Cybercrime-Trends 2024

Die größten Angriffstrends und
Best Practices für mehr Sicherheit

sosafe

Inhalt

2023 veränderte alles.
Es ist Zeit, sich für die Zukunft zu wappnen.

Das Jahr 2023 war aus vieler Sicht ein Wendepunkt. Seit der offiziellen Einführung von ChatGPT-3 im November 2022 schreiten KI-getriebene Innovationen in rasantem Tempo voran und **unsere Interaktion mit Technologie hat sich von Grund auf geändert**. Diese Entwicklung machte sich auch im Bereich der IT-Sicherheit bemerkbar, wo KI als zentrale Antriebskraft agiert – sie stärkt unsere Abwehrmechanismen und ermöglicht Cyberkriminellen gleichzeitig, immer ausgefeiltere Angriffstaktiken zu entwickeln.

Anfang 2024 stehen wir nun aufgrund dieser **nie dagewesenen Geschwindigkeit technologischer Innovation** vor einem verworrenen Netz aus Herausforderungen: Die wachsende Präsenz von KI bei Cyberangriffen, das zweischneidige Schwert neuer Technologien, wie 5G und Quantum Computing, und die Professionalisierung der Cyber-kriminalität in ein professionelles Geschäftsmodell. Noch komplizierter und weitreichender wird die Bedrohungslage durch den Anstieg des Hacktivismus und der Cyberangriffe in weltweiten politischen Krisen sowie die gezielte Verbreitung von Fehlinformationen. Und während sich die Lage weiter zuspitzt, haben Cyber-Sicherheitsteams mit Fachkräftemangel und Burnout zu kämpfen.

Während das Risiko eines **durch menschliches Versagen verursachten Cyberangriffs unter diesen Bedingungen vermutlich weiter ansteigen wird**, ist eine starke Sicherheitskultur unsere größte Hoffnung. Deshalb nehmen wir in diesem Report die neun Cybercrime-Trends für 2024 unter die Lupe und empfehlen sichere Verhaltensweisen, die Ihnen helfen, sich effektiv gegen die wachsende Bandbreite an Bedrohungen zu wappnen.

1 KI-basierte Cybercrime-Innovationen: Der Sturm am Horizont

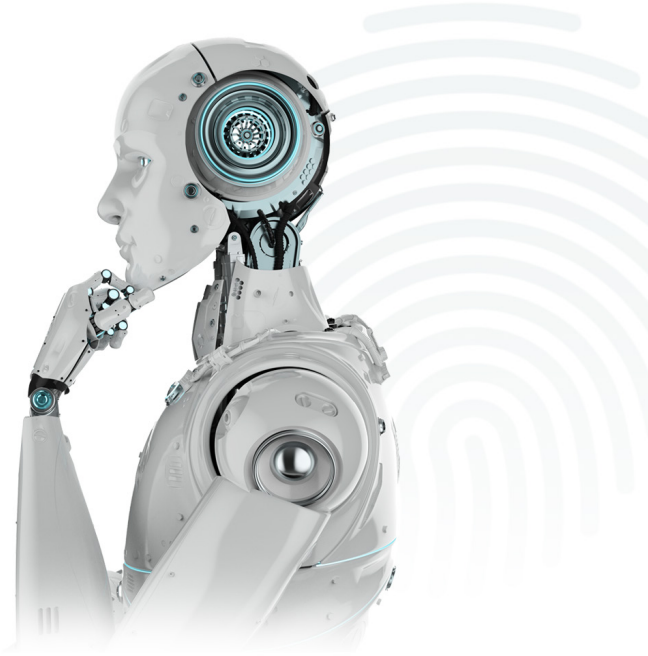
KI breitet sich aus wie ein Lauffeuer. Bis 2024 sollen bereits mehr als 300 Millionen User davon Gebrauch machen und bis 2030 sind es geschätzt 700 Millionen.[1] Diese Zahlen verdeutlichen nicht nur das Ausmaß der aktuellen und künftigen Tech-Revolution; sie lösen auch Bedenken in Bezug auf die Tragweite und möglichen Sicherheitsrisiken aus. Beim Thema KI-Risikofaktoren kommt man um die **Deepfakes** und **Voice-Cloning** nicht herum.

Schon seit geraumer Zeit setzen Cyberkriminelle beide Technologien für ihre betrügerischen Zwecke ein. In jüngster Zeit häufen sich die Fälle jedoch aufgrund der schnellen Verbreitung von Tools, mit denen sich überzeugende Deepfake-Videos erstellen lassen, die nun vor allem bei **Fehlinformations-Kampagnen und zur sozialen Manipulation** genutzt werden.[2] (Mehr dazu im Kapitel zu Disinformation-as-a-Service)

1 von 4

Personen wurden bereits **Opfer von Voice-Cloning** oder kennen jemanden, der es schon einmal erlebt hat.

Quelle: McAfee[3]



Voice-Cloning steht dem in nichts nach. Eine aktuelle Studie zeigte, dass eine von vier Personen bereits Opfer von Voice-Cloning wurde oder jemanden kennt, der es schon einmal erlebt hat.[3] Die Polizei in Everett, Washington, gab eine Warnung vor zunehmendem Finanzbetrug heraus, bei dem Voice-Cloning genutzt wird.[4] Während Voice-Cloning von Cyberkriminellen vor allem für Finanzscams eingesetzt wird – bis hin zur gefakten Entführung einer jungen Frau – ist es ihnen inzwischen auch gelungen, mit dieser Technologie **auf Stimmerkennung basierende MFA-Systeme hinters Licht führen**.[5] Einer Journalistin gelang es Anfang des Jahres, anhand einer Aufzeichnung ihrer

1 **Statista (2023).** Artificial Intelligence Worldwide.

2 **Heise (2024).** Was uns 2024 in der Künstlichen Intelligenz erwartet.

3 **McAfee (2023).** Artificial Imposters—Cybercriminals Turn to AI Voice Cloning for a New Breed of Scam.

4 **Fox 13 Seattle (2023).** Everett Police warn of AI voice-cloning phone scam after case reported in Snohomish County.

5 **CNN (2023).** 'Mom, these bad men have me': She believes scammers cloned her daughter's voice in a fake kidnapping.

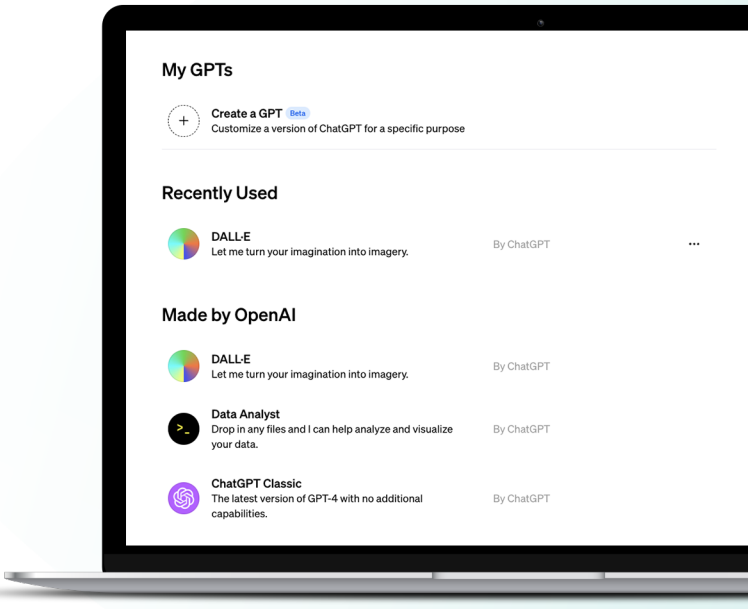
eigenen geklonten Stimme Zugriff auf ihr Bankkonto zu erlangen.[6] Das war zwar ein harmloses Experiment, doch die mögliche Tragweite der Bedrohung ist nicht zu unterschätzen.

Und das ist noch längst nicht der einzige Zweck, zu dem Cyberkriminelle KI missbrauchen. Durch die Innovation der generativen KI haben führende Tools im letzten Jahr ein Repertoire an Fähigkeiten dazu gewonnen. Einige davon, wie die Möglichkeit Bilder zu analysieren, können für betrügerische Zwecke missbraucht werden. Dazu gehört auch die Funktion der sogenannten **Prompt Injection**, bei der das Tool in der Abbildung enthaltene Anweisungen ausführt, anstatt den anfänglichen, beim Upload der Abbildung eingegebenen Prompt zu befolgen.[7] Was zunächst harmlos erscheinen mag, bietet unzählige Möglichkeiten der Manipulation von Usern.

Die Option des Bilduploads birgt weitere Risiken, wie die Möglichkeit, einen der bekanntesten Schutzmechanismen zu umgehen: **CAPTCHA-Codes**. Bis vor Kurzem war es für Cyberkriminelle vor allem aufgrund der ethischen Einschränkungen der Tools unmöglich, CAPTCHA zu lesen. Nun hat sich jedoch gezeigt, dass Bing Chat bei Vorgabe einer plausiblen Begründung oder eines überzeugenden Pretextes diese Codes entschlüsseln kann.[8] Organisationen und Webseiten weltweit stellt dies vor die Frage, **ob aus Sicherheitsgründen auf andere Methoden umgestellt werden muss**.

Während die KI-Technologie voranschreitet, **nutzen Hacker bestehende Sprachmodelle als Basis, um ihre eigenen mächtigen KI-Tools zu entwickeln**. So entstanden die schädlichen ChatGPT-Varianten FraudGPT und WormGPT.[9] Bis Ende 2023 waren für die Erstellung solcher Tools (nicht für ihre Nutzung) noch technische Kenntnisse nötig.

Das hat sich kürzlich geändert, als OpenAI die Möglichkeit einführte, auf einfache Art seinen eigenen GPT-Chatbot zu erstellen und diesen für spezifische Aufgaben zu trainieren – ohne Coding-Skills und technisches Know-how. Personalisierte GPTs können zwar für viele Personen ein wertvoller Helfer sein, der sie bei täglichen Aufgaben unterstützt. Wir können jedoch davon ausgehen, dass **2024 auch Cyberkriminelle sich diese Möglichkeit zunutze machen und ihre ganz persönlichen Hacking-Assistenten erschaffen**[10] und sie dazu trainieren, extrem überzeugende Smishing-Nachrichten, Spear-Phishing-Mails oder polymorphe Malware zu verfassen.[11]



6 **The Wall Street Journal (2023).** I Cloned Myself With AI. She Fooled My Bank and My Family.

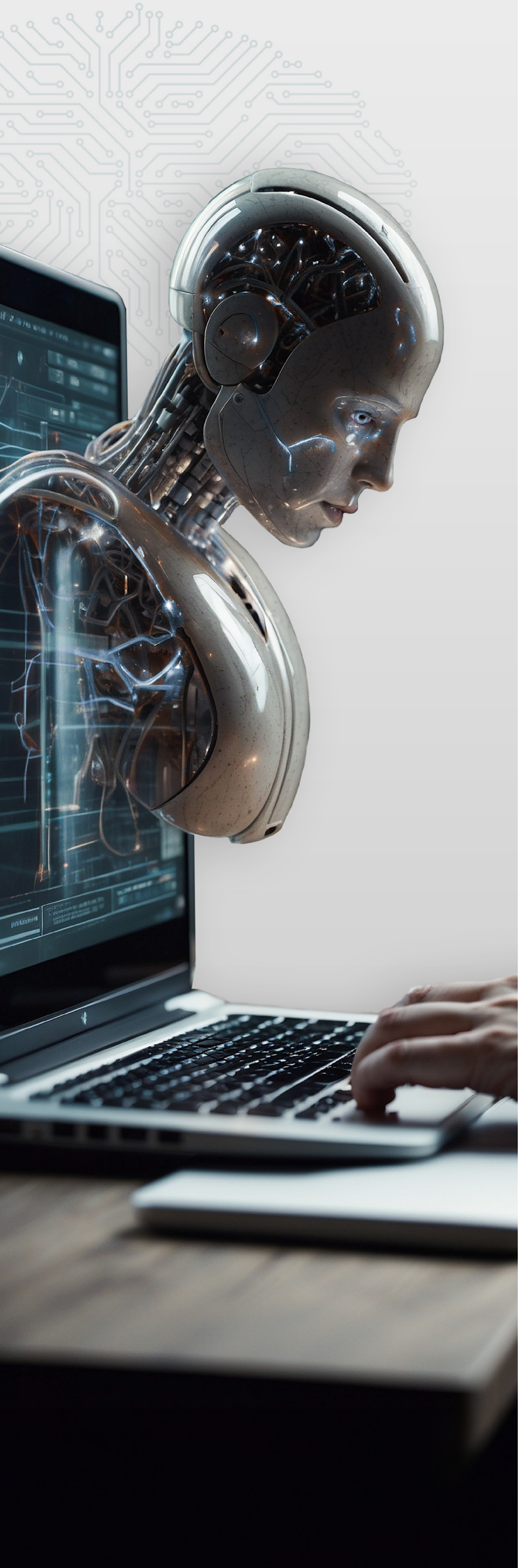
7 **Windows Central (2023).** CGPT-4 Vision: A breakthrough in image deciphering unveils potential for 'prompt injection attacks'.

8 **Digital Trends (2023).** Bing Chat just beat a security check to stop hackers and spammers.

9 **Handelsblatt (2023).** KI macht auch „weniger Talentierte" zu Trickbetrügern.

10 **BBC (2023).** ChatGPT tool could be abused by scammers and hackers.

11 **HYAS (2023).** Blackmamba: Using AI to generate polymorphic malware.



Doch nicht nur die neuen Möglichkeiten, die KI mit sich bringt, bergen Risiken; auch ihre **Einschränkungen**. Die Fähigkeit innovativer KI-Modelle, Code zu schreiben, ist ein großer Fortschritt, den bis zu 92 Prozent aller Entwicklerinnen und Entwickler bereits nutzen – in und außerhalb der Arbeit.[12] Es werden aber auch Bedenken zur **Zuverlässigkeit von KI-generiertem Code** laut. Expertenmeinungen zufolge ist eine Tendenz zur Priorisierung von Funktionalität über Sicherheit zu beobachten, was zu einer deutlich geringeren Code-Zuverlässigkeit führt.[13] Schwachstellen bestehen in der Anfälligkeit für SQL-Injection, Hard-Coded Credentials und der Nutzung von unsicheren Passwort-Hashing-Algorithmen.[14]

Doch die vielleicht bekannteste Einschränkung von KI ist ein Phänomen namens **Halluzinationen**, bei dem das Tool falsche oder gefakte Informationen bereitstellt. **Diese Halluzinationen nutzen Hacker zu ihrem Vorteil, um schädliche Dateien zu infiltrieren**.[15] Auf eine User-Anfrage hin „halluziniert" das Tool und empfiehlt Namen nicht bestehender Code-Bibliotheken. Daraufhin erstellen Hacker schädliche Code-Libraries oder -Packages unter diesen Namen und laden sie auf öffentliche Repositories hoch. Alle User, denen in Zukunft eines dieser Pakete empfohlen wird, laden die von den Hackern erstellte schädliche Code-Library herunter.

In Anbetracht der neuen Bedrohungen durch KI und der rasanten technologischen Innovationen **ist es unerlässlich, robuste Abwehrmethoden zu implementieren**. Ein proaktiver IT-Sicherheitsansatz ist sowohl für Organisationen als auch für Privatpersonen wichtig, die sich in einer immer stärker von KI beeinflussten Welt schützen wollen.[11]

12 **GitHub Blog (2023).** Survey reveals AI's impact on the developer experience.

13 **The Register (2023).** Perhaps AI is going to take away coding jobs – of those who trust this tech too much.

14 **Nord Security (2023).** ChatGPT and secure coding: The good, the bad, and the dangerous.

15 **Infosecurity Magazine (2023).** New ChatGPT Attack Technique Spreads Malicious Packages.

CHECKLISTE

So reduzieren Sie Ihr Risiko

- **Prüfen Sie KI-generierten Code vor der Implementierung:** Selbst wenn Sie das Tool beauftragen, sicheren Code zu generieren, ist es ratsam, seine Sicherheit durch automatisierte Codeprüfungs-Tools bestätigen zu lassen oder standardisierte Security-Benchmarks einzuführen.
- **Kennen Sie die neuesten KI-Trends und passen Sie Ihre Sicherheitsstrategie an:** Da manche Sicherheitsmaßnahmen aufgrund neuer Technologien nicht mehr verlässlich sind, brauchen Sie zum Schutz Ihrer Organisation alternative Lösungen. Ein erster Schritt wäre eine spezielle Arbeitsgruppe oder Intelligence Unit, die sich darauf konzentriert, KI-basierte Angriffe zu überwachen und zu analysieren, ob die genutzten Methoden Ihre Sicherheitslage beeinflussen.
- **Setzen Sie KI-Tools mit Bedacht ein:** Geben Sie keine persönlichen Daten ein und vertrauen Sie nicht blind auf alle Informationen, die KI-Tools bereitstellen. Bedenken Sie, dass manche Antworten falsch oder nicht mehr aktuell sein können – alle Angaben sorgfältig zu prüfen, zahlt sich aus.
- **Stärken Sie Ihre Abwehr mit KI:** KI-getriebene Tools können die Analyse großer Datensätze immens beschleunigen, was es Organisationen erleichtert, Abweichungen zu erkennen oder Bedrohungen in Echtzeit zu identifizieren. Die Integration von KI mit SOAR-Technologien (Security Orchestration, Automation und Response) ermöglicht automatisierte, intelligente Entscheidungsfindung und schnellere Reaktion bei einem Sicherheitsvorfall. Durch den Einsatz von KI in No-Code-Automation können Security-Workflows zudem schnell an neue Bedrohungen angepasst werden. KI-basierte Authentifizierungssysteme lernen und optimieren Sicherheitsmaßnahmen kontinuierlich. In Kombination mit ständiger menschlicher Überwachung wird sichergestellt, dass sie zudem mit Ihren Richtlinien und ethischen Aspekten in Einklang sind.
- **Seien Sie bei verdächtigen Voice- oder Videonachrichten wachsam:** Auch wenn sie zunächst glaubwürdig erscheinen, sollten Sie bei ungewöhnlichen Anfragen oder verdächtigen Aussagen wachsam werden. Lassen Sie sich die Anfrage im Zweifelsfall von der jeweiligen Person über einen anderen Kanal bestätigen.
- **Sensibilisieren Sie Ihre Mitarbeitenden zu den Sicherheitsrisiken von KI:** Ihre Mitarbeitenden sind Ihre stärkste Verteidigungslinie, wenn sie das nötige Know-how haben, um sich selbst und Ihre Organisation zu schützen. Befähigen Sie sie außerdem, generative KI verantwortungsbewusst zu nutzen, um sensible Daten zu schützen.

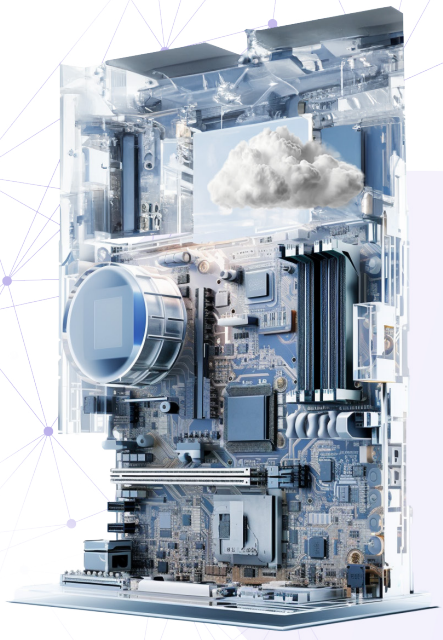
2 Jenseits von KI: Keine neue Technologie ist immun gegen Cyberkriminalität

Sie mag die größte Technologieinnovation des Jahrhunderts sein, doch trotzdem fokussieren sich Cyberkriminelle nicht allein auf KI. Stattdessen **erweitern sie ihren Horizont**, indem sie ihren Nutzen aus verschiedensten neuen Technologien ziehen – mit dem Ziel, die Angriffsfläche zu vergrößern und möglichst viele Personen zu treffen. Dadurch wird jede neue **Technologie sowohl zum Werkzeug als auch zur Zielscheibe** für ausgefeilte Cyberangriffe.

Dieser Trend ist jedoch nicht völlig neu. Schon zuvor konnten wir ähnliche Muster bei aufstrebenden Technologien beobachten; so auch beim **Cloud Computing**. In den letzten Jahren steckten Organisationen Investitionen in Milliardenhöhe in cloudbasierte Speicher, anstatt sich auf traditionelle Speicherlösungen zu verlassen – eine Entwicklung, die auch von Cyberkriminellen nicht unbemerkt blieb. Laut dem Global Threat Report von CrowdStrike verdoppelten sich die Angriffe auf Cloud-Systeme 2022 nahezu, während sich die Anzahl an Hackergruppierungen, die zur Ausführung solcher Angriffe in der Lage sind, künftig verdreifachen wird.[1]

Das wurde beim Ransomware-Angriff in Sri Lanka Anfang August 2023 nur allzu deutlich.[2] Dabei drangen die Angreifenden in das Cloud-System der Regierung Sri Lankas ein, indem sie Regierungsangestellten schädliche Links schickten. Bei diesem Angriff wurden Regierungsdaten der letzten vier Monate ausgelöscht, weil dem Cloud-System die nötigen Back-up-Lösungen fehlten.

Ein ähnliches Schicksal ist für andere neue Technologien wie **Quantencomputing** zu erwarten. Dabei gehen Cyberkriminelle nach einer potenziell gefährlichen Methode vor: „Harvest now, decrypt later“ (HNDL).[3] Das heißt, sie fokussieren sich zunächst auf das Sammeln verschlüsselter Daten in der Hoffnung, dass sie durch den Fortschritt im Quantencomputing in Zukunft in der Lage sein werden, die gesammelten Daten zu entschlüsseln. Dieses Szenario könnte zu Datenschutzverstößen, Diebstählen geistigen Eigentums und Freilegung nationaler Sicherheitsstrategien von nie dagewesenem Ausmaß führen.



1 **CrowdStrike (2023).** Global Threat Report.

2 **Infosecurity Magazine (2023).** Ransomware attack wipes out Sri Lankan government data.

3 **Computerwoche (2022).** Zwischen Chance und Sicherheitsrisiko.

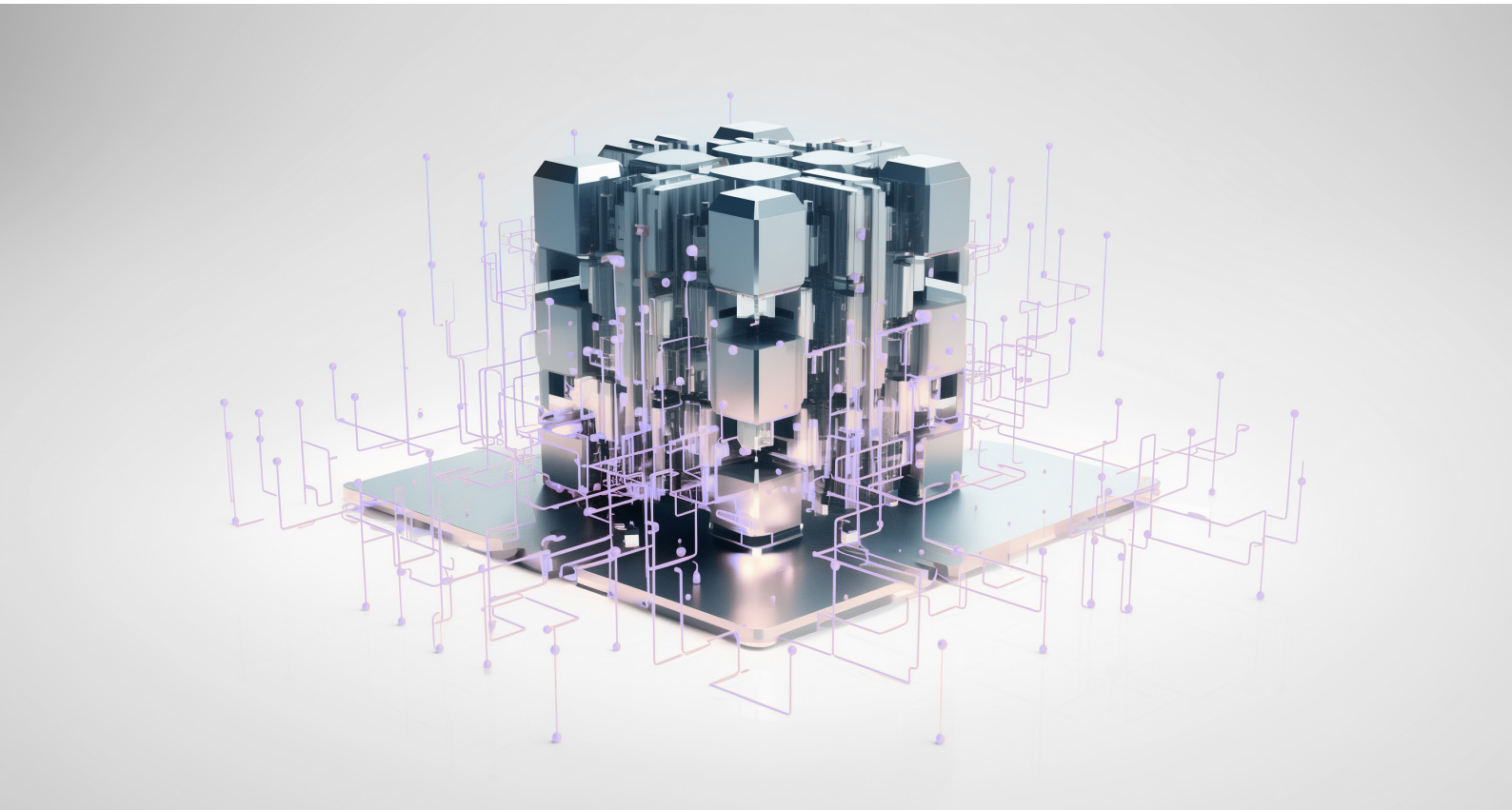
Das National Cyber Security Centre in Großbritannien erkannte die Problematik und verfasste bereits 2020 ein White Paper mit Empfehlungen für die Umstellung auf quantenresistente Algorithmen.[4] Dem zufolge sei es wichtig, den Prozess frühzeitig einzuleiten, um sich vor möglichen Bedrohungen durch Quantum Computing zu schützen. Die Bedrohungslage ist besonders komplex, da nicht vorherzusehen ist, wie schnell die nächsten Meilensteine in der Entwicklung des Quantum Computing erreicht werden. Organisationen sehen sich deshalb gezwungen, die Kosten einer frühzeitigen Einführung quantenresistenter Schutzmaßnahmen abzuwägen, um bei einem plötzlichen technologischen Durchbruch nicht völlig unvorbereitet zu sein.

Die **5G-Technologie** ist eine weitere bahnbrechende Technologie, die sich als zweischneidiges Schwert erweist – sie verspricht nie dagewesene Konnektivität und Geschwindigkeit, während sie gleichzeitig neue Eintrittstore für Cyberkriminelle öffnet. Die Cybersecurity and Infrastructure Security Agency (CISA) der USA definierte die folgenden mit 5G verbundenen Risiken: vermehrte Schwachstellen durch komplexe Netzwerke und lokale 5G-Einrichtungen; Supply-Chain-Angriffe mittels schädlicher Hardware und Software; vererbte Schwachstellen aus alten Infrastrukturen und nicht vertrauenswürdigen Komponenten; Abhängigkeit von potenziell unsicheren proprietären Lösungen aufgrund von beschränktem Marktwettbewerb; sowie eine erweiterte Angriffsfläche, die neue Schwachstellen und ein erhöhtes Risiko für Datenlecks mit sich bringt.[5]

Nach alldem ist eines klar: **Während sich diese und andere neue Technologien weiterentwickeln, gilt dasselbe für die Methoden und Zielscheiben der Cyberkriminellen**. Es ist ein stetiger Wettlauf und jede aufstrebende Technologie öffnet Türen für neue Betrugsmöglichkeiten. Die Konsequenz: Wir brauchen agile und adaptive Cyber-Security-Strategien, die sich zusammen mit den technologischen Innovationen entwickeln und so unsere Risiken reduzieren.

4 **National Cyber Security Centre (2020).** Preparing for quantum-safe cryptography.

5 **CISA (2023).** 5G Security and Resilience.



CHECKLISTE

So reduzieren Sie Ihr Risiko

- **Stärken Sie Ihre Cloud-Sicherheit:** Investieren Sie in umfassende Back-up- und Recovery-Systeme für Ihre Cloud-Speicher und führen Sie routinemäßig regelmäßige Updates und Patches durch, um Ihren Schutz bei neuen Bedrohungen aufrechtzuerhalten.
- **Reduzieren Sie das Diebstahlrisiko verschlüsselter Daten:** Nutzen Sie Mikrosegmentierung zum Schutz Ihrer Daten, wechseln Sie Kodierungsschlüssel regelmäßig je nach Datenklassifizierung und stellen Sie sicher, dass Ihre Software und Sicherheitsmaßnahmen stetig aktualisiert werden.
- **Setzen Sie auf Krypto-Agilität:** Durch einen agilen Ansatz sind Sie bei neuen Angriffsmethoden jederzeit bereit, Algorithmen und kryptografische Verfahren schnell zu wechseln.
- **Sichern Sie 5G-Netzwerke:** Schließen Sie Schwachstellen in komplexen Netzwerken und lokalen Implementierungen und gewährleisten Sie die Sicherheit der Lieferkette, einschließlich der Hardware- und Softwarekomponenten.
- **Beheben Sie Schwachstellen alter Infrastrukturen:** Aktualisieren oder ersetzen Sie veraltete Systeme, um damit verbundene Sicherheitslücken zu beseitigen, und berücksichtigen Sie Sicherheitsaspekte bei der Implementierung neuer Technologien.
- **Beobachten Sie die Bedrohungslage und passen Sie sich an:** Halten Sie sich zu neu aufkommenden Angriffstaktiken auf dem Laufenden, passen Sie Ihre Sicherheitsstrategien an und implementieren Sie durchgehende Überwachung und Bedrohungsanalyse in Echtzeit.
- **Stärken Sie das Cybersicherheits-Wissen Ihrer Mitarbeitenden:** Genau wie beim KI-Trend gilt auch hier: Kontinuierliches Training und Weiterbildung befähigen sowohl Ihr Sicherheitsteam als auch andere Mitarbeitende, neue Bedrohungen zu erkennen und im Ernstfall schnell zu reagieren.

3 Cybercrime wird als Geschäftsmodell immer professioneller und profitabler

Die Professionalisierung der Cyberkriminalität schreitet weiter voran und wird 2024 ein neues Level der Profitabilität erreichen. Diese Skalierung ist unter anderem auch auf die Verbreitung von **Ransomware-as-a-Service (RaaS)** zurückzuführen. Schon letztes Jahr gingen wir in unserem Report darauf ein, wie fortschrittliche RaaS-Tools Kriminellen den Einstieg in Cybercrime erleichtern und gleichzeitig die Komplexität und Auswirkungen von Cyberangriffen exponentiell steigern können.

Im letzten Jahr hat sich die Bedrohungslage rapide zugespitzt; 2023 **verdoppelte sich die Anzahl an Opfern von Ransomware-Angriffen** im Vergleich zum April 2022.[1] Dieser besorgniserregende Anstieg verdeutlicht, dass Ransomware **für Organisationen im EMEA-Raum immer noch die schädlichste, kostspieligste und häufigste Angriffsmethode ist**.[2]

Diese Entwicklung zeigt sich auch deutlich in der immer präziser ausgewählten Zielgruppe von Ransomware-Angriffen. Wie wir an späterer Stelle noch erläutern werden, gibt es einen deutlichen Trend hin zu **gezielten Angriffen auf den öffentlichen Sektor und kritische Infrastrukturen** – vor allem das Gesundheits- und Bildungswesen und Regierungsorganisationen. Der Grund: Einrichtungen in diesen Sektoren fehlen oft die nötigen Sicherheitsressourcen. Dadurch sind sie eher bereit, zur Aufrechterhaltung wichtiger Dienste und zum Schutz sensibler Daten auf die Lösegeldforderung einzugehen. Ein schockierendes Beispiel für einen solchen Angriff trug sich im Mai 2023 in Maine zu, als eine Ransomware-Gruppe eine Schwachstelle in dem von staatlichen Behörden genutzten Dateiübertragungsprogramm MOVEit ausnutzten. Die **Angreifenden stahlen Daten von 1,3 Millionen Personen**, darunter Namen, Geburtsdaten, Versicherungsnummern, Führerscheinnummern und andere Identifikations- und Steuernummern.[3]

Doch es hat auch andere Sektoren getroffen. MGM Resorts, eine der größten Hotel- und Casinoketten weltweit, wurde im September 2023 Zielscheibe eines Angriffs durch Scattered Spider, einer Untergruppe der ALPHV-Ransomware-Gruppe.[4] Die Angreifenden machten einen der Mitarbeitenden auf LinkedIn ausfindig und riefen das Help Desk an, das sie mittels Social-Engineering-Taktiken manipulierten. **Ein zehnminütiges Gespräch genügte, um das Milliarden-Dollar-Unternehmen zu hacken**. Der Cyberangriff auf MGM Resorts hatte großflächige Ausfälle zur Folge; Bargeldautomaten und Spielautomaten waren lahmgelegt, genauso wie die Webseite und Buchungssysteme. Der Gewinn des dritten Quartals fiel Schätzungen zufolge infolge des Angriffs 100 Millionen US-Dollar geringer aus, während das Unternehmen weitere 10 Millionen US-Dollar an Wiederherstellungskosten für Tech-Consulting, Rechtskosten und Honorare anderer externer Berater einbüßte.

1 **Black Kite (2023).** Ransomware threat landscape report.

2 **Gulf Business (2023).** Cybersecurity 2023: Threats proliferate but best practice still works.

3 **Mashable (2023).** An entire state's population just had its data stolen by a ransomware group.

4 **TechCrunch (2023).** MGM Resorts confirms hackers stole customers' personal data during cyberattack.

> **Im Schnitt dauert es 23 Tage, den grundlegenden Betrieb nach einem weitreichenden Ransomware-Angriff wiederherzustellen. Die Wiederherstellung des gesamten Systems und vollen Funktionsumfangs kann Monate dauern.**

Inge van der Beijl
Expertin für Human Resilience und Kommunikation mit Cyberkriminellen bei Northwave, auf der Human Firewall Conference 2023

Das stetig aggressivere Vorgehen der Cyberkriminellen zeigt sich vor allem in den skrupellosen Ransomware-Methoden. **Immer häufiger werden Double-Extortion-Angriffe**, bei denen die Angreifenden sensible Daten verschlüsseln und im gleichen Zug mit ihrer Veröffentlichung drohen.[5] Zudem sind weitere Mehrfacherpressungen zu beobachten, wie **Dreifach-Erpressung**, bei der eine weitere Angriffsmasche wie DDoS hinzukommt; oder gar **vierfache Erpressungstaktiken**, bei denen im Nachhinein Kunden, Zulieferer und Mitarbeitende der betroffenen Organisation unter Druck gesetzt werden. Als der Hardware-Anbieter Quanta Computer nicht auf die Lösegeldforderung der Hackergruppe REvil einging, nahmen die Angreifenden Apple ins Visier, einer von Quantas Kunden.[6] Apple wurde mit der Veröffentlichung seiner vertraulichen Produkt-Blueprints gedroht. Zusätzlich erhöhten die Angreifenden den Druck, indem sie die Veröffentlichung zum Zeitpunkt einer Produkteinführung durchführen wollten – mit Folgen unvorstellbaren Ausmaßes aufgrund der Aufmerksamkeit der Öffentlichkeit und Medien.

Die Professionalisierung der Cyberkriminalität geht über RaaS hinaus und macht auch vor aufstrebenden Technologien wie Voice-Cloning keinen Halt. Wie wir bereits im Kapitel zur KI gesehen haben, ist auch **Voice-Cloning-as-a-Service** (VCaaS) zu einer ernstzunehmenden Bedrohung geworden, die es selbst Kriminellen ohne technische Kenntnisse ermöglicht, überzeugende Täuschungsangriffe auszuführen.[7] Mit Plattformen wie ElevenLabs, auf der User individuelle Sprachausgaben generieren können, wird die Zutrittsschwelle zur Cyberkriminalität immer geringer.

Während die Professionalität und Komplexität der Cyberangriffe weiter zunimmt, wird die Sicherheit der Lieferkette wichtiger denn je, um unseren Schutz zu verbessern. Outsourcing spielt heute für Organisationen eine entscheidende Rolle, doch es schafft auch Schwachstellen und bietet Cyberkriminellen die Möglichkeit, **über Partner und Zulieferer in das Unternehmensnetzwerk einzudringen**. So erging es 2023 zum Beispiel Airbus. Hacker verschafften sich Zugang zu den Systemen einer seiner Kunden, Turkish Airlines, wobei die Daten von mehr als 3.000 Zulieferern gestohlen wurden.[8] Eine Organisation ist nur so stark wie das schwächste Glied in ihrer Lieferkette. Zu ihrem eigenen Schutz müssen Organisationen auch die Sicherheit ihrer Zulieferer, Partner und Kunden kritisch hinterfragen.

Die Prognose für die Zukunft ist eindeutig: **Die Cyberkriminalität ist dabei, als Geschäftsmodell noch professioneller und profitabler zu werden** – ein Trend, den wir weder ignorieren noch unterschätzen dürfen. Jetzt ist für Organisationen die Zeit gekommen, in ihre Sicherheit zu investieren. Die beunruhigenden Entwicklungen der letzten Jahre sind erst die Spitze des Eisbergs, denn Cyberkriminelle werden auch in Zukunft ihre Methoden weiter perfektionieren.

5 **IT Daily (2023).** Ransomware: Immer mehr Double Extortion-Angriffe.

6 **Heise (2021).** Ransomware bei Fertiger Quanta: REvil-Gruppe will Apple erpressen.

7 **Recorded Future (2023).** I have no mouth, and I must do crime.

8 **The Register (2023).** Airbus suffers data leak turbulence to cybercrooks' delight.

CHECKLISTE

So reduzieren Sie Ihr Risiko

- **Bauen Sie eine resiliente Infrastruktur gegen Ransomware auf:** Entwickeln Sie einen ganzheitlichen Sicherheitsansatz, der sowohl vorbeugende Maßnahmen als auch solide Reaktionspläne umfasst. Dazu gehören moderne Threat-Detection-Systeme, wie KI-getriebene Anomalie-Erkennung, sowie eine Zero-Trust-Architektur zur Stärkung der Sicherheit. Führen Sie regelmäßig Security-Audits durch und entwickeln Sie effektive Disaster-Recovery-Pläne. Überarbeiten Sie zudem regelmäßig Ihre Back-up-Methoden und stellen Sie sicher, dass ein solider Reaktionsplan vorhanden ist, der bei einem Datenschutzverstoß eine schnelle Reaktion ermöglicht.

- **Schützen Sie sich vor Social-Engineering- und Phishing-Angriffen:** Sensibilisieren Sie Ihre Mitarbeitenden zu den Risiken von Social-Engineering-Angriffen, insbesondere zu den beliebtesten Strategien von Ransomware-Gruppen. Durch kontinuierliches Training in Form von Micro-Modulen und Phishing-Simulationen steigern Sie Ihre Awareness und befähigen sie, mögliche Bedrohungen zu erkennen. Personalisierte Lernerfahrungen mit Gamification-Elementen steigern zudem die Motivation und den Wissenserhalt.

- **Setzen Sie sich mit Zero-Day-Schwachstellen auseinander:** Entwickeln Sie Strategien, die eine schnelle Reaktion bei Zero-Day-Angriffen ermöglichen. Dazu gehören Patch-Management-Lösungen für die systematische Durchführung von Software-Updates und das zeitnahe Schließen von Sicherheitslücken.

- **Stärken Sie die Sicherheit Ihrer Lieferkette:** Werfen Sie einen genauen Blick auf Ihre Lieferkette. Überprüfen Sie die Sicherheitsprotokolle Ihrer Partner und Zulieferer und implementieren Sie strenge Zugriffsverwaltungs- und Überwachungssysteme.

- **Verbessern Sie die Datensicherheit und -integrität:** Nutzen Sie moderne Verschlüsselungsmethoden und implementieren Sie einen mehrschichtigen Ansatz beim Datenschutz durch die Nutzung datenzentrierter Sicherheitsframe-works und DLP-Technologien (Data Loss Prevention). Dadurch reduzieren Sie das Risiko der Freilegung und des Diebstahls sensibler Daten.

- **Nutzen Sie Threat Intelligence und Analytics:** Threat-Intelligence-Tools helfen Ihnen bei der Bestimmung und Analyse aktueller und künftiger Bedrohungen. Dadurch können Sie gezieltere Schutzmaßnahmen einrichten und Ihre Reaktionsfähigkeit bei einem Zwischenfall verbessern.

INTERVIEW

Ralf Schneider

Allianz Senior Fellow and Head of Cyber Security and NextGenIT Think Tank

Ralf Schneiders beeindruckende Laufbahn in der IT und Cyber Security erstreckt sich über zwei Jahrzehnte und ist durch seine lange Tätigkeit bei der Allianz geprägt, wo er 13 Jahre lang Group CIO war. Zudem war er Vorstand der Allianz Managed Operations & Services und hat seit Kurzem die Position Allianz Senior Fellow and Head of Cybersecurity and NextGenIT Think Tank inne. Er promovierte in Computerwissenschaft an der Ludwig-Maximilians-Universität München.

> Kriminelle brauchen immer weniger Skills und immer weniger Organisationspower, um einen wirklich guten Angriff zu fahren. Letztlich wird uns das vor ein Mengenproblem stellen.

Wie war Ihr Weg in die Informationssicherheit?

Mein Startpunkt in der Informationssicherheit war mit meiner Ernennung zum Group CIO der Allianz im Januar 2011. Mit 3.000 Offices und 63 Business Units in der ganzen Welt wurde mir schnell klar, dass wir eine Kommunikationsinfrastruktur brauchten, zu der auch Videokonferenzen gehörten. Wir mussten unsere IT so bauen, dass wir nach dem Motto „Any place, any device, anytime“ sozusagen rund um die Uhr von jedem Ort der Welt aus mit jedem Device auf IT-Ressourcen zugreifen können. Dazu braucht man eine Netzinfrastruktur, ein konsolidiertes Data Center, damit die Applikationen überhaupt global funktionieren, und einen virtualisierten End-Arbeitsplatz – und das alles muss zudem sicher sein. Dass Cyber Security ein Riesenthema für uns sein würde, stand damit außer Frage.

Als es 2013 zu den Snowden-Disclosures kam und das Handy von Frau Merkel gehackt wurde, war klar, dass Cybersicherheit immer brisanter wird. Neben dem Infrastrukturnetz, Data Center und virtualisierten Arbeitsplatz haben wir 2013 dann auch die Cyber-Security-Infrastruktur, Global Identity und Access Management, Global Privilege Access Management und das Allianz Cyber Defense Center global ins Leben gerufen.

Wie schätzen Sie die aktuelle Bedrohungslage und die Entwicklung in den nächsten Jahren ein?

Spätestens seit dem Ukraine-Krieg ist klar, dass wir uns in einem Cyberwar befinden. Neben staatlichen und militärischen Akteuren haben wir es in der Cyber Security auch mit einer hochausgebildeten, kriminellen Energie zu tun. Das Vorgehen der Cyberkriminellen wird immer ausgefeilter und sie sind besser organisiert. Hinzu kommt die Industrialisierung von Cyberattacken, die die Cyberkriminalität immer mehr zu einem kriminellen Big Business werden lässt.

Doch es gibt eine dritte Komponente: Cyber Security tendiert dazu, sich wiederholende Wellen zu durchlaufen. 2013 war DDoS eines der zentralen Themen, zwischenzeitlich war es verschwunden und jetzt steht es wieder ganz hoch im Kurs. Genauso müssen wir damit rechnen, dass der Fokus auf Aktivisten wie auch Hacking Kits wiederkommen, auch angetrieben von AI. Kriminelle brauchen immer weniger Skills und immer weniger Organisationspower, um einen wirklich guten Angriff zu fahren. Letztlich wird uns das vor ein Mengenproblem stellen. Anstatt sich auf einige Gruppen zu fokussieren, stehen wir dann vor hunderten, wenn nicht tausenden.

Dass die Welt sich immer weiter in Arm und Reich spaltet, macht das Szenario umso gefährlicher. Man muss nicht mehr Profisportler werden, um gutes Geld zu verdienen – man kann auch Hacker werden. Das Gute ist, dass wir uns auch immer besser verteidigen können.

Sie haben den Aufschwung von generativer AI erwähnt. Werden Technologien wie Deep Fakes und Voice-Cloning Ihrer Einschätzung nach auch zu einem Massenproblem?

Voice-Cloning und ähnliche Methoden sind massiv im Kommen. Ich sehe aber noch eine andere Gefahr durch die neuen Technologien. Es geht nicht mehr nur darum, eine Sicherheitslücke zu finden oder eine Person als Schwachstelle auszumachen. Es geht auch um die Response, das heißt das Ausschalten bzw. Umgehen von Detection Tools. Genau da wird AI auch verstärkt zum Einsatz kommen.

Abgesehen von komplexen AI-gestützten Angriffen, sehe ich aktuell noch keine große Gefahr durch automatisierte AI-basierte Angriffe, da AI noch zu viele Fehler macht und auf die richtige Bedienung durch den Menschen angewiesen ist. Aber wir stehen ja noch am Anfang und letztlich sollte man sich immer auf das Worst-Case-Szenario vorbereiten. Wovon wir im Moment noch profitieren, ist, dass diese große Skalierung noch nicht stattgefunden hat. Derzeit lernen wir mit jedem Angriff – ob erfolgreich oder nicht – dazu und können unsere Verteidigung verbessern. Aber letztlich besteht das Risiko nicht nur in der Menge, sondern auch in der Gleichzeitigkeit, die die AI ermöglicht. Solch gleichzeitige Skalierungsangriffe werden in Zukunft zu einer großen Herausforderung.

Wie können wir Ihrer Ansicht nach mit den rasanten Entwicklungen der Bedrohungslage Schritt halten?

Kurz gesagt: Durch die richtige Cyberhygiene und indem man die Bedrohungslage im Auge behält. Die Cyberhygiene gilt es heute von Grund auf richtig aufzubauen, was eine große Herausforderung wird. Um Multifaktor-Authentifizierung kommt man meiner Meinung nach auch nicht mehr herum. Bevor man mit dem Auto losfährt, schnallt man sich an. Bevor man lossurft, macht man Multifaktor-Authentifizierung. Bei der Allianz haben wir Multifaktor-Authentifizierung während Corona aufgrund von Remote Work eingeführt.

Und das Allerwichtigste, um mit der Geschwindigkeit mitzuhalten: Man muss ganz am Anfang richtig gut und flächendeckend arbeiten und dann am Markt bleiben. Wir erneuern derzeit unsere Cyber Defense Plattform und rüsten sie mit AI nach. Die große Aufgabe ist nun, das zu integrieren und auf die Straße zu bringen, aber da investieren wir. Letztlich hängt aber alles am Faktor Mensch. Die richtigen Menschen zu finden und ihnen die Möglichkeiten zu bieten, sich eigenverantwortlich weiterzubilden. Wenn man keine Capability oder Awareness im Unternehmen hat, dann nützen sämtliche Technologien nur bedingt etwas.

Letztlich hängt alles am Faktor Mensch. Die richtigen Menschen zu finden und ihnen die Möglichkeiten zu bieten, sich eigenverantwortlich weiterzubilden. Wenn man keine Capability oder Awareness im Unternehmen hat, dann nützen sämtliche Technologien nur bedingt etwas.

Ein weiterer Cybercrime-Trend ist die Digitalisierung, die alles zunehmend miteinander vernetzt. Welche Risiken sehen Sie dadurch im Cyber-Security-Bereich?

Eine Webseite zu betreiben, ohne von einem Proxy-Schild vor den grundlegenden Bedrohungen geschützt zu sein, ist hochriskant. Jedes Unternehmen braucht also ein gutes Proxy-Schild und das ist auch wieder mit Kosten verbunden.

Heute ist alles mit allem vernetzt, und das sozusagen in Lichtgeschwindigkeit. Zudem wird es von Software operiert, die in Millisekunden Aktionen ausführen kann. Ohne Automatisierung ist da eine Überwachung und Steuerung nicht mehr möglich. Dabei dürfen wir aber nicht hoffen, dass AI alles für uns macht. Wir werden von Menschen mit AI angegriffen, dann müssen wir uns auch als Menschen mit Hilfe von AI verteidigen. Und diese Menschen müssen ausgebildet sein und das nötige Verständnis und Wissen mitbringen. Hinzu kommt, dass die Kontaktpunkte zu den IT-Systemen nicht nur Maschinen, sondern meistens Menschen sind. Als kritisches Momentum muss jeder dieser Kontaktpunkte überwacht und gegen Angriffe abgesichert werden.

Die Frage ist, sollten Unternehmen erst die technische Lücke schließen und darauf den Menschen setzen oder umgekehrt. Was ist aus Ihrer Sicht eine holistische Strategie, die den Faktor Mensch einschließt?

Wenn du einfach so in eine Schlacht ziehst, dann verlierst du jede Schlacht. Wenn du deinen Gegner kennst, dann verlierst du wahrscheinlich jede zweite Schlacht. Aber wenn du dich kennst und deinen Gegner kennst, dann hast du eine große Chance, jede Schlacht zu gewinnen. Ähnlich ist auch die Cyber Security ein Angriff- und Verteidigungsspiel. Wir begannen 2013 mit zwei Controls, die wir flächendeckend ausgerollt haben – DDoS und Absicherung der mobilen Endgeräte. Wir haben also mit Awareness und mit der Absicherung gegen DDoS und der mobilen Endgeräte flächendeckend begonnen und danach kamen sämtliche Layer hinzu, wie Protection, Detection, Response und Recovery Layer.

Nach unserer 2000 Jahre alten Weisheit geht es in einem Angriffs- und Verteidigungsszenario darum, seinen Gegner und sich selbst zu kennen. Das bedeutet für uns heute, dass wir neben der Bedrohungslage auch unsere eigenen IT-Systeme, unser Netzwerk und unsere Schwachstellen kennen müssen. Denn man kann nichts verteidigen, das man nicht kennt. Da die IT-Systeme von Menschen entwickelt und bedient werden, muss man auch die Menschen kennen und ihre Awareness für sichere IT steigern.

Wie sehen Sie beim Thema Awareness Training die Entwicklung von einer reinen Compliance-Pflicht hin zu einer kontinuierlichen Maßnahme, die die Menschen befähigt, zu einem Teil der Verteidigung zu werden?

Im heutigen Digitalisierungsumfeld kann IT nicht mehr nur funktional sein – sie muss funktional, sicher und compliant sein. Doch nicht alles, was gut für die Compliance ist, verbessert automatisch auch die Sicherheit. Ein gutes Beispiel ist das Thema Awareness. Man führt ein Awareness-Programm in Form eines webbasierten Trainings ein, erhält seinen Compliance-Haken und der Regulator ist zufrieden. Damit hat man im Bereich Sicherheit noch nichts gewonnen, solange die User nicht sensibilisiert sind.

Hier kommt die Befähigung der Mitarbeitenden ins Spiel. Wir haben früh erkannt, dass man das Thema Awareness spielerisch angehen muss, nicht mit Druck. Dabei ist auch der Zeitpunkt der Schulung entscheidend. Ideal ist, wenn ich gerade eine Phishing-Kampagne bekommen habe oder eine echte Phishing-Mail. Die nächste Herausforderung ist, die Aufmerksamkeit zu halten. Ein extrem nützliches Tool ist da der Phishing-Meldebutton von SoSafe. Wenn sich Mitarbeitende unsicher sind, ob es sich um eine Phishing-Mail handelt, sagt der ihnen, ob es Phishing ist und woran er das festmacht. Der Lernerfolg ist da immens. Hinzu kommt der Spaßfaktor und die Motivation, dadurch, dass die Menschen selbstständig lernen und gleichzeitig den Meldebutton als eine Art Assistenten nutzen können. Die direkte Belohnung kommt dadurch, dass man das Erlernte direkt anwenden kann.

> Wir werden von Menschen mit AI angegriffen, dann müssen wir uns auch als Menschen mit Hilfe von AI verteidigen. Und diese Menschen müssen ausgebildet sein und das nötige Verständnis und Wissen mitbringen.

Auf den IT-Teams lastet jede Menge Druck, sowohl was die Verteidigung angeht als auch die Security Awareness Trainings. Was wären aus Ihrer Sicht mögliche Maßnahmen, mit denen man die IT-Teams entlasten kann?

Dazu müssen wir uns fragen, wo die Probleme wirklich liegen. Durchführen von Crisis Drills auf allen Ebenen bis zum Top Management im Gesamtvorstand. Das haben wir in der Allianz über die Jahre umgesetzt und die Crisis Drills werden regelmäßig wiederholt. Dabei spielen verschiedene psychologische Faktoren eine Rolle. Zum einen zeigen Leute ungern, wenn sie etwas nicht können. Zum anderen muss der Nutzen der investierten Zeit von vornherein klar sein und sich schnell zeigen. Denn Awareness-Training ist auch mit finanziellem und Ressourcen-Aufwand verbunden.

Den Geschäftsleitungen aller Geschäftseinheiten die Dringlichkeit der Cyber-Sicherheitsbelange greifbar zu veranschaulichen, ist eine der großen Herausforderungen. IT muss im Hinblick auf die Geschäftsziele in erster Linie funktional, gleichzeitig aber auch sicher sein. Solange jedoch noch nichts Schwerwiegendes passiert ist, ist es schwer einzuordnen, ob man durch die Implementierung verschiedener Maßnahmen nun besser gesichert ist als zuvor. Die Wirksamkeit zu beweisen und das Misstrauen zu beseitigen, ist eine große Herausforderung, denn man kann verbesserte Sicherheit nicht belegen, sondern muss über Angriffssimulationen zeigen, dass die Verteidigungsfähigkeit der Organisation immer schneller, effizienter und effektiver wird.

Gibt es Ihrer Ansicht nach KPIs, von denen sich die Führungsebene besser überzeugen lässt?

Bei der Allianz haben wir acht Cyber-Security-Health-Indikatoren gemäß dem NIST-Standard, die wir mit einem Art Ampelsystem mit den Farben Rot, Orange, Gelb, Hellgrün und Grün bewerten, um den Erfolg unserer Maßnahmen messbar aufzeigen zu können; dazu gehören Govern, Identify, Prevent, Detect, Response und Recover. Genauso wie Blutdruck, Puls und Cholesterinspiegel beim Menschen müssen auch unsere acht Health-Indikatoren in einem bestimmten Bereich liegen.

Zwei dieser Indikatoren haben sich als besonders effektiv erwiesen. Einer davon ist unsere Zero Tolerance gegenüber toxischen Komponenten, für die es keine Sicherheits-Patches mehr gibt. Die hat dazu geführt, dass wir alle veralteten, unzureichend geschützten Applikationen aufgespürt haben. Dazu haben wir automatisiert, alle veralteten Datenbanken und Betriebssysteme analysiert, toxische Komponenten bestimmt und so systematisch unser IT-System rundum erneuert. Die Zero-Tolerance-Komponente wurde aus Security-Gründen eingeführt, geht aber weit darüber hinaus.

Der zweite wirkungsvolle Indikator ist unser sogenannter Awareness-Score, den wir mit weltweiten Phishing-Kampagnen messen. Dabei messen wir die Klickrate, aber auch wie viele Personen eine schädliche Mail tatsächlich melden.

In einem Interview sagten Sie, dass hierarchische Strukturen in Unternehmen Cybersicherheit verhindern könnten. Was meinen Sie damit?

Die von außen kommenden, mit Tools ausgeführten Angriffe können nur von Experten mit den richtigen Tools abgewehrt werden. Deshalb müssen es auch die Sicherheitsexperten sein, die entscheiden, was zu tun ist. Die Führungsetage muss zwar alles im Blick haben und im richtigen Moment Ressourcen, Steuerungsimpulse und Support bieten. Doch die Ausführung findet „vor Ort“ statt und dazu ist eine Autonomie erforderlich. Die Führung schafft den Rahmen und stellt die Ressourcen zusammen für eine wirksame Cyberdefense und bringt die Sicherheitsexperten mit internen und externen Partnern zusammen.

> Die Sicherheitsexperten müssen entscheiden, was zu tun ist. Die Führungsetage muss alles im Blick haben und im richtigen Moment Ressourcen, Steuerungsimpulse und Support bieten.

4 Globale Spaltung und digitale Irreführung: Die zwei Gesichter von Hacktivismus und Cybercrime

Zur angespannten Cybercrime-Lage tragen nicht nur Kriminelle bei, die zu ihrem eigenen finanziellen und persönlichen Vorteil handeln. Die wachsenden politischen und gesellschaftlichen Spannungen befeuern ein weiteres gefährliches Element im Cybercrime-Labyrinth: **Hacktivismus**. Angetrieben durch den Wunsch, ihren Unmut oder ihre Unterstützung zu Themen wie bewaffnete Konflikte oder soziale Ungerechtigkeit kundzutun, **nutzen Hacktivisten gezielt Schwachstellen und Sicherheitslücken aus** – und die Lage verschärft sich dadurch immer weiter.

Dem jüngsten Bericht von Motorola zufolge nahm Hacktivismus im dritten Quartal 2023 um 27 Prozent zu.[1] Ein Beispiel dafür ist die pro-russische Hacktivisten-Gruppe **DDoSia**, die für ihre Cyberangriffe gegen die westliche Welt bekannt ist. Die Gruppierung erlebte 2023 rasantes Wachstum – ihre Anhängerschaft wuchs um 2.400 Prozent und den Telegram-Kanal haben inzwischen 45.000 Menschen abonniert.[2]

Der inzwischen zweijährige Konflikt zwischen Russland und der Ukraine verdeutlicht, dass Konflikte in der modernen Zeit als **hybride Kriege sowohl in der realen als auch in der digitalen Arena** ausgefochten werden. Dabei nutzen Hacktivisten wie auch staatlich induzierte Gruppen **Cyberangriffe** als **schärfstes Tool der modernen Kriegsführung**. Ein Paradebeispiel dafür ist der Angriff der ukrainischen Gruppe Cyber. Anarchy.Squad gegen Infotel JSC, einen großen russischen Telekommunikationsanbieter, der den Betrieb der wichtigsten russischen Banken und Finanzinstitutionen gewährleistet.[3] Infolge des Angriffs wurden zahlreiche Bankensysteme Russlands unterbrochen und konnten stundenlang keine Online-Zahlungen verarbeiten.

Auch der Konflikt zwischen Israel und Gaza verdeutlicht die große Tragweite des Hacktivismus. Kurz nach Beginn des Konflikts führten Anonymous Sudan ihren ersten Cyberangriff gegen das Notfall-Warnsystem Israels aus.[4] Dabei drohten sie die Deaktivierung von Anwendungen an, die die Zivilbevölkerung vor Raketenangriffen warnten. Fast zur gleichen Zeit versuchte Killnet, mehrere israelische Regierungswebseiten zu unterbrechen.

1 **Motorola Solutions (2023).** New Report Outlines Q3 2023 Cyber Threats to Public Safety.

2 **Bleeping Computer (2023).** Pro-Russia DDoSia hacktivist project sees 2,400% membership increase.

3 **Bleeping Computer (2023).** Ukrainian hackers take down service provider for Russian banks.

4 **Security Week (2023).** Hackers Join In on Israel-Hamas War With Disruptive Cyberattacks.

Als Vergeltungsmaßnahme für diese und andere Angriffe stellte sich die in Indien ansässige Hacktivisten-Gruppe Indian Cyber Force hinter Israel und brachte die Webseiten der Hamas, Palestine National Bank, Palestine Web Mail Government Services und Palestine Telecommunications Company zum Einsturz.[5]

Doch Hacktivismus ist nicht nur bei bewaffneten Konflikten oder politischen Anspannungen zu beobachten; er reicht bis in den **sozialen Aktivismus**. Ein Beispiel dafür war der Cyberangriff von Anonymous Sudan auf Scandinavian Airlines Anfang dieses Jahres.[6] Dieser Angriff war die Reaktion auf die öffentliche Verbrennung des Korans durch eine rechtsnationalistische Gruppierung vor der türkischen Botschaft in Stockholm. Die Folge des Angriffs waren massive Probleme in den Online-Systemen der Airline, durch die Passagierdaten, wie Kontaktinformationen, Details vergangener und künftiger Flüge und Teile der Kreditkartennummern, freigelegt wurden.

Später im Jahr 2023 bekannte sich die VulzSec-Hackergruppe zum Diebstahl und der Veröffentlichung sensibler Daten der französischen Polizei als Gegenschlag infolge von polizeilichen Übergriffen.[7] Dabei wurden 7.092 Datensätze und die Profile von 30 Polizeibeamten veröffentlicht. Dieser Zwischenfall spiegelt einen größeren Trend wider; die Zunahme von Cyberangriffen gegen die Strafverfolgung um 28 Prozent, zu der der Hacktivismus maßgeblich beigetragen hat.[8]

Wichtig ist zu unterscheiden, dass für Hacktivisten nicht der finanzielle Aspekt im Vordergrund steht. Vielmehr werden sie durch ihre Überzeugungen angetrieben. Es gibt jedoch auch Cyberkriminelle, die versuchen, persönlichen Nutzen aus sozialer Instabilität zu ziehen. Inspiriert durch die im Russland-Ukraine-Konflikt genutzten Strategien, schießen nun gefälschte Charity-Webseiten aus dem Boden, die die Hilfsbereitschaft der Menschen während der Gaza-Krise ausnutzen.[9] Und es geht noch weiter. Wie aus der WildCard-Hacker-Kampagne hervorging, sind auch staatliche finanzierte Cyberkriminelle involviert, die mit ausgeklügelter Malware wie „SysJoker“ auf israelische Einrichtungen abzielen.[10] Für die Opfer wird es zunehmend schwieriger festzustellen, aus welcher Ecke ein Angriff stammt. Gleichzeitig wird die Cyber-Bedrohungslage stets komplexer mit vielen verschiedenen Akteuren, von denen jeder seine eigene Agenda verfolgt.

↗ **28 %**

Zunahme von Cyberangriffen gegen die Strafverfolgung, zu der **Hacktivismus** maßgeblich beigetragen hat.

Quelle: Motorola Solutions[8]

Während die politische Lage weltweit angespannt bleibt, kann für 2024 geradezu sicher davon ausgegangen werden, dass der Hacktivismus weiter zunimmt. Hacktivisten tragen genauso wie Cyberkriminelle dazu bei, dass die digitale Welt immer mehr ins Wanken gerät. Sie agieren in einer Art gegensätzlicher Synergie, wobei eine Partei die von der anderen Partei bloßgelegten Schwachstellen für ihre eigenen Zwecke ausnutzt. Dieses Zusammenspiel kreiert ein dynamisches Netz aus Cyberbedrohungen, die ebenso komplex wie unvorhersehbar sind.

5 **CSO (2023).** Israel-Hamas conflict extends to cyberspace.

6 **CSO (2023).** Hackerangriff auf Scandinavian Airlines.

7 **The Cyber Express (2023).** Cyber Attack on French National Police: VulzSec Hacking Group Claims to Leak Sensitive Data.

8 **Motorola Solutions (2023).** New Report Outlines Q3 2023 Cyber Threats to Public Safety.

9 **IT Daily (2023).** Israel-Hamas-Konflikt: Cyberkriminelle verbreiten gefälschte Spendenaufrufe.

10 **Cyberscoop (2023).** Shadowy hacking group targeting Israel shows outsized capabilities.

CHECKLISTE

So reduzieren Sie Ihr Risiko

Erstellen Sie redundante Netzwerkinfrastrukturen: Mittels mehrerer Datenpfade werden Ihre Dienste selbst bei einem DDoS-Angriff nicht unterbrochen. Dazu gehören zusätzliche Server, alternative Datenzentren sowie Cloud-Dienste. Ist ein Pfad kompromittiert oder überlastet, kann der Datenverkehr auf einen anderen Pfad umgeleitet und Dienstunterbrechungen vermieden werden.

Führen Sie regelmäßig Stresstests durch: Führen Sie Stresstests in Ihrer Infrastruktur durch, um zu überprüfen, wie sie auf hohen Datenverkehr reagiert. Wertvolle Einblicke verschaffen auch Red Team Exercises mit Simulationen realistischer Angriffsszenarien.

Nutzen Sie Ratenbegrenzung, Scrubbing-Services und Bandbreiten-Überversorgung: Diese Strategien ermöglichen Ihnen, die auf einem Server eingehende Datenmenge zu kontrollieren, schädlichen Traffic herauszufiltern und eine höhere Bandbreitenkapazität beizubehalten, um plötzliche Datenverkehrsspitzen zu bewältigen.

Regelmäßige Back-ups und externe Datenspeicher: Erstellen Sie regelmäßig Back-ups kritischer Daten und speichern Sie sie extern oder auf einer Cloud-Plattform. So vermeiden Sie, bei einem erfolgreichen Hackerangriff sämtliche Daten zu verlieren. Es ist ratsam, unveränderliche Back-ups zu erstellen und die 3-2-1-Back-up-Regel zu befolgen: Die Daten werden dreimal kopiert – zwei Kopien werden für den einfachen Zugriff lokal auf verschiedenen Geräten gesichert und eine weitere Kopie wird für zusätzliche Sicherheit extern gespeichert.

Nutzen Sie Netzwerksegmentierung: Segmentieren Sie Ihr Netzwerk, um die Ausbreitung von Malware einzuschränken. Im Ernstfall werden dann nur einzelne Segmente und nicht gleich das gesamte Netzwerk infiziert. Ratsam ist auch Mikrosegmentierung für eine erhöhte Granularität der Filterung und besseren Schutz sensibler Daten innerhalb der Segmente.

CHECKLISTE

So reduzieren Sie Ihr Risiko

Schränken Sie Nutzerrechte ein: Implementieren Sie das Least-Privilege-Prinzip, das jedem User nur die für seine Aufgaben notwendigen Zugriffsrechte gewährt. Dieser Ansatz ist ein zentraler Bestandteil der Zero-Trust-Netzwerkarchitektur zur Risikoverringerung interner Bedrohungen. Die Zugriffsrechte sollten zudem regelmäßig überprüft und aktualisiert werden.

Nutzen Sie eine Web Application Firewall (WAF): Eine WAF dient zur Überwachung des Datenverkehrs von Webanwendungen und hilft, nicht genehmigte Änderungen an Webseiten zu verhindern. Webanwendungs-Firewalls ermöglichen Integrationen mit anderen Sicherheitstools und die Einrichtung zentraler Threat-Management-Systeme. Wählen Sie gegebenenfalls eine erweiterte WAF, die Machine-Learning umfasst und sich dynamisch an neue Cyberbedrohungen anpasst.

Implementieren Sie sichere Authentifizierungs-methoden: Setzen Sie sichere Passwortrichtlinien um und schaffen Sie einen zusätzlichen Schutzwall durch Multi-Faktor-Authentifizierung (MFA), insbesondere beim Zugriff auf sensible Systeme und das Backend von Webseiten. Um die Sicherheit noch weiter zu erhöhen, nutzen Sie passwortlose und biometrische Authentifizierungsverfahren.

Überwachungs- und Warnsysteme: Nutzen Sie Tools zur Überwachung von Netzwerk-Traffic, Systemleistung und Zugriffsprotokollen. SIEM-Systeme (Security Information und Event Management) und SOAR-Systeme (Security Orchestration, Automation, Response) ermöglichen umfassende Überwachung, Analysen und automatisierte Reaktionen. Indem Sie Warnhinweise für auffällige Aktivitäten oder Veränderungen aktivieren, kann das Sicherheitsteam bei einem potenziellen Sicherheitsvorfall schneller reagieren.

5 Disinformation-as-a-Service: Ein gefährliches Instrument im Cybercrime-Arsenal

Seit dem Cambridge-Analytica-Skandal trugen Fehlinformations-Kampagnen massiv zur sozialen Polarisierung bei. Immer häufiger **verbreiten kriminelle Akteure gezielt falsche Informationen**. Das Ziel: Die Manipulation der öffentlichen Meinung, Rufschädigung oder die Einflussnahme auf geschäftliche und politische Entscheidungen.[1] 2023 nahmen Desinformations-Kampagnen jedoch ein neues Ausmaß an. In der **Ära der generativen KI** ist das Erstellen manipulativer Inhalte heute kostengünstiger und einfacher denn je, was es **nahezu unmöglich macht, wahre von erfundenen Geschichten zu unterscheiden**.

Ein Paradebeispiel für den Einfluss von Desinformations-Kampagnen sind die Präsidentschaftswahlen in den USA. Angetrieben durch rechtsextreme Aktivisten, Einmischungen aus dem Ausland und Fake-News-Webseiten breiteten sich während der Wahlen 2016 falsche Informationen in den sozialen Medien aus. Auch die Wahlen 2020 standen im Zeichen von Verschwörungstheorien und unbegründeten Wahlbetrugsvorwürfen, die Millionen von Menschen erreichten und eine antidemokratische Bewegung auslösten.[2] Im Vorfeld der Wahlen 2024 werden Bedenken laut, wie die neuesten Fortschritte in der KI möglicherweise für **noch ausgeklügeltere Fehlinformations-Kampagnen**, wie Deepfakes und gezielte Propaganda, missbraucht werden könnten.

Welche **möglichen Gefahren Deepfakes für die Demokratie bedeuten**, wurde schon bei der Parlamentswahl in der Slowakei deutlich, bei der ein KI-generiertes Deepfake-Audio Fehlinformationen in den sozialen Netzwerken verbreitete.[3] In dem Audio, das Tausende User erreichte, sprachen die bekannte Journalistin Monika Tódová und Michal Šimečka, der Vorsitzende der progressiven Partei, angeblich darüber, die Wahl zu manipulieren. Obwohl die Beteiligten sofort Einspruch gegen die Echtheit der Inhalte erhoben und mehrere Prüfeinrichtungen bestätigten, dass das Audio ein Fake war, erzielte es eine unglaubliche Reichweite, was vor allem dem Zeitpunkt der Veröffentlichung zu verdanken war. Da es während einer 48-stündigen Ruhephase vor den Wahlen veröffentlicht wurde, dauerte es einige Zeit, bis die Medien und Politiker es öffentlich anfechten konnten.

1 **The New York Times (2021).** Disinformation for Hire, a Shadow Industry, Is Quietly Booming.

2 **The Guardian (2023).** Disinformation reimagined: how AI could erode democracy in the 2024 US elections.

3 **Basecamp (2023).** Eine Herausforderung für Wahlen und Demokratie.

In diesem Zusammenhang bringt **Disinformation-as-a-Service (DaaS)** das Ausmaß und die Ausgereiftheit von Fehlinformations-Angriffen auf ein neues Niveau. Diese **neue Art von Informationskrieg** macht für Einzelpersonen und Organisationen den Kauf und die Verbreitung von Fake-News und Desinformations-Kampagnen einfacher als je zuvor. Angetrieben durch den schnellen Fortschritt generativer KI und ein Netzwerk aus professionellen Trolls, Bots und modernen Online-Bearbeitungstools machte DaaS Desinformations-Kampagnen für alle zugänglich – eine Entwicklung, die Cyberkriminelle und Hacktivisten zweifellos zu ihrem Vorteil nutzen werden.[4]

Das Fazit: **2024 müssen wir mit einem Anstieg politisch und finanziell motivierter Fehlinformations-Kampagnen rechnen**. Davon werden die verschiedensten Branchen betroffen sein, wie das Gesundheits- und Finanzwesen, Technologie, Bildung und Medien. Hinzu kommt, dass Hacktivisten und staatlich gestützte Cyberkriminelle weiterhin mittels Desinformation versuchen werden, Regierungen und politische Organisationen ins Wanken zu bringen, mit dem Ziel, die öffentliche Meinung zu beeinflussen und Unterstützung für ihre Sache zu gewinnen. Ein Beispiel dafür war 2023 die Verbreitung eines Deepfake-Bildes, das Fans von Atlético de Madrid mit einer palästinensischen Flagge zeigte.[5] Dieses irreführende Bild erlangte im Internet große Aufmerksamkeit. Solche Angriffe können sogar den **Aktienmarkt** beeinflussen und somit weitreichende wirtschaftliche Auswirkungen haben. Im Mai 2023 war dies der Fall, als ein gefaktes Bild einer Explosion in der Nähe des Pentagons in den sozialen Medien geteilt und von verschiedenen Medien, darunter auch der staatlichen russischen Nachrichtenagentur RT, verbreitet wurde. Das Foto löste Angst aus, die die Aktienmärkte kurzzeitig absacken ließ.[6]

Dem gegenüber stehen finanziell motivierte Cyberkriminelle, die alles daran setzen werden, Organisationen und Unternehmen zu destabilisieren. Mittels DaaS **setzen sie Fehlinformationen in ausgeklügelten Phishing- und Social-Engineering-Angriffen ein** und üben durch besorgniserregende Meldungen Angst und Druck auf Einzelpersonen aus. Doch das ist noch nicht alles; Fehlinformationen können auch den **Ruf von Organisationen langfristig beschädigen**.[7] So erging es beispielsweise Wayfair, als mit der QAnon-Gruppe verbundene Verschwörungstheoretiker die Verwirrung während der Pandemie ausnutzten, um den Ruf des E-Commerce-Versandhauses zu trüben. Unter anderem auf Twitter, Instagram und Reddit verbreiteten sie die Behauptung, dass Wayfair in sexuellen Missbrauch von Kindern verwickelt sei. Obwohl sich das Unternehmen gegen die Anschuldigungen wehrte, kursierten sie weiter im Netz, was verdeutlicht, wie schädigend Fake-News für den Ruf von Organisationen sein können.

Aufgrund ihrer öffentlichen Sichtbarkeit sind auch CEOs ein beliebtes Ziel für Deepfake-Angriffe. Durch ihre regelmäßige Teilnahme an Earnings Calls, Aktionärsversammlungen und Fernsehinterviews ist es für Cyberkriminelle ein Leichtes, Audio- und Videomaterial zu sammeln. Und im Kapitel zur KI haben wir bereits gesehen, was Angreifende mit der Hilfe von KI aus solchen Inhalten fabrizieren können.

Während sich Fehlinformations-Kampagnen zuspitzen und die weltweite Informationsverbreitung bedrohen, werden Organisationen ihre möglichen Auswirkungen, wie hohe finanzielle Verluste und langfristige Rufschädigung, immer stärker bewusst. Während die Strategien der Cyberkriminellen immer ausgeklügelter und flächendeckender werden, sehen sich Organisationen gezwungen, solide Abwehrmaßnahmen zu entwickeln, um ihre Integrität zu schützen und das Vertrauen der Öffentlichkeit zu bewahren.

4 **Hackernoon (2022).** Disinformation-as-a-Service: Content Marketing's Evil Twin.

5 **Reuters (2023).** Fact Check: Image of Atletico Madrid fans holding giant Palestinian flag is fake.

6 **Heise (2023).** Viral auf Twitter: Fake-Foto von Rauch am Pentagon lässt Aktienkurse absacken.

7 **The Globe and Mail (2023).** Disinformation campaigns, including those using AI deepfakes, are creating risks for corporations.

CHECKLISTE

So reduzieren Sie Ihr Risiko

Bewerten Sie mögliche Bedrohungen: Es ist wichtig, dass Organisationen in regelmäßigen Abständen ihre Anfälligkeit für Desinformations-Kampagnen überprüfen. Ein solider Threat-Modeling-Ansatz ermöglicht nicht nur, die Wahrscheinlichkeit, sondern auch die möglichen Auswirkungen eines Angriffs zu analysieren. Auch Sentiment-Analysis- und Trend-Monitoring-Tools können für Organisationen nützlich sein, um die öffentliche Meinung und Trends zu analysieren und sich so effektiv auf potenzielle Fehlinformations-Angriffe vorzubereiten.

Trainieren und sensibilisieren Sie Ihre Mitarbeitenden: Klären Sie Ihre Mitarbeitenden über die Funktionsweise von Fehlinformations-Kampagnen und damit verbundene Folgen für die Organisation auf. Verdeutlichen Sie die Wichtigkeit, Inhalte kritisch zu hinterfragen, und zeigen Sie auf, wie sie Informationen auf ihre Richtigkeit überprüfen und vertrauenswürdige Quellen erkennen können. Eine gesunde Skepsis und routinemäßige Überprüfungen können Ihre Organisation vor den Folgen irreführender Informationen schützen.

Optimieren Sie die interne Kommunikation: Stellen Sie sicher, dass interne Kommunikationskanäle eine schnelle Reaktion und Abwehr von Fehlinformationen ermöglichen. Mit der Hilfe von Kommunikationstools wie Sofie Rapid Awareness – die MS-Teams-Integration von SoSafe – können Sie Ihre Mitarbeitenden sofort informieren, wenn Fehlinformationen über Ihre Organisation in Umlauf sind.

Bilden Sie ein Krisenkommunikations-Team: Führen Sie ein Rapid-Response-Team ein, das sich auf Krisenkommunikation spezialisiert und Fake-Infos zeitnah mit faktenbasierten Gegenargumenten den Wind aus den Segeln nehmen kann.

CHECKLISTE

So reduzieren Sie Ihr Risiko

Fördern Sie Wachsamkeit und Reporting: Organisationen sollten eine Kultur der Wachsamkeit schaffen, in der Mitarbeitende jederzeit bereit sind, auffällige Online-Aktivitäten zu melden, wie irreführende Nachrichten, Deepfake-Bilder oder manipulierte Video- und Audioinhalte. Dazu gehört auch, dass Mitarbeitende das Vertrauen haben, dass sie beim Melden von Fehlinformationen nicht verurteilt werden. Zu diesem Zweck bieten sich benutzerfreundliche, anonyme Meldungssysteme an.

Automatisieren Sie die Überwachung von Social Media: Behalten Sie die sozialen Netzwerke im Auge, um Spuren von DaaS-Angriffen, Fake-News, manipulierten Fotos und manipulierten Audioclips festzustellen. Dazu ist eine enge Zusammenarbeit mit dem PR- und Marketingteam erforderlich. Es gibt bereits KI-getriebene Social-Media-Überwachungstools, die potenzielle Fehlinformationen in Echtzeit erkennen und melden und somit schnelles Eingreifen ermöglichen.

Betreiben Sie Informationsaustausch mit Dritten: Verknüpfen Sie sich mit externen Cybersicherheits-Netzwerken und bauen Sie Partnerschaften mit anderen Organisationen Ihrer Branche, Regierungseinrichtungen und globalen Allianzen für Cybersicherheit auf. So können Sie wertvolle Insights zu Fehlinformationstrends und Best Practices zum Schutz austauschen.

6 2024: Ein Jahr voller Herausforderungen für den öffentlichen Sektor und kritische Infrastrukturen

Dieses Jahr steht der öffentliche Sektor vor vielschichtigen Herausforderungen. Während öffentliche Einrichtungen beliebte Ziele für Hacktivisten sind, wird die Lage durch **staatlich finanzierte Cyberkriminelle und unabhängige Hackergruppen** zusätzlich verschärft. Das Ziel ist bei Angriffen auf öffentliche Einrichtungen oft die Zerstörung von Daten, Betriebsunterbrechungen, finanzieller Gewinn oder Spionage – alle mit weitreichenden Konsequenzen. Laut IBM-Bericht über die Kosten einer Datenschutzverletzung **belaufen sich die Kosten eines Cyberangriffs auf den öffentlichen Sektor auf schockierende 2,6 Millionen US-Dollar**.[1]

Die Digitalisierung sensibler Daten in öffentlichen Einrichtungen in Kombination mit oft kritischen Dienstleistungen machen den öffentlichen Sektor zu einer **attraktiven Zielscheibe für Cyberkriminelle**, die es auf Datendiebstahl und Betriebsunterbrechungen abgesehen haben. Im Jahr 2022 **stiegen Cyberangriffe durch nationalstaatliche Akteure, die speziell auf kritische Infrastrukturen abzielten, weltweit von 20 auf 40 Prozent an** – ein Wachstum, das größtenteils auf staatlich finanzierte Angriffe im Rahmen des Russland-Ukraine-Konflikts zurückzuführen ist.[2] Während der Ukraine-Konflikt wie auch der Israel-Gaza-Krieg weiter anhalten, ist für 2024 eine Fortsetzung dieses Trends zu erwarten.

> **Cyber ist ein geopolitisches Machtinstrument und gleichzeitig ein neuer Angriffsvektor geworden, den Staaten für Ihre Interessen einsetzen.**

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

Die immensen Mengen wertvoller Daten, die öffentliche Einrichtungen speichern, ist eine wahre Goldgrube für Kriminelle – das musste auch das Bildungswesen schmerzlich feststellen. Letztes Jahr beliefen sich die **Kosten einer erfolgreichen Datenschutzverletzung im Bildungssektor auf 3,65 Millionen US-Dollar**.[3] In einem Fall aus dem Jahr 2023 veröffentlichte die Hackergruppe Vice Society sensible Daten der Pates Grammar School in England, darunter Scans der Ausweise von Schülerinnen und Schüler, Lohntabellen der Lehrerschaft und Details aus Arbeitsverträgen.[4] Daraufhin folgten weitere Angriffe in ganz Europa.

1 **IBM (2023).** Bericht über die Kosten einer Datenschutzverletzung 2023.
2 **Microsoft (2022).** Digital Defense Report 2022.
3 **IBM (2023).** Bericht über die Kosten einer Datenschutzverletzung 2023.
4 **CSO (2023).** 14 britische Schulen von Cyberangriffen betroffen.

An Universitäten in Frankreich[5] und Deutschland[6] wurden interne Netzwerke und IT-Infrastrukturen lahmgelegt. Durch einen DDoS-Angriff auf die Online-Prüfungsplattform eines griechischen Gymnasiums konnten zeitweise keine Klausuren mehr geschrieben werden.[7]

Auch öffentliche Verwaltungseinrichtungen weltweit stehen durch den Anstieg an Cyberangriffen unter massivem Druck. Im Juli 2023 brach Kenias eCitizen-Portal nach einem Cyberangriff zusammen.[8] Die Unterbrechung der digitalen Plattform führte dazu, dass mehr als 5.000 Regierungsdienste unzugänglich waren. Menschen konnten nicht mehr auf ihre Reisepassanträge, Besuchervisas, Führerscheine, Personalausweise und Gesundheitsakten zugreifen. Auch Online-Banking- und Transportdienste waren zwischenzeitlich nicht verfügbar. Dieser Zwischenfall verdeutlicht, wie anfällig moderne Systeme aufgrund ihrer starken Vernetzung sind.

Und er zeigt noch etwas auf: In der komplexen geopolitischen Lage von heute können **Regierungsbehörden aller Ebenen** – ob Städte, Länder oder Bundesregierung – **Opfer von Cyberangriffen werden**. Und das mit verheerenden Folgen, die **nicht nur sensible Daten, sondern auch die öffentliche Sicherheit gefährden**. Doch die möglichen Auswirkungen gehen über die Unterbrechung von Diensten hinaus; werden kritische Infrastrukturen kompromittiert, kann es zu wirtschaftlicher Aufruhr und sogar zur Gefährdung von Menschenleben kommen. Hinzu kommen kostspielige und zeitintensive Wiederherstellungsprozesse, die öffentliche Budgets und das Vertrauen belasten.

5 **The Record (2023).** Aix-Marseille, France's largest university, hit by cyberattack.

6 **Rheinische Post (2022).** NRW-Städte fast täglich Ziel von Hackern.

7 **The Record (2023).** Cyberattack disrupts Greek national high school exams.

8 **Ntv (2023).** Afrikas erster Cyber-War.

Die erhöhte Angreifbarkeit zeigt sich vor allem bei öffentlichen Gesundheitseinrichtungen, in denen die Integrität und Verfügbarkeit von Daten kritisch sind. Der ENISA Threat Landscape: Health Sector Report zeigt, dass **knapp die Hälfte aller Ransomware-Angriffe auf öffentliche Gesundheitseinrichtungen Datendiebstahl und Datenlecks zur Folge haben**.[9] Ein drastisches Beispiel spielte sich im März letzten Jahres bei einem Ransomware-Angriff auf eines der größten Krankenhäuser Barcelonas ab.[10] Der Angriff zwang das Krankenhaus Clínic Barcelona, 150 nicht-dringende Operationen sowie 3.000 geplante Untersuchungen in drei Hauptzentren und mehreren externen Kliniken abzusagen.

Cyberangriffe auf Gesundheitseinrichtungen erlebten im vergangenen Jahr einen Anstieg. Im Dezember 2023 fiel die Katholische Hospitalvereinigung Ostwestfalen Ransomware zum Opfer, die Betriebsunterbrechungen in drei Krankenhäusern zur Folge hatte.[11] Zuvor war schon ein Krankenhaus in Brüssel von einem Cyberangriff getroffen worden, der dazu führte, dass Rettungswagen zu anderen Krankenhäusern umgeleitet werden mussten.[12] In diesem Fall waren die IT-Systeme dank des vorhandenen Notfallplans schon am nächsten Tag wieder voll funktionsfähig. **Solide Sicherheitsmaßnahmen und kurze Response-Zeiten sind im Ernstfall besonders wichtig**.

Leider ist eine **schnelle Wiederherstellung nach Cyberangriffen auf öffentliche Einrichtungen die Seltenheit** – die Hauptgründe sind **unzureichende Budgets, veraltete Technologien und unterbesetzte Teams**. Organisationen im öffentlichen Sektor verfügen meist nicht über die nötigen Ressourcen, um effektive Sicherheitsmaßnahmen einzurichten. Einem Bericht der ENISA zufolge verfügen nur 27 Prozent der Gesundheitseinrichtungen über ein Programm zum Schutz vor Ransomware und 40 Prozent haben kein Security Awareness-Programm für Mitarbeitende außerhalb der IT.[13] Um dem entgegenzuwirken, ist die **Einführung von präventiven Schutzmaßnahmen unerlässlich** – wie regelmäßige Security-Audits und eine Zero-Trust-Architektur. Zudem gilt es, die **Sicherheitskultur durch personalisiertes Awareness-Training zu stärken**, das auf die individuellen Anforderungen der jeweiligen Organisation abgestimmt ist. Da die Öffentlichkeit von diesen Einrichtungen abhängig ist, sind effektive Sicherheitsmaßnahmen nicht nur zu ihrem eigenen Schutz, sondern zum Schutze aller notwendig.

9 **ENISA (2023).** ENISA Threat Landscape: Health Sector.

10 **Heise (2023).** Ransomware-Angriff: Krankenhaus muss hunderte Operationen absagen.

11 **Heise (2023).** Cyberangriff auf Kliniken in Ostwestfalen.

12 **The Record (2023).** Hospital in Brussels latest victim in spate of European healthcare cyberattacks.

13 **ENISA (2023).** ENISA Threat Landscape: Health Sector.

CHECKLISTE

So reduzieren Sie Ihr Risiko

Analysieren und bewerten Sie Risiken: Machen Sie Risikoanalyse und -management zu einem zentralen Bestandteil des Geschäftsbetriebs. Sie können regelmäßig, wie zum Beispiel bei der Einführung neuer Technologien oder Planung von Geschäftsprozessen, durchgeführt werden. Risiko-Assessments sind zur Entwicklung von Security Baselines wichtig sowie zur Gewährleistung von Compliance und zum Erhalt der Datenintegrität.

Ernennen Sie eine Leitung für Digitalisierung: Öffentliche Einrichtungen sollten die Ernennung eines Chief Information Security Officer (CISO) in Betracht ziehen, der sich in allen Belangen der Digitalisierung auskennt. Diese Position ist beim Aufbau von Cyber Security-Strategien zentral.

Richten Sie eine Zero-Trust-Architektur (ZTA) ein: Dieses Framework setzt voraus, dass jede Zugriffsanfrage unabhängig ihres Ursprungs einer strengen Überprüfung unterzogen wird. Eine Zero-Trust-Architektur ist insbesondere im Hinblick auf die steigende Zahl an Cyberangriffen auf den öffentlichen Sektor essentiell.

Lernen Sie aus Vorfällen und ergreifen Sie Maßnahmen: Optimieren Sie Ihre Sicherheitsmanagement-Prozesse basierend auf dem Wissen aus vorherigen Sicherheitszwischenfällen. Zudem sollten Sie einen Incident Response Plan entwickeln und regelmäßig aktualisieren. Dieser Plan sollte alle Schritte enthalten, die bei einem Cyberangriff auszuführen sind, und so eine schnelle, effektive Response ermöglichen, die weitreichenden Schaden reduziert.

Führen Sie regelmäßige Schwachstellenbewertungen durch: Kontinuierliche, detaillierte Sicherheitsüberprüfungen helfen Ihnen, Schwachstellen im System aufzuspüren und mögliche Eintrittstore zeitnah zu schließen, bevor Cyberkriminelle sie ausnutzen können.

Führen Sie personalisierte Trainingsprogramme ein: Stellen Sie sicher, dass Mitarbeitende regelmäßige Schulungen zum Thema Cybersicherheit erhalten, die auf ihre speziellen Anforderungen und Aufgabenbereiche abgestimmt sind. Besonders relevant sind Trainingsmodule für das Gesundheitswesen, die auf die häufigsten Social-Engineering-Methoden eingehen. Auch die Phishing-Simulationen sollten auf den jeweiligen Sektor zugeschnitten sein.

INTERVIEW

John Noble

Nicht geschäftsführender Direktor und Vorsitzender des Cyber Security Committee bei NHS Digital, England

John Noble war von 2016 bis 2018 Director of Incident Management am britischen National Cyber Security Centre (NCSC), wo er die Response auf knapp 800 Sicherheitsvorfälle leitete und dazu beitrug, Großbritannien zum sichersten Standort für Onlinehandel zu machen. Derzeit ist er nicht geschäftsführender Direktor bei NHS Digital (National Health Service) und Vorsitzender des Information Assurance und Cyber Security Committee.

> Indem Regierungen auf internationaler Ebene Informationen austauschen und der private Sektor mit Regierungsbehörden zusammenarbeitet, erhalten wir ein präziseres Bild der Bedrohungslage.

Was ist das National Cyber Security Center (NCSC) und was ist seine Hauptfunktion?

Die Gründung des NCSC hatte einen politischen Hintergrund und wurde vom damaligen Premierminister Gordon Brown angestoßen. In Anbetracht der Entwicklung hin zu einer digitalen Gesellschaft, die im naturgemäß unsicheren Internet ansässig war, sah die Regierung die Notwendigkeit für eine Einrichtung mit beratender und unterstützender Funktion.

Wie kam es zu dem Beschluss, das NCSC an den Nachrichtendienst GCHQ anzuschließen?

Das NCSC an den britischen Nachrichtendienst Government Communications Headquarters (GCHQ) anzuschließen, war eine strategische Entscheidung. Durch seine Expertise in Network-Defense und als etablierte Cyber-Sicherheitsdienst schien es einfach ideal.

Was ist die Aufgabe des NCSC?

Am Anfang ging es darum, herauszufinden, auf welche Weise die Regierung ihren Beitrag leisten konnte und wie das Zentrum für Cybersicherheit dazu beisteuern konnte, Großbritannien zum sichersten Ort für Onlinehandel zu machen. Wir erkannten, dass der Erfahrungsaustausch zwischen Regierungen unumgänglich war und wir eine Partnerschaft zwischen den Regierungsbehörden und dem privaten Sektor aufbauen mussten.

Warum ist die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor in Cybersicherheitsbelangen so wichtig?

Regierungsbehörden haben ihre einzigartigen Stärken im Bereich Cyber Security; dasselbe gilt für den privaten Sektor. Deshalb analysiert das NCSC, wie von Regierungsseite eine Zusammenarbeit zwischen den beiden Sektoren ermöglicht werden kann. Infolgedessen entstanden zwei Initiativen: das Cyber Information Sharing Partnership (CISP), das Organisationen ermöglicht, Bedrohungsinformationen anonym in Echtzeit auszutauschen; und Cyber 100, eine Initiative, die Expertinnen und Experten aus dem privaten Sektor involviert, die ihr Wissen mit dem NCSC teilen.

Manche Organisationen haben Bedenken, ihre Schwachstellen öffentlichen Einrichtungen preiszugeben, da sie befürchten, die Informationen könnten gegen sie verwendet werden. Wie können wir kommunizieren, dass die Regierung Organisationen helfen und nicht schaden will?

Dabei spielen Vertrauen und Offenheit eine entscheidende Rolle. Entdeckt ein Nachrichtendienst eine Schwachstelle in einer Software und legt sie nicht offen, spielt das Cyberkriminellen in die Hände. Einrichtungen wie das NCSC müssen das Vertrauen der Unternehmen gewinnen, um Beweise für die Schwachstellen liefern zu können. Daraus können äußerst profitable und wichtige Beziehungen entstehen.

> **Die Regierung hat erkannt, dass der Schutz der Digitalwirtschaft – und der digitalen Unternehmen – höchste Priorität haben muss.**

Ich denke auch, dass die Regierung erkannt hat, dass der Schutz der Digitalwirtschaft – und der digitalen Unternehmen – höchste Priorität haben muss. Die Menschen müssen verstehen, dass wir die digitale Wirtschaft nur schützen können, wenn wir Informationen mit Regierungsbehörden teilen.

Welche großen Entwicklungen der Bedrohungslage konnten Sie in den letzten zehn Jahren beobachten?

Insbesondere im Cyberbereich hat sich die Bedrohungslage im letzten Jahrzehnt rasant gewandelt. Ein zentraler Aspekt ist die explosive Zunahme von Ransomware, die sich zu einem ausgeklügelten und hochspezialisierten Ökosystem entwickelt hat. Kriminelle Gruppen wie Conti haben inzwischen geschäftsähnliche Strukturen und Hierarchien mit verschiedenen Abteilungen und sogar Jobbezeichnungen. Auch wenn die Behörden einigen Organisationen das Handwerk legt, lernen die ihre Lektion, verbessern ihre Prozess und passen sie an.

Es gibt einen wachsenden Trend, bei dem Cyberkriminelle in Systeme eindringen, dann aber nichts weiter unternehmen. Wie lässt sich das erklären?

Sobald Cyberkriminelle eine Schwachstelle gefunden haben, infiltrieren sie das System und hinterlassen sogenannte Implantate in zahlreichen Unternehmen – mit dem Ziel, zu einem späteren Zeitpunkt wieder zurückzukommen. Davon sind auch kritische Infrastrukturen betroffen, bei denen es deshalb besonders wichtig ist, Schwachstellen zeitnah zu patchen.

Das Beheben von Schwachstellen ist im öffentlichen Sektor eine Herausforderung, da der Geschäftsbetrieb rund um die Uhr läuft. Können Sie darauf eingehen, wie der NHS dieses Problem angeht?

Der NHS hat aus Zwischenfällen wie WannaCry wichtige Lektionen gezogen. WannaCry nutzte eine bekannte Schwachstelle aus, die viele Krankenhausgruppen nicht behoben hatten. Dieser Zwischenfall traf die Krankenhäuser nicht nur finanziell, sondern beeinträchtigte auch die Patientenpflege.

Wenn es um Schwachstellen im Gesundheitswesen geht, wurden zwei wichtige Strategien implementiert. Die erste besteht darin, kritische Schwachstellen zu identifizieren, die aktiv ausgenutzt werden und dringendes Patching erfordern. Als Zweites werden klare verbindliche Normen etabliert, die die Einrichtungen einhalten müssen.

Wie wirkte sich die Zentralisierung der Gesundheitssysteme, wie beim britischen NHS, auf den Umgang mit Security-Herausforderungen aus?

Die Zentralisierung der Gesundheitssysteme hat sowohl positive als auch negative Auswirkungen auf die Security. Positiv ist, dass zentralisierte Systeme klarere Standards und Erwartungen mit sich bringen. Das erleichtert die Kommunikation und die Einführung von Sicherheitsmaßnahmen über Netzwerke hinweg. Durch den zentralisierten Ansatz konnte auch die Patientenversorgung verbessert und schneller auf Schwachstellen reagiert werden. Eine der Herausforderungen ist, dass bei einer Kompromittierung des Systems, automatisch auch andere Bereiche betroffen sein können – ein Ausfall in einem Bereich kann also weitreichendere Folgen für das gesamte System haben.

> Der Russland-Konflikt hat Hacktivismus auf beiden Seiten befeuert.

Wie beeinflusst die Geopolitik die Entwicklung der Cyber-Lage und die Interaktion zwischen Nationalstaaten und privaten Einrichtungen?

Bei der Analyse eines Angriffstrends müssen wir immer zwei Dinge berücksichtigen: die Absichten der Angreifenden und ihre Fähigkeiten. Der Einmarsch in die Ukraine hat zum Beispiel dazu geführt, dass Nationalstaaten Cyberangriffe zur Unterstützung ihrer Kriegsanstrengungen einsetzen. Und die Fähigkeiten, die nationalstaatliche Akteure entwickeln, werden letztlich auch gegen uns eingesetzt.

Wie ist es mit Hacktivismus?

Der Russland-Konflikt hat Hacktivismus auf beiden Seiten befeuert. Eine ukrainische Cyber-Armee führte Angriffe auf russische Unternehmen, Medienkonzerne usw. aus. Andererseits führten auch Gruppen wie KillNet, die sich stark mit Russlands Vorhaben identifizieren, DDoS-Angriffe aus und machten kein Geheimnis daraus, dass sie Länder ins Visier nehmen würden, die die Ukraine unterstützen.

Gibt es eine Grauzone, in der sich die kommerziell motivierte und die politisch motivierte Cyberkriminalität überschneiden?

Was Länder normalerweise davon abhält, Cybercrime für ihre Zwecke einzusetzen, sind die möglichen Konsequenzen und die Angst vor der Bloßstellung. In einer Situation wie dem Ukraine-Krieg spielt es für Staaten jedoch keine große Rolle, was andere über sie denken oder welche Konsequenzen ihr Handeln haben könnte.

Vorher waren wir in einer Situation, in der wir effektiv gegen Hackergruppen vorgehen konnten. Jetzt sieht die Sache so aus, dass diese Gruppen mit den Staaten gemeinsame Sache machen. In der obersten Riege der russischen Politik wird gerade sogar diskutiert, Cyberangriffe zu legitimieren. Dass ein Land kriminelle Handlungen gegen

andere legitimieren könnte, möchte man sich gar nicht vorstellen. Ich hoffe wirklich, dass es nicht so weit kommt.

Welche Strategien verfolgen Nationalstaaten in dieser Zusammenarbeit noch?

Für die Länger ist wichtig, dass sie ihre Beteiligung abstreiten und ihre Handlungen so verheimlichen können. Wir können beobachten, dass die Nationalstaaten dieselben Tools nutzen wie Cyberkriminelle, um ihre Beteiligung an den Angriffen abstreiten zu können. Wird zum Beispiel ein kommerziell erhältliches Implantat in einem Bereich einer kritischen nationalen Infrastruktur entdeckt, ist es sehr schwer festzustellen, ob ein nationalstaatlicher Akteur dahintersteckt oder nicht. Und der Staat selbst kann es einfach abstreiten. Tools wie die Implantate ermöglichen den Nationalstaaten mit Cyberkriminellen zusammenzuarbeiten.

Im Russland-Kontext hatten Sie von anderen Ländern gesprochen. Welche Staaten mischen sonst noch in der aktuellen Cyber-Bedrohungslage mit?

Wenn es um die größten strategischen Knackpunkte geht, müssen wir den wachsenden Einfluss Chinas erwähnen, die Spannungen im Südchinesischen Meer und Chinas Haltung gegenüber Taiwan und anderen Nachbarländern wie den Philippinen. China hat sich im Cyberbereich stark weiterentwickelt, was sich in der gesteigerten Raffinesse und im Einsatz neuer Zero-Day-Angriffsmethoden äußert. Es hat seine Geheimdienste reformiert, um Konflikte zu vermeiden, und geht heute viel professioneller vor. China hat auch seinen Interessenbereich erweitert. Grundsätzlich nehmen sie immer eine langfristige Perspektive ein und erweitern ihre Fähigkeiten mit der Zeit.

Europa und Großbritannien haben hingegen eine ähnliche Sicht auf Cyber. Wir haben erkannt, dass wir aus der reaktiven Position herauskommen und strategischer vorgehen müssen.

Mit welchen Schritten können wir das Cyberrisiko reduzieren, insbesondere wenn es um Advanced Persistent Threats (APT) geht?

Indem Regierungen auf internationaler Ebene Informationen austauschen und der private Sektor mit Regierungsbehörden zusammenarbeitet, erhalten wir ein präziseres Bild der Bedrohungslage. Durch den Austausch von Kompromittierungsindikatoren (IOC) und den Aufbau eines Vertrauensverhältnisses zwischen beiden Sektoren, können wir geschäftliche Bedenken überwinden – und den Weg für eine gemeinsame Front im Kampf gegen neue Cyber-Bedrohungen ebnen.

Fanden Sie das Interview aufschlussreich?

Hören Sie sich die vollständige Fassung in unserem Human Firewall Podcast an. Tauchen Sie in das Gespräch zwischen SoSafe CEO Dr. Niklas Hellemann und John Noble ein und erhalten Sie noch mehr wertvolle Einblicke in die Bedeutung internationaler Kooperation für die Cybersicherheit.

7 Pretexting und Multichannel-Strategien machen Cyberangriffe noch überzeugender und gefährlicher

Ausgefeilte Social-Engineering-Methoden wie **Pretexting** werden bei Cyberkriminellen immer beliebter. Beim Pretexting geben sich die Angreifenden als Vertrauensperson des Opfers aus und führen es mit einer überzeugenden Geschichte hinters Licht, um finanzielle Ziele zu erreichen oder an sensible Daten zu gelangen. Laut einem Bericht von Verizon von 2023 **macht Pretexting mehr als 50 Prozent aller Social-Engineering-Angriffe aus**.[1] Das zeigt, dass der Faktor Mensch weiterhin im Fokus der Cyberkriminellen steht, die darauf abzielen, einzelne Personen gekonnt zu täuschen und zu manipulieren.

Bei besonders ausgeklügelten Formen von Pretexting **spionieren die Cyberkriminellen ihr Opfer zunächst über mehrere Kanäle**, wie die sozialen Medien, Blogs oder Webseiten, aus, um möglichst viele Informationen über ihre Zielperson zu sammeln. Um ihre Geschichte überzeugender zu gestalten und das Vertrauen ihres Opfers zu gewinnen, lassen sie gesammelte Informationen, wie zum Arbeitsplatz, Sozialleben, Haustier oder Partner der Zielperson, in die Geschichte einfließen.[2]

Die Kanäle, über die die Angreifenden an die Informationen gelangen, dienen dabei gleichzeitig auch als Angriffsvektoren. Wie aus unserem Human Risk Review 2023 hervorgeht, steht Phishing per E-Mail weiterhin an der Spitze; davon waren 61 Prozent aller Organisationen schon einmal betroffen.[3] Die Angriffe weiten sich jedoch auf andere Kanäle aus, so erfolgen 34 Prozent inzwischen über Social Media. Für viele Kleinunternehmen sind die sozialen Medien ein wichtiger, wenn nicht sogar der einzige Verkaufskanal. Das machen sich Hacker zunutze, indem sie die Kontrolle über ihre Accounts übernehmen und sie erpressen. So erging es einem kleinen Unternehmen, das Müsli über Instagram verkaufte.[4] Die Angreifenden nahmen auf Instagram Kontakt zur Geschäftsinhaberin auf und gaben sich als ein Unternehmen aus, dem sie vertraute. Mit der Bitte, in einem Wettbewerb für sie zu stimmen, forderten sie sie auf, auf einen Link zu klicken. Die Angreifenden übernahmen die Kontrolle über ihr Instagram-Konto und forderten 10.000 US-Dollar von ihr, die sie bezahlte, um wieder die Kontrolle über ihr Geschäft zu übernehmen. Das ist nur eine Art, wie Cyberkriminelle soziale Plattformen ausnutzen. In anderen Fällen übernehmen sie die

1 **Verizon (2023).** Data Breach Investigation Report.

2 **Security Insider (2022).** 4 Social Engineering Tricks der Hacker.

3 **SoSafe (2023).** Human Risk Review.

4 **Security Insider (2020).** Social Media wird für Phishing-Angriffe missbraucht.

Kontrolle über Mitarbeiterkonten, um von Teamkollegen sensible Informationen abzufragen oder sie dazu zu bringen, schädliche Anhänge, die als legitime Geschäftsdokumente getarnt sind, herunterzuladen.

Auch Messaging-Apps wie WhatsApp und Microsoft Teams gehören zu den Lieblingskanälen Cyberkrimineller, und zwar im privaten wie im beruflichen Umfeld. Vor Kurzem warnte die Polizei von Kalkutta in Indien vor einer Reihe von WhatsApp-Angriffen.[5] Dabei verschickten die Angreifenden Nachrichten zum Weltyogatag als Pretext und boten darin Yogakurse an. Um das Angebot anzunehmen, mussten die User auf einen Link klicken und einen sechsstelligen OTP-Code eingeben. So verschafften sie den Angreifenden unwissentlich Zugriff auf Ihr WhatsApp-Konto. Danach schickten die Cyberkriminellen Nachrichten an die Kontakte der Zielperson, unter Vorgabe eines dringenden Grundes nach Geld fragten. Bei einem anderen Angriff verschickten kriminelle Akteure Nachrichten über die professionelle Kommunikationsapp Microsoft Teams, gaben sich als Mitarbeiter des HR-Teams aus und informierten ihre Opfer über angebliche Änderungen bei ihren Urlaubstagen.[6] Sie forderten die Zielpersonen auf, dringend den vermeintlichen Urlaubsplan herunterzuladen, der stattdessen Malware namens DarkGate enthielt.

Doch damit nicht genug. Cyberkriminelle verfeinern ihre Methoden immer weiter, um noch überzeugender zu sein. Bei **extrem ausgeklügelten Angriffen nehmen sie sogar über mehrere Kanäle Kontakt zu ihrem Opfer auf**, wie per SMS, E-Mail und Telefon. In einem Fall kombinierten die Angreifenden SMS mit Voice-Phishing: Zunächst schickten sie ihrem Opfer eine SMS, in der sie fragten, ob sie eine Überweisung von 7.500 Dollar genehmigt habe. Kurz danach machten sie sich die Angst der Frau zunutze. Sie riefen sie an, gaben sich als Betrugsermittler aus und forderten die Frau auf, ihre Zugangsdaten zu ändern, damit die Hacker nicht an ihr Geld gelangen konnten. Insgesamt stahlen sie 15.000 US-Dollar von zwei Bankkonten.[7]

Solche Multichannel-Angriffe werden noch überzeugender, wenn KI im Einsatz ist. Ein schonungsloses Beispiel dafür erlebte ein Mitarbeiter von Retool.[8] Die Angreifenden begannen mit einer SMS, in der sie sich als Mitglied des IT-Teams ausgaben und ein Problem bei der Gehaltsabrechnung als Vorwand nannten. Daraufhin gab der Mitarbeitende seine Zugangsdaten auf einer gefakten Landingpage ein. Da er jedoch MFA aktiviert hatte, riefen die Cyberkriminellen ihr Opfer im zweiten Schritt an und nutzen dafür die mittels KI geklonte Stimme eines IT-Mitarbeiters, um den einmaligen Bestätigungscode abzufragen. So verschafften sie sich Zugriff auf 27 Kundenkonten und stahlen Kryptowährung im Wert von tausenden von Dollar.

Während die Methoden Cyberkrimineller immer ausgeklügelter und professioneller werden, müssen wir **in Zukunft noch wachsamer sein und sichere Verhaltensweisen verinnerlichen**.

5 **The Times of India (2023).** Police warns netizens about WhatsApp hacking, here's how fraudsters hack accounts.

6 **Chip (2023).** Hacker nutzen Datenleck: Malware verbreitet sich über Skype- und Teams-Konten.

7 **The Guardian (2023).** Gone in seconds: rising text message scams are draining US bank accounts.

8 **The Hackers News (2023).** Retool Falls Victim to SMS-Based Phishing Attack Affecting 27 Cloud Clients.

CHECKLISTE

So reduzieren Sie Ihr Risiko

- **Überprüfen Sie die Absender- und Anruferidentität:** Es ist wichtig, dass Ihre Mitarbeitenden wissen, wie sie die Identität von E-Mail-Absendern und Anrufern eigenständig überprüfen können. Es ist immer sicherer, die Person über einen vertrauenswürdigen Kommunikationskanal direkt zu kontaktieren, insbesondere wenn es um sensible oder verdächtige Anfragen geht.
- **Überprüfen Sie externe Parteien:** Ihre Wachsamkeit sollte sich über Ihre Mitarbeitenden hinweg auf alle Personen ausweiten, die mit Ihren Systemen interagieren. Wenn Sie mit externen Personen zu tun haben, die auf sensible Daten zugreifen müssen, stellen Sie sicher, dass sie die Cyber-Sicherheitsprotokolle Ihrer Organisation einhalten.
- **Fördern Sie schnelles und selbstbewusstes Reporting:** Bauen Sie in Ihrer Organisation eine starke Meldekultur auf, in der Mitarbeitende Phishing-Angriffe oder andere verdächtige Aktivitäten ohne Angst vor negativen Folgen sofort melden. Zeitnahes Reporting bietet Sicherheitsteams die Chance einzugreifen, bevor ein Angriff weitreichendere Folgen haben kann.
- **Aktualisieren Sie Sicherheitsrichtlinien:** Aktualisieren Sie Ihre Cyber-Security-Richtlinien regelmäßig, um sie an neue Social-Engineering-Taktiken wie Pretexting anzupassen. So bleibt Ihre Verteidigungskette stabil und auf dem neuesten Stand.
- **Optimieren Sie Reaktionspläne:** Um die möglichen Auswirkungen eines erfolgreichen Pretexting-Angriffs oder anderer Angriffstaktiken zu reduzieren, halten Sie Ihren Incident Response Plan aktuell. Klar definierte Vorgehensweisen zur Erkennung, Unterbrechung und Eindämmung der Folgen eines Cyberangriffs sind unerlässlich, um die Geschäftskontinuität und Sicherheit zu gewährleisten. Regelmäßige Tabletop-Exercises tragen außerdem zum Wissenserhalt bei.
- **Kontinuierliches Awareness-Training für Mitarbeitende:** Führen Sie regelmäßiges und kontinuierliches Awareness-Training zu den aktuellen Cyberbedrohungen, wie unter anderem Pretexting und Multichannel-Methoden, ein. Festigen Sie Erlerntes durch Simulationen mit realitätsnahen Szenarien. Das hilft Ihren Mitarbeitenden, verdächtige Aktivitäten zu erkennen und selbstbewusst darauf zu reagieren. Eine solche Weiterbildung ist unerlässlich, um Ihre Mitarbeitenden zu sensibilisieren und zur Erkennung und Abwehr von Betrugsmaschen zu befähigen.

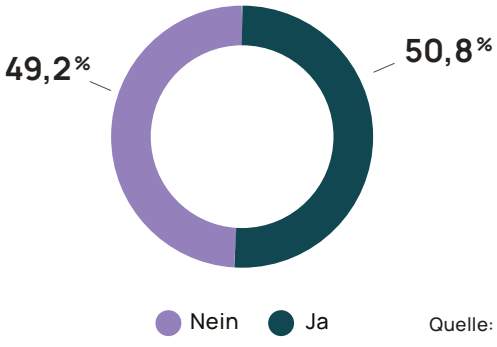
8 Steigende Burnout-Zahlen erhöhen den Druck auf Security-Teams wie nie zuvor

Schon letztes Jahr gingen wir in unserem Bericht auf die Problematik von Burnout in Security-Teams ein. Doch die globalen Spannungen und die Professionalisierung der Cyberkriminalität – zusätzlich befeuert durch KI – sorgen für noch komplexere Angriffe und erhöhen den Druck auf Sicherheitsbeauftragte zusätzlich. Die unnachgiebige Flut an Herausforderungen stellt die Resilienz und Anpassungsfähigkeit unserer Teams wie nie zuvor auf die Probe.

Ein Faktor, der den Druck weiter erhöht, ist der akute Fachkräftemangel in der Branche. Einem Bericht von ISC2 zufolge, gibt es weltweit 3,9 Millionen unbesetzte Positionen im Bereich Cybersicherheit.[1] Die Zahl ist 2023 im Vergleich zu 2022 somit um weitere 12,6 Prozent gestiegen, wobei der größte Anstieg im asiatisch-pazifischen Raum (vor allem Japan und Indien) und in Nordamerika zu beobachten war. Doch auch in Europa ist der Fachkräftemangel im Vergleich zum Vorjahr um 9,7 Prozent angestiegen. Und das ist noch nicht alles. Laut einer Studie von ISACA haben 59 Prozent aller Organisationen nicht genügend Cybersicherheits-Fachkräfte, was die Arbeitsbelastung der Teams dramatisch erhöht und **Sicherheitsbeauftragte nicht selten an die Schwelle des Burnouts oder bis zur Kündigung treibt**.[2]

Das bestätigte eine Umfrage unter tausenden Mitgliedern von Sicherheitsteams in den USA und Europa: **66 Prozent der Befragten berichteten von extremem Arbeitsstress**, 51 Prozent wurden Medikamente für die psychische Gesundheit verschrieben und 19 Prozent konsumieren als Bewältigungsmechanismus mehr als drei alkoholische Drinks am Tag.[3] Die Problematik erstreckt sich jedoch über die persönliche Belastung hinaus. Die erhöhte Belastung kann dazu führen, dass **Teams wichtige Details übersehen, dadurch nicht effektiv auf Bedrohungen reagieren können** und das Risiko für Cyberangriffe in der Organisation dadurch signifikant ansteigt. Weiter erhöht wird das Risiko durch die Tatsache, dass Cyberkriminelle ihre Methoden stetig verfeinern und optimieren, wie wir schon in vorherigen Kapiteln gesehen haben.

Wurden Ihnen schon einmal ärztlich Medikamente für die geistige Gesundheit verschrieben?



Quelle: Tines[3]

1 **ISC2 (2023).** How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce.

2 **ISACA (2023).** New ISACA Research: 59 Percent of Cybersecurity Teams are Understaffed.

3 **Tines (2022).** State of Mental Health in Cybersecurity.

Der Fall AccessPress veranschaulicht die enormen Herausforderungen von Security-Teams.[4] Der Anbieter von WordPress-Plug-ins wurde Opfer eines ausgeklügelten Cyberangriffs, bei dem Hacker 40 Themes und 53 Plug-ins kompromittierten, die auf über 360.000 aktiven Webseiten in Verwendung waren. Das verdeutlicht die mögliche Reichweite von Supply-Chain-Attacken im Softwarebereich. Dieser großflächige Angriff, der Cyberkriminellen Zugriff auf eine große Anzahl an Webseiten verschaffte, zeigt, welch wirksamen und komplexen Angriffstaktiken wir in der heutigen Cyber-Bedrohungslage gegenüberstehen. Dabei geht es nicht nur um technische Herausforderungen, sondern auch um das menschliche Element der Cyber Security – insbesondere die extreme Belastung der Sicherheitsteams.

Hinzu kommt, dass Sicherheitsteams nicht nur den Schutz anderer Abteilungen innerhalb der Organisation gewährleisten und schnell auf Angriffe reagieren müssen. Laut unserem Human Risk Review 2023 gehören sie zudem selbst zu den Abteilungen mit dem höchsten Angriffsrisiko.[5] Auch Cyberkriminelle sind sich der Schwächen gestresster Sicherheitsteams bewusst und nutzen Burnout als Angriffsvektor. Sie greifen gezielt Organisationen an, deren Sicherheitsteams eher schwach aufgestellt sind.

Dies unterstreicht, dass **Unternehmen unbedingt in ihre Security-Teams und das Wohlbefinden ihrer Mitarbeitenden investieren** sollten. Es ist wichtig, entsprechende Budgets zuzuweisen und Karrierepläne zur Bindung der Mitarbeitenden zu entwickeln, um Burnout vorzubeugen, Fachkräfte zu halten und über die nötigen Ressourcen für die richtigen Sicherheitsmaßnahmen zu verfügen. Nur wenn diese Schritte erfüllt werden, können Security-Teams effektiv arbeiten, Cyberangriffe bekämpfen und die Sicherheit stärken.

> **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 des CyberPeace Institute

4 **Heise (2022).** Vollzugriff durch Hintertür in WordPress-Erweiterungen.

5 **SoSafe (2023).** Human Risk Review.

CHECKLISTE

So reduzieren Sie Ihr Risiko

- **Machen Sie geistige Gesundheit und Work-Life-Balance zur Priorität:** Entwickeln Sie Programme zur Förderung des mentalen Wohlbefindens Ihres Sicherheitsteams. Flexible Arbeitszeiten, Zugang zu Beratungsdiensten und regelmäßige Pausen können dazu beitragen, Burnout vorzubeugen.
- **Nutzen Sie effektive Threat Detection-Tools:** Implementieren Sie moderne Tools, wie KI-getriebene Systeme zur Bedrohungserkennung und andere Instrumente, wie den Phishing-Meldebutton oder den E-Mail-Assistenten PhishFeedback von SoSafe. So können Bedrohungen leichter erkannt und Zeit gespart werden.
- **Automatisieren Sie die Analyse von E-Mails:** Führen Sie Automatisierungstools für Security Operations Center (SOC) ein, die gemeldete E-Mails analysieren. Dadurch wird die Auswertung potenziell gefährlicher E-Mails massiv beschleunigt, während SOC-Teammitglieder sich auf kritischere und komplexere Sicherheitsfragen fokussieren können.
- **Automatisieren Sie Routineaufgaben:** Indem Sie wiederholende Routineaufgaben automatisieren, ermöglichen Sie Security-Verantwortlichen, sich auf strategische Aspekte der Cybersicherheit zu konzentrieren.
- **Fördern Sie Training und Weiterbildung:** Befähigen Sie Ihr Team durch kontinuierliche Weiterbildungsprogramme, effektiv mit aktuellen Cyberbedrohungen und neuen Technologien umzugehen. Fördern Sie zudem die Zusammenarbeit mit anderen Tech-Teams und ernennen Sie Security-Champions.
- **Investieren Sie in die Bindung von Mitarbeitenden:** Durch Karrierepläne und Aufbauprogramme stärken Sie die Bindung von Fachkräften und reduzieren Mitarbeiterwechsel.
- **Regelmäßige Feedback- und Lagegespräche:** Organisieren Sie regelmäßig persönliche Treffen zum Austausch von Feedback. So kennen Sie die Bedürfnisse Ihrer Mitarbeitenden und können gezielt darauf eingehen.

2024 rückt **der Faktor Mensch** bei Cyberangriffen weiter in den Fokus

Alle Trends des Jahres laufen auf ein gemeinsames Fazit hinaus: **Unsere Sicherheitsmaßnahmen werden erst dann wirklich wirksam, wenn wir uns – genau wie die Cyberkriminellen – auf den Faktor Mensch fokussieren**. Kriminelle Akteure wissen nur zu gut, dass sie durch das Spiel mit den menschlichen Emotionen ihre Erfolgschancen maximieren. Deshalb bildet Social Engineering auch den gemeinsamen Nenner aller Angriffstaktiken, wie in diesem Report mehrfach deutlich wurde.

Schätzungen im Data Breach Investigations Report von Verizon zufolge spielte der Faktor Mensch 2023 in bis zu 74 Prozent aller Datenschutzverletzungen eine Rolle; und sogar Tech-orientierte Branchengruppen erkennen inzwischen das menschliche Element bei der Ausbeutung von Technologie an.[1] Doch das ist erst die Spitze des Eisbergs. Dem Forrester-Report „Prognosen 2024“ zufolge, wird **im Jahr 2024 der Anteil an Datenschutzverstößen, an denen der Faktor Mensch beteiligt ist, noch weiter ansteigen**.[2] Die Professionalisierung der Cyberkriminalität und der Aufstieg der Künstlichen Intelligenz ermöglichen Cyberkriminellen, komplexe Social-Engineering-Angriffe überzeugend und erschreckend realitätsnah aufzusetzen. Zwischen echten und trügerischen Nachrichten zu unterscheiden, wird in Zukunft deutlich schwerer, während sich die Bedrohungen über immer mehr digitale Kommunikationskanäle schneller verbreiten denn je.

Auch der Allianz Risk Barometer 2024 schätzt Cybervorfälle als größtes Geschäftsrisiko für 2024 ein – für Security-Verantwortliche führt kein Weg mehr daran vorbei, den Faktor Mensch in ihren Sicherheitsstrategien ernstzunehmen.[3] Die gute Nachricht ist, dass es eine mächtige Gegenmaßnahme gibt: **Cyber Security Awareness und Training**. Indem wir die Menschen mit dem Thema Cybersicherheit dort abholen, wo sie stehen, und sichere Verhaltensweisen verinnerlichen, können wir uns Cyberbedrohungen effektiv entgegensetzen. Eines dürfen wir nie vergessen: Nicht Systeme, sondern Menschen sind die Zielscheibe von Cyberangriffen; und sie sind es auch, die die Last der angespannten Bedrohungslage auf ihren Schultern tragen. Deshalb können **Angriffe nur von Menschen effektiv abgewehrt werden**. Eine starke Sicherheitskultur ist nicht nur die Verantwortung der Organisation, sondern die eines jeden Einzelnen. Gemeinsam können wir den drohenden Schatten der Cyberkriminalität aufhalten und eine sicherere Zukunft schaffen.

1 **Verizon (2023).** Data Breach Investigations Report.

2 **Forrester (2024).** Prognosen 2024: Fortschritt durch neue Entdeckungen.

3 **Allianz (2024).** Allianz Risk Barometer: Die wichtigsten Geschäftsrisiken 2024.

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 Prozent DSGVO-konform

CONNECT — Sofie Rapid Awareness

Cyberkriminelle entwickeln ihre Methoden schneller weiter als je zuvor, aber Sie können das auch. Rapid Awareness ermöglicht es Ihnen, Ihre Mitarbeitenden schnell und einfach in MS Teams zu erreichen. Halten Sie durch effektives Micro-Learning mit Cyberbedrohungen Schritt, versorgen Sie Ihr Team mit Alerts zu den neuesten Angriffsmaschen und machen Sie Ihre Mitarbeitenden zu Ihrer stärksten Verteidigungslinie.

- Erreichen Sie Ihre Mitarbeitenden direkt in MS Teams
- Sparen Sie Zeit und kommunizieren Sie mit Leichtigkeit
- Senden Sie kurze und leicht verständliche Alerts an Ihre Mitarbeitenden
- Verfolgen Sie, wie viele Mitarbeitende die Alerts gesehen haben

Human Firewall Conference

HuFiCon ist eine Cyber-Security-Konferenz, die Sicherheitsverantwortlichen hilft, ihre Teams in **Cyber-Heroes** zu verwandeln. Erleben Sie Expertenvorträge und praxisnahe Workshops und tragen Sie als Teil einer Community dazu bei, dass der Faktor Mensch in der Cybersecurity die Aufmerksamkeit erhält, die er verdient.

Werden Sie die Zukunft der Cybersicherheit mitgestalten?

Zur HuFiCon24 anmelden

Wo? @Halle Tor 2, Köln

Wann? 14.-15. November 2024

Kontakt

Bei weiterführenden Fragen zu diesem Report wenden Sie sich bitte an:

Laura Hartmann
Head of Corporate Communications
press@sosafe.de

SoSafe GmbH
Lichtstraße 25a
50825 Köln

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