Cybersecurity im Zeitalter von KI

F.A.Z.-INSTITUT

sopra steria

Inhalt

3 Vorwort

4 Executive Summary

5 Methodik

6 Kapitel 1: KI transformiert Cybersecurity
Interview: Dr. Barbara Korte, Sopra Steria

11 Kapitel 2: Schwachstelle Mensch
Interview: Stefan Beck, Sopra Steria

17 Kapitel 3: KI- trifft auf Fachexpertise
Interview: Olaf Janßen, Sopra Steria

22 Kapitel 4: Gefahren begegnen
Interview: Prof. Timo Kob, Professor an der FH Campus Wien

IMPRESSUM

Haftungsausschluss: Alle Angaben wurden sorgfältig recherchiert und zusammengestellt. Für die Richtigkeit und Vollständigkeit des Inhalts sowie für zwischenzeitliche Änderungen übernehmen Redaktion, Verlag und Herausgeber keine Gewähr.

© Juni 2024

Sopra Steria SE, Hans-Henny-Jahnn-Weg 29, 22085 Hamburg
F.A.Z.-Institut für Management-, Markt- und Medieninformationen GmbH, Pariser Straße 1, 60486 Frankfurt am Main

Verlag: F.A.Z. BUSINESS MEDIA GmbH — Ein Unternehmen der F.A.Z.-Gruppe, Pariser Straße 1, 60486 Frankfurt am Main
Geschäftsführung: Dominik Heyer, Hannes Ludwig

Alle Rechte vorbehalten, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien.

Titelfoto: KI-generiert

Redaktion: Jacqueline Preußer, Dr. Fabian Sickenberger, Fabian Westermeyer, Mira Würzberger
Gestaltung und Satz: Christine Lambert
Lektorat: Juliane Streicher

Genderhinweis: Wir streben an, gut lesbare Texte zu veröffentlichen und in unseren Texten alle Geschlechter abzubilden. Das kann durch Nennung des generischen Maskulinums, Nennung beider Formen („Unternehmerinnen und Unternehmer“ bzw. „Unternehmer/-innen“) oder die Nutzung von neutralen Formulierungen („Studierende“) geschehen. Bei allen Formen sind selbstverständlich immer alle Geschlechtergruppen gemeint — ohne jede Einschränkung. Von sprachlichen Sonderformen und -zeichen sehen wir ab.

VORWORT

Die neuen Cyberrisiken durch generative Künstliche Intelligenz (GenKI; engl. GenAI) sind kein Zukunftsthema – sie sind jetzt da, und zwar branchenübergreifend. Die Ergebnisse der Befragung von 564 Fach- und Führungskräften sowie von 1.003 Erwerbstätigen in Deutschland geben einen Überblick zur derzeitigen Lage. Die Auswertung zeigt, inwiefern Unternehmen und Behörden aktuell betroffen sind und wie sie den Risiken strategisch begegnen.

Die neue Lage erfordert ein Umdenken – eine Security-Strategie, die KI auf der angreifenden Seite berücksichtigt und auf der verteidigenden Seite integriert. Sie sollte darauf ausgelegt sein, mit automatisiertem Lernen eine permanente und vor allem schnelle Anpassung der Abwehrfähigkeiten herbeizuführen. Für Organisationen ist es erfolgsentscheidend, selbst auf KI zu setzen.

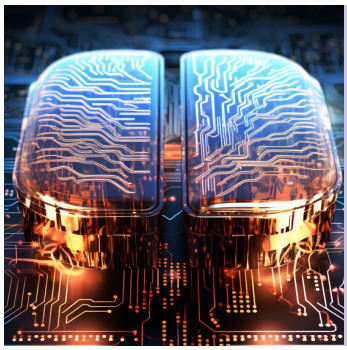
Dazu gehört eine Angriffserkennung, die nicht nur auf klassischen Regeln und bekannten Fällen basiert, sondern durch eine systematische Erkennung von Anomalien ergänzt wird – Stichwort: AI on Big Data. So lassen sich unbekannte Angriffsmuster früher und effektiver erkennen. Zudem benötigen Wirtschaft und öffentliche Verwaltung gut ausgebildetes Personal mit GenAI- und Security-Expertise, das KI-Lösungen trainieren, kontrollieren und integrieren kann. Diese Mischung ist rar gesät, auch das zeigt dieser Report. Doch es gibt Auswege aus diesem Dilemma.

Eine Lösung ist mehr Zusammenarbeit: Noch kocht jeder mehr oder weniger sein eigenes Cybersecurity-Süppchen und konkurriert um die Expertinnen und Experten. Wenn Unternehmen und öffentliche Verwaltung untereinander und übergreifend Ressourcen und Know-how bündeln, um gemeinsame Fragestellungen zu adressieren, werden alle davon profitieren. Dies beinhaltet auch die Kooperation mit Start-ups und Cybersecurity-Partnern.

Eine strategische Neuausrichtung steht jetzt an. Denn nur sie wird Unternehmen und Behörden in die Lage versetzen, Cyberrisiken richtig zu managen. Das Motto sollte lauten: Besser gewappnet mit KI statt hoffnungslos ohne KI.

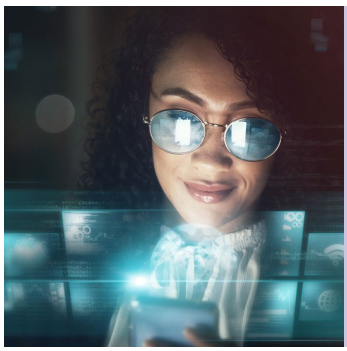
Sopra Steria
F.A.Z.-Institut

Executive Summary



- 73 Prozent der befragten Organisationen sehen durch böswillige KI-Nutzung eine verschärfte Bedrohungslage im digitalen Raum.
- 81 Prozent der Befragten planen, in den nächsten zwölf Monaten in eine höhere Cybersicherheit zu investieren.
- 54 Prozent sagen, dass Organisationen ohne KI-Einsatz in der Cybersecurity zukünftig chancenlos gegen Cyberkriminelle sind.

- Mitarbeitende sind häufig das Einfallstor für Cyberattacken.
- Phishing nimmt zu – und wird schwieriger zu erkennen.
- Nur 48 Prozent der Organisationen schulen ihre Belegschaft regelmäßig zu Cybersecurity.
- 65 Prozent der Erwerbstätigen haben bereits KI im Job genutzt. Klare Richtlinien sind allerdings selten, was Gefahren birgt.



- 34 Prozent der Organisationen nennen neue Schutzmöglichkeiten durch KI als Grund dafür, ihre Cybersecurity zu erhöhen.
- Mehr als die Hälfte der Befragten sieht sich mit einem Mangel an Personal und Expertenwissen im Bereich Cybersicherheit konfrontiert.
- 80 Prozent sind der Ansicht, dass Organisationen zusammenarbeiten sollen, um sich effektiv gegen Cyberangriffe zu schützen.

- Die Befragten sehen die größten Schadensszenarien in den Bereichen Datendiebstahl/-sabotage und Datenverschlüsselung.
- 72 Prozent verstehen Cybersecurity als strategisches Thema, das sie bei jedem neu aufgesetzten Prozess mitbedenken.
- Das Verständnis von Cyberabwehr ist nicht mehr zeitgemäß: Im KI-Zeitalter braucht es einen Paradigmenwechsel zu Cyberresilienz.

Methodik

Für die Studie „Cybersecurity im Zeitalter von KI“ von Sopra Steria und dem F.A.Z.-Institut hat F.A.Z. Business Media | research im April und Mai 2024 zwei Befragungen dazu durchgeführt, wie Organisationen und Erwerbstätige beim Thema Cybersecurity und beim Einsatz von KI aktuell aufgestellt sind.

Fach- und Führungskräfte-Befragung

Hierfür wurden 564 Personen per computergestütztem Web Interview (CAWI) befragt. Diese arbeiten in ihrer jeweiligen Organisation in Fach- und Führungspositionen und verteilen sich auf drei ausgewählte Branchen: 38 Prozent der Befragten sind bei Finanzdienstleistern tätig, darunter insbesondere Banken und Versicherungen. Rund ein Drittel stammt aus der öffentlichen Verwaltung, unter anderem aus der Kommunal-, Landes- und Bundesebene. Etwa ein Viertel gehört zum Bereich Automotive und Zulieferer.

Erwerbstätigen-Befragung

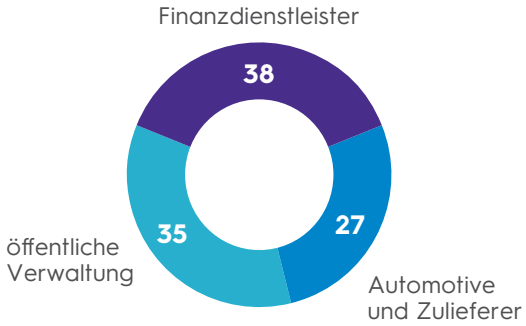
Hierfür wurden 1.003 Erwerbstätige ab 15 Jahren in Deutschland per computergestütztem Web Interview (CAWI) befragt. Die Erhebung ist quotenrepräsentativ für die Merkmale Geschlecht, Alter, Branche und Bundesgebiet (Nord, Ost, Süd, West).

Einordnende Experteninterviews

Vier Experteninterviews ergänzen die Umfrageergebnisse dieser Studie. Die Gespräche liefern Vertiefungen zu den Auswertungen und bieten zusätzliches Hintergrundwissen. Die Interviews und Zitate spiegeln die Meinung der jeweiligen Interviewten wider.

Branche der befragten Organisationen

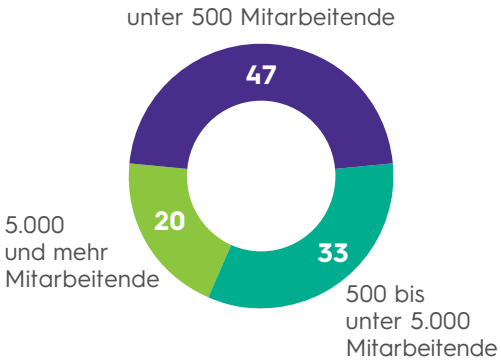
In Prozent der Befragten, n = 564



Quelle: F.A.Z-Institut, Sopra Steria

Mitarbeiteranzahl der befragten Organisationen

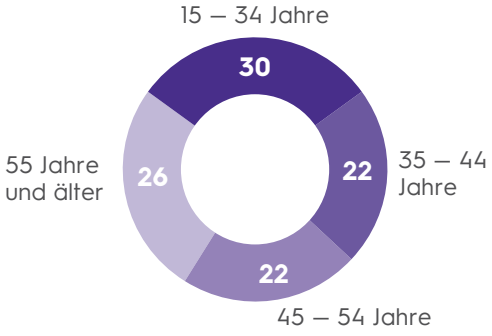
In Prozent der Befragten, n = 564



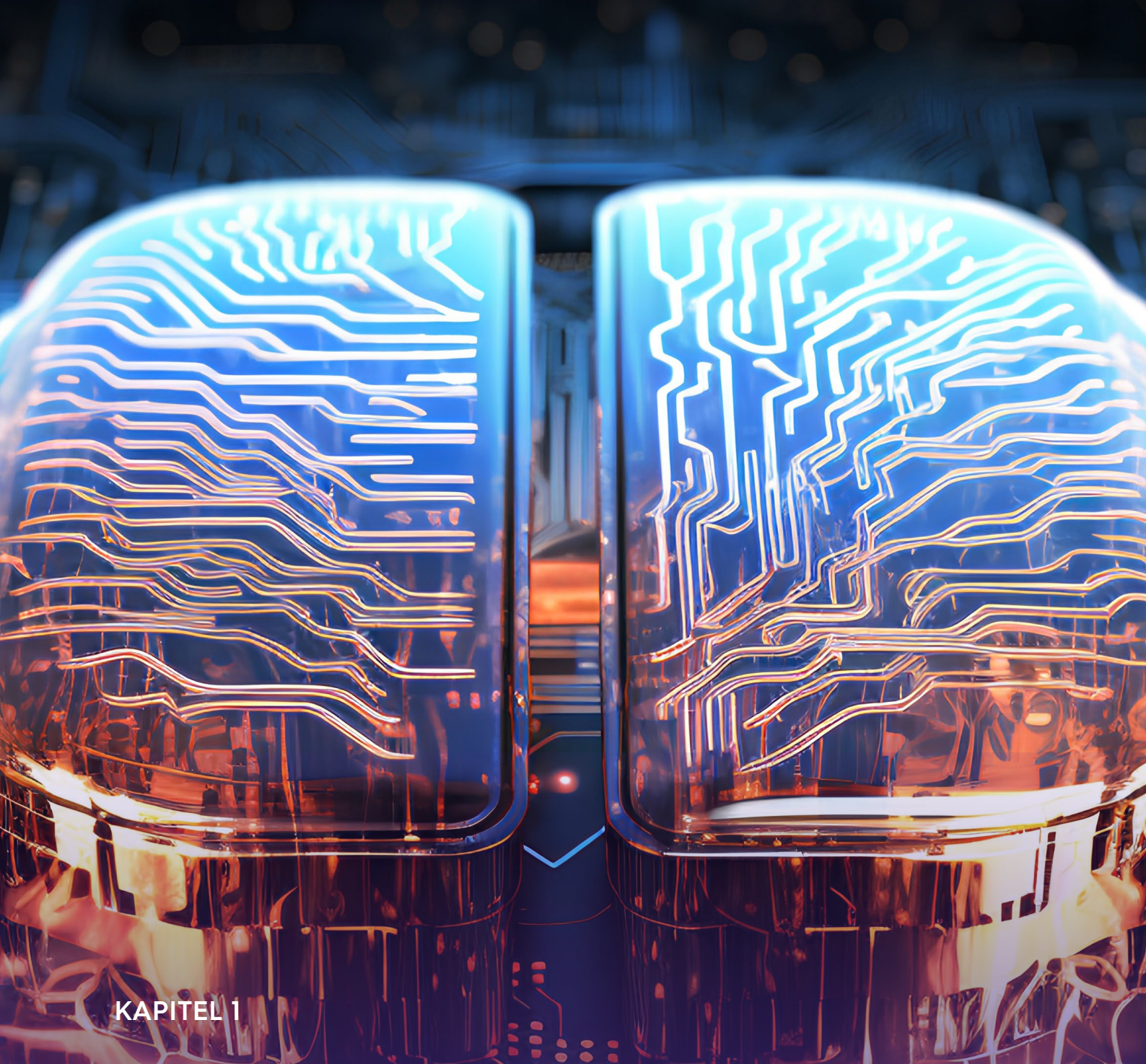
Quelle: F.A.Z-Institut, Sopra Steria

Altersverteilung der befragten Erwerbstätigen

In Prozent der Befragten, n = 1.003



Quelle: F.A.Z-Institut, Sopra Steria



KAPITEL 1

KI transformiert Cybersecurity

Nie war das Arsenal von Cyberkriminellen so mächtig wie heute – ein Grund dafür ist Künstliche Intelligenz. Sie verschärft die Bedrohungslage von Unternehmen und Behörden. Doch KI-Anwendungen können nicht nur schädlich, sondern auch sehr hilfreich sein.

© TensorSpark – stock.adobe.com

Mit rasender Geschwindigkeit verändert KI die Cyberwelt. Im Jahr 2024 ist sie zu einem festen Bestandteil geworden – für diejenigen, die sie für Angriffe nutzen, aber auch für Organisationen, die mit solchen Angriffen umzugehen haben. KI, vor allem GenKI, erleichtert die Massenproduktion und Individualisierung von Cyberattacken. Organisationen müssen sich auf diese neuen Herausforderungen einstellen.

73%

sagen, die böswillige Nutzung von KI hat die Bedrohungslage im Cyberraum drastisch verschärft.

564 Fach- und Führungskräfte

Quelle: F.A.Z.-Institut; Sopra Steria

Die Bedrohung hat sich weiter zugespitzt

Cyberkriminelle nutzen die Technologie, um Attacken zu personalisieren und zu automatisieren. Mit Hilfe von Sprachgenerierung durch GenAI können sie beispielsweise den „Enkeltrick" authentischer wirken lassen. Die KI ermöglicht es ihnen, Beziehungen in sozialen Netzwerken schnell und einfach zu analysieren. Dadurch können sie ihre Angriffe noch individueller ausrichten.

Die meisten Unternehmen und Behörden spüren den dadurch entstandenen Druck: Etwa drei Viertel der befragten Entscheiderinnen und Entscheider geben an, die böswillige Nutzung von KI habe die Bedrohungslage im Cyberraum drastisch verschärft. Auch mit Blick in die Zukunft ist keine Entspannung in Sicht: 93 Prozent gehen davon aus, dass sich bestimmte Bedrohungsszenarien in den kommenden zwölf Monaten zuspitzen werden.

Die Angriffe häufen sich – und werden besser

Mittels KI lassen sich Cyberangriffe besser skalieren. Bei breit angelegten Phishing-Kampagnen können schnell auch kleine Organisationen, die sich selber nicht im Fokus von Cyberkriminellen sehen, zum Opfer werden. Die wahrgenommene Bedrohung hängt aber nicht nur mit der gestiegenen Häufigkeit von Cyberangriffen, sondern auch mit deren höherer Qualität zusammen. Knapp die Hälfte der Befragten sagt daher, durch KI habe die Cyberkriminalität ein ganz neues Niveau erreicht.

Die wichtigsten Motivatoren für mehr Cybersecurity

Aus welchen Gründen möchte Ihre Organisation die eigene Cybersecurity erhöhen?

Fach- und Führungskräfte, die zuvor angaben, in den nächsten zwölf Monaten in die eigene Cybersecurity zu investieren; n = 461

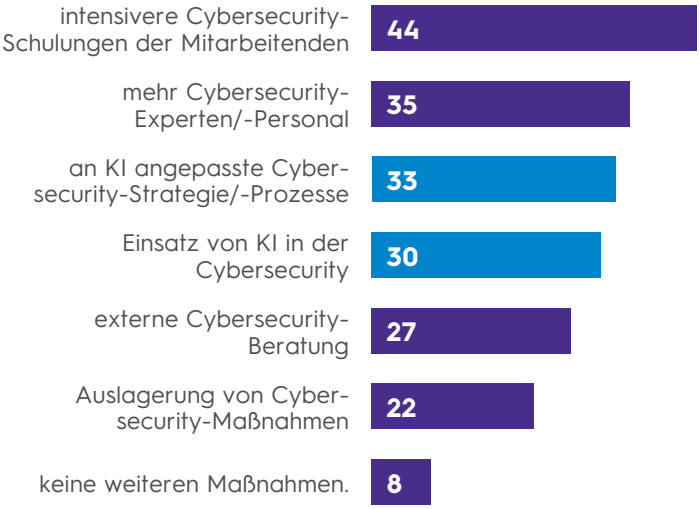
Quelle: F.A.Z.-Institut; Sopra Steria

Nicht später, sondern jetzt

KI-basierte Cyberangriffe sind kein Thema der Zukunft – sondern eines, das sich umgehend auf Cybersecurity-Strategien auswirken muss. Aus diesem Grund halten die meisten Fach- und Führungskräfte zeitnahe Investitionen zum besseren Schutz für nötig: 81 Prozent geben an, im kommenden Jahr in die eigene Cybersecurity investieren zu wollen, um diese zu stärken. Jeder Dritte hat dabei speziell den missbräuchlichen Einsatz von KI im Blick und passt die Cybersecurity-Strategie und die entsprechenden Prozesse daran an. Grundsätzlich sind die geplanten Maßnahmen jedoch breit gestreut.

KI wird immer wichtiger

In welche Bereiche plant Ihre Organisation in den nächsten zwölf Monaten zu investieren, um die eigene Cybersecurity noch einmal zu erhöhen?



Mehrfachauswahl; in Prozent der 564 Fach- und Führungskräfte; ohne „weiß nicht/keine Angabe" (11%)

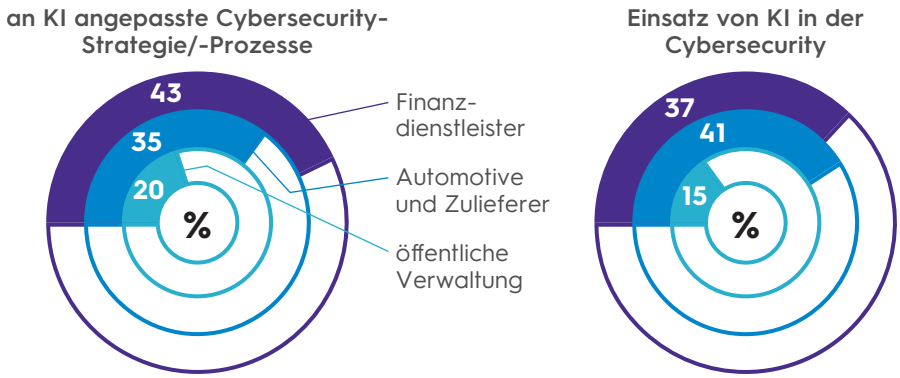
Quelle: F.A.Z.-Institut; Sopra Steria

Die Behörden hinken hinterher

Während die Investitionsabsichten im Bereich Cybersecurity bei den Finanzdienstleistern und im Automotive-Sektor ähnlich ausfallen, sind diese Pläne bei der öffentlichen Verwaltung weniger umfassend. Dies zeigt sich besonders in Bezug auf KI: Eine an KI angepasste Cybersecurity-Strategie oder -Prozesse plant nur jede fünfte Behörde, beim Einsatz von KI in der Cybersecurity sind es 15 Prozent. Die öffentliche

KI erhält nicht überall die gleiche Aufmerksamkeit

In welche Bereiche plant Ihre Organisation in den nächsten zwölf Monaten zu investieren, um die eigene Cybersecurity noch einmal zu erhöhen?



Mehrfachauswahl; ausgewählte Antwortmöglichkeiten; 564 Fach- und Führungskräfte
Finanzdienstleister n = 214; Automotive und Zulieferer n = 153; öffentliche Verwaltung n = 197

Quelle: F.A.Z.-Institut; Sopra Steria

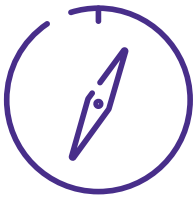
Verwaltung ist hier im Rückstand. Mit 13 Prozent weist sie auch den höchsten Wert derjenigen auf, die mittelfristig keine weiteren Maßnahmen planen.

Mit KI gegen KI-Attacken

Dabei bietet KI zahlreiche Chancen, um präventiv statt reaktiv zu handeln. Mit Hilfe dieser Technologie kann es gelingen, den Angreifern einen oder mehrere Schritte voraus zu sein: KI-Anwendungen helfen bei der Mustererkennung, beim Lernen aus Daten, beim Erstellen von Lageberichten und Prognosen oder beim automatisierten Durchspielen von Analysen. Die Mehrheit der Befragten (54 Prozent) hat erkannt, dass Organisationen ohne den Einsatz von KI in der Cybersecurity in Zukunft keine Chance gegen Cyberkriminelle haben. Das Bewusstsein ist somit vorhanden, die Investitionen in der Breite fehlen noch.

Organisationen kämpfen um den Anschluss

Während Hackergruppen sich darauf spezialisiert haben, die Cybersecurity von Organisationen zu umgehen, können Organisationen angesichts ihres Hauptgeschäfts nur einen Bruchteil an Ressourcen in Cybersecurity investieren. Dies zeigt sich auch bei der Einschätzung der Befragten bezüglich der KI-Kompetenz in Unternehmen und Behörden: Mehr als sieben von zehn gehen davon aus, dass Cyberkriminelle KI deutlich besser für Angriffe nutzen als Organisationen zur Abwehr. Nur etwa jeder Neunte widerspricht dieser These.



71%

meinen, Cyberkriminelle nutzen KI deutlich besser für einen Angriff, als Organisationen dies zur Abwehr eines Angriffs tun.

564 Fach- und Führungskräfte

Quelle: F.A.Z.-Institut; Sopra Steria

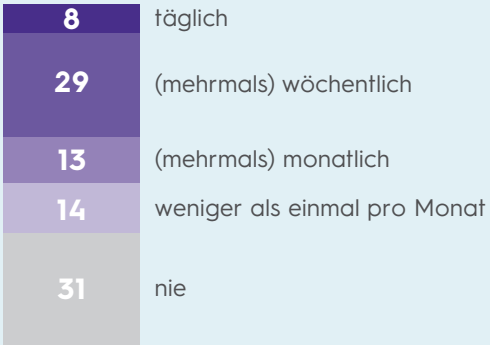
ERWERBSTÄTIGEN-BEFRAGUNG

KI-Tools helfen Erwerbstätigen

Zusätzlich zu den 564 Entscheiderinnen und Entscheidern aus Unternehmen und öffentlicher Verwaltung wurden im Rahmen dieser Untersuchung 1.003 Erwerbstätige befragt. Die Ergebnisse sind mit Blick auf die Relevanz von KI im Arbeitsalltag aufschlussreich: Fast zwei Drittel der Befragten haben im Job bereits KI-Tools wie ChatGPT, DeepL oder Midjourney eingesetzt. 37 Prozent nutzen KI-Anwendungen wöchentlich oder gar täglich. Angesichts der offensichtlichen Vorteile dürfte die Nutzung noch weiter zunehmen: KI-Anwendungen beschleunigen zahlreiche Arbeitsschritte, einige Routineaufgaben lassen sie sogar vollständig automatisiert ablaufen. Das spart Zeit – und das wiederum schafft Ressourcen für kreative und strategisch wichtige Aufgaben.

Mittendrin statt nur dabei

Wie häufig nutzen Sie KI-Anwendungen wie etwa ChatGPT, Midjourney oder DeepL in Ihrem Arbeitsalltag?



in Prozent der 1.003 Erwerbstätigen; ohne „weiß nicht/keine Angabe" (4%)

Quelle: Sopra Steria, F.A.Z.-Institut

INTERVIEW

„All das passiert jetzt – es gibt keine Vorbereitungszeit"

GenAI verändert die gesamte Cyberinfrastruktur grundlegend. Wie es Organisationen gelingen kann, sich in diesem Umfeld zu bewegen, erklärt Cybersicherheits-Expertin Dr. Barbara Korte.

Frau Korte, warum bedeutet der Einsatz von GenAI eine Zeitenwende für die Cybersecurity?

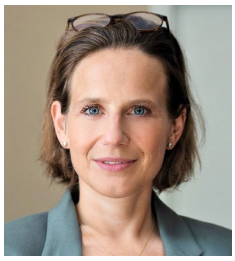
Mit GenAI kann man beispielsweise mit Informationen aus dem Netz individualisierte Phishing-Angriffe erstellen. Sprachmodelle helfen beim Coden sogenannter polymorpher Malware. Die passt sich ihrer Zielumgebung an und kann so nicht entdeckt werden. Diese Kombination aus Individualisierung und Skalierbarkeit ist revolutionär. Cybersecurity muss heute aus dem Kontext heraus Anomalien erkennen, anstatt wie früher nach bekannten Angriffsmustern zu suchen. Und so wie Angreifende Angriffsvektoren mit neuronalen Netzen systematisch durchspielen können, können das natürlich auch Pentester. KI hilft uns also auch.

Wie schützt man sich gegen GenAI-basierte Cyberkriminalität?

Der US-General Stanley McChrystal sagte über den Kampf gegen das Terrornetzwerk Al-Qaida: „It takes a network to defeat a network." Das trifft es auch hier: Wer GenAI-gestützte Angriffe wirksam und effizient bekämpfen will, wird das nur mit Hilfe von neuronalen Netzen schaffen.

Was empfehlen Sie für eine KI-basierte Cybersecurity?

Zunächst muss man sich bewusst sein: All das passiert jetzt – es gibt keine Vorbereitungszeit. Das zeigt auch unser Report. Zweitens dürfen wir nicht erwarten, dass GenAI-Lösungen schon perfekt sind. Die bisherige Entwicklung ist erstaunlich, und doch gibt es viel Luft nach oben. Drittens: GenAI muss gesamthaft gedacht und jeder mögliche Einsatzfall, jede Transferoption für Modelle geprüft werden. Ein vierter Punkt ist, dass ein gutes KI-Fachmodell sowohl KI-Expertise als auch Fach-Know-how braucht. Diese Kombination muss sich personell widerspiegeln. Zudem gilt, was der Neurowissenschaftler Manfred Spitzer generell über KI sagt, auch für die Cybersicherheit: KI wird Fachleute nicht ersetzen – aber Fachleute, die KI einsetzen, werden denjenen, die es nicht tun, eindeutig überlegen sein. Ergo lohnt sich jede Investition in KI-Ausbildung.



Dr. Barbara Korte
ist Expertin für KI in der Cybersicherheit bei Sopra Steria.
barbara.korte@soprasteria.com

54%

sagen, ohne den Einsatz von KI in der Cybersecurity haben Organisationen zukünftig keine Chance gegen Cyberangriffe.

564 Fach- und Führungskräfte
Quelle: F.A.Z.-Institut; Sopra Steria

KAPITEL 2

Schwachstelle Mensch

Menschen machen Fehler. Cyberkriminelle versuchen, diese Fehler zu provozieren und auszunutzen. Daher gilt es, in der Belegschaft ein umfassendes Bewusstsein für die Bedeutung von Cybersecurity zu entwickeln. Bislang sind viele Organisationen aber sehr nachlässig.

© Oxy Grizzly – stock.adobe.com

Nach wie vor stellen Mitarbeitende das Hauptrisiko für die Cybersecurity dar. Unangemessene Reaktionen auf Phishing-Nachrichten und andere Attacken sind in den Augen der Fach- und Führungskräfte auch 2024 die größte Schwachstelle. Trotz des Wissens um die Schwachstelle Mensch schaffen Unternehmen und Behörden keine nachhaltige Awareness.

48%

geben an, dass ihre Organisation die Belegschaft regelmäßig zu Themen der Cybersecurity schult.

564 Fach- und Führungskräfte
Quelle: F.A.Z.-Institut; Sopra Steria

Schulen, schulen und nochmals schulen

Angriffsziele für breit angelegte Phishing-Kampagnen oder Social-Engineering-Angriffe sind alle Mitarbeitenden in Unternehmen und Behörden gleichermaßen. Da diese in der Regel nicht über IT-Fachexpertise verfügen, müssen folglich ein Grundverständnis für Cybersecurity und ein Bewusstsein für die Gefahren von Cyberkriminalität verankert werden. Gelingt dies nicht, bleiben viele sonstigen Anstrengungen wirkungslos. Hierfür ist es nötig, dass Organisationen ihre Mitarbeitenden professionell, regelmäßig und personalisiert schulen. Doch nur 48 Prozent der Befragten geben an, dies momentan zu tun. Dieser Mangel an Schulungen erstreckt sich über alle befragten Branchen.

Über die Gefahren und Potenziale von KI aufklären

Bei jenen Organisationen, die regelmäßig Cybersecurity-Schulungen anbieten, spielt KI inzwischen eine zentrale Rolle. Fast drei von vier Fach- und Führungskräften geben an, ihre Belegschaft systematisch auf durch KI verbesserte Phishing-Angriffe vorzubereiten. Identitätsdiebstahl und Social Engineering werden etwa in der Hälfte der Cybersecurity-Trainings berücksichtigt, während Schulungen zur sicheren Nutzung von KI-Tools bislang die Ausnahme sind.

Der Faktor Mensch als Hauptrisiko

Was sehen Sie aktuell als die drei größten Schwachstellen in der Cybersecurity Ihrer Organisation an?

Mehrfachauswahl mit maximal drei Antworten; Darstellung der drei häufigsten Antwortkategorien; 564 Fach- und Führungskräfte
Quelle: Sopra Steria, F.A.Z.-Institut

ERWERBSTÄTIGEN-BEFRAGUNG

Phishing nimmt zu – und wird besser

Betrügerische Nachrichten sind eine große Gefahr für Organisationen: Zwar werden Spam-Filter und Sicherheitsvorkehrungen in E-Mail-Programmen immer besser, doch auch die Angriffsmethoden der Hacker entwickeln sich weiter. Dass Phishing-Nachrichten immer häufiger im E-Mail-Postfach oder auf dem Smartphone landen, belegt die Erwerbstätigen-Befragung: Dort berichten etwa vier von zehn Befragten über eine Zunahme entsprechender Nachrichten.

41%

der Befragten geben an, in den vergangenen zwölf Monaten mehr Phishing-Nachrichten erhalten zu haben als zuvor.

1.003 befragte Erwerbstätige
Quelle: F.A.Z.-Institut; Sopra Steria

Diese Werte betreffen allerdings nur diejenigen Organisationen, die regelmäßig schulen. Bezogen auf alle Befragten sind die Zahlen nur halb so groß. Aktuell bietet folglich nicht einmal jede achte Organisation Schulungen zum Umgang mit KI-Tools wie ChatGPT im Beruf an.

Sicherheit im Umgang mit KI gewinnen

Im Vergleich der Branchen schulen Finanzdienstleister hinsichtlich KI besonders umfassend, gefolgt von Automotive und – mit deutlichem Rückstand – der öffentlichen Verwaltung. Dies betrifft sowohl Schulungen zu Möglichkeiten des Identitätsdiebstahls als auch zu Social Engineering sowie zur sicheren Nutzung von ChatGPT und Co. in der Organisation. Ein Grund hierfür ist, dass Banken und Versicherungen schon seit einigen Jahren Produkte und Services komplett auch über das Internet zur Verfügung stellen und sich daher der Bedeutung von Awareness-Strategien zur Cybersicherheit bewusst sind.

73%

geben an, Mitarbeitende zu verbesserten Phishing-Angriffen zu schulen, die durch den Einsatz von KI durch Cyberkriminelle entstehen.

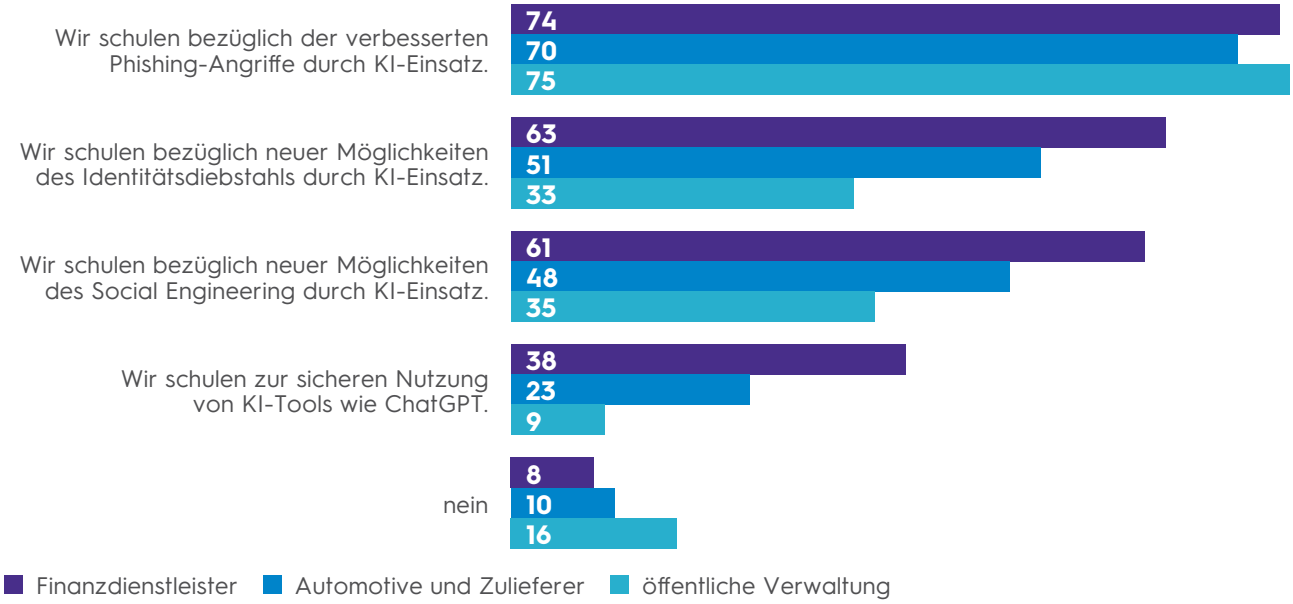
24%

sagen, ihre Organisation schule zur sicheren Nutzung von KI-Tools wie ChatGPT im Arbeitskontext.

Fach- und Führungskräfte, die zuvor angaben, die Belegschaft regelmäßig zu schulen; n = 272
Quelle: F.A.Z.-Institut; Sopra Steria

Die Finanzbranche schult am breitesten

Schult Ihre Organisation die eigene Belegschaft auch hinsichtlich der Bedrohungen und Risiken von KI?



Mehrfachauswahl; in Prozent der Fach- und Führungskräfte, die zuvor angaben, die Belegschaft regelmäßig zu schulen; n = 272
Finanzdienstleister n = 104; Automotive und Zulieferer n = 73; öffentliche Verwaltung n = 95; ohne „weiß nicht/keine Angabe“ (2%)
Quelle: F.A.Z.-Institut; Sopra Steria

Je größer das Unternehmen oder die Behörde der befragten Fach- und Führungskräfte, desto häufiger wird geschult. Auch die thematische Vielfalt der Schulungen nimmt mit steigender Mitarbeiterzahl zu. Dennoch ist es auch für kleine Organisationen wichtig, ihre Beschäftigten für Gefahren zu sensibilisieren. Wenn keine eigene Cybersecurity-Abteilung möglich ist, sollte nicht auch noch am Basisschutz gespart werden.

Große Organisationen sind aktiver

Welche Maßnahmen ergreift Ihre Organisation aktuell, um die eigene Cybersecurity zu verbessern?

„Wir schulen unsere Belegschaft regelmäßig zu Themen der Cybersecurity.“

in Prozent der 564 Fach- und Führungskräfte
unter 500 Mitarbeitende n = 266; 500 bis unter 5.000 Mitarbeitende n = 186; 5.000 Mitarbeitende und mehr n = 112
Quelle: Sopra Steria, F.A.Z.-Institut

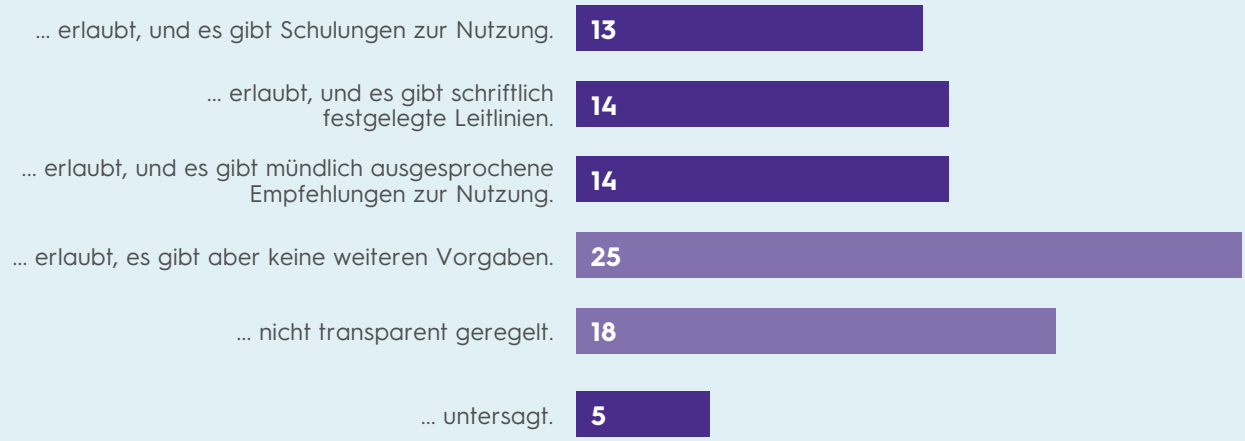
Klare Regelungen für KI-Tools sind selten

Auf die Frage, wie ihre Arbeitgeber den Einsatz von KI-Anwendungen regeln, liefert die Erwerbstätigen-Befragung ein heterogenes Bild: Nur gut eine von vier Organisationen macht klare Vorgaben mit Hilfe schriftlicher Leitlinien oder mündlich ausgesprochener Empfehlungen. Ein Viertel verzichtet hingegen gänzlich auf entsprechende Regelungen, obwohl die Nutzung dort grundsätzlich erlaubt ist. In knapp einem Fünftel der Unternehmen und Behörden fehlen transparente Regelungen. Die Beschäftigten sind sich dort folglich nicht im Klaren darüber, ob und welche Tools sie nutzen dürfen. Wenn Mitarbeitende dieses Vakuum selbst füllen, indem sie auf eigene Faust KI-Anwendungen einbinden, kann dies weitreichende Folgen für den Datenschutz und die Cybersicherheit haben.

KI am Arbeitsplatz

Wie regelt Ihr Arbeitgeber den Einsatz von KI-Anwendungen wie etwa ChatGPT, Midjourney oder DeepL?

Der Einsatz von KI-Anwendungen ist …



Mehrfachauswahl; in Prozent der 1.003 Erwerbstätigen; ohne „weiß nicht/keine Angabe" (18%)
Quelle: Sopra Steria, F.A.Z.-Institut

INTERVIEW

„Awareness-Maßnahmen mit Risiken mitentwickeln“

Mit individuellen Schulungen, Technik und klaren Prozessen können Organisationen Phishing-Attacken entgegentreten. Wie dies im Detail aussehen sollte, erläutert Cybersecurity-Experte Stefan Beck.

Herr Beck, Cyberkriminelle nehmen im KI-Zeitalter gezielt wenig informierte Mitarbeitende ins Visier. Wie sollten Arbeitgeber darauf reagieren?

Es braucht eine Sensibilisierung für eine neue Form von Phishing-Angriffen, die durch KI immer raffinierter werden. Unsere Umfrage zeigt zudem, dass KI-Tools im Büroalltag bereits sehr verbreitet sind. Auch für deren Nutzung braucht es Regelungen und Schulungen mit kontinuierlichen Updates. Generell gilt, dass sich die Awareness-Maßnahmen mit den Risiken mitentwickeln müssen.

Was können Unternehmen oder Behörden konkret verändern?

Aufklärung und Stichprobentests allein reichen heute ebenso wenig aus wie pauschale Maßnahmen. Entwicklerinnen und Entwickler benötigen beispielsweise andere Schulungen als Mitarbeitende mit administrativen Aufgaben. Nur durch individuelle Programme kann das Bewusstsein für Sicherheitsrisiken nachhaltig gestärkt werden. Darüber hinaus sollten Organisationen technische Mittel einsetzen und Prozesse so definieren, dass Phishing-Attacken erfolglos bleiben. Schutzklassen für Dokumente sind ein erster Schritt, um etwa zu verhindern, dass Informationen aus E-Mails in ein Übersetzungsmodell geladen werden und anschließend im Internet kursieren. Zudem können Sandbox-Umgebungen eingesetzt werden, um Schadsoftware abzufangen, bevor sie Schaden anrichtet.

Sollten Organisationen KI nutzen, um die Awareness zu erhöhen?

Absolut. Arbeitgeber können beispielsweise mit KI-Modellen Test-Angriffe personalisieren, um individuelle Awareness-Lücken gezielt zu schließen. Nicht jeder fällt auf dieselben Tricks herein. Lernende KI-Tools können zudem Awareness-Kampagnen an neue oder nicht bekannte Angriffsmuster anpassen. KI ist auch in anderen Bereichen ein Teil der Lösung. Denn mit herkömmlichen Methoden wird es immer schwieriger, enorme Datenmengen in kurzer Zeit auf Indizien für Cyberangriffe zu analysieren. KI-basierte Lösungen können das. Und sie können bislang unbekannte Angriffsmethoden erkennen und abwehren. Perspektivisch stehen wir hier ein Stück weit vor einem Kampf zwischen Maschinen, ähnlich wie in manchen Science-Fiction-Romanen — nur dass es hier eben auch Maschinen gibt, die auf der Seite der Menschheit stehen.

Stefan Beck
ist Senior Manager Cyber Security Public Sector bei Sopra Steria.
stefan.beck@soprasteria.com

26%
erachten die ungeregelte Verwendung von KI-Tools als eine der drei größten Schwachstellen.

564 Fach- und Führungskräfte
Quelle: F.A.Z.-Institut; Sopra Steria

KAPITEL 3

KI- trifft auf Fachexpertise

Nicht alle Organisationen sind beim Thema Cybersecurity auf der Höhe der Zeit. Die Gründe? Fehlendes Personal, fehlendes Know-how und fehlendes Geld. Vor allem in der öffentlichen Verwaltung gefährden diese Faktoren die Sicherheit.

© Angelo-peopleimages.com – stock.adobe.com

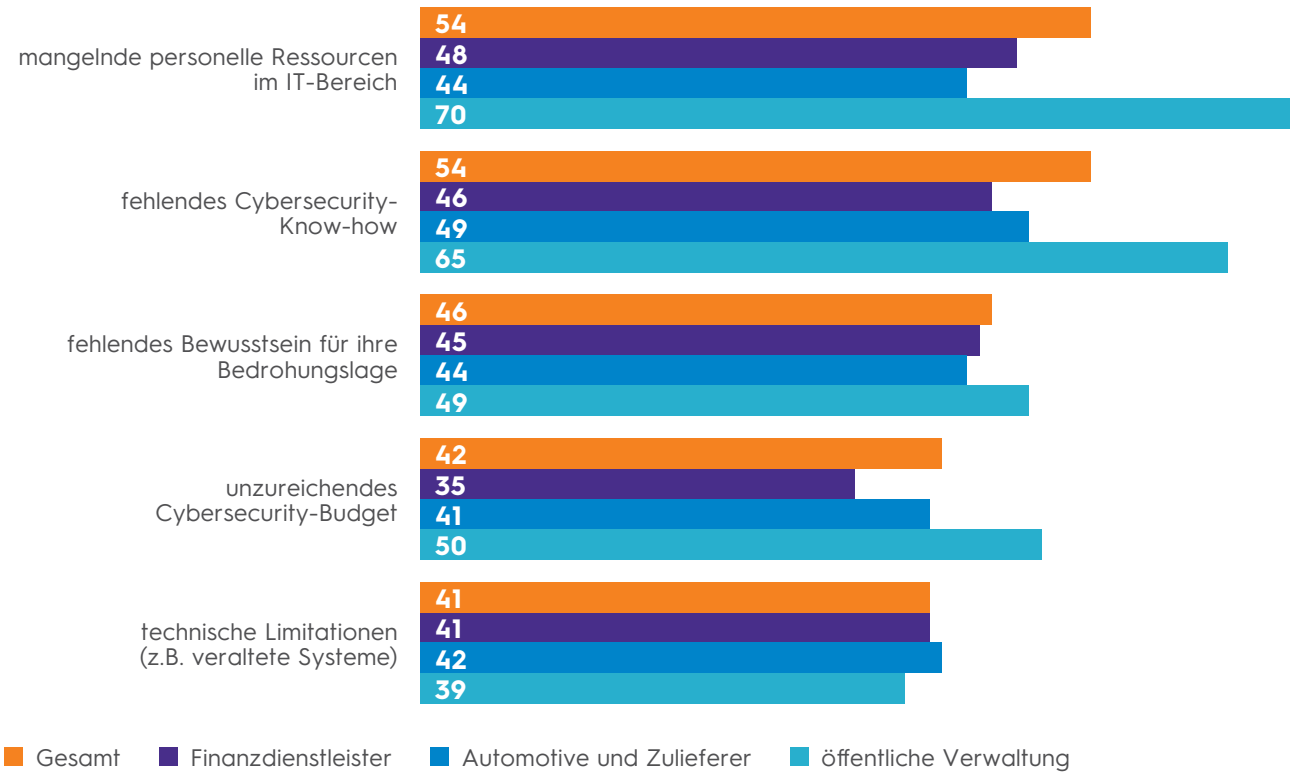
Eine erfolgreiche Cybersecurity hängt vom Zusammenspiel vieler Faktoren ab. Defizite in wenigen Bereichen können schnell die gesamte Sicherheit gefährden. Aktuell erweisen sich der Fachkräftemangel und fehlendes Know-how als größte Hindernisse auf dem Weg zu mehr Cybersicherheit. Eine steigende Nachfrage nach Expertinnen und Experten trifft auf ein knappes Angebot. Daneben fehlt es für 46 Prozent der Befragten am Bewusstsein für die Gefahren, die mit einer unzureichenden Cyberresilienz einhergehen.

In den Behörden sind die Probleme am gravierendsten

Vor allem die Befragten aus der öffentlichen Verwaltung berichten in puncto Personal und Know-how über enorme Schwachstellen. Auch Sofortmaßnahmen wie die IT-Fachkräftezulage sind lediglich ein kleiner Schritt und nicht ausreichend, um solche personellen Engpässe zu beheben. Die verbleibenden IT-Mitarbeitenden müssen immer größere Bereiche schützen und immer mehr Vorfälle überprüfen.

Fehlendes Personal, wenig Know-how

Was hindert Unternehmen und Behörden Ihrer eigenen Einschätzung nach daran, an der eigenen Cybersecurity zu arbeiten?

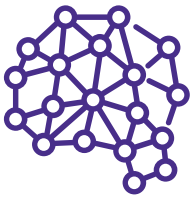


Mehrfachauswahl; in Prozent der 564 Fach- und Führungskräfte
Finanzdienstleister n = 214; Automotive und Zulieferer n = 153; öffentliche Verwaltung n = 197
Darstellung der fünf häufigsten Antworten

Quelle: F.A.Z.-Institut; Sopra Steria

In den Branchen Finance und Automotive fallen beide Aspekte weniger stark ins Gewicht als in der öffentlichen Verwaltung. Ein möglicher Grund ist die verhältnismäßig weniger strenge Regulatorik, die im öffentlichen Sektor oft als Hemmschuh für den Einsatz neuer Technologien wirkt. Ähnlich fallen die Unterschiede beim Budget aus: Auch hier geben mehr Entscheiderinnen und Entscheider aus den Behörden eine unzureichende Finanzausstattung an als jene aus den Unternehmen.

Den Befragten aus den Behörden sind die bisherigen Versäumnisse bewusst: 30 Prozent derjenigen, die in den kommenden zwölf Monaten in die Cybersecurity investieren wollen, geben an, in diesem Bereich bisher zu wenig gemacht zu haben. Im Bereich Automotive sagen dies 22 Prozent, bei den Finanzdienstleistern nur 13 Prozent.



34%

nennen die neuen Möglichkeiten durch KI zum Schutz von IT-Systemen als einen Grund dafür, ihre Cybersecurity zu erhöhen.

564 Fach- und Führungskräfte
Quelle: F.A.Z.-Institut; Sopra Steria

Sofortmaßnahmen und langfristige Umbauten

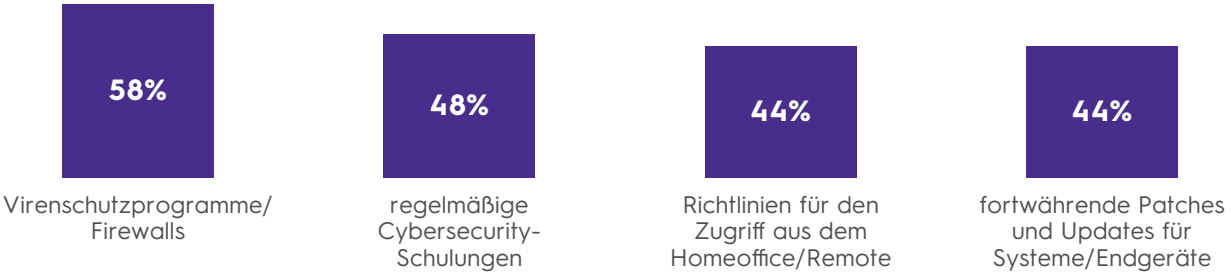
Die beiden meistgenannten Faktoren Personal und Know-how lassen sich nicht schnell und einfach über Nacht ändern. Personal zu gewinnen und Expertise aufzubauen benötigen Zeit. Hier gilt es, mittel- und langfristig zu planen und ein durchdachtes Sicherheitskonzept zu verfolgen. Dazu gehört die Integration von KI in die eigene Sicherheitsarchitektur. Das bedeutet zusätzliche Anstrengungen, die allerdings auf langfristige Sicht das Personal entlasten und die Qualität der Leistungen steigern werden.

KI als Katalysator für Modernisierung

Dieser Aspekt wird von Teilen der Verantwortlichen erkannt: Gut ein Drittel sagt, man wolle die Cybersicherheit verbessern, weil KI neue Möglichkeiten zum IT-Schutz biete. Zusätzlich zur Integration von KI in die Cybersecurity sind Sofortmaßnahmen wichtig: So können etwa technische Updates und die

Basisschutz oftmals vernachlässigt

Welche Maßnahmen ergreift Ihre Organisation aktuell, um die eigene Cybersecurity zu verbessern?



Mehrfachauswahl; 564 Fach- und Führungskräfte; Darstellung der vier häufigsten Antworten
Quelle: F.A.Z.-Institut; Sopra Steria

unverzügliche Investition in grundlegende Schulungen schnell den Basisschutz erhöhen. Das schafft die nötige Sicherheit für größere Änderungen.

Es mangelt bereits an einfachen Hilfsmitteln

Dass manche Organisationen den aktuellen Handlungsdruck noch nicht vollständig erkannt haben, zeigt ein Blick auf den Status quo: Selbst einfachste IT-Grundschutz-Maßnahmen, die das Bundesamt für Sicherheit in der Informationstechnik als zwingend notwendig erachtet, fehlen in zahlreichen Organisationen. Weniger als die Hälfte von ihnen bietet regelmäßig Schulungen zur Cybersecurity an, und lediglich 58 Prozent arbeiten mit Virenschutzprogrammen oder Firewalls. 44 Prozent führen fortwährend Patches und Updates aller Systeme und Endgeräte durch, 38 Prozent testen ihre Systeme aktiv auf Schwachstellen. Potenziellen Angreifern wird durch diese Passivität Tür und Tor geöffnet. Um diese Sicherheitslücken zu schließen, reichen schon niedrigschwellige Maßnahmen aus.

ERWERBSTÄTIGEN-BEFRAGUNG

Datenschutz als Grunderwartung

Die Bevölkerung erwartet, dass Unternehmen oder Verwaltung beim Umgang mit Daten Vorsicht und Verantwortung walten lassen. Doch viele Organisationen tun sich bislang schwer damit, ein hohes Maß an Cybersicherheit zu gewährleisten. Das zeigt die Erwerbstätigen-Befragung. Diese hohen Erwartungen werden in Zukunft sicherlich nicht kleiner: Im KI-Zeitalter mit zunehmendem Datenfokus dürfte die Bedeutung eines verantwortungsvollen Umgangs mit Daten weiter steigen.

84%

„Wenn ich meine Daten einem Unternehmen oder einer Verwaltung gebe, erwarte ich, dass diese alle nötigen Schritte unternehmen, um meine Daten vor Kriminellen zu schützen."

Zustimmungsquote; 1.003 befragte Erwerbstätige
Quelle: F.A.Z.-Institut; Sopra Steria

INTERVIEW

„Kein lästiger Zusatz“

Budgetknappheit, Fachkräftemangel, hohe Anforderungen an die Belegschaft. Wie lässt sich all das im KI-Zeitalter meistern? Darüber spricht Olaf Janßen, Head of Cyber Security bei Sopra Steria, im Interview.

Fach- und Führungskräfte sagen im vorliegenden Report mehrheitlich, dass Cyberkriminelle GenAI besser nutzen als Unternehmen und Behörden. Sind die Angreifer immer einen Schritt voraus?

Für Kriminelle sind Cyberangriffe das Kerngeschäft. Unternehmen und öffentliche Hand machen in der Regel andere Dinge als Cyberabwehr. Sie können dafür oft nicht so viele Ressourcen einsetzen, wie sie benötigen – es sei denn, sie sind Dienstleister auf diesem Gebiet. Um nicht nur mitzuhalten, gilt es, Cybersecurity stärker in das Kerngeschäft zu integrieren. Das gelingt am besten, indem man sich in Ökosystemen organisiert und gemeinschaftlich Strategien findet. Es ist unsinnig, sich gegenseitig Fachkräfte abspenstig zu machen bei einer Aufgabe, die alle betrifft und bei der niemand mit dem anderen konkurriert.

Olaf Janßen
ist Head of Cyber Security bei Sopra Steria.
olaf.janssen@soprasteria.com

Viele Organisationen haben in der Cybersecurity mit Budget- und Personalmangel sowie hohen Kompetenzanforderungen zu kämpfen. Wie lassen sich diese Herausforderungen meistern?

Zunächst einmal ist es wichtig, Cybersecurity nicht als lästigen Zusatz zu betrachten, der nur Geld kostet. Damit steigt der Stellenwert, auch bei der Verteilung von Mitteln. Der viel zitierte Fachkräftemangel ist in der Cybersecurity deutlich zugespitzt. Hier braucht es kooperative Ansätze zwischen Wirtschaft und öffentlicher Hand, um den Personalmangel zu adressieren, Fachkräfte zu fördern und im Ergebnis mehr Fachkräfte zur Verfügung zu haben. Auch Sharing-Modelle sollten kein Tabu darstellen. Denn trotz aller Automatisierungschancen sind hochqualifizierte Menschen unerlässlich, die KI-Modelle trainieren, überwachen und im Security-System integrieren. Ein dritter Strategiehebel ist Outsourcing, also der Einsatz von Managed Security Services, bei denen externe Experten die Sicherheitsüberwachung und -verwaltung übernehmen.

80%

„Um sich effektiv gegen Cyberangriffe zu schützen, sollten Organisationen zusammenarbeiten.“

Zustimmungsquote; 564 Fach- und Führungskräfte

Quelle: F.A.Z.-Institut; Sopra Steria

Welche Cybersecurity-Instrumente lassen sich mit Hilfe von KI verbessern?

Security Operations Center (SOC) und Endpoint-Detection-and-Response-Lösungen (EDR) arbeiten bereits vielfach mit KI-Bestandteilen. Es steckt großes Potenzial in KI bei der Prävention, also im Erkennen von Bedrohungen, noch bevor sie Schäden anrichten. Zudem lässt sich das Mapping regulatorischer Vorschriften automatisieren, um Anforderungen zügiger umzusetzen und vorhandene Regelungslücken schneller zu schließen. Das erleichtert die Einhaltung von Vorschriften und verbessert Sicherheitsmaßnahmen.

KAPITEL 4

Gefahren begegnen

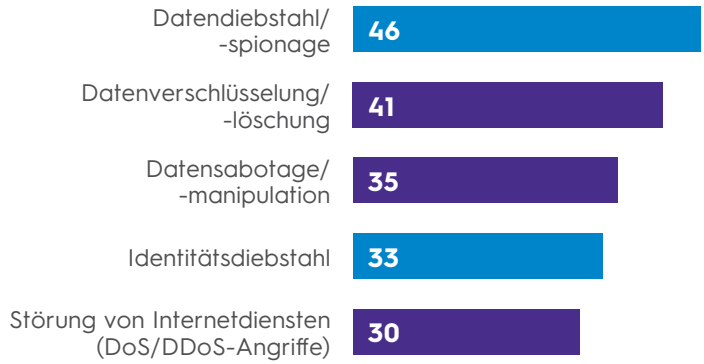
Im Moment sehen sich deutsche Unternehmen und Behörden vielen verschiedenen Gefahrenherden ausgesetzt – von der Datenspionage bis zum Identitätsdiebstahl. Um darauf adäquat zu reagieren, braucht es ein Umdenken hin zu gezielter Cyberresilienz.

© Christian - stock.adobe.com

Daten sind ein wertvoller Schatz für Organisationen und daher eine attraktive Beute für Hacker. In Bezug auf die schädlichsten kriminellen Aktivitäten im Cyberraum nennen die Befragten Szenarien mit Datenbezug, darunter Diebstahl/Spionage, Verschlüsselung/Löschung und Sabotage/Manipulation am häufigsten. Kein Szenario sticht hervor. Die Bedrohungslage ist vielfältig, die Anzahl der potenziellen Angreifer hoch. Der Schutz vor einzelnen Gefahrenquellen reicht daher nicht mehr aus, Organisationen müssen ihre Cybersecurity deshalb breit aufstellen.

Sorge vor Daten- und Identitätsdiebstahl

Welche drei Szenarien im Cyberraum verursachen Ihrer Ansicht nach derzeit den größten Schaden für Organisationen aus Ihrer Branche?



Mehrfachauswahl mit maximal drei Antworten, in Prozent der 564 Fach- und Führungskräfte, Darstellung der fünf häufigsten Antworten

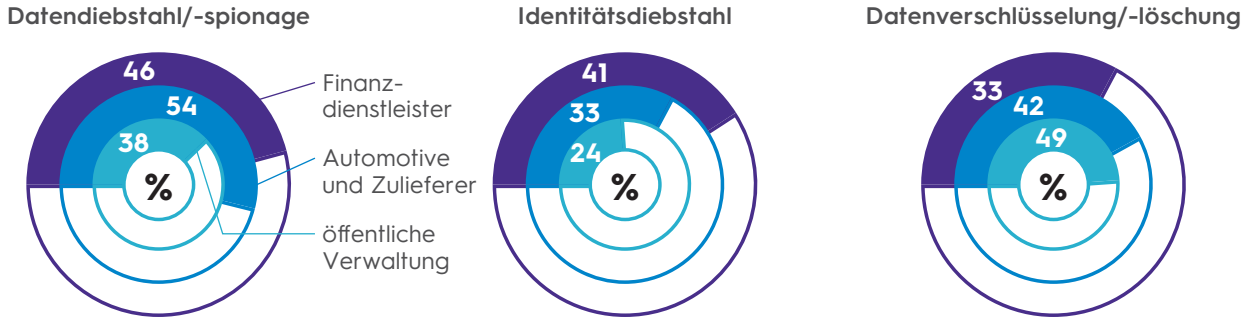
Quelle: F.A.Z.-Institut; Sopra Steria

Branchen kämpfen mit unterschiedlichen Risiken

Den Finanzdienstleistern bereiten Datendiebstahl und -spionage sowie Identitätsdiebstahl die größten Probleme. So bringen etwa KI-Tools, die für Voice Cloning oder Deepfake-Videos genutzt werden, bestehende Identifizierungsverfahren an ihre Grenzen. Andererseits können Finanzdienstleister IT-Tools auch verwenden, um etwa Anomalien im Zahlungsverkehr zu identifizieren und so Cyberkriminalität aufzuspüren. Bei den Automobilherstellern und Zulieferern nennt mehr als die Hälfte der Befragten Datendiebstahl und -spionage als größtes Schadensszenario. Die öffentliche Verwaltung führt vor allem Datenverschlüsselung und -löschung als schädlich für ihren Bereich an.

Identitätsdiebstahl bedroht die Finanzbranche

Welche drei Szenarien im Cyberraum verursachen Ihrer Ansicht nach derzeit den größten Schaden für Organisationen aus Ihrer Branche?



Mehrfachauswahl mit maximal drei Antworten; ausgewählte Antwortmöglichkeiten
564 Fach- und Führungskräfte: Finanzdienstleister n = 214; Automotive und Zulieferer n = 153; öffentliche Verwaltung n = 197

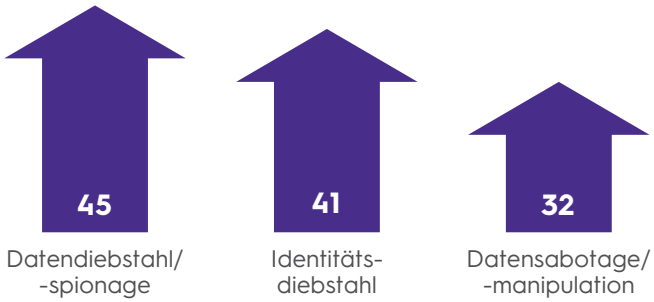
Quelle: F.A.Z.-Institut; Sopra Steria

Auf mehr und neue Schadens-szenarien vorbereiten

93 Prozent der befragten Fach- und Führungskräfte gehen davon aus, dass es in den nächsten zwölf Monaten eine Zunahme von Schadensszenarien durch den Einsatz von KI geben wird. Der stärkste Anstieg wird im Bereich Datendiebstahl/-spionage erwartet, in dem die Befragten auch jetzt schon die größten Schäden durch Cyberkriminelle verorten. Mit KI haben Hacker nun eine weitere Waffe, um Organisationen zielgenauer zu attackieren. Angesichts der neuen technischen Möglichkeiten erwarten die Befragten ebenfalls eine Zunahme beim Identitätsdiebstahl.

Digitaler Diebstahl durch KI auf dem Vormarsch

Welche drei Szenarien werden infolge der Nutzung von KI durch Cyberkriminelle Ihrer Meinung nach in den nächsten zwölf Monaten am stärksten zunehmen?



Mehrfachauswahl mit maximal drei Antworten; ausgewählte Antwortoptionen; in Prozent der 564 Fach- und Führungskräfte, Darstellung der drei häufigsten Antworten

Quelle: Sopra Steria, F.A.Z.-Institut

Nachrichtendienste als Vorbilder

Um den zahlreichen Gefahren im Cyberraum zu begegnen, müssen Unternehmen und öffentliche Verwaltung ihre Perspektive und Fähigkeiten erweitern. Es braucht ein neues Mindset, das sich ein Stück weit an der Denkweise von Nachrichtendiensten orientiert. Organisationen sollten ein wachsames Auge darauf werfen, wie sich die Bedrohungslage entwickelt, und sich in potenzielle Angreifer hineinversetzen. Dabei müssen zunehmend auch ausländische staatliche Akteure berücksichtigt werden, die ein Interesse an (Wirtschafts-) Spionage und Sabotage haben.

Externe Expertise für den Umstieg

Gegen gut organisierte und spezialisierte Angreifer hilft die Zusammenarbeit mit externen Expertinnen und Experten: Dienstleister haben die Gefahren oft besser im Blick und können diese branchenübergreifend und vergleichend einordnen. Sie beobachten die regulatorischen Anforderungen an die Cybersecurity für alle ihre Kunden laufend, womit sie die Regulatorik deutlich effizienter und in

31%

sagen, dass ihre Organisation einen externen Dienstleister für Cybersecurity beauftragt hat.

564 Fach- und Führungskräfte

Quelle: F.A.Z.-Institut; Sopra Steria

besserer Qualität umsetzen können. Dienstleister haben zudem Maßnahmen zur Hand, um die Cybersecurity fest in die DNA der jeweiligen Organisation zu integrieren und das nötige Bewusstsein bei allen Mitarbeitenden zu verankern – um das gesamte technologische Potenzial für mehr Sicherheit auszuschöpfen.

Und: Expertinnen und Experten helfen dabei, den jeweiligen Herausforderungen – so bedrohlich sie auch sein mögen – mit der nötigen Ruhe und Weitsicht zu begegnen. Gegenwärtig hat knapp ein Drittel der Organisationen externe Dienstleister für Cybersecurity engagiert. 27 Prozent der Befragten ziehen in den kommenden zwölf Monaten die Zusammenarbeit mit einer externen Cybersecurity-Beratung in Betracht.

72%

„Cybersecurity ist ein strategisches Thema. Sie wird bei jedem neu aufgesetzten Prozess in unserer Organisation mitbedacht."

Zustimmungsquote;
564 Fach- und Führungskräfte

Quelle: F.A.Z.-Institut;
Sopra Steria

Bedachtes Handeln mit klarer Strategie

Der Stellenwert von Cybersecurity hat in den vergangenen Jahren zugenommen. Rund sieben von zehn Befragten sagen, dass sie Cybersecurity bei neuen Prozessen und Produkten von Beginn an mitdenken. In bestimmten Bereichen ist dies ohnehin regulatorisch geboten wie beispielsweise im Kontext Kritischer Infrastrukturen (KRITIS) oder des Digital Operational Resilience Act (DORA). In der Praxis läuft der Strategie-Shift aber oft noch schleppend.

Paradigmenwechsel in der Cybersecurity

Insgesamt – und insbesondere mit Blick auf die steigende Bedrohung durch GenAI in der Cyberkriminalität – gilt: Unternehmen und Behörden müssen präventiv handeln, statt Angriffe reaktiv zu beantworten. Hierfür benötigen sie eine Sicherheitsstrategie, die mit ihren taktischen und operativen Mechanismen dafür sorgt, dass Organisation, Prozesse und Technologie sich an verändernde Risiken anpassen können. Bedrohungen müssen im Sinne einer hochwertigen Threat Intelligence erkannt werden, bevor Schäden entstehen.

Hierfür braucht es in Zukunft ein Echtzeit-Lagebild, für das die jeweilige Organisation fortlaufend nach Risiken durchforstet wird. Das gelingt nur, wenn alle verfügbaren Quellen pausenlos herangezogen und zusammengeführt werden. KI spielt in diesem Zusammenhang eine entscheidende Rolle: Sie hilft dabei, vor die Lage zu kommen.

INTERVIEW

„Wir sind in einem Wettrennen“

IT-Systeme sind vielen Bedrohungen ausgesetzt. Ein erfolgreicher Hackerangriff hat massive Folgen für die betroffene Organisation und kann sich auch auf die Gesellschaft auswirken. Im Interview erklärt Timo Kob, Professor für Cybersecurity und Wirtschaftsschutz an der FH Campus Wien, wo Unternehmen und Behörden derzeit und zukünftig handeln müssen.

Herr Kob, wie hat sich die Bedrohungslage im Cyberraum für Unternehmen und öffentliche Verwaltungen in den vergangenen Jahren entwickelt?

Die Situation verschärft sich tendenziell seit Jahren. Dafür gibt es mehrere Gründe: Zunächst einmal wird jeder zunehmend abhängiger von IT-Systemen. Wir leben und arbeiten in einer Welt, die sich immer mehr ins Digitale verlagert. Zudem wachsen der Kreis der Angreifer und die potenziellen Angriffsziele seit Jahren. Cyberkriminalität wird durch eine zunehmende Professionalisierung und neue Technologien immer profitabler. Gleichzeitig ist das Risiko von staatlicher Spionage und Sabotage angesichts geopolitischer Spannungen deutlich gestiegen. Vor diesem Hintergrund erhöht sich automatisch die Bedrohungslage.

© Kühnapfel Fotografie

Prof. Timo Kob
ist Professor für Wirtschaftsschutz und Cybersecurity an der FH Campus Wien und Vorstand der HiSolutions AG.

Welche Rolle spielt dabei Künstliche Intelligenz?

KI ist ein Thema, das uns in der Cybersecurity stark beschäftigt. Wir sind in einem Wettrennen zwischen Angreifern und Verteidigern: Beide Seiten bekommen durch KI neue Waffen. Die Lage wird sich bei beidseitigem Einsatz wahrscheinlich nicht fundamental ändern. Aber dieses Gleichgewicht besteht nur, wenn Organisationen sich darauf konzentrieren, KI in der Verteidigung anzuwenden. Wenn es heißt: „Da passiert schon nichts“, kann dieses Zurückfallen schnell in einer Katastrophe enden.

„Cyberkriminalität wird durch eine zunehmende Professionalisierung und neue Technologien immer profitabler.“

Auf wen haben es die Hacker abgesehen?

Wer Geld oder Wissen hat, ist ein attraktives Opfer. Und wer sich nicht schützt, ist es umso mehr. Der Cyberkriminelle ist ein Homo oeconomicus: Wenn er nach ein paar Versuchen nicht ins Haus gelangt, probiert er es bei einer anderen Adresse. Manche Unternehmen lassen durch fehlenden Basisschutz ihre Eingangstür aber quasi unverschlossen. Die Zielgruppe von Hackern reicht von Konzernen

Technologien wie KI bringen eine neue Dynamik in die Cybersecurity und wirken sich auf weite Teile der IT-Sicherheits-architektur aus.

über Kommunen bis hin zu Arztpraxen. Bei Ransomware-Kampagnen werden viele Ziele angegriffen, um die Erfolgschancen zu erhöhen.

Welche Branchen und Organisationen sind besonders stark gefährdet?

Deutschland versteht sich als Land der Hidden Champions, aber das bedeutet nicht, dass diese Unternehmen für potenzielle Angreifer unsichtbar sind. Es gibt viel wertvolles Know-how, aber auch viel Blauäugigkeit im Umgang damit. Vielen ist nicht bewusst, dass sie ein relevantes Ziel für Spionage sind, und entsprechend mangelhaft ist ihre Cybersecurity.

Ein weiterer Aspekt ist die Gefahr bewusster Sabotage durch staatliche oder staatlich finanzierte Akteure. Hier stehen Kritische Infrastrukturen wie Finanzdienstleister, Telekommunikation und Energieversorger besonders im Fokus. Seit dem Ukrainekrieg hat diese Dimension deutlich an Bedeutung gewonnen. Es ist wichtig, dass Unternehmen ihre eigene Cybersecurity auch in Bezug auf staatliche Bedrohungen durchdenken.

„Es ist wichtig, dass Unternehmen ihre eigene Cybersecurity auch in Bezug auf staatliche Bedrohungen durchdenken."

Welche Folgen kann ein erfolgreicher Hackerangriff auf eine Organisation haben?

Nach einem Vorfall kann die Funktionsfähigkeit einer Organisation über Monate hinweg teilweise oder vollständig ausfallen. Da wird es schnell existenzbedrohend auch für größere Player. Bei einem Ransomware-Angriff wissen Organisationen zudem oft nicht mehr, welchen Systemen und Daten sie vertrauen können. Selbst wenn sie das Lösegeld zahlen, müssen sie in den meisten Fällen ihre gesamte IT austauschen und neu aufbauen. Kein PC bleibt unberührt.

Haben Sie dafür ein konkretes Beispiel?

Ein eindrücklicher Fall ist der Landkreis Anhalt-Bitterfeld. Die Verwaltung sah sich 2021 als erste Kommune gezwungen, den Katastrophenfall aufgrund eines Hackerangriffs auszurufen. In den ersten Tagen des Angriffs war die Handlungsfähigkeit der Verwaltung massiv eingeschränkt. So konnten etwa keine Sozial- und

75%

sagen, dass die Bedrohung weiter steigen wird, solange Organisationen nur versuchen, bestehende Gefahren zu bekämpfen, und nicht neue Gefahren vorhersehen.

564 Fach- und Führungskräfte

Quelle: F.A.Z.-Institut; Sopra Steria

Unterhaltsleistungen ausgezahlt werden. Erst nach mehreren Monaten und mit der Hilfe des Bundes konnte wieder Normalität hergestellt werden.

Inwieweit hilft ein Notfallplan, um die Schäden klein zu halten?

Vorbereitungen für den Ernstfall sind zentral. Es ist ein klassischer Fehler, dass Unternehmen ihren kompletten Fokus nur darauf verwenden, Angreifer draußen zu halten. Man kann die Firewall auf technischer Seite noch so hoch bauen, wenn ein Angreifer durch menschliche Fehler ins System gelangt, müssen weitere Schutzmechanismen greifen. Andernfalls hat der Hacker ein leichtes Spiel.

Es braucht zusätzlich Resilienz: Der Schlüsselbegriff ist hier Zero Trust Security, aber die wenigsten setzen das auch konsequent um. Resilienz bedeutet in der Praxis, dass IT-Systeme in mehrere Segmente eingeteilt werden, die bei Bedarf isoliert werden können. Es bedeutet, dass regelmäßige Back-ups wichtiger Daten erfolgen, um Datenverluste und mehrmonatige Ausfälle zu vermeiden. Zudem sollten klare Notfallprozesse und ein schneller Zugang zu einem Incident-Response-Team gewährleistet sein. Mit diesem Vorgehen lassen sich die Konsequenzen stark minimieren.

„KI ist aber nicht nur Werkzeug, KI-Systeme können auch selbst zum Angriffsziel von Hackern werden."

Worauf müssen sich Organisationen zukünftig einstellen?

Viele Prozesse müssen neu gedacht werden. Ich bin seit 30 Jahren in der IT-Sicherheit tätig. Am Anfang war das ein Nischenthema für IT-Administratoren. Es hat sich zwar viel getan, aber viele Vorstandsebenen unterschätzen die Bedeutung der Cybersecurity für andere Unternehmensbereiche. Wir brauchen mehr ganzheitliches Denken.

Ein Beispiel: Immer mehr Organisationen entwickeln und integrieren KI-Anwendungen in ihre Geschäftsprozesse. KI ist aber nicht nur Werkzeug, KI-Systeme können auch selbst zum Angriffsziel von Hackern werden. Die Ergebnisse von KI-Anwendungen sind bereits heute nur schwer nachvollziehbar. Wenn es einem Angreifer gelingt, einen Bias einzuschleusen, können die verfälschten Ergebnisse Organisationen auf Abwege führen. Manipulierte Trainingsdaten oder Parameter in KI-Systemen sind ein neues Gefahrenpotenzial.

Das ist aber nur eine Facette von zukünftiger Cybersecurity: Organisationen müssen sich permanent weiterentwickeln, wenn sie ihr aktuelles Sicherheitsniveau aufrechterhalten wollen. Gleichzeitig gilt es, den Basisschutz nie zu vergessen.

Das Interview führte Fabian Westermeyer.

Ansprechpartnerinnen

Sopra Steria SE
Corporate Communications
Birgit Eckmüller
Hans-Henny-Jahnn-Weg 29
22085 Hamburg
Telefon: (040) 22703-0
E-Mail: birgit.eckmueller@soprasteria.com

F.A.Z.-Institut für Management-, Markt- und Medieninformationen GmbH
Jacqueline Preußer
Pariser Straße 1
60486 Frankfurt am Main
Telefon: (069) 7591-1961
E-Mail: j.preusser@faz-institut.de

F.A.Z.-INSTITUT

sopra steria