sosafe

# Human Risk Review 2022

Eine Analyse der europäischen Cyber-Bedrohungslage

Die Professionalisierung von Cyberkriminalität hat einen gefährlichen Höhepunkt erreicht.



# Editorial

## Innovativ und höchst professionell – Die neue Generation von Cyberkriminalität

Weltweite Krisen, geopolitische Herausforderungen, die COVID-19-Pandemie – das vergangene Jahr ließ uns keine Zeit durchzuatmen. Und leider mussten wir auch im Bereich Informationssicherheit dramatische Entwicklungen beobachten. Denn Cyberkriminelle ließen nicht lange mit Angriffen auf sich warten, als es darum ging, den dynamischen gesellschaftlichen Kontext für ihre skrupellosen Absichten auszunutzen.

Hinzu kommt eine zunehmende Professionalisierung im Bereich Cyberkriminalität. Organisationen sehen sich nun einer innovativen Dark Economy gegenübergestellt, in der Cybercrime-as-a-Service das gängige Geschäftsmodell ist. Taktiken werden beinahe im Minutentakt weiterentwickelt. Auch die IT-Landschaft wird immer diverser: Hybride Arbeitsweisen haben neue Kommunikationskanäle mit sich gebracht, die Cyberkriminellen zusätzliche Eintrittswege für tückische Angriffe auf Unternehmenssysteme eröffnen.

Die Schnittstelle zwischen Mensch und Maschine bleibt dabei weiterhin Einstiegstor Nummer 1 – mehr als 85 Prozent aller Angriffe starten beim Faktor Mensch. Das ist nicht überraschend. Denn die Menschen hinter den Bildschirmen lassen sich auch beim Einsatz der vielfältigsten Tools immer auf eine ähnliche Art und Weise angreifen – über emotionale Manipulation. Gerade Supply-Chain- und Ransomware-Angriffe – und davon haben wir im vergangenen Jahr neben eindrücklichen Fällen wie Kaseya und Kronos viele weitere beobachten müssen – starten oft mit Phishing.

Was solche Vorfälle aber auch zeigen: Mitarbeitende sind aktiver Lösungsbestandteil des Billionen-Dollar-Problems Cybercrime. Wissen sie mit den Gefahren umzugehen und diese abzuwenden, schützen sie ihre Organisation proaktiv vor kostspieligen Vorfällen. Um nicht von der Innovationskraft der Cyberkriminellen überrollt zu werden, sollten Organisationen deshalb auf verhaltenswissenschaftlich fundierte Awareness-Maßnahmen setzen. Unser „Behavioral Security Model“ (Seite 52) zeigt, wie sich so nachhaltig eine starke Sicherheitskultur aufbauen lässt.

So dramatisch die Lage auch in vielerlei Hinsicht ist, eine positive Änderung bringt sie doch mit sich: Informationssicherheit bekommt endlich mehr Aufmerksamkeit. Der Anstieg von Cybercrime lässt Security-Budgets steigen und Organisationen können sich effektiver schützen. Jetzt ist der richtige Zeitpunkt, sich professionalisierten Cyberkriminellen entgegenzustellen – und durch die Minimierung menschlicher Sicherheitsrisiken den Schutz von Daten und Systemen sicherzustellen!

**Dr. Niklas Hellemann**
Managing Director SoSafe

# Inhaltsangabe


**Editorial** 3

**Executive Summary** 6

**01 Die Cyber-Bedrohungslage** 9

1.1 Malware zeigt ungebrochenen Aufwärtstrend 12

1.2 Die größten Cybercrime-Trends 2022 14

1.3 Globale Bedrohungen sorgen für verschärfte Regularien 22

1.4 Hybride Kriegsführung 24

**Interview: Achim Berg, Bitkom** 26

**02 Sektoren im Fokus** 29

2.1 Einzelhandel 30

2.2 Produktion 32

2.3 Finanzwesen 34

2.4 Öffentlicher Sektor 36

2.5 KRITIS 38

**Interview: Vivien Bilquez, Zurich Resilience Solutions** 40

**03 Menschliche Sicherheitsrisken durch Social Engineering** 42

3.1 Psychologische und technische Angriffsvektoren bei Phishing-Simulationen 44

3.2 Unterschiede zwischen Personengruppen 50

**04 Das „Behavioral Security Model“** 52

**Interview: Marisa Fagan, Atlassian** 58

**05 Die Wahrnehmung der Cyber-Bedrohungslage 2021** 60

**06 Ausblick & Handlungsempfehlungen** 68

**Über SoSafe** 70

# Executive Summary

**9 von 10 IT-Experten und IT-Sicherheitsverantwortliche sagen:**

Die Cyber-Bedrohungslage hat sich verschärft. Jede dritte Organisation hat 2021 selbst einen erfolgreichen Cyberangriff erlebt.

---

**Die erfolgreichsten Phishing-Betreffzeilen 2021...**

...setzen auf die Thematisierung hybrider Arbeitsprozesse und Emotionen wie Druck und Autorität:

| | |
|---|---|
| 66 % | Folgende Aufgabe ist zu erledigen: Verteilung der Dokumente und Aufgabenprüfung |
| 66 % | Sie haben 2 Erwähnungen |
| 57 % | Wichtig: CORONA Update |

**Die Top 5 Cybercrime-Trends 2022**

01 3 von 4 Befragten geben an, dass sich durch hybride Arbeitsmodelle die Angriffsmöglichkeiten und Erfolgschancen von Cyberkriminellen erweitert haben. Mehr als 80 % sehen eine Kombination technischer und organisatorischer Maßnahmen als Lösung.

02 Die ENISA spricht von der „goldenen Ära für Ransomware“. Komplexe Angriffstaktiken wie Mehrfacherpressungen erhöhen dabei die Gefahr von Datenmissbrauch um knapp 800 %. Auch die Menge an Malware erreichte laut AV-Test 2021 einen neuen Höhepunkt – mehr als 150 Millionen Schadprogramm-Varianten wurden erkannt, davon 59 % Trojaner.

03 Groß angelegte Supply-Chain-Angriffe zielen auf schwache Glieder in Lieferketten und legen ganze Versorgungssysteme lahm.

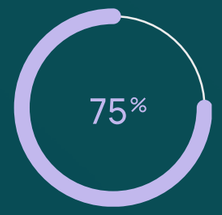
04 Der Ausbau von KI-as-a-Service-Angeboten ermöglicht Cyberkriminellen tückische, neue Angriffstaktiken wie Deepfakes, Voice Cloning und automatisiertes und damit massentaugliches Spear Phishing.

05 Phishing und Social Engineering bleiben Dauerbrenner unter den Angriffsmethoden und werden anlassbezogen weiterentwickelt. Fast jede dritte Person klickt auf schädliche Inhalte in Phishing-Mails.





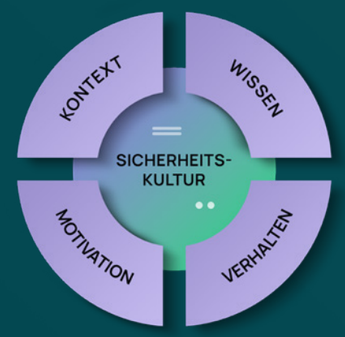
**Europaweit verschärfte Cyber-Security-Regularien erhöhen die Haftungsrisiken für Führungskräfte.**



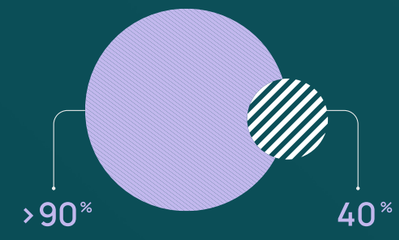

Gartner geht davon aus, dass bei cyber-physischen Vorfällen schon bis 2024 75 % der CEOs persönlich haften werden.

> “Der Mensch ist definitiv der wichtigste Faktor für die Cyberresilienz von Organisationen.”
>
> **Vivien Bilquez,** Principal Cyber Risk Engineer bei Zurich Resilience Solutions

**Das Behavioral Security-Modell: Psychologisch fundierte Awareness-Maßnahmen minimieren menschliche Risiken um bis zu 90 %.**



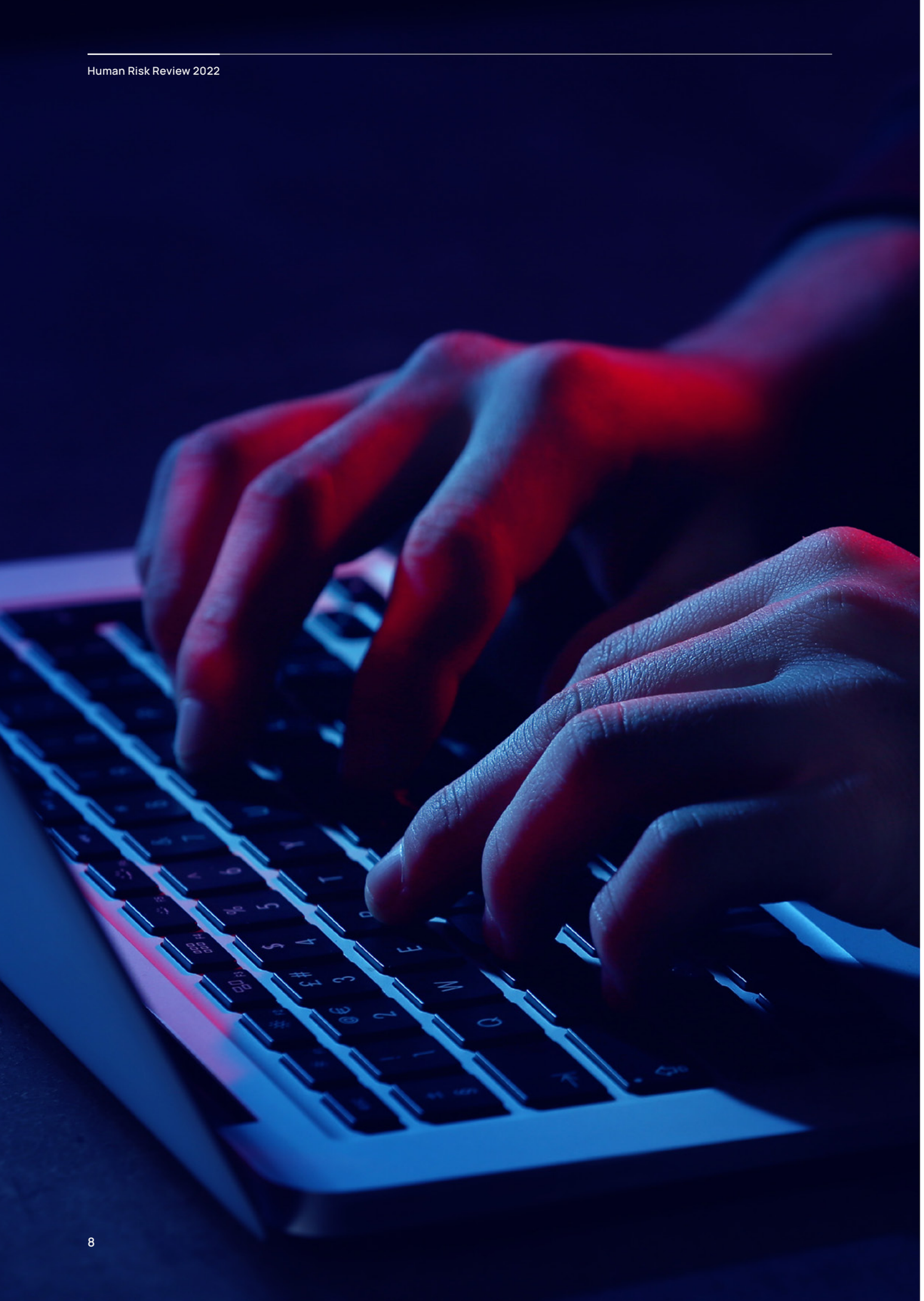

**Mehr als 90 % der IT-Experten und IT-Sicherheitsverantwortlichen sagen:**




Awareness sei wichtig in ihrer Organisation. Doch 40 % dieser Organisationen geben an, das Awareness-Level der Mitarbeitenden sei niedrig. Mehr als zwei Drittel der Befragten planen deshalb, ihre Awareness-Maßnahmen im kommenden Jahr auszuweiten.


**Nahezu einstimmig geben 99 % der Befragten an, dass im nächsten Jahr das Stärken der organisationseigenen Sicherheitskultur wichtig sein wird.**

> „Es braucht entscheidungsfreudige und leitende Hand auf Führungsebene.“
>
> **Achim Berg,** Präsident des Bitkom







# 01 Die Cyber-Bedrohungslage: Alte Bekannte und neue Extreme

## Ein Blick auf einige alarmierende Zahlen und Fakten aus dem vergangenen Jahr

Auch im Jahr 2021 konnten wir in Sachen Informationssicherheit nicht aufatmen. Cyberkriminelle professionalisieren sich seit Jahren zusehends und entwickeln ihre Methoden stetig weiter. Viele ihrer Taktiken sind längst zu einem eigenen Geschäftsmodell geworden und Cybercrime-as-a-Service boomt.[1]

### Mit Billionen-Dollar-Schäden ist Cybercrime weltweit Geschäftsrisiko Nr. 1

Im zweiten Pandemie-Jahr standen laut einer Umfrage der Allianz-Versicherung Cybervorfälle weltweit auf Platz 1 der größten Business-Risiken.[2] Schon der Report aus dem Vorjahr bezifferte die Kosten der Cyberangriffe für die Weltwirtschaft auf unglaubliche 1 Billionen Dollar – 50 Prozent mehr als noch vor zwei Jahren.[3] Andere Quellen gehen von noch höheren Schadenssummen aus. Auf der RSA Conference 2021 sprach Cisco CEO Chuck Robbins von 6 Billionen Dollar Schaden pro Jahr.[4]

### Mehr als 800 % erhöhte Gefahr von Datenmissbrauch bei Ransomware

Gerade Ransomware-Angriffe haben sich zuletzt deutlich ausgeweitet, vor allem solche mit dem Ziel der Mehrfacherpressung. Die Gefahr, dass gestohlene Daten bei Ransomware-Attacken veröffentlicht werden, stieg durch den Einsatz dieser Taktik

1 Forbes (2021). The Destructive Rise of Ransomware-As-A-Service.
2 Allianz (2022). Allianz Risk Barometer 2022: Cyber perils outrank Covid-19 and broken supply chains as top global business risk.
3 Allianz (2021). Allianz Risk Barometer – Identifying the major business risks for 2021.
4 SDX Central (2021). Cisco CEO: Cybercrime Damages Hit $6 Trillion.

von 8,7 Prozent im Jahr 2020 auf 81 Prozent im zweiten Quartal 2021.[5] Gleichzeitig lagen die durchschnittlichen Kosten einer Datenschutzverletzung 2021 laut IBM mit 4,24 Millionen US-Dollar höher als je zuvor.[6] Durch geopolitische Auseinandersetzungen wird die Weiterentwicklung von Ransomware zusätzlich vorangetrieben und die Konflikte mithilfe der Taktik auch im Cyberspace ausgetragen. Im Kontext des Angriffskriegs Russlands auf die Ukraine schlug sich so beispielsweise die Ransomware-Gruppe Conti auf die Seite des Kremls, um unter anderem ukrainische KRITIS-Organisationen anzugreifen (mehr dazu Seite 24).[7]

## Unerwartete Schwachstelle in Java-Logging-Bibliothek sorgt für Schäden in Millionenhöhe

Keine 72 Stunden nach Bekanntwerden der Log4j-Sicherheitslücke im Dezember 2021 konnten weltweit bereits 800.000 Cyberattacken festgestellt werden, die diese ausnutzten.[8] CISA-Direktorin Jen Easterly sprach von „den schwerwiegendsten Schwachstellen [ihrer] Karriere".[9] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rechnet mit Schaden in Millionenhöhe – allein für die deutsche Wirtschaft.[10]

## Der „König der Schadsoftware" Emotet ist zurück – und stärker als je zuvor

Nachdem internationalen Behörden um Europol Anfang 2021 der Takedown der gefährlichen Schadsoftware „Emotet" gelungen war, kehrte sie weniger als ein Jahr später mit voller Wucht zurück. Seit November 2021 ist der Trojaner wieder aktiv und nutzt die Infrastruktur des Banking-Trojaners Trickbot, um beispielsweise über Spam-Mails und kompromittierte Excel-Dateien auf Systeme zuzugreifen. Internationale Behörden gehen einheitlich davon aus, dass es in den kommenden Monaten wieder zu Angriffswellen kommen wird.[11]

5 European Union Agency for Cybersecurity (ENISA) (2021). ENISA Threat Landscape 2021.
6 IBM (2021). How much does a data breach cost?
7 TechCrunch (2022). Conti ransomware gang's internal chats leaked online after declaring support for Russian invasion.
8 Ars Technica (2021). Hackers launch over 840,000 attacks through Log4J flaw.
9 National Security Agency (2021). CISA, FBI, NSA, and International Partners Issue Advisory to Mitigate Apache Log4J Vulnerabilities.
10 Spiegel (2021). Log4j-Schwachstelle könnten Millionenschäden zur Folge haben.
11 Dark Reading (2022). Emotet is Back and More Dangerous than Before.

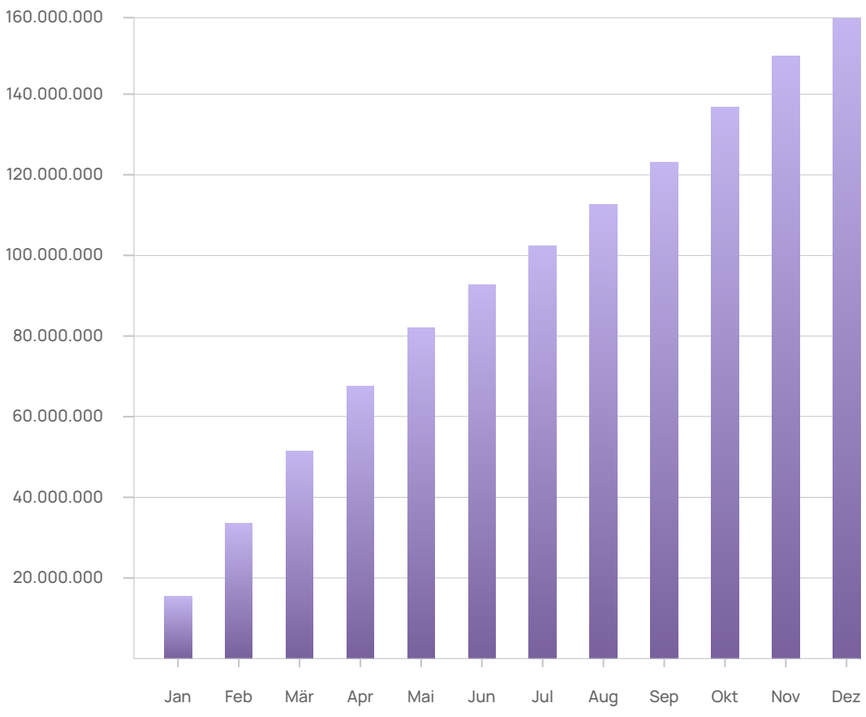




# 1.1 Malware zeigt ungebrochenen Aufwärtstrend

Diese Analyse stützt sich auf Daten aus der AV-ATLAS Threat Intelligence Plattform der AV-TEST GmbH, welche Schadsoftware (auch: Malware) vollautomatisch analysiert und klassifiziert und so umfassende Vergleichstests ermöglicht.[12]

## Anzahl neu erkannter Malware-Typen 2021

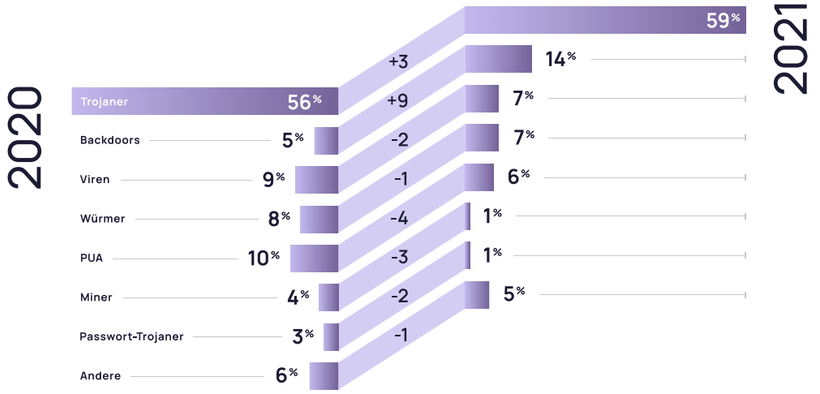



2021 wurden über 160 Millionen neue Malware-Typen erkannt – mit je über 15 Millionen neuen Schadprogrammen besonders viele davon zwischen Januar und April. Insgesamt liegt die Gesamtmenge nun bei über einer Milliarde erkannten Schadprogrammen seit 2008 – und ist damit mehr als doppelt so hoch wie noch vor fünf Jahren.





## Häufigkeit verschiedener Malware-Typen 2020 vs. 2021




Mit fast zwei Dritteln der Gesamtmenge an Kategorien machen Trojaner auch 2021 den Hauptteil der erkannten Schadprogramme aus. Im Vergleich zum Vorjahr ist ein deutlicher, anteiliger Zuwachs bei Backdoor-Attacken zu erkennen, die mit 14 Prozent nun fast dreimal so häufig sind wie zuletzt. Sie werden häufig über Trojaner oder Phishing-Mails verbreitet und über User so unwissentlich in die Systeme geschleust. Der Anteil an Potenziell Unerwünschten Anwendungen (kurz: PUA) wie Adware ist dagegen gesunken.

Angriffe über Schadsoftware sind also weiterhin ein gefährliches Risiko für Organisationen und die Weiterentwicklung der Typen macht eine rein technische Prävention schwierig bis unmöglich. Ein Großteil der erkannten Malware-Kategorien wie Trojaner (darunter fällt auch der „König der Schadsoftware" Emotet[13]) und Backdoors nutzen den Menschen als Tor zu sensiblen Daten und Systemen. Wie schon zuvor beschrieben, setzen Kriminelle dabei zunehmend auf Erpressungstrojaner, sogenannte Ransomware. Im Frühjahr 2022 wurden interne Chatverläufe und sensible Daten aus der Arbeit der Ransomware-Gruppe Conti geleakt. Dabei kam heraus, dass die Beteiligten über solche Angriffe im vorausgegangenen Jahr vermeintlich knapp 200 Millionen US-Dollar Umsatz[14] gemacht hatten. Damit bleiben Mitarbeitende die wichtigste Schutzbarriere in Organisationen, denn die professionalisierten Cybercrime-Geschäftsmodelle setzen genau dort an – beim Menschen.

12 AV-TEST – The independent IT-Security Institute (2022). AV-ATLAS.

13 Bundesamt für Sicherheit in der Informationstechnik (2021). Emotet-Infrastruktur zerschlagen – BSI informiert Betroffene.

14 Krebs on Security (2022). Conti Ransomware Group Diaries, Part III: Weaponry.

# 1.2 Die größten Cybercrime-Trends


## 1.2.1 Anlassbezogene Phishing-Angriffswellen: Skrupellose Täuschungen

Phishing ist und bleibt der Dauerbrenner unter den Angriffstaktiken der Cyberkriminellen. Sie greifen dabei aktuelle Themen und Entwicklungen immer schneller für zielgenaue Angriffe auf – besonders dann, wenn sie Angst als Motiv nutzen können. So bot ihnen beispielsweise die Pandemie bereits 2020 optimale Ausgangschancen für dieses Vorgehen. Auch 2021 hielten die Cyberkriminellen ihre Füße nicht lange still und griffen ihre Opfer ohne Skrupel in einer höchst verwundbaren Situation an.

Bereits wenige Wochen nachdem die COVID-19 Omikron-Variante weltweit bekannt wurde, griff ein erster Phishing-Betrug das Thema auf. Als Nationaler Gesundheitsdienst (NHS) getarnt, boten die Betrügenden im Dezember 2021 vermeintlich kostenlose PCR-Tests an, die angeblich speziell für den Nachweis der Omikron-Variante entwickelt wurden. Bürgerinnen und Bürger in ganz Großbritannien wurden per SMS, E-Mail oder sogar per Telefon kontaktiert und zur Herausgabe persönlicher Daten manipuliert. Über eine fingierte Bestellmaske baten die Cyberkriminellen ihre Opfer etwa dazu, ihre Namen und Adressen sowie ihre Bankdaten preiszugeben und hochsensible Sicherheitsfragen zu beantworten.[15]

Ein extremer Fall solcher anlassbezogener Angriffswellen: Der Angriffskrieg Russlands auf die Ukraine sorgte für einen beispiellosen Anstieg an Cybercrime-Aktivitäten





(mehr dazu Seite 24). Dabei wurden nicht nur regierungsnahe Organisationen auf sowohl russischer als auch ukrainischer Seite attackiert. Auch die Hilfsbereitschaft von Bürgerinnen und Bürgern wurde von den Kriminellen ausgenutzt. So wurden in den Sozialen Medien und über Phishing-Mails etwa gefälschte Spendenaufrufe verbreitet.[16] SoSafe warnte außerdem vor einer besonders perfiden Masche, bei der Links geteilt wurden, die vermeintlich DDoS-Angriffe auf russische Server und Dienste unterstützen sollten. Über die Klicks schleusten Cyberkriminelle stattdessen aber Viren und Trojaner in die Systeme von Privatpersonen.[17]

Die Vorfälle zeigen deutlich, wie wichtig es ist, die emotional manipulativen Tricks zu antizipieren und zu verstehen, um sich vor ihnen und den oftmals kostspieligen Folgen schützen zu können – sowohl im privaten als auch insbesondere im beruflichen Kontext.

## 1.2.2 Supply-Chain-Angriffe: Gewinnmaximierung durch gezielte Attacken auf Dienstleister

Bereits 2020 häuften sich gezielte Angriffe auf Lieferketten. 2021 gab es einen weiteren Anstieg dieser sogenannten Supply-Chain-Attacken, bei denen über vermeintlich schwache Glieder in der Lieferkette gleich mehrere Unternehmen attackiert werden – mit zum Teil weitreichenden Folgen. Gruppen wie REvil, BlackMatter oder DarkSide machten so beispielsweise mit groß angelegten Angriffen auf die HR-Plattform Kronos, das Ölpipelinesystem Colonial Pipeline und den Fleischproduzenten JBS von sich zu hören. Unterdes attackierte die chinesische Cyber-Spionagegruppe APT27 – auch bekannt als LuckyMouse oder EmissaryPanda – vermehrt kleinere Unternehmen. Über die Lieferkette wurden anschließend weitere Opfer angegriffen, darunter insbesondere Organisationen aus dem Bereich Pharma und Technologie.[18]

Besonders eindrücklich zeigte der Ransomware-Angriff auf den IT-Dienstleister Kaseya das Ausmaß der komplexen Angriffsmethoden: Er betraf weltweit schätzungsweise 1.500 Unternehmen, unter anderem in den USA, Deutschland und den Niederlanden.[19] Über ein vermeintliches Software-Update gelangten die Täter nicht nur in die Systeme von Kaseya, sondern konnten die infizierte Software darüber

15 The Independent (2021). Scam warning over fake omicron testing text messages.
16 Zeit Online (2022). Wie können wir helfen?
17 SoSafe (2022). SoSafe warnt vor Social-Engineering-Angriffen im Kontext des Angriffskrieges auf die Ukraine.
18 Bleeping Computer (2022). German government warns of APT27 hackers backdooring business networks.






hinaus auch auf die Informationstechnik ihrer Kunden und der gesamten Lieferkette verbreiten. Auch Unternehmen, die keine direkte Beziehung zu Kaseya besaßen, waren betroffen. „Es reicht, wenn ein IT-Systemhaus, bzw. Managed Service Provider (MSP) des Unternehmens Dienste von Kaseya nutzt“, so das BSI in seiner Sicherheitswarnung.[20]

Für Organisationen wird die Auswahl ihrer Partner und das Abwägen der damit verbundenen Risiken nun immer mehr zu einem Drahtseilakt. Denn innerhalb eines Netzwerks müssen alle Akteure für eine starke Sicherheitskultur sorgen, um Gefahren effektiv abzuwenden. In Zukunft wird eine solche „Connected (Human) Resilience” also von enormer Wichtigkeit sein.

### 1.2.3 Mehrfacherpressungen: Erweiterte Ransomware-Maschen

Die ENISA spricht zurzeit von der „goldenen Ära für Ransomware“.[21] Angriffe mit horrenden Erpressungssummen dominieren die Nachrichtenspalten weltweit. Einfache Erpressungen und rein technische Angriffe gehören dabei aber der Vergangenheit an. Cyberkriminelle setzen längst auf ausgeklügelte und psychologisch versierte Erpressungstaktiken – und knüpfen weitere Angriffe an sie an. Bei diesen sogenannten Mehrfacherpressungen (Multiple Extortions) war beispielsweise von zusätzlichen DDoS-Attacken, Crypto-Mining oder auch Botnetzen zu lesen.

Doch zusätzlich zum initialen Raub und zur Verschlüsselung von sensiblen Daten (sowie der Drohung, diese bei Nicht-Zahlung zu veröffentlichen) wenden sich Angreifende mit ihren Lösegeldforderungen nun auch an die Kunden oder Partner des eigentlichen Opfers, sollte dieses nicht kooperieren. Im April 2021 griff REvil beispielsweise den Computerhersteller Quanta Computer an. Als das Unternehmen der Lösegeldforderung nicht nachging, versuchten es die Angreifenden bei Apple – einem Auftraggeber von Quanta Computer – und drohten damit, die zuvor beim Hersteller gestohlenen Daten zum neuesten MacBook Pro zu veröffentlichen. Es blieb unklar, ob die Lösegeldforderung von 50 Millionen Dollar von Apple gezahlt wurde.[22]

19 The Washington Post (2021). Ransomware attack struck between 800 and 1,500 businesses, says company at center of hack.

20 Bundesamt für Sicherheit in der Informationstechnik (2021). Kaseya - IT-Systemhäuser und deren Kunden weltweit durch SupplyChain-Attacke mit REvil-Ransomware angegriffen.

21 European Union Agency for Cybersecurity (ENISA) (2021). ENISA Threat Landscape 2021.

22 European Union Agency for Cybersecurity (ENISA) (2021). ENISA Threat Landscape 2021.; Computerbase (2021). Quanta: Angreifer stehlen Baupläne des nächsten MacBook Pro.

### 1.2.4 Künstliche Intelligenz und Deepfakes: Neue Technologien eskalieren das Angriffsgeschehen

Künstliche Intelligenz (KI) wird immer alltäglicher. Berühmte Beispiele wie Amazons Sprachassistent Alexa zeigen, wie sich intelligente Technologien den Weg in unseren Alltag bahnen – und sich zu unentbehrlichen Helfern entwickeln. Laut einer Vorhersage der International Data Corporation werden Unternehmen weltweit im Jahr 2025 mehr als 204 Milliarden US-Dollar für KI-Software ausgeben. Das entspricht einer jährlichen Wachstumsrate von 24,5 Prozent zwischen 2021 und 2025.[23] Auch im Bereich Informationssicherheit kommen immer häufiger KI-basierte Tools zum Schutz vor Angriffen zum Einsatz. Doch Cyberkriminelle haben schnell erkannt, dass sie diese Technologien ebenso für Social Engineering und Phishing nutzen und ihre Gewinne mit KI maximieren können.

Voice Phishing (Vishing) wird zum Beispiel bereits erfolgreich mit Deepfake-Technologien kombiniert und dazu genutzt, Phishing-Mails vorab zu legitimieren. Beim sogenannten „Voice Cloning" imitieren die Angreifenden die Stimme eines Vorgesetzten künstlich und bringen Mitarbeitende anschließend über einen Anruf dazu, sensible Informationen freizugeben oder Überweisungen zu tätigen. Kriminellen war es so bereits 2020 gelungen, eine Bank in Hongkong um 35 Millionen Dollar zu bestehlen.[24] Einige Quellen gehen davon aus, dass es nur eine Frage der Zeit ist, bis die KI-Technologien auch für breit angelegte, politische Desinformationskampagnen genutzt werden.[25]

### 1.2.5 Hybrides Arbeiten: Neue Arbeitsmodelle als Cyber-Gefahrenquelle

Seit Beginn der COVID-19-Pandemie steigt die Zahl der Organisationen, die auf mobiles oder hybrides Arbeiten setzen, rasant an. Sie stehen nun nicht nur vor logistischen Herausforderungen, sondern vor allem auch vor einem erhöhten Risiko von Cyberangriffen. Laut IBM sind die Kosten für Datenschutzverletzungen bei Angriffen darüber hinaus durchschnittlich 1,07 Millionen US-Dollar höher, wenn Remote Work bei dem Vorfall involviert ist.[26] Allein 2021 ist Schätzungen des Instituts für

23 International Data Corporation (2021). Investment in Artificial Intelligence Solutions Will Accelerate as Businesses Seek Insights, Efficiency, and Innovation, According to a New IDC Spending Guide.

24 Forbes (2021). Fraudsters Cloned Company Director's Voice In $35 Million Bank Heist, Police Find.

25 BBC (2020). Deepfakes: A threat to democracy or just a bit of fun?

26 IBM (2021). How much does a data breach cost?

27 Wired (2021). AI Wrote Better Phishing Emails Than Humans in a Recent Test.





INFOBOX

**Masse und Klasse dank KI – Die nächste Generation Phishing**

In einer Studie fand ein Forschungsteam der Singapurer Government Technology Agency vor kurzem heraus, dass mithilfe von KI-as-a-Service-Modellen überzeugende Spear-Phishing-Mails erstellt werden können. Die künstlich generierten Mails wurden dabei häufiger geklickt als die vom Menschen erstellten Gegenstücke.[27]

→ **Phishing im großen Stil**

Die Studie war zunächst zwar klein angelegt. Die Forschungsergebnisse bestätigen dennoch, dass Taktiken wie Spear, Voice oder Dynamite Phishing durch KI-Modelle und unzureichend kontrollierte KI-as-a-Service-Angebote massentauglich werden. Kriminelle können so legitim erscheinende Spear-Phishing-Mails ohne große Umstände oder Hintergrundwissen erstellen und versenden – und das in großer Anzahl und mit hohen Erfolgschancen.

→ **Was tun, um sich zu schützen?**

Die Ergebnisse des Singapurer Forschungsteams zeigen auch: KI-Tools, die selbst schädlichen KI-Text oder Bots erkennen sollen, sind bislang oft noch fehlerbehaftet. Sie empfehlen deshalb KI-assistierte, menschliche Schutzvorkehrungen zu treffen.

Um sich auf die Flut an automatisiert erstellten Angriffen vorzubereiten, sollten Organisationen auf die Schulung ihrer Mitarbeitenden setzen und sie zusätzlich mit Tools ausrüsten, die ihnen bei der Erkennung von schädlichen Inhalten helfen. Kontextbasierte und stets aktuelle Sensibilisierungsmaßnahmen minimieren das Risiko, einem solchen Cyberangriff zum Opfer zu fallen (siehe auch Behavioral Security Model, Seite 52).




nur **38%** der deutschen Organisationen **sichern Geschäftshandys oder Laptops** mit einer Verbindung zum Firmennetzwerk ab





Deutsche Wirtschaft zufolge so durch Cyberangriffe im Homeoffice ein Schaden von 52,5 Milliarden Euro entstanden.[28] Die Gefahr ist aus verschiedenen Gründen erhöht: Zurzeit sichern lediglich 38 Prozent der deutschen Organisationen Geschäftshandys oder Laptops mit einer Verbindung zum Firmennetzwerk ab. Darüber hinaus bieten verstärkt eingesetzte Kollaborationstools wie Microsoft Teams oder auch Mobiltelefone neue Angriffsflächen. Eine vom Security-Anbieter 1Password durchgeführte Studie in den USA und Kanada zeigt zugleich, dass auch die Mitarbeitenden selbst angreifbarer geworden sind. Von Pandemie und Homeoffice erschöpft, setzen sie sich wesentlich weniger mit Sicherheitsrichtlinien auseinander – und sind so fehleranfälliger. Das gelte auch und insbesondere für Sicherheitsverantwortliche, die durch die Veränderungen noch stärkerem Druck als zuvor ausgesetzt sind.[29]

Der folgenreiche Ransomware-Angriff auf Colonial Pipeline im April 2021 konnte beispielweise einem Angriff auf ein VPN-Netzwerk zugeschrieben werden, welches Mitarbeitende zum Arbeiten aus dem Homeoffice verwendeten. So fiel ein unvorsichtig genutztes Passwort in die Hände der Cyberkriminellen und ermöglichte den Zugriff auf den VPN-Account und zahlreiche interne Systeme und Daten.[30] Die Folgen: Eine wochenlange Versorgungsunterbrechung mit Benzin an der US-amerikanischen Ostküste. Eine klare Mehrheit der IT-Experten und IT-Sicherheitsverantwortlichen in Organisationen bestätigen das Risiko, das hybride Arbeitsmodelle mit sich bringen: 9 von 10 Befragten für diesen Report geben an, dass sich die Bedrohungslage verschärft hat. Davon sagen 75 Prozent, dass mobile Arbeitsmodelle hier eine Rolle gespielt haben. Schon der Human Risk Review 2021 zeigte: Der Erfolg von Phishing-Attacken ist bei dezentralem im Vergleich zu zentralem Arbeiten um das Dreifache erhöht. Mehr als zwei Drittel der Befragten möchten deshalb ihre Awareness-Maßnahmen im kommenden Jahr erweitern (mehr dazu in Kapitel 05).

28 Engels, Barbara (2021). Cybersicherheit. 52,5 Mrd. Euro Schaden durch Angriffe im Homeoffice, IW-Kurzbericht, Nr. 54, Köln.

29 ZDNet (2021). Everyone is burned out. That's becoming a security nightmare.

30 Bloomberg (2021). Hackers Breached Colonial Pipeline Using Compromised Password.

# 1.3 Globale Bedrohungen sorgen für verschärfte Regularien

1,6 Milliarden Euro: So viel investiert die Europäische Union (EU) im Rahmen des Projekts „Digitales Europa“ bis 2027 in Cybersicherheit.[31] Mit der Neufassung der NIS-Richtlinie „NIS 2“ sollen Cybersicherheitsstandards in den EU-Mitgliedsstaaten vereinheitlicht werden.[32] Und auch im Bereich der organisierten Kriminalität gehören Cyberangriffe EU-weit längst zu den Top 10 der priorisierten Themen.[33] Je professioneller Cyberkriminalität wird, desto sektoren- und grenzübergreifender werden auch die Angriffe zukünftig ausfallen. Das erfordert Zusammenarbeit zwischen verschiedenen Ländern sowie zwischen Staaten und privatwirtschaftlichen Unternehmen.

## Neue Verordnungen und Haftungsrisiko für CEOs

Neben europaweiten Regelungen wie der Datenschutzgrundverordnung (DSGVO) ziehen branchenspezifische Regularien wie das Krankenhauszukunftsgesetz (KHZG) oder die „Bankaufsichtliche Anforderungen an die IT-Sicherheit“ (BAIT) Unternehmen verstärkt in die Pflicht. So wird Informationssicherheit immer mehr Teil der unternehmerischen Verantwortung. Längst ist das Thema nicht nur relevant für IT-Sicherheitsexpertinnen und -experten, sondern vielmehr auch Chefsache. Für die Geschäftsführung von GmbHs und Vorstände von Aktiengesellschaften gilt: Sie müssen das Unternehmen vor Schäden schützen. Kann im Falle eines Cyberangriffs nicht nachgewiesen werden, dass ausreichende Schutzmaßnahmen getroffen wurden, haftet immer öfter die Geschäftsführung. Besonders pikant wird es, wenn es um Physical-Security-Vorfälle geht (siehe auch „Sektoren im Fokus“, Seite 29).

31 Europäischer Rat (2021). Cybersicherheit: Wie die EU Cyberbedrohungen begegnet.

32 Bundesverband der Deutschen Industrie (2021). Cybersicherheit in der EU: NIS 2-Richtlinie.

33 Europäischer Rat (2021). Bekämpfung der organisierten Kriminalität: Rat legt zehn Prioritäten für die nächsten vier Jahre fest.





## Das müssen Unternehmen jetzt beachten

### → IT-Sicherheitskultur etablieren

Auch in Zukunft werden Unternehmen mehr und mehr gesetzlich dazu aufgefordert werden, aktiv Schutzmaßnahmen gegen cyberkriminelle Angriffe zu ergreifen. Dabei reichen allein technische Maßnahmen nicht aus. Binden Sie alle Mitarbeitenden ein und sensibilisieren Sie sie für potenzielle Gefahren, um sich umfassend abzusichern.

### → Compliance-Nachweise sicherstellen

Nachweise für Zertifizierungen wie TISAX, BAIT oder auch die ISO/IEC-27001-Zertifizierung werden immer flächendeckender über alle Branchen hinweg benötigt. Unternehmen sollten sich schon heute darum kümmern, entsprechende Nachweise vorweisen zu können. Mit entsprechenden Lösungen und Compliance-Dashboards sind Sie auf der sicheren Seite.

### → Zusammenarbeit mit Expertinnen und Experten

Regelmäßige Zusammenkünfte zwischen CISOs, IT-Sicherheitsverantwortlichen und der Führungsetage geben einen Überblick über die aktuellen Sicherheitsprogramme des Unternehmens und neueste Richtlinien. Das erleichtert Ihnen die weitere gemeinsame Sicherheitsstrategie- und Budgetplanung.

### → Regelmäßiges Reporting an die Geschäftsführung

Um die Relevanz des Themas Informationssicherheit auch in der Führungsetage deutlich zu platzieren, sollten Sie regelmäßig mit Geschäftsführenden über aktuelle Risiken und den Erfolg Ihrer IT-Sicherheitsmaßnahmen sprechen. Nutzen Sie das Reporting um konkrete Zahlen vorzustellen und im Fall der Fälle schnell Entscheidungen zu treffen, beispielsweise nötige Gegenmaßnahmen schnell und effizient einleiten zu können.

# 1.4 Hybride Kriegsführung – Wie der Angriffskrieg Russlands auf die Ukraine auch im Cyber-space ausgetragen wird


Cyberkriminelle nutzen aktuelle politische, soziale und gesellschaftliche Situationen immer wieder aus, um nach dem Prinzip des Social Engineering anzugreifen (siehe auch Seite 42). Besonders extrem fallen anlassbezogene Cyber-Angriffswellen aus, wenn es um geopolitische Auseinandersetzungen geht. Kriege werden längst nicht mehr nur im physischen Raum, sondern auch im Cyberspace ausgetragen, wie erst jüngst der Angriffskrieg Russlands auf die Ukraine zeigte. Die Tragweite ist zurzeit noch schwer zu beurteilen und die Gesamtsituation aufgrund einer Vielzahl an Akteuren und Gruppen unübersichtlich.

Fest steht aber: Cyberattacken werden zur hybriden Kriegsführung eingesetzt und sollen die Handlungsfähigkeit der Gegenseite schwächen. Bei der Auswahl ihrer Angriffstaktiken sind die Bedrohungsgruppen höchstkreativ und setzen unter anderem auf Phishing, DDoS-Angriffe und Ransomware. Check Point Security zufolge ist die Zahl an Cyberangriffen auf die Ukraine allein in den ersten drei Tagen des Krieges um 196 Prozent gestiegen – in Russland dagegen nur um etwa 4 Prozent. Insgesamt habe sich die Anzahl der Phishing-Mails in ostslawischen Sprachen versiebenfacht.[34] Auch Googles Threat Analysis Group berichtet von mehreren Bedrohungsgruppen, etwa FancyBear und Ghostwriter, die mit Spionage, DDoS-Angriffen und Phishing-Kampagnen im Konflikt mitmischen.[35] Vor allem KRITIS-Organisationen wie Banken, Versorger und Versicherer stehen seit Kriegsbeginn unter digitalem Beschuss. Als Reaktion auf westliche Sanktionen gelangen aber auch weitere Organisationen weltweit ins Fadenkreuz.[36]

34 Check Point Security (2022). Cyber Attack Trends In The Midst Of Warfare – The numbers behind the first days of the conflict.

35 Google (2022). An update on the threat landscape.

36 Spiegel Netzwelt (2022). Cyberangriff auf deutsche »Hochwertziele« könnte schon bald starten.

37 Handelsblatt (2022). Anonymous hackt die größte russische Bank und Moscow Exchange.

38 Bundesamt für Sicherheit in der Informationstechnik (BSI) (2022). Einschätzung der aktuellen Cyber-Sicherheitslage in Deutschland nach dem russischen Angriff auf die Ukraine.

Die Ransomware-Gruppe Conti, die für großangelegtes „Big Game Hunting“ (also Angriffe auf große Konzerne) bekannt ist, verkündete, sie stünde auf der Seite Russlands – kurz darauf wurden interne Chatverläufe und sensible Daten des „Unternehmens“ selbst geleakt. Der Cyberwar ist also nicht einseitig, es werden auch Gegenangriffe verzeichnet, zum Beispiel vom Hacker-Kollektiv Anonymous. Und: Anonymous rief weitere Hacker-Kollektive zum Angriff auf russische Aggressoren und Verbündete auf.[37]

Neben der nicht zu bemessenden Zerstörung und den physischen und psychischen Folgen, die der Angriffskrieg auf Betroffene hat, zeichnen sich für Organisationen auch „Spill-Over-Effekte” ab. In einer digitalen, vernetzten Welt werden sich Cyber-angriffe auf KRITIS in Windeseile auf Lieferketten (auch Software-Lieferketten) verteilen – und damit die Online-Sicherheit von Organisationen weltweit auf die Probe stellen. SoSafe rät Organisationen deshalb in diesen unsicheren Zeiten unbedingt zu erhöhter Wachsamkeit. Warnungen vor Ransomware und trügerischen Social-Engineering-Kampagnen – auch auf Einzelpersonen – fallen in eine ohnehin ange-spannte Cyber-Bedrohungslage. Das BSI stuft die Lage in Deutschland momentan als „orange” ein, somit als „geschäftskritisch”.[38] Auch die US-amerikanische Cyber-security & Infrastructure Security Agency (CISA) und das britische National Cyber Security Centre (NCSC) raten dazu, die Lage genau im Blick zu behalten und schüt-zende Maßnahmen einzuleiten. Fahren Sie Ihre Schutzmaßnahmen entsprechend hoch und stellen Sie sicher, dass Sie alle notwendigen Schritte zur Absicherung Ihrer Organisation vorgenommen haben – auch aus Haftungsgründen. Dazu gehören auch Business-Continuity-Pläne, damit Sie im Ernstfall weiter handlungsfähig bleiben. Und: Cyber Security ist mehr als nur IT – Cyber Security ist eng mit der physischen Sicherheit von Menschen weltweit verbunden. Führungskräfte aus allen Bereichen sollten deshalb zusammen an ganzheitlichen Lösungen arbeiten und gemeinsam starke Sicherheitsstrategien aufbauen und umsetzen.

# Achim Berg, Bitkom

> „Es braucht leitende und entscheidungsfreudige Hand auf Führungsebene.“

**Achim Berg** ist **Präsident des Digitalverbands Bitkom**, war lange Zeit in Führungspositionen in IT-Konzernen wie Microsoft tätig und ist mittlerweile als Partner bei General Atlantic und Aufsichtsratsmitglied in mehreren Digitalunternehmen aktiv, darunter Flix und powercloud.

**Welche Rolle spielt Informationssicherheit in Ihrem beruflichen und auch privaten Alltag?**

Informationssicherheit begegnet mir und uns ständig im Alltag, häufig auch unterbewusst, etwa bei der routinemäßigen Nutzung von Zwei-Faktor-Authentifizierung, verschlüsselter Kommunikation oder beim automatisierten Backup. Die Gewährleistung der informationstechnischen Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität spielen für mich persönlich, aber auch für die gesamte Wirtschaft und Gesellschaft, eine zentrale Rolle im beruflichen wie privaten Alltag.

**Der Bitkom hat vor kurzem Ergebnisse veröffentlicht, die zeigen, dass 8 von 10 Internet-Nutzer:innen im vergangenen Jahr Opfer von Cyberkriminalität geworden sind. Wie schätzen Sie die allgemeine Bedrohungslage im Netz ein?**

Die Bedrohungslage im Cyberraum ist angespannt. Kein Unternehmen, keine Behörde und keine Einzelperson ist in der heutigen Zeit vor Cyberangriffen sicher. Die Vielzahl an potenziellen Einfallstoren stellt gerade Unternehmen vor große Herausforderungen. Während ein Großteil der Angriffe mit Phishing und Social Engineering beginnt, öffnen natürlich auch ungepatchte Systeme den Kriminellen Tür und Tor. Im Endeffekt ist es unerheblich, ob die Angreifer per Phishing, Supply-Chain-Angriff oder über 0-/n-Day Schwachstellen, fehlkonfigurierte Cloud-Umgebungen, Schatten-IT oder Innentäter zum Ziel kommen. Die kriminelle Energie findet ihren Weg. Deshalb ist es entscheidend, sich für den Ernstfall zu wappnen und sich mit dem Thema Cybersicherheit proaktiv auseinanderzusetzen.

**Wir haben in diesem Jahr spektakuläre Phishing- und Ransomware-Fälle gesehen – mit entsprechend kostspieligen Folgen. Nehmen Sie eine Zunahme der Bedeutung des Themas in Vorstandsetagen wahr?**

Definitiv. Cybersicherheit darf nicht unkoordiniert in den Händen von vielen liegen. Es braucht einen zentralen erantwortungsbereichs auf Führungsebene, wo Prioritäten festgelegt und Budgets kanalisiert werden. Nur so kann eine gesamtheitliche Sicherheitskultur gefördert und ein robustes Sicherheitsmanagement aufgebaut werden. Neben der technischen und organisatorischen Säule spielt der Faktor Mensch dabei natürliche eine ebenso wichtige Rolle.

**Welche Rolle spielen Führungskräfte im Bereich Informationssicherheit?**

Die Führungskräfte haben im Bereich Informationssicherheit eine wichtige Vorbildfunktion, da sie mit der Priorisierung des Themas in die Belegschaft hineinwirken. Ein zentrales Problem ist, dass Cybersicherheit noch viel zu oft rein technisch und als Aufgabe der IT-Abteilung verstanden wird. Dort soll das Thema dann häufig gelöst werden. Leider greift das zu kurz. Neben technischen Lösungen gehört zu einem robusten Sicherheitsmanagement eben auch, Mitarbeitend zielgruppengerecht zu schulen, Prozesse für den Notfall aufzusetzen und das Sicherheitskonzept regelmäßig zu überprüfen. Hierfür braucht es die leitende und entscheidungsfreudige Hand auf Führungsebene.

**Was sind Ihrer Meinung nach die wichtigsten Entwicklungen, die Organisationen im Bereich Informationssicherheit im kommenden Jahr im Blick behalten sollten?**

Aus Sicht eines normalen Unternehmens ist es wichtig, gar nicht so stark nach außen zu schauen und neue Entwicklungen zu verfolgen. Vielmehr muss der Blick nach innen gerichtet werden. Bin ich für den Ernstfall gerüstet? Falls ja, funktioniert mein Notfallmanagement auch in der Praxis? Sollte ich mich nicht doch dazu entscheiden ein Informationssicherheitsmanagementsystem aufzubauen, um präventiv vor die Welle zu kommen? Stellen wir genügend Ressourcen – sowohl personell als auch finanziell – bereit? Diese und weitere Fragen sollten offen und ehrlich in den Unternehmen diskutiert werden. Darauf kommt es an.

**Das letzte Jahr hat die Bedrohungslage rund um den Faktor Mensch noch einmal erhöht. Sind wir in diesem Bereich in Deutschland und Europa optimal aufgestellt?**

Digitalisierung und Cybersicherheit sind zwei Seiten einer Medaille. Mit der schleppenden Digitalisierung in Deutschland gehen leider unzureichende digitale Kompetenzen in der Breite einher. Das wirkt sich natürlich auch unmittelbar auf die Cybersicherheit aus. Gleichwohl haben wir in Deutschland und Europa eine hervorragende Ausgangsposition, wenn es um die IT- und Cybersicherheit geht. Unsere Forschung zählt zur internationalen Spitze und wir haben viele sehr starke und hochinnovative heimische IT-Sicherheitsunternehmen. Das müssen wir nutzen.

**Was sind die drei wichtigsten Aspekte für eine ausgewogene Informationssicherheitsstrategie?**

Es ist absolut entscheidend, eine gesamtheitliche Sicherheitskultur im Unternehmen zu fördern und ein robustes Sicherheitsmanagement aufzubauen. Sicherheit ist ein Prozess und keine Einmallösung. Dieses Verständnis muss in Unternehmen und Behörden gelebt werden. Konkret ist es also die Balance der drei Säulen: 1. Technik, 2. Organisation und 3. Mensch.



# 02 Sektoren im Fokus: Branchenspezifische Cyberrisiken und Regulierungen

Mit der Professionalisierung von Cybercrime geht auch die Spezialisierung von Angreifenden auf die einzelnen Sektoren und Branchen einher. Jede Branche steht so mit ihren eigenen Herausforderungen und Schwachstellen im Fokus von Cyberkriminellen. Wir zeigen auf, womit ausgewählte Industrien im Bereich Informationssicherheit besonders kämpfen und welche Maßnahmen in Zukunft schützen.

# 2.1 Einzelhandel
# Überstürzte Digitalisierung und global vernetzte Lieferketten

### Gerade der Einzelhandel spürte in den letzten zwei Jahren die Schnelligkeit der voranschreitenden Digitalisierung

Lockdown-bedingte Schließungen von Ladenlokalen und die Zunahme von Online-Bestellungen verlagerten zahlreiche Prozesse in den digitalen Raum. Viele lokale Händler stiegen erstmals in das Onlinegeschäft ein – und sind oft noch unzureichend vorbereitet auf die damit einhergehenden Risiken.

Retail-Unternehmen sind durch die Arbeit mit sensiblen Kundendaten ohnehin ein attraktives Ziel für Cyberkriminelle. Gleichzeitig ist die Sensibilisierung für Cyber-gefahren durch eine hohe Fluktuation von Mitarbeitenden und saisonbedingte Hochzeiten eine Herausforderung, die gemeistert werden muss.

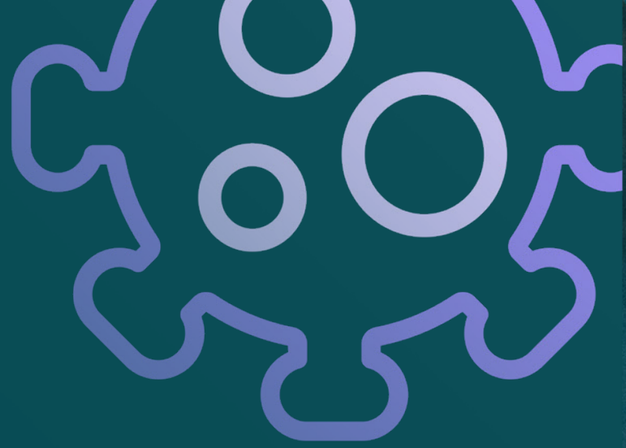
Gerade zu umsatzstarken Zeiten wie im Weihnachtsgeschäft oder am Black Friday warnen etwa das BSI und die US-Behörden immer wieder vor einer erhöhten Bedrohungslage.[39] Eine von SoSafe gestartete Phishing-Simulations-Kampagne zum Black Friday zeigt außerdem: Phishing-Angriffe mit Bezug auf aktuelle Ereignisse erhöhen die durchschnittliche Klickrate um mehr als 120 Prozent.

39 Süddeutsche Zeitung (2021). BSI befürchtet Cyberattacken auf den Handel am Black Friday.

40 CPO Magazine (2021). IKEA Suffers Ongoing Phishing Attacks From Compromised Internal and Vendor accounts.

41 BBC (2021). Swedish Coop supermarkets shut due to US ransomware cyber-attack.





### Fallbeispiel: IKEA kämpft mit Reply-Chain-Attacke

Kurz vor dem Weihnachtsgeschäft 2021 wurde der schwedische Möbelhersteller IKEA das Ziel von Cyberkriminellen, die mit Hilfe gestohlener E-Mail-Credentials eine Reply-Chain-Attacke gestartet hatten.[40] Dabei verwendeten sie echte IKEA-Mail-Adressen, um Schadsoftware wie Emotet oder Qbot intern oder an Partner in der Lieferkette zu verschicken.

Diese Art des Phishings ist besonders gefährlich, da Mitarbeitende die bösartigen E-Mails nur schwer erkennen können. Obwohl im Fall von IKEA größere Schäden durch eine frühzeitige Reaktion seitens der Organisation ausblieben, zeigt er, wie professionell Angreifende mittlerweile vorgehen. Einzelhändler sehen sich dabei dem Risikokost-spieliger Geschäftsunterbrechungen gegenüber-gestellt. Der schwedische Supermarkt Coop musste nach einer Cyberattacke im Sommer 2021 beispielsweise circa 500 Filialen vorübergehend schließen.[41]

# 2.2 Produktion
# Industrie 4.0, kostspielige Produktionsstopps und exklusive immaterielle Güter






## Neue Angriffsflächen machen die Produktion zum Ziel Cyberkrimineller

Vor einigen Jahren wogen sich Produktionsunternehmen noch in relativer Sicherheit vor Cyberattacken. Doch seit der umfassenden Digitalisierung im Kontext von Industrie 4.0 und Connectivity sind neue Angriffsflächen entstanden. Unternehmen der Branche sind besonders durch Angriffe auf Lieferketten und daraus entstehende Produktionsausfälle verwundbar. Durch Schadsoftware herbeigeführte, kostspielige Stopps der Anlagen bieten Cyberkriminellen eine ideale Grundlage für Erpressungen.

Die Automobilbranche reagiert auf die wachsenden Risiken, indem sie bereits großflächig einen Standard in der Informationssicherheit voraussetzt: Ohne eine Trusted Information Security Assessment Exchange-Zertifizierung, kurz TISAX, sind Hersteller, Lieferanten oder Dienstleister aus dem Automobilsektor heute kaum mehr wettbewerbsfähig. Die Sensibilisierung aller Akteure innerhalb der Lieferkette durch umfassende Awareness-Maßnahmen schützt nicht nur zuverlässig vor erfolgreichen Cyberangriffen, sondern stellt auch die TISAX-Compliance sicher. Ein Nachweis erfolgt am einfachsten über spezielle Compliance-Dashboards.

## Fallbeispiel: Ransomware legt IT-Infrastruktur bei Eberspächer lahm

Die anhaltende Corona-Pandemie und der Halbleitermangel machte es Unternehmen aus der Automobilindustrie 2021 nicht leicht. Autozulieferer Eberspächer wurde im Oktober 2021 Opfer eines Ransomware-Angriffs.

Das Familienunternehmen aus Baden-Württemberg beschäftigt rund 10.000 Mitarbeitende an 80 Standorten in 28 Ländern. Es gehört weltweit zu den umsatzstärksten Zulieferern, unter anderem für Fahrzeugelektronik. Der Angriff beeinträchtigte die IT-Infrastruktur des Familienunternehmens massiv; die Website war zeitweise nicht mehr aufrufbar, sämtliche IT-Systeme wurden zum Schutz heruntergefahren.[42] Im Dezember 2021 gab unterdes der Autobauer Volvo den Diebstahl von vertraulichen Forschungsdaten bekannt.[43]

42 Eberspächer (2021). Nach Hackerangriff auf Eberspächer Group.
43 Volvo Cars (2021). Notice of cyber security breach by third party.

# 2.3 Finanzwesen
# Sensible Daten und zunehmend strikte Regulierungen

## Extremer Anstieg an Cyberattacken auf den Finanzsektor

Kredit- und Finanzdienstleistungsinstitute haben zuletzt schnellere und smartere Online-Zahlungsprozesse eingeführt – und gleichzeitig viele ihrer Mitarbeitenden ins Homeoffice geschickt. Auch bekamen Online-Banken wie N26 und andere FinTechs Aufschwung. Bereits in der ersten Lockdown-Phase zwischen Februar und April 2020 zeigte sich, dass Cyberkriminelle diesen Umschwung nutzen: Die Anzahl der Cyberattacken auf den Finanzsektor stieg um 238 Prozent.[44] Die sensiblen und persönlichen Bankdaten der Kundinnen und Kunden lassen sich auf dem Schwarzmarkt zu horrenden Summen verkaufen. Entsprechend hoch sind auch Lösegeldforderungen bei Ransomware-Angriffen. Eine Datenpanne im Finanzsektor kommt Instituten mit durchschnittlich 5,72 Millionen Dollar teuer zu stehen.[45]

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat erkannt, wie sehr gerade menschliche Risiken im Finanzwesen ausgenutzt werden. Obwohl die meisten Kredit- und Finanzdienstleistungsinstitute Schulungen zur Informationssicherheit durchführen, wurden die Anforderungen nun regulatorisch weiter verschärft. In der Neuauflage der BAIT vom August 2021 wird die Sensibilisierung von Mitarbeitenden zu Themen wie Social Engineering detailliert festgelegt. Es heißt außerdem: „Das Institut hat ein kontinuierliches und angemessenes Sensibilisierungs- und Schulungsprogramm für Informationssicherheit festzulegen. Der Erfolg der festgelegten Sensibilisierungs- und Schulungsmaßnahmen ist zu überprüfen“.[46]

[44] Allianz (2021). Financial services: Risk trends.
[45] IBM (2021). Cost of Data Breach.
[46] BaFin Rundschreiben 10/2017 (BA) in der Fassung vom 16.08.2021.
[47] Handelsblatt (2021). Sabotageangriff legt Onlinebanking bei mehr als 820 Banken lahm.
[48] Heise (2021). Cybercrime: US-Versicherung zahlte angeblich 40 Millionen als Lösegeld.





## Fallbeispiel: Imageschäden bei Volksbanken & Big-Game-Hunting bei CNA Financial

Im Juni 2021 konnten zahlreiche Kundinnen und Kunden von Volks- und Raiffeisenbanken keine Transaktionen per Onlinebanking durchführen und nicht mehr digital auf ihr Konto zugreifen. Auch Internetseiten mehrerer genossenschaftlicher Banken waren vorübergehend nicht verfügbar.

Die Ursache: Cyberkriminelle sabotierten die Rechenzentren des IT-Dienstleisters der Banken Atruvia.[47] Während die Volks- und Raiffeisenbanken in diesem Vorfall vergleichsweise glimpflich mit einem angeschlagenen Image davon kamen, ist der Cyberangriff auf den US-Versicherer CNA Financial ein klassisches Beispiel für die Großwildjagd Cyberkrimineller, sogenanntem Big Game Hunting. Der Angriff sorgte vor allem aufgrund der Lösegeldsumme für Schlagzeilen. Mit 40 Millionen US-Dollar zahlte CNA Financial die bislang höchste bekannte Lösegeld-Zahlung nach einem Ransomware-Vorfall.[48]

# 2.4 Öffentlicher Sektor
# Erhöhtes Medieninteresse als Druckmittel

## Ransomware als branchenspezifische Bedrohung

Erfolgreiche Angriffe auf Städte und Gemeinden häufen sich. Erst kürzlich warnte das Bundeskriminalamt (BKA) vor einem „neuerlichen Anstieg krimineller Cyber-Aktivitäten in Form von Ransomware-Angriffen auf öffentliche Verwaltungen“.[49] Die Folgen: Der Arbeitsbetrieb fällt wochen-, manchmal sogar monatelang aus.

Häufig ist die IT-Infrastruktur im öffentlichen Sektor veraltet, was es professionellen Angreifenden leicht macht, sich Zugriff zu verschaffen. Außerdem ist das Medieninteresse in den Fällen groß. Schließlich sind viele Bürgerinnen und Bürger auf die Leistungen von Kommunalverwaltungen wie Unterhaltszahlungen oder KFZ-Zulassungen angewiesen. Und gelangen sensible Daten in die falschen Hände, hat das auch Folgen für Einzelpersonen. Das erhöht den Druck auf die betroffene Organisation. Die Kriminellen erhoffen sich dadurch, dass ihre Lösegeldforderungen erst recht erfüllt werden.[50]

### Fallbeispiel: Erster deutscher Cyber-Katastrophenfall nach Angriff auf Landkreis

Mehrere Server des Landkreises Anhalt-Bitterfelde wurden im Juli 2021 mit Ransomware infiziert und zahlreiche Daten infolge verschlüsselt. KFZ-Anmeldungen, Elterngeldanträge und viele weitere Leistungen konnten nicht mehr bearbeitet werden.

Die Bundeswehr rückte zur Unterstützung an. Auch Monate nach dem Angriff galt noch der ausgerufene Katastrophenfall. Das Lösegeld wurde nicht gezahlt.[51] Aber die Lage verschärft sich auch andernorts: Mehr als 150 amerikanische Regierungsbehörden und Nichtregierungsorganisationen (NGO) wurden im vergangenen Jahr Opfer der Gruppe Nobelium, die auch den bekannten Angriff auf den US-Softwarehersteller SolarWinds verübte.[52] Im Frühjahr 2021 traf eine Ransomware-Attacke Spaniens Arbeitsagentur – während einer durch die Coronakrise ohnehin angespannten Lage.[53]

49 Bundeskriminalamt (2021). BKA warnt vor Cyber-Angriffen auf öffentliche Verwaltungen.

50 Stern (2021). Warum Verwaltungen für Hacker attraktiv sind – und es keinen Überblick über deren Sicherheit gibt.

51 Frankfurter Allgemeine Zeitung (2021). Erster Cyber-Katastrophenfall in Deutschland.

52 Frankfurter Allgemeine Zeitung (2021). Solarwinds-Hacker greifen amerikanische Behörden und NGOs an.

53 Infosecurity Magazine (2021). Ransomware “Paralyzes” Spanish Employment Agency.

# 2.5 KRITIS
# Cyber-physische Vorfälle mit dramatischen Folgen – und vermehrten Haftungsrisiken






## Angriffe auf Operational Technology bergen große Gefahren

Im Juli 2021 fand Gartner-Analyst Wam Voster dramatische Worte: Schon bald werde es durch cyber-physische Vorfälle Tote geben.[54] Die Vorhersage bezieht sich auf vermehrte Angriffe auf sogenannte Operational Technology (OT), mit der physische Prozesse überwacht und gesteuert werden. Sie kommt insbesondere bei Kritischen Infrastrukturen (KRITIS) zum Einsatz – also Organisationen, deren Ziel es ist, die allgemeine Versorgung sicherzustellen. KRITIS-Organisationen sind zuweilen allerdings noch auf veraltete Software angewiesen. Denn die eingesetzten Anlagen, zum Beispiel medizinische Großgeräte, sind teuer – und werden entsprechend nur selten aktualisiert oder gar gegen neue ausgetauscht. Sie sind so optimale Einstiegstore und Angriffsziele für Cyberkriminelle.

Laut Gartner ist in Zukunft gehäuft mit solchen Angriffen zu rechnen. Neben den nicht zu beziffernden persönlichen Verlusten gehen die Analysten von einem finanziellen Schaden von mehr als 50 Milliarden US-Dollar bis 2023 aus. Auch die Haftungsrisiken für Führungskräfte und Vorstände werden sich in diesem Zusammenhang weiter erhöhen. 75 Prozent der CEOs sollen schon 2024 für solche fatalen Vorfälle einstehen müssen (siehe auch Kapitel 1.3).[55] Umso wichtiger ist es, sich proaktiv zu schützen und für entsprechende Compliance-Nachweise zu sorgen, die im Fall der Fälle vor kostspieligen Konsequenzen schützen..

## Fallbeispiele: Fernsteuerung mit fast fatalen Folgen

Eine Wasseraufbereitungsanlage in Florida musste jüngst selbst erfahren, wie ein solcher Angriff aussehen kann. Eine unbekannte Person verschaffte sich über eine Remote-Access-Software Zugang zum Steuerungssystem der Anlage und passte die Natriumhydroxid-Werte auf ihr 100-faches Niveau an – ein gesundheitsgefährdendes Level.

Durch umsichtiges Verhalten eines Mitarbeitenden wurde der Angriff schnell erkannt und die Werte konnten wieder heruntergefahren werden. Das bewahrte Verbraucherinnen und Verbraucher vor dem Schlimmsten.[56]

54 Gartner (2021). Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans.

55 Gartner (2020). Gartner Predicts 75% of CEOs Will be Personally Liable for Cyber-Physical Security Incidents by 2024.

56 CNN (2021). Florida water treatment facility hack used a dormant remote access software, sheriff says.

# Vivien Bilquez, Zurich Resilience Solutions

> “Der Mensch ist definitiv der wichtigste Faktor für die Cyber-resilienz von Organisationen.”


**Vivien Bilquez** ist seit über 15 Jahren in der IT- und Cyber-Security-Branche tätig und lehrte bis vor kurzem IT- und Informationssicherheit an der Université de Lorraine. Derzeit ist er als **Principal Cyber Risk Engineer bei Zurich Resilience Solutions** tätig und unterstützt Unternehmen dabei, ihre Cybersicherheitsrisiken kontinuierlich zu reduzieren.

**In Anbetracht der jüngsten geopolitischen Veränderungen und zunehmend professionalisierter Cyberkriminalität: Was werden Ihrer Meinung nach die größten Cyberrisiken in den kommenden Monaten und Jahren sein?**

Wenn man sich die jüngsten Cybervorfälle in den Nachrichten ansieht, findet man schnell eine Gemeinsamkeit: Ransomware. Dabei ist es unerheblich, ob ein Cyberangriff von Cyberkriminellen, Insidern, Hacktivisten oder staatlichen Hackern verübt wird. Die Zahl der Ransomware-Angriffe hat sich im Jahr 2021 verdoppelt (im Vergleich zu 2020). Dabei wurden oft nicht nur Unternehmensdaten verschlüsselt, sondern diese oft auch exfiltriert und veröffentlicht. Da die Schäden durch Cybercrime in diesem Jahr voraussichtlich weiter erheblich zunehmen werden, müssen wir damit rechnen, dass auch Ransomware-Angriffe häufiger und ausgefeilter werden. Der Anstieg von Ransomware ist vor allem dem Wechsel von einem linearen Angriffsmodell zu einem heimtückischen, mehrdimensionalen Ransomware-as-a-Service-Modell (RaaS) zuzuschreiben. Bei diesem abobasierten Modell kann jeder (ein sogenannter „Affiliate“) gebrauchsfertige Ransomware-Tools verwenden, um Angriffe auszuführen und einen Anteil an jeder Lösegeldzahlung zu verdienen. Wurden Hackerangriffe in der Vergangenheit von hochqualifizierten IT-Entwicklern ausgeführt, kann heutzutage jeder Hacker werden. Dadurch vervielfacht sich die Zahl der Bedrohungsakteure und natürlich auch der Cyberrisiken.

**Was sind die wichtigsten Trends und Veränderungen, die Sie in der Cyberversicherungsbranche sehen?**

Beim Onboarding neuer Kunden oder Vertragsverlängerungen waren unsere Cyber-Risikobewertungen früher hauptsächlich technischer Natur. Da die meisten unserer Kunden Teile ihrer IT-Infrastruktur zu Drittanbietern oder in die Cloud ausgelagert haben, hat sich das im Laufe der Zeit verändert. Wir konzentrieren uns nun mehr und mehr auf Governance und Compliance sowie auf das Risikomanagement von Drittanbietern und der Cloud. Die technischen Kontrollen bleiben dabei bestehen, werden aber spezifischer. Mit dem Aufkommen von vernetzter Hard- und Software zur Steuerung von Industrieanlagen (OT – Operational Technology) oder vernetzten Objekten (IOT – Internet of Things) in Büros achten wir beispielsweise nicht mehr nur auf die Sicherheit der Informationstechnologie (IT), sondern auch auf die OT- und IOT-Sicherheit. Wir waren schon immer vorsichtig und empfehlen unseren Kunden in der Regel, IT- und OT-Umgebungen physisch zu trennen, um eine gegenseitige Kontamination zu verhindern. Ein Trend auf dem Markt ist jedoch die Zusammenführung von IT und OT, da IT-Teams die Verantwortung für die Sicherheit der physischen Geräte übernehmen. Diese integrierte Umgebung, die wir als industrielle Informationstechnologie bezeichnen, vergrößert die Angriffsfläche. Wir sollten uns auch fragen, ob die neuen Trends neue Risiken mit sich bringen. Ich persönlich befürchte, dass sich Cyberangriffe weg von einem Modell des Datendiebstahls hin zu einem Modell des Kontrolldiebstahls entwickeln. Durch die Kontrolle von Geräten, die direkt mit Menschen interagieren, könnte dies in naher Zukunft letztlich den Menschen selbst schaden.

**Wie sehen Sie den menschlichen Faktor im Bereich Cyber Security aus der Perspektive eines Risikomodells?**

Der Faktor Mensch ist wahrscheinlich der komplexeste Faktor, den es zu berücksichtigen gilt. Ich beschäftige mich in einer externen Initiative gerade damit, wie man eine “Human-Centered Security” umsetzen kann. Die Gruppe setzt sich aus Experten für Cybersicherheit (CISO) und Experten aus verschiedenen Branchen wie dem NCSC, Rechtsexperten, Neurowissenschaftlern, Awareness-Spezialisten und Technologiepartnern zusammen. Es ist wirklich interessant, die akademische Sicht den praktischen Erfahrungen, mit denen CISOs tagtäglich zu kämpfen haben, gegenüberzustellen. Der Mensch ist definitiv der wichtigste Faktor für die Cyberresilienz von Organisationen. Wenn ein Unternehmen von Ransomware getroffen wird, liegt das oft daran, dass jemand auf einen bösartigen Link in einer Phishing-Mail geklickt hat, einer Person am Telefon vertrauliche Informationen mitgeteilt hat oder sein Mobilgerät an einem öffentlichen Ort unbeaufsichtigt gelassen hat. Wie wir das vermeiden können? Awareness-Trainings, Phishing-Übungen und Rewards für Mitarbeitende sind meiner Meinung nach fundamental. Das ist ein kontinuierlicher Prozess und Unternehmen müssen diese Botschaft kreativ übermitteln. Da Mitarbeitende eins der häufigsten Einstiegstore für Cyberangriffe sind, empfehle ich immer, mit Cyber-Security-Trainings für die Führungsebene zu beginnen. Unternehmen müssen verstehen, dass sie ständig Cyberrisiken ausgesetzt sind, und sie sollten Sicherheitsziele als grundlegenden Bestandteil in ihre Gesamtstrategie einbeziehen. Das ist der Ansatz, den wir bei Zurich verfolgen. Einerseits sind die Accounts der C-Levels ein bevorzugtes Ziel für Hacker, weil sie Zugang zu den sensibelsten Informationen eines Unternehmens haben. Andererseits haben Führungskräfte eine Vorbildfunktion für den Rest des Unternehmens. Als solche müssen sie die Sicherheitskultur vorantreiben und Sicherheitsmaßnahmen jederzeit wahrnehmen. Andernfalls wird es schwierig, von allen anderen zu erwarten, dass sie die internen Security-Richtlinien befolgen.

**Viele Vorschriften werden derzeit verschärft, und die Haftung im Falle eines erfolgreichen Angriffs wird gerade für die Führungsebene zu einem kritischen Thema. Welche Rolle spielen Cyberversicherungen dabei? Welches sind jetzt die wichtigsten Handlungsfelder für die Führungsebene?**

Cyberversicherungen helfen Unternehmen, ihre finanziellen Risiken im Online-Geschäft zu verringern. Sie decken in der Regel finanzielle Verluste ab, die durch einen Cybervorfall entstehen, und umfassen standardmäßig den Schutz von Sicherheit und Privatsphäre. Haftpflichtansprüche, insbesondere gegen die Führungsebene, können durch eine spezielle D&O-Versicherung (Directors & Officers) abgedeckt werden. Um die Cyberrisiken zu mindern, würde ich C-Levels auf jeden Fall empfehlen, an mehr Cyber-Security-Trainings teilzunehmen, aber auch Table-Top-Übungen zu organisieren und daran teilzunehmen, um verschiedene Cyberszenarien zu simulieren und ihre Cyberresilienz zu testen.

**Welches sind die drei Dinge, die jeder CISO aus Sicht der Cyberversicherung im Blick haben sollte?**

Unternehmen müssen eine gewisse Cybersicherheitsreife nachweisen, um für eine Cyberversicherung in Frage zu kommen. Wenn wir die oben bereits besprochenen Elemente berücksichtigen, würde ich jedem CISO empfehlen, Folgendes zu tun:

1. Definieren, implementieren und testen Sie die Ransomware-Resilienz Ihres Unternehmens (auf IT-, aber auch auf OT/IOT-Ebene);
2. Stellen Sie ein angemessenes Risikomanagement für Dritte sicher;
3. Treiben Sie eine Sicherheitskultur und -strategie voran, die auf einem Top-Down-Ansatz beruht.

# 03 Menschliche Sicherheitsrisiken durch Social Engineering – eine Analyse

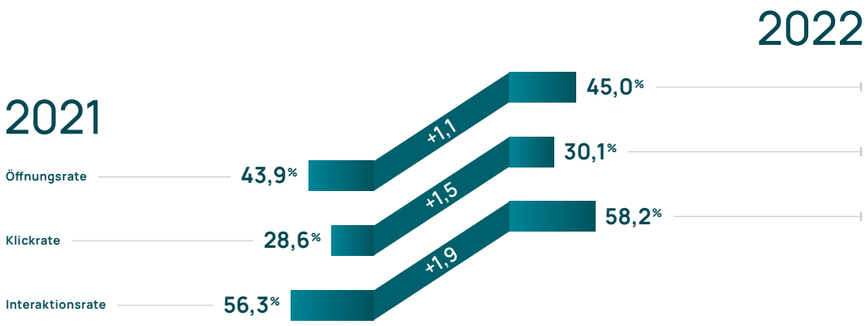
Die vorangegangenen Kapitel zeigen vor allem eines: Die Bedrohungslage hat sich weiter verschärft – und dabei steht der Mensch zunehmend im Fokus.

Doch wie genau greifen uns die Cyberkriminellen an? Welche Social-Engineering-Taktiken funktionieren besonders gut? Und welche Trends und Handlungsempfehlungen lassen sich aus den Einblicken ableiten?

In unserer jährlichen Kernanalyse rund um Phishing und Social Engineering tragen wir psychologische und technische Daten und Analysen aus verschiedenen Quellen zusammen und beantworten genau diese Fragen.

# 3.1 Psychologische und technische Angriffsvektoren bei Phishing-Simulationen

Diese Analysen (Seite 44-48) basieren auf exklusiven Reaktionsdaten aus der SoSafe Awareness-Plattform. Dazu wurden über 4,3 Millionen simulierte Phishing-Angriffe von 1.500 Kundenorganisationen aus dem Jahr 2021 anonym ausgewertet und die Erfolgswahrscheinlichkeit verschiedener Angriffstaktiken analysiert. So ergeben sich exklusive Einblicke in psychologische, technische und weitere Vektoren, die menschliche Risiken in Organisationen beeinflussen.



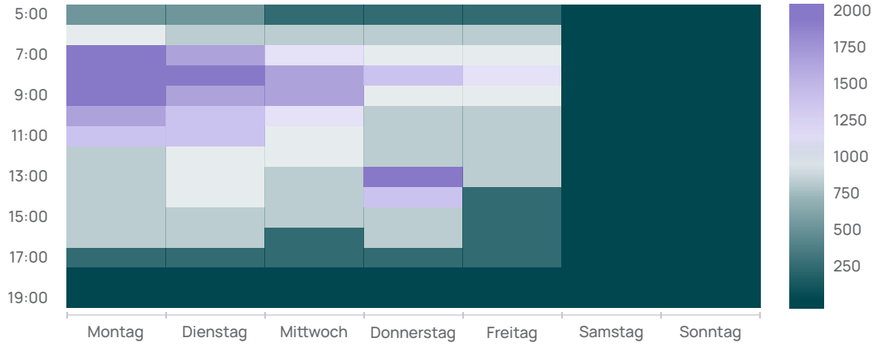

Die Cyber-Bedrohungslage hat sich verschärft – und auch menschliche Risiken haben nicht abgenommen. Die Öffnungs-, Klick- und Interaktionsraten bei Phishing-Mails sind weiterhin auf hohem Niveau. Im Vergleich zum Vorjahr sind sie sogar noch weiter angestiegen.

Fast die Hälfte aller Nutzenden öffnet Phishing-Mails – davon klickt fast jede und jeder Dritte auf enthaltene Links, Anhänge oder andere schädliche Inhalte. 58 Prozent dieser Nutzenden wiederum interagieren zudem mit den Inhalten und geben beispielsweise persönliche Daten in fingierte Login-Masken ein.

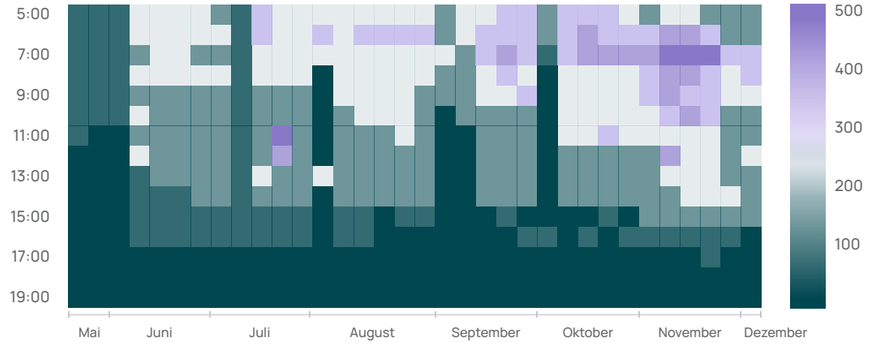




## Melderaten: Der frühe Vogel bekommt Phishing-Mails



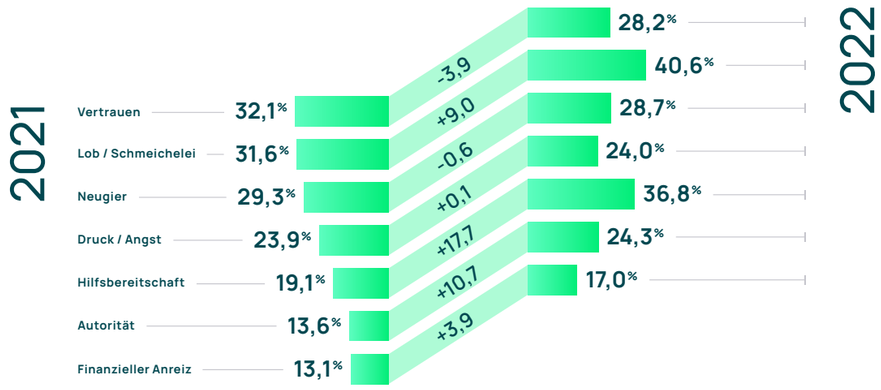

Die meisten Phishing-Versuche werden montags morgens von Mitarbeitenden bemerkt. Zwischen 07:00 und 09:00 Uhr meldeten Nutzende an Montagen die meisten verdächtige E-Mails. Im Verlauf der Woche bleibt die Anzahl der gemeldeten Phishing-Mails morgens am höchsten – vor allem vor oder während des ersten Kaffees ist daher besondere Vorsicht geboten. Das heißt aber nicht, dass man sich nach der Mittagspause generell in Sicherheit wägen kann: Der Ausschlag donnerstags zeigt, dass auch unaufmerksames Verhalten im Laufe des Tages Gefahren birgt.




Heatmaps basierend auf echter Phishing-Mails, die über den SoSafe Phishing-Meldebutton gemeldet wurden.

Die Sicht auf das gesamte Jahr bestätigt die Erkenntnisse aus der Wochen-Analyse – generell werden vor 09:00 Uhr die meisten Phishing-Mails von Mitarbeitenden erkannt.  Zum Ende des Jahres wird außerdem deutlich: Cyberkriminelle nutzen vor allem umsatzstarke Zeiten im Einzelhandel gerne aus. In den Monaten Oktober bis Dezember werden deutlich mehr Phishing-Versuche gemeldet als in der Mitte des Jahres. In diese Zeit fallen zum Beispiel der Black Friday, der Cyber Monday und die Weihnachtsfeiertage.

## Positive Emotionen verleiten zum Trugschluss




In Phishing-Mails verwenden Cyberkriminelle verschiedene psychologische Taktiken, um potenzielle Opfer dazu zu verleiten, Daten preiszugeben oder kompromittierte Dateien zu öffnen. Am anfälligsten sind Empfängerinnen und Empfänger bei positiv konnotierten Emotionen: Zu den erfolgreichsten Taktiken gehören wie auch schon im letzten Jahr Hilfsbereitschaft, Lob/Schmeichelei, Neugier und Vertrauen. Mit Lob und vermeintlicher Hilfsbereitschaft verleiten Cyberkriminelle mehr als ein Drittel der Empfängerinnen und Empfänger zum Klick auf schädliche Inhalte.

Der hohe Anstieg der Klickraten in den Bereichen Hilfsbereitschaft und Autorität zeigt Parallelen zur neuen Normalität im Kontext der Pandemie und hybriden Arbeitsmodellen. Durch die vermehrte Kommunikation über digitale Kanäle und den Wegfall persönlicher Begegnungen gehört es heute zum Alltag, von Kolleginnen und Kollegen per Mail oder Kollaborationstool um Hilfe gebeten zu werden. Meist wird eine schnelle Reaktion erwartet. Das verleitet dazu, unüberlegt zu handeln – gerade, wenn die Anfrage von einer Autoritätsperson kommt. Auch Cyberkriminelle wissen das und nutzen genau diese Kanäle für ihre Angriffe.

Positiv zu vermerken ist, dass die Menschen skeptischer geworden sind, wenn es um scheinbar vertrauenserweckende Inhalte geht, so beispielsweise gefälschte Newsletter von bekannten Organisationen oder vermeintliche Lieferinformationen von Versanddienstleistern. Hier fielen die Zahlen im Vergleich zum Vorjahr. Generell fielen die wenigsten Empfängerinnen und Empfänger auf Phishing mit finanziellen Anreizen hinein. Die Vermutung liegt nahe, dass diese Taktik bereits lange im Einsatz und entsprechend gut bekannt ist.

## Die Top 10 Phishing-Betreffzeilen

**1** 66 %
Autorität
Folgende Aufgabe ist zu erledigen: Verteilung der Dokumente und Aufgabenprüfung

**2** 66 %
Hilfsbereitschaft; Neugier
Sie haben 2 Erwähnungen

**3** 57 %
Autorität; Druck/Angst
Wichtig: CORONA Update

**4** 51 %
Autorität; Neugier
Allgemeine Information: Neue Lohnabrechnungssoftware

**5** 50 %
Druck/Angst
Missed meeting

**6** 49 %
Neugier; Vertrauen
Newsletter für September 2021

**7** 46 %
Autorität; Neugier
Beitrag vom Vorstand

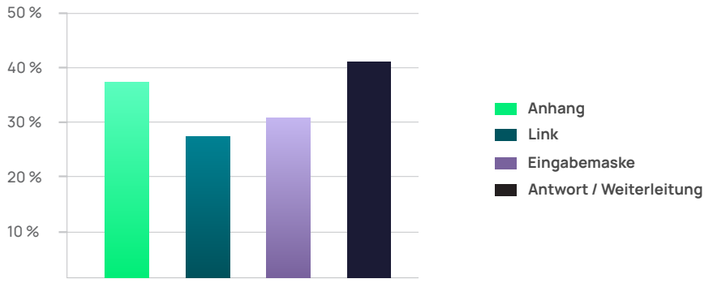
**8** 46 %
Autorität
[EXT] Aktualisierung Organisationsanweisung für mobile Geräte

**9** 42 %
Neugier
Ihr eingescanntes Formular

**10** 41 %
Vertrauen; Druck/Angst
Ihr Office 365 Passwort läuft heute ab

Welche Betreffzeilen verleiten Empfängerinnen und Empfänger am ehesten zum Klick auf eine Phishing-Mail? Auch in dieser Auswertung zeigt sich: Das Vorgaukeln von Autorität und das Ausnutzen der Hilfsbereitschaft von Menschen funktionieren – vor allem dann, wenn ein Element der Neugier hinzukommt. Der Bezug auf neue, hybride Arbeitsmodelle (Platz 1 und Platz 5) und COVID-19 (zum Beispiel Platz 3) in Betreffzeilen durchbricht aber das typische Schema. Das Einsetzen negativer Emotionen wie Druck und Angst führt in diesem Kontext zu besonders hohen Öffnungs- und Klickraten. Die pandemiebedingte Verunsicherung der Menschen spielt den Cyberkriminellen anscheinend noch immer deutlich in die Karten. Ein deutliches Zeichen für Sicherheitsverantwortliche: Gerade bei hybriden Arbeitsmodellen sollten Mitarbeitende die Möglichkeit bekommen, ihr Verhalten im Umgang mit Cyberrisiken zu trainieren, um sich vor den Gefahren schützen zu können.

## Verdächtige Formate oder Tippfehler: Diese technischen Vektoren verursachen die meisten Klicks




Nicht nur mit emotionalen, psychologisch effektiven Inhalten versuchen Cyberkriminelle sich Zugang zu sensiblen Informationen und Daten zu verschaffen. Auch über technische Änderungen und Tricks innerhalb der Phishing-Nachrichten selbst gelingt es ihnen, ihre Opfer hinters Licht zu führen.

Am gefährlichsten sind für Organisationen Phishing-Mails, die eine E-Mail-Konversation vorgaukeln. Etwa 40 Prozent aller Mitarbeitenden klicken auf diese vermeintlichen Folgemails. Auch Anhänge scheinen oftmals nicht als schädlich wahrgenommen zu werden – mehr als jede und jeder dritte Mitarbeitende klickt hier.

## Manipulieren Cyberkriminelle Absendeadressen, zeigt sich ein ebenso gefährliches Bild

**23,6 %** **Typo-Squatting**
Ein unauffälliger Rechtschreibfehler wird in eine Webadresse eingebaut.

**31,3 %** **Subdomain-Squatting**
Eine fingierte Subdomain wird vor eine unscheinbare Top-Level-Domain gesetzt.

**31,2 %** **Mail-Address-Spoofing**
Der Absender im E-Mail-Kopf wird überlagert.

**19,8 %** **Domain-Squatting**
Die fingierte Domain ähnelt der imitierten Domain stark.

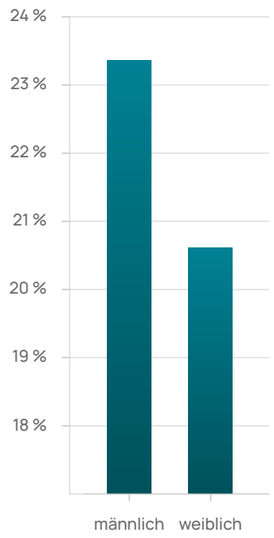




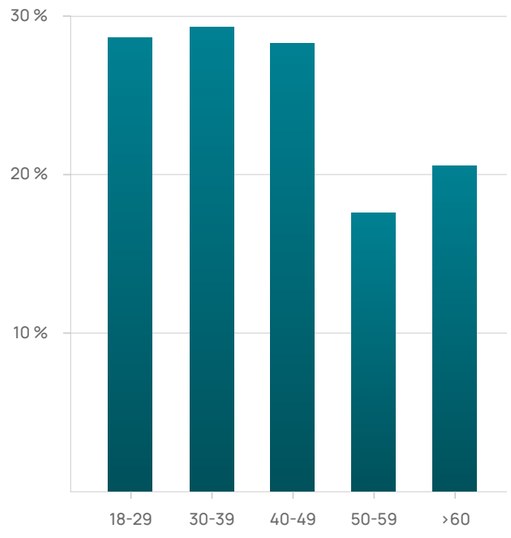
# 3.2 Unterschiede zwischen Personengruppen

Die jährlich von SoSafe und Botfrei durchgeführte Studie „Phish-Test“ zur allgemeinen Phishing-Awareness liefert demografische Einblicke in das Klickverhalten von Nutzenden. 2021 nahmen über 1350 User teil und erhielten innerhalb einer Woche drei in der Simulation als mittelschwer eingestufte Phishing-Mails, die es zu erkennen galt.

Klickrate nach Geschlecht




Klickrate nach Alter in Jahren




Mit einer durchschnittlichen Klickrate von 23 Prozent über alle demografischen Gruppen hinweg zeigt sich, dass Bürgerinnen und Bürger noch stärker im Umgang mit Cybergefahren sensibilisiert werden sollten.

Wie schon im vergangenen Jahr interagierten trotz der nur mittleren Komplexität der simulierten Phishing-Mails vor allem männliche Teilnehmer mit den Inhalten – knapp jeder Vierte klickte. Dagegen klickte nur jede fünfte Frau.

Insbesondere auch in den Altersgruppen zeichnet sich ein interessantes Bild ab: so klickten gerade die jüngeren Teilnehmenden zwischen 18 und 49 Jahren mit einer Rate von 28,6 Prozent deutlicher häufiger als Über-50-Jährige mit im Durchschnitt nur 19 Prozent. Wie auch schon in den Vorjahren zeigt sich anhand dessen, dass sich gerade auch „Digital Natives“ eventuell etwas unbedarfter im digitalen Raum bewegen.

**+24 %**

Besonders spannend: Bei Personen, die ihren Wissensstand zur Informationssicherheit selbst als niedrig einschätzen, liegt die Klickrate im Schnitt 24 Prozent höher als bei Personen, die diesen eher als hoch einschätzen. Das gibt Grund zur Hoffnung: Sind den Personengruppen Wissenslücken bewusst, können sie diese aktiv auffüllen – und sich so vor Cyberangriffen schützen.

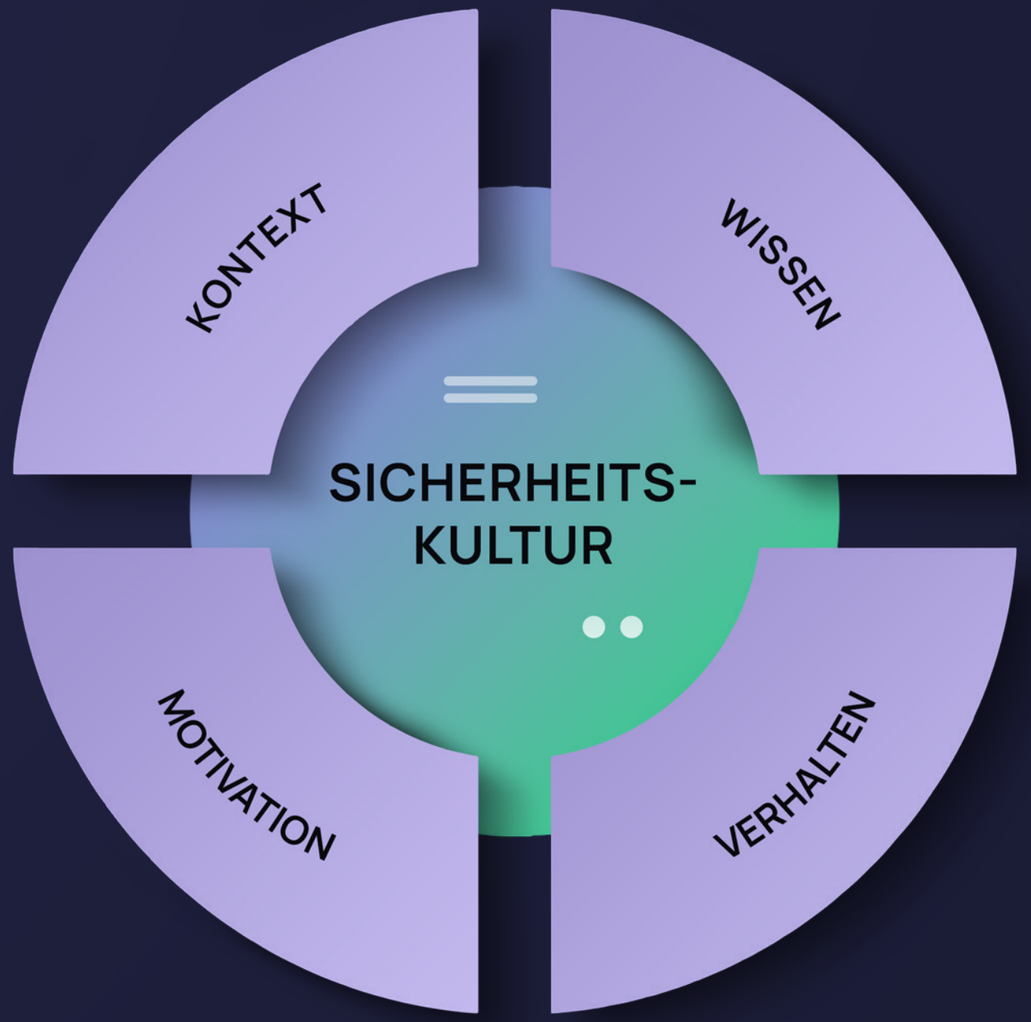
# 04 Das „Behavioral Security Model“ Sicherheitskultur ganzheitlich aufbauen

Dass ein Großteil der Cyberangriffe beim Faktor Mensch ansetzt, ist einfach zu erklären: Er lässt sich in jeder Organisation angreifen – und das immer auf eine ähnliche Art und Weise. Dabei ist es unerheblich, wie komplex die Infrastruktur einer Organisation aufgebaut ist. Mitarbeitende sind für Kriminelle die Universaltools, um in interne Systeme zu gelangen, weil sie sich emotional manipulieren lassen.

Gleichzeitig spielt der Mensch aber auch eine zentrale Rolle bei der Verteidigung vor Cyberangriffen. Aufmerksame Mitarbeitende, die eine Phishing-Mail erkennen, können dazu beitragen, dass schwerwiegende Cybervorfälle verhindert werden. Das richtige Verhalten zum richtigen Zeitpunkt kann Unternehmen also hohe Kosten ersparen. Das zu ermöglichen und zu fördern ist somit das Ziel einer nachhaltigen Sicherheitskultur. Dass diese auch von einer Risiko-Perspektive einen klaren ROI aufweisen kann, zeigen die Zahlen aus der SoSafe Awareness-Plattform: So kann sich das Risiko für einen erfolgreichen Phishing-Angriff durch systematische Sensibilisierungsmaßnahmen um bis zu 90 Prozent reduzieren.

Im „New Normal“ einer hybriden Arbeitswelt stehen Mitarbeitende vor enormen Herausforderungen. Kollaborationstools und neue Kommunikationsformen buhlen immer stärker um unsere Aufmerksamkeit. Eine immer vernetztere Arbeitswelt führt zu einem erhöhten Informationsaufkommen. Komplexere Angriffstaktiken bringen zudem den Bedarf für ein gesteigertes digitales Skill-Level mit sich. Versuche, dieser Herausforderung mit Methoden der reinen Wissensvermittlung oder dem Bestätigen von Policies zu begegnen, führen nicht nur zu Frustration auf allen Seiten, häufig sogar zu Phänomenen wie der sogenannten Security Fatigue – der Überforderung von Mitarbeitenden durch zu viele Sicherheitsthemen.

Eine moderne Sicherheitskultur versucht den Menschen dort zu begegnen, wo sie sind und sie ganzheitlich zu verstehen. Ziel ist es nicht, reines Wissen zu vermitteln oder eine „Checkbox“ abzuhaken. Sie soll stattdessen Mitarbeitende dabei unterstützen und dazu motivieren, ihr Verhalten zu betrachten und sichere Routinen einzuüben. Das dargestellte „Behavioral Security Model“ hat vier Dimensionen, die für eine moderne Security Awareness alle gleichermaßen betrachtet und als Interventionsebenen genutzt werden sollten.



## → Kontext

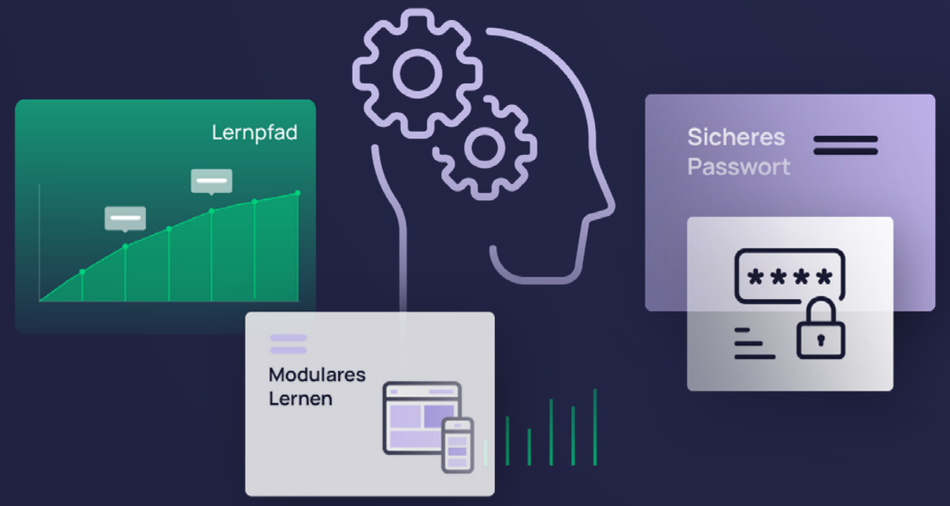
Nicht jede Person innerhalb einer Organisation hat die gleiche Ausgangslage: Die individuelle Rolle beeinflusst maßgeblich, wie sich Cyberrisiken gestalten. Angestellte in Führungspositionen, Personen mit Diensthandy, bestimmten Zugriffsrechten und Tools, oder Mitarbeitende in der Finanzabteilung sind so beispielsweise stärkeren Gefahren ausgesetzt, weil Cyberkriminelle ihre Position für zielgerichtete Angriffe ausnutzen. Die Branche eines Unternehmens hat ebenso Einfluss auf das Risiko (siehe dazu auch „Sektoren im Fokus“, Seite 29).

Deshalb sollten Organisationen einen Kontext schaffen, der sicheres Verhalten generell begünstigt. Bestehen im Unternehmen beispielsweise keine etablierten Meldeketten oder klare Ansprechpersonen für mögliche Vorfälle, wird entsprechendes Meldeverhalten stark erschwert. Können Mitarbeitende hingegen schnell und ohne Aufwand verdächtige E-Mails melden, zum Beispiel durch einen Phishing-Melde-button, erleichtert dies das entsprechende Verhalten enorm. Auf Basis der SoSafe-Plattformdaten lassen sich nach der Einführung eines Buttons bis zu 70 Prozent der Mitarbeitenden aktiv in die Verteidigung einbinden. Durch diese Schwarmintelligenz können zahlreiche potenziell gefährliche Situationen vermieden werden.

Kontext ist zugleich noch auf eine andere Art und Weise zu verstehen. Der persönliche Kontext von Mitarbeitenden beeinflusst die individuelle Lernerfahrung. Zum Beispiel benötigen nicht alle Mitarbeitenden Informationen zur sicheren Bedienung eines Diensthandys, wenn sie gar keines verwenden. Deshalb sollten Lernerfahrungen auf die Mitarbeitenden abgestimmt werden: Personalisierte Lernpfade gehen beispiels-weise genauer auf die individuelle Situation der Lernenden ein und machen Erlerntes so greifbar und relevant.





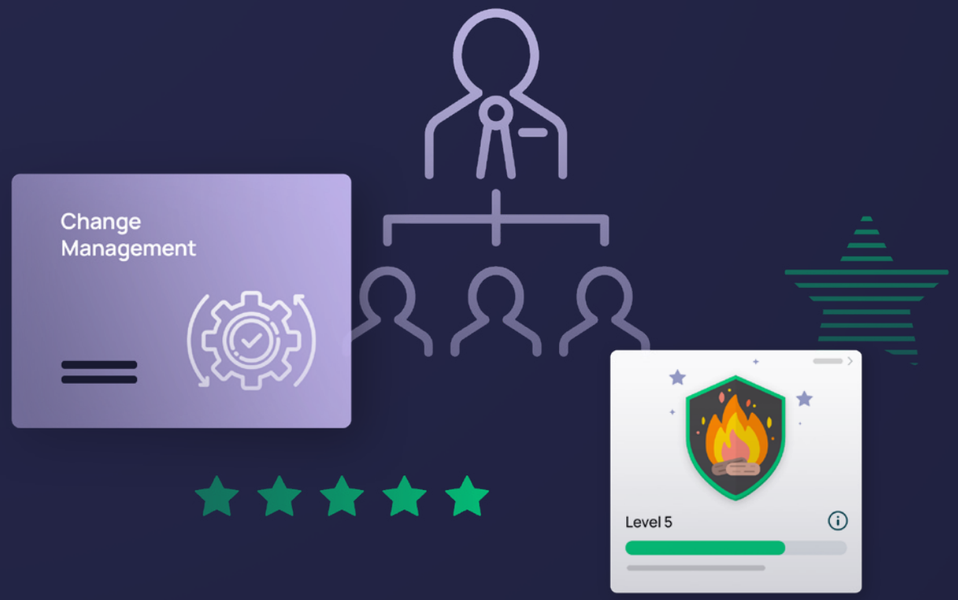




## → Wissen

Um ein bestimmtes Verhalten zu zeigen, muss zunächst das Wissen über das richtige Verhalten vorhanden sein. Der erste Schritt in Richtung einer starken Sicherheitskultur war deshalb auch traditionell immer, Wissen zu vermitteln – zum Beispiel darüber, wie sichere Passwörter erstellt oder Phishing-Mails erkannt werden. In der Vergangenheit wurde Wissen allerdings häufig sehr linear und in „hoher Dosis“ vermittelt. Auf lange Videos oder Seminare folgte ein einfacher Wissenstest zum Lernnachweis.

Dass lineares und „massiertes“ Lernen aber nur begrenzt zur langfristigen Wissensaufnahme beiträgt, ist lange bekannt. Bereits in den 1950er Jahren zeigte der deutsche Psychologe Hermann Ebbinghaus, dass Schülerinnen und Schüler bereits nach wenigen Tagen den Großteil des Lernstoffes vergessen hatten. Ebbinghaus fand ebenso heraus: Stabile Gedächtnisengramme (die „Abdrücke“ des Wissens im Gehirn) entstehen besser, wenn Wissen verteilt und aktiv wiederholt wird.

Um Cyber-Security-Wissen zu vermitteln, sollten Organisationen daher statt auf reine „Frontbeschallung“ auf lernpsychologisch fundierte Ansätze zurückgreifen. Hoch-modularisierte Trainings und stetige Anstupser zum Lernen, sogenannte „Nudges“, lassen die Vergessenskurve abflachen – und minimieren dadurch menschliche Risiken langfristig. Ergebnisse aus der SoSafe Awareness-Plattform zeigen, dass durch Nudging die Engagement-Rate kontinuierlich um 30 Prozent, in der Einfüh-rungsphase sogar um bis zu 90 Prozent, erhöht wird. So prägen sich Mitarbeitende Wissen effektiv und nachhaltig ein.




## → Motivation

Sicheres Verhalten ist immer von verschiedensten Faktoren beeinflusst. Das lässt sich einfach am Alltagsbeispiel Straßenverkehr veranschaulichen: Obwohl wir wissen, dass wir in der Innenstadt nicht mit 80 km/h fahren dürfen, müssen wir auch verstehen, warum das so ist, damit wir uns tatsächlich an die Vorschriften halten. In einer starken Sicherheitskultur wissen Mitarbeitende deshalb nicht nur über Cyberrisiken Bescheid und verstehen, wie sie sich diesen in ihrem individuellen Kontext proaktiv entgegenstellen können. Eine solche Kultur ist davon geprägt, dass sie die Motivation der Beteiligten begünstigt – und die Relevanz der Maßnahmen betont.

Das Stärken der Motivation und Sicherheitskultur liegt in den Händen der Führungsetage und umfasst die Anpassung von Prozessen unter Aspekten der Informationssicherheit. Damit gehört es zum Bereich Change Management. Aktuelle Studien zeigen, dass das Engagement der Führungskräfte dabei eine entscheidende Rolle spielt. Involvieren Führungskräfte Mitarbeitende frühzeitig und kommunizieren direkt mit ihnen, sind diese wesentlich eher dazu bereit, ihr Verhalten zu verändern und sogar selbst die Entwicklung mit voranzutreiben – mit positiven Auswirkungen auf die Minimierung menschlicher Risiken. Auch der Einsatz spielerischer Elemente hat in diesem Kontext deutliche Effekte: Beim Einsatz von Gamification erhöht sich die Aktivierungsrate im Security-Awareness-Training um bis zu 50 Prozent.





## → Verhalten

Letztlich hängt das menschliche Risiko in einer Organisation vor allem davon ab, wie gut Mitarbeitende das Erlernte auch in die Tat umsetzen und sichere Gewohnheiten pflegen. Kontext, Wissen und Motivation spielen dabei eine Rolle. Entscheidend ist aber, wie gut sicheres Verhalten „in Fleisch und Blut" übergeht.

Um sicheres Verhalten einzutrainieren, gilt es, das notwendige Wissen motivierend – zum Beispiel mithilfe von Gamification – zu vermitteln. Die Verhaltenspsychologie zeigt außerdem: Insbesondere kontinuierliches, inzidentelles Lernen festigt Gewohnheiten. Über laufende Angriffssimulationen wird das erlernte Verhalten beispielsweise immer wieder auf die Probe gestellt und in das aktive Gedächtnis der Mitarbeitenden gerufen. Ergebnisse aus der SoSafe Awareness-Plattform belegen, dass Phishing-Klickraten sich so langfristig auf einem niedrigen und die Melderaten auf einem hohen Niveau einpendeln.


### Warum sich die Investition in Behavioral Security rentiert

Indem Organisationen sicheres Verhalten ermöglichen und fördern, minimieren sie also effektiv und nachhaltig Risiken – und sparen dadurch langfristig Kosten ein. Denn das Investment in Security Awareness sollte als Investment in die Sicherheit der Organisation gesehen, und gegen die potenziellen Kosten im Schadensfall gerechnet werden. Im Falle eines erfolgreichen Cyberangriffs kommt einem Unternehmen mit 10 Milliarden Euro Umsatz dieser beispielsweise mit 106 Millionen Euro teuer zu stehen. Durch systematische Awareness-Maßnahmen werden die Klickraten auf Phishing-Mails jedoch drastisch reduziert. Bei einer Verringerung der Klickrate um 70 Prozent reduziert sich der zu erwartende Schaden damit auf 32 Millionen Euro. Investieren Organisationen in Security Awareness und den Aufbau ihrer Sicherheitskultur, können sie also mit langfristigen Kostenersparnissen rechnen.

# Marisa Fagan, Atlassian

> “Awareness-Programme sollten immer verhaltenswissenschaftlich fundiert sein.”

**Marisa Fagan** hat einen Background in Informationssicherheit und Community Building und arbeitet seit mehr als 10 Jahren in der Technologie- und Sicherheitsbranche. Sie war zuvor bei Salesforce und Synopsys tätig und ist derzeit **Head of Trust Culture & Training bei Atlassian**, wo sie die Mitarbeitenden dazu befähigt, fundierte Sicherheitsentscheidungen zu treffen.

**Sie sind Head of Trust Culture & Security. Was steckt hinter der gemeinsamen Betonung von „Kultur“ und „Sicherheit“?**

Wir möchten unsere Mitarbeitenden dazu befähigen, sicher zu arbeiten. Wir orientieren uns an dem Verhaltensmodell von BJ Fogg: Befähigung setzt sich für uns aus Fähigkeiten, Motivation und Anreizen zusammen. Awareness kann man nicht einfach vermitteln. Man muss auch die Motivation der Mitarbeitenden erhöhen, was am besten durch die Beeinflussung der Unternehmenskultur gelingt.

**In den letzten fünf Jahren fand im Bereich Security Awareness und Training ein grundlegender Paradigmenwechsel statt. Was sind aus Ihrer Sicht die wichtigsten Aspekte dieses Wandels?**

Immer mehr Unternehmen haben nun Security-Awareness-Teams. Gleichzeitig stellen viele Start-ups diesen Teams nun detaillierte Daten bereit. Sie bemessen beispielsweise Sicherheitsvorfälle oder das Verhalten von Mitarbeitenden und ordnen diese Daten in Risikostufen ein. Damit wird es leichter, sich das Organisationsrisiko ganzheitlich anzuschauen – und auch Führungskräften einen Überblick darüber zu verschaffen. Dieser Perspektivwechsel wird sich fortsetzen, bis wir den Mitarbeitenden glaubhaft veranschaulichen können, wie wichtig es ist, sicheres Verhalten zu trainieren.

**Was ist der Unterschied zwischen der Schulung von Mitarbeitenden, indem man einfach Informationen bereitstellt, und der Schaffung einer nachhaltigen Vertrauens- und Sicherheitskultur? Gibt es eine Geheimzutat zum Aufbau einer Sicherheitskultur?**

Jeder Mensch ist anders. Deshalb sollten wir die Mitarbeitenden in ihrem individuellen Kontext abholen. Es gibt solche, die kurze Schulungen bevorzugen, und andere, die erst einmal die Tools kennenlernen müssen. Es gibt also durchaus noch einen Platz





für klassische Schulungen, aber auch viele andere Strategien. Je mehr Optionen Sie den Mitarbeitenden geben, umso eher werden sie sich auf das einlassen, was Sie von ihnen verlangen. Die Geheimzutat für eine starke und nachhaltige Sicherheitskultur ist also eine Mischung aus verschiedenen Methoden. Wir sind ein vierköpfiges Team, das sich darum kümmert: Neben Online-Schulungen bieten wir einen Blog, einen Newsletter, Slack-Kanäle, ein Event im Rahmen des Security Awareness Month, einen Kalender mit ganzjährigen monatlichen Veranstaltungen sowie eine Security Champions Community an.

**Welche Rolle spielt aus Ihrer Sicht die Verhaltenswissenschaft im Zusammenhang mit Awareness und einer Trust Culture?**

Jedes Awareness-Programm sollte auf verhaltenswissenschaftlichen Techniken basieren. Wir verwenden das Fogg-Verhaltensmodell, um herauszufinden, warum unsere Schulungen nicht die Ergebnisse liefern, die wir uns erhofft haben. Sobald wir wissen, ob wir die Fähigkeit, die Motivation oder andere Anreize verbessern wollen, wählen wir eine von verschiedenen verhaltenswissenschaftlichen Methoden, um schnell Fortschritte zu erzielen. Wir veröffentlichen zum Beispiel eine Rangliste nach Teams, um zu zeigen, welches Team das Training am schnellsten abgeschlossen hat. Diese Technik basiert auf der Sozialpsychologie und wird “sozialer Vergleich” genannt. Menschen nehmen eher an einer Schulung teil, wenn ihre Kolleginnen und Kollegen sie bereits absolviert haben.

**Sie sprechen immer wieder über sogenannte Security-Champion-Programme und wie man Menschen dazu motiviert, sich für Sicherheit zu engagieren. Wie ermutigen Sie Ihre Mitarbeitenden dazu, Informationssicherheit in ihren Alltag einzubauen?**

Ich glaube, die Leute in diesem Bereich vergessen oft, dass auch sie Teil der Zielgruppe sind. Sind Sie selbst von den Security-Maßnahmen überzeugt und gehen Sie als Beispiel voran? Um Mitarbeitende zu motivieren, müssen die Maßnahmen vor allem eines sein: Angemessen. Stellen Sie sicher, dass Sie alle nötigen technischen Vorkehrungen getroffen haben und bitten Sie die Mitarbeitenden als Schutzschild im Notfall zu agieren. Der wichtigste Schritt ist eine klare Kommunikation, das Ziel der Bemühungen betont. Wenn die Gründe nachvollziehbar sind, holen Sie Ihre Mitarbeitenden leichter an Bord. So gehen wir beispielsweise bei der Verwendung von Passwortmanagern vor. Wir teilen den Mitarbeitenden mit, dass “laut einer Studie von Google aus dem Jahr 2019 65 % der Menschen dasselbe Passwort für mehrere Konten verwenden” und “85 % der Sicherheitsverletzungen im letzten Jahr gestohlene Passwörter betrafen”. Das zeigt, wie risikoreich dieses Verhalten ist und lässt die Mitarbeitenden entsprechende Entscheidungen treffen. Kommunikation und Transparenz überzeugen nicht jeden, aber den Menschen alle Informationen zu geben und ihnen zu vertrauen, dass sie die richtigen Entscheidungen treffen, ist ein wichtiger Teil unserer Kultur.

**Erheben Sie nun auch andere Kennzahlen als zuvor?**

Wir kombinieren mittlerweile alle kleinen Signale zu einer ganzheitlichen Kennzahl. Wir haben eine Metrik für menschliche Risiken in unserer Organisation, die sich aus gewichteten Werten aus verschiedenen Bereichen zusammensetzt: gestohlene Phishing-Anmeldedaten, Phishing-Berichte, abgeschlossene Schulungen und die Nutzung von Passwortmanagern. So können wir ein differenziertes Bild des Risikos auf Unternehmensebene zeichnen. Unser Plan ist es, dieser Liste weitere “Verhaltensweisen” hinzuzufügen und so noch besser bemessen zu können, wie sicher unsere Mitarbeitenden arbeiten.

**Sehen Sie neue Herausforderungen, die sich aus dem „New Normal“ und hybriden Arbeitsweisen ergeben?**

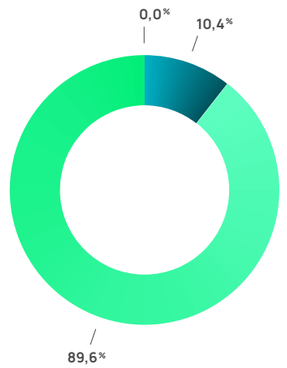
Definitiv! Wir mussten unseren Schulungskalender straffen. Die Leute haben jetzt viel weniger Zeit. Die Kurse sind nun auf 60 Minuten begrenzt, während wir früher alle für ein dreitägiges Treffen versammelt haben. Wir konzentrieren uns jetzt mehr darauf, Mitarbeitenden von Anfang an Schulungen mitzugeben, sowohl in Form von Präsentationen direkt am ersten Tag als auch in Form von Self-Service-Trainings, auf die neue Mitarbeitende später zurückgreifen können.

# 05 Sicherheitsverantwortliche bestätigen: Cyberrisiken steigen – und Cyberresilienz wird wichtiger

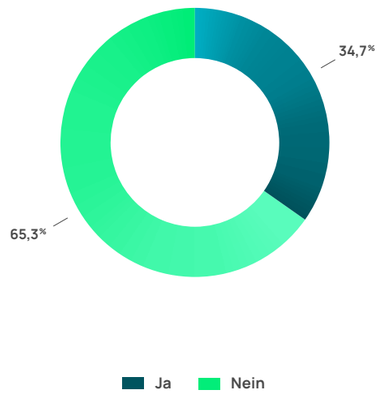
Eine professionelle Cybercrime-Industrie und zunehmend erfolgreiche Social-Engineering-Taktiken – wie reagieren Organisationen auf die gesteigerten Herausforderungen? Für unseren HumanRisk Review befragen wir jedes Jahr IT-Experten und IT-Sicherheitsbeauftrag te dazu, wie sie die Cyber-Bedrohungslage wahrgenommen haben und welche Pläne sie hinsichtlich Awareness in ihrer Organisation haben. Dieses Jahr haben 251 Expertinnen und Experten ihre Erfahrungen mit uns geteilt.

## Die Wahrnehmung der Cyber-Bedrohungslage 2021

Rückblick auf das Jahr 2021: Wie haben Sie die Cyberbedrohungslage wahrgenommen?




Unsere Organisation (oder einer unserer Dienstleister) hat selbst einen Cyberangriff erlebt.




9 von 10 Befragten sind sich einig: Die Cyberbedrohungslage hat sich 2021 verschärft. Mehr als ein Drittel der Befragten haben sogar innerhalb ihrer Organisation oder bei einem Dienstleister selbst einen Cyberangriff erlebt. Die hohen Zahlen zeigen: Kaum eine Organisation wiegt sich noch in Sicherheit vor Cyberangriffen. Doch welche Treiber sehen die befragten Expertinnen und Experten für diese Entwicklung?

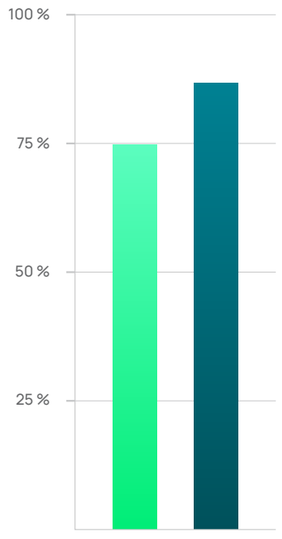




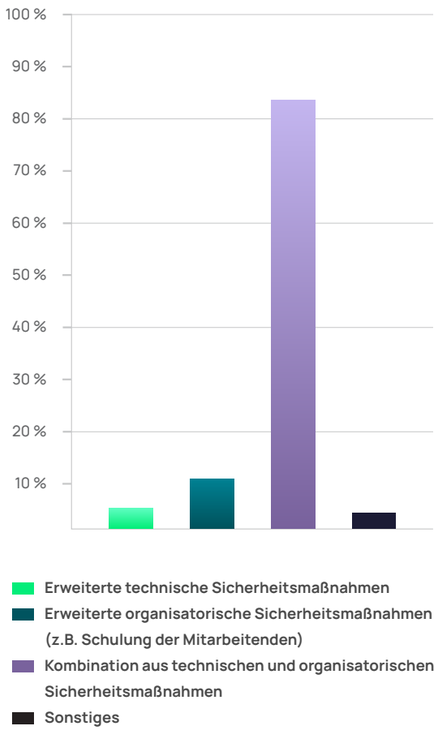
Drei Viertel der IT-Experten und IT-Sicherheitsbeauftragten bestätigen, dass der Anstieg von mobilen Arbeits- bzw. Homeoffice-Modellen neue Angriffspunkte bietet. Über 85 Prozent sehen die Ursache für die verschärfte Bedrohungslage in der Professionalisierung von Cyberkriminalität.

Zwar sind sich die Befragten einig, dass die Arbeit aus dem Homeoffice neue Angriffsflächen bietet – sie sind jedoch auch zuversichtlich, dass verschiedene Sicherheitsmaßnahmen das Arbeiten von Zuhause aus sicherer machen.

Diese Treiber haben zur Verschärfung der Cyberbedrohungslage beigetragen.




Was würde hybrides Arbeiten / Homeoffice sicherer machen?




Aus den Antworten geht hervor, dass primär eine Kombination aus technischen und organisatorischen Sicherheitsmaßnahmen, wie beispielsweise Awareness-Trainings, als förderlich für ein sichereres Arbeitsumfeld beim mobilen Arbeiten eingeschätzt werden.

## Menschliche Risiken in der eigenen Organisation

Die Einschätzungen zur Bedeutung von Security Awareness in Organisationen zeigen einen klaren Trend: 9 von 10 Befragten erkennen Security Awareness als wichtiges oder sogar sehr wichtiges Thema an – und je wichtiger das Thema innerhalb einer Organisation ist, desto höher schätzen die Befragten im Schnitt auch das Awareness-Level der Mitarbeitenden ein. Das bestätigt, dass das Bewusstsein für Cybergefahren aus einer Sicherheitskultur wächst, in der das Thema entsprechend klar platziert wird.

Trotzdem zeigt sich bei Betrachtung aller Antworten zur Einschätzung der menschlichen Risiken ein deutlicher „Security Awareness Gap“: In 40 Prozent der Organisationen, die das Thema als wichtig oder sehr wichtig ansehen, wird das Awareness-Level der Mitarbeitenden noch immer als niedrig oder sehr niedrig eingeschätzt. Das zeigt: In vielen Unternehmen besteht aktuell Handlungsbedarf.

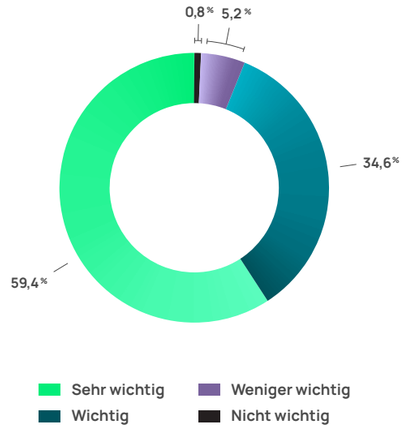
Mehr als zwei Drittel der Befragten schätzen das Risiko eines Cyberangriffs in ihrer Organisation sogar als hoch oder sehr hoch ein. Der Zusammenhang zwischen menschlichen Risiken und der Gefährdung der eigenen Organisation scheint den meisten IT-Verantwortlichen also durchaus bewusst zu sein.

Wie hoch schätzen Sie das Risiko ein, dass Ihre Organisation Opfer eines Cyberangriffs wird?

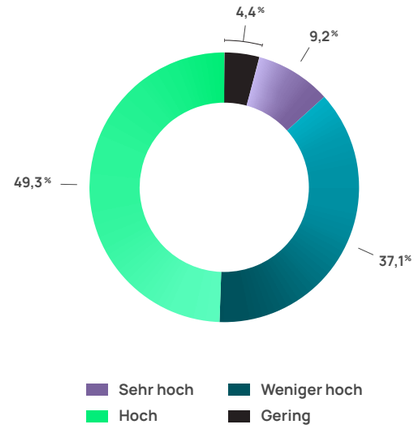




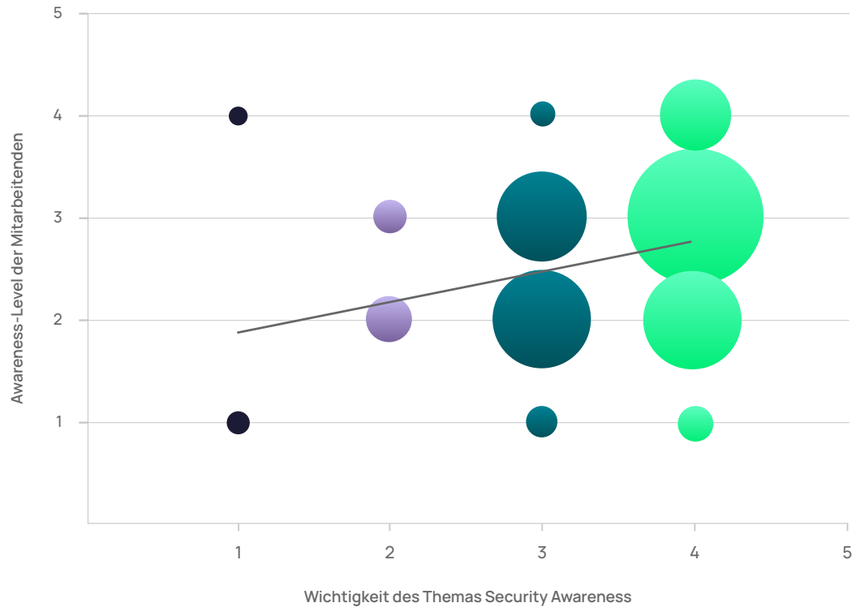

Wie wichtig ist das Thema Security Awareness in Ihrer Organisation?




Wie hoch schätzen Sie das Awareness-Level unter den Mitarbeitenden in Ihrer Organisation ein?



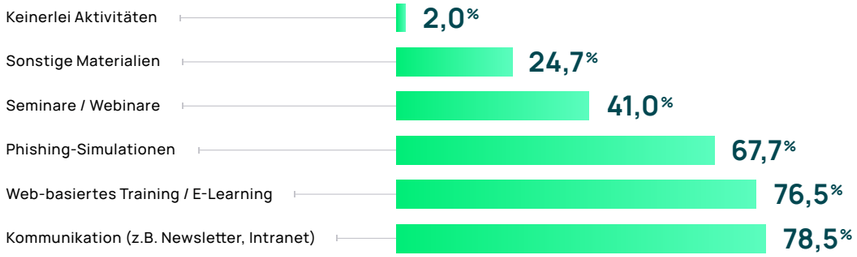

Zusammenhang zwischen Wichtigkeit des Themas Security Awareness und Awareness-Level von Mitarbeitenden



## Awareness-Maßnahmen in der eigenen Organisation

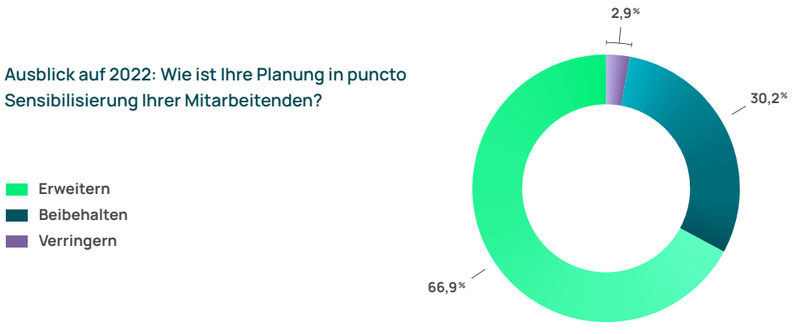
Das spiegelt sich auch im Einsatz von Awareness-Maßnahmen in der eigenen Organisation wider. Im Jahresvergleich zeigt sich: Organisationen haben aufgeholt! Während die Mehrheit noch immer vor allem auf interne Kommunikationsmaßnahmen setzt, hat der Einsatz von webbasierten Trainings und Phishing-Simulationen stark zugenommen und gehört nun zum Standard.

Mit welchen Maßnahmen wird die Awareness unter den Mitarbeitenden in Ihrer Organisation gestärkt?




Zusätzlich planen zwei von drei Befragten, die Maßnahmen zur Steigerung der Cyber Security Awareness unter den Mitarbeitenden noch weiter auszuweiten. Besonders erfreulich: Organisationen, die in der Befragung angaben, dass das Thema Security Awareness aktuell weniger wichtig oder nicht wichtig ist, geben im Schnitt häufiger an, die Maßnahmen zum Schutz vor Cyberrisiken im Jahr 2022 ausweiten zu wollen. Unternehmen haben verstanden, dass der Faktor Mensch bei einer umfassenden Sicherheitsstrategie eine entscheidende Rolle spielt.

Ausblick auf 2022: Wie ist Ihre Planung in puncto Sensibilisierung Ihrer Mitarbeitenden?




57 ZDNet (2022). Microsoft: Here's how we stopped the biggest ever DDoS attack.

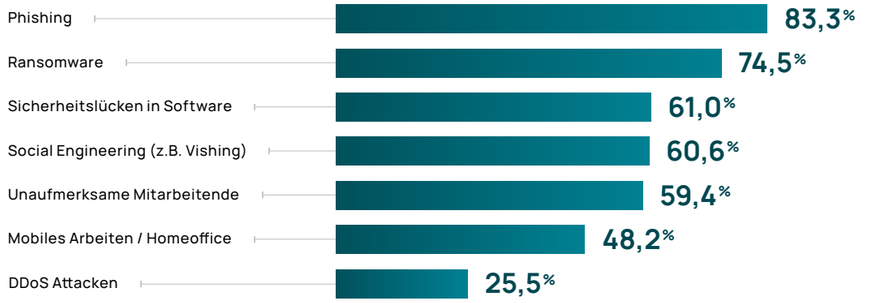




## Ein bunter Blumenstrauß an Angriffsvektoren

Bei der Frage, welche Angriffsvektoren laut Meinung der Befragten in der Zukunft am häufigsten zum Einsatz kommen, stechen vor allem diese heraus, die den Faktor Mensch betreffen. Allen voran werden Phishing und Ransomware als zukünftige Risikofaktoren wahrgenommen. DDoS-Angriffe scheinen weniger im Fokus der Expertinnen und Experten zu stehen – nichtsdestotrotz werden immer neue Rekord-Attacken verzeichnet, so beispielsweise die laut Microsoft bislang größte DDoS-Attacke aller Zeiten auf Azure im November 2021.[57] Software-Sicherheitslücken werden ebenfalls als gefährlich eingeschätzt – der Vektor bleibt vermutlich nicht zuletzt durch die große Log4j-Lücke im Gedächtnis der Befragten verankert.

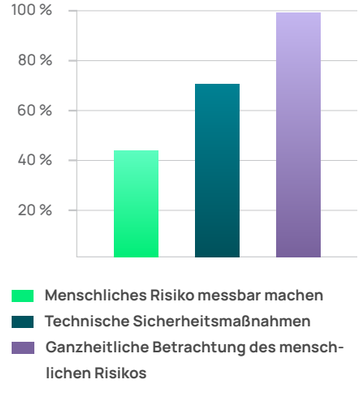
Was glauben Sie: Welche Angriffsvektoren werden in Zukunft am häufigsten genutzt werden?




## Wie geht es weiter? Die Aussichten für 2022

Nahezu einstimmig geben 99,2 Prozent aller Befragten an, dass im Jahr 2022 Security Awareness Training und das Stärken der eigenen Sicherheitskultur wichtiger werden. Darüber hinaus ist neben dem weiteren Ausbau bestehender technischer Sicherheitsmaßnahmen auch die ganzheitliche Betrachtung des Faktors Mensch (vgl. Kapitel 04) von Bedeutung für die Befragten.

Welche Themen werden 2022 im Bereich Informationssicherheit wichtiger werden?






INFOBOX

## → Neues Gutachten bestätigt Zweifel an DSGVO-Konformität von US-amerikanischen Software-Anbietern

Nach den Schrems-Urteilen der vergangenen Jahre zweifelt nun auch ein neues Gutachten des US-amerikanischen Juristen Stephen Vladeck die DSGVO-konforme Datenverarbeitung durch US- und auch deren EU-Tochterunternehmen an. Das Gutachten hält den aktuellen Stand zum US-Überwachungsrecht fest und zieht Rückschlüsse auf die Möglichkeit von US-Unternehmen, europäische Datenschutzstandards einzuhalten. Es reiche tatsächlich nicht aus, Daten auf EU-Servern zu verarbeiten, um den Zugriff von Behörden oder Geheimdiensten aus dem EU-Ausland zu verhindern.

Organisationen gibt das insofern Klarheit, als dass das neue Gutachten bestätigt, dass sie bei der Wahl ihrer Software-Anbieter auf Nummer Sicher gehen sollten. Um sensible Mitarbeitendendaten umfassend zu schützen – und sich selbst vor aufsichtsrechtlichen Bußgeldern und Beschwerden oder Klagen von Mitarbeitenden zu schützen – sollten Organisationen Anbieter wählen, die:

- Daten ausschließlich innerhalb der EU verarbeiten, und
- auch ihren Hauptsitz innerhalb der EU haben.

**Dr. Judith Nink, Director Legal & Risk bei SoSafe:**

„Auch fast zwei Jahre nach Schrems-II gibt es für den Einsatz von Anbietern, die von außerhalb der EU auf Daten von EU Bürger:innen zugreifen keine eindeutige und rechtssichere Lösung. Neben dem Damokles-Schwert von Bußgeldern und der Verpflichtung der Abschaltung von Anbietern stehen Unternehmen weiterhin vor der Herausforderung, die Daten ihrer Mitarbeitenden (rechts)sicher und vertrauenswürdig zu verarbeiten. Der sichere Weg ist daher die Auswahl eines innerhalb der EU datenverarbeitenden Anbieters mit Sitz in der EU."

# 06 Ausblick & Handlungsempfehlungen

## Neue Prozesse, neue Bedrohungen – neue Kanäle: Hybride Arbeitsweisen verlangen nach neuen Awareness-Ansätzen

Die Welt hat sich verändert, Cybercrime professionalisiert sich – und auch die Informationssicherheit muss nun eine Entwicklung durchlaufen. Security-Awareness-Maßnahmen müssen sich auf hybride Arbeitsweisen und neueKommunikationskanäle einstellen. Gleichzeitig gilt es, auf die verschärfteBedrohungslage zu reagieren und neue Angriffsarten, die sich Remote Work zunutze machen, zu antizipieren. Diese Umstellung umfasst nicht nur, die Lerninhalte laufendzu aktualisieren. Moderne Awareness-Maßnahmen sollten Mitarbeitende auchinsbesondere auf den verschiedenen neuen Kanälen mit in die Verantwortung für den Schutz ihrer Organisation nehmen – neben klassischer E-Mail-Kommunikation zum Beispiel auch via Telefon oder Kollaborationstool, und mithilfe verhaltenswissenschaftlich fundierter Ansätze wie Gamification und Nudging. Nur so gelingt es Ihnen, die Mitarbeitenden in einer hybriden Arbeitswelt zu erreichen und sie nachhaltig dazu zu motivieren, sich aktiv vor Online-Bedrohungen zu schützen.

## Security Awareness gehört in die Vorstandsebene: Involvieren Sie Ihr Management beim Thema Informationssicherheit

Die aktuelle Cybercrime-Lage wird immer häufiger im Board diskutiert. Denn die Relevanz für die Führungsetage ist dem Thema nicht abzusprechen: Cyberangriffe sind oftmals folgereich für den kurz- und auch langfristigen Geschäftserfolg. Involvieren Sie Ihr Management deshalb aktiv beim Thema Security Awareness. Regulatorische Frameworks und Standards geben sowohl national als auch global rechtliche Pflichten vor und können bei der Entscheidungsfindung helfen. Wichtig ist außerdem: Untermauern Sie den Handlungsbedarf mit Erfolgskennzahlen und KPIs zu den wirtschaftlichen Effekten der Awareness-Maßnahmen statt sich lediglich auf Security-Kennzahlen wie Klickraten zu beziehen. Nutzen Sie dazu Tools, die den ROI der Maßnahmen kontinuierlich bemessen und so den Wert langfristiger Sicherheitsstrategien anschaulich belegen.

58 Gartner (2021). The Top 8 Cybersecurity Predictions for 2021-2022.





## Sicherheit ist eine Sache von Kultur: Etablieren Sie die richtigen Verhaltensweisen und Ansichten unter den Mitarbeitenden

Ihre Sicherheitsmaßnahmen sind nur so gut wie die Sicherheitskultur in Ihrer Organisation. Ist Mitarbeitenden die Relevanz von Informationssicherheit und Awareness-Maßnahmen nicht bewusst, wird sich auch ihr Umgang mit Cybergefahren nicht verbessern. Stärken Sie dieses Bewusstsein durch interne und anhaltende Kommunikation sowie Sensibilisierungsmaßnahmen und rücken Sie umsichtiges Verhalten in den Mittelpunkt aller digitalen Prozesse.

## Ganzheitliche Betrachtung des menschlichen Risikos: Verschaffen Sie sich durch Tools und umfassende Metriken einen Überblick

In Unternehmen fallen zwangsläufig Sicherheitsrisiken an – auch durch menschliches Verhalten. Verschaffen Sie sich mit entsprechenden Tools einen Überblick über diese, um im Ernstfall schnell reagieren und bereits präventiv Maßnahmen ergreifen zu können. Laut Gartner werden schon 2025 fast zwei Drittel aller Organisationen Cyberrisiken als Faktor nutzen, um zu entscheiden, mit wem sie eine Geschäftsbeziehung eingehen.[58] Die Minimierung menschlicher Risiken wird demnach ein entscheidender Faktor für den Erfolg von Unternehmen, den Sie selbst in der Hand haben. Organisationen sollten diese Herausforderung ganzheitlich angehen: Um nachhaltig Risiken zu reduzieren, gilt es, Metriken auf den verschiedenen Ebenen des „Behavioral Security Models" zu erheben und entsprechende Awareness-Maßnahmen zu ergreifen, die Wissen, Motivation, Kontext und Verhalten der Mitarbeitenden positiv beeinflussen.

# Über SoSafe

SoSafe unterstützt Organisationen mit seiner agilen Awareness-Plattform dabei, ihre Sicherheitskultur zu stärken. Die dynamischen Schulungen stellen den Menschen in den Mittelpunkt und verbinden verhaltenspsychologische Erkenntnisse mit smarten Algorithmen – so werden die Mitarbeitenden zur menschlichen Firewall ihrer Organisation. Organisationen fördern damit nicht nur das sichere Verhalten ihrer Belegschaft, sondern können mithilfe kontextbezogener Daten Schwachstellen erkennen, diese angehen und den ROI ihrer Awareness-Maßnahmen messen.

Die Mitarbeitenden durchlaufen personalisierte Micro-Lernmodule und smarte Angriffssimulationen in ihrer alltäglichen Arbeitsumgebung. Die maßgeschneiderten und sorgfältig ausgewählten Inhalte sind dank Gamification gleichermaßen informativ, motivierend und effektiv. Unsere selbstlernenden Systeme reagieren auf Risikoprofile und ermöglichen individuelle Lernerfahrungen. So wird in allen Arbeitsbereichen fortlaufend sicheres Verhalten gefördert.

Die DSGVO-konforme Lösung von SoSafe zeichnet sich dadurch aus, dass sie besonders einfach implementiert, verwaltet und skaliert werden kann und somit Zeit und Ressourcen spart. Organisationen können sich entweder für ein unkompliziertes Self-Service-Modell entscheiden oder Implementierung und Service durch ein Team von Expertinnen und Experten umsetzen lassen.





TEACH

## Motivierendes Micro-Learning

Verhaltenswissenschaftlich fundierte Lernmodule, die Mitarbeitende lieben.

Spielen Sie effiziente und effektive Lernerfahrungen einfach über verschiedene Kanäle aus. Unser dynamisches und zielgerichtetes Training ist motivierend und stärkt die Compliance mit stets aktuellen E-Learning-Modulen, die auf die Ansprüche Ihrer Organisation zugeschnitten sind.

- Sorgfältig ausgewählte, gamifizierte Micro-Lerninhalte und erprobte Lernpfade
- Automatisierte Anpassung der Inhalte an Ihre Richtlinien und Ihr Branding
- Verschiedene Integrationen und einfache LMS-Einbindung über SCORM-Streaming

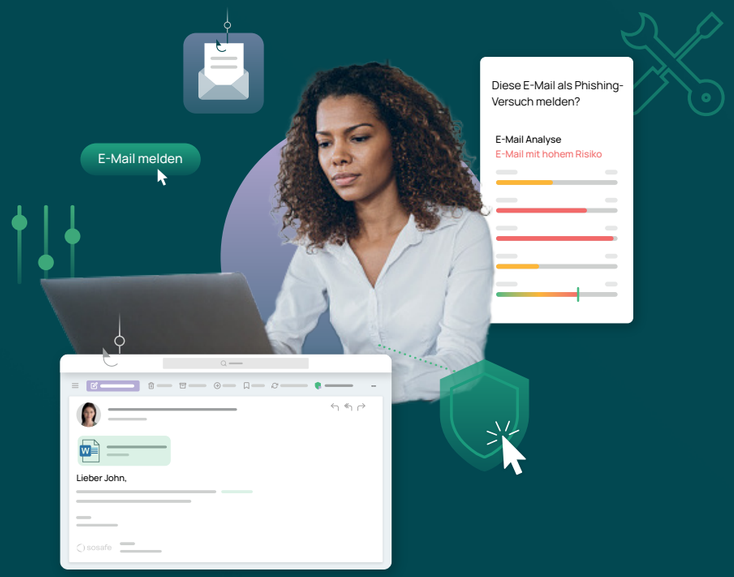
TRANSFER

# Smarte Angriffssimulation

Kontinuierliche und differenzierte Phishing-Simulationen, die messbar sicheres Verhalten stärken.

Automatisieren Sie simulierte Spear-Phishing-Mails basierend auf realen Bedrohungen in Ihrer Branche und dem Risikopotenzial Ihrer Organisation. Über personalisierte Simulationen und kontextbasierte Lernerfahrungen lernen Mitarbeitende effektiv, wie sie Phishing-Attacken erkennen und melden.

- → Massenpersonalisierte Phishing- und Vishing-Simulationen
- → Kontextbasierte Lernseiten mit interaktiven Walkthroughs
- → UX-optimierter Reporting-Button inklusive kontextueller Datenanalyse und Empfehlungen für User








ACT

# Risk Cockpit & Strategisches Reporting-Tool

Verstehen Sie genau, wo Schwachstellen liegen und agieren Sie proaktiv.

Setzen Sie auf strategisches Risk-Monitoring und nutzen Sie unsere umfassenden Analysen, um Risiken in Ihrer Organisation zu bemessen. Einfach Schwachstellen identifizieren und datengetriebene Entscheidungen treffen.

- → Kontextbezogene, umfassende Auswertungen basierend auf technischen und psychologischen KPIs
- → Klare Einblicke in die Bereiche, in denen Verbesserungspotenzial liegt und entsprechende Handlungsempfehlungen
- → Dashboards zum Tracking der Compliance (z. B. ISO/IEC-27001) oder des ROI der Awareness-Maßnahme

SoSafe GmbH
Ehrenfeldgürtel 76
50823 Köln

info@sosafe.de
www.sosafe.de
+49 221 65083800