nein, der Anstieg ist nicht ausschließlich politisch motiviert. Viele Cyberangriffe werden durch halbstaatliche Akteure durchgeführt – das ist vergleichbar mit Soldaten ohne Hoheitsabzeichen. Sie unterliegen keinen Regeln, man kann keine Staaten verantwortlich machen, man kann sich auf keine Konventionen berufen – das macht die Situation so unglaublich kompliziert. In unserer neuen Weltordnung mit starken nationalstaatlichen Interessen können solche Strukturen immer weiter wachsen. Diese halbstaatlichen Hacker nutzen geopolitische Entwicklungen für ihren eigenen Profit aus – sei dies beispielsweise zur Unterstützung politischer Interessen oder zur Erwirtschaftung großer finanzieller Gewinne durch erbeutete Daten. Insofern ist Geopolitik auch ein Treiber für Cyberkriminalität: Durch geopolitische Krisen nehmen nicht nur politisch, sondern auch kriminell motivierte Cyberangriffe zu.

Welche anderen Entwicklungen beeinflussen unsere Cybersicherheit?

Der Kernpunkt ist, dass wir im Zeitalter der Digitalisierung leben. Nahezu alles ist mit allem verknüpft – also kann auch alles gehackt werden. Die Digitalisierung hat außerdem dazu geführt, dass Technologie wichtiger geworden ist. Und durch den hohen Grad der Technologisierung gibt es weitere Einfallstore für Angreifende.

Welchen Einfluss hat das auf unsere Kritische Infrastruktur? Früher waren Energiekraftwerke nicht am Internet – geht das überhaupt noch, wenn wir über dezentrale Energieverteilung nachdenken?

Natürlich werden wir immer rote Netze haben, wie bei der Bundeswehr zum Beispiel – also isolierte Bereiche, die nicht am Internet hängen. Aber trotzdem wird auch die Kritische Infrastruktur (KRITIS) immer stärker vernetzt und abhängig vom Internet sein. Das macht mir Sorgen. Außerdem werden ja zunehmend auch Menschen direkt angegriffen und manipuliert – die dann wiederum Zugriff auf isolierte Netze haben könnten. Es gibt zwar die KRITIS-Gesetzgebung und Verordnungen, die diesen Bereich regulieren sollen, aber schaut man sich die dezentrale Versorgung an, zum Beispiel kleine kommunale Energieversorger, die haben es schwerer sich zu schützen. Ihnen fehlen finanzielle und personelle Ressourcen, um die IT entsprechend aufzusetzen.

Können wir all diese Entwicklungen in der IT-Sicherheit überhaupt im Blick behalten?

Oft wird gesagt, dass im Cyberraum alles neu ist und wir das nicht kennen. Aber das stimmt nicht: Die Prinzipien zum Beispiel von Sicherheit und Schutz sind dieselben, Passwortschutz ist wie Händewaschen, wieder und immer wieder. Wir sollten nicht so tun, als wäre im digitalen Raum alles neu, unvorhersehbar und unkontrollierbar. Das stimmt zum einen nicht und zum anderen macht es ohnmächtig.

> Die letzten 10 Jahre haben Unternehmen eher in Technik investiert als in Menschen. Inzwischen haben sie verstanden, dass Technik nicht alles ist, und dass Social Engineering – und insbesondere Phishing – ein echtes Problem ist.

Dr. Katrin Suder
Strategieexpertin (digitale Technologien, Wirtschaft & Politik)

Kommen wir zur Verteidigungsseite: Sie haben ein Mandat im Advisory Board von Cloudflare. Ist Cyber Security in den Aufsichtsräten dieser Welt angekommen?

Ja, eindeutig. Das ist zwar von Branche zu Branche anders: Je weniger digitalisiert eine Industrie ist, desto weniger präsent ist Cyber Security. Aber generell beobachte ich, dass Cybervorfälle inzwischen zu den Top-Risiken gehören.

Nicht jedem Aufsichtsrat gehört jemand an, der das Thema beherrscht. Das ist auch ein Generationsthema: Aufsichtsräte sind in der Regel schon etwas lebenserfahrener, und insofern oft weiter weg von Digitalisierung und von Cyber. Hinzu kommt, dass Cyber ein Rat Race ist – Cyber dreht sich schnell, man muss ständig nachlernen.

Umso wichtiger ist es, neue Modelle zu entwickeln, zum Beispiel jüngere Leute mit spezifischer Expertise in Aufsichtsräte berufen, auch wenn sie noch nicht Vorstand eines Unternehmens waren, oder verstärkt in Schulungen zu investieren. Die Frage, die wir uns hier stellen müssen, ist: Wie präsent ist das Wissen zu Cyber? Und wie kann man es aktuell halten? Das ist eine Herausforderung, vor der viele Unternehmen, insbesondere im Mittelstand, stehen.

Machen Unternehmen genug, um sich abzusichern – insbesondere in Bezug auf die Human Layer?

Unternehmen können nicht genug in Security Awareness investieren. Das Thema „Human Factor" ist erst seit ein paar Jahren in den Unternehmen angekommen. Deshalb dauert es noch, bis Unternehmen ihre Best Practices entwickelt haben und sie eine Strategie gefunden haben, um mit dem Rat Race mitzuhalten. Die letzten 10 Jahre haben Unternehmen eher in Technik investiert als in Menschen. Inzwischen haben sie verstanden, dass Technik nicht alles ist, und dass Social Engineering – und insbesondere Phishing – ein echtes Problem ist.

„Technik versus Mensch": Eine viel geführte Diskussion in der Informationssicherheit ist, wo und wie priorisiert werden soll. Wie sehen Sie das?

Das ist ein künstlicher Widerspruch. Wir diskutieren doch auch nicht, ob Unternehmen eher in ihre Fabrikanlage oder in ihre Mitarbeitenden investieren sollen. Natürlich können Unternehmen versuchen durch ein technisches Set-Up Schlupflöcher dicht zu machen und mit Software Skalierung zu erreichen – das sollten sie auch unbedingt tun. Aber Unternehmen müssen unbedingt auch in Menschen investieren.

Sie erwähnen das Rat Race in der Informationssicherheit: Sehen Unternehmen Cyber Security als einmaliges Schulungsprojekt? Oder haben sie verstanden, dass wir kontinuierlich investieren müssen?

Das Phishing-Problem ist in Unternehmen angekommen und die meisten haben verstanden, dass es kontinuierlicher Aufmerksamkeit bedarf. Viele tun sich in der Umsetzung noch schwer und arbeiten noch mit traditionellen Maßnahmen – lange PowerPoint-Präsentationen, „witzige" Videos oder steife Frontalschulungen, die Mitarbeitende sensibilisieren sollen. Wenn wir aber schauen, wie viele Informationen wir an unsere Mitarbeitenden vermitteln müssen – neben Cyber noch Themen, wie Compliance, Datenschutz, ESG – dann müssen Strategien wie Gamification und Einsichten aus dem Bereich des Erwachsenen-Lernens genutzt werden. Da stehen viele Unternehmen noch am Anfang.

Was sind die Fragen, die in Aufsichtsräten gestellt werden, um Cybersicherheit von menschlicher und technischer Seite im Unternehmen zu evaluieren?

In dieser Hinsicht sind wir in Aufsichtsräten noch nicht gut genug besetzt. Oft bleiben Fragen und Diskussionen fokussiert auf Kontrolle und Prozessen. Eigentlich sollten wir aber viel tiefer einsteigen und sollten auch in den Aufsichtsräten

Fragen stellen wie: Welches Gefahrenpotenzial liegt in unserem Geschäftsmodell? Welche Daten liegen wo? Was wäre der maximale Geschäftsschaden eines Cyberangriffs in der aktuellen Situation? Wie sehen unsere Angriffsvektoren geopolitisch aus? Welche Krisenvorsorgepläne existieren? Das wirkt auf den ersten Blick kompliziert, eigentlich ist es das aber nicht. In der Produktion werden ja auch spezifische Fragen etwa nach den Ausfallkosten oder Fehlerhäufigkeiten gestellt.

Wie sollte Cyber Security im Unternehmen verankert werden?

Cyber ist ein klassisches Risikomanagement-Thema. Entweder Unternehmen integrieren Cyber in ihre Risikomanagement-Prozesse oder sie machen es zu einem Querschnittsthema und etablieren ein eigenes Cyberrisiko-Assessment. Ich habe beides schon in Unternehmen gesehen und beides kann funktionieren.

Kann man Cyber als Digitale Steuer sehen? Und müssen wir uns dann darauf einstellen, dass das mit steigender Digitalisierung ein steigender Kostenblock bleibt?

Natürlich müssen wir diese neue Sicherheitsdimension einpreisen. Das Problem ist, dass „Versicherungsprämien" gestiegen sind – für Gesundheit (COVID), für Industriepolitik, für physikalische Sicherheit, für Energie, für Cybersicherheit. Unternehmen haben dadurch hohe zusätzlich Kosten, und die EBIT-Margen kommen somit auch aufgrund der geopolitischen Entwicklungen unter Druck. Das bedeutet in Summe, dass wir Wohlstandsverluste haben – denn EBIT-Margen, die nicht verdient werden, können nicht für Investitionen, für Mitarbeitende oder ähnliches eingesetzt werden. Ich sehe geopolitisch nicht, warum diese Versicherungsprämien abnehmen sollten. Auch der Staat kann nicht für alles aufkommen oder alles regeln. Deshalb finde ich den Steuerbegriff in dieser Diskussion irreführend.

Welche Rolle sollte der Staat im Cyber-Thema spielen?

Eine wichtige Aufgabe des Staates ist es, in zeitgemäße Bildung zu investieren – und das passiert in Bezug auf IT-Sicherheit noch nicht genug. Alle Heranwachsenden sollten im Laufe der Schulzeit zumindest die Kernprinzipien von Cybersicherheit kennen, ebenso wie den Umgang mit Daten. Neben Bildung brauchen wir eine funktionierende (digitale) Polizei sowie generell mehr Unterstützung und Anlaufstellen – hier sind wir noch nicht gut genug im Cyberraum aufgestellt.

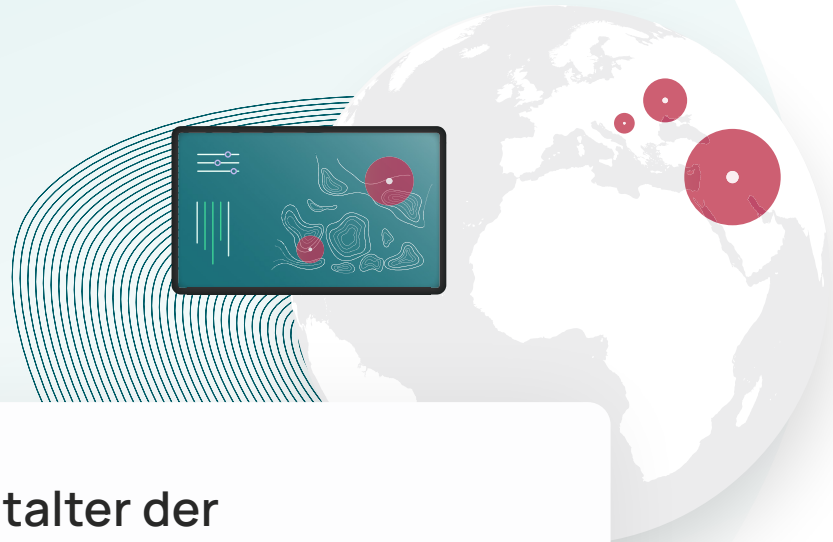
Wie lösen wir das Fachkräfteproblem in der IT?

Wir müssen weiter über Automatisierung in der IT nachdenken, auch um sicherer zu werden. Wir reden hierbei nicht mehr über Entlassungen und Effizienzverbesserungen durch Automatisierung, sondern darüber, ob wir IT-Sicherheit überhaupt noch garantieren können. Der Fachkräftemangel ist real und ist in seinen Konsequenzen für viele Unternehmen spürbar – im MINT-Bereich ist die Situation sogar verschärft. Gleichzeitig steigt der Bedarf immer weiter. Diese Situation verlangt nach neuen Lösungen, zum Beispiel Skalierung durch Automatisierung. Wir sollten weiter, in den Bereichen, wo wir es können – sei es mit ChatGPT oder anderer Technologie – Kapazitäten freiräumen.

Sie erwähnen ChatGPT: Welchen Einfluss hat Generative AI aus Ihrer Perspektive auf unsere IT-Sicherheit?

Ich mache mir in Bezug auf Generative AI mehr Sorgen aus Bildungs- und Demokratiesicht als aus einer Arbeitskräfteperspektive. Denn Generative AI führt uns zu einem neuen Bildungsauftrag: Wenn wir immer mehr generierende KIs haben, dann müssen wir uns damit beschäftigen, wie wir Innovation oder Inhalte noch kategorisieren können. Wie beurteilen wir Texte? Wie betreiben wir Recherche? Der Output dieser Tools kommt von einer Maschine – den Empfängerinnen und Empfängern fehlt also der Mensch als Quelle, den sie einschätzen können. Nutzende müssen lernen, die Antworten von AI-Tools zu bewerten.

Geopolitische Krisen:
Wie globale Konflikte Cyberkriminalität befeuern



> **Wir leben im Zeitalter der Digitalisierung. Nahezu alles ist mit allem verknüpft – also kann auch alles gehackt werden.**

Dr. Katrin Suder
Strategieexpertin (digitale Technologien, Wirtschaft & Politik)

Das Zitat von Dr. Suder bringt die weitreichenden Folgen moderner Entwicklungen auf den Punkt: Stetige technologische Innovationen und die wachsende Vernetzung digitaler Geräte und Systeme haben uns neue Türen im Bereich der Kommunikation, des Handels und der Innovation geöffnet. Gleichzeitig stellen sie aber unsere Cyberresilienz auf eine harte Bestandsprobe. Durch das **Zusammenspiel von Digitalisierung und Geopolitik** ist die **Cybercrime-Industrie heute komplexer als je zuvor**. Staatlich induzierte Cyberangriffe, kriminelle Organisationen und einzelne Hacker nutzen jede Schwachstelle der digitalen Infrastruktur für ihre politischen und wirtschaftlichen Ziele aus. Die weltweit angespannte Lage zwingt Regierungen, Organisationen, aber auch Privatpersonen, sich intensiv mit ihrer Informationssicherheit auseinanderzusetzen.

Verschobene Machtverhältnisse: Cybersicherheit im Regierungssektor

Nach Jahrzehnten der rasanten Digitalisierung und fortschreitenden Globalisierung erlebt die Welt heute insbesondere aus geopolitischer Sicht einen neuen Megatrend: **Deglobalisierung**. Während es 2008 bereits die ersten Anzeichen dafür gab, nahm diese Entwicklung, angetrieben durch den strategischen Wettbewerb zwischen den USA und China, in jüngster Zeit an Fahrt auf.[1] Nachdem die Stimmung zwischen den beiden Wirtschaftsmächten seit geraumer Zeit angespannt war, tragen sie nun ihren Konkurrenzkampf auch im Cyberraum aus – sie beschuldigten sich gegenseitig für staatlich induzierte Cyberangriffe, Diebstahl geistigen Eigentums und Spionage. Bei einer Reihe von DDoS-Angriffen im vergangenen Jahr wurden mehrere Webseiten offizieller Institutionen von Taiwan vom Netz genommen. Da die Angriffe im Zeitraum des Besuchs der US-Politikerin Nancy Pelosi stattfanden, wurden Bedenken über Chinas Beteiligung laut.[2]

Ein weiteres Beispiel ist der andauernde Konflikt zwischen Israel und dem Iran, die seit geraumer Zeit einen verdeckten Cyberkrieg führen. Der bekannte Stuxnet-Wurm, der auf iranische Atomkraftwerke abzielte, war lang nicht das einzige Beispiel. Danach kam es zu zahlreichen weiteren Cyberattacken, wie der versuchte Angriff auf Israels Wasser- und Abwasserinfrastruktur im April 2020, auf Irans Shahid Rajaee-Hafen im Mai 2020, gegen die iranischen Transportsysteme im Juli 2021 und ein Hackerangriff auf ein israelisches Hosting-Unternehmen, bei dem im Oktober 2021 persönliche Nutzerdaten geleakt wurden.[3] Da derartige Cyberangriffe, auch im Kontext des Ukraine-Kriegs, immer größere Ausmaße annehmen, mehren sich die Bedenken, dass sie **weniger der eigenen Abwehr gelten, sondern verstärkt auf die Störung kritischer Infrastrukturen und auch auf die Zivilbevölkerung abzielen** – eine geteilte Sorge der Regierungen weltweit in Anbetracht der wachsenden politischen Spannungen.

1 **Deutschlandfunk (2023).** Wie sich weltweite Handelsströme verändern könnten.

2 **Tagesspiegel (2023).** Vor Besuch von Nancy Pelosi: Hacker legen Webseite der taiwanischen Präsidentin lahm.

3 **ntv (2023).** Israel und der Iran - Der Schattenkrieg tritt in eine neue Phase.

Die Anzahl versuchter Cyberangriffe ist seit Februar 2022 um circa 8.000 Prozent gestiegen.

Sascha Czech
CSO Uniklinikum Münster

Sascha Czech ist CSO am Uniklinikum Münster (UKM) und trägt damit die Gesamtverantwortung für die Unternehmenssicherheit des Klinikums. Dort baute er als erste Klinik in Deutschland ein mit eigenem Fachpersonal betriebenes Security Operation Center (SOC) auf, wofür er 2022 von Certification Information Security (CIS) als CISO of the Year ausgezeichnet wurde.

Sie waren schon in verschiedenen Security-Führungsrollen im Gesundheitswesen tätig. Was sind dabei die größten Herausforderungen?

Wir sehen eine signifikant steigende Bedrohungslage – und das nicht erst seit gestern. Nicht nur neue Angriffstaktiken nehmen zu, sondern vor allem das typische konstante „Hintergrundrauschen". Die größte Herausforderung sehe ich im Gesundheitswesen in der Kombination von Cyber- und physischer Perimetersicherheit.

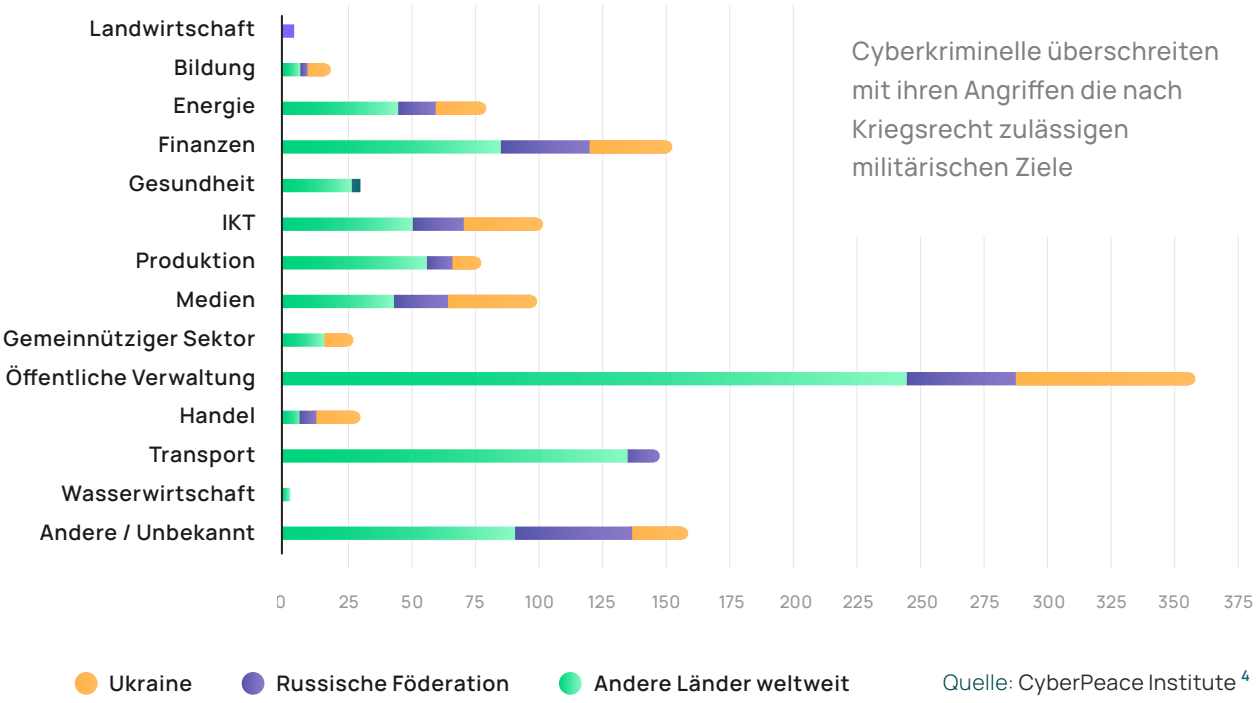
Was sehen Sie als Haupttreiber dieser Entwicklungen?

Zum einen auf jeden Fall die weltweit politisch angespannte Lage. Beim Uniklinikum Münster haben wir seit Februar letzten Jahres bei dem bereits erwähnten „Hintergrundrauschen" von Angriffen einen Anstieg von circa 8.000 Prozent im Vergleich zum Vorjahreszeitraum wahrnehmen können. Schadhafte E-Mails – egal ob Phishing oder Ransomware – erreichen uns in immer kürzeren Intervallen. Und die einzelnen Wellen werden außerdem wesentlich heftiger.

Nehmen Sie denn einen Mindset-Wechsel in Bezug auf Informationssicherheit wahr?

Durch die hohe Medienpräsenz glaube ich schon, dass das Thema allgemein präsenter ist. Man muss allerdings trotzdem einen Weg finden, dass Menschen sich ihrer Verantwortung in dem Bereich bewusst werden – und sie offen dafür sind, sich in dem Bereich auch weiterzubilden. In dem Moment, in dem Mitarbeitende Sicherheit nicht mehr als „störend" verstehen, sondern realisieren, dass es ein erfolgsrelevanter Prozess ist, hat man als Unternehmen gewonnen. Wir haben das Thema daher im ersten Schritt unter den Mantel der allgemeinen Sicherheit, wie zum Beispiel Brandschutz, untergebracht. Darüber hinaus fokussieren wir uns darauf, den Menschen auch in die Lage eines Cyberangriffs zu versetzen – zu zeigen, wie schnell und leise es dazu kommen kann und welche Konsequenzen das haben könnte. So versuchen wir ein neues Verständnis zu prägen: Der Mensch ist nicht nur ein Teil der Verteidigungskette – er ist das wertvollste Glied.

Anzahl an Cyberangriffen nach Sektor und Standort im Kontext des Russland-Ukraine-Konflikts



Quelle: CyberPeace Institute [4]

Die Herausforderungen für Organisationen

> Es wäre fast schon naiv anzunehmen, dass Kriminelle nicht schon lange begriffen hätten, dass sie über die Cyber-Ebene sehr profitable Angriffe ausführen können.

Dr. Stefan Lüders
Computer Security Officer CERN

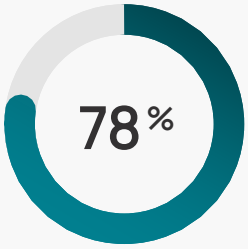
Die Tatsache, dass **Geopolitik und Cybersicherheit heute untrennbar miteinander verschweißt** sind, wirkt sich jedoch längst nicht nur auf Regierungen und kritische Infrastrukturen, sondern auch auf Organisationen weltweit aus. Letztere wurden in jüngsten Jahren vermehrt Opfer von geopolitisch motivierten Cyberangriffen.

So beschuldigten die USA und Großbritannien Nordkorea für den WannaCry-Angriff, von dem mehr als 300.000 Rechner in 150 Ländern betroffen waren – darunter Krankenhäuser, Unternehmen und Banken mit einem Gesamtschaden in Milliardenhöhe.[5]

4 **Cyberpeace Institute (2023).** Impact & Harm. How do cyberattacks and operations impact civilians?

5 **ZEIT Online (2021).** USA und Verbündete werfen China „bösartige Cyberaktivitäten" vor.

Der chinesischen Regierung wurde 2021 unterdes vorgeworfen, an dem Hackerangriff auf Microsoft Exchange Server beteiligt gewesen zu sein, von dem mindestens 30.000 Organisationen weltweit betroffen waren.[6] Diese Angriffe verdeutlichen, dass sich die Auswirkungen von der globalen Ebene auf Organisationen ausweiten, die sich mit steigenden Sicherheitsrisiken konfrontiert sehen.



der Sicherheitsexpertinnen und -experten bestätigen, dass die geopolitische Lage das Cyberrisiko ihrer Organisation erhöht hat.

Doch die geopolitischen Spannungen sind bei Weitem nicht das einzige weltweite Ereignis, das Cyberkriminelle zu ihrem Vorteil nutzen. Bereits wenige Stunden nach dem Zusammenbruch der Silicon Valley Bank im März dieses Jahres begannen Cyberakteure, in Vorbereitung auf Business Email Compromise (BEC)-Angriffe, verdächtige Domains zu registrieren.[7] Mit der Intensivierung der politischen Instabilität werden Cyberkriminelle ihre Betrugsmethoden weiter verfeinern und vor allem besonders geschwächte Branchen und Regionen ins Visier nehmen.

Wie geopolitische Konflikte instrumentalisiert werden: die Zivilbevölkerung als Zielscheibe

> **Die Zivilbevölkerung wird durch Krisen oder Konflikte dazu getrieben, sich an großflächigen Cyberangriffen zu beteiligen. Diese Art von Crowdsourcing von Cyberangriffen ist äußerst besorgniserregend, da es die Grenzen zwischen Zivilpersonen, Militär und Opfern immer mehr verschwimmen lässt.**
>
> **Stéphane Duguin**
> CEO CyberPeace Institute

Politische Spannungen wirken sich auch auf die Emotionen der Bevölkerung aus: Die Menschen sind **besorgt, verunsichert und häufig in ihrer Meinung polarisiert** – das alles macht sie zur perfekten Zielscheibe für Social-Engineering-Taktiken. Cyberkriminelle sind sich dieser Verunsicherung bewusst und nutzen Spannungen aus, indem sie Falschinformationen verbreiten, die öffentliche Meinung manipulieren oder gar zum Einsatz von Gewalt anstacheln. Bei ihren Phishing-Angriffen vermitteln sie auf den verschiedensten Kanälen ein Gefühl der Dringlichkeit und Sorge und bewegen die Zielpersonen so zu überstürzten, unüberlegten Handlungen.

6 **Süddeutsche Zeitung (2021).** Hacker unterwegs im Auftrag der Partei.

7 **Heise (2023).** Betrugsversuche nach Zusammenbruch von Silicon Valley Bank.

Russlands Krieg gegen die Ukraine führte so zu einem rapiden Anstieg an koordinierten Cyberangriffen als Teil der Offensive, der an Organisationen und Zivilpersonen in den beiden Ländern, aber auch weltweit, nicht spurlos vorbeiging. Selbst mehr als ein Jahr nach Beginn des Kriegs versuchen Scammer immer noch, die Menschen auf hunderten von betrügerischen Fake-Websites angeblicher Hilfsorganisationen zu vermeintlichen Spenden für die Ukraine zu bewegen.[8]

Die weitreichenden Auswirkungen der Geopolitik auf die Cyber-Bedrohungslage sollten wir zum Anlass nehmen, uns stetig über aktuelle Trends zu informieren und die nötigen Sicherheitsmaßnahmen einzuführen, um mit der komplexen und höchst innovativen Cybercrime-Industrie Schritt halten zu können.

> **Wir müssen uns auf eine weitere Angriffswelle vorbereiten: Wir wissen, dass der Krieg hybrid geführt wird. Dafür haben sich eine Reihe von Menschen zur Unterstützung einer der Seiten Know-how im Bereich der Cyberkriminalität angeeignet. Wenn der Konflikt irgendwann vorbei ist, haben wir es potenziell mit einer hohen ‚Arbeitslosenquote' unter den Angreifern zu tun. Diese ‚Cyber-Arbeitslosen' werden dann auf der Suche nach einer neuen Herausforderung sein – und diese auch finden.**
>
> **Tobias Ludwichowski**
> CISO Signal Iduna

8 **Netzwelt (2022).** Spenden für die Ukraine: Hütet euch vor diesen gefälschten Hilfsorganisationen.

Cyber-Awareness muss, wie das Anlegen eines Sicherheitsgurtes vor einer Autofahrt, zur eingeübten Alltagsroutine werden.

Generalmajor Jürgen Setzer
CISO Bundeswehr

BUNDESWEHR

Generalmajor Jürgen Setzer trat 1980 als Offizieranwärter des Heeres in die Bundeswehr ein. An die Ausbildung zum Jägeroffizier schloss sich ein Studium der Informatik an der Universität der Bundeswehr in München an. Seit April 2018 ist Generalmajor Jürgen Setzer Stellvertreter des Inspekteurs Cyber- und Informationsraum, Chief Information Security Officer der Bundeswehr (CISOBw) und Beauftragter Weltraum des Kommandos Cyber- und Informationsraum. Generalmajor Jürgen Setzer (geb. 1960) ist verheiratet und Vater zweier Kinder.

Das Kommando „Cyber- und Informationsraum" wurde 2017 ins Leben gerufen. Was war der ausschlaggebende Faktor für die Gründung?

Um sich den Herausforderungen im Cyber- und Informationsraum möglichst wirkungsvoll entgegenzustellen, wurde neben der Aufstellung einer Abteilung Cyber/ IT (CIT) im Verteidigungsministerium auch die Bündelung der Fähigkeiten in einem neuen militärischen Organisationsbereich Cyber- und Informationsraum, kurz CIR, angewiesen. In diesem Bereich sind die Kräfte und Mittel der Bundeswehr in der Dimension Cyber- und Informationsraum zusammengefasst.

Welche Aufgaben hat der Cyber- und Informationsraum der Bundeswehr?

Die Angehörigen des Organisationsbereiches sind ganzheitlich für die Dimension Cyber- und Informationsraum verantwortlich. Sie gewährleisten den Schutz und Betrieb des IT-Systems der Bundeswehr, sowohl im Inland als auch im Einsatz. Darüber hinaus stellen sie die Fähigkeiten zur Aufklärung und Wirkung im Cyber- und Informationsraum bereit und entwickeln diese weiter.

Zudem unterstützen sie mit Geoinformationen alle Bereiche der Bundeswehr bei ihrer Auftragserfüllung und tragen durch Austausch und Kooperation mit anderen Institutionen zur gesamtstaatlichen Sicherheitsvorsorge bei.

Wie vielen und welcher Art von Cyberangriffen ist die Bundeswehr jeden Tag ausgesetzt?

Cyberangriffe gehören heute zum allgemeinen Risiko einer zunehmend digitalisierten Welt und machen auch vor der Bundeswehr nicht halt. Sie stellen keine Besonderheit dar und finden millionenfach im Jahr statt. Allerdings hat die rein quantitative Betrachtung von Angriffs- bzw. Zugriffs-

versuchen auch für die Bundeswehr wenig Aussagekraft, da sie keine Rückschlüsse auf konkrete Gefährdungen erlaubt.

Und wie hat sich das im letzten Jahr verändert?

Generell ist das Bedrohungspotential im Cyberraum durch Malwareangriffe, wie zum Beispiel digitale Erpressungen mit Ransomware, Spionage und Versuche Daten und Informationen abfließen zu lassen, steigend. Seit Jahren ist ein fortschreitender Trend zu immer gezielteren und technisch ausgereiften Cyberangriffen auf IT-Systeme staatlicher Organisationen, kritischer Infrastrukturen, der Industrie und der Wissenschaft zu beobachten.

Als potenzielles Hochwertziel ist die Bundeswehr zunächst den gleichen Bedrohungen ausgesetzt wie jede andere Organisation, muss sich aber zusätzlich gegen maßgeschneiderte Cyberattacken hoher Komplexität wappnen.

Hinzu gekommen ist im letzten Jahr - mit klarem Bezug zum RUS-Überfall auf die Ukraine - die deutliche Erhöhung von technisch weniger anspruchsvollen Attacken mit dem Ziel der Sabotage durch Denial of Service. Die Vermutung liegt nahe, dass nichtstaatliche Akteure auf diese Weise im Cyberraum politische Botschaften platzieren wollen.

Hat sich das Verhältnis zwischen physischer und digitaler Bedrohung verschoben?

Der Cyberraum bietet potentiellen Gegnern auch und insbesondere unterhalb der Schwelle eines konventionellen Konfliktes, die Möglichkeit z.T. schwere Schäden im physischen Raum hervorzurufen. Beispielsweise könnte die Ransomwareerpressung eines Krankenhauses lebenserhaltende medizinische Geräte unbrauchbar machen, und in Folge dadurch Menschenleben gefährden.

Dieses schließt ausdrücklich staatliche aber auch nichtstaatliche Akteure mit ein. Gerade die Möglichkeit, seinen eigenen Standort zu verschleiern und verdeckt zuschlagen zu können, macht den Cyberraum für potentielle Gegner interessant, so dass es sich um eine permanente Bedrohung handelt, die schon weit vor einer potentiell auftretenden klassischen physischen Bedrohung präsent ist.

Wie hat der Kriegsbeginn in der Ukraine diese Entwicklung beeinflusst?

Vor Beginn des russischen Angriffskrieges im Februar 2022 gingen viele Experten davon aus, dass der nächste Konflikt zu großen Teilen im Cyber- und Informationsraum stattfinden würde. Man erwartete Cyberangriffe, Desinformation und Propaganda sowie kleinere militärische Operationen verdeckter Kräfte. Schlachten, in denen Massen konventioneller Streitkräfte zum Einsatz kommen, konnten sich die Wenigsten vorstellen. Nun sehen wir aber genau diese Art Krieg. Er wird begleitet durch eine nie dagewesene Vielzahl an Aktivitäten im Cyber- und Informationsraum, die allerdings nicht den Schwerpunkt darstellen. Man hat offenbar festgestellt, dass sich ein Elektrizitätswerk immer noch einfacher, billiger und schneller durch einen Flugkörper ausschalten lässt, als durch einen Cyberangriff. Das müssen wir zur Kenntnis nehmen und unsere Schlüsse daraus ziehen. Wir dürfen jedoch nicht den Fehler machen, zu glauben, dass dies jetzt die Blaupause für zukünftige Konflikte ist.

Haben Sie eine hybride Kriegsführung beobachtet?

Ja. Jeder, der die Medien verfolgt konnte sehen, wie Russland mit viel Aufwand Desinformationen von beispielsweise einer militärischen Spezialoperation zum Schutz der eigenen Sicherheit und Teilen der UKR Bevölkerung verbreitete. Für Cyberangriffe steht beispielhaft die Attacke auf das von der Ukraine genutzte Satellitenkommunikationssystem, die auch Auswirkungen auf den Betrieb deutscher Windräder hatte. Und zusammen mit den klassischen militärischen Angriffen haben wir drei Elemente einer offensiven hybriden Strategie.

> Der russische Angriffskrieg wird begleitet durch eine nie dagewesene Vielzahl an Aktivitäten im Cyber- und Informationsraum.

Würden Sie sagen, der Cybersicherheit sollte in Deutschland eine ähnliche Priorität zukommen wie anderen Streitkräften? Oder ist das schon der Fall?

Für die Cyberabwehr (Gefahrenabwehr) ist grundsätzlich das Bundesministerium des Innern, für Bau und für Heimat (BMI) mit seinen nachgeordneten Behörden sowie den Polizeien der Bundesländer zuständig. Die Bundeswehr arbeitetet ressortübergreifend eng mit den Behörden der Inneren Sicherheit (insb. über das Nationale Cyberabwehrzentrum, NCAZ) zusammen. Im Falle eines Verteidigungs- oder Bündnisfalles verfügt die Bundeswehr über defensive und offensive Fähigkeiten, die neben der Aufklärung und Wirkung im Cyberraum auch zur Verhinderung, Erkennung und Bewältigung von Cyberangriffen gegen die IT der Bundeswehr im In- und Ausland dienen.

Innerhalb der Bundeswehr genießt Cybersicherheit somit einen hohen Stellenwert, der durch die Schaffung eines eigenen militärischen Organisationsbereiches CIR, gleichberechtigt neben den klassischen Teilstreitkräften Heer, Luftwaffe und Marine, unterstrichen wurde.

Was sind aus Ihrer Sicht die Top 3 Trends auf Angreiferseite?

Social Engineering, Malwareangriffe – insbesondere mit Ransomware, und Denial oder Distributed Denial of Services (DoS oder DDoS).

Welche Rolle spielt der Faktor Mensch in einer (Cyber-) Verteidigungsstrategie? Wie gehen Sie dieses Thema bei der Bundeswehr an?

Die technischen Maßnahmen zum Schutz der Netze sind heutzutage so hoch, dass unmittelbare Angriffe über den Perimeterschutz kaum hinauskommen. Daher haben Cyberangriffe oft den IT-Endnutzer im Visier und erreichen von innen heraus ihr Ziel. Die Aufmerksamkeit der Menschen an den Endgeräten ist entscheidend, um schnell und richtig zu reagieren. Für mich als Chief Information Security Officer ist es somit essentiell, die Angehörigen der Bundeswehr in der Cyber-Awareness zu schulen und Resilienzen auszuprägen. Die Wirksamkeit von Maßnahmen zur Cybersicherheit werden in der Bundeswehr regelmäßig überprüft, so beispielweise auch mit unserer Inhouse-Sicherheitskampagne „Phishing as a Service in der Bundeswehr (PaaSBw)". Unsere Soldatinnen und Soldaten sowie zivile Mitarbeiterinnen und Mitarbeiter sind bildlich gesprochen, die letzte Verteidigungslinie – „The last Line of Defense." Und diese gilt es zu sensibilisieren und zu härten. Denn Cyberawareness muss, wie das Anlegen eines Sicherheitsgurtes vor einer Autofahrt, zur eingeübten Alltagsroutine werden.

Cybersicherheit funktioniert dabei nur gesamtstaatlich und erfordert eine Zusammenarbeit über Ressortgrenzen hinweg. Ganz in diesem Sinne beteiligen sich viele Dienststellen der Bundeswehr u.a. auch jährlich mit Beiträgen und Sensibilisierungsmaßnahmen im europäischen Cybersicherheitsmonat Oktober, um alle Mitarbeitenden für die Gefahren bei der Nutzung der Informationstechnik zu sensibilisieren. Ziel der Beteiligung ist, die Awareness gegen potenzielle Gegner, die digitale Innovationen auch für Angriffe auf die Bundeswehr und ihre Verbündeten nutzen, zu stärken.

Wie gestalten Sie den Wandel, um IT-Sicherheit als Kernthema in der Bundeswehrkultur zu etablieren und ggf. auch eine Sicherheitskultur zu etablieren?

Informationssicherheit wird inzwischen als eine wichtige Führungsaufgabe in der Bundeswehr wahrgenommen. Das ist bereits ein großer Schritt. Ausschlaggebend für eine erfolgreiche Sicherheitskultur ist zudem das Zusammenspiel aller Akteure im System Bundeswehr – von der Führungsebene bis hin zum jedem einzelnen Angehörigen. Seit 2020 animieren wir externe IT-Sicherheitsforscherinnen und -forscher, den sogenannten White-Hat-Hackern, Schwachstellen an Systemen/Webportalen der Bundeswehr zu finden und uns zu melden.

Mit der Vulnerability Disclosure Policy der Bundeswehr (VDPBw) schufen wir einen rechtlichen Rahmen für IT-Sicherheitsprofis, um diese Schwachstellen identifizieren und mitteilen zu können, und somit vor versehentlichem oder vorsätzlichem Missbrauch zu schützen. Dank der Unterstützung der Meldenden und ihrer ausführlichen Dokumentationen konnte das Sicherheitsniveau der Bundeswehr-IT bereits verbessert werden. Die Bundeswehr ist damit Vorreiter einer solchen Richtlinie von Schwachstellenmeldungen im Behördenumfeld.

100 Milliarden Sondervermögen für die Bundeswehr: Wie hat das Ihre Arbeit beeinflusst? Was tut sich in Bezug auf Ihre Cyberabwehr, wo investieren Sie?

Es gibt nicht das eine große Projekt für Cybersicherheit. Cybersicherheit spielt vielmehr in jedem Rüstungsvorhaben eine wichtige Rolle und wird von Beginn an mitgedacht.

Social Engineering: Die ungebrochene Kraft emotionaler Manipulation

Die Top 3 der erfolgreichsten Cyber-Angriffstaktiken

1. Malware
2. Phishing
3. Ransomware

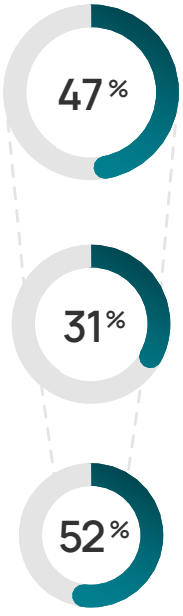
> Wir sehen bei Cyberangriffen fast immer die gleichen Eintrittstore: das Einschleusen von Schadsoftware oder das Abgreifen sensibler Daten, zum Beispiel über Phishing.

Dr. Stefan Lüders
Computer Security Officer CERN

Geopolitische Unruhen und globale Krisen erweitern die Angriffsfläche für Cyberkriminelle, während technologische Innovationen die Skalierung ihrer illegalen Geschäftsmodelle antreiben. Dennoch kam es bisher nur zu wenigen großflächigen Angriffen hoher Komplexität (mehr dazu im nächsten Kapitel). Stattdessen verlassen sich Cyberkriminelle weiterhin auf ihre bewährten Methoden: Social Engineering, oft in der Form von Phishing. In unserer Umfrage besetzte Phishing unter den erfolgreichsten Cyber-Angriffstaktiken den zweiten Rang. Die Top 3 teilt sich Phishing mit Malware und Ransomware – zwei Taktiken, die ebenfalls oft Phishing oder eine andere Art der emotionalen Manipulation als Eintrittstor haben. Hinzu kommt, dass **61 Prozent der befragten Security-Verantwortlichen angaben, dass ihre Organisation bereits über E-Mails angegriffen wurde** – ein Trend, der immer noch weiter an Fahrt aufnimmt.

> **Schadhafte E-Mails erreichen uns in immer kürzeren Intervallen und die einzelnen Wellen werden wesentlich heftiger.**
>
> Sascha Czech
> CSO Uniklinikum Münster

Cyberkriminelle setzen nicht ohne Grund immer noch stark auf Phishing. Daten unserer Plattform zeigen, dass Phishing unter Umständen ein hocheffektives Tool zum Abgreifen sensibler Daten und zum Eindringen in Unternehmenssysteme sein kann. Die Tatsache, dass jeder dritte User auf schädliche Inhalte in Phishing-Mails klickt, spricht für sich.



Öffnungsrate

Nahezu jeder zweite User öffnet Phishing-Mails, …

+2 seit 2022

Klickrate

ein Drittel davon klickt auf in der Mail enthaltene schädliche Inhalte, …

+1 seit 2022

Interaktionsrate

und wiederum die Hälfte davon interagiert weiter mit den Inhalten.

-6 seit 2022

User sind bei der Interaktion mit schädlichen Inhalten im Vergleich zu 2022 zwar etwas vorsichtiger geworden (von 58 % auf 52 % gesunken). Dennoch bleibt die Rate besorgniserregend hoch. Wir beobachten immer noch, dass die Hälfte der User, die zu einem Klick in einer Phishing-Mail bewegt werden, weiter mit den Inhalten interagieren – zum Beispiel Daten in eine gefälschte Eingabemaske eingeben. **Technologische Innovationen wie generative KI-Tools werden diese KPIs voraussichtlich weiter in die Höhe treiben**, indem sie Cyberkriminellen ermöglichen, ihre Phishing-Inhalte zu optimieren und in kürzerer Zeit mehr schädliche Inhalte zu generieren (mehr dazu im nächsten Kapitel).

Doch was macht Social Engineering überhaupt so erfolgreich? Um ihre Ziele zu erreichen und die Erfolgschancen ihrer Angriffe zu steigern, passen Cyberkriminelle verschiedene Vektoren stetig an aktuelle Trends an. Beim genaueren Blick auf diese Vektoren wird deutlich, warum die emotionale Manipulation der Zielpersonen einen fundamentalen Bestandteil der meisten Angriffstaktiken ausmacht: Unabhängig von den technischen Sicherheitsmaßnahmen führt sie extrem oft zum Erfolg.

Technische Manipulation mit emotionaler Wirkung

Ein höchst skalierbarer Ansatz zur Steigerung der Erfolgschancen von Phishing-Angriffen liegt für Cyberkriminelle in der technischen Manipulation ihrer Phishing-Mails – sei es in Form eines Anhangs, eines Links, einer Eingabemaske oder einer imitierten E-Mail-Konversation. All diese Vektoren sind immer noch äußerst wirksam, auch wenn die Erfolgsrate technisch manipulierter Phishing-Mails im Vergleich zu den Vorjahren insgesamt zurückgeht. Auffällig ist, dass **User vorsichtiger mit Anhängen umgehen**, was sich im Vergleich zu 2022 in einer um 8 Prozentpunkte gesunkenen Klickrate zeigt.

Klickraten nach Angriffstyp (vs. 2022)

Anhang	Link
32 % -8	25 % -1
Eingabemaske	**Antwort/Weiterleitung**
27 % -2	34 % -5

Doch auch die Manipulation von Domains oder E-Mail-Adressen gehört zu den beliebtesten Strategien der Cyberkriminellen. Während eine kleine Änderung der Zieldomain nur jede fünfte oder sechste Person zum Klicken bewegt, **gehören Subdomain-Squatting und E-Mail-Spoofing zu den erfolgreicheren Methoden** – mit Klickraten in Höhe von 26 Prozent beziehungsweise 29 Prozent.

Diese Entwicklungen veranschaulichen, dass sich das Bewusstsein der User für technische Manipulationsmethoden vergrößert hat. Traditionelle Angriffsmethoden, wie schädliche Dateien im Anhang, verlieren nach und nach an Wirkung und die Klickraten sinken. Als Konsequenz ist zu erwarten, dass Cyberkriminelle in Zukunft von massentauglichen, technischen Manipulationstaktiken zu ausgeklügelten, personalisierten Betrugsmaschen wechseln werden.

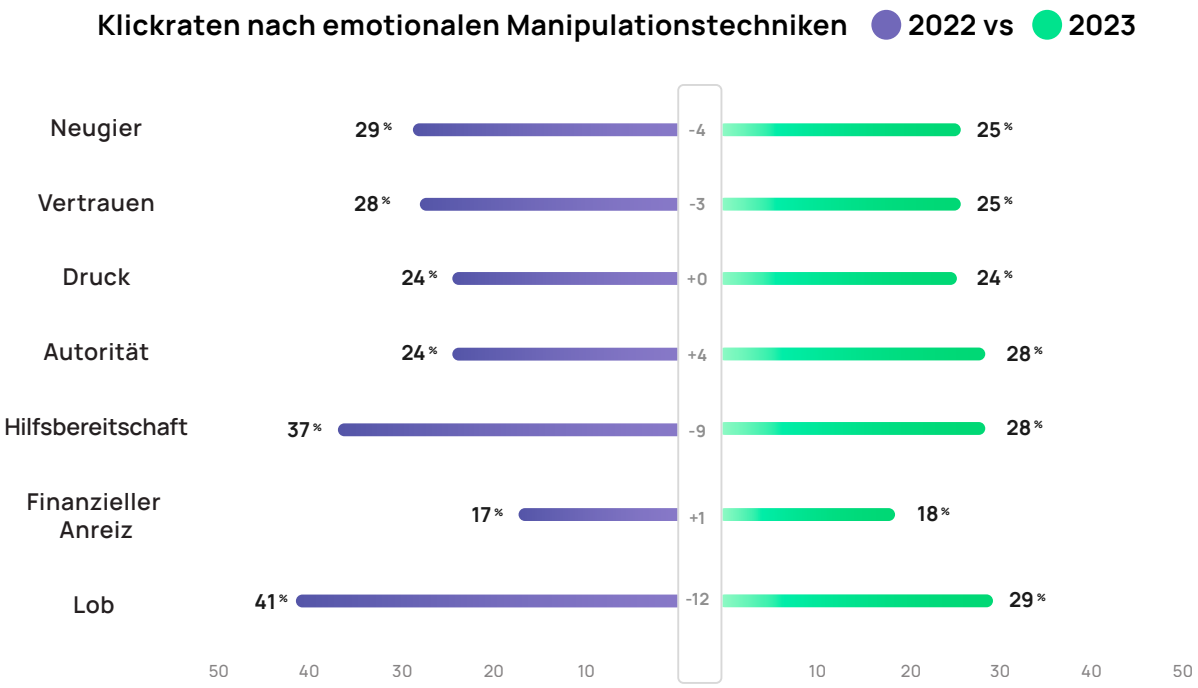
Klickraten nach Angriffsmethode

Typo-Squatting	Subdomain-Squatting
17%	**26%**
E-Mail-Spoofing	Domain-Squatting
29%	**20%**

Die Psychologie der emotionalen Täuschung

Social Engineering ist aus einem Grund für die Zwecke der Cyberkriminellen besonders attraktiv – aufgrund der Anpassbarkeit. Kaum eine andere Angriffstaktik kann so gezielt auf aktuelle gesellschaftliche oder politische Entwicklungen abgestimmt werden, um die Menschen hinter den Bildschirmen zu manipulieren. Das veranschaulichen die psychologischen Vektoren von Phishing-Kampagnen auf beeindruckende Weise. Letztlich bestimmen zwei Faktoren, wie viele Menschen auf schädliche Inhalte klicken: Wie überzeugend die Inhalte der E-Mail sind und ob sie die User auf emotionaler Ebene erreichen.

Im Vergleich zu 2022 lässt sich eine leichte Veränderung bei den emotionalen Hebeln in Phishing-Mails beobachten, die besonders erfolgreich hinters Licht führen. Das Hervorrufen positiver Gefühle durch das Vorgaukeln von Lob oder Hilfsbereitschaft führt zwar immer noch zu einer höheren Klickrate. Gleichzeitig ist aber die Erfolgsrate von Taktiken, die negative Emotionen auslösen sollen – wie durch den Einsatz von Autorität, Druck oder finanziellen Versprechen – leicht angestiegen. Die Menschen scheinen für diese Art von emotionaler Manipulation und Ausbeutung allgemein anfälliger geworden zu sein. Eine mögliche Erklärung für diese Entwicklung ist, dass die Menschen aufgrund der weltweiten Krisen und Konflikte der letzten Jahre generell ängstlicher und verunsichert sind. Als Folge ist es für Angreifende leichter, negative Emotionen bei ihnen hervorzurufen.



Auch ein Blick auf die Betreffzeilen zeigt, dass Mitarbeitende anfälliger für negative Emotionen geworden sind: vier der fünf erfolgreichsten Betreffzeilen nutzen ein Element des Drucks.

Die Top 5 der Phishing-Betreffzeilen 2022

1. Auto beschädigt (Druck/Neugier)
2. Teams-Einladung (Neugier)
3. Fehler in der Gehaltsabrechnung (Druck/Neugier)
4. Ihr Office Passwort läuft heute ab (Druck)
5. Teams verpasste Chatnachricht (Druck/Neugier)

Warum Security Awareness Training im Kampf gegen Phishing unerlässlich ist

Trotz allem gibt es auch gute Nachrichten: Mitarbeitende können für diese und andere Social-Engineering-Taktiken durch modernes Security Awareness Training sensibilisiert werden. Die Daten der SoSafe Awareness-Plattform zeigen, dass die Phishing-Meldequote durch eine **Kombination aus gamifiziertem E-Learning, Phishing-Simulationen und kontextbezogenen Reporting-Tools auf bis zu 80 Prozent gesteigert** werden kann. Dieser Wert wirkt sich wiederum direkt positiv auf die Informationssicherheit von Organisationen und deren Reaktionsfähigkeit im Falle eines Angriffs aus (mehr dazu im Ausblick). Bei der Umsetzung der Trainingsmaßnahmen sollte stets der Mensch im Vordergrund stehen.

Erkenntnisse aus der Verhaltenswissenschaft helfen dabei, die effektivsten Trainingsmethoden zu finden und sichere Verhaltensweisen im Team nachhaltig zu fördern. Ansätze wie das „Behavioral Security Model“, das auf dem Zusammenspiel aus Kontext, Wissen, Motivation und Verhalten basiert, können für Sicherheitsbeauftragte als wertvoller Wegweiser beim Aufbau einer nachhaltigen Sicherheitskultur dienen (siehe auch Human Risk Review 2022).

> Es herrscht die Überzeugung, dass es für den Cyberraum keine Regulierungen gibt, was schlichtweg falsch ist. Es gibt sehr wohl Cybersicherheitsgesetze – sie werden bloß nicht ausreichend vollstreckt.

Stéphane Duguin
CEO CyberPeace Institute

Stéphane Duguin ist CEO des CyberPeace Institute und analysiert seit zwei Jahrzehnten, wie Technologie als Waffe gegen gefährdete Gemeinschaften eingesetzt wird. Er sitzt im Vorstand der Datasphere Initiative, ist Mitglied des Beirats des Global Forum on Cybercrime Expertise (GFCE) und ein Vordenker im Bereich digitale Transformation und Konvergenz disruptiver Technologien. Zuvor war Stéphane Duguin Senior Manager bei Europol, wo er wichtige operative Projekte zur Bekämpfung von Cyberkriminalität und Online-Terrorismus leitete.

Bei der Arbeit des CyberPeace Institute steht der Mensch im Fokus. Wie können sich Cyberangriffe Ihrer Erfahrung nach auf einzelne Personen auswirken?

Wir sollten uns stets bewusst sein, dass die meisten Cyberangriffe mit der emotionalen Reaktion ihrer Zielpersonen spielen, das heißt, die Manipulation spielt eine entscheidende Rolle. Ransomware ist beispielsweise eine der wenigen Angriffsmethoden, bei denen das Opfer als Komplize agieren muss. Tappt man in die Falle von Erpressungssoftware, steht man vor komplizierten Entscheidungen mit psychologischem Faktor, wie: Zahle ich das Lösegeld oder melde ich den Angriff?

Als zweiter Faktor kommen die Schuldgefühle der Zielperson ins Spiel. NGOs werden sehr häufig Opfer von CEO-Fraud. In solchen Fällen muss sich die Person, die den Fehler begangen hat, vor der gesamten Organisation verantworten.

Eine weitere Folge betrifft eher das System und hängt von der Art von Aktivität der jeweiligen Organisation ab – und zwar die Auswirkungen auf die Begünstigten der NGO. Das Gesundheitssystem ist hier ein gutes Beispiel. Eine Studie der Vanderbilt-Gruppe zeigte, dass die Nachwirkungen eines Cyberangriffs in Krankenhäusern noch Monate – oder sogar Jahre – danach spürbar sein können. So stieg bei Patientinnen und Patienten in kritischem Zustand das Risiko für einen tödlichen Ausgang aufgrund der Tatsache, dass sie nicht dieselben hohen Standards an Pflege erhielten.

Auch die langfristigen psychologischen Auswirkungen für die Zielperson sind nicht zu unterschätzen. Ein sehr gutes Beispiel hierfür ist der Ransomware-Angriff auf die Vastaamo Clinic in Finnland. Nachdem das Krankenhaus die Lösegeldzahlung verweigerte, erpressten die Cyberkriminellen alle Patienten und Patientinnen damit, ihre privaten Informationen zu ihrem psychologischen Befinden zu veröffentlichen. Damals war Finnland gezwungen, eine Ad-hoc-Opferhilfe zu organisieren, um mehr als 25.000 Personen zu betreuen.

Wie hat sich die Cyber-Bedrohungslage Ihrer Ansicht nach im vergangenen Jahr verändert?

Das Cybercrime-as-a-Service-Geschäftsmodell hat deutlich an Fahrt aufgenommen. Kriminelle Gruppierungen machen außerdem verstärkt Gebrauch von innovativen Technologien. Cyberkriminelle schließen sich häufig zusammen und machen sich nun neue Technologien als Angriffsvektoren zunutze. Das wird heute mit ChatGPT deutlich, aber war auch schon lange vorher zu beobachten, als die ersten Deepfakes auftauchten.

Zweitens sehen wir keine Verbesserung in den staatlichen Schutzmaßnahmen der Bevölkerung vor Cyberangriffen. Dazu müssten Gesetze, Normen und Richtlinien im Cyberspace konsequenter umgesetzt werden. Es herrscht die Überzeugung, dass es für den Cyberraum keine Regelungen gibt, was schlichtweg falsch ist. Es gibt sehr wohl Cybersicherheitsgesetze – sie werden bloß nicht ausreichend vollstreckt. Die Ressourcen der Strafverfolgung reichen nicht aus, um systematisch gegen Cyberkriminelle vorzugehen. Überwachungsangriffe sind ein weiterer Aspekt, der uns zeigt, dass Länder nicht aktiv zur Verbesserung der Bedrohungslage beitragen – im Gegenteil: Indem Staaten ihre Ressourcen weiterhin zur Durchführung von Überwachungsangriffen nutzen, investieren sie aktiv in eine globale Cyber-Unsicherheit, denn damit solche Überwachungen funktionieren, sind sie auf Schwachstellen im Cyberspace angewiesen.

Die dritte Problematik besteht bereits seit längerer Zeit, ist heute aber durch den Ukraine-Krieg besonders relevant geworden: die „Zivilisierung" von Cyberangriffen. Das heißt, die Zivilbevölkerung wird durch Krisen oder Konflikte dazu getrieben, sich an großflächigen Cyberangriffen zu beteiligen. Zum Beispiel gab es russische Gruppen von Kriminellen, die jede Person angriffen, die sich gegen die Interessen Russlands äußerte, und Hacker, die sich freiwillig der ukrainischen IT-Armee anschlossen. Diese Art von Crowdsourcing von Cyberangriffen ist äußerst besorgniserregend, da es die Grenzen zwischen Zivilpersonen, Militär und Opfern immer mehr verschwimmen lässt.

Neue Tools wie ChatGPT haben zu einem regelrechten Boom der künstlichen Intelligenz gesorgt. Wie wird sich das Ihrer Meinung nach auf die Cyber-Bedrohungslage auswirken?

KI hat schon 2017 für viele Entwicklungen im Bereich Deepfake-Engineering gesorgt. Seitdem ist einige Zeit vergangen. Heute ist es für Hackergruppen ein Leichtes, die Menschen mit extrem überzeugenden und authentischen Inhalten zu manipulieren – sei es durch die Imitation von Stimmen, Gesichtern oder durch ausgeklügelte E-Mails. Darüber hinaus werden KI-basierte Technologien eingesetzt, um unser soziales Ökosystem auszuspionieren, mit dem Ziel, effiziente Social-Engineering-Angriffe oder Angriffsvektoren zu entwickeln.

Eine weitere Methode, die unter Cyberkriminellen immer beliebter wird, sind generative KI-Angriffe bzw. KI-basierte Angriffsmethoden. Angriffe können so besser automatisiert und die Infrastruktur leichter aufgedeckt werden. Im Rückschluss bedeutet das: Wir müssen verstärkt KI-Tools einsetzen, um uns besser vor Angriffen zu schützen.

> Das führt uns zu dem zugrunde liegenden Problem, das wir derzeit in der Cyber-Security-Industrie überall beobachten können: Burnout. Wir haben zu viele Daten, zu viele Fälle, aber nicht genug Zeit.

Da wir gerade von den Vorteilen von KI als Teil unserer Cybersicherheit sprechen: Welche Herausforderungen prognostizieren Sie bei einer solchen Verwendung von KI?

Ein großes Risiko besteht darin, dass die künstliche Intelligenz massive Datenmengen hervorbringt, die dann von echten Menschen überprüft werden müssen. Das führt uns zu dem zugrunde liegenden Problem, das wir derzeit in der Cyber-Security-Industrie überall beobachten können: Burnout. Wir haben zu viele Daten, zu viele Fälle, aber nicht genug Zeit. KI wird diese Problematik leider weiter verschärfen, da sie die Datenmenge um ein Vielfaches erhöhen wird – eine beunruhigende Vorstellung.

Aus einem breiteren Blickwinkel betrachtet ist einer der Gründe für Burnout, dass man den Wert der eigenen Arbeit nicht mehr sieht. In der Ära der künstlichen Intelligenz ist die Wahrscheinlichkeit, den Unterschied zwischen echten und manipulierten Materialien zu erkennen, eher gering, was das Fundament der Demokratie ins Wackeln bringt. Als Folge kann zum Beispiel vor Gericht jeder behaupten, dass die Beweise manipuliert wurden. Dieser Zweifel bringt das gesamte System, in dem digitale Forensiker und Sicherheitsexperten tätig sind, zum Einstürzen und sie verlieren den Glauben an ihre Arbeit.

Demografische Erfolgsvektoren von Social-Engineering-Angriffen

Cyberkriminelle planen ihre Angriffe bis ins kleinste Detail. Es gibt unabhängig davon aber auch einige demografische Variablen, die die Erfolgsrate ihrer Methoden beeinflussen. Das Alter ist und bleibt beispielsweise ein entscheidender Faktor, der sich in der Klickrate auf schädliche Inhalte in Phishing-Mails widerspiegelt: Bei „Digital Natives“ ist die Wahrscheinlichkeit eines Klicks um 65 Prozent höher als bei Usern älterer Altersgruppen. Eine mögliche Erklärung dafür könnte sein, dass ältere Nutzer dank ihrer Erfahrung und ihres eher vorsichtigen Online-Verhaltens potenzielle Bedrohungen zuverlässiger erkennen und abwehren. Im Gegensatz dazu bringen jüngere Menschen (in dieser Analyse im Alter zwischen 18 und 40 Jahren), die mit modernen Technologien aufgewachsen sind, digitalen Kommunikationsmitteln gegenüber mehr Vertrauen mit. Sie hinterfragen Inhalte tendenziell weniger kritisch als ältere User (in dieser Analyse zwischen 41 und 60 Jahren).

Jüngere User (18-40 Jahre) klicken mit

↗ 65%

höherer Wahrscheinlichkeit auf Phishing-Mails als ältere User (41-60 Jahre).

Wir müssen die Wahrscheinlichkeit, dass es zu einem Cyberangriff kommt, von Anfang an stärker in die Kultur und unsere tägliche Arbeit mit einbinden.

Thomas Schumacher
Managing Director Accenture Security

Sektoren im Fadenkreuz

Die Erfolgsraten von Social-Engineering- und Phishing-Angriffen unterscheiden sich auch je nach Branche der Organisationen. Branchen, die stark von den jüngsten gesellschaftlichen Entwicklungen betroffen sind, weisen zum Beispiel die höchsten Phishing-Klickraten auf – darunter die Logistik-, Energie- und Tourismusbranche. Die niedrigsten Klickraten finden sich hingegen in Branchen, in denen vergleichsweise wenige Mitarbeitende am Computer arbeiten, wie die Landwirtschaft, das Bauwesen und die Chemie- und Rohmaterialbranche.

Branche	Klickrate
Transport und Logistik	38%
Energie und Umwelt	35%
Tourismus und Gastronomie	35%
Pharma und Gesundheit	33%
E-Commerce	32%
Bildung	31%
Dienstleistung und Handwerk	29%
Finanzen, Versicherungen und Immobilien	28%
Technologie und Telekommunikation	27%
Metall und Elektronik	26%
Medien und Marketing	25%
Konsum und FMCG	25%
Handel	24%
Zivilgesellschaft	24%
Verwaltung und Verteidigung	24%
Internet	23%
Freizeit	23%
Landwirtschaft	20%
Bauwesen	20%
Wirtschaft und Politik	20%
Chemie und Rohmaterialien	16%

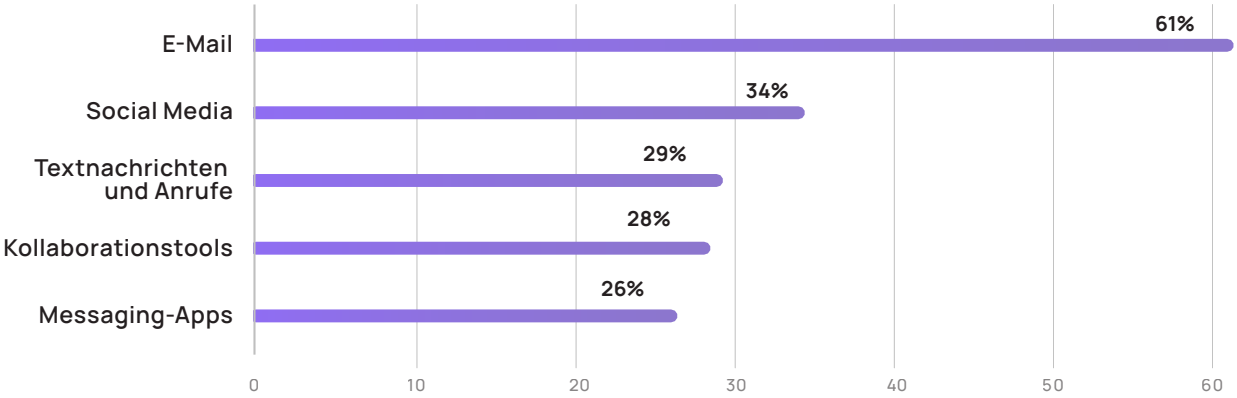
Die Zukunft von Phishing: Von E-Mails zu Kollaborationstools und Social Media – was kommt als Nächstes?

Innovation ist die engste Verbündete der Cyberkriminellen. So haben sie nicht nur technische, psychologische und demografische Vektoren gefunden, mit denen sie ihre Angriffstaktiken optimieren können. Sie finden dank innovativer Technologien auch stetig neue Tools zur Umsetzung dieser Strategien. Während E-Mail-basierte Betrugsmaschen weiterhin zu den meistgenutzten gehören, so werden auch andere Kanäle immer häufiger für Cyberangriffe genutzt.

E-Mails sind schon längst nicht mehr der einzige relevante Kommunikationskanal für Unternehmen. Immer öfter kommen auch andere Kollaborations- und Kommunikationstools, oft sogar in Kombination, zum Einsatz – eine vielversprechende Aussicht für die Cybercrime-Industrie.

Die ersten Multi-Channel-Angriffe haben bereits schwere Folgen nach sich gezogen, wie zum Beispiel der Angriff auf Uber.[1] In diesem Fall wurde ein Mitarbeiter dazu gebracht, eine Multifaktor-Authentifizierung durchzuführen, indem sich die Hacker über WhatsApp als Kolleginnen und Kollegen aus der IT-Abteilung ausgaben. Daraufhin war das Unternehmen gezwungen, einen Großteil seiner Systeme vom Netz zu nehmen, um einen weiteren Zugriff auf sensible Daten durch die Angreifenden einzuschränken.

Kanäle, über die Organisationen 2022 angegriffen wurden



> **Wenn wir in neue Technologiesphären reingehen, müssen wir die Risiken von Anfang an mitdenken. Sonst wird das in einer Katastrophe enden.**
>
> **Thomas Tschersich**
> CSO Deutsche Telekom

Organisationen sind nur unzureichend vor den Social-Engineering-Taktiken der Cyberkriminellen geschützt. Dabei entwickeln diese immer ausgefeiltere Methoden und technologische Entwicklungen schreiten im Minutentakt voran – der beste Beweis sind derzeit generative KI-Tools. Diese Entwicklungen haben bereits viele Organisationen dazu bewegt, verstärkt Ressourcen in ihre Sicherheitskultur zu investieren und dabei den Faktor Mensch in den Fokus ihrer Strategien zu rücken.

1 **Infopoint Security (2022).** Ransomware-Attacken auf Uber und Rockstar – ist MFA nicht sicher genug?

Eine umfassende Security-Strategie sollte die drei Themengebiete Technologie, Mensch und Prozesse einschließen.

Thomas Schumacher
Managing Director Accenture Security

Thomas Schumacher leitet das Security-Geschäft bei Accenture für Österreich, Schweiz und Deutschland (ASG). Er ist zudem Mitglied des ASG Leadership Teams, sowie des globalen Accenture Security Leadership Teams. Herr Schumacher berät seit über 20 Jahren führende deutsche Unternehmen in Fragen der IT-Sicherheit sowie zum Betrieb von sicheren IT-Infrastrukturen. Er ist Experte für komplexe Transformationsprojekte in verschiedenen Industrien, insbesondere im Kontext von Digitalisierung, Post-Merger-Integration und Steigerung der IT-Effizienz.

Was ist Ihrer Meinung nach der wichtigste Punkt, den Unternehmen in Bezug auf ihre Sicherheitsstrategie im Blick behalten sollten?

Das Thema Cybersicherheit und Cyberresilienz, wie wir es bei Accenture nennen, fängt aus meiner Sicht strategisch an. Eine umfassende Strategie sollte die drei Themengebiete Technologie, Mensch und Prozesse einschließen. Unternehmen müssen Fragen wie „Was ist meine DNA?“, „Was muss auf jeden Fall laufen, damit ich meinen Geschäftsbetrieb aufrechterhalten kann?“, und „Was will ich überhaupt absichern?“ beantworten können. Erst, wenn ich diese Übung abgeschlossen habe, kann ich mir überlegen, wie ich das am besten angehe. Viele Unternehmen gehen diesen Prozess noch recht planlos an. Das zeigt sich dann spätestens im Falle eines Angriffs.

Sie nennen den Menschen als einen Aspekt in einer solchen Strategie. Welche Rolle spielen die Mitarbeitenden Ihrer Meinung nach konkret?

Ich kann natürlich immer sagen: Mitarbeitende werden früher oder später irgendwo draufklicken. Das ist wahrscheinlich auch so, denn wir können uns nicht vor allem schützen. Die Frage ist aber, wie schnell alle Schutzbarrieren fallen. Ich muss die drei Dimensionen Technologie, Mensch und Prozesse deshalb synchronisieren. Aus meiner Sicht ist man schlecht beraten, wenn man auf Technologie allein setzt, weil die Kosten überproportional steigen. All das, was ich durch Schulungen und Awareness von Mitarbeitern abdecken kann – unterstützt von der richtigen Technologie – macht mich per se erstmal resilienter. Denn die Human Layer schützt Unternehmen nicht nur vor Angriffstaktiken, die auf einen konkreten Anwendungsfall zugeschnitten sind. Ich spare so Geld, Zeit und natürlich auch Nerven und Risiko.

Wo besteht die größte Herausforderung in Bezug auf auf den Faktor Mensch?

Die größte Herausforderung sehe ich in unserer Fehlerkultur. Wenn es doch einmal zu einem Klick auf eine Phishing-Mail kommt, brauchen wir nicht die Mentalität: Klappe zu, ich sage es keinem. Sondern dann kommt es wirklich darauf an, dass schnell gehandelt wird, dass schnell gemeldet wird, dass man sich dessen bewusst ist, was da gerade passiert.

Ist das ein Faktor, der generell durch die Unternehmenskultur beeinflusst wird?

Das ist wie in der Kindererziehung. Ich selbst habe einen großen Bruder – ich habe relativ schnell gelernt zu leugnen, wenn es hart auf hart kommt. Das ist aber nicht besonders clever, denn später explodiert das Problem dann. Deswegen ist es so wichtig, eine Meldekultur zu schaffen und zu sagen: es ist okay – sogar gut – wenn jemand sich schnell meldet. Gerade im Mittelstand ist diese Einstellung nicht weit verbreitet – besonders dann, wenn schon finanzielle Forderungen oder Verluste auf dem Tisch liegen.

Wie kann man diese Kultur denn positiv beeinflussen?

Ich glaube, der erste Punkt ist, nochmal zu betonen: Wir können Angriffe und menschliche Fehler nicht verhindern. Wir müssen die Wahrscheinlichkeit, dass etwas passiert, von Anfang an stärker in die Kultur und unsere tägliche Arbeit mit einbinden. Außerdem sollten wir die Meldewege so beschleunigen oder vielleicht sogar so anonymisieren, dass am Ende Konsequenzen gar nicht mehr auf Einzelpersonen zurückfallen. Das ist gerade in großen Unternehmen einfacher, weil der Bezug zum Verlust und zum Investment, das getätigt werden muss, kleiner ist als bei einer Privatperson.

Wenn wir uns konkret den Bereich Security Awareness anschauen: Beobachten Sie eine Entwicklung weg von Pflichtunterweisungen und Policies hin zu kontinuierlichem Training?

Ich nehme immer noch wahr, dass Unternehmen stark Compliance-getrieben handeln. Aber natürlich sehen immer mehr mittlerweile die Notwendigkeit für Schulungen der Mitarbeitenden. Besonders im Hinblick auf Remote-Mitarbeitende liefert ein Security-Grundwissen einen echten Mehrwert. Wir sehen zudem, dass manche Unternehmen denken, sie müssten dafür selbst Lösungen bauen. Aber es gibt mittlerweile viele Tools am Markt, die diesen Bereich konkret abdecken.

Gehen große und mittelständische Unternehmen Security Awareness unterschiedlich an?

Bei großen Unternehmen ist es aus meiner Sicht ein grundsätzliches Problem, dass sie glauben, sie hätten die Dinge im Griff. Ich würde da aber kein Unternehmen ganz von freisprechen, weil das Thema Cyberresilienz in sich ein sehr komplexes ist. Vielleicht müssen wir den Bogen etwas größer spannen: Wir sind gerade in einer Zeit, in der wir uns vor Cyberangriffen, vor physikalischen Bedrohungen, vor einer Pandemie und vor Naturkatastrophen absichern müssen. Das sind viele große Geschäftsrisiken auf einen Schlag. Darauf eine Antwort zu finden ist viel schwieriger als „nur“ für Cyberbedrohungen. Die Komplexität sorgt aber auch noch einmal für eine ganz andere Dimension im Bereich Cyber: Ich muss meine Mitarbeitenden auf komplett neue Szenarien vorbereiten, zum Beispiel darauf, dass sie plötzlich gar nicht mehr in meinen Filialen arbeiten können. Wir müssen Cyberresilienz und Business-Resilienz viel stärker zusammenbringen.

> Es ist enorm wichtig, eine Meldekultur zu schaffen und zu sagen: es ist okay – sogar gut – wenn jemand einen selbst verursachten Vorfall schnell meldet.

Wird kontinuierliches Awareness-Training durch diese angespannte Lage notwendiger?

Nicht nur die Technologie entwickelt sich weiter, sondern auch die Angriffe. Im Grunde genommen müssen die Menschen deshalb auch ein Stück weit ihre täglichen Gewohnheiten darauf ausrichten. Es ist ein Klassiker: Ich stelle fest, die Zeit hat sich geändert, gegebenenfalls auch durch technische Entwicklungen, aber ich mache immer noch so weiter wie vor 20 Jahren. Deshalb glaube ich: Wir müssen weg davon, den Leuten zu sagen, was zu tun ist und dafür sorgen, dass sichere Verhaltensweisen in persönliche Fähigkeiten übergehen. Und die Gründe dafür sind nicht einmal nur auf den Arbeitsplatz beschränkt. Wenn ich heute ein Auto kaufe und das besitzt die „Keyless Go"-Technologie, muss ich mich auch damit auseinandersetzen, dass die Dinge vernetzt sind und mein Verhalten dementsprechend anpassen. Wir müssen also weiterhin auch im Privatleben diesen Sicherheitsgedanken stärken und kontinuierlicher in unseren Alltag einpflegen. Damit jeder selbst in der Lage ist, sein Verhalten jederzeit zu hinterfragen.

Die technologische Innovation, die Sie ansprechen, ist längst da, aber Angreifer springen nicht höher als sie müssen. Nehmen Sie das auch so wahr?

Ja, die Angriffe sind oft ganz banal und kommen trotzdem zum Erfolg. Wir sehen aber auch destruktive Attacken von Angreifern, die so hohe finanzielle Mittel haben, dass alles möglich ist. Ich bin mir ziemlich sicher: Der erste Quantencomputer wird bei irgendeinem Angreifer stehen, der ihn benutzt, um kryptografische Verfahren aufzulösen. Wir müssen uns darüber im Klaren sein, dass die Angreifer zum Teil enorme Mittel haben und uns entsprechend vorbereiten.

Das klingt alles recht bedrohlich. Muss man den Menschen vielleicht auch die Angst vor dem Thema nehmen?

Angst ist immer ein schlechter Berater. Die Frage ist vielmehr: Was kann man tun? Wo kann man helfen? Es ist nicht aussichtslos. Man muss nur eben ein paar Grundregeln, ein paar Spielregeln haben.

Wie haben sich die Security-Budgets entwickelt? Passen sie sich dieser Entwicklung an?

Man muss auch hier wieder zwischen großen Unternehmen und dem Mittelstand unterscheiden – und da auch nochmal branchenspezifisch. Die ganze Finanzindustrie, also Banken und Versicherer, werden seit 2014 quasi von der Aufsicht dazu gedrängt, die Initiative zu ergreifen. Sie haben die Phase überstanden, in der „Angst-machen" Budgets freisetzt. Diese Unternehmen sind sehr kontrolliert und restriktiv in ihren Investitionen, weil sie gelernt haben, mit dem Thema umzugehen. Was dort immer noch eine Frage ist, ist: Investieren sie richtig? Ich glaube, nein, weil immer noch zu viel toolbasiert eingekauft wird. Und man eben glaubt, dass man Risiken mit einem neuen Tool komplett loswerden kann.

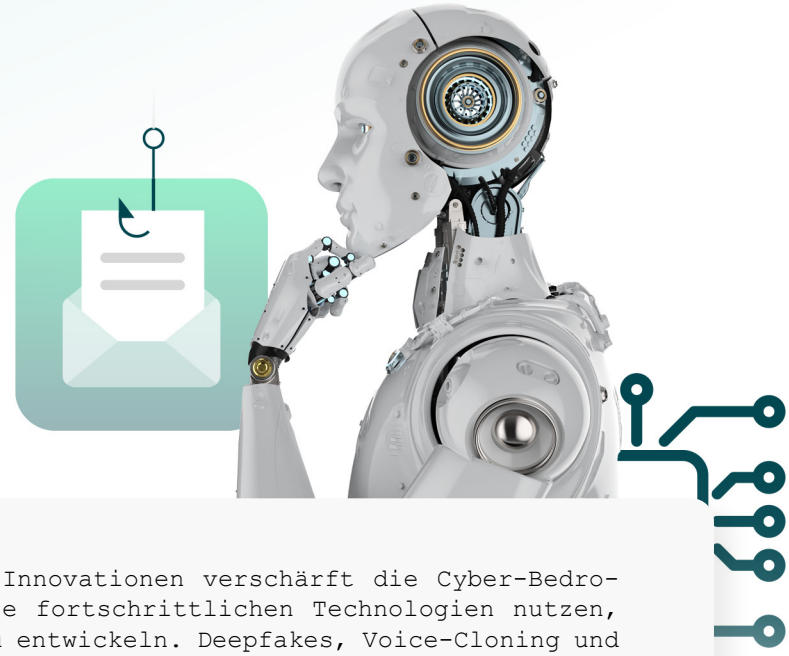
Ich glaube prinzipiell, dass die Budgets nicht mehr ganz so leicht verfügbar sind. Im Mittelstand ist das noch ein bisschen anders. Viele dachten, Cyber betrifft mich nicht, aber haben jetzt über Angriffe gemerkt: das betrifft gerade mich. Hier besteht gerade die große Gefahr, dass planlos Dinge eingeführt werden und rein technisch gelöst werden sollen. Oft haben diese Unternehmen gar keine internen IT-Abteilungen. Wir brauchen also eine neue Generation von Unternehmern, die die Cyberrisiken neben den Marktrisiken einschätzen können.

Was möchten Sie anderen Security-Verantwortlichen mit auf den Weg geben?

Der erste Punkt ist: Es geht bei Cyberresilienz um ein gesellschaftliches Problem, das gelöst werden muss. Das heißt, wir müssen alle zusammen an der Lösung arbeiten – umso erfolgreicher sind wir.

Der zweite Punkt ist: Wir werden keine Goldmedaillen damit verdienen, wer am besten mit den Risiken zurechtkommt. Es geht hier um das „Überleben". Das ist vielleicht ein bisschen apokalyptisch, aber es trifft die Situation ganz gut. Die Gefahr ist da, und das müssen wir stärker kommunizieren, ohne den Menschen Angst zu machen.

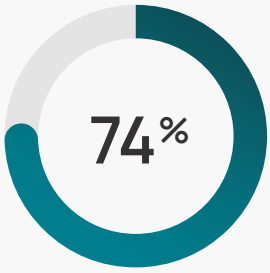
Wenn KI auf Cybercrime trifft:
Eine explosive Mischung



Die Verbreitung von KI-Innovationen verschärft die Cyber-Bedrohungslage, da Hacker die fortschrittlichen Technologien nutzen, um neue Angriffsarten zu entwickeln. Deepfakes, Voice-Cloning und KI-gestütztes Phishing sind zu wirkungsvollen Waffen geworden, während KI-Tools die Cyberkriminalität demokratisieren, indem sie das Entwerfen bösartiger E-Mails und Software vereinfachen. Parallel dazu werfen Anwendungen wie ChatGPT erhebliche Datenschutzbedenken auf, da der mögliche Missbrauch sensibler Informationen zu weiteren Cyber-Schwachstellen führen könnte.

Darüber hinaus hat KI das Potenzial, soziale Manipulation zu verstärken und globale Spannungen zu verschärfen, indem ihre Fähigkeiten für Desinformation und Propaganda genutzt werden. Auch biometrische Authentifizierungssysteme, die einst als sicher galten, sind bedroht, da KI-Tools solche Sicherheitsmaßnahmen umgehen können. In einer Welt, die von digitalen Entwicklungen und globalen Krisen geprägt ist, braucht es einen proaktiveren Ansatz bei der Cybersicherheit und eine Neubewertung der aktuellen Verteidigungsstrategien.

Diese Einführung wurde von ChatGPT-4 erstellt.



der Sicherheitsbeauftragten gehen davon aus, dass künstliche Intelligenz die Cyber-Bedrohungslage verschärfen wird.

KI-basiertes Social Engineering: Deepfakes und Voice-Cloning

Deepfake-Technologien gibt es nicht erst seit kurzem. Trotzdem sind sie derzeit in aller Munde, und das aus gutem Grund: Angreifende nutzen sie immer öfter zur **großflächigen Manipulation** und zur **Intensivierung geopolitischer Spannungen**. Die inszenierte Kapitulation vonseiten des ukrainischen Präsidenten Selenskyj, die sich im Nachhinein als Deepfake-Video entpuppte, veranschaulichte das 2022 nur zu deutlich.[1]

Doch Cyberkriminelle schrecken auch in Bereichen abseits der Politik nicht vor dem Einsatz von Deepfake-Technologien zurück. Mit Taktiken, in denen sie Vishing mit Voice-Cloning kombinieren, greifen Cyberkriminelle oft erfolgreich Daten und Geld von Einzelpersonen wie auch Organisationen ab. In einem der jüngsten Beispiele täuschte man einer Mutter in Arizona vor, ihre 15-jährige Tochter sei gekidnappt worden, indem man ihr die verzweifelten Schreie ihrer Tochter am Telefon vorspielte. Letztlich stellte sich heraus, dass sich die Tochter in Sicherheit befand und ihre Stimme künstlich imitiert worden war. Die Mutter gab später an, dass sie nie in Frage gestellt hatte, ob es sich wirklich um die Stimme ihrer Tochter handelte.[2] In einem anderen Fall imitierten die Angreifenden per Deepfake-Audio die Stimme eines CEO und brachten Mitarbeitende dazu, 35 Millionen US-Dollar an eine kriminelle Gruppierung zu überweisen.[3] Und die Technologie wird **immer fortschrittlicher**, zum Beispiel durch neue Tools wie VALL-E von Microsoft, das schon mit einer drei-sekündigen Sprachvorlage Stimmen perfekt imitieren kann.[4]

Immer mehr Organisationen steigen heute außerdem auf biometrische Authentifizierungsmethoden um, die eine sicherere Alternative zu Passwörtern und PINs bieten sollen. Aber auch diese Methoden könnten durch Voice-Cloning und Video-Deepfakes umgangen werden. In einigen Teilen der USA wurde deshalb in Regierungskreisen die Nutzung von Gesichtserkennungssoftware bereits verboten.[5] Während sich Deepfake-Technologien weiterentwickeln und sich somit neue Einsatzbereiche eröffnen, müssen sich **der öffentliche und der private Sektor** gemeinsam dafür einsetzen, das **Bewusstsein** über die Möglichkeiten und Grenzen solcher Technologien zu steigern.

Ausnutzung generativer KI: ChatGPT als Angriffsvektor

Cyberkriminelle nutzen neue KI-Tools zur Optimierung ihrer Angriffsmethoden – insbesondere ihrer Social-Engineering-Taktiken. Generative

1 **Golem (2022).** Meta löscht gefälschtes Selenskyj-Video.

2 **Golem (2023).** Mutter wird von KI-Stimme ihrer Tochter getäuscht.

3 **Dark Reading (2021).** Deepfake audio scores $35M in Corporate Heist.

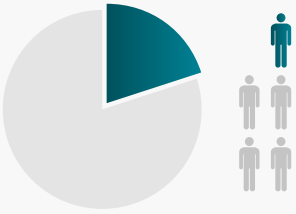
4 **ZDNet (2023).** VALL-E: AI-Modell für Text-to-Speech von Microsoft simuliert Stimmen.

5 **Built in (2023).** 5 AI trends to watch in 2023.

KI-Tools wie ChatGPT verbieten zwar ausdrücklich die Nutzung zu betrügerischen Zwecken. Trotzdem finden Angreifende immer wieder einen Weg, derartige Einschränkungen zu umgehen.

Phishing-Mails, die von ChatGPT oder anderen generativen KI-Tools erstellt wurden, sind extrem personalisiert und so präzise formuliert, dass sie **weniger verdächtig** wirken als vom Menschen verfasste Phishing-Mails. Für Spamfilter, aber auch für den Menschen wird das **Erkennen solcher Phishing-Mails so zu einer immer größeren Herausforderung**.

Eine kürzlich vom Social-Engineering-Team von SoSafe durchgeführte Studie zeigte, dass Phishing-Mails mit generativen KI-Tools 40 Prozent schneller erstellt werden können. Die Daten – basierend auf 1.500 simulierten Phishing-Attacken von der SoSafe Awareness-Plattform, die im März 2023 anonym ausgewertet wurden – zeigten außerdem: Durch KI erstellte Phishing-Mails werden von 78 Prozent der Personen geöffnet. Von diesen Personen klickte im Folgenden jede fünfte in der E-Mail auf schädliche Inhalte wie Links oder Anhänge.[6] 65 Prozent gaben sogar weitere Informationen in Eingabefeldern preis. Und das ist erst der Anfang: Dieser Test wurde mit nicht-personalisierten, von ChatGPT-3.5 generierten Phishing-Mails durchgeführt. Tagtäglich kommen jedoch weitere, moderne Sprachmodelle auf den Markt und bestehende Tools entwickeln sich in rasantem Tempo weiter. Schon der Schritt von ChatGPT-3 auf ChatGPT-4 hat die Personalisierung der Inhalte auf ein nie dagewesenes Level gebracht.



Jede **5. Person**
klickt auf KI-generierte Phishing-Mails.

Phishing ist jedoch nur eine von vielen Angriffstaktiken, die Cyberkriminelle mithilfe von KI optimieren. Mit KI-Technologien kann beispielsweise jede Person – ohne technische Vorkenntnisse – ausgeklügelte polymorphe Malware erstellen, die traditionelle Sicherheitsmechanismen einfach umgeht.[7] Nützliche Tools werden so zur frei zugänglichen Cyberwaffe und führen somit zur Demokratisierung der Cyberkriminalität.

> **Die Sicherheitsmechanismen greifen nur, wenn die KI erkennt, dass jemand sie dazu auffordert, bösartigen Code zu schreiben. Gibt man den Befehl in einzelnen Schritten ein, lassen sich diese Sicherheitsvorkehrungen einfach umgehen.**
>
> **EUROPOL** [8]

6 **SoSafe (2023).** Jeder Fünfte klickt auf KI-erstellte Phishing-Mails.

7 **ZDNet (2023).** ChatGPT wird zum Schreiben von Malware eingesetzt.

8 **EUROPOL (2023).** ChatGPT The impact of Large Language Models on Law Enforcement.

9 **Heise (2023).** ChatGPT: Datenleck ermöglichte Einsicht in Informationen fremder Benutzer.

10 **Tagesschau (2023).** Italien sperrt ChatGPT.

11 **Datenschutz-Praxis (2023).** Maschinelles Lernen: neue Ansätze beim Datenschutz.

12 **European Commission (2023).** Intellectual Property in ChatGPT.

ChatGPT – Sind Ihre Daten sicher?

KI-Tools benötigen immense Datenmengen. Dies ruft unter Einzelpersonen und Organisationen unweigerlich Bedenken zum Datenschutz und zur Sicherheit der Informationen hervor, die sie bei der Eingabe von Befehlen preisgeben.

Was sind die Risiken?

Anfang dieses Jahres sorgte ein relativ einfacher Bug dafür, dass User von ChatGPT die Chatverläufe und sogar die E-Mail-Adressen und Telefonnummern anderer User einsehen konnten.[9] Dieser Vorfall verdeutlichte die Tücken, die in der Speicherung und Nutzung sensibler Daten durch OpenAI liegen. Aber auch das Speichern massiver Datensätze auf großen Servern an sich bringt ein gewisses Risiko mit sich. Italien ging sogar so weit, ChatGPT zwischenzeitlich mit der Begründung zu verbieten, dass für das Training des KI-Algorithmus unerlaubt persönliche Daten verwendet worden seien und das Tool die DSGVO nicht erfülle.[10]

Hinzu kommt, dass bestimmte Angriffsmethoden, bei denen durch Reverse-Engineering des Chat-Outputs sensible Nutzerdaten freigelegt werden, verheerende Folgen in Form massiver Datenlecks haben können.[11] Was Expertinnen und Experten zudem Sorgen bereitet, ist die Möglichkeit, den Output dieser Tools gezielt zu manipulieren und zur Verbreitung von Fehlinformationen sowie zur gesellschaftlichen Manipulation zu nutzen – ein Risiko, das insbesondere im Kontext der derzeitigen globalen Krisen höchst relevant ist.

Auch ist der mögliche Diebstahl geistigen Eigentums und Urheberrechtsverletzungen beim Output von ChatGPT nicht ganz unbedenklich. Laut Nutzungsbedingungen von OpenAI erhalten User das Eigentumsrecht an den ausgegebenen Inhalten, bei denen es sich um originale Texte handeln solle – diese Texte basieren jedoch auf Inhalten, für die möglicherweise Dritte das Urheberrecht halten.[12]

Wie können wir uns schützen?

Generative KI-Tools wie ChatGPT sind zwar noch eine recht neue technologische Entwicklung. Trotzdem arbeiten Institutionen wie die Europäische Union bereits an neuen Gesetzen, die die rechtlichen Aspekte solcher Tools klar definieren sollen. Um sich selbst zu schützen, sollten User zudem die folgenden Tipps befolgen:

- **Geben Sie keinesfalls sensible Daten (ob persönlich oder beruflich) ein.** Ihre Daten könnten für weiterführende Analysen und Optimierungen des Tools gesammelt oder im Falle eines Datenlecks veröffentlicht werden.
- **Überprüfen Sie stets die Richtigkeit der ausgegebenen Informationen.** KI-Tools sind nicht perfekt. Sie können falsche Annahmen anstellen oder sich Wissen von fehlerhaften Quellen angeeignet haben.
- **Sichern Sie sich rechtlich ab, bevor Sie Output für kommerzielle Zwecke nutzen.** Stellen Sie sicher, dass Sie gegen keine Gesetze oder geistigen Eigentumsrechte verstoßen.

Die „Dry-Powder-Hypothese“

Der technologische Fortschritt schreitet in schwindelerregendem Tempo voran – und genauso schnell eröffnen sich neue Anwendungsszenarien der künstlichen Intelligenz für Cyberangriffe. Auch wenn wir bereits einige ausgefeilte Angriffe beobachten mussten, **haben Cyberkriminelle das Potenzial dieser Tools bisher noch nicht voll ausgeschöpft**.

Solange konventionelle Taktiken, wie großangelegte Phishing- oder Spear-Phishing-Angriffe, weiterhin den menschlichen Faktor überlisten und Systeme effektiv infiltrieren, zahlt sich für Cyberkriminelle der zeitliche und finanzielle Aufwand großflächiger KI-basierter Angriffe nicht aus. Eines steht dennoch fest: Künstliche Intelligenz treibt die Innovation und Demokratisierung im Bereich Cybercrime an, während sie gleichzeitig die Reichweite und Erfolgsrate „traditioneller“ Angriffsmethoden steigert. Die Folge: Das Sicherheitsrisiko für Zivilpersonen wie auch Organisationen ist heute größer als je zuvor.

> Fortschrittliche Technologien wie Voice-Cloning stehen Cyberkriminellen bereits seit geraumer Zeit zur Verfügung. Trotzdem kam es bisher nicht zu breit angelegten Social-Engineering-Angriffen dieser Art. Eine Erklärung dafür: Simplere Methoden führen noch immer zum Erfolg. In Anbetracht der Datenlecks von Large Language Models und des rasanten Fortschritts im Bereich generativer KI wird sich das aber mit hoher Wahrscheinlichkeit bald ändern.

Dr. Niklas Hellemann
CEO SoSafe

Wie Menschen KI-basierte Cyberangriffe verhindern können

Künstliche Intelligenz wird bereits seit geraumer Zeit für verschiedenste Aufgaben, von der Threat Detection bis hin zur automatisierten Incident Response, genutzt. Nach den jüngsten KI-Entwicklungen haben sich nun jedoch auch für Angreifende neue Anwendungsmöglichkeiten eröffnet. Sie transformieren die Bedrohungslage und machen **Cyberkriminalität für die breite Masse zugänglich**. Deshalb setzen sich mittlerweile auch die Strafverfolgung, internationale Institutionen und KI-Tool-Anbieter verstärkt dafür ein, dem Missbrauch von KI als Angriffsvektor einen Riegel vorzuschieben. Cyberkriminelle finden aber trotz aller regulatorischen Bemühungen ständig neue Angriffswege. Um schwerwiegende Folgen zu vermeiden, ist es an den Sicherheitsteams, mit der ständig wechselnden Bedrohungslage Schritt zu halten. Da Bedrohungen durch technische Sicherheitsmaßnahmen immer schwerer zu erkennen sind, kommt es mehr denn je auf eine starke Sicherheitskultur, hohe Security Awareness und aufmerksame Mitarbeitende an.

> Die tägliche Arbeit bringt zwangsläufig Risiken mit sich. Irgendwann müssen wir diese E-Mail öffnen und dann auf den Anhang klicken. Während die Technologie immer weiter voranschreitet und hinsichtlich der Security bereits eine große Last von unseren Schultern nimmt, bleibt der menschliche Risikofaktor immer erhalten. Deshalb müssen wir unsere menschliche Firewall kontinuierlich stärken.

Stefanie Boem
Datenschutzbeauftragte Sport-Thieme

Eine neue Ära digitaler Risiken: Die Professionalisierung der Cyberkriminalität

Der Vormarsch generativer KI-Tools treibt nicht nur die Demokratisierung, sondern **auch die Professionalisierung der Cyberkriminalität** voran. Gleichzeitig werden Cybercrime-as-a-Service-Modelle (CaaS) als Geschäftsmodell immer beliebter unter Angreifenden. Das Zusammenspiel dieser Faktoren bildet den perfekten Nährboden für Cyberkriminelle, um gemeinsam Innovationen anzustoßen und gezielt Organisationen, die sicherheitstechnisch nicht gut genug aufgestelltsind, anzugreifen.

Insbesondere Erpressungssoftware ist zu einem festen Bestandteil der CaaS-Modelle geworden. Seit ihrer Anfänge Ende der 1980er-Jahre ist und bleibt **Ransomware eine der vorherrschenden Angriffstaktiken**, die Organisationen wie auch Privatpersonen beunruhigt.

> **Ransomware ist eine der wenigen Angriffsmethoden, bei denen das Opfer als Komplize agieren muss. Tappt man in die Falle von Erpressungssoftware, steht man vor komplizierten Entscheidungen mit psychologischem Faktor, wie: Zahle ich das Lösegeld oder melde ich den Angriff?**

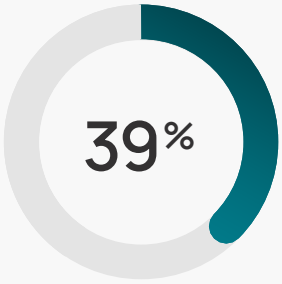
Stéphane Duguin
CEO CyberPeace Institute

Diese beunruhigende Tatsache wird durch unsere Studie bestätigt: Ransomware gehört immer noch zu den am häufigsten genutzten Cyber-Angriffstaktiken. Eine von drei Organisationen, die in den vergangenen drei Jahren Opfer eines Cyberangriffs geworden ist, wurde mit Erpressungssoftware angegriffen. Von den betroffenen Organisationen gaben außerdem 39 Prozent an, das verlangte Lösegeld gezahlt zu haben – bei kleineren Organisationen war sogar die Hälfte von ihnen gezwungen zu zahlen.

Seine größte Transformation erlebte die Ransomware-Methode jedoch in den letzten Jahren. Die Entstehung und stetige Weiterentwicklung von Ransomware-as-a-Service (RaaS) im letzten Jahrzehnt ist der beste Beweis, dass Cyberkriminelle ihre Geschäftsstrategien diversifizieren und ihre illegalen Methoden immer weiter optimieren.

31%

der Organisationen, die in den letzten drei Jahren Opfer eines Cyberangriffs wurden, hatten es mit Ransomware zu tun, und



gaben an, das Lösegeld gezahlt zu haben.

Ransomware-as-a-Service: Eine weltweite Pandemie

Um einen Ransomware-Angriff durchzuführen, brauchen Angreifende heutzutage **keine IT- oder Hacking-Kenntnisse** mehr. Eine kurze Suche im Darkweb und eine schnelle Kryptozahlung reichen aus, um Ransomware-as-a-Service-Plattformen zu nutzen – diese bieten Abonnementmodelle und oft sogar einen Kundendienst (wie die Conti-Leaks eindrucksvoll veranschaulichten).[1] Das zerstörerische Ausmaß für die Wirtschaft macht eine neue IBM-Studie deutlich, laut der ein erfolgreicher Ransomware-Angriff Unternehmen durchschnittlich 4,54 Millionen US-Dollar kostet – das Lösegeld selbst noch nicht einberechnet.[2] Und die Anzahl möglicher Cyberkrimineller steigt durch RaaS-Plattformen in exponentiellem Tempo an.

4,54 Mio. USD

kostet Unternehmen ein erfolgreicher Ransomware-Angriff durchschnittlich – das Lösegeld nicht einberechnet.

Quelle: IBM [2]

So erschütterte unter anderem die bekannte REvil-Gruppierung 2021 mit ihrem groß angelegten Supply-Chain-Angriff auf den Softwareanbieter Kaseya, von dem tausende von Unternehmen weltweit betroffen waren, die Geschäftswelt. Für Aufsehen sorgte auch die Forderung von 70 Millionen US-Dollar – eine Lösegeldforderung in bis dahin nie dagewesener Höhe.[3] Während Kaseya sich gegen die Zahlung entschied, gab es andere bekannte Unternehmen, wie den US-Versicherer CNA Financial und den brasilianischen Fleischproduzenten JBS, die mit 40 Millionen US-Dollar und 11 Millionen US-Dollar zwei der bislang höchsten bekannten Lösegeldsummen nach erfolgreichen Ransomware-Angriffen zahlten.[4]

1 **ZDNet (2022).** Conti-Ransomware zielt auf Europa.

2 **IBM (2022).** Kosten eines Datenschutzverstoßes 2022.

3 **PC-Welt (2021).** Kaseya: Erpresser fordern 70 Millionen Dollar Lösegeld.

4 **Heise (2021).** Cybercrime: US-Versicherung zahlte angeblich 40 Millionen als Lösegeld.

Die 10 höchsten Lösegeldzahlungen durch Unternehmen

Projekt	Gezahltes Lösegeld	Ransomware-Gruppe	Ursprung
CNA Financial	$40,000,000	Phoenix	Russland
JBS	$11,000,000	REvil/Sodinokibi	Russland
CWT	$4,500,000	Ragnar Locker	N/A
Brenntag	$4,400,000	Darkside	Osteuropa
Colonial Pipeline	$4,400,000	Darkside	Osteuropa
Travelex	$2,300,000	REvil/Sodinokibi	Russland
UCSF	$1,140,895	Netwalker Ransomware	N/A
BRB Bank	$957,245	LockBit	Osteuropa
Jackson County, Georgia	$400,000	Sam Sam	Iran
Universität Maastricht	$218,000	Ciop Ransomware	Russland

Quelle: Immunefi [5]

Auch die RaaS-Gruppierung HIVE sorgte letztes Jahr mit ihren groß angelegten Cyberangriffen für Schlagzeilen. HIVE nahm nicht nur große internationale IT- und Öl-Konzerne ins Visier, sondern drang zudem in Daten- und Computersysteme im Gesundheits- und öffentlichen Sektor ein. Seit Juni 2021 waren mehr als 1.500 Organisationen in 80 Ländern von durch HIVE durchgeführte Angriffe betroffen – mit einer gesamten Lösegeldsumme von nahezu 100 Millionen Euro.[6]

Als neuerer Akteur zielt Sugar Ransomware, die erstmalig im November 2021 vom Sicherheitsteam bei Walmart entdeckt wurde, anstatt auf große Unternehmensnetzwerke nun aktiv auch auf Geräte von Einzelpersonen ab.[7] Durch den Wechsel vom Whaling von Führungskräften hin zum Angriff von Zivilpersonen und Kleinunternehmen mit niedrigeren Lösegeldforderungen erweitern die Angreifenden die Anzahl potenzieller Opfer, während sie gleichzeitig das Risiko einer rechtlichen Nachverfolgung minimieren. Dies verdeutlicht, dass Cyberkriminelle sich verstärkt zusammenschließen und Ressourcen, aber auch Wissen, miteinander teilen – so schaffen sie die idealen Voraussetzungen für besser **koordinierte und effektivere Angriffe**.

Partnerschaften in einem komplexen globalen Netzwerk – ein Spießrutenlauf

Der Cyberangriff auf Kaseya führt uns nicht nur die gewaltige Reichweite von Ransomware-as-a-Service vor Augen. Er zeigt auch, dass sich **Umfang, Ausmaß und Komplexität von Supply-Chain-Attacken** durch die Professionalisierung der

5 **Immunefi (2023).** Top Crypto Ransomware Payments Report.

6 **Heise Online (2023).** Cybercrime: Polizei übernimmt IT-Infrastruktur der Ransomware-Gruppe „Hive".

7 **BleepingComputer (2022).** A look at the new Sugar ransomware demanding low ransoms.

Cyberkriminalität vervielfacht haben – zum Leid der Organisationen, die in der heutigen vernetzten Welt noch angreifbarer werden. Der Angriff auf Kaseya zielte auf die unternehmenseigene VSA-Software ab, ein Remote-Management-Tool zur Überwachung und Verwaltung der IT-Services von Kunden.[8] Indem sie in die Software eindrangen, gelangten die Angreifenden auf einen Schlag in die Systeme tausender Unternehmen, die die Dienste von Kaseya nutzten – eine erneute Warnung, dass **unsere eigene Sicherheit von der Sicherheit anderer abhängt**.

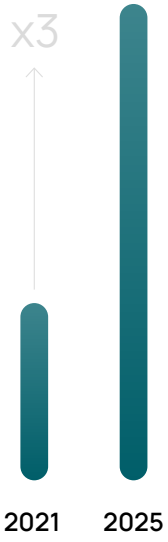
8 von 10

Sicherheitsverantwortlichen sagen, dass die Sicherheit ihrer Organisation **zunehmend von der Sicherheit ihrer Partner und Lieferanten abhängt**.

Bei Supply-Chain-Attacken nutzen Angreifende meist das schwächste Glied in der Lieferkette aus – oft kleinere Zulieferer oder Dienstleiter mit niedrigeren Sicherheitsstandards – um sich Zugang zu einer größeren Organisation zu verschaffen. Diese Vorgehensweise war auch Anfang dieses Jahres zu beobachten, als Nissan North America bekanntgab, dass es bei einem ihrer Softwareentwickler zu einer Datenschutzverletzung kam, bei der vollständige Namen und Geburtsdaten von tausenden Nissan-Kunden gestohlen wurden.[9]

Ein aktueller Cyberangriff auf den Desktop Client von 3CX demonstriert die Reichweite von Angriffen auf die digitale Lieferkette. 3CX ist der Entwickler eines softwarebasierten Telefonsystems, das von mehr als 600.000 Organisationen weltweit genutzt wird, darunter BMW und McDonald's.[10] Ähnlich wie bei SolarWinds wurde bei diesem Angriff das 3CX-Desktop-App-Installationsprogramm trojanisiert, um Infostealer-Malware in Unternehmensnetzwerke einzuschleusen, Systemdaten abzugreifen und Daten beliebter Webbrowser zu stehlen.

Es gibt keinerlei Anzeichen dafür, dass der Trend der Supply-Chain-Attacken in naher Zukunft nachlassen wird. Im Gegenteil: Laut Gartner werden bis 2025 45 Prozent aller Organisationen weltweit Angriffe auf ihre digitale Lieferkette erlitten haben – dreimal so viele Organisationen wie noch 2021.[11]



45%

aller Organisationen werden bis 2025 Angriffe auf ihre digitale Lieferkette erlitten haben.

Quelle: Gartner [11]

Organisationen sind heute verstärkt auf Dienste und Software Dritter angewiesen, um mit den Innovationen der digitalen Zeit Schritt zu halten. Umso wichtiger ist es, die eigene Sicherheitsstrategie zu optimieren und Lieferkettenrisiken zu reduzieren – für sich und für andere.

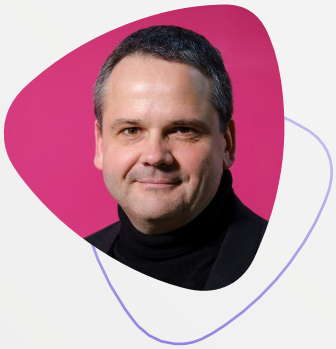
8 **Wirtschaftswoche (2021).** Hackerangriff REvil: Die perfide Strategie der Kaseya-Hacker.

9 **Cybernews (2023).** Nissan data breach exposed clients' full names and dates of birth.

10 **IT Daily (2023).** Telefonsystem 3CX weltweit für DLL-Sideloading-Angriff genutzt.

11 **Gartner (2022).** Gartner Identifies Top Security and Risk Management Trends for 2022.

Wenn wir in neue Technologiesphären reingehen, müssen wir die Risiken von Anfang an mitdenken. Sonst wird das in einer Katastrophe enden.



Thomas Tschersich
CSO Deutsche Telekom

Thomas Tschersich ist Chief Security Officer (CSO) der Deutschen Telekom AG und Chief Executive Officer der Telekom Security. In dieser Funktion verantwortet er neben der Cybersicherheit auch alle anderen operativen Sicherheitsthemen der Telekom. Der Diplom-Ingenieur der elektrischen Energietechnik ist Vorstandsvorsitzender der Initiative Deutschland sicher im Netz und weiterhin in zahlreichen beratenden Funktionen tätig, darunter als Mitglied im Cybersicherheitsrat und im UP Kritis Rat.

Gibt es Ihrer Meinung nach Probleme dabei, wie Unternehmen Security auslegen – und ihre Strategien gestalten?

Security hat viel mit Attitude, also der allgemeinen Einstellung zum Thema, zu tun. Es gibt noch viele Security-Einheiten, die bestimmte Dinge komplett verbieten oder unnötig verkomplizieren. Man muss aber meiner Meinung nach jeden Tag einen Kompromiss zwischen Sicherheit und Convenience, also einem gewissen Grad an Komfort eingehen. Warum? Wenn ich letzteres nicht berücksichtige, finden die User einen Weg um die Security-Maßnahme herum.

Haben Sie Beispiele dafür?

Das zeigt sich in verschiedensten Bereichen. Wenn man Personen dazu zwingt, ihr Passwort häufig zu wechseln, wird die Stärke des Passworts häufig mit jedem Wechsel schlechter. Auch wenn sie dazu gezwungen werden, sehr komplizierte Multi-Faktor-Authentifizierungs-Prozesse zu durchlaufen, ergeben sich schnell Probleme wie "MFA Fatigue": Cyberkriminelle fordern dabei vielfach die Authentifizierung an, bis die betroffene Person davon ermüdet ist und schließlich bestätigt. Und verbietest du USB-Sticks, senden die Leute sich sensible Dateien vielleicht an ihren privaten E-Mail-Account, um sie von da aus weiter zu kopieren. Da stellt sich letztlich die Frage: Was ist besser – die Datei auf einem geschützten und kontrollierbaren USB-Stick oder auf einem privaten Account?

Ich bin deshalb fest davon überzeugt, dass Sicherheitsmaßnahmen transparent und nachvollziehbar sein müssen. Wenn Menschen verstehen, warum bestimmte Maßnahmen und Prozesse eingeführt werden, ist die Motivation, sich daran zu halten, viel höher. Wenn sie es nicht verstehen, nehmen sie es eher als störend wahr und versuchen, einen Weg daran vorbei zu finden.

Viele Unternehmen haben lange auf das Abhaken von Security Policies gesetzt. Wie sehen Sie deren Rolle heute?

Als ich bei der Telekom angefangen habe, war ich auch für Policies zuständig. Heute sage ich scherzhaft: Ich habe damals Policies geschrieben – die 200.000 anderen Kolleginnen und Kollegen haben sie ignoriert. Natürlich muss ich bestimmte Dinge schon allein aus Compliance-Gründen aufschreiben, das ist auch gut so. Aber mit einer Policy allein habe ich noch nichts erreicht.

Ich habe auch noch nie einen Hacker gesehen, der sagt: Das Unternehmen hat eine Policy, da traue ich mich nicht ran.

Ich glaube, nur den rein formalen Weg zu gehen, ist einer der größten Fehler, den wir in puncto Sicherheit machen. Auch eine ISO-27001 Zertifizierung macht mich nicht sicher. Sie zeigt erst einmal nur, dass ich befähigt bin, Sicherheit zu leben. Wir dürfen uns hinter diesen Regularien und Zertifizierungen nicht verstecken.

Worauf setzen Sie stattdessen?

Mir sind die praktischen Dinge wichtiger, zum Beispiel ein konstantes Patch Management, mit dem ich Schwachstellen schnell flicken kann.

Wir halten unsere Policies mittlerweile minimal und beschreiben darin unser allgemeines Anforderungsniveau an die Sicherheit. So haben wir mehr Zeit, Maßnahmen tatsächlich zu implementieren.

In unserem Privacy- und Security-Assessment-Verfahren arbeiten wir Sicherheitsnotwendigkeiten heraus und können direkt entsprechende technische und organisatorische Maßnahmen ergreifen. Das ist aus meiner Sicht viel effektiver und greift da, wo Sicherheitsprobleme entstehen.

Was raten Sie anderen Unternehmen: Wie können Organisationen eine gute Sicherheitsstrategie aufbauen?

Viele Unternehmen haben keine Sicherheitsstrategie aus Angst vor zu großer Komplexität. Ich bin ein starker Verfechter davon, Dinge zunächst einfach zu lösen. Wir zeigen diesen Unternehmen, dass es viele einzelne Schritte auf dem Weg zu einer Sicherheitsstrategie gibt: Fangen wir mit Software-Updates an – schon damit hat man ein gutes Niveau. Dann können sie in technische Abwehrsysteme investieren, wie Virenschutz, Endpoint Detection Response – damit bekommen Unternehmen schon vieles abgeblockt. Und dann kommt das Thema Bewusstsein bei Mitarbeitenden – daran müssen Unternehmen aber dann konstant arbeiten.

Wie können Unternehmen das Bewusstsein ihrer Mitarbeitenden für Sicherheitsthemen verbessern?

Früher war Security Awareness gleichbedeutend mit webbasiertem Training. Für mich heißt das: Ich klicke mich schnell durch alles durch und beantworte ein paar Fragen. Damit habe ich dem Thema direkt einen negativen Stempel aufgedrückt. Die Mitarbeitenden nehmen es eher als Störung als eine Bereicherung wahr.

Wie kann man es besser machen?

Man sollte Security Awareness mit Spaß gestalten und den Mitarbeitenden auch den sekundären Nutzen vermitteln: Das Training hilft nämlich auch privat. Dann wird Security als Unterstützung wahrgenommen und die Menschen adaptieren ihr Verhalten entsprechend. Besonders wichtig ist auch das Feedback an Lernende: Wenn wir Phishing-Angriffe simulieren, nützt es nichts, wenn die User erst Wochen später erfahren, was passiert ist. Die Rückmeldung muss unmittelbar in der Situation kommen – denn dann sind Aufmerksamkeit und Lerneffekt am größten.

Das Gefährliche ist, dass die Angriffe extrem gut geworden sind.

Wir sehen gerade viele neue Angriffstaktiken und Trend-Themen, die Einfluss auf Security haben. Was sehen Sie da?

Mit dem Wort “Trend” bin ich immer vorsichtig. Zuletzt war das große Buzzword die Blockchain, davor die Cloud. Wir sollten nicht immer nur auf diesen Hypes unterwegs sein. Das größte Problem ist meiner Ansicht nach, dass wir die Basics nicht erledigen. Wir müssen erst einmal unsere Hausaufgaben machen.

Dann sehe ich aber verschiedene Themen, die einen Einfluss haben: Identitätsdiebstahl (über Phishing oder CEO-Fraud-Calls), DDoS-Angriffe und Ransomware. Das sind momentan die größten Vektoren, über die man reden muss.

Oft sind auch bei diesen Attacken fehlende Software-Updates eine Ursache. Dazu kommt noch das Thema Awareness: Man klickt aus Neugier oder Hilfsbereitschaft auf Dateien und das Übel nimmt seinen Lauf. Das Gefährliche ist, dass die Angriffe extrem gut geworden sind. Früher sprangen einem Rechtschreibfehler oder maschinell erstellte Texte ins Auge, wo man direkt wusste, dass das nicht sein kann. Heute sind wir längst davon weg, und Phishing-Mails sind nicht mehr auf den ersten Blick erkennbar.

Machine Learning wird in der Security ja schon lange für Verteidigungszwecke genutzt. Jetzt sehen wir generative KI, die beispielsweise neue Arten von Voice-Cloning-Angriffen vereinfacht. Sehen Sie solche Angriffe schon „in der freien Wildbahn”?

Voice-Adaptierung in CEO-Fraud-Calls haben wir tatsächlich schon gesehen, allerdings noch mit Artefakten. Die große Schwierigkeit ist: Wir sind alle gewohnt, in Videokonferenzen zu sein. Mit dieser neuen Technologie wird es einfach, gefakte Teilnehmer einzuschleusen. Grundsätzlich werden wir das Thema „digitale Identitäten“ in Zukunft deshalb anders betrachten müssen. Wir brauchen eine „identity of everything” - für Services, Maschinen, und so weiter.

Nehmen Sie in der Führungsetage eine veränderte Wahrnehmung für Security wahr?

Eine veränderte Wahrnehmung schon, aber nicht unbedingt ein verändertes Handeln. Es gibt keinen Kundentermin mehr, bei dem Security nicht in aller Munde ist. Oft höre ich trotzdem eher das Lebensmotto heraus: Es ist noch immer gut gegangen. Wenn es dann aber doch zu einem Angriff kommt, wird das mitunter sehr teuer.

Prävention ist letztlich immer die bessere Alternative. Ist das in einem Unternehmen, das schon einmal selbst betroffen war, denn präsenter?

Leider ist das meist nur ein sehr kurzfristiger Effekt. Oft planen und analysieren die Fachbereiche anschließend. Wenn sie dann mit einem Plan wiederkommen und die Kosten von ein paar Millionen Euro auf den Tisch legen, ist der Schmerz nicht mehr groß genug, damit das Geld auch wirklich in die Hand genommen wird. Das ist vor allem bei kleineren Unternehmen der Fall.

Bei Konzernen ist das Bewusstsein ein anderes, die haben aber auch komplette Teams dafür. Häufig wird Sicherheit weiterhin als indirekter Kostenblock gesehen, als nicht produktionsrelevant. Wenn Sicherheit nicht da ist, kann dadurch aber sehr schnell ein direkter Kostenblock entstehen. Der nachhaltige Schaden kann immens sein.

Welche Top-Technologien empfehlen Sie anderen CIOs/CISOs?

Die Cloud hat die Welt deutlich verändert. Früher wurde Security über die Netzwerksicherheit sichergestellt. Das geht heute nicht mehr – die Firewalls stehen mitunter bei Amazon und Microsoft. Deshalb muss ich mich auf die Applikationsebenen fokussieren. Da sehe ich zum einen Identitätsmanagement, Verschlüsselung und Rechtemanagement. Zum anderen wird durch den Trend zum Arbeiten von überall der Endpoint wichtiger. Ich muss zu jederzeit sicherstellen können, wie vertrauenswürdig ein Gerät gerade ist. Dafür braucht man eine Kombination aus EDR-Lösungen und Conditional Access. Und zu guter Letzt sollte man die Infrastruktur regelmäßig patchen und kontrollieren. Bei Awareness-Maßnahmen können sich Unternehmen nach Abhaken dieser technischen Maßnahmen dann auf ganz bestimmte Probleme fokussieren - und Mitarbeitende so viel dosierter und gezielter sensibilisieren.

> Oft höre ich das Lebensmotto heraus: Es ist noch immer gut gegangen. Wenn es dann aber doch zu einem Angriff kommt, wird das mitunter sehr teuer.

Thomas Tschersich
CSO Deutsche Telekom

Burnout und Fachkräftemangel:
Der Druck auf Sicherheitsteams steigt

Cyberkriminelle lassen uns keine Zeit durchzuatmen – unablässig professionalisieren sie ihr Geschäftsmodell und entwickeln neue, innovative Angriffstaktiken. Da ist es nicht verwunderlich, dass die übermäßige Arbeitsbelastung Sicherheitsbeauftragte bis ins Burnout oder zur Kündigung treibt.

Eine Studie der Information Systems Audit and Control Association (ISACA) ergab, dass 2022 **60 Prozent der Organisationen damit zu kämpfen hatten, qualifiziertes Cybersicherheitspersonal** in ihren Teams zu halten. Extremer Stress bei der Arbeit war einer der häufigsten Gründe für ihre Kündigungen.[1] Der Mangel an Arbeitskräften in der Security-Branche generell, der sich auf 3,5 Millionen Personen beläuft, macht die Lage nicht besser – ganz im Gegenteil.[2]

3,5 Millionen

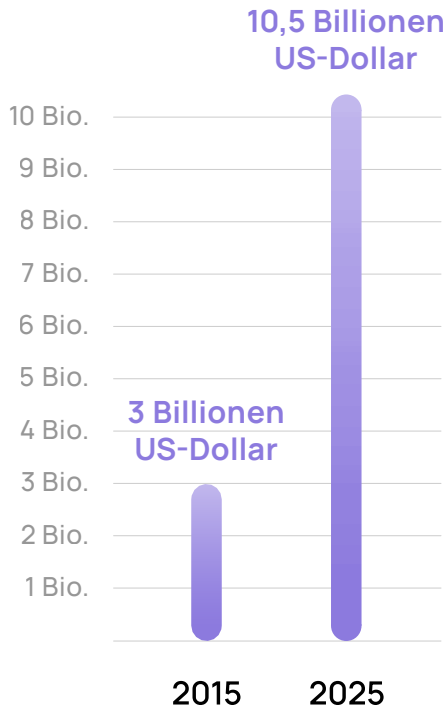
Fachkräfte fehlen in der Security-Branche.

Quelle: Chartered institute of information Security [2]

1 **ISACA (2022).** State of cybersecurity 2022: cyber workforce challenges.

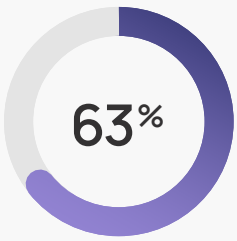
2 **Chartered Institute of Information Security (2022).** The security profession 2021/2022.

Das Ergebnis sind unterbesetzte Informationssicherheitsteams, die nur schwer mit der innovativen und rasant ansteigenden Cyberkriminalität mithalten können – einer weltweiten Branche, die Schätzungen zufolge bis 2025 jährlich finanzielle Schäden in Höhe von 10,5 Billionen US-Dollar verursachen soll. Im Vergleich dazu lagen die Kosten 2015 noch bei 3 Billionen US-Dollar.[3]



Quelle: Security Magazine[3]

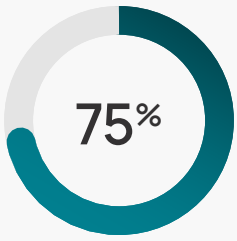
Wie in den vorherigen Kapiteln bereits deutlich wurde, entwickeln Cyberkriminelle unaufhörlich neue Strategien und nutzen technologische Innovationen zu ihrem Vorteil – was die eingeschränkten Mittel der ohnehin überforderten Security-Teams weiter unter Druck setzt. Daraus ergibt sich ein Teufelskreis: Der Mangel an Cybersicherheitspersonal befeuert Burnout in Sicherheitsteams, was es für Organisationen schwierig macht, mit der verschärften Bedrohungslage Schritt zu halten.



der Sicherheitsbeauftragten fühlen sich aufgrund der wachsenden Bedrohungslage gestresst.

Hybrides Arbeiten erhöht das Risiko von Cyberangriffen weiter

Während es manche Mitarbeitende nach zwei Jahren im Homeoffice zurück ins Büro zieht, ist hybrides Arbeiten dennoch stark im Kommen und immer mehr Organisationen entscheiden sich für dieses flexible Arbeitsmodell. Alle Vorteile dieses Modells haben jedoch auch ihren Preis: Die hybride Arbeitswelt öffnet neue Sicherheitslücken, die das Risiko von Cyberangriffen weiter ansteigen lassen.



der Sicherheitsbeauftragen bestätigen, dass Remote Work oder hybrides Arbeiten das Risiko für Cyberangriffe erhöht.

3 **Security Magazine (2023).** One of the biggest threats of a cybersecurity team? Employee burnout.

Dies sind einige der Faktoren, die zur Erhöhung des Risikos beitragen:

- **Schwachstellen im Heim-Netzwerk:**

  Heimische WLAN-Netze sind oft weniger gut gesichert als Firmennetzwerke. Dafür verantwortlich sind schwächere Verschlüsselungen, Standardeinstellungen und unzureichende Updates – alles Faktoren, die Cyberkriminellen den Zugriff auf sensible Daten erleichtern.

- **Nutzung ungesicherter Verbindungen:**

  Mitarbeitende, die remote arbeiten, haben eine höhere Tendenz, geschäftliche Anrufe auch von unterwegs anzunehmen. Auch die Nutzung öffentlicher Netzwerke erhöht das Cyberrisiko erheblich.

- **Kognitive Überlastung:**

  Die virtuelle Interaktion ermüdet unser Gehirn, unsere Konzentration leidet und die Erfolgschancen von Phishing-Mails steigen. Davon profitieren Cyberkriminelle, indem sie in unseren schwächsten Momenten zuschlagen – wie zum Beispiel kurz vor Feierabend.

- **Verstärkter Gebrauch von Kollaborationstools:**

  Remote Work bringt oft die vermehrte Nutzung von Tools wie Microsoft Teams mit sich – und damit neue Kanäle, die Cyberkriminelle für ihre Angriffe nutzen können.

- **Unzureichendes Security-Training:**

  Die schnelle Umstellung auf hybride Arbeitsmodelle hatte zur Folge, dass viele Mitarbeitende unzureichend zur Informationssicherheit geschult wurden.

> Im Homeoffice sind viele User weniger fokussiert – es ist eine lockerere Umgebung. Man mischt vielleicht private Aktivitäten zwischen den Arbeitsalltag. Das führt zu Unaufmerksamkeit.

Dr. Stefan Lüders
Computer Security Officer CERN

Das Ergebnis: Burnout als neuer Angriffsvektor

Stress, Unterbesetzung und eine durch neue Arbeitsmodelle vergrößerte Angriffsfläche bilden die optimalen Voraussetzungen für Cyberkriminelle. **Sie nutzen die Erschöpfung der Sicherheitsverantwortlichen zu ihrem Vorteil**. Denn in dieser Situation übersehen diese leichter kleine Details und können Probleme weniger effizient lösen.[4]

> Das führt uns zu dem zugrunde liegenden Problem, das wir derzeit in der Cyber-Security-Industrie überall beobachten können: Burnout. Wir haben zu viele Daten, zu viele Fälle, aber nicht genug Zeit.

Stéphane Duguin
CEO CyberPeace Institute

Hinzu kommt, dass Sicherheitsteams nicht nur den Schutz anderer Abteilungen innerhalb der Organisation gewährleisten und schnell auf Angriffe reagieren müssen. Laut unserer Studie gehören sie zudem selbst zu den Abteilungen mit dem höchsten Angriffsrisiko.

Die **Abteilungen** mit dem höchsten Risiko, Opfer eines Cyberangriffs zu werden

1. IT
2. Finance
3. Security

Auch Cyberkriminelle sind sich der Schwächen gestresster Sicherheitsteams bewusst und nutzen Burnout als neuen Angriffsvektor. **Sie greifen gezielt Organisationen an, deren Sicherheitsteams eher schwach aufgestellt sind**.

Dies unterstreicht, dass Unternehmen unbedingt Zeit und Ressourcen in die Bindung und stetige Weiterbildung ihrer Mitarbeitenden investieren sollten. Damit ermächtigen sie ihre Sicherheitsbeauftragten und fördern eine starke Sicherheitskultur, die ihnen hilft, mit der komplexen Cyber-Bedrohungslage Schritt zu halten.

4 **Security Magazine (2023).** One of the biggest threats of a cybersecurity team? Employee burnout.

Es ist wichtig, Cyber- und Informations-sicherheitsstrategien immer im Dreiklang zu betrachten: Mensch, Technik und Prozess.

Tobias Ludwichowski
CISO Signal Iduna

Tobias Ludwichowski ist studierter Wirtschaftsingenieur und seit 2015 in unterschiedlichen Funktionen für die SIGNAL IDUNA Gruppe tätig. Er hat unter anderem Führungsaufgaben im Risikomanagement und in der IT-Governance übernommen und leitet seit 2022 den Bereich Chief Information Security Office und ist als CISO für die deutschen Versicherungsgesellschaften der SIGNAL IDUNA Gruppe zuständig.

Wird Informationssicherheit heute anders wahrgenommen als noch vor einigen Jahren – insbesondere im Top-Management und Aufsichtsräten?

Das Aufsichtsrecht für Versicherungen im Bereich Informationssicherheit zieht extrem an – es entstehen immer mehr Gesetze und Regularien. Darüber hinaus prüft die BaFin das Thema seit ein paar Jahren sehr aktiv. Beides zusammen führt zu einem hohen Druck auf das Top-Management in Bezug auf dieses Thema.

Hinzu kommt eine komplexer werdende Bedrohungslage, mit der wir konfrontiert sind. Deshalb ist die Aufmerksamkeit für Cybersicherheit im Top-Management inzwischen sehr hoch – da das Bewusstsein in den letzten Jahren massiv gestiegen ist. Erfreulicherweise sind entsprechend auch die verfügbaren Ressourcen gewachsen, die investiert werden können.

Schauen wir uns das Versicherungswesen im Cyberbereich genauer an: Was sind Trends, die sie dort als Vertreter der Branche am Markt sehen können?

Wir sehen aktuell eine Tendenz, dass sich Cyberversicherungen auf wenige Anbieter zentralisieren, die bereit sind, Cyberrisiken im größeren Umfang zu versichern.

Das liegt an der Schwierigkeit, das Cyberrisiko in einem Unternehmen messbar und greifbar zu machen, während wir dem gegenüber eine hohe Dynamik am Bedrohungsmarkt haben. Es ist extrem schwierig objektiv zu bewerten, wie gut ein Unternehmen aktuell und in Zukunft tatsächlich gegen Cyberrisiken abgesichert ist.

Darüber hinaus muss die Versicherung auch immer noch attraktiv für den Kunden bleiben. Es bringt beispielsweise keinem größeren Mittelständler

etwas, wenn die Deckungssumme auf 200.000 Euro begrenzt ist. Darüber hinaus müssen wir es schaffen, dass Unternehmen auch trotz Cyberversicherung weiter aktiv gegen das Risiko vorgehen und sich kein Rücklehneffekt einstellt. Daher sind Cyberversicherungen aktuell ein herausforderndes Produkt.

Wie schafft man es, das Thema Informationssicherheit aus seinem Nischen-Dasein herauszuholen und es zu einem Gemeinschaftsprojekt zu machen, an dem – im besten Fall – jeder aktiv mitwirken möchte?

Hier muss man zwei Richtungen einschlagen: Der erste Punkt ist kontinuierliche Kommunikation und Schulung, um damit Transparenz darüber zu schaffen, welche Auswirkungen Sicherheitsvorfälle haben können. Es hilft beispielsweise schon, aktiv über die Bedrohungslage und bestimmte Verhaltensweisen zu informieren. Dabei können auch private Auswirkungen mit einfließen, um das Thema greifbarer zu machen – „schütze auch deine eigenen Kontodaten".

Der andere Punkt ist, dass wir die Themen so in Prozesse einbetten, dass den Mitarbeitenden gar nicht unbedingt bewusst ist, dass sie damit einen Sicherheitsmehrwert schaffen. Prozesse müssen so gestaltet werden, dass Mitarbeitende automatisch compliant sind. Das fühlt sich im Ergebnis dann weniger aufwändig für Mitarbeitende an.

Denn Richtlinien rauszuschicken und zu erwarten, dass diese gelesen, verstanden und in richtiges Verhalten umgesetzt werden, wird nicht funktionieren.

> Die besten Tools bringen nichts, wenn es keine passenden Prozesse dazu gibt und wenn Mitarbeitende nicht in der Lage sind, Gefahren zu erkennen.

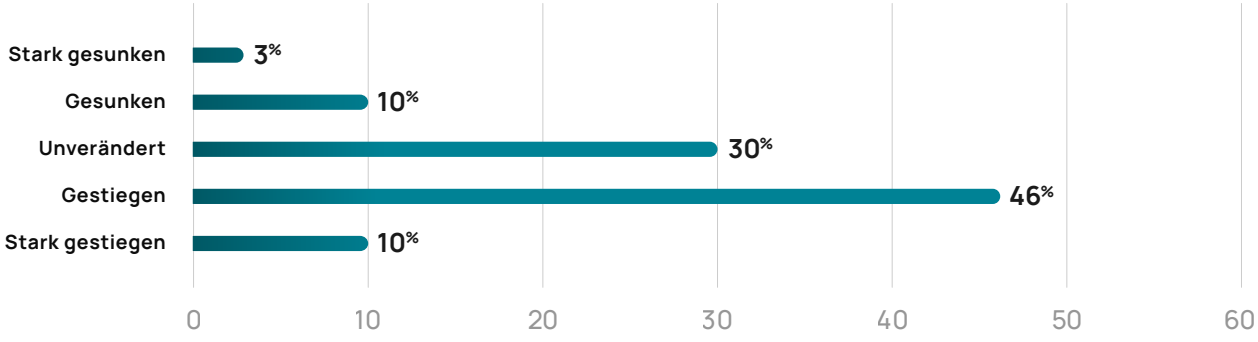
Tobias Ludwichowski
CISO Signal Iduna

Informationssicherheit auf Führungsebene: Warum sie für Führungskräfte an Relevanz gewinnt

Wir stehen im Bereich Informationssicherheit großen Herausforderungen gegenüber. Als logische Konsequenz positionieren Organisationen die Relevanz des Themas auch stärker in der Führungsebene. In unserer Umfrage gaben 56 Prozent der Security-Verantwortlichen an, dass die Awareness für Informationssicherheit auf oberster Führungsebene im Vergleich zu den Vorjahren gestiegen sei.

Informationssicherheit spielt heute eine zentralere Rolle in der Unternehmensstrategie, dem Risikomanagement und für den langfristigen Geschäftserfolg als noch vor wenigen Jahren. Dieser Bewusstseinswandel stößt zeitgleich weitreichende Veränderungen der Unternehmensstrukturen an. Die Cyber-Problematik in der Führungsetage zu platzieren, erleichtert in Organisationen nicht nur Prozesse, sondern auch die Planung: die Ausrichtung der Sicherheitsstrategie entlang der Geschäftsziele, die Budgetplanung, das Einleiten von Veränderungen und das Definieren klarer Verantwortungsbereiche. Die Vorteile spiegelten sich auch in den Ergebnissen unserer Umfrage wider:

Wie, falls überhaupt, hat sich die Aufmerksamkeit Ihres Top Managements für Security-Belange im vergangenen Jahr verändert?



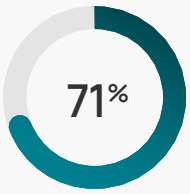
In Organisationen, deren Führungsebene für Cyberrisiken sensibilisiert ist, ist die Wahrscheinlichkeit

↗ 67 %

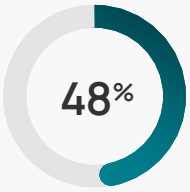
höher, dass ausreichende Ressourcen für Sicherheitsbelange zugewiesen werden, als in Organisationen, in denen die Awareness der Führungsebene niedrig ist.

Laut Gartner wird es bis 2026 für mindestens 50 Prozent der Führungskräfte vertraglich festgehaltene Performance-Anforderungen im Bereich Informationssicherheit geben.[1] Diese Entwicklung ebnet den Weg für schnellere und bessere Entscheidungen in der Informationssicherheit, die immer mehr von Entscheidungsträgern außerhalb der IT- oder Security-Teams getroffen werden. Zudem findet eine Verschiebung der formellen Verantwortlichkeit hin zu Führungskräften in anderen Geschäftsbereichen statt. In Anbetracht dieser Aussichten, werden in einigen Ländern wie den USA bereits neue Cyber-Sicherheitsrichtlinien für die Führungsebene eingeführt. Die SEC (Security and Exchange Commission) schlug im März 2022 eine Regelung vor, nach der Aktiengesellschaften öffentlich bekannt machen müssen, ob ihre Vorstandsmitglieder über Expertise im Bereich Informationssicherheit verfügen. Denn diese Information kann die Investitionsentscheidung von Aktionärinnen und Aktionären sowie deren Stimmenvergabe beeinflussen.[2]

Security-Awareness-Level einer Organisation abhängig von der Awareness der Führungsebene



der Security-Verantwortlichen bewerten die Awareness in der Organisation als hoch, wenn die oberste Führungsetage für Cyberrisiken sensibilisiert ist.



schätzen die Awareness als hoch ein, wenn die oberste Führungsetage nicht sensibilisiert ist.

Das Maß an Aufmerksamkeit, das der Informationssicherheit von der Führungsetage zukommt, hat also grundlegenden Einfluss auf die Cyberresilienz von Organisationen – auch auf menschlicher Ebene. Unsere Umfrage zeigte, dass das Security-Awareness-Level in Organisationen maßgeblich von der Awareness der Führungsebene bestimmt wird: 71 Prozent der Sicherheitsverantwortlichen, die überzeugt waren, dass Cyberrisiken für ihre oberste Führungsebene hohe Relevanz haben, bewerteten die unternehmensweite Security Awareness als hoch. Das Gleiche sagten nur 48 Prozent der Befragten, wenn sie die Awareness der Führungsetage als gering einschätzten.

1 **Gartner (2022).** Gartner Says the Cybersecurity Leader's Role Needs to Be Reframed.

2 **Harvard Business Review (2022).** Is Your Board Prepared for New Cybersecurity Regulations?

Flexibilität auf der Chefetage: Nur so können wir den Cyber-Wettlauf gewinnen

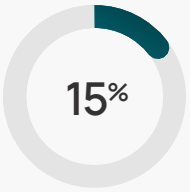
Hinzu kommt, dass Cyber ein Rat Race ist – Cyber dreht sich schnell, man muss ständig nachlernen. Umso wichtiger ist es, neue Modelle zu entwickeln, zum Beispiel jüngere Leute mit spezifischer Expertise in Aufsichtsräte berufen, auch wenn sie noch nicht Vorstand eines Unternehmens waren, oder verstärkt in Schulungen zu investieren.

Dr. Katrin Suder
Strategieexpertin
(digitale Technologien, Wirtschaft & Politik)

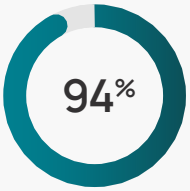
Kontinuierlich mit den neuen Entwicklungen der Cyber-Bedrohungslage Schritt zu halten, kann sich wie ein ständiger Wettlauf anfühlen. Auf oberster Führungsebene wird Informationssicherheit zwar verstärkt zur Priorität. Doch nicht alle Board-Mitglieder sind ausreichend mit Digitalisierung und Cyberrisiken vertraut. Deshalb sind kontinuierliches Lernen und Training auch für Führungskräfte unerlässlich. Dasselbe gilt für die Umstrukturierung der Führungsriege, indem Raum für neue spezialisierte Positionen geschaffen wird, selbst wenn diese weniger unternehmerische Fähigkeiten mitbringen. Als weitere Option kann das Sicherheitsteam regelmäßig bei Vorstandssitzungen involviert werden, um einen offenen und transparenten Austausch über die interne Sicherheitslage und das Sicherheitsrisiko in der Organisation zu fördern. Ein flexibles und kollaboratives Umfeld ermöglicht, Bereiche mit hohem Cyberrisiko zu identifizieren, Sicherheitsziele anzupassen und somit die Cyberresilienz der Organisation zu stärken.

Steigende Security-Budgets sind nicht genug

In den vergangenen Jahren investieren Organisationen zudem aktiver in ihre Cybersicherheit. Laut Gartner sollen die weltweiten Ausgaben für Security und Risikomanagement 2023 um mehr als 11 Prozent steigen und 188 Milliarden US-Dollar erreichen – verglichen mit 158 Milliarden US-Dollar von 2021.[3] Diese positive Entwicklung geht Hand in Hand damit, dass mehr Organisationen Cyber Security auch im Board thematisieren. Unsere Umfrage zeigte, dass es nur 15 Prozent der Organisationen mit unzureichenden Sicherheitsressourcen gelingt, ihre Sicherheitskultur zur Priorität zu machen. Unter den Organisationen mit genügend Ressourcen beläuft sich der Wert hingegen auf 94 Prozent.



Von den Organisationen mit **unzureichenden Sicherheitsbudgets** priorisieren nur 15 % ihre Sicherheitskultur.



94 % sind es bei **ausreichendem Budget.**

Zu einer effektiven Cyber-Security-Strategie gehören jedoch nicht nur Investitionen in neue Technologie und Tools. Entscheidend ist auch, Sicherheitsmaßnahmen mit den Geschäftszielen in Einklang zu bringen und Informationssicherheit fest in der Führungsetage zu verankern – das alles am besten in einem strategischen Rahmen.

Die Häufigkeit der Cyberangriffe steigt derzeit weit schneller als die Security-Budgets. Gleichzeitig haben Angreifende schon längst erkannt, wie wertvoll das menschliche Element für den Erfolg ihrer Angriffe ist – 82 Prozent der Datenschutzverletzungen sind auf den Faktor Mensch zurückzuführen.[4] Die Förderung sicherer Verhaltensweisen unter den Mitarbeitenden durch effektives Security Awareness Training kann und darf also nicht mehr aufgeschoben werden.

3 **Gartner (2022).** Gartner Identifies Three Factors Influencing Growth in Security Spending.

4 **Verizon (2022).** 2022 Data Breach Investigations Report.

> Wir reden zu oft darüber, dass die IT-Kosten zu hoch seien, aber eigentlich sind IT-Investitionen der Hebel, um über Automatisierung in den Fachbereichen Kosten zu sparen.

Jens Becker
CIO & CDO Zurich Gruppe Deutschland

Jens Becker ist seit Januar 2021 Chief Information Officer und Chief Digital Officer der Zurich Gruppe Deutschland und treibt in dieser Rolle die „Accelerated Evolution" der Zurich IT. Zuvor war Becker in der IT-Beratung bei KPMG und über 12 Jahre in verschieden IT-Führungsrollen bei der AXA tätig. Unter anderem verantwortete er dort mehrere Digitalisierungsprojekte, führte als Bereichsleiter für den IT-Betrieb DevOps ein und initiierte die Cloud-Migration der AXA.

Was muss Ihrer Meinung nach passieren, damit auch die Führungsebene mit an Bord kommt und beim Thema Awareness mitzieht?

Dass Security eine gewisse Priorität hat oder haben muss, haben die meisten intellektuell verstanden. Die Frage ist, ob es in der Aktion ankommt, zu nachhaltiger Security Awareness führt oder es im Zweifel doch bequemer ist, den Rechner nicht zu sperren oder die Daten nicht zu verschlüsseln. Ich glaube, wir müssen, neben der Unternehmensebene, an anderer Stelle anfangen, um die Awareness für das Thema, für die Bedrohungslage, für die Erfordernis der Cybervorsorge, den sensiblen Umgang mit Daten, etc. gesellschaftlich viel stärker zu verankern. Eigentlich ein Pflichtfach für alle – das sollte in der Schule anfangen. Schülerinnen und Schüler müssen verstehen, dass ihre Passwörter und Identitäten gestohlen werden können. Wir müssen sensibilisieren ohne Angst zu machen und einen kompetenten, verständnisvollen Umgang damit schaffen.

Auf Unternehmens- bzw. Konzernebene ist die Erwartungshaltung natürlich noch einmal höher. Auch – und gerade – da müssen die Kollegen sensibel mit unseren Kundendaten umgehen und sich ihrer Verantwortung bewusst sein. Dazu sprechen wir auch im Vorstand, dass es in der Verantwortung der Fachbereiche liegt, Themen wie Berechtigungskonzepte, Business Continuity Management oder individuelle Datenverarbeitung ernst zu nehmen.

Sie haben kürzlich bei einem Event davon gesprochen, dass Unternehmen mit IT Geld sparen sollten und nicht an IT. Können Sie das noch ein wenig erläutern?

Sehr gerne: Wir reden ganz oft darüber, dass IT-Kosten zu hoch sind, aber IT-Investitionen sind der Hebel, um über Automatisierung Business-Wachstum zu ermöglichen, Servicequalität zu verbessern oder Kosten in den Fachbereichen zu sparen.

Wiederkehrende einfache Tätigkeiten sollten wir automatisieren, damit unser Kundenservice sich auf wertvollere Aufgaben fokussieren kann. Chatbots können Anrufannahme, Kundenidentifikation und Anliegenerkennung kostengünstig übernehmen, damit der Sachbearbeiter sich anschließend auf das eigentliche Anliegen konzentrieren kann. Auch hilft die Automatisierung dabei, Reaktionszeiten an die Kundenerwartung anzupassen. Auf eine Antwort auf meinen Brief habe ich noch verständnisvoll zwei Wochen gewartet, auf meine E-Mail erwarte ich die Antwort innerhalb von zwei Tagen. Schnelle Verarbeitung, "first time right" steigert die Kundenzufriedenheit und reduziert Prozesskosten.

Wo wir gerade über Digitalisierung sprechen, ist die Digitalisierung des Outputs, zum Beispiel der physischen Post, noch ein Bereich, in dem wir als Branche noch viel zu tun haben und Investitionen mit Porto-, Papier- und CO2-Reduktion belohnt werden.

Also sollte man lieber heute investieren, um Risiken zu minimieren?

Definitiv. Lieber heute eine Firewall einbauen als morgen den übergesprungenen Brand zu löschen und die Reparaturkosten zu tragen. Die Frage nach der „richtigen" Balance bleibt aber. Es gibt Guidance, die sagt, du musst sieben Prozent deines IT-Budgets in Security investieren. Aber du kannst letztlich auch dein ganzes Budget in Security investieren und bist trotzdem nicht sicher.

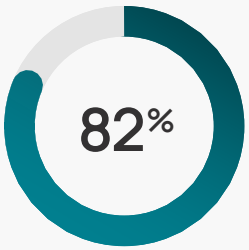
Deshalb braucht man einen risikoadjustierten Approach, bei dem man auf die Top-Risiken schaut. Orientierung geben Standards wie NIST oder ISO. Diese können auch in der Zusammenarbeit mit Partnern eine Signalwirkung haben, wenn man nachweisen kann: Ich habe ein gewisses Sicherheitslevel erreicht. Wichtig ist, dass man weiter kontinuierlich investiert und sich niemals auf einem Status-quo ausruht.

Wird denn grundsätzlich genügend investiert? Oder wird Security noch immer als Projekt gesehen, dass irgendwann vermeintlich abgeschlossen ist?

Jein und nein. Zur ersten Frage: Ich glaube, es wird eine Menge investiert, aber es ist nie genug. Daher verfolgen wir bei Zurich einen sogenannten Forced-Ranking-Ansatz, also eine Risiko-Matrix, in der wir unsere Security-Risiken eintragen und entsprechend dieser Risiko-Matrix sukzessive abarbeiten. Zur zweiten Frage: Das machen wir jetzt seit mehreren Jahren und damit werden wir auch in Zukunft nicht aufhören.

Ausblick: Warum Cyber Security stärker in unseren Alltag gehört

Die vorherigen Kapitel sollten eines deutlich gezeigt haben: Cybercrime ist längst eine höchst professionelle, weltweit aktive Branche. Im Sekundentakt spüren Angreifende Schwachstellen auf und wenden neue, ausgeklügelte Strategien an. Diese Schnelllebigkeit stellt Unternehmen, Regierungen und Einzelpersonen vor ungeheure Herausforderungen beim Schutz ihrer Daten und Ressourcen in einer immer stärker vernetzten Welt. Am beunruhigendsten ist, dass für die absehbare Zukunft keine Besserung in Sicht ist – im Gegenteil: Laut unserer Studie gehen 8 von 10 Sicherheitsverantwortlichen davon aus, dass sich die Cyber-Bedrohungslage in den kommenden zwölf Monaten nicht entspannen wird.



der Security-Verantwortlichen erwarten in den nächsten zwölf Monaten keine Entspannung der Bedrohungslage.

Ein genauerer Blick auf die Daten zeigt, dass insbesondere Social Engineering weiterhin eine zentrale Rolle im Repertoire der Cyberkriminellen spielen wird. E-Mail ist und bleibt dabei ein beliebter Angriffskanal und auch weitere Kanäle, wie die sozialen Medien und Kollaborationstools, werden dahingehend zunehmend ausgenutzt. Immer mehr Organisationen erkennen deshalb den Wert einer starken Sicherheitskultur und einer Strategie, die den Faktor Mensch in den Mittelpunkt rückt.

Unsere Mitarbeitenden erhalten Tag für Tag unzählige Spam-Mails. Viel bedenklicher ist aber die Menge an gefährlichen Phishing-Nachrichten, die trotz mehrerer Sicherheitschecks die E-Mail-Postfächer erreichen. Die Mitarbeitenden müssen wissen, wie sie die damit verbundenen Risiken meiden können. Deshalb ist Awareness-Training so wichtig für uns.

Frank Heymann
Senior IT-Team Manager Buhlmann

Effektives Security Awareness Training wird in diesem Zusammenhang unumgänglich für Organisationen, denn es befähigt die Mitarbeitenden, proaktiv zur Informationssicherheit beizutragen. So können Organisationen mit der angespannten Bedrohungslage Schritt halten und Sicherheitsrisiken ganzheitlich reduzieren.

> Die letzten 10 Jahre haben Unternehmen eher in Technik investiert als in Menschen. Inzwischen haben sie verstanden, dass Technik nicht alles ist, und dass Social Engineering – und insbesondere Phishing – ein echtes Problem ist.

Dr. Katrin Suder
Strategieexpertin
(digitale Technologien, Wirtschaft & Politik)

Security Awareness Training als bester Schutz vor Angriffen

> Menschliches Verhalten wird immer noch am besten von einem Menschen erkannt. Wenn man sich zu 100 % auf die Technik verlässt und annimmt, dass die Technik alles abfangen wird, dann macht man einen grundsätzlichen Fehler.

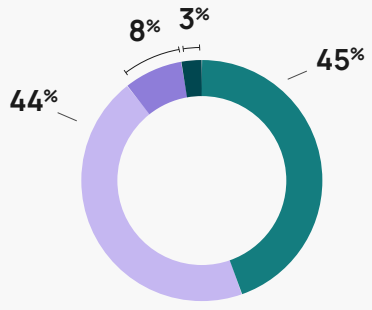
Tobias Ludwichowski
CISO Signal Iduna

Glücklicherweise sind sich bereits viele IT- und Sicherheitsteams der Bedeutung des menschlichen Faktors bewusst. Unsere Umfrage zeigte, dass die Steigerung der Security Awareness der Mitarbeitenden für Sicherheitsverantwortliche heute an oberster Stelle steht – gefolgt von Identity und Access Management sowie der Sicherung hybrider Arbeitsmodelle und bestehender Prozesse. Zudem bestätigten 9 von 10 Sicherheitsbeauftragten, dass sie in ihrer Organisation den Umfang der Security-Awareness-Maßnahmen beibehalten oder diese sogar ausweiten werden.

Die Top-Prioritäten von IT- und Sicherheitsteams

1. Die Security Awareness der Mitarbeitenden erhöhen
2. Identity und Access Management verbessern
3. Hybride Arbeitsmodelle besser absichern
4. Sicherheit bestehender Prozesse steigern

Welche Pläne haben Sie für den Ausbau oder die Reduzierung Ihrer Security-Awareness-Maßnahmen für 2023?



Voraussetzung ist die Unterstützung der Führungsetage

Die Involvierung der Führungsetage spielt für Sicherheitsbelange allerdings eine zentrale Rolle – eine Tatsache, die auch unsere Umfrage eindeutig belegt: Es ist ein direkter Zusammenhang erkennbar zwischen dem Bewusstsein für Cyberrisiken auf Führungsebene und der Bereitschaft, in Security-Awareness-Maßnahmen zu investieren.

Hohe Awareness im Top Management vs. Niedrige Awareness im Top Management

Außerdem zeigte die Studie, dass für **94 Prozent der Organisationen, die Cybersicherheit ein angemessenes Budget zuweisen, der Aufbau einer starken Sicherheitskultur hohe Priorität** hat. Im Gegensatz dazu spielt die Stärkung der Sicherheitskultur für nur 15 Prozent der Organisationen mit unzureichenden Sicherheitsressourcen eine zentrale Rolle. Diese Diskrepanz veranschaulicht eines ganz deutlich: Dass sich die verfügbaren Ressourcen und die Involvierung der Führungsebene direkt darauf auswirken, welchen Stellenwert Informationssicherheit in der Organisation hat.

Aus diesem Grund ist es unerlässlich, dass IT- und Security-Teams im stetigen Dialog mit der Führungsebene stehen und ihre Anliegen durch Erfolgsmetriken und aussagekräftige KPIs stützen. Um Cybersicherheit langfristig zur Priorität zu machen, sollte der Fokus bei der Kommunikation mit dem Top Management nicht nur auf Performance-Metriken wie der Klickrate liegen. Sicherheitsverantwortliche sollten stattdessen vor allem auch kommunizieren, wie sich das Verhalten der Mitarbeitenden auf lange Sicht ändern lässt und wie sich diese Verhaltensänderung positiv auf die Sicherheit insgesamt auswirkt (zum Beispiel, dass ein Phishing-Meldebutton die Meldequote langfristig erhöht).

Verhaltenswissenschaft als Grundpfeiler für Erfolg im Security Training

Zwar ist für viele Organisationen verschiedener Größen und Branchen der Begriff „Security Awareness“ längst kein Fremdwort mehr. Derzeit wandelt sich der Awareness-Ansatz aber grundlegend, damit wir die aktuellen Herausforderungen im Bereich Informationssicherheit effektiv angehen können. **Traditionelle Schulungsmodelle**, die in erster Linie auf die Erfüllung von Regularien abzielen, **reichen nicht mehr aus**, um die Motivation und das Engagement der Mitarbeitenden zu wecken – und sich der aktuellen Cyber-Bedrohungslage proaktiv entgegenzustellen. Dies wurde auch in unserer Umfrage deutlich:

Die Top 3 Gründe, die User am Security Awareness Training kritisieren

1. **Training ist zeitaufwändig**
2. **Informationen sind zu allgemein**
3. **Training ist zu eintönig**

Der Aufbau einer starken Sicherheitskultur beinhaltet also weit mehr als das Erfüllen von Compliance-Vorgaben. Stattdessen müssen Organisationen bei ihren Mitarbeitenden aktiv sichere Gewohnheiten

fördern und die Maßnahmen auf deren Arbeitsmodelle und -alltag abstimmen. Das heißt, **Security-Awareness-Programme sollten den Menschen in den Mittelpunkt stellen** und idealerweise **verhaltenspsychologische Methoden**, wie Micro-Learning, Gamification und Nudging, integrieren. Solche Ansätze helfen Mitarbeitenden dabei, sichere Verhaltensweisen im Arbeitsalltag, aber auch in ihrem Privatleben zu verinnerlichen.

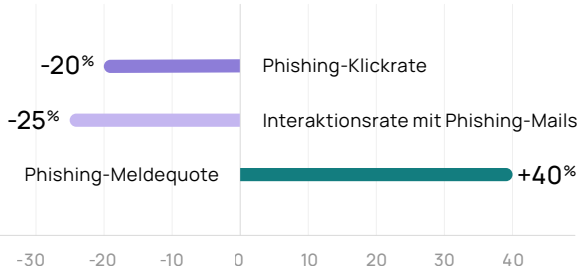
Außerdem wichtig: Mitarbeitende dort abholen, wo sie in ihrem Arbeitsalltag ohnehin aktiv sind, sodass das Training nahtlos in ihren Arbeitsalltag einfließt. So kann Informationssicherheit sich in bestehende Geschäftsprozesse einbetten. Nur durch eine solche proaktive Herangehensweise können wir heute der milliardenschweren Cybercrime-Industrie die Stirn bieten. Wenn wir nicht von ihr überrollt werden wollen, müssen wir es den Cyberkriminellen gleichtun und dürfen – genau wie sie – nie stillstehen.

Nachhaltige Verhaltensänderungen anstoßen

Verschiedene psychologisch fundierte Ansätze und Methoden ermöglichen Organisationen, den Erfolg ihrer Awareness-Maßnahmen zu maximieren und ihre Mitarbeitenden in ihrem individuellen Kontext abzuholen. Beim **Spaced Learning** wird Wissen kontinuierlich über verschiedene Kanäle vermittelt, sodass die User das Erlernte mehrmals wiederholen – in einem Tempo, das nachhaltige Lernerfolge fördert. Ein ähnlicher Ansatz ist das sogenannte **Nudging**. Dabei findet beispielsweise mittels regelmäßiger, automatisierter System-Mails eine stetige Interaktion mit den Usern statt, die dafür sorgt, dass die Thematik in ihren Köpfen präsent bleibt. **Micro-Learning** ist eine weitere effektive Methode zur langfristigen Verankerung von Wissen und zur Steigerung des Lernerfolgs. Die SoSafe Awareness-Plattform vereint alle Ansätze in leicht verdaulichen Lernmodulen und immersiven Handlungssträngen, die zum Weiterlernen anregen.

Diese Lernmethoden führen im Bereich Security Awareness zu höheren Abschlussquoten und infolgedessen auch zu einer Senkung der Klick- und Interaktionsraten mit Phishing-Mails sowie einer Steigerung der Meldequote. Auf diese Weise kommen Organisationen dem Schutz ihrer Daten und Systeme und der proaktiven Abwehr von Angriffen einen großen Schritt näher.

Produktnutzung
Ergebnisse von Nutzenden mit einer hohen Abschlussquote der Lernmodule



Phishing-Simulationen und die Bedeutung kontextbasierter Funktionen

Der Erfolg von Awareness Training wird von einem weiteren Faktor beeinflusst: von der Kontextualität der Inhalte. Ein Paradebeispiel für kontextbezogene Awareness-Maßnahmen sind **Phishing-Simulationen**, die das zuvor in Micro-Modulen oder anderen Lerninhalten angeeignete Wissen auf die Probe stellen. So festigen sich sichere Gewohnheiten bei den Lernenden. Expertinnen und Experten sind sich einig: Simulationen und andere kontextbasierte Lernerfahrungen tragen dazu bei, Sicherheitsrisiken effektiv zu reduzieren:

> Besonders wichtig ist auch das Feedback an Lernende: Wenn wir Phishing-Angriffe simulieren, muss die Rückmeldung unmittelbar in der Situation kommen – denn dann sind Aufmerksamkeit und Lerneffekt am größten.

Thomas Tschersich
CSO Deutsche Telekom

> In einer Welt, in der jeder mit Informationen überschüttet wird und keine Zeit zum Lernen hat, ist es wichtig, dass die Lerninhalte in kleinen Einheiten aufgeteilt und am Punkt des „Scheiterns“ präsentiert werden, da dann die Motivation zu lernen am höchsten ist. Eine effektive Methode ist zum Beispiel, eine Lernseite direkt nach dem Klick auf eine Phishing-Simulationsmail bereitzustellen. Eine kurze Fünf-Minuten-Einheit lässt sich auch in einem arbeitsreichen Tag gut unterbringen.

Martin Schmidt
Global Director of Digital Advisory
Freudenberg Home and Cleaning Solutions

> Nach einem Klick auf eine Phishing-Simulation und dem damit verbundenen Aha-Moment haben die meisten ein besseres Verständnis für digitale Gefahren und wie man mit ihnen umgeht.

Dr. Stefan Lüders
Computer Security Officer CERN

Die Integration **kontextbezogener Elemente und Tools** in die bestehende Lernumgebung festigt sichere Gewohnheiten von Mitarbeitenden langfristig. So ist die Interaktionsrate mit Phishing-Mails bei Mitarbeitenden, denen der SoSafe **Phishing-Meldebutton** zur Verfügung steht, um 30 Prozent niedriger als bei anderen, die keinen Zugriff auf die Funktion haben. Die Erfolgschancen von Phishing-Angriffen werden durch dieses Feature somit effektiv reduziert, das darüber hinaus weitere messbare Vorteile bietet:

Die Wirkung des Phishing-Meldebuttons

↗ 38 %
E-Learning-Akzeptanzrate

↗ 25 %
Modul-Abschlussquote

Innovation voraus: Diese verhaltensbasierten Features wünschen sich Organisationen

In unserer Umfrage wollten wir von Security-Verantwortlichen im europäischen Raum wissen, welches Feature ihrer Meinung nach den Erfolg ihres Awareness-Trainings weiter steigern könnte. Das waren ihre Antworten:

Diese Antworten zeigen eines ganz deutlich: Sicherheitsverantwortliche sind sich bewusst, dass der Mensch beim Thema Informationssicherheit im Fokus stehen muss. Beim Ansatz der **„Multichannel-Awareness“** werden Mitarbeitende beispielsweise über eine eher konversationsbasierte Methode trainiert. Indem sie über verschiedene Kommunikationstools wie Microsoft Teams in Echtzeit über neue Angriffstaktiken informiert werden, bleibt die Sicherheitsthematik im Arbeitsalltag stets präsent. Auch **personalisierte Lerninhalte**, die auf die Position und Aufgaben der einzelnen Mitarbeitenden abgestimmt sind, werden als eines der wirkungsvollsten Features von Awareness-Programmen angesehen – eine weitere Bestätigung dafür, dass die Cyber-Thematik den Menschen in ihrem individuellen Kontext begegnen muss.

Zuletzt gilt auch die **Customization des Lernprogramms** als effektiver Hebel zur Steigerung des Lernerfolgs. Dazu gehören etwa Features, die die visuelle Anpassung der E-Learning-Plattform an die Corporate Identity des Unternehmens ermöglichen, aber auch das Einbinden unternehmenseigener Security-Inhalte und Richtlinien. Die tiefere Botschaft: Security Awareness kennt keine allgemeingültige Lösung. Um erfolgreich zu sein, muss sie auf den jeweiligen geschäftlichen und menschlichen Kontext abgestimmt sein.

Die effektivsten Hebel zur Steigerung der Security Awareness

1. Awareness-Maßnahmen via Kommunikationstools
2. Personalisierte Lernmöglichkeiten
3. Customization des Awareness-Programms

Handlungsempfehlungen

Keine einfache Aufgabe: Sicherheitsmaßnahmen auf das wechselnde menschliche Verhalten abstimmen

1 Informationssicherheit sollte oberste Priorität haben

Wenn die Cyber-Bedrohungslage uns eines gelehrt hat, dann dass Informationssicherheit uns alle betrifft. Weder Einzelpersonen noch Organisationen können noch abstreiten, dass uns die Digitalisierung und technologischen Fortschritte für alle Arten von Online-Bedrohungen angreifbar gemacht haben. Um uns effektiv vor immer fortschrittlicheren Angriffstaktiken schützen zu können, müssen wir sichere Verhaltensweisen im Alltag verinnerlichen. Gleichermaßen sollten Organisationen Informationssicherheit auch stärker in der Führungsetage platzieren, denn letztendlich können Sicherheitsmaßnahmen nur wirklich wirksam sein, wenn ihnen im gesamten geschäftlichen Kontext Priorität eingeräumt wird. Der Mangel an Ressourcen für Security-Belange könnte schon bald der Vergangenheit angehören, wenn Organisationen ein Bewusstsein dafür schaffen, dass Cybercrime nicht nur Einzelpersonen betrifft, sondern maßgeblich auch den Geschäftserfolg.

2 Verhaltensänderung als Schlüssel zu nachhaltigem Erfolg

Verhaltensbasierte Kennzahlen sind der beste Weg, um den Erfolg von Awareness-Maßnahmen für verschiedenste Stakeholder innerhalb der Organisation greifbar zu machen. In der Vergangenheit wurden allerdings oft ausschließlich leistungsbasierte KPIs wie Phishing-Klickraten oder E-Learning-Abschlussquoten herangezogen. Diese sind zwar ein erster Schritt, um die Awareness der Mitarbeitenden einzuschätzen. Viel aussagekräftiger und überzeugender sind für Entscheidungsträger, die von der Notwendigkeit des Awareness-Trainings überzeugt werden sollen, jedoch Einblicke dazu, wie erfolgreich die Maßnahmen den aktuellen Zustand ändern. Das gelingt am besten mit verhaltensbasierten Kennzahlen, wie der Phishing-Meldequote, und über die Einführung von Human Risk Scores. Die Daten aus unserer Umfrage belegen: Jede zweite Organisation verlässt sich noch auf traditionelle Metriken. Verhaltensbasierte Kennzahlen werden jedoch schon von einem Drittel der Organisationen genutzt, Tendenz steigend. Vor dem Hintergrund, dass Cyberkriminelle verstärkt auf Social-Engineering-Taktiken setzen, kann anhand von verhaltensbasierten Daten und Human Risk Scores zuverlässig festgemacht werden, wie gut Organisationen vor ausgefeilten Angriffen geschützt sind.

3 Anpassen, anpassen und noch mal anpassen

Es gibt kaum eine andere Branche, die in den vergangenen Jahren und Jahrzehnten eine solch rasante Entwicklung erlebt hat wie die Cybersicherheit. Der Grund ist mehr als deutlich: Technologische Innovationen machen einen Stillstand unmöglich. Und täglich schreiten sie weiter voran. Als Konsequenz sind Organisationen gezwungen, ihre Sicherheitsstrategie noch schneller an neue Bedingungen anzupassen: an die professionellen Geschäftsmodelle der Cyberkriminellen und die wachsende Komplexität der Bedrohungslage. Das reine Abhaken von Compliance-Anforderungen reicht längst nicht mehr aus. Informationssicherheit muss zum festen Bestandteil der Geschäftsstrategie werden. Gleichzeitig sollte sichergestellt werden, dass die Maßnahmen mit den Erfahrungen und dem individuellen Risikokontext der Mitarbeitenden harmonieren. Die kontinuierliche Anpassung der Maßnahmen ist insbesondere in einer durch mangelnde Sicherheitsressourcen und Burnout geprägten Situation kein einfaches Unterfangen. Doch mit den richtigen Partnern an der Seite ist sie zu bewältigen.

4 Der Mensch als Dreh- und Angelpunkt

In der angespannten Bedrohungslage von heute muss der Faktor Mensch in der Informationssicherheit im Vordergrund stehen. Menschen sind Opfer und Leidtragende von Cyberangriffen – aber gleichzeitig können Menschen Angriffe auch effektiv abwehren. Eine starke Sicherheitskultur in Organisationen – und ein starkes Sicherheitsbewusstsein im Alltag – kann maßgeblich dazu beitragen, uns künftig vor der Professionalisierung der Cyberkriminalität und ihren Auswirkungen zu schützen. Dazu sollten wir Sicherheitsstrategien auf die Bedürfnisse der Mitarbeitenden abstimmen und die Prinzipien der Verhaltenspsychologie nutzen. Denn einer Sache können wir uns sicher sein: Cyberkriminelle hören nie auf, sich neue Betrugsmaschen auszudenken. Es liegt an uns, wachsam zu bleiben, uns ständig an die aktuellen Trends anzupassen und uns proaktiv für bevorstehende Herausforderungen zu rüsten.

Stärken Sie Ihre Sicherheitskultur – einfach und effektiv

Mit seiner Awareness-Plattform hilft SoSafe Organisationen, ihre Sicherheitskultur zu stärken und menschliche Risikofaktoren zu minimieren. Die Plattform bietet motivierende Lernerfahrungen und smarte Angriffssimulationen, die Mitarbeitende dazu befähigen, Cyberbedrohungen zu erkennen und aktiv abzuwehren – alles basierend auf verhaltenspsychologischen Erkenntnissen, die das Lernen spannender und effektiver gestalten. Anhand umfassender Analytics werden Verhaltensänderungen gemessen und Schwachstellen aufgedeckt, sodass Cyberbedrohungen proaktiv vorgebeugt werden kann. Die SoSafe Plattform ist im Handumdrehen eingerichtet und wächst mit Ihrem Unternehmen, um so sicheres Verhalten bei den Mitarbeitenden nachhaltig zu festigen.

TEACH

Motivierendes Micro-Learning

Eine verhaltenspsychologisch fundierte E-Learning-Plattform, mit der Lernen Spaß macht. Dynamische und wirkungsvolle Lernerfahrungen auf verschiedenen Kanälen helfen Ihnen, Ihre Abwehr gegen Cyberbedrohungen zu stärken, volle Compliance zu erzielen und mühelos sichere Verhaltensweisen aufzubauen.

- Storybasierte Micro-Lerninhalte mit Gamification-Elementen motivieren und fördern nachhaltig sichere Verhaltensweisen
- Ausgewählte, strukturierte Inhalte, die sich einfach skalieren lassen
- Benutzerfreundliche Customization- und Content-Management-Optionen, auf Ihr Unternehmen abgestimmt

TRANSFER

Smarte Angriffssimulationen

Zielgerichtete Phishing-Simulationen, um sichere Verhaltensweisen bei Ihren Mitarbeitenden zu fördern. Mit regelmäßigen, automatisierten Spear-Phishing-Simulationen befähigen Sie Ihre Mitarbeitenden, Cyberattacken zu erkennen und Security Awareness zu einem festen Bestandteil ihres Arbeitsalltags zu machen. Reduzieren Sie Ihr Cyberrisiko und Ihre Reaktionszeit im Falle eines Angriffs.

- Personalisierbare, realistische Simulationen von Cyberangriffen
- Kontextbasierte Lernseiten, die sichere Verhaltensweisen des Teams festigen
- Unmittelbares Reporting mit nur einem Klick dank Phishing-Meldebutton

ACT

Strategisches Risk Monitoring

Behalten Sie menschliche Risikofaktoren mit unserer Lösung immer im Blick und schützen Sie Ihre Organisation vor kostspieligen Sicherheitsvorfällen. Mit umfangreichen Daten und verhaltenspsychologisch fundierten Insights können Sie mögliche Schwachstellen beheben. Sie erhalten zudem ein ganzheitliches Bild über das Verhalten Ihrer Mitarbeitenden und den Erfolg Ihres Security-Awareness-Programms und können dadurch fundierte strategische Entscheidungen treffen.

- Aufschlussreiche Insights durch kontextuelle Daten, wie technische KPIs und verhaltensbasierte Kennzahlen
- Branchenspezifische Benchmarks und Handlungsempfehlungen für den Ernstfall
- Auf Audits nach ISO/IEC 27001 ausgelegt und 100 % DSGVO-konform

Danksagungen

Wir bedanken uns herzlich bei allen, die zu diesem Report beigetragen haben. Das gilt insbesondere für die Expertinnen und Experten, die in Interviews ihre Einblicke mit uns geteilt haben.

Jens Becker
Chief Information Officer & Chief Digital Officer
Zurich Gruppe Deutschland

Stefanie Boem
Datenschutzbeauftragte Sport-Thieme

Sascha Czech
Chief Security Officer Uniklinikum Münster

Stéphane Duguin
Chief Executive Officer CyberPeace Institute

Frank Heymann
Senior IT-Team Manager Buhlmann

Tobias Ludwichowski
Chief Information Security Officer Signal Iduna

Dr. Stefan Lüders
Computer Security Officer CERN

Martin Schmidt
Global Director of Digital Advisory
Freudenberg Home and Cleaning Solutions

Thomas Schumacher
Managing Director Accenture Security

Generalmajor Jürgen Setzer
Chief Information Security Officer Bundeswehr

Dr. Katrin Suder
Strategieexpertin für digitale Technologien, Wirtschaft und Politik

Thomas Tschersich
Chief Security Officer Deutsche Telekom und Chief Executive Officer Telekom Security

Kontakt

Bei weiterführenden Fragen zu diesem Report oder der zugrundeliegenden Recherche und Studie, wenden Sie sich bitte an:

Laura Hartmann
Head of Corporate Communications
press@sosafe.de

Haftungsausschluss:

Die Inhalte dieses Dokuments wurden mit größtmöglicher Sorgfalt recherchiert. Eine Haftung für die Richtigkeit, Vollständigkeit und Aktualität kann jedoch nicht übernommen werden. SoSafe übernimmt insbesondere keinerlei Haftung für eventuelle Schäden oder Konsequenzen, die durch die direkte oder indirekte Nutzung entstehen.

(ISC)² | CPE SUBMITTER

Sammeln Sie (ISC)² CPE-Punkte mit diesem Report.

SoSafe bietet (ISC)²-Mitgliedern die Möglichkeit, CPE-Punkte (Continuing Professional Education) zu erwerben. (ISC)²-Cybersicherheitszertifizierungen sind weltweit als der höchste Standard für herausragende Leistungen im Bereich der IT-Sicherheit anerkannt.

Wenn Sie nach der Lektüre dieses Reports Ihre CPE-Punkte anrechnen lassen möchten, scannen Sie dazu einfach den QR-Code.

sosafe

SoSafe GmbH
Lichtstraße 25a
50825 Köln

info@sosafe.de
www.sosafe-awareness.com/de
+49 221 65083800