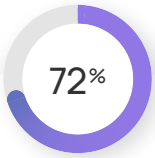
Cybercrime-Trends 2025

sosafe

Inhalt

Executive Summary

Die Reichweite der Cybercrime-Branche hat einen neuen Höhepunkt erreicht



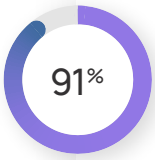
aller Organisationen weltweit berichten vom **steigenden Cyberrisiko**.[1]

Der **Schaden durch Cybercrime**[2] betrug 2024 allein in Deutschland

178,6 Mrd. Euro

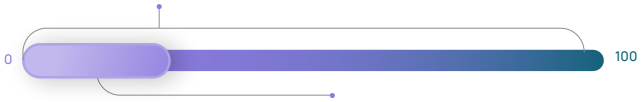
Das sind **20%** mehr als im Vorjahr.

Cyberkriminelle hängen Organisationen bei der Nutzung von KI ab ...



der Sicherheitsbeauftragten weltweit erwarten in den nächsten drei Jahren einen **deutlichen Anstieg** KI-getriebener Angriffe.

Und obwohl sich **96%** der Sicherheitsexperten einig sind, dass es wichtig ist, KI-basierte Angriffe zu erkennen, ...



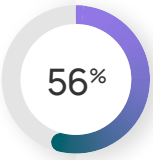
... schätzen nur **26%** ihre eigene Fähigkeit diesbezüglich als hoch ein.

... doch in den richtigen Händen wird KI zum wertvollen Verbündeten

> Wir sollten KI nicht nur nutzen, um ihre eigenen Risiken zu reduzieren. Wenn wir KI gezielt trainieren, um praktisch jedes Szenario durchzuspielen, was passieren kann, dann können wir darauf auch besser reagieren.

Frank Schätzing
Science-Fiction-Bestsellerautor

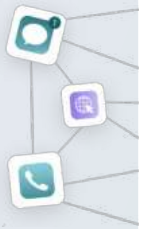
Angreifende nutzen jeden verfügbaren Kanal als mögliches Eintrittstor



der Sicherheitsbeauftragten in der DACH-Region zufolge ist **E-Mail** immer noch der primäre Angriffskanal.

98%

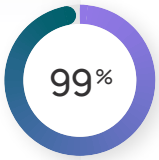
der Organisationen in Deutschland, Österreich und der Schweiz berichten von einem Anstieg bei **Multi-Channel-Angriffen** via E-Mail, Messaging-Apps, Social Media und Deepfake-Sprachanrufen.



[1] **World Economic Forum (2025).** Global Cybersecurity Outlook.

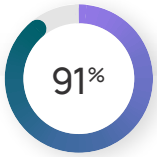
[2] **Bitkom (2024).** Angriffe auf die deutsche Wirtschaft nehmen zu.

Ihr eigener Schutz ist nicht mehr genug – denn auch Ihr Netzwerk wird zur Zielscheibe



der Organisationen in der DACH-Region verlassen sich auf **Zulieferer** – und jede einzelne Abhängigkeit erweitert die Angriffsfläche für Cyberkriminelle.

Selbst Ihr privates Umfeld wird zum möglichen Zugangstor

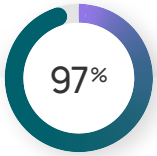


der Organisationen in Deutschland, Österreich und der Schweiz wurden bereits **über persönliche Geräte oder Konten** angegriffen.

Security-Training muss über die Unternehmensgrenzen hinaus gehen. Schulen Sie auch Familie und Freunde, denn sie alle werden zur möglichen Zielscheibe.

Andrea Szeiler
Global CISO bei Transcom

In dieser immer komplexeren Bedrohungslage machen Angreifende auch vor den Schwächsten nicht Halt



der Befragten aus Deutschland, Österreich und der Schweiz sind der Meinung, dass sich die **Kluft bei der Cyberresilienz** immer weiter vertieft.

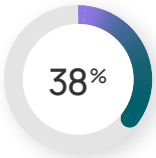
Kritische Sektoren und kleinere Unternehmen sind nicht ausreichend auf neue Bedrohungen vorbereitet.

Laut World Economic Forum beurteilen

über 1/3

der Kleinunternehmen weltweit ihre Cyberresilienz als **unzureichend**[1].

Auch im **öffentlichen Sektor** ist die Lage besorgniserregend...



der Unternehmen weltweit berichten von **unzureichender Resilienz**[1].

Nur mit vereinten Kräften können wir Cyberkriminellen die Stirn bieten

Die Zusammenarbeit zwischen privatem und öffentlichem Sektor ist unerlässlich. Nicht umsonst heißt es „Es braucht ein internationales Netzwerk, um ein internationales Netzwerk zu besiegen."

Philipp Amann
Group CISO, Österreichische Post AG

[1] **World Economic Forum (2025).** Global Cybersecurity Outlook.

Die neue Ära der Cyberkriminalität

Verschwimmende Grenzen, wachsende Risiken. **Die Methoden der Cyberkriminellen werden immer ambitionierter – ausgeklügelt nutzen sie jeden Bereich unseres digitalen Lebens zu ihrem Vorteil**. Die diesjährigen Cybercrime-Trends machen einen klaren Wandel deutlich: Die Angreifenden zielen nicht mehr nur direkt auf die unternehmenseigenen Netzwerke ab. Sie haben es verstärkt auch auf unsere persönlichen Identitäten, privaten Konten und Familienmitglieder abgesehen, die sie als Eintrittstor in Organisationen benutzen. Gleichzeitig gehen sie **immer strategischer und effizienter** vor. Mit der Hilfe von KI entwickeln Cyberkriminelle immer komplexere Angriffsmethoden, über Schwachstellen in unseren Lieferketten skalieren sie ihre Reichweite und mittels Multi-Channel-Taktiken umgehen sie traditionelle Abwehrmechanismen. Indem sie Kanäle wie E-Mail, SMS, Social Media und Kollaborationsplattformen kombinieren, erschleichen sie sich das Vertrauen ihrer Zielpersonen und lassen kein Schlupfloch ungenutzt. Die Folge? Das Cyberrisiko ist so hoch wie nie zuvor – laut World Economic Forum berichten 72 Prozent der Organisationen weltweit von einem Anstieg der Cyberangriffe – und auch **die Angriffsfläche ist größer denn je**. Organisationen müssen sich für eine Zukunft wappnen, in der Cyberbedrohungen immer personalisierter, großflächiger und schwerer zu erkennen werden.

Diese neuen Trends zu kennen, ist entscheidend, um nicht von ihnen überrollt zu werden. In diesem Bericht beleuchten wir den Stand der Cyber-Bedrohungslage für 2025 und geben Ihnen Praxistipps der Sicherheitsexpertinnen und -experten von SoSafe an die Hand, damit Sie den Angreifenden auch in Zukunft zwei Schritte voraus sind.

Methodik und Datenquellen

Umfrage zu den Cybercrime-Trends 2025

Für diese Umfrage zu den aktuellen Cybercrime-Trends 2025 haben wir uns mit dem in London ansässigen unabhängigen Marktforschungsunternehmen Censuswide zusammengetan. Im Dezember 2024 befragten wir dabei 500 Sicherheitsexpertinnen und -experten aus neun Ländern (Großbritannien, Frankreich, Deutschland, Österreich, Schweiz, Niederlande, Belgien, Luxemburg und Australien).

Umfrage zu den neuesten Social-Engineering-Methoden

Bei dieser Umfrage befragten wir 2024 **mehr als 100 Kunden von SoSafe aus mehr als zehn Ländern weltweit** zu den Social-Engineering-Strategien der neuesten Generation und dem daraus entstehenden wachsenden Risiko für Organisationen.

1 Der Vormarsch von KI schafft neue Angriffsvektoren

Cyberkriminelle vervielfachen ihre Angriffsfläche durch KI ...

Künstliche Intelligenz revolutioniert verschiedenste Branchen weltweit. Doch gleichzeitig bietet sie auch für Cyberkriminelle nie dagewesene Möglichkeiten. Angreifende nutzen KI als Angriffsvektor für ausgeklügelte Cyberangriffe, zum Beispiel in Form von realistischen Deepfakes. Gleichzeitig erstellen sie mit ihrer Hilfe großangelegte Phishing-Kampagnen, die mit weniger Ressourcen zu größeren Gewinnen führen. Laut World Economic Forum wurde **beim Handel mit Deepfake-Tools im Darkweb zwischen Q1 2023 und Q1 2024 ein globaler Zuwachs von 223 Prozent festgestellt**.[1] Die Folgen dieses Anstiegs zeigen sich jetzt in der Realität. Erst kürzlich fiel der CEO der weltweit größten Werbe-Holding WPP einem extrem ausgeklügelten Multi-Channel-Deepfake-Angriff zum Opfer.[2] Dabei imitierten die Angreifenden mittels Voice-Cloning seine Stimme und gelangten damit an das Geld und die persönlichen Daten von Mitarbeitenden.

KI ist jedoch nicht mehr nur ein Tool, um in Organisationen einzudringen – sie vergrößert jetzt auch deren Angriffsfläche. Viele Organisationen setzen inzwischen zur Optimierung ihres Geschäftsbetriebs eigene, intern entwickelte KI-Tools ein, wie beispielsweise zur Prozessautomatisierung und zur Analyse sensibler Daten. Vielen dieser Tools fehlen jedoch die nötigen Schutzmechanismen, was sie zu einer großen Schwachstelle macht. Wenn Cyberkriminelle Zugriff auf solche Tools erlangen, können sie sensible Informationen freilegen, Schwachstellen aufspüren und Sicherheitssysteme unbemerkt umgehen – mit verheerenden Folgen für die Organisation.

... und lassen die Abwehrmechanismen von Organisationen hinter sich zurück

Laut unserer globalen Kundenumfrage rechnen 91 Prozent der Teilnehmenden damit, dass Bedrohung und Intensität KI-basierter Cyberangriffe in den nächsten drei Jahren zunehmen werden. Auch die Komplexität der Angriffe steigt – etwa durch **Verschleierungsstrategien, bei denen beispielsweise der Ursprung und die Absicht eines Angriffs mittels KI verborgen wird**.

91 Prozent der Sicherheitsexpertinnen und -experten in unserer globalen Umfrage halten es für entscheidend, solche Angriffe zu erkennen. Doch nur 26 Prozent schätzen ihre eigene Fähigkeit dazu als „hoch“ ein. KI kann selbst einen wichtigen Beitrag zur Lösung leisten – etwa durch Mitarbeitertraining mit smarten Simulationen, die zentrale Zusammenführung von Security-Alerts oder automatisierte Code-Korrektur. Mit ihrer rasanten Entwicklung ist KI nicht nur ein zunehmendes Risiko, **sondern kann auch entscheidend dazu beitragen, den Schutz von Organisationen zu stärken**.

> Wir sollten Künstliche Intelligenz nicht nur zur Bekämpfung ihrer Gefahren einsetzen, sondern sie auch nutzen, um uns durch gezieltes Training auf mögliche Szenarien vorzubereiten.

Frank Schätzing
Science-Fiction-Bestsellerautor

1 **World Economic Forum (2025).** Global Cybersecurity Outlook.
2 **New York Post (2024).** CEO of WPP, world's biggest advertising agency, falls victim to elaborate deepfake scam.

Praxistipps

- **Schaffen Sie Awareness für KI:** Schulen Sie Ihre Mitarbeitenden zu den Fähigkeiten und Risiken von KI und wie sie KI-basierte Angriffe wie Deepfakes erkennen können. Für Early Adopter sollte die Sicherheit bei der Entwicklung, Implementierung und Wartung von KI-Technologien an oberster Stelle stehen.
- **Definieren Sie KI-Zuständigkeiten:** Etablieren Sie einen Governance-Ausschuss und Verwaltungsprozesse für alle KI-Lösungen innerhalb Ihrer Organisation. Führen Sie Inventar zu Ihren KI-Tools, bestimmen Sie Verantwortliche, bewerten Sie Risiken und arbeiten Sie Recovery-Pläne für mögliche Zwischenfälle aus. Etablieren Sie Mechanismen zur Überwachung neuer Risiken bei der Nutzung von KI in Ihrer Organisation. Nutzen Sie Richtlinien wie ISO 420001 als Ausgangspunkt.
- **Vermeiden Sie die Nutzung einer Standard-KI:** Eine einzige KI, die Zugriff auf alle Daten hat, kann zwar die Nutzererfahrung verbessern, sie birgt jedoch auch massive Risiken. Isolieren Sie Trainings-Datensätze, um zu vermeiden, dass beispielsweise Lagerarbeiter Zugang zum Netzwerkdesign haben oder ein Entwickler versehentlich HR-Daten freilegt. Nutzen Sie spezialisierte KIs, anstatt eines allgemeinen Systems.
- **Stärken Sie Ihre Sicherheits-Basics:** Optimieren Sie Ihre grundlegenden Schutzmechanismen, wie Least-Privilege-Zugriff, Trennung von Verantwortlichkeiten, regelmäßige Prüfungen von Zugriffsrechten, MFA und Patching. Stellen Sie sicher, dass Sie einen soliden Incident Response Plan haben, der regelmäßig überarbeitet wird.
- **Wenden Sie bestehende Richtlinien auf KI an:** Behandeln Sie KI-Outputs und KI-bezogene Entscheidungen aus dem Gesichtspunkt bewährter Richtlinien. Stellen Sie sicher, dass Ihre KI-Systeme DSGVO-Vorgaben und andere Frameworks erfüllen, indem Sie Audit-fähige Aufzeichnungen führen und Zuständigkeiten klar definieren.

Welche Aspekte KI-getriebener Angriffe beunruhigen Sie am meisten, falls überhaupt?

	Alle	DACH	AUS	FR	GB	BENELUX
Erschwerte Zurückverfolgung von Angriffen	50,8 %	54 %	52 %	52 %	55 %	41 %
Aufkommen völlig neuer Angriffsmethoden	44,8 %	38 %	43 %	56 %	45 %	42 %
Täuschungskraft KI-generierter Inhalte	41,6 %	36 %	44 %	40 %	45 %	43 %
Präzision der Zielsetzung	41,4 %	48 %	49 %	33 %	46 %	31 %
Schlechte Vorbereitung und fehlende KI-Bedrohungserkennungstools	38,8 %	41 %	48 %	37 %	29 %	39 %
Umfang und Schnelligkeit automatisierter Angriffe	38 %	32 %	43 %	38 %	38 %	39 %

2 Multi-Channel-Angriffe auf dem Vormarsch

Cyberkriminelle kombinieren Kanäle in komplexe 3D-Phishing-Angriffe ...

Cyberkriminelle haben ihr Repertoire an Angriffstaktiken und -kanälen in den letzten Jahren in rasantem Tempo vergrößert. **E-Mail ist 56 Prozent der Sicherheitsbeauftragten in der DACH-Region zufolge zwar immer noch der primäre Angriffskanal**.[1] Doch gleichzeitig diversifizieren Angreifende ihre Strategien und nutzen oft für einen einzigen Angriff mehrere Kanäle. Hinzu kommt, dass das Voranschreiten von KI ihnen ermöglicht, schwer aufspürbare und zielgerichtete Angriffe von hoher Komplexität durchzuführen. In unserer Umfrage zu den aktuellen Cybercrime-Trends **berichten 98 Prozent der Organisationen in der DACH-Region von einem Anstieg der Multi-Channel-Angriffe im vergangenen Jahr**.

Die Hintergründe? Angreifende haben es leichter denn je, da wir ständig neue Kommunikationskanäle nutzen. Sie nehmen ihre Zielpersonen durch eine Kombination aus E-Mail und Social Media, Telefonanrufen und Messenger-Apps ins Kreuzfeuer. Damit ahmen sie unsere normalen Kommunikationsmuster nach, was sie glaubhafter wirken lässt, – zum Beispiel, indem sie ein Dokument per E-Mail senden und danach über eine Messenger-App nachfragen, ob ihr Opfer es erhalten hat.[2] Strategien dieser Art, zu denen Phishing, Vishing, Smishing und QR-Phishing gehören, entwickeln sich in komplexe **„3D-Phishing-Angriffe“**.[3] Angetrieben durch KI integrieren sie nahtlos Voice-, Video- und textbasierte Elemente und werden so erschreckend überzeugend. Der in Trend 1 erwähnte Angriff auf den CEO von WPP veranschaulicht diese Vorgehensweise nur zu gut: Die Angreifenden bauen über WhatsApp Vertrauen auf, nutzen Microsoft Teams, um weiter mit ihrem Opfer zu interagieren, und führen danach mittels KI-generiertem Deepfake Anrufe durch, um an sensible Daten und Geld zu gelangen.[4]

... die noch nie so zielgerichtet und schwierig zu erkennen waren

Nicht nur ihr Multi-Channel-Ansatz macht diese Angriffe erschreckend komplex, sondern auch ihre äußerst zielgerichtete Ausführung. Für fortschrittliche Social-Engineering-Methoden wie Pretexting machen sich Cyberkriminelle online verfügbare Informationen über ihre Zielperson zunutze. Um diese realen Angaben herum bauen sie ihre erfundenen Szenarien auf und erschleichen sich so Vertrauen und Glaubwürdigkeit. Diese Art von Angriff wird immer häufiger – laut Verizon **sind weltweit 73 Prozent der Datenschutzverstöße bei Social-Engineering-Angriffen auf Phishing und Pretexting zurückzuführen**.[5]

Diese Angriffsmethoden sind für Zielpersonen wie auch die Behörden schwer zu erkennen, da sie oft über Plattformen mit unzureichenden Schutzmaßnahmen, wie Telegram, durchgeführt werden. Solche Plattformen spielen nicht nur bei der Ausführung von Angriffen, sondern auch bei der Professionalisierung der Cyberkriminalität eine zentrale Rolle. In

1 **SoSafe (2024).** Human Risk Review 2024.
2 **Northdoor (2024).** Phishing Threat Trends Report.
3 **Cyber security insiders (2024).** New Surge in Risky Business Email Compromise Phishing Attacks.

einem **Report berichtet die UN von kriminellen Netzwerken in Südostasien, die Telegram als Drehscheibe für ihre illegalen Geschäfte nutzen** und im großen Stil mit gestohlenen Daten, Hacking-Tools und anderen kriminellen Diensten handeln.[6] Das befeuert wiederum den Vormarsch von Multi-Channel-Angriffen und intensiviert die ohnehin bereits angespannte Cyber-Bedrohungslage weiter.

Praxistipps

- **Schulen Sie Mitarbeitende zu den Angriffsmethoden:** Ihre Mitarbeitende müssen die Vorgehensweisen von Cyberkriminellen kennen. Ihr Awareness-Programm sollte über die wichtigsten Strategien und Angriffskanäle aufklären, um das Sicherheitsgespür Ihrer Mitarbeitenden zu stärken.
- **Multi-Channel-Awareness-Training:** Beziehen Sie über Phishing-Mails hinaus auch Smishing und Vishing in Ihr Awareness-Training mit ein, damit Ihre Teams die verschiedenen Angriffsvektoren kennenlernen.
- **Kommunizieren Sie nur über sichere Tools:** Kollaborationstools bieten oft die Möglichkeit, dass sich auch externe Parteien verbinden können – ein mögliches Eintrittstor für Cyberkriminelle. Aktivieren Sie dieses Feature nur, wenn es dringend erforderlich ist.
- **Stärken Sie zentrale Zugriffskontrollen:** Stellen Sie sicher, dass wichtige Protokolle, wie die Trennung von Verantwortlichkeiten und der Least-Privilege-Zugriff, effektiv implementiert sind. Überprüfen Sie diese Kontrollmaßnahmen regelmäßig, um das Risiko für unberechtigten Zugriff zu minimieren.

> Schon seit Jahren predigen wir „Bei Zweifeln zur Echtheit einer E-Mail rufen Sie zur Prüfung den Absender an“. Jetzt wissen wir, selbst wenn wir die Stimme hören, nicht mehr, ob sie echt ist. Das zu überprüfen, wird immer komplizierter.

Yasemine Douadi
Cyber-Sicherheitsexpertin und CEO
von RISKINTEL MEDIA und RISK SUMMIT

4 **New York Post (2024).** CEO of WPP, world's biggest advertising agency, falls victim to elaborate deepfake scam.
5 **Verizon (2024).** Data Breach Investigations Report.
6 **Reuters (2024).** Telegram app hosts 'underground markets' for Southeast Asian crime gangs, UN says.

3 Supply-Chain-Attacken: Drittanbieter als Risiko für großflächige Datenschutzverstöße

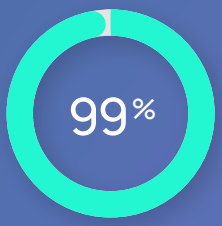
Drittanbieter sind aus dem Geschäftsbetrieb nicht mehr wegzudenken ...

Die Sicherheitsstrategie Ihrer Organisation ist immer nur so stark wie die Ihrer Drittanbieter. Laut unserer Umfrage zu den aktuellen Cybercrime-Trends **sind heute 99 Prozent der Organisationen in der DACH-Region bei der Bereitstellung ihres wichtigsten Angebots von Drittanbietern abhängig**. Doch diese Abhängigkeit hat ihren Preis. Jeder einzelne Anbieter bringt mehr Abhängigkeiten, Datenaustausch und Zugriffspunkte mit sich – alles potenzielle Eintrittstore für Cyberkriminelle. Anstatt in ihr Zielunternehmen direkt einzudringen, können Angreifende einen Umweg über einen weniger stark gesicherten Zulieferer nehmen und so lateral profitablere Opfer infiltrieren. Oder sie unterbrechen einen einzigen Service und treffen damit gleich mehrere Organisationen gleichzeitig.

Im vergangenen Jahr wurde deutlich, mit welcher Effizienz Cyberkriminelle Profit aus digitalen Lieferketten schlagen. Im Juli 2024 machten sich Angreifende schwere Sicherheitslücken in den Fortinet-Produkten FortiOS und FortiProxy zunutze.[1] Es gelang ihnen, Schutzmechanismen zu umgehen und sich unberechtigten Zugriff auf die betroffenen Systeme zu verschaffen. Nur einen Monat zuvor wurde CDK Global durch einen Ransomware-Angriff gezwungen, seine Systeme abzuschalten.[2] Dies hatte großflächige Geschäftsunterbrechungen und massive finanzielle Verluste bei über 15.000 US-Autohändlern zur Folge, die Dienste des Softwareanbieters nutzten.

... doch jeder weitere Partner vergrößert auch die Angriffsfläche

In den **komplexen und stark verknüpften Ökosystemen** vor allem der großen Unternehmen sind die Auswirkungen von Schwachstellen in der Lieferkette noch weitreichender. Große Organisationen sind nicht nur von **ihren eigenen Zulieferern abhängig, sondern wiederum auch von deren Zulieferern** – es entsteht ein großflächiges Netz an Schwachstellen, das auch als **Viertparteienrisiken** bezeichnet wird.[3] Da es für Organisationen kaum möglich ist, einen Überblick über sämtliche Verknüpfungen zu haben, können sie das Risiko ihrer Partnerschaften und das gesamte Ausmaß ihrer Angriffsfläche nur schwer einschätzen.



Prozent der Organisationen in der DACH-Region sind bei der Bereitstellung ihres wichtigsten Angebots von Drittanbietern abhängig.

1 **Golem (2024).** Kundendaten von Cybersecurity-Konzern abgeflossen.
2 **IT-Daily (2024).** Cyberangriff auf Software-Anbieter trifft tausende US-Autohändler.
3 **Dataminr (2024).** Third-party Vulnerabilities Put the Public Sector at Risk: What to Consider.

Praxistipps

- **Führen Sie Inventar über Ihre Drittanbieter:** Vielen Organisationen fehlt der Überblick über ihre Drittanbieter. Inventar zu führen, ist jedoch mehr, als eine Liste aller Anbieter zu erstellen. Dazu gehört auch das Scannen von Web-Datenverkehr, Workstations und Gateways auf Schatten-IT, die Überprüfung von Rechnungen und Kreditkartentransaktionen sowie Selbstauskünfte der Geschäftsbereiche im Rahmen der Business-Continuity- und DR-Planung. Um verborgene Abhängigkeiten zu erkennen und Risiken zu beheben, sind regelmäßige Updates des Inventars unerlässlich.

- **Klassifizieren Sie Drittanbieter nach ihrem Risikolevel:** Entwickeln Sie ein Risikomodell, um die möglichen Bedrohungen der einzelnen Zulieferer zu bewerten. Wenden Sie je nach Risikolevel Nachverfolgungen, vertragliche Verpflichtungen und Kontrollmaßnahmen an und stellen Sie sicher, dass diese vom Supplier Management Team umgesetzt werden.

- **Optimieren Sie Ihre Risiko-Assessments:** Ergänzen Sie traditionelle Fragebögen durch Vor-Ort-Prüfungen, Penetrationstests und Perimeter-Scans, um technische Risiken präziser zu bewerten. Beachten Sie auch menschliche Faktoren, wie die Security Awareness und Sicherheitskultur Ihrer Drittanbieter.

- **Isolieren Sie Kollaborationsbereiche:** Halten Sie Kollaborationsbereiche von Ihren kritischen Systemen getrennt. So können Sie die Auswirkungen eines Angriffs auf die Systeme Ihres Zulieferers für Ihre Organisation minimieren.

- **Diversifizieren Sie Ihre Lieferkette:** Machen Sie sich nicht zu abhängig von einem einzelnen Drittanbieter. Stellen Sie sicher, dass Sie bei Bedarf die nötige operationale Flexibilität haben, um schnell auf Alternativen umzulenken und bei einem Angriff auf wichtige Partner Ihr eigenes Risiko zu reduzieren.

> Vor dem Kauf von Software müssen wir sicherstellen, dass bei ihrer Entwicklung Sicherheitsaspekte beachtet wurden. Dazu fordere ich Berichte und Informationen zu Sicherheitskriterien an und überprüfe, dass die Entwicklungsmethoden sicher sind.

Lars Kukuk
CISO der Bundesagentur für Arbeit

4 Persönliche Identitäten: Das geheime Schlupfloch in die Unternehmenssysteme

Private Geräte werden zur Bedrohung für Organisationen …

Persönliche Identitäten sind heute angreifbarer denn je. Schon immer waren Einzelpersonen die Zielscheibe von Cyberkriminellen, doch jetzt mit anderen Zielen und neuen Methoden. Heute nutzen sie persönliche Identitäten als Hintertüren, um in Unternehmensnetzwerke einzudringen. Beunruhigende **91 Prozent der Sicherheitsverantwortlichen in der DACH-Region gaben an, dass ihre Organisation bereits über persönliche Geräte oder Konten Ihrer Mitarbeitenden angegriffen wurde**. Solche Angriffe umgehen traditionelle Abwehrmechanismen, erweitern die Angriffsfläche und stellen ein nie dagewesenes Risiko für Organisationen dar.

Zusätzlich steht noch mehr auf dem Spiel, da die Cyberkriminellen ihre Angriffsmethoden skalieren. Durch den Einsatz von KI können sie ihre Angriffe auf Endverbraucher automatisieren, was es ihnen ermöglicht, mehrere kleinflächige, aber extrem gezielte Angriffe gleichzeitig auszuführen. Unsere globale Kundenumfrage zeigt, dass **73 Prozent der Befragten einen Anstieg bei den Angriffen auf Verbraucher festgestellt haben**. Mit ihren Angriffen auf Privatpersonen erbeuten die Cyberkriminellen zwar kleinere Beträge. Da diese Angriffe aber großflächig aufgesetzt sind, erreichen sie so letztlich ihre finanziellen Ziele.

… und selbst das persönliche Umfeld bleibt nicht verschont

Die Problematik wird immer dringlicher, da die Grenzen zwischen der privaten und beruflichen Nutzung von Geräten verschwimmen. Durch neue Arbeitsmodelle, wie Hybrid- und Remote-Work, nutzen Mitarbeitende immer häufiger private Geräte und Konten für berufliche Zwecke – der Angriffsradius erstreckt sich weit über die Firewalls der Unternehmen hinaus.

Als wäre das nicht genug, haben Cyberkriminelle es durch großangelegte Datendiebstähle und den freizügigen Umgang mit persönlichen Daten im Netz leichter denn je, sensible Daten wie Passwörter, Adressen und Familienbande auszuspionieren. Über die Verwandten Ihrer Mitarbeitenden versuchen Angreifende heute, über Umwege in Ihre Organisation einzudringen. In einem aktuellen Fall zielten Cyberkriminelle mit SIM-Swapping auf das Kind einer Führungsperson ab, um so durch psychologische Manipulation Lösegeld zu fordern.[1] Nicht nur die Mitarbeitenden und Führungsetage werden zur Zielscheibe, sondern auch deren Familien.

Das Ergebnis: Auf die Einzelpersonen prasselt eine endlose Flut an großflächigen Betrugsmaschen ein, die die Wahrscheinlichkeit für menschliches Versagen in die Höhe treibt.

> Wir müssen über die Sicherheitsschulung im Unternehmen hinausgehen. Schulen Sie Ihre Familie und Ihre Freunde - denn Angreifer haben es auf jeden abgesehen.

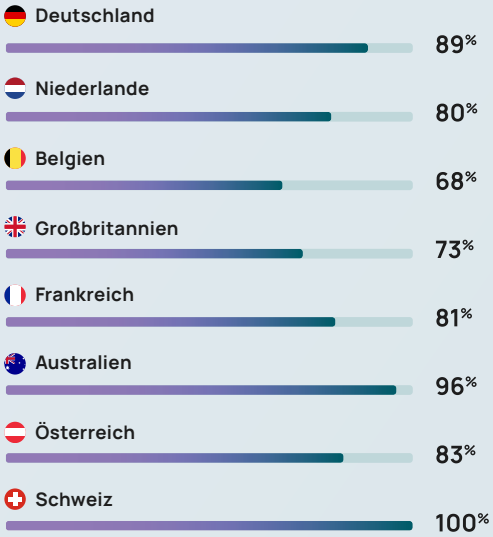
Andrea Szeiler
Global CISO bei Transcom

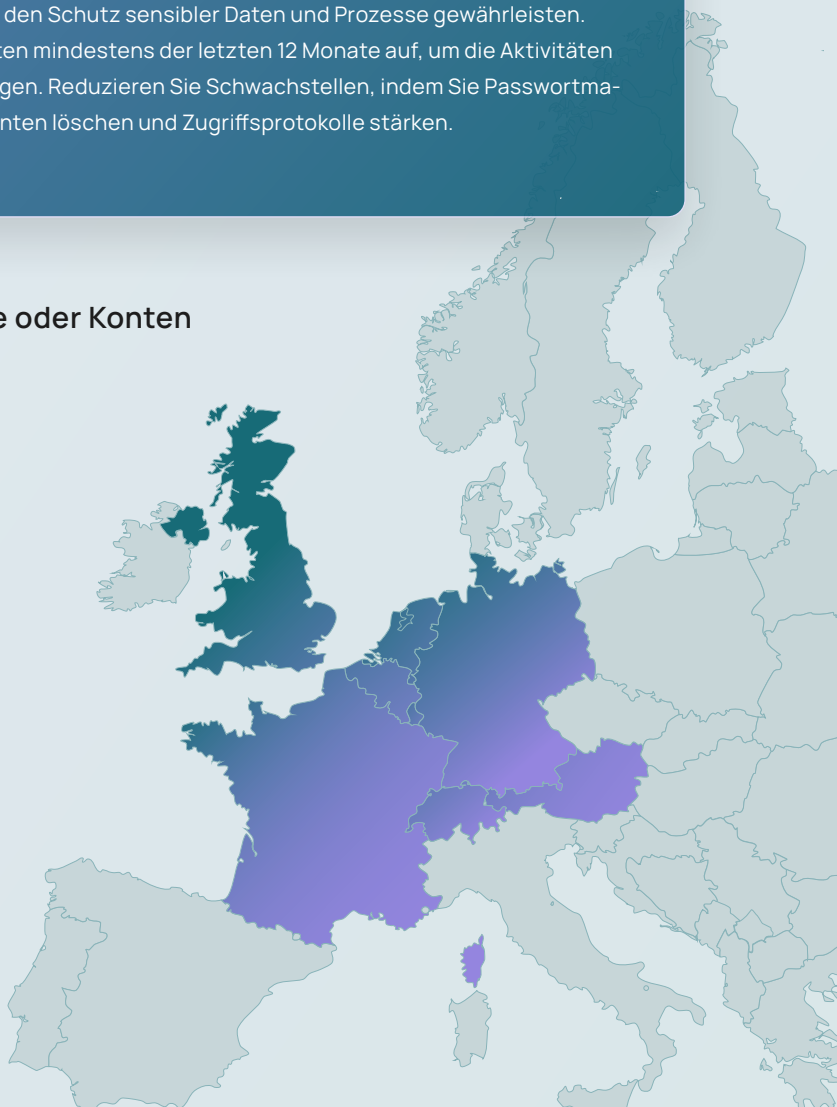
1 **Golem (2024).** Hacker erpressen Führungskräfte über Rufnummern ihrer Kinder.

Praxistipps

- **Beziehen Sie die persönliche wie auch berufliche Identität ins Training mit ein:** Fokussieren Sie Ihr Training auf die Bedeutung persönlicher und beruflicher Identitäten der Mitarbeitenden. Klären Sie über Angriffsmethoden und ihre Konsequenzen auf und verdeutlichen Sie, wie wertvoll Ihre Mitarbeitenden für die Angreifenden sind.
- **Erweitern Sie das Training auf den Familienkreis:** Beziehen Sie Familienmitglieder in Trainings mit ein, um ihre Sicherheit im digitalen Raum zu verbessern, da Cyberkriminelle auch die Familie ausnutzen, um über sie in Netzwerke einzudringen oder Ihre Mitarbeitenden zu erpressen.
- **Decken Sie mit technischen Schutzmaßnahmen auch private Geräte und firmenfremde Hardware ab:** Nicht selten nutzen Mitarbeitende private Geräte für die Arbeit. Manche Software-Anbieter bieten Rabatte auf Tools und Maßnahmen, die die Sicherheit privater Geräte erhöhen, ohne Ihr Sicherheitsteam zusätzlich mit der Verwaltung neuer Hardware zu belasten.
- **Sichern Sie Remote-Verbindungen:** Stärken Sie den Schutz remoter Verbindungen durch MFA, VPNs, Endpunktprüfung und DLP, um die Freilegung sensibler Daten außerhalb der unternehmenseigenen Schutzmaßnahmen zu verhindern.
- **Stärken Sie Zugriffskontrollen:** Führen Sie unter der Annahme, dass es zu Datenschutzverstößen kommen wird, Audits aller Systeme durch, die den Schutz sensibler Daten und Prozesse gewährleisten. Bewahren Sie die Log- und Überwachungsdaten mindestens der letzten 12 Monate auf, um die Aktivitäten von Mitarbeitenden im Notfall zurückzuverfolgen. Reduzieren Sie Schwachstellen, indem Sie Passwortmanager überprüfen und aufräumen, geteilte Konten löschen und Zugriffsprotokolle stärken.

Organisation, die über persönliche Geräte oder Konten Ihrer Mitarbeitenden angegriffen wurde



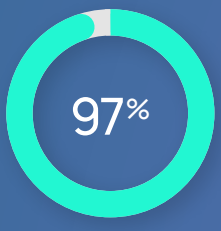


5 Mangelnde Cyberresilienz gefährdet die Sicherheit wichtiger Dienste

Cybercrime stellt kritische Sektoren vor immense Herausforderungen ...

Informationssicherheit ist nicht für alle gleichermaßen zugänglich und diese Lücke in Sachen Cybersicherheit wächst zwischen verschiedenen Branchen immer weiter. Stark regulierte Sektoren, wie die Finanzbranche, und weltweit agierende Konzerne stärken ihre Resilienz stetig weiter, indem sie beachtliche finanzielle wie auch personelle Ressourcen investieren und modernste Technologien nutzen. Weniger regulierte Sektoren mit eingeschränkten Ressourcen – wie kritische Infrastrukturen, das Gesundheitswesen, der Einzelhandel oder der Wohltätigkeits- und Produktionssektor – können damit kaum mithalten. Unserer Umfrage zum Thema Cybercrime-Trends zufolge sind 97 Prozent der Befragten in der DACH-Region der Meinung, dass sich die Kluft immer weiter vertieft, was die betroffenen Sektoren übermäßig angreifbar macht. Dieses Ungleichgewicht ist nicht nur ein technisches Problem – es ist eine systemische Schwachstelle, die das Gemeinwohl und die wirtschaftliche Stabilität gefährdet.

> Die Informationssicherheit der Lieferketten kritischer Infrastrukturen und des öffentlichen Sektors muss sich verbessern. Zwischen der Resilienz unserer Infrastruktur und den neuen Cyberbedrohungen besteht eine wachsende Diskrepanz.
>
> **National Cyber Security Centre**
> in Großbritannien



der Sicherheitsexpertinnen- und experten in der DACH-Region sind der Meinung, dass sich die Kluft bei der Cyberresilienz immer weiter vertieft.

... und Angreifende nutzen diese Schwachstellen gezielt aus

Das Ungleichgewicht bei der Cyberresilienz basiert auf systemischen Herausforderungen. Finanzdienstleister profitieren von strengen Regularien und Großunternehmen nehmen großzügige Ressourcen in die Hand, um ihre Abwehr zu stärken. Im Gegensatz dazu fehlen kleineren Unternehmen und Sektoren, wie kritischen Infrastrukturen, dem Gesundheitswesen und der Produktionsbranche der Überblick und die

Ressourcen – was sie angreifbarer macht. Eingeschränkte Budgets, veraltete Systeme und unzureichendes Engagement auf Führungsebene vergrößern die Kluft weiter. Laut World Economic Forum schätzen weltweit über ein Drittel der kleinen Organisationen (35 %) ihre Cyberresilienz als unzureichend ein – ein siebenfacher Anstieg seit 2022.[1] Im öffentlichen Sektor sind die Zahlen sogar noch etwas höher: Dort berichten 38 Prozent von unzureichender Resilienz, während es in privaten Organisationen nur 10 Prozent sind.

Der weltweite Mangel an Sicherheitsexperten schüttet weiter Öl ins Feuer. Während kapitalkräftige Sektoren die besten Fachkräfte anziehen, haben Organisationen mit geringeren Budgets Schwierigkeiten, erfahrenes Sicherheitspersonal für sich zu gewinnen. Wie zuvor erwähnt, sind Organisationen des öffentlichen Sektors weltweit weiterhin am schlechtesten aufgestellt: 49 Prozent berichten von einem Fachkräftemangel, der ihren Cyber-Sicherheitszielen im Weg steht – 33 Prozent mehr als 2024.[1] Die entstehenden Schwachstellen machen weniger gut aufgestellte Sektoren als Angriffsziel für Cyberkriminelle und staatlich finanzierte Akteure immer attraktiver und intensivieren das wachsende Risiko für grundlegende Dienste und die öffentliche Sicherheit. Dringender denn je muss diese Lücke geschlossen werden.

Praxistipps

- **Halten Sie sich an anerkannte Frameworks:** Bauen Sie Ihre Strategie, unabhängig von regulatorischen Anforderungen, auf bewährten Richtlinien, wie ISO 27001 und NIST CSF, auf.
- **Kollaborieren Sie mit Regulierungsbehörden:** Arbeiten Sie proaktiv mit den regulierenden Instanzen Ihres Sektors zusammen. Entwickeln Sie gemeinsam praktische Richtlinien, von denen die gesamte Branche zum Wohle ihrer Sicherheit profitieren kann.
- **Verteilen Sie die Verantwortung auf verschiedene Abteilungen:** Sicherheitsteams sollten nicht die Ineffizienzen anderer Abteilungen ausbügeln müssen. Stellen Sie sicher, dass die richtigen Teams für OS-Patching, Code-Härtung und das Aufspüren veralteter Systeme zuständig sind und dass die Verantwortung für entstehende Risiken klar zugewiesen wird.
- **Orientieren Sie sich an reiferen Branchen:** Vernetzen Sie sich mit Organisationen in stark regulierten Sektoren und finden Sie heraus, welche Schutzmaßnahmen diese für mehr Resilienz einführen. Nutzen Sie günstigere Alternativlösungen, die die Anforderungen Ihrer Branche erfüllen.
- **Nutzen Sie neue Kanäle, um Fachkräfte zu gewinnen:** Bauen Sie Partnerschaften mit Universitäten und Fachschulen für die Bereiche auf, in denen Ihnen Fachkräfte fehlen. Bieten Sie Praktikums- und Ausbildungsplätze an, um vielseitig qualifizierte Fachkräfte anzuziehen.
- **Informieren Sie alle Teams über Sicherheitsstrategien:** Als CISO in weniger stark regulierten Branchen und kleineren Organisationen sollten Sie sicherstellen, dass Ihre Cyber-Sicherheitsstrategie klar und einfach umsetzbar ist. So können auch weniger technische Teams, wie zum Beispiel Fabrikarbeiter, aktiv zur Verteidigung der Organisation beitragen.

1 **World Economic Forum (2025).** Global Cybersecurity Outlook.

6 Der Cybercrime-Markt boomt

Cyberkriminelle nutzen die weltweite Vernetzung zu ihrem Vorteil ...

Die Cybercrime-Industrie hat sich in ein durchorganisiertes, globales Geschäftsmodell entwickelt, dessen Erfolg durch unsere wachsende Abhängigkeit von Technologie genährt wird. Die rasante Zunahme von Remote-Work, vernetzten Geräten und neuen Technologien, wie KI, IoT und Cloud-Umgebungen – das alles hat die Angriffsfläche um ein Vielfaches vergrößert. Cyberkriminelle haben heute mehr mögliche Zutrittstore in unsere Systeme als je zuvor. Jeder Sektor und jede Einzelperson sind heute Teil eines eng verzweigten digitalen Netzes, in dem sich ein einziger Angriff schockwellenartig auf mehrere Unternehmen, Branchen und ganze Gemeinschaften ausbreiten kann. Und das mit verheerenden finanziellen Folgen – **die weltweiten Kosten von Cybercrime sollen dieses Jahr 10 Billionen US-Dollar erreichen**.[1]

Angetrieben wird das Wachstum dieses lukrativen Markts jedoch nicht nur durch seine Größe, sondern vor allem auch durch die ausgeklügelten Methoden der Cyberkriminellen. In Sachen Präzision, Koordination und Anpassungsfähigkeit haben sie ihre Vorgehensweise perfektioniert und zielen oft auf vielversprechende Einzelpersonen oder Organisationen in Rechtssystemen ab, in denen die Nachverfolgung von Cybercrime-Zwischenfällen nicht ausreichend durchgesetzt wird. Für die Koordination ihrer Angriffe über Landesgrenzen hinweg nutzen Cyberkriminelle globale Online-Plattformen wie Telegram, die eine große Reichweite und kaum Einschränkungen bieten. Auch die **Professionalisierung der Cyberkriminalität** durch Dienste wie Ransomware-as-a-Service (RaaS) hat dazu beigetragen, dass der Cybercrime-Markt immer lukrativer wird und die Zutrittsschwelle zur Cyberkriminalität immer weiter sinkt. Aus diesem illegalen Geschäftsmodell hat sich ein breiteres Cybercrime-as-a-Service-Ökosystem entwickelt, das weniger erfahrenen Cyberkriminellen und Neueinsteigern Malware-Kits, Phishing-Templates und Tools für DDoS-Angriffe (Distributed Denial of Service) bereitstellt.[2]

... doch nur durch globale Zusammenarbeit können wir uns den neuen Cyberbedrohungen entgegenstellen

Aktuellen Prognosen zufolge verursachte Cyberkriminalität in Deutschland im Jahr 2024 einen Schaden von 178,6 Milliarden Euro – ein Anstieg von rund 30 Milliarden Euro im Vergleich zum Vorjahr (2023: 148,2 Milliarden Euro).[3] Ohne umgehende Gegenmaßnahmen werden die Zahlen weiter steigen. Isolierte Initiativen sind nicht genug, um uns der wachsenden Bedrohung entgegenzustellen – dazu müssen wir alle an einem Strang ziehen. Durch die Zusammenarbeit über Organisationen, Branchen und Regierungen hinweg können wir Threat Intelligence austauschen, einheitliche Abwehrstrategien entwickeln und die lückenlose Durchsetzung von Richtlinien gewährleisten.

1 **Statista (2024).** Cybercrime Expected to Skyrocket in Coming Years.
2 **Europol (2024).** Cyber-attacks: the apex of crime-as-a-service.
3 **Bitkom (2024).** Angriffe auf die deutsche Wirtschaft nehmen zu.

> Die Zusammenarbeit zwischen privatem und öffentlichem Sektor ist unerlässlich. Nicht umsonst heißt es „Es braucht ein internationales Netzwerk, um ein internationales Netzwerk zu besiegen.

Philipp Amann
Group CISO,
Österreichische Post AG

Praxistipps

- **Kennen Sie Ihre wachsende Angriffsfläche und priorisieren Sie sie:** Verstehen Sie, welche Elemente in Ihrer Kontrolle liegen und welche nicht. Gehen Sie technische, menschliche und Drittrisiken durch entsprechende Nachverfolgung, sorgfältige Prüfung und den Einsatz von Ressourcen basierend auf Ihrem Ausmaß an Bedrohungen an.
- **Vereinfachen Sie Prozesse im Sinne der Agilität und Kostensenkung:** Jede zusätzliche Layer, jeder Prozess und jedes System steigert die Komplexität im Alltag und erschwert eine schnelle Reaktion im Fall eines Angriffs. Konsolidieren Sie Zulieferer und Systeme und etablieren Sie Geschäftsbereiche, um sicherzustellen, dass sie alle ihre Prozesse vereinfachen.
- **Stärken Sie Ihre operationale Resilienz:** Arbeiten Sie Hand in Hand mit den Verantwortlichen für Geschäftsprozesse, um sicherzustellen, dass wichtige Aufgaben auch im Falle eines Cyberangriffs fortgesetzt werden können – unter anderem auch durch analoge Abläufe. So gewährleisten Sie, dass Ihre Organisation in jeder Lage ein Minimum Viable Product oder Service bereitstellen kann.
- **Verteilen Sie die Verantwortung auf Abteilungen:** Vermeiden Sie, dass mangelnde Qualitätskontrollen in anderen Bereichen der Organisation auf das Sicherheitsteam zurückfallen. Weisen Sie die Zuständigkeit für OS-Patching, Code-Härtung und das Aufspüren veralteter Systeme den entsprechenden Teams zu, die dann auch für entstehende Risiken verantwortlich sind.

Cybercrime-Trend Resilience Matrix

Wie gut ist Ihre Organisation gegen die aktuellen Cybercrime-Trends aufgestellt?

Die folgende Cybercrime-Trend Resilience Matrix bietet Ihnen klare **Richtwerte zur Einschätzung der Cyberresilienz Ihrer Organisation** mit Blick auf die aktuellen Angriffstrends. Sie zeigt **wichtige Schritte** auf, die Sie von einem reaktiven Sicherheitsansatz zu maximaler Cyberresilienz bringen.

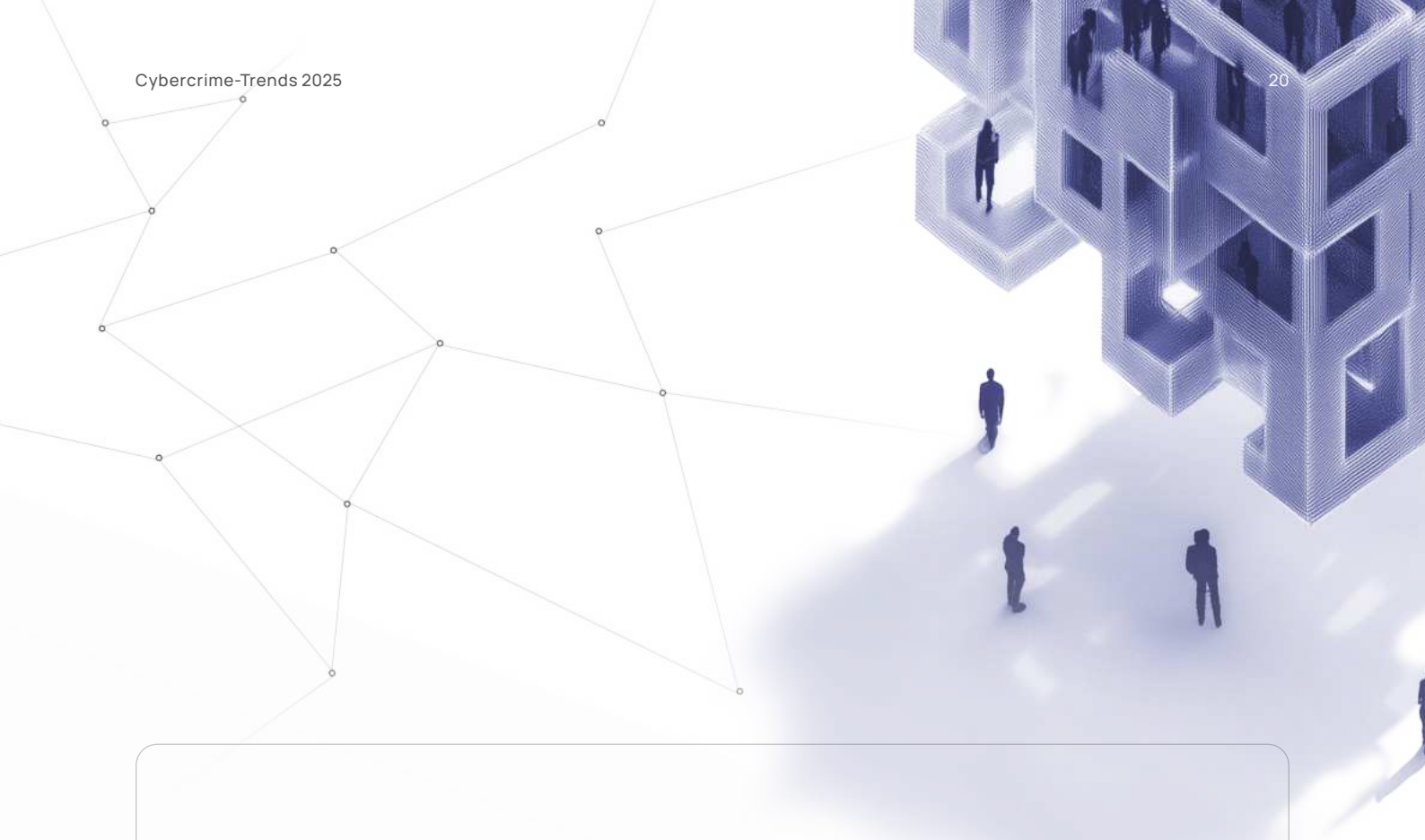
	Stufe 1 - Elementar	Stufe 2 - Proaktiv	Stufe 3 - Resilient
KI als Angriffsfläche	› Nutzung und Kontrolle von KI-Tools unzureichend reguliert › Mangelnde Sicherheitskontrollen interner KI-Tools › KI-getriebene Angriffsmethoden (Deepfakes, Phishing) nicht überwacht	› KI-Governance-Ausschuss vorhanden; eigene Risiken durch KI sind bekannt oder dokumentiert › Eingeschränkter Zugriff auf KI-Daten; bestimmte Prompt-Prüfungen vorhanden, um schädliche Absichten aufzudecken › KI-getriebene Angriffsmethoden werden sporadisch überwacht	› Sicherheit ist entscheidender Aspekt bei Entwicklung und Wartung von KI-Tools › Strenge Datenzugriffskontrollen; stetige Überwachung KI-getriebener Angriffsmethoden › KI-bezogenes Mitarbeitertraining und Risiko-Assessment
Multi-Channel-Angriffe	› Schutzmaßnahmen auf E-Mail fokussiert › Angriffe per SMS, Anruf oder Social Media nur in Richtlinien und Schulungen ein Thema › Kein Reaktionsplan für Multi-Channel-Angriffe vorhanden	› Teilweise Überwachung von SMS, Kollaborationstools und Social Media › Threat Detection vorhanden, doch die Response variiert je nach Kanal › Nur geringes Training zu Multi-Channel-Phishing	› Eine einheitliche Verteidigungsstrategie für alle Angriffskanäle › Proaktive Überwachung von E-Mail, SMS und sozialen Medien › Regelmäßige personalisierte Multi-Channel-Simulationen für Mitarbeitende
Lieferketten- und Drittparteienrisiko	› Mangelnder Überblick über die Abdeckung des Drittanbieterrisikos › Drittanbieter-Sicherheit auf Compliance-Anforderungen begrenzt › Viertparteienrisiken werden nicht erfasst › Kein fester Reaktionsplan für Datenschutzverstöße bei Zulieferern	› Assessment von Zulieferern, doch Drittparteienrisiko dennoch unklar › Sicherheitsanforderungen an Zulieferer, jedoch mangelnde Umsetzung und Nachverfolgung › Incident Response umfasst Datenschutzverstöße bei Dritten, es fehlen jedoch die formellen Prozesse	› Regelmäßige Drittparteienrisiko-Assessments mit auf Risiko/Abhängigkeit abgestimmten Prüfungen und Audits › Sicherheitsanforderungen in Lieferantenverträgen verankert, ggf. mit verpflichtender Übertragung auf Viertparteien › Viertparteienrisiken werden bedacht, beurteilt und verwaltet › Klar definierter Notfallplan für Supply-Chain-Attacken › Zulieferer in Business-Continuity-Simulationen miteinbezogen

	Stufe 1 - Elementar	Stufe 2 - Proaktiv	Stufe 3 - Resilient
Bedrohungen für persönliche Identitäten	› Grundlagentraining zu Social-Engineering-Methoden › Keine Schutzmaßnahmen für persönliche Konten der Mitarbeitenden › Risiko im privaten Bereich hat keine Priorität	› Awareness-Training für Mitarbeitende, doch kein geregelter Schutz für persönliche Identitäten › Mitarbeitende werden zum Schutz privater Konten ermutigt, aber nicht verpflichtet › Schutz von persönlichen Identitäten gilt nur auf Führungs- und Vorstandsebene als wichtig	› Awareness-Programm bezieht Schutz persönlicher Identitäten und Geräte mit ein › Starker Schutz der Identitäten von Führungspersonen und Mitarbeitenden › Laufendes Monitoring auf gestohlene Zugangsdaten
Ungleich-gewicht bei Cyberresilienz	› Geringe Investitionen in Cybersicherheit › Compliance wird als ärgerliche Verpflichtung betrachtet › Security-Entscheidungen werden reaktiv getroffen	› Schutzmaßnahmen vorhanden, doch Budgets und Support der Führungsebene sind begrenzt › Compliance mit vorgeschriebenen Mindestanforderungen › ISO27k gilt als Orientierungsgrundlage oder wird aufgrund begrenzter Reichweite implementiert › Cyber-Sicherheitsstrategie vorhanden, aber nur kurzfristig › Incident Response Plan nicht getestet oder nicht formell festgehalten	› Sicherheit wird Priorität und entsprechende Ressourcen eingeräumt › Für den Großteil aller wichtigen Systeme ISO27k-zertifiziert › Entwicklung regulatorischer Anforderungen im Austausch mit zuständigen Regulierungsbehörden › Aktive Unterstützung der Cyber-Security-Initiativen durch die Führungsebene › Sicherheitsstrategien im Einklang mit Geschäftsanforderungen
Boom der Cybercrime-Branche	› Reaktive Haltung gegenüber Cyberbedrohungen › Informationen zu neuesten Angriffstrends aus allgemeinen Quellen bezogen › Keine langfristige Strategie zur Anpassung	› Cybercrime-Trends im Blick, doch die Reaktion beschränkt sich auf direkte Bedrohungen › Sporadisches Sammeln und Weitergeben von Informationen, doch begrenzte Anpassung an neue Angriffstrends › Mitarbeitende werden über Trends informiert, aber nicht regelmäßig dazu geschult	› Sicherheitsstrategie basiert auf personalisierten Threat-Intelligence-Diensten › Stetige Anpassung an neue TTP (Taktiken, Techniken und Prozeduren) der Angreifenden › TTP der Angreifenden zu kennen, gehört zur Unternehmenskultur

Wie steht es um die Sicherheit Ihrer Organisation?

Nutzen Sie unser Assessment für eine individuelle Einschätzung Ihrer Cyber-Resilienz.

Jetzt Cyber-Resilienz testen



Das „Cyber-Labyrinth“ wandelt sich – doch es gibt einen Ausweg

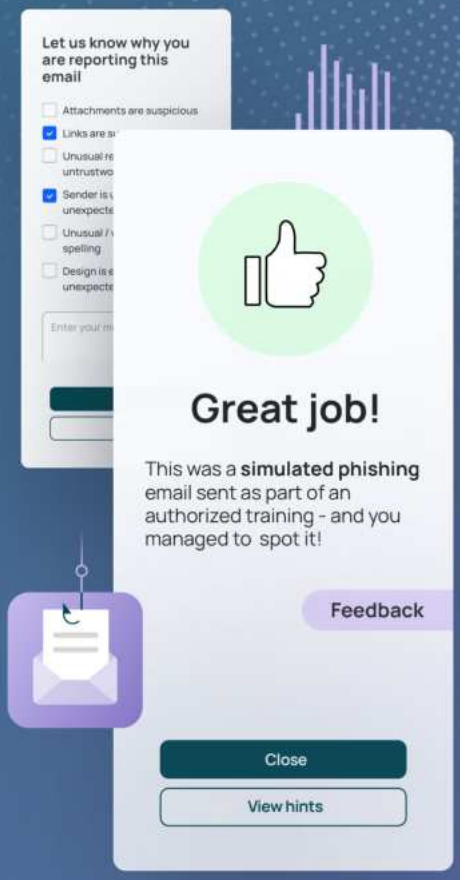
Wie schon das Cover dieses Reports veranschaulicht, ist die Cyber-Bedrohungslage zu einem **immer komplexeren Labyrinth herangewachsen**. Die Angreifenden entwickeln ihre Strategien in rasantem Tempo weiter und nutzen KI, Lieferketten und persönliche Identitäten aus, um über die verschiedensten Schlupflöcher in Organisationen einzudringen. Die Angriffsfläche wächst stetig weiter und mit ihr die Herausforderungen in der Cyber Sicherheit. Doch trotz der Skalierung und steigenden Komplexität der Angriffsmethoden gibt es immer noch Möglichkeiten, unseren Schutz zu stärken.

Um unsere Cyberresilienz zu verbessern, müssen wir auf Kollaboration und Innovation setzen. Organisationen müssen sich über Branchen hinweg zusammenschließen, Informationen austauschen und ihre Verteidigung gemeinsam stärken. KI ist ein beliebtes Tool der Angreifenden. Doch auch für unseren Schutz hat es massives Potenzial – sei es zur schnellen Erkennung von Angriffen, zur Automatisierung von Schutzmechanismen oder zur Verkürzung von Reaktionszeiten. Doch Technologie ist nur ein Teil der Gleichung. Durch eine starke Sicherheitskultur machen Sie jeden Einzelnen – vom Mitarbeitenden bis zur Führungsperson – zu einem aktiven Teil Ihrer Verteidigungslinie.

Und genau dabei wollen wir von SoSafe Ihnen helfen. Dazu geben wir Ihnen die Best Practices führender Sicherheitsexpertinnen und -experten an die Hand und entwickeln ständig neue Lösungen, die Ihrer Organisation helfen, ihre Cyberresilienz zu stärken. Im Zeitalter KI-getriebener Angriffe, wachsender digitaler Vernetzung und einer immer komplexeren Cyber-Bedrohungslage wollen wir Ihnen zeigen, **dass es immer eine Lösung gibt**.

Die Cyber-Bedrohungslage ist ein Labyrinth – das muss nicht für Ihre Sicherheitsstrategie gelten

KI-getriebene Angriffe, Multi-Channel-Betrugsmaschen und Schwachstellen in den Lieferketten treiben die Sicherheitsrisiken von Organisationen immer weiter in die Höhe. Das erfordert einen smarten **Human-Risk-Management-Ansatz**, der Bedrohungen erkennt, vermeidet und abwehrt, bevor es zu spät ist. So hilft SoSafe Ihrer Organisation, ihren Schutz gegen die neuesten Angriffstrends zu stärken:



1 Partnern Sie mit KI, damit sich Ihr Sicherheitsteam um das wirklich Wichtige kümmern kann

Sofie – KI-basierter Sicherheits-Copilot: Unser KI-basierter Chatbot unterstützt Mitarbeitende in Echtzeit bei Sicherheitsfragen, ermöglicht sofortige Interventionen und stellt Mikro-Lerninhalte zu neuen Bedrohungen bereit.

KI-getriebene Phishing-Kampagnen: Automatisieren Sie die Erstellung und Durchführung realistischer Phishing-Simulationen via E-Mail, SMS und Voice-Kanäle.

Simulation Studio, angetrieben durch KI: Erstellen Sie mit der Hilfe von KI adaptive Phishing-Templates, die den manuellen Aufwand reduzieren und stets die neuesten Angriffstrends berücksichtigen.

Verhaltensbasierte Phishing-Simulationen: KI-getriebene Simulationen, deren Häufigkeit und Schwierigkeitsgrad automatisch an das individuelle Risikolevel angepasst werden.

2 Erreichen Sie umfassenden Schutz vor Phishing, ohne zusätzlichen Zeitaufwand

Verteidigung gegen Vishing: Befähigen Sie Ihre Mitarbeitenden, Phishing-Versuche am Telefon zu erkennen und richtig darauf zu reagieren.

Schutz vor Smishing: Erstellen Sie SMS-basierte Phishing-Simulationen und helfen Sie Ihren Mitarbeitenden, betrügerische Textnachrichten und Phishing-Angriffe auf Mobilgeräten zuverlässig zu erkennen.

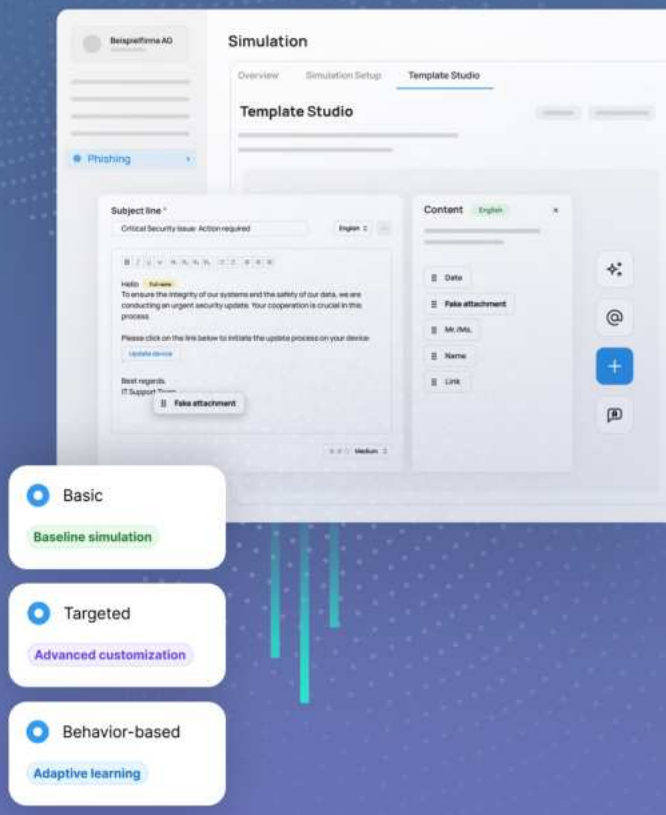
3 Erreichen Sie ganzheitliche Security Awareness – bei der Arbeit, zu Hause und unterwegs

Personalisiertes Micro-Learning: Unsere Micro-Lerninhalte bieten ein zielgerichtetes Trainingserlebnis, das individuell auf die Verhaltensweisen, Risiken und Lernanforderungen der Mitarbeitenden abgestimmt ist.

Zielgerichtete Simulationen: Passen Sie Ihre Phishing-Simulationen an die individuellen Risikoprofile und Aufgaben der einzelnen Mitarbeitenden an.

Wissen für alle Lebensbereiche: Wir vermitteln Security Awareness, die über das berufliche Umfeld hinausgeht und den Schutz Ihrer Mitarbeitenden auch im privaten Bereich stärkt.

Awareness-Training für Familie und Freunde: Steigern Sie die Wirkung Ihres Awareness-Trainings, indem Sie Security-Grundlagenwissen auch für den Familien- und Freundeskreis Ihrer Mitarbeitenden bereitstellen.



4 Nutzen Sie datenbasierte Insights, um zielgerichtete Entscheidungen zu treffen

Human Risk OS: Unser Human Risk Operating System transformiert Security Awareness in proaktives Risikomanagement. Es analysiert menschliche Verhaltensmuster, überwacht Risikosignale aus verschiedenen Quellen und ermöglicht automatisierte, gezielte Interventionen, die entstehende Bedrohungen im Kern ersticken.

Phishing-Meldebutton: Unser Phishing-Meldebutton unterstützt Mitarbeitende dabei, verdächtige E-Mails schnell zu melden, und ermöglicht Sicherheitsteams, Bedrohungen durch Echtzeit-Informationen zu erkennen und schnell abzuwehren.

5 Stärken Sie Ihre Sicherheit auf jeder Etappe Ihrer Security-Journey

Vollständige Compliance und Vorbereitung auf Audits: Organisationen, die gerade mit dem Aufbau ihrer Sicherheitskultur beginnen, unterstützen wir mit Assessments, Compliance-Frameworks und Awareness-Programmen dabei, globale und branchenspezifische Richtlinien zu erfüllen und ihren Schutz zu stärken.

Personalisierte Sicherheit und Verhaltensänderung: Für Organisationen, die auf ihrer Security-Journey weiter vorangeschritten sind, stellen wir personalisiertes Security-Training und gezielte Interventionen bereit, um Security Awareness und sicheres Verhalten in ihrer Kultur zu verankern.

Proaktives Risikomanagement: Bei ausgereifteren Security-Programmen bieten wir datenbasiertes, proaktives Risikomanagement mit Behavioral-Analytics, Daten zu den menschlichen Sicherheitsrisiken und adaptiven Schutzmaßnahmen, damit Ihre Organisation neuen Angriffstrends immer einen Schritt voraus ist.

Kontakt

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

Simona Dunsche
Corporate Communications Manager
press@sosafe-awareness.com

SoSafe SE
Lichtstraße 25a
50825 Köln

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

sosafe