

2024

# Lagebericht Security

Der Wettlauf um KI-Vorteile

splunk>



In über 20 Jahren als Sicherheitsexperte und Führungskraft habe ich schon oft erlebt, dass sich die Branche gewandelt hat. Aber dieses Mal ist es anders. Die Cybersicherheit stößt in ganz neue Regionen vor – in das wilde Terrain der Chancen und Risiken generativer KI. Der Splunk-Lagebericht Security 2024 zeigt, dass viele CISOs und Security-Fachleute sich beherzt dorthin aufmachen. Doch was vor ihnen liegt, wissen sie nicht, denn noch ist nicht klar, wie sich neue Compliance-Vorgaben auf den CISO-Verantwortungsbereich auswirken.

Dass Sicherheitsfachleute austesten, wie generative KI in den Cyberumgebungen der Gegenwart zu mehr Resilienz beitragen kann, ist verständlich. Nun sind es aber ganze 93 % der Befragten, die angeben, dass sie bereits künstliche Intelligenz einsetzen. Und für viele ist dies ein entscheidender Innovationswendepunkt. Generative KI wird genutzt, um die Cyberabwehr zu optimieren, um besser informierte Entscheidungen zu treffen und um kritische Kompetenzlücken zu schließen. Allerdings hat mindestens ein Drittel der Befragten keine Richtlinien für generative KI. Und was befürchten sie am meisten? KI-gestützte Angriffe.

Parallel dazu werden die CISOs durch strengere Meldevorschriften der US-Börsenaufsicht SEC und durch die NIS-2-Richtlinie der EU stärker in die Pflicht genommen. Wir glauben aber, dass Security-Abteilungen auch neue Möglichkeiten entdecken werden, ihre Rollen und ihre Teams zu gestalten. Für die CISOs heißt dies, dass sie ihre Prioritäten gegenüber dem Vorstand durchsetzen müssen, und die in der Praxis Sicherheitsverantwortlichen brauchen eine engere Zusammenarbeit mit den ITOps-, Engineering- und Cloud-Teams, damit sie die nötige Transparenz schaffen, die Reaktionszeiten weiter verkürzen und noch mehr Resilienz aufbauen.

Während die Sicherheitsfachleute diesen neuen Weg beschreiten, sind wir bei Splunk gespannt, wie sich das Potenzial generativer KI für die Verteidigung entfalten wird – und wir beobachten zuversichtlich, wie schnell Security-Prioritäten zu Business-Prioritäten werden.



Jason Lee

Chief Information Security Officer, Splunk



# Innovation im Umbruch

Die Lage der Security im Jahr 2024 ist ein wenig widersprüchlich. Trotz der Hindernisse – rasant zunehmende geopolitische Spannungen, strengere Compliance-Vorgaben und eine immer komplexere Bedrohungslandschaft – macht die Branche Fortschritte.

So sagen viele Unternehmen, dass die Cybersicherheit im Vergleich zu früher einfacher zu handhaben sei. Die Unternehmen arbeiten mehr zusammen, erkennen Bedrohungen schneller, und die meisten haben auch die Befugnisse und die Ressourcen, um die anstehenden Probleme zu lösen.

Der Sieg rückt jedoch immer wieder in die Ferne, auch wenn die Abwehr bemüht ist, den Gegner im Wettlauf um KI-Vorteile abzuhängen. Security-Teams machen sich verständlicherweise Sorgen, dass die Angriffe, die sie seit Jahren gekonnt abwehren, durch generative KI nun neue Durchschlagskraft erhalten.

Wir sind der Ansicht, dass die Verteidigung ihrer Aufgabe gewachsen ist. Wie sich generative KI auf die Cybersicherheit auswirkt, bleibt letztlich noch abzuwarten. Aber eines ist sicher: Der Wettlauf hat bereits begonnen.

## Inhalt

- 3 Innovation im Umbruch
- 6 Aufbruch ins KI-Abenteuer
- 14 Die Bausteine der Leader-Unternehmen
- 18 Einschätzung der Bedrohungslage
- 23 Der zunehmende Compliance-Stress
- 27 Es geht voran
- 31 Branchen-Highlights
- 34 Länder-Highlights

# Auf lange Sicht wird Cybersicherheit immer leichter

Vorbeugen und abwehren bedeutet, dass die Erfolge der eigenen Arbeit nur selten sichtbar werden. Und natürlich fragen sich viele: Funktioniert das, was wir machen, überhaupt? Wenn es darum geht, mit den Cybersicherheitsanforderungen Schritt zu halten, gibt es zwei etwa gleich große Fraktionen: 41 % sagen, dass es einfacher geworden ist, 46 % finden es heute schwieriger als früher.

In der Langzeitbetrachtung zeigt sich jedoch ein Bild, das Grund zur Zuversicht gibt: Seit dem Lagebericht Security 2022 ist das Cybersecurity-Management immer einfacher geworden.

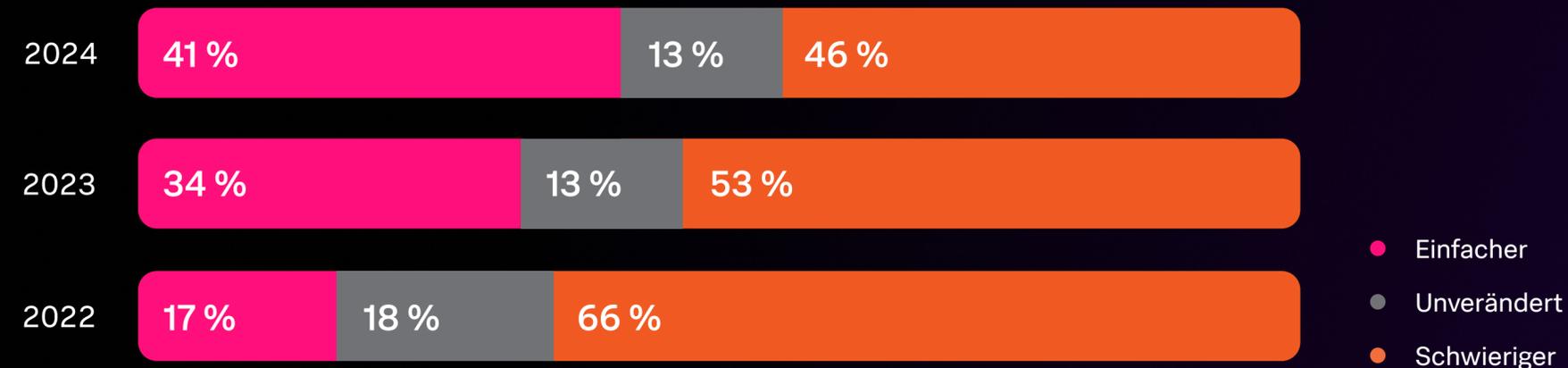
Dieser Befund mag angesichts der zunehmenden Komplexität der Umgebungen und der immer größeren Raffinesse der Angriffe überraschen. Aber für Unternehmen mit gut etablierten Sicherheitskontrollen und -prozessen dürfte es heute tatsächlich einfacher sein, Bedrohungen abzufangen, die auf altbewährte Angriffsstrategien setzen.

Dass in Sachen Cybersicherheit so manches einfacher geworden ist, könnte an der verstärkten Zusammenarbeit liegen: 87 % der Befragten geben an, dass sie enger mit anderen Teams zusammenarbeiten als noch vor einem Jahr. Drei Viertel (75 %) arbeiten insbesondere enger mit den IT Operations zusammen.

Darüber hinaus arbeiten 54 % verstärkt mit den Software-Teams zusammen. Und wenn Sicherheit bereits in der Konzeptions- und der Programmierphase ansetzen kann, wird die Behandlung von Schwachstellen natürlich eher machbar.

Die Unternehmen erkennen Bedrohungen jetzt auch schneller. 55 % der Befragten schätzen ihre MTTD (Mean Time to Detect) bei schweren Incidents, die zu Ausfällen führen, auf maximal 14 Tage. Dies ist eine deutliche Verbesserung gegenüber dem Vorjahr – 2023 trauten sich nur 28 % eine Erkennung innerhalb von zwei Wochen zu. Allerdings haben die Angreifer damit immer noch viel zu viel Zeit.

## Jahresvergleich: Den Cybersicherheitsanforderungen gerecht werden



## Offene Baustellen

Von denjenigen, die finden, dass Cybersicherheit schwieriger geworden ist, nennen 38 % die Komplexität der Bedrohungslandschaft als Grund: Geopolitische Spannungen und Cyberkriegsführung haben zugenommen, IoT, KI und Multiclouds führen dazu, dass die Datenmengen exponentiell anwachsen. Infolgedessen werden Unternehmen, die erst noch dabei sind, die grundlegenden Cybersicherheitskontrollen zu implementieren, Schwierigkeiten haben, zusätzliche Assets und Endpunkte zu schützen. Es fällt ihnen auch schwerer, einfache menschliche Fehler auszuschließen, z. B. Fehlkonfigurationen – und diese sind in diesem Jahr der Angriffsvektor Nr. 1.

Die strengeren Compliance-Vorgaben machen das Ganze noch zusätzlich riskant, und zwar konkret für die Sicherheitsverantwortlichen, die jetzt persönlich für Verstöße ihrer Unternehmen haften. 28 % der Befragten sind der Ansicht, dass regulatorische Vorschriften ihre Arbeit erschweren. Und es ist absehbar, dass neue Auflagen vonseiten der Politik diesen Druck noch weiter erhöhen werden.

Ähnlich wie in den Vorjahren finden 27 % der Sicherheitsteams nicht ausreichend Zeit für die strategische Verbesserung der Cybersicherheit, weil sie zu oft mit Notfalleinsätzen beschäftigt sind. Dies deutet darauf hin, dass langfristige Strategien und Investitionen zu kurz kommen. Die Flut von Warnbenachrichtigungen macht es nicht leichter, den Überblick zu behalten – 26 % empfinden die Menge der Meldungen als belastend.

## KI vor der Cloud

Zu den bemerkenswertesten Erkenntnissen der diesjährigen Umfrage gehört, dass der KI-Hype tatsächlich der Realität entspricht. Fast die Hälfte der Befragten (44 %) nennt KI als eines ihrer drei wichtigsten Handlungsfelder 2024, noch vor der Cloud-Sicherheit.

Ebenso wie Sicherheitsteams die zahlreichen Vorteile von KI erkennen, so attraktiv ist künstliche Intelligenz auch für die Bedrohungsakteure, die nicht an Gesetze und Richtlinien gebunden sind. Bei der Frage, ob KI das Kräftegleichgewicht zugunsten von Verteidigung oder Angriff verschieben werde, sind die Antworten in zwei fast gleich große Gruppen geteilt: 45 % glauben, dass die Gegner am meisten profitieren werden, 43 % sagen, dass am Ende die Abwehr die Oberhand behalten wird.

Der kompetente Aufstieg generativer KI hat die Fantasie beflügelt und man darf sich nun ausmalen, was alles kommen könnte – aber auch folgende durchaus ernsten Fragen müssen aufgeworfen werden: Was kommt realistisch auf uns zu? Was bedeutet KI für die Arbeit im SOC? Werden die Unternehmen interne Richtlinien etablieren, um eine sichere und effektive KI-Nutzung zu ermöglichen? Und wie werden sie diese Richtlinien durchsetzen, ohne Innovationen auszubremsten? Antworten auf diese Fragen zeichnen sich allmählich ab.

## Die wichtigsten Handlungsfelder 2024

44 % Künstliche Intelligenz



35 % Cloud-Sicherheit



20 % Sicherheitsanalysen



# Aufbruch ins KI-Abenteuer

Zur Zeit des Goldrauschs in Kalifornien suchten Hunderttausende von Abenteurern ihr Glück im Wilden Westen. Ähnlich geht es beim KI-Boom unserer Zeit zu. In rasendem Tempo stoßen wir in unbekanntes Gebiet vor, in eine Welt schier unbegrenzter Möglichkeiten und enormer Risiken. Alle versuchen die Ersten zu sein und hoffen, auf eine Goldader zu stoßen. Und das ist durchaus möglich. Man muss sich nur anstrengen.

# Verheißungen und Chancen generativer KI

Generative KI hat den Mainstream erreicht. Unternehmen implementieren KI-Lösungen und wollen damit bewusst ihr Business transformieren. KI liefert personalisierte Produkt-Empfehlungen, kartiert das menschliche Gehirn und führt den Pinsel wie Picasso persönlich – es gibt zahllose Use Cases für praktisch alle Branchen.

Und das sind keine hypothetischen Szenarien. 93 % der Befragten geben an, dass die Produktverantwortlichen ihre Arbeit mithilfe von öffentlichen KI-Tools erledigen. Das bedeutet mehr Arbeit für die Sicherheitsteams, die das Unternehmen vor KI-bedingten Gefahren schützen sollen, vor Datenlecks und anderen Schwachstellen.

Der Optimismus in Bezug auf generative KI ist jedoch so groß, dass selbst die skeptischsten Security-Fachleute überzeugt werden. Die KI-Akzeptanz ist bei den Sicherheitsteams fast so hoch wie in den Unternehmen insgesamt: 91 % der Befragten nutzen

öffentliche generative KI. Mehr noch, sie drücken der Technologie die Daumen: 46 % glauben, dass sich generative KI für ihre Teams als „bahnbrechend“ erweisen wird.

Der Wettlauf um KI-Vorteile ist offenbar in vollem Gange. 50 % der Befragten geben an, dass ihr Unternehmen gerade dabei ist, einen formellen Plan für den Einsatz generativer KI in der Cybersicherheit zu entwickeln, auch wenn diese Pläne noch nicht ausgereift oder abgestimmt sind.

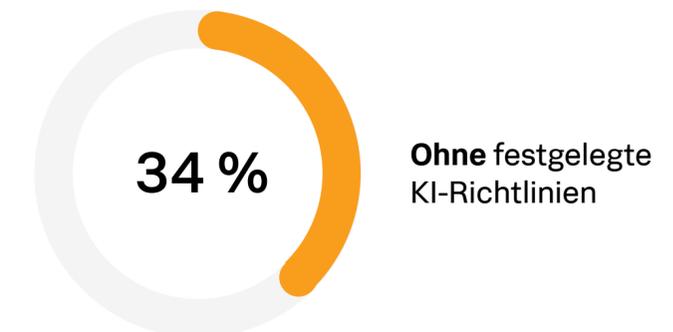
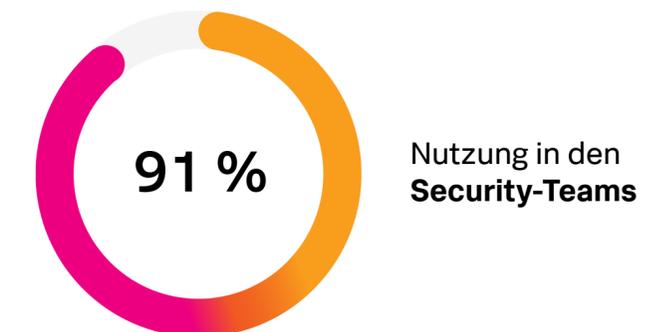
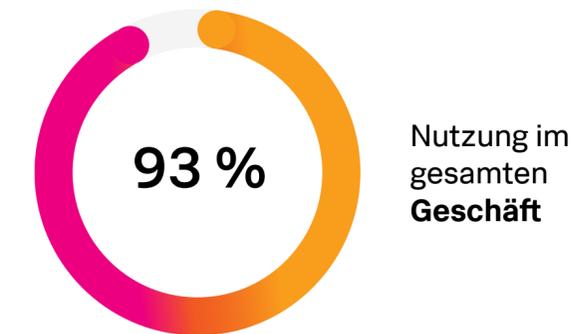
Sicherheit und Innovation schließen einander keineswegs aus – wenn man es richtig angeht. Allerdings fragen wir uns schon, ob die Einführung von KI-Funktionen in den Sicherheitsteams nicht eher durch Druck der Geschäftsführung oder aus betriebswirtschaftlichen Gründen geschieht (oder weil sich niemand vorwerfen lassen will, etwas verschlafen zu haben).



**Noch vor zwei Jahren wäre es geradezu grotesk gewesen, wenn wir gefragt hätten, wie viele End-User im Unternehmen mit öffentlichen KI-Tools arbeiten. Heute gehört generative KI in der Wirtschaft wie selbstverständlich dazu.**

— Kirsty Paine, Field CTO und Strategic Advisor EMEA, Splunk

## Generative KI läuft der strategischen Planung davon



## Generative-KI-Richtlinien sind Pionierarbeit

Wenn sie „Move fast and break things“ hören, reagieren die meisten Sicherheitsfachleute mehr als zurückhaltend. Dennoch könnte die Parole in die richtige Richtung weisen, angesichts des Tempos, mit dem die Unternehmen Innovationen anstreben. Und obwohl die Security-Teams kaum eine Gelegenheit auslassen, Richtlinien festzulegen, haben 34 % der Unternehmen keine verbindlichen Vorgaben für den Umgang mit generativer KI, auch wenn die Technologie bereits großflächig im Einsatz ist.

„Unternehmen, die den Einsatz generativer KI zu stark einschränken, gehen nicht nur das Risiko ein, dass sie hinter der Konkurrenz zurückbleiben, sondern setzen sich auch den Bedrohungsakteuren aus, die keine Hemmungen haben, diese Tools einzusetzen“, sagt Shannon Davis, Principal Security Strategist von Splunk SURGe.

Wenn wir aus der Cloud- und der IoT-Einführung etwas gelernt haben, dann dieses: dass ungeordnete Prozesse und mangelnde Planung am Ende den Sicherheitsteams auf die Füße fallen. Dass auf betriebswirtschaftlichen Druck hin diesen Trends mehr oder weniger blind gefolgt wurde, hat schmerzhaft Folgen gehabt – von irregulären Cloud-Services, die mit privaten Kreditkarten geordert wurden, bis hin zu ungesicherten IoT-Geräten voller Schwachstellen. Also: Die Sicherheitsteams müssen das Innovationstempo irgendwie mit durchdachten, haltbaren Prozessen in Einklang bringen.

Stabile Richtlinien hängen jedoch davon ab, wie gut Technologie verstanden wird. Nur geben 65 % der Befragten zu, dass es ihnen in puncto generativer KI an Wissen und Know-how mangelt. Allerdings darf es nicht allein Aufgabe des Cybersecurity-Teams sein, die übrigen Abteilungen in KI weiterzubilden.

„Unternehmen sollten ein funktionsübergreifendes Governance-Gremium bilden, das die KI-Entwicklung und -Einführung mit einem umfassenden Framework für verantwortliche KI kontrolliert“, sagt Hao Yang, Vice President of AI bei Splunk.

Generative KI hat weitreichende Folgen, sodass auf Steuerebene ganz unterschiedliche Perspektiven und Spezialisierungen erforderlich sind. Das AI Committee von Splunk etwa vereint eine Vielzahl von Geschäftsbereichen und Abteilungen, u. a. Technologie, Recht, Datenschutz, Sicherheit, Personalwesen, Produkteinführung und Marketing.

Natürlich lässt sich auch mit durchdachten Sicherheitsrichtlinien nicht allen Eventualitäten vorbeugen. Doch sie sind die erste und wichtigste Maßnahme, wenn es darum geht, Datenlecks zu unterbinden und neue Schwachstellen minimal zu halten.

## Die KI-Regulierung rollt gerade erst an

Wie die Governance in den Unternehmen, so ist auch die Lage im öffentlichen Raum noch relativ wild und kaum von durchgesetztem Recht geregelt – vorerst jedenfalls. Die KI-Regulierung nimmt jedoch allmählich feste Formen an.

Das [KI-Gesetz der Europäischen Union](#) z. B. sieht einen gemeinsamen Regulierungsrahmen auf der Grundlage von Risikostufen vor. 2023 hat das EU-Parlament den ursprünglichen Vorschlag auf Generative-KI-Modelle ausgedehnt, die nun bestimmten Transparenzanforderungen genügen müssen. Hierzu gehören etwa die Registrierung des Foundation-Modells in einer Datenbank und die Vorhaltung der technischen Unterlagen.

In den USA hat die Biden-Regierung eine [AI Bill of Rights](#) vorgelegt, zu der gehört, dass User informiert werden sollen, wenn sie mit einem automatisierten System kommunizieren. Und sie sollen unter Umständen eine Opt-out-Möglichkeit bekommen, wenn sie statt mit einer KI mit einer realen Person kommunizieren möchten. Solche Leitlinien geben einen Vorgeschmack darauf, welche Maßnahmen künftig aus der Politik noch kommen könnten.

Der zu erwartende Umfang politischer KI-Regulierung dürfte der Grund dafür sein, dass 45 % der Befragten eine bessere Ausrichtung an Compliance-Vorgaben als wichtigsten Optimierungsbereich nennen, und zwar direkt nach Datenlecks. Wer sich in diesem Punkt nicht abhängen lassen will, muss sich aber zuerst gründlich den internen Compliance-Kontrollen widmen.



**Unternehmen sollten ein funktionsübergreifendes Governance-Gremium bilden, das die KI-Entwicklung und -Einführung mit einem umfassenden Framework für verantwortliche KI kontrolliert.**

— Hao Yang, Vice President of AI, Splunk

# Generative KI: Freund oder Feind?

Welche Seite hat mehr von generativer KI?  
Die Befragten sind geteilter Ansicht.



# 43%

Die Abwehrenden  
profitieren am meisten.

# 12%

Die Vorteile  
gleichen sich aus.

# 45%

Die Angreifenden  
profitieren am meisten.

# Generative KI als Security-Beistand

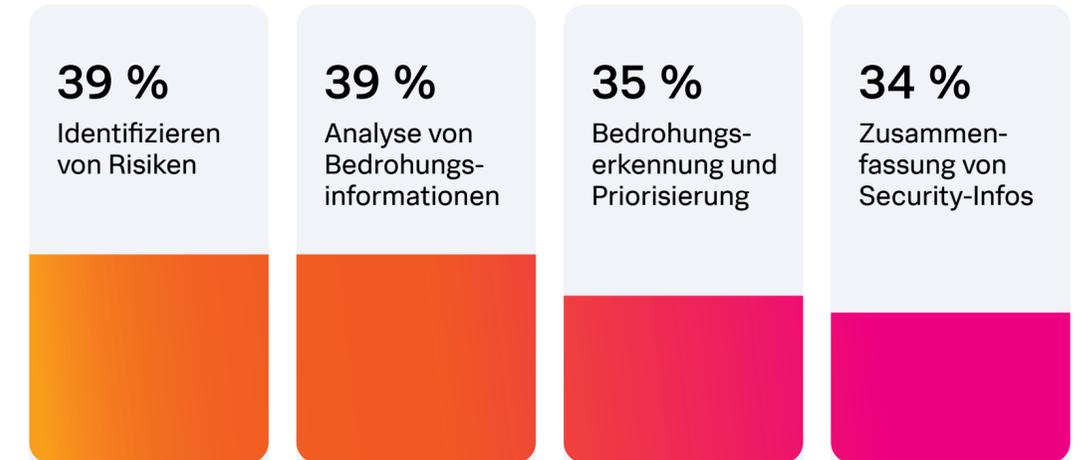
Wie generative KI wahrgenommen wird, ändert sich schnell. Noch vor acht Monaten waren in unserem [CISO-Report](#) nur 17 % der Meinung, dass generative KI der Abwehr einen Vorteil verschaffen wird. Nun ist fast die Hälfte (43 %) dieser Ansicht.

Immer mehr Anbieter integrieren KI-Funktionen in ihre Produkte – sie führen damit vor Augen, welchen Nutzen die Technologie in Sicherheitsworkflows haben kann, und aufseiten der Abwehr werden diese Möglichkeiten auch erkannt.

Es besteht zwar weiterhin das Risiko neuartiger KI-gestützter Angriffe und von Data Poisoning, doch das bleiben bislang Ausnahmeerscheinungen.

Die Verteidigung ist offenbar recht zuversichtlich und insgesamt der Ansicht, dass generative KI für eine Reihe von Use Cases gut zu gebrauchen ist. Als wichtigste Anwendungsbereiche werden die Analyse von Bedrohungsinformationen (Threat Intelligence Analysis) und die Risikoidentifizierung genannt.

## Die wichtigsten KI-Use-Cases im Bereich Cybersicherheit



### Realistische Use Cases generativer KI in der Praxis



#### Identifizieren von Risiken

KI kann risikobasierte Warnmeldungen (Risk-based Alerting) verbessern, indem sie Datensätze zusammenführt, sodass die Analysten mehr Kontext bekommen. Große Sprachmodelle (LLMs) leisten dies in einer Geschwindigkeit, die weit über menschliche Kapazitäten hinausgeht.



#### Analyse von Bedrohungsinformationen

LLMs können die in Threat Intelligence Reports beschriebenen Indicators of Compromise (IoC) und MITRE-ATT&CK-Techniken auslesen. Damit würden sich die Teams eine Menge Schinderei ersparen und könnten schneller zu tiefergehenden Analysen gelangen.



#### Bedrohungserkennung und Priorisierung

Die Sortierung und Priorisierung von Warnmeldungen ist eine Aufgabe, die besonders anfällig für Fehlklassifizierungen aufgrund von Alarmmüdigkeit und Irrtum sind. Generative KI kann nicht nur mehrere Bedrohungen parallel verarbeiten, sondern außerdem die Genauigkeit verbessern.



#### Zusammenfassung von Security-Infos

Generative KI kann Nachrichten und Texte schnell, gründlich und präzise zusammenfassen, sodass Sicherheitsteams ohne großen Zeitaufwand auf dem Laufenden bleiben – z. B. zur Cybersecurity-Verordnung ([Executive Order on Improving the Nation's Cybersecurity](#)) von Präsident Biden.

## KI kann den Security-Fachkräftemangel abfedern

Qualifizierte Fachkräfte sind das, was ein SOC ausmacht. Viele Unternehmen haben aber weiterhin mit dem Fachkräftemangel in diesem Bereich zu kämpfen. Generative KI könnte zumindest übergangsweise für Entlastung sorgen.

86 % der Unternehmen glauben, dass es ihnen mit generativer KI eher gelingt, Cybersecurity-Berufseinsteiger für sich zu gewinnen, und 58 % meinen, dass generative KI das Onboarding von Berufseinsteigern beschleunigen könnte. 90 % sagen, dass die Einsteiger mit Unterstützung durch generative KI ihre SOC-Kompetenzen im Unternehmen entwickeln könnten. Hierzu könnten ganz grundlegende Aufgaben wie das Schreiben eines Python-Skripts oder das Einrichten von Testumgebungen gehören.

Aber auch für erfahrene Sicherheitsfachleute wird generative KI eine Art Kraftverstärker sein. 65 % glauben, dass sie dadurch produktiver werden, weil generative KI z. B. Infos und Nachrichten für Analysten effizienter zusammenfassen, Recherchen beschleunigen und die Entwicklung von Erkennungen erleichtern kann.

Die Angst, dass KI Arbeitsplätze vernichtet, ist zwar nicht ganz unbegründet – etwa die Hälfte der Befragten (49 %) schätzt, dass generative KI einige der bestehenden Security-Rollen obsolet machen wird –, doch wahrscheinlicher ist es, dass KI hilft, neue Talente heranzuziehen und Fachkräfte vor dem Burn-out bewahrt. Vielleicht mischt KI auch nur die Rollen der Security durch, wenn neue Aufgabenbereiche wie Prompt Engineering entstehen.

## Wie generative KI Qualifikationslücken schließen könnte

**86 %** glauben, dass KI helfen kann, mehr Nachwuchskräfte einzustellen



**65 %** glauben, dass KI erfahrene Sicherheitsfachleute produktiver macht



# Generative KI als Bedrohungsverstärker

Zu Recht machen sich die Sicherheitsteams Sorgen, dass generative KI das Arsenal der Angreifer um neue Waffen erweitert. 45 % der Befragten sind der Ansicht, dass von generativer KI letztlich die Cyberangreifer profitieren. 77 % meinen, dass KI die Angriffsfläche in besorgniserregendem Maße vergrößert.

## Bekannte Angriffe kommen mit KI zurück

Welche bislang ungekannten Bedrohungen wird generative KI auf die Welt loslassen? Wahrscheinlich wird es eher so sein, dass generative KI nicht einen Sturm neuartiger Angriffe entfesselt, sondern vielmehr die bekannten Bedrohungen verstärkt und vervielfacht, mit denen die Sicherheitsteams bereits zu kämpfen haben.

32 % der Befragten befürchten am meisten, dass Schadakteure generative KI einsetzen, um vorhandene Angriffsformen weiter zu optimieren, etwa indem sie damit Phishing-E-Mails generieren, die von genuinen Schreiben kaum zu unterscheiden sind, oder wenn sie KI den Code ihrer Schadroutinen überarbeiten lassen. Andere, eher opportunistische Hacker, die weniger versiert sind, könnten mit generativer KI ihre Social-Engineering-Attacken verschärfen. 28 %



**Es ist wie bei der Frage: ‚Würden Sie eher gegen eine Ente kämpfen, die so groß wie ein Pferd ist, oder gegen 100 Pferde, die so groß sind wie Enten?‘. Eine einzige Bedrohung wäre wohl leichter anzugehen, doch generative KI wird leider das andere Szenario Wirklichkeit werden lassen und als Multiplikator bekannter Angriffe agieren.**

— Kirsty Paine, Field CTO und Strategic Advisor EMEA, Splunk

der Befragten befürchten außerdem, dass bekannte Angriffe durch generative KI im Umfang deutlich zunehmen werden.

## Generative KI ist datenhungrig

Nicht alle KI-Bedrohungen kommen von außerhalb. 77 % der Befragten gehen davon aus, dass mit dem zunehmenden Einsatz generativer KI auch mehr Datenlecks einhergehen. Allerdings räumen nur 49 % entsprechenden DLP-Lösungen (Data Leakage Prevention) aktiv Priorität ein – vielleicht deshalb, weil es noch gar nicht viele Lösungen gibt, die den Datenfluss in die und aus den neuen KI-Tools kontrollieren können.

Das mangelnde Wissen über generative KI gibt diesen Befürchtungen zusätzliche Nahrung. Wenn 65 % der Sicherheitsverantwortlichen eingestehen, dass sie generative KI nicht vollständig verstehen, dann kann man davon ausgehen, dass Nicht-Security-Funktionen noch mehr im Dunklen tappen. Ohne angemessene Ausbildung werden die End-User zwangsläufig Fehler machen und z. B. LLMs mit sensiblen Unternehmensdaten füttern. Ausbaden müssen das dann die Sicherheitsteams.

## Generative KI im Dienste der Angreifer

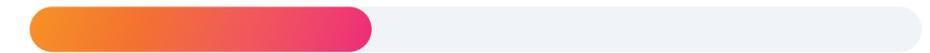
**32 %** KI macht bekannte Angriffe effektiver



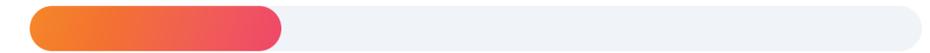
**28 %** KI erhöht das Volumen bekannter Angriffe



**23 %** KI schafft neue Angriffsformen



**17 %** KI dient zur Ausspähung

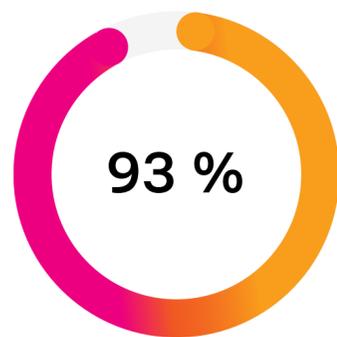


# Ein Ausblick in die KI-Zukunft

Wie wird sich generative KI weiter entwickeln? Leider kann niemand die Zukunft vorhersagen, aber wir wissen, dass die Sicherheitsteams sich schon geraume Zeit mit KI-Formen wie maschinellem Lernen (ML) beschäftigen. 93 % der Befragten sind überzeugt, dass diese Erfahrungen den künftigen Umgang mit generativer KI prägen werden.

Viele Unternehmen haben durch bisherige ML-Tools schon eine Ahnung davon, welche Produktivitätssteigerungen mit KI möglich sind. 92 % profitieren bereits erheblich. Die Technologie ist jedoch keineswegs unfehlbar und erfordert besondere Sorgfalt: 73 % sagen, dass Tools mit klassischen KI- und ML-Funktionen bisweilen falsch positive Ergebnisse liefern, und 91 % geben an, dass die KI-Systeme erst angepasst werden müssen. In vergleichbarer Weise ist auch bei generativer KI eine gewisse Kontrolle erforderlich, etwa um Halluzinationen zu erkennen und zu verhindern, weil die Ergebnisse sonst kaum brauchbar sind.

Die Pioniere der Branche, die schon solide praktische Erfahrungen mit bisherigen KI- und ML-Funktionen gesammelt haben, werden die Reise Richtung generativer KI vermutlich auf der Überholspur unternehmen.



sagen, dass ihre Herangehensweise an generative KI von ihren Erfahrungen mit ML abhängen wird

# Die Bausteine der Leader-Unternehmen

Im Wettlauf um KI-Vorteile gegenüber den Angreifern richten manche Unternehmen eigene Kompetenzzentren ein und wollen dort ausgereifere Cybersecurity-Verfahren entwickeln. 2024 finden 47 % der Befragten, dass ihre Sicherheitsprogramme bereits „extrem fortgeschritten“ sind. Diese Gruppe stufen wir als Leader ein. Und wir vergleichen ihre besonderen Merkmale und ihre Antworten auf die Umfrage mit denjenigen der Kohorte, die ihre Programme als „im Aufbau befindlich“ bezeichnen.



Zunächst einmal sind die Leader zuversichtlich, dass sie mit der Entwicklung der Bedrohungslage Schritt halten können. 49 % von ihnen finden, dass die Anforderungen an die Cybersicherheit heute leichter zu managen sind. Bei den Befragten, deren Security-Programme erst im Aufbau begriffen sind, teilen nur 29 % diese Einschätzung. Die Leader übertreffen die Vergleichsgruppe der Nachzügler noch in etlichen weiteren Punkten; ihre Verfahren lassen sich insofern als Goldstandard betrachten.

### Erfolgreiche Teams bekommen, was sie brauchen

Leader-Unternehmen fallen nicht vom Himmel, sondern haben hart daran gearbeitet. Ihr Erfolg ist nicht zuletzt Ausdruck enger Kontakte zum Vorstand und den Stakeholdern auf wirtschaftlicher Seite, einer abteilungsübergreifenden Zusammenarbeit und stabiler Investitionen. Die Leader-Sicherheitsteams bekommen das Budget, das ein proaktives Vorgehen erst möglich macht: 67 % werden ihre Ausgaben für Cybersicherheit in den nächsten ein bis zwei Jahren deutlich steigern; bei der Vergleichsgruppe der Teams in den Aufholunternehmen ist dies nur bei 28 % der Fall.

Die engen Verbindungen zur betriebswirtschaftlichen Seite des Unternehmens zahlt sich für die Leader auch aus. Ganze 95 % sagen, dass sie ausreichende Ressourcen und Befugnisse haben, um Herausforderungen anzugehen – das entspricht den Ergebnissen unseres [CISO-Reports](#), demzufolge 47 % der CISOs mittlerweile direkt dem CEO unterstellt sind.

### Leader setzen auf Zusammenarbeit und Resilienz

Der Brückenschlag zur geschäftlichen Seite bedeutet nicht nur, dass die Geschäftsführung ein offenes Ohr für die Security hat. Es gehört auch die Zusammenarbeit mit den anderen technischen Bereichen des Unternehmens dazu. Die Leader-Unternehmen arbeiten vor allem mit den folgenden Teams enger zusammen:

Zusammenarbeit mit	Leader-Unternehmen	Aufhol-Unternehmen
Software-Engineering	56 %	46 %
Engineering Operations	51 %	31 %
IT-Operations	76 %	67 %

Die Zusammenarbeit erstreckt sich auch auf die Compliance. 49 % der Leader stimmen voll und ganz der Aussage zu, dass Compliance eine Aufgabe ist, die alle im Sicherheitsteam angeht; in den Aufhol-Unternehmen liegt dieser Anteil bei nur 27 %.

Den Leader-Unternehmen ist auch bewusst, dass in puncto digitaler Resilienz viel auf dem Spiel steht. Ihre Zustimmung fällt deutlicher aus, wenn sie gefragt werden, wie sich eine stärkere digitale Resilienz auswirkt, nämlich in mehr Innovation (41 %), weniger Geschäftsunterbrechungen (39 %) und in der Vermeidung von Compliance-Geldbußen (39 %). Das dürfte daran liegen, dass den Leadern die Geschäftslogik vertrauter ist.



**Ein höherer Cybersecurity-Reifegrad ist ohne Engagement der Geschäftsleitung praktisch nicht zu erreichen.**

— Jason Lee, CISO von Splunk

## Innovationen dank generativer KI

Die Leader-Unternehmen sind auch eher dazu geneigt, Innovationen mittels KI voranzutreiben. Bei 48 % ist dies ein Vorhaben mit oberster Priorität – unter den Aufhol-Unternehmen nur bei 30 %. Generative KI hat sich bei den Leadern auch in den Security-Teams selbst stärker etabliert: 75 % der Leader geben an, dass bei ihnen die meisten Leute in den Sicherheitsteams generative KI einsetzen, in der Vergleichsgruppe sind es lediglich 23 %.

Im Vergleich mit den Aufhol-Unternehmen gehen die Leader-Unternehmen beim Einsatz generativer KI methodischer und weniger experimentell vor:

- **82 % der Leader haben Sicherheitsrichtlinien zum Einsatz generativer KI etabliert – bei den Aufholunternehmen sind es nur 46 %.**
- **55 % der Leader haben einen Plan zu Use Cases generativer KI in der Cybersicherheit formuliert – das können von den Aufhol-Unternehmen nur 15 % von sich sagen.**

## Leader agieren und reagieren schneller

Ein hoher Cybersecurity-Reifegrad heißt nicht, dass weniger Angriffe vorkommen. Sondern dass die Leader-Unternehmen Vorfälle schneller erkennen und schneller darauf reagieren können. Ein Schlag trifft sie daher deutlich weniger hart.

Für Incidents, die zu Unterbrechungen führen, nennen die Leader-Unternehmen eine Mean Time to Detect (MTTD) von 21 Tagen. Die Aufholer brauchen dagegen im Schnitt über einen Monat (34 Tage), bis sie die Bedrohung in ihrem Netzwerk erkennen. Bei den Leadern ist auch die Wiederherstellungsphase kürzer; ihre Mean Time to Recover/Repair (MTTR) bei geschäftskritischen Workloads liegt bei etwas über 44 Stunden. Dagegen beträgt die durchschnittliche Wiederherstellungsdauer bei den Unternehmen, deren Security-Programme noch im Aufbau begriffen sind, 5,7 Tage.

„Wenn ein Unternehmen seine Erkennungs- und Reaktionszeiten minimieren kann, dann sagt das direkt etwas über den Reifegrad des Sicherheitsprogramms aus. Aus diesem Grund sind MTTR und MTTD für Management und Führungskräfte so enorm wichtige Metriken. Sie wollen auf lange Sicht messbare Erfolge sehen“, erklärt Mick Baccio, Global Security Advisor im SURGe Security Research Team von Splunk.



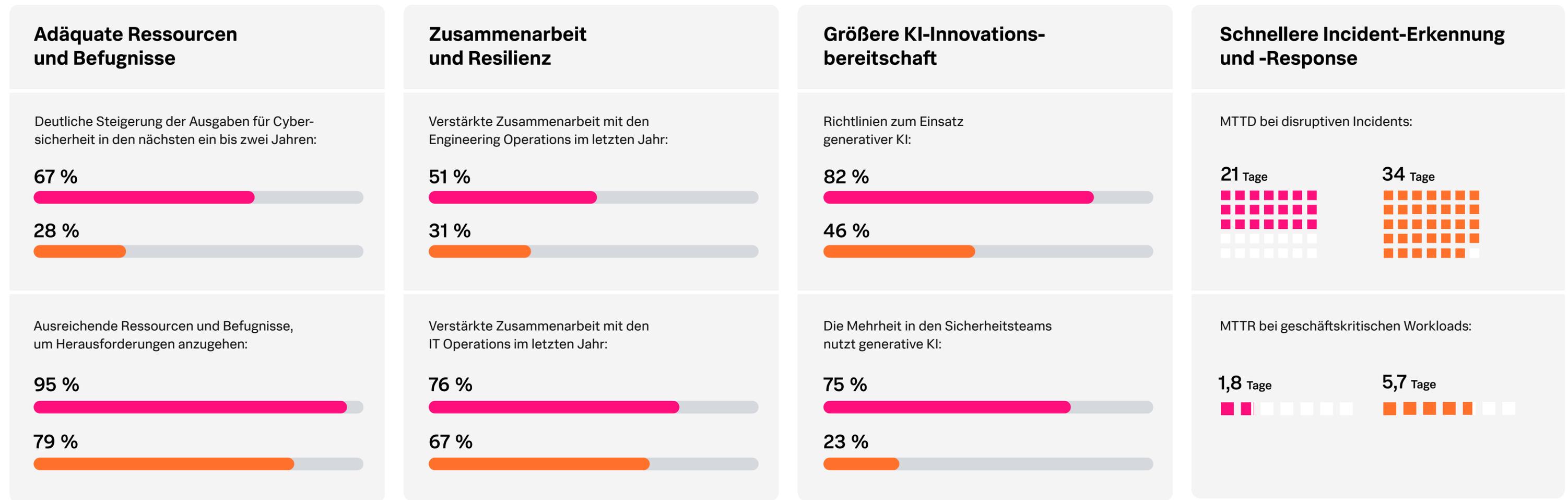
**Wenn ein Unternehmen seine Erkennungs- und Reaktionszeiten minimieren kann, dann sagt das direkt etwas über den Reifegrad des Sicherheitsprogramms aus. Aus diesem Grund sind MTTR und MTTD für Management und Führungskräfte so enorm wichtige Metriken. Sie wollen auf lange Sicht messbare Erfolge sehen.**

— Mick Baccio, Global Security Advisor, Splunk

# Kernelemente des Leader-Erfolgs

Unternehmen, die ihre Cybersicherheitsprogramme als extrem fortgeschritten bezeichnen, übertreffen das übrige Feld in vier wichtigen Bereichen.

- Leader-Unternehmen
- Aufhol-Unternehmen



# Einschätzung der Bedrohungslage

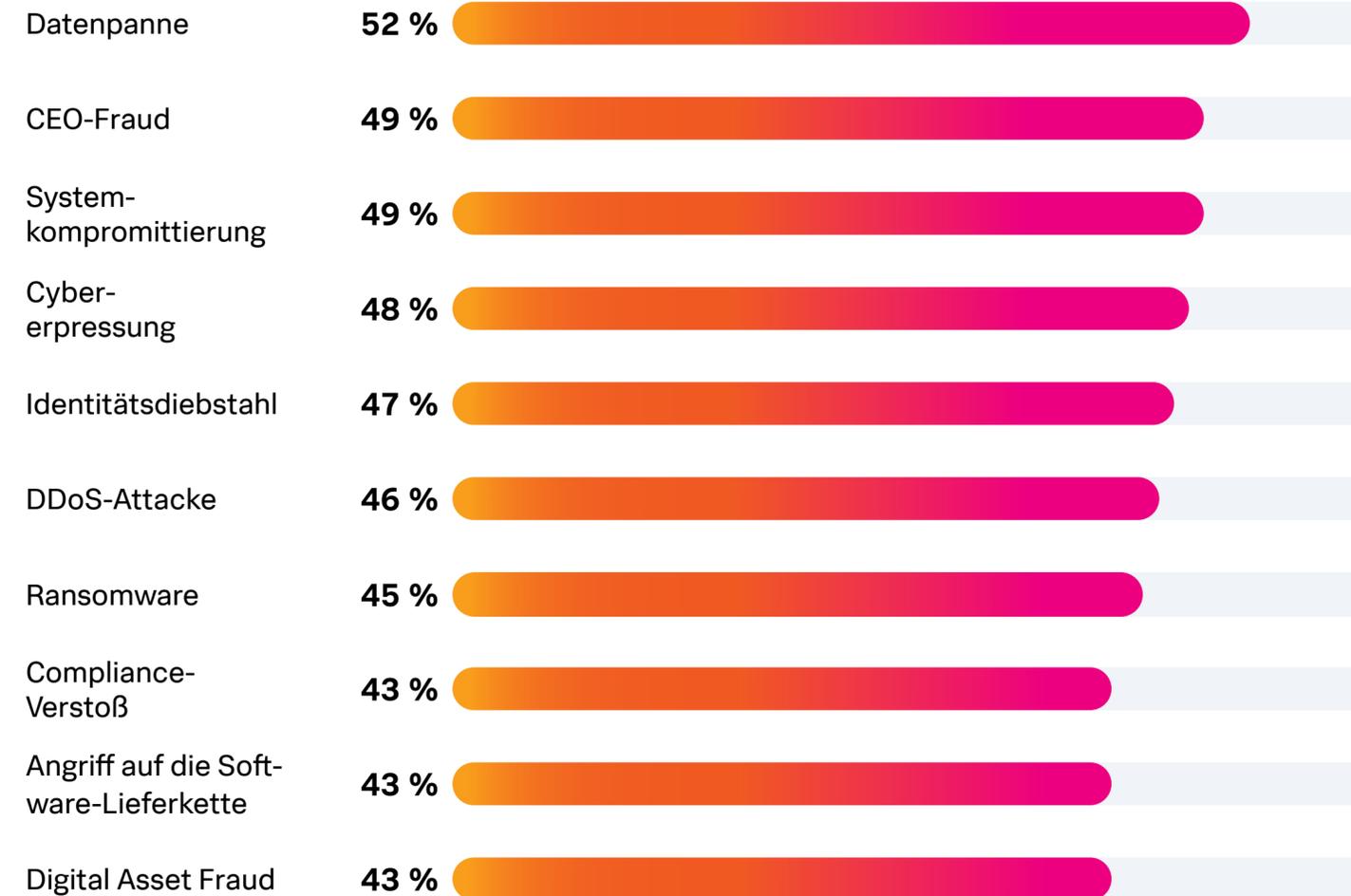
Auch wenn Sicherheitsteams ihr Bestes geben, finden Bedrohungsakteure doch immer Wege, auf denen sie selbst die besten Abwehrmaßnahmen überlisten. Der Lagebericht Security 2024 zeigt, dass die Angreifer nicht nachlassen: Datenlecks und Ransomware haben seit 2021 um 13 % bzw. 14 % zugenommen.



2024 sind die Angriffstaktiken zwar relativ unterschiedlich – vom CEO-Fraud mit leichtgläubigen Angestellten bis zu DDoS-Attacken mit Brute-Force-Methoden –, doch die Ansätze haben eines gemeinsam: Disruption. Ihr Ziel ist es, Störungen zu verursachen.

Cybersecurity-Incidents haben nach wie vor weitreichende Folgen, sie schaden dem Ruf von Unternehmen und Marken, sie ziehen juristische Konsequenzen nach sich, und dann kommen noch die finanziellen Kosten dazu. Allerdings kann die Wirtschaft diese Schläge offenbar besser einstecken – und das, obwohl sie insgesamt zunehmen. So sagen diesmal z. B. nur 44 % der Befragten, dass die Behebung von Incidents einen beträchtlichen Aufwand an Zeit und Personal erfordert – das sind 13 Prozentpunkte weniger als im Vorjahr. Außerdem sind in diesem Jahr weniger Produktivitätseinbußen und Datenkompromittierungen zu verzeichnen, was darauf hindeutet, dass das Bemühen um digitale Resilienz Früchte trägt.

## Die häufigsten Incidents der vergangenen beiden Jahre



## Irrationale Angstgegner

Lösegeldzahlungen in Millionenhöhe, CISOs auf der Anklagebank und Zero Day Exploits machen zwar Schlagzeilen, sind aber eher selten. Fragt man Cybersicherheitsfachleute nicht danach, was sie tatsächlich erleben, sondern nach den Bedrohungen, die sie am meisten fürchten, so zeigt sich, dass die Ängste meist an der Realität vorbeigehen. So nennen die Befragten KI-gestützte Angriffe als ihre größte Sorge, doch in Wirklichkeit sind sie weitaus häufiger von Datenpannen, CEO-Fraud, Systemkompromittierung und Identitätsdiebstahl betroffen.

Dasselbe gilt umgekehrt: Die gefühlte Bedrohung bleibt unverhältnismäßig blass im Vergleich zur Realität. So nennen nur 18 % der Befragten die CEO-Fraud-Betrugsmasche als die Bedrohung, die ihnen am meisten Sorgen bereitet, doch tatsächlich stehen angebliche Vorgesetzte, die auf die Schnelle die Auszahlung eines größeren Geldbetrags anweisen, gleich an zweiter Stelle auf der Liste der häufigsten Incidents 2024.

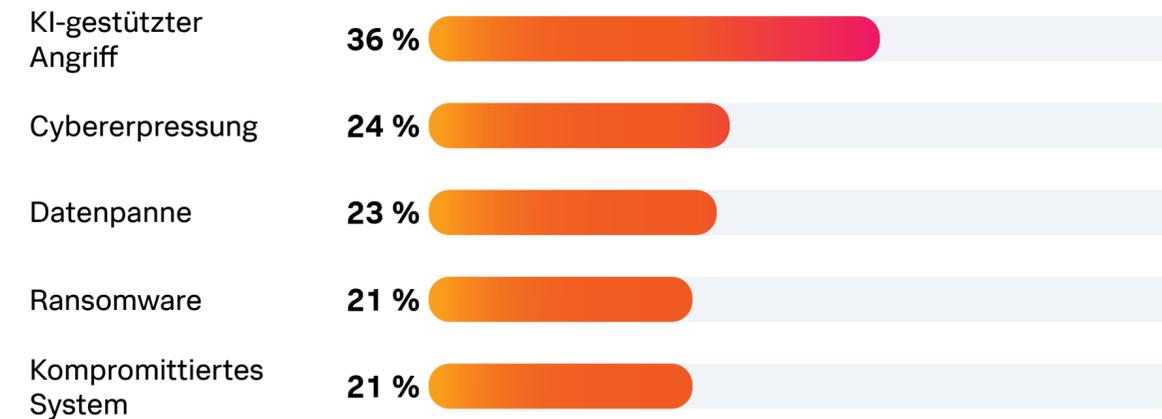
Manche Befürchtungen entsprechen aber der Wirklichkeit. So sind Datenkompromittierungen nicht nur eine Hauptsorge, sondern auch der häufigste Incident: 52 % der Unternehmen berichten von mindestens einer Datenpanne in den letzten beiden Jahren.



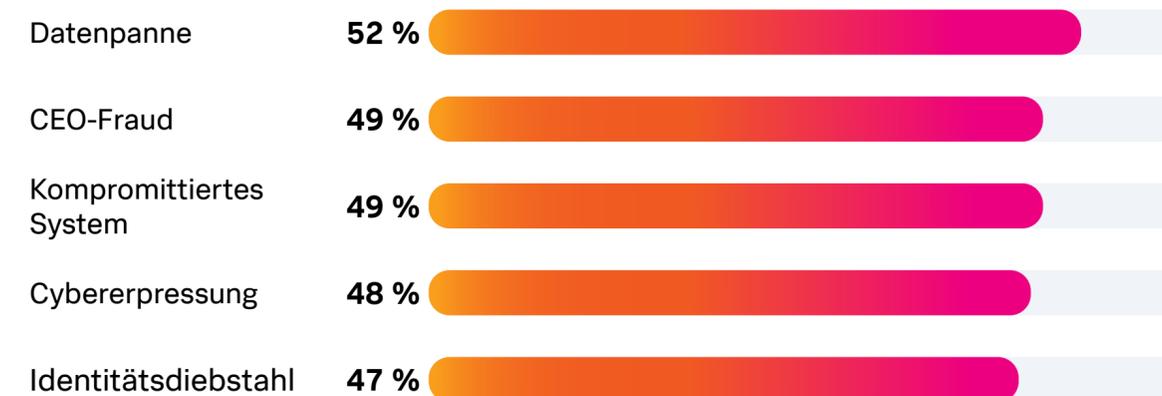
**Es ist die Furcht vor dem Unbekannten. Unternehmen haben Prozesse und Verfahren zur Abwehr bekannter Angriffe wie Datendiebstahl, aber sie wissen noch nicht, ob und wie sie KI-gestützte Angriffe stoppen können.**

— Marcus LaFerrera, SURGe-Leiter, Splunk

### Welche Cyberangriffe bereiten die meisten Sorgen?



### Welche Cyberangriffe wurden tatsächlich erlebt?

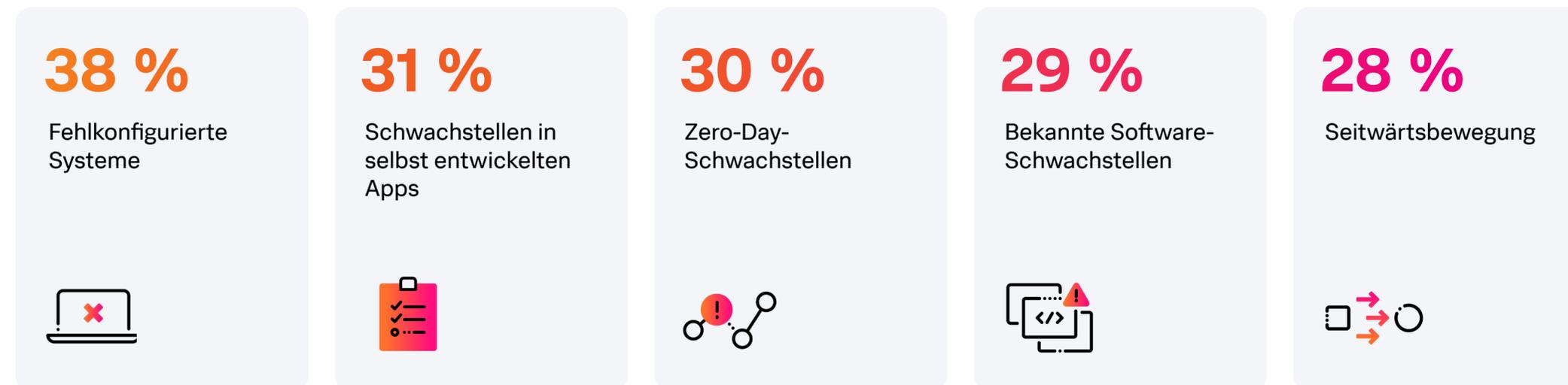


# Menschen machen Fehler – und die Security weiß das

Wie verschaffen sich Angreifer Zugang? Trotz fortschreitender Automatisierung und generativer KI ist das schwächste Glied immer noch der Mensch. Die Befragten nennen fehlerkonfigurierte Systeme als den häufigsten Bedrohungsvektor (38 %) – und auch als den, den sie am meisten fürchten (35 %).

Wenn in diesem Punkt die Besorgnis dem Erlebnis entspricht, dann könnte dies ein Indiz dafür sein, dass die Sicherheitsteams zwar wissen, dass Fehlkonfigurationen ein Problem sind – Hut ab vor dem Monitoring! –, dass sie aber nicht imstande sind, es effektiv zu lösen. Die zunehmende Systemkomplexität und der Mangel an Security-Fachkräften könnten dieses Problem noch verschärfen. Ein Zustand ganz ohne Fehlkonfigurationen wäre dann in weite Ferne gerückt.

## Die häufigsten Bedrohungsvektoren



## Geldgier bleibt ein Hauptmotiv

Datendiebstahl, Ransomware und Erpressung – das Kleeblatt der Angriffe aus Habsucht – sind eine reale Bedrohung, die zu Recht gefürchtet ist. Der Anteil der Befragten, die bereits eine Geiselnahme von Daten und Systemen mitmachen mussten, ist von 35 % (2022) auf 42 % (2024) angewachsen. Cyber-Erpressung, also die Ransomware-Variante, bei der nach dem Diebstahl mit der Veröffentlichung der Daten gedroht wird, kommt mittlerweile häufiger vor als reine Ransomware: 48 % der Befragten hatten bereits mit Cyber-Erpressern zu tun, 45 % wurden Opfer von Ransomware.

Dass Cyber-Erpressung dermaßen en vogue ist, dürfte auf den Erfolg des Colonial-Pipeline-Angriffs 2021 zurückzuführen sein sowie auf die MOVEit-Sicherheitslücke 2023 – Schätzungen zufolge könnte die in Russland ansässige Ransomware-Gruppe Clop damit **\$ 75 Millionen bis \$ 100 Millionen an Lösegeld** einstreichen.

Ein weiterer Faktor könnte sein, dass die Unternehmen erkannt haben, wie wichtig es ist, ihre Backups zu testen. Vielleicht versuchen es Cyberkriminelle deshalb weniger mit der Verschlüsselung von Daten und Systemen und konzentrieren sich lieber auf Exfiltration und Erpressung – das erfordert insgesamt weniger Aufwand, wirft mehr Gewinn ab, und der Erfolg hängt nicht davon ab, dass das Unternehmen keine funktionierenden Backups hat.

## Politische Spannungen finden Ziele im Cyberraum

Die Welt im Jahr 2024 ist von Unruhen geprägt. Die zunehmenden geopolitischen Spannungen haben Online-Folgen, die auch unpolitische Organisationen treffen. Der politisch motivierte Angriff auf eine [Wasseraufbereitungsanlage in Pennsylvania 2023](#) hat gezeigt, dass letztlich niemand vor nationalstaatlich gesponserten Gegnern und terroristischen Gruppen sicher sein kann.

86 % der Befragten sagen, dass das derzeitige geopolitische Klima dazu beiträgt, dass ihr Unternehmen stärker in die Schusslinie rückt. Vor allem Technologieunternehmen teilen diese Ansicht voll und ganz (42 %) – das ist deutlich mehr als im Gesamtdurchschnitt (29 %). Spektakuläre Kompromittierungen mit geopolitischem Bezug wie die von SolarWinds sind eine dauernde Warnung an Technologieunternehmen, insbesondere die Anbieter von IT-Services, dass sie von politisch motivierten Akteuren als Vehikel für Angriffe auf weitere Unternehmen missbraucht werden könnten.

Interessanterweise stimmen aus dem öffentlichen Sektor nur 17 % der Befragten voll und ganz zu, dass die zunehmenden geopolitischen Spannungen sie stärker ins Fadenkreuz der Angreifer rücken. Das könnte daran liegen, dass Behörden und öffentliche Institutionen schon immer das Ziel geopolitischer Attacken waren – und wohl auch immer sein werden.

„Hacktivismus ist nicht immer sonderlich raffiniert“, sagt Audra Streetman, Security Strategist bei Splunk SURGe. „Politisch motivierte Angreifer nutzen oft ältere Schwachstellen, Standardpasswörter und andere leicht zugängliche Wege. Darum ist Cyberhygiene heute wichtiger denn je.“



**Wachsende geopolitische Spannungen werden die Risiken weiter erhöhen, selbst für offenbar unpolitische Organisationen. Das Risiko steckt in jedem digitalen Link, es ist ein Nebenprodukt unserer globalen Lieferketten.**

— Mick Baccio, Global Security Advisor, Splunk

# Der zunehmende Compliance-Stress

Für Sicherheitsverantwortliche ist Compliance vergleichbar mit Steuern und dem Tod – niemand kommt darum herum. Tatsächlich sagen 62 % der Befragten, dass sie bereits Fälle hatten, in denen neue Compliance-Vorgaben vorschreiben, dass Datenlecks offenzulegen sind.



Den Sicherheitsverantwortlichen ist sehr wohl bewusst, dass die regulatorischen Rahmen zu gewollten und vielleicht auch zu ungewollten Änderungen ihrer Arbeitsweise führen werden. So sind 87 % der Befragten der Ansicht, dass sie Compliance in einem Jahr ganz anders handhaben werden. Compliance und Cybersicherheit sind zwar keineswegs direkte Widersprüche, dennoch könnte es sein, dass die eine auf Kosten der anderen geschieht. 86 % sagen, dass sie ihre Budgets umschichten werden, sodass die Compliance Vorrang vor den Security-Best-Practices bekommt.

Diese Antworten entsprechen den Erkenntnissen aus unserem [CISO-Report](#) vom Oktober 2023. Auf die Frage, ob sie sich Sorgen machen, bei Cybersecurity-Vorfällen persönlich haftbar gemacht zu werden, antworten dort 84 % mit teils nachdrücklicher Zustimmung. In derselben Studie sagen auch 84 % der CISOs, dass ihr Vorstand bzw. Leitungsgremium unter starker Sicherheit eher die Einhaltung regulatorischer Vorgaben versteht als Best Practices.

## Die Auswirkungen der neuen Meldepflichten bei erheblichen Verstößen

63 %

gehen davon aus, dass aus Furcht vor Strafe eher „übermeldet“ wird.

61 %

erwarten, dass börsennotierte Unternehmen an Wert verlieren, wenn sie Verstöße als „erheblich“ melden.

26 %

glauben, dass beides eintreten wird.

Die Gründe dafür liegen auf der Hand. In den USA ist neuerdings Vorschrift, dass Unternehmen, die der Börsenaufsicht (Securities and Exchange Commission) unterstehen, alle „wesentlichen“ („material“) Cybersecurity-Incidents offenlegen und beschreiben müssen sowie dass sie jährlich Auskunft über ihr Risikomanagement geben. Compliance-Verstöße gegen diese SEC-Vorgaben können saftige Bußgelder, Strafverfahren und sogar Haftstrafen für Führungskräfte zur Folge haben. In der EU sieht die risikobasierte NIS-2-Richtlinie neue Melde- und Berichtspflichten sowie ein erweitertes Risikomanagement und konkrete Maßnahmen für Unternehmen und Einrichtungen aus 18 Sektoren vor, außerdem kann die Geschäftsführung bei Verstößen persönlich haftbar gemacht werden.

Sicherheitsverantwortliche balancieren damit auf Messers Schneide. Wenn sie das Schadensrisiko unterschätzen, drohen ihnen Betrugsvorwürfe und unter Umständen Gefängnis; wenn sie auf

Nummer sicher gehen und das Risiko überschätzen, kann es sein, dass das Unternehmen an Wert verliert und der Kurs einbricht – abgesehen davon dürfte der Vorstand eine übervorsichtige Security mit Misstrauen beäugen.

In jedem Fall gehören regulatorische Vorgaben heute zur Sicherheitsstrategie. Durch Simulationen und Übungen in der Form von Strategiespielen können Unternehmen einerseits Lücken in der Abwehr aufdecken, andererseits den Aufsichtsbehörden gegenüber nachweisen, dass sie um kontinuierliche Optimierung bemüht sind. Und zwar nicht erst dann, wenn sie in den Schlagzeilen stehen.

# Security, Rechtsabteilung und Compliance-Teams bündeln ihre Kräfte

Es gab einmal eine Zeit, in der war Compliance hauptsächlich im Wertpapierhandel und ähnlichen Dingen wichtig. Die Compliance-Teams arbeiteten in ihren eigenen Silos und hatten mit den Security-Teams meist nichts zu tun, geschweige denn, dass das eine Team überhaupt wusste, was das andere tat.

Diese Ära der klassischen Aufsicht ist längst Geschichte, heute haben Compliance-Verstöße sehr viel ernstere und direktere Folgen. Im Oktober 2023 erhob die US-Börsenaufsicht gegen den ehemaligen CISO von SolarWinds Anklage wegen Betruges und Täuschung der Aktionäre durch falsche Angaben zur IT-Sicherheit des Unternehmens im Vorfeld des verheerenden Cyberangriffs 2020. Die Security-Kapazitäten seien nicht ausreichend gewesen, die internen Kontrollen hätten versagt.

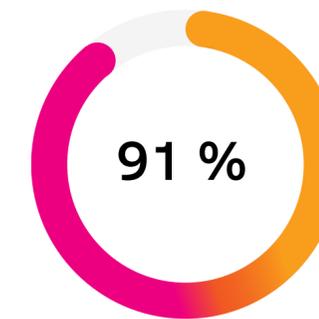
Die Kommunikation zwischen Vorstand, Rechtsabteilung, Compliance-Abteilung und den Sicherheitsteams ist also unerlässlich. Die einzelnen Teams müssen zusammenarbeiten und einsehen, dass sie an einem Strang ziehen.

Unternehmen und Geschäftsführung werden sich gründlich überlegen müssen, wer bei Verstößen zuerst in der Haftung steht. Die Frage ist nicht, ob dieser Fall eintritt, die Frage ist nur, wann. Meist werden es die CISOs sein, die den Schwarzen Peter ziehen. Aber auch CTOs, CIOs und sogar die Cyberfachleute im Aufsichtsrat könnten von abgeleiteten Aktionärsklagen getroffen werden oder müssten unangenehme Untersuchungen über sich ergehen lassen.

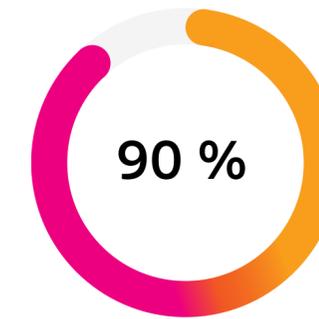
All dies ist auch an den Sicherheitsteams nicht spurlos vorübergegangen. Bei der Mehrheit der Befragten wurden mittlerweile die Sicherheitsmaßnahmen verschärft, außerdem hat man die Abstimmung mit der Rechtsabteilung und dem Compliance-Team erleichtert.

Die gute Nachricht: Es zahlt sich aus, wenn alle Beteiligten Compliance als gemeinsame Aufgabe begreifen und einander informiert halten. Eine Neuausrichtung von Prioritäten, Rollen und Zuständigkeiten im Unternehmen macht die Security effektiver, und sie macht Rechtsabteilungen und Compliance-Teams handlungsfähig.

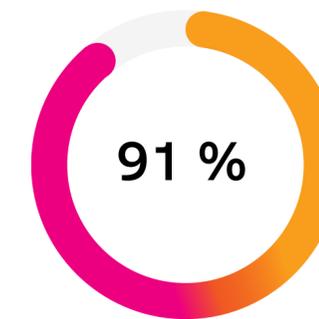
## Wie Security- und Compliance-Teams zusammenarbeiten



schulen Rechtsabteilung und Compliance-Teams verstärkt in **Security**



schulen die Sicherheitsteams verstärkt in **Recht** und **Compliance**



sagen, dass alle im Security-Team Compliance als Teil ihrer Aufgaben verstehen

## Compliance wird persönlich

Die SolarWinds-Anklage war ein Wendepunkt – es war das erste Mal, dass die Börsenaufsicht einen CISO im Zusammenhang mit einem Cybersecurity-Incident vor Gericht brachte. Dieses bis dahin beispiellose Vorgehen markiert einen Wechsel in der Weise, wie die Welt auf die Cybersicherheit blickt; für Sicherheitsverantwortliche und ihre Teams änderte sich ab diesem Punkt so manches. „Cyberrisiko“ ist ab jetzt gleichbedeutend mit „Geschäftsrisiko“.

Die Securities and Exchange Commission (SEC) macht Führungskräfte und andere Stakeholder verantwortlich, und zwar nicht zu knapp. Abgesehen von einer ganzen Menge neuer, strafbewehrter Vorschriften müssen die Security-Teams Incidents jetzt innerhalb kürzerer Fristen melden. Die NIS-2-Richtlinie der EU sieht 24 bis 72 Stunden vor, während die SEC mit bis zu vier Werktagen etwas mehr Spielraum gibt. Doch das Zeitfenster wird enger – eine Entwicklung, die auch für die erfahrensten Fachleute eine Herausforderung darstellen dürfte.

Freilich können schärfere Rechenschaftspflichten bei Incidents zu besseren Security-Programmen führen. Doch sie können auch abschreckende Wirkung entfalten und einen Chilling-Effekt auf die ganze Branche haben. Denn wer wäre schon bereit, für einen Fehler im Job in den Knast zu wandern?

Vermutlich ist die Angst übertrieben, aber die Extremfälle wirken nun einmal abschreckend. In Zeiten, in denen die Cybersicherheit mit einem bitteren Fachkräftemangel zu kämpfen hat, sind drohende Compliance-Strafen ein Grund mehr, doch lieber einen anderen Berufsweg in Betracht zu ziehen.

## Der Compliance-Druck führt zu Karriere Zweifeln

**76 %** finden, dass die Cybersicherheit durch das Risiko persönlicher Haftung weniger attraktiv wird



**70 %** sagen, dass sie schon erwogen haben, die Branche zu wechseln, weil der Beruf so viel Stress mit sich bringt



36 % geben an, dass sie schon öfter daran gedacht haben, die Branche zu wechseln

# Es geht voran

Die Cybersicherheit im Jahr 2024 ist von ganz unterschiedlichen Dynamiken geprägt, von geopolitischen Spannungen ebenso wie von neuen Compliance-Anforderungen. Doch es gibt auch Grund zur Hoffnung. Ein beherzter und offener Umgang mit KI verheißt Gutes für die Cyberabwehr – vor allem dann, wenn das Unternehmen es schafft, die Risiken in Grenzen zu halten und zu regeln, wie die Beschäftigten mit KI-Tools umgehen.

Ein weiterer Grund zur Zuversicht ist die Tatsache, dass die Unternehmen mehr in Cybersicherheit investieren. Fast alle befragten Organisationen (96 %) geben an, dass sie ihre Ausgaben in den nächsten ein bis zwei Jahren erhöhen werden.



# Guter Rat zum Schluss

Inmitten so vieler Veränderungen und neuer Technologien fällt es vielen Unternehmen nicht leicht, zu entscheiden, worauf sie ihre Bemühungen konzentrieren sollten. Hier sind – vor dem Hintergrund der diesjährigen Erkenntnisse – die Empfehlungen der Fachleute von Splunk.

## Generative KI akzeptieren und fruchtbar machen.

Generative KI ist bereits im Unternehmen insgesamt (93 %) und in den Sicherheitsteams (91 %) angekommen. Wer jetzt zögert, riskiert, abgehängt zu werden. Wer versucht, den Einsatz von KI ganz zu unterbinden, verstellt sich selbst den Weg zu Innovationen – und provoziert unkontrollierte Schatten-KI.

## Durchdachte KI-Regeln aufstellen, die Spielraum für Innovationen lassen.

Eine überhastete Einführung generativer KI ohne Berücksichtigung ihrer Risiken und Auswirkungen wäre ein schwerer Fehler. Stellen Sie Regeln und Richtlinien auf und entwickeln Sie Pläne für Use Cases in Security und Business, dann sind Sie den Unternehmen, die noch keinen Plan haben (34 %), schon ein gutes Stück voraus. Finden Sie heraus, welche Risiken generativer KI am bedenklichsten sind – und setzen Sie Richtlinien auf, die speziell auf diese Risiken zugeschnitten sind.

## Zusammenarbeit der Teams fördern und Tools konsolidieren.

Digital resiliente Unternehmen brechen ihre Silos auf, in der Softwareentwicklung, im operativen Betrieb und vor allem in der IT. 76 % der Leader-Unternehmen haben die Zusammenarbeit von Security und IT Operations verstärkt, um ihre digitale Resilienz zu verbessern. Eine weitere Möglichkeit, Reibungsverluste zu reduzieren, liegt in der Konsolidierung der Tools; damit verhindern Sie unübersichtlich vollgestopfte Dashboards, und die Teams können sich auf die wirklich wichtigen Bedrohungen konzentrieren. Momentan sagen 43 % der Befragten, dass sie zwischen zu vielen einzelnen Sicherheitstools und Management-Konsolen hin und her wechseln.

## Rechtsabteilung und Compliance-Teams ins Boot holen.

2024 beginnt ein neues Compliance-Zeitalter. Sicherheitsverantwortliche sollten jetzt die enge Kooperation mit der Rechtsabteilung und den Compliance-Zuständigen suchen und ihre Prozesse optimal abstimmen. 91 % der Security-Teams sagen, dass Compliance bereits zum Job gehört. Mit Simulationen und Tabletop-Übungen können Sie Lücken in der Abwehr aufdecken und zugleich den Aufsichtsbehörden gegenüber darlegen, dass Ihr Unternehmen auf kontinuierliche Optimierung bedacht ist.

## Die 5 Cybersecurity-Prioritäten der nächsten beiden Jahre



1. Beschäftigte aus Cybersecurity und IT-Betrieb in Security Operations schulen



2. Tools für Security Operations beschaffen, die die Automatisierung/Orchestrierung von SecOps-Prozessen unterstützen



3. Eine Softwarearchitektur entwickeln und aufbauen, die Sicherheitsanalysen und Security Operations integriert.



4. Zusätzlich zu den vorhandenen Tools Cloud-Technologien für Sicherheitsanalysen und Security Operations ausfindig machen, testen und einsetzen.



5. Verstärkt externe Ressourcen für die Security Operations mobilisieren (z. B. Managed Security Services).

### **Effektiv von oben Ressourcen einwerben.**

Welchen Reifegrad Ihre Cybersicherheit erreichen kann, hängt davon ab, wie das Management dazu steht. 95 % der Leader-Unternehmen sagen, dass sie Herausforderungen angehen können, weil sie über ausreichend Ressourcen und Befugnisse verfügen. Insbesondere CISOs sollten Sicherheitsrisiken aus Business-Perspektive betrachten, vermitteln und diskutieren können, wenn sie in der Führungsriege Gehör finden wollen. Sprechen Sie mit den Entscheidern aus der Betriebswirtschaft so, dass diese den geschäftlichen Nutzen von Cybersicherheitsinvestitionen nachvollziehen können. Dazu gehört auch ein Reporting zu den (potenziellen) Auswirkungen von Cybersecurity Incidents auf das Geschäft und dass Sie Compliance-Anforderungen thematisieren, die ernsthafte juristische oder finanzielle Folgen haben könnten.

### **Dem Fachkräftemangel mit unkonventionellen Ideen begegnen.**

Die Daten des Lageberichts Security 2024 zeigen, dass Leader-Unternehmen weniger auf die klassischen Methoden von Personalgewinnung und Weiterbildung setzen. 53 % der Leader setzen KI und maschinelles Lernen ein, um Lücken in der Belegschaft zu schließen – deutlich mehr als die Unternehmen mit Aufholbedarf, bei denen dieser Wert nur 28 % erreicht. Mit kreativen Einstellungs- und Schulungsstrategien (z. B. Programmen, die es Leuten aus anderen Aufgabenbereichen ermöglichen, im SOC mitzuarbeiten und auszuweichen) können Sie den Fachkräftemangel abfedern – und Sie sorgen für eine dringend benötigte Vielfalt im Security-Team.

### **Grundlagen nicht vergessen.**

Einerseits werden die Bedrohungen immer raffinierter, andererseits setzen die Bedrohungsakteure weiterhin die altbewährten Hebel an. Fehlkonfigurierte Systeme sind auch 2024 noch ein Hauptangriffsvektor. Die Einrichtung grundlegender Kontrollen ist daher das Handlungsfeld, das Ihrem Unternehmen den meisten ROI verspricht – und für die Security-Teams wird es damit auf lange Sicht sehr viel leichter, den Anforderungen gerecht zu werden. Zwar finden 76 %, dass die Inventarisierung des IT-Assets zu viel Zeit in Anspruch nimmt, doch diese Zeit ist in unseren Augen gut investiert. Eine stets aktuelle Übersicht über Assets und Abhängigkeiten verhindert tote Winkel, aus denen Gefahr droht.

### **Globale Dynamiken beobachten und mitverfolgen, wie sie die Cybersicherheitslandschaft prägen.**

Cybersicherheit existiert nicht im luftleeren Raum. Politik, internationale Konflikte und strengere Compliance-Vorgaben wirken sich direkt und indirekt auf die Bedrohungslandschaft aus. 86 % der Befragten sagen, dass das derzeitige geopolitische Klima dazu beiträgt, dass ihr Unternehmen stärker in die Schusslinie rückt. Und 62 % mussten sich schon handfest mit neuen Compliance-Vorgaben auseinandersetzen. Wer diese Dynamiken auf dem Schirm hat und hellhörig bleibt, wird die Hindernisse leichter überwinden.

# Erfahren Sie, wie Sie mit Splunk den Turbo für digitale Resilienz zünden



## Podcast Digitaler Kompass: Unternehmen auf Kurs Richtung digitale Resilienz

Neugierig auf weitere verwertbare Erkenntnisse zu aktuellen Security-Trends und darüber hinaus? Erfahren Sie, wie Leader die drängendsten Cyber-Herausforderungen von heute angehen: KI, neue Bedrohungen, Compliance-Vorgaben und mehr.

Jetzt anhören



## Schaffen Sie digitale Resilienz

Die Security-Teams von heute stehen unter Dauerdruck durch Cyberbedrohungen, Regulierungsänderungen und zunehmende geopolitische Spannungen. Erfahren Sie, wie Ihr Unternehmen disruptive Zeiten nicht nur übersteht, sondern wächst und gedeiht.

Erste Schritte

# Branchen-Highlights

Die wichtigsten Erkenntnisse aus 6 ausgewählten Branchen weltweit.

## Fertigung

Die **Produktion** konzentriert sich stärker als andere Branchen auf die Cloud-Sicherheit: 40 % nennen dies als eines der wichtigsten Arbeitsfelder. Auch Zero-Day-Schwachstellen sind ein wichtiges Thema: Bei 39 % sind sie die Hauptsorge, was daran liegen könnte, dass es notorisch schwierig ist, OT und Anlagen zu patchen. Die Fertigung hat außerdem Mühe, mit den Veränderungen der Bedrohungslandschaft Schritt zu halten:

- **51 % der Befragten aus der Fertigung sagen, dass die Sicherheitsanforderungen in den letzten zwölf Monaten strenger geworden sind.**
- **Die Befragten aus der Fertigung geben auch häufiger an, dass die zunehmende Komplexität der Bedrohungen ihre Bemühungen ausbremst. Das ist bei 50 % der Fall, während der Gesamtdurchschnitt aller Branchen bei 38 % liegt.**

Diese Rückschläge könnten auf mangelnde Investitionsunterstützung hindeuten, denn die Wahrscheinlichkeit, dass die Ausgaben für Cybersicherheit deutlich steigen, ist bei den Fertigungsunternehmen geringer (36 %) als im Branchendurchschnitt (48 %). Allerdings hat die Branche die Nase vorn, wenn darum geht, Security-Fachkräfte zu gewinnen und zu halten:

- **27 % der Befragten sagen, dass der Stress am Arbeitsplatz schon mehrfach dazu geführt hat, dass sie selbst oder Teammitglieder einen Ausstieg aus der Cybersecurity erwogen haben – ein Anteil, der deutlich unter dem Gesamtdurchschnitt liegt (36 %).**
- **27 % sagen auch, dass sich kritische Projekte aufgrund des Fachkräftemangels bereits mehrfach verzögert haben – im Gesamtdurchschnitt liegt dieser Wert deutlich höher: bei 37 %.**

Da es in den Fertigungsunternehmen offenbar nicht leicht fällt, zusätzliche Mittel für die Cybersicherheit zu bekommen, sollten Security-Verantwortliche die finanziellen Folgen von Incidents aufzeigen und sich auf die Hauptrisiken konzentrieren, damit sie Unterstützung aus der Führungsebene und dem Vorstand erhalten.

## Finanzdienstleister

Im Vergleich zu anderen Branchen sind die **Finanzdienstleister** zuversichtlicher, was ihre Fähigkeit angeht, mit den Anforderungen an die Cybersicherheit Schritt zu halten: 50 % sagen, dass es dieses Jahr einfacher war, also mehr als im Gesamtdurchschnitt aller Branchen, der bei 41 % liegt.

Der Grund für diesen Optimismus könnte die stärkere Zusammenarbeit bei IT und Engineering sein. 64 % der Finanz-Sicherheitsteams arbeiten in puncto digitaler Resilienz nach eigener Auskunft tendenziell enger mit den Engineering Operations zusammen, im Durchschnitt sind es nur 46 %.

Die Befragten aus dem Finanzdienstleistungssektor machen sich auch größere Hoffnungen, wenn es um die Frage geht, wie generative KI dem Fachkräftemangel abhelfen könnte. Vor allem in diesen Punkten, meinen sie, könnte künstliche Intelligenz helfen:

- **63 % glauben, dass Unternehmen mit generativer KI Fachkräfte schneller finden und onboarden können (der Gesamtdurchschnitt zum Vergleich: 58 %).**
- **71 % sind der Ansicht, dass erfahrene Security-Fachleute mit KI-Unterstützung produktiver werden (Durchschnitt: 65 %).**

Nichtsdestotrotz sind sich die Finanzdienstleister der Risiken bewusst. Während im Gesamtdurchschnitt aller Branchen 65 % angeben, dass sie nicht genug über generative KI wissen, um die Auswirkungen vollständig zu verstehen, sind es in der Finanzbranche 76 %. Entsprechend nennen diese Befragten auch zu 39 % KI-gestützte Angriffe als ihre größte Sorge.

Ebenso wenig überrascht, dass von den Finanzdienstleistern 43 % ein eigenes Team für die Compliance abgestellt haben, weil die Einhaltung von Vorschriften eine so umfangreiche Aufgabe geworden ist. Im Gesamtdurchschnitt ist das nur bei 39 % der Fall. Plausibel ist auch, dass der Finanzdienstleistungssektor öfter mit Cyber-Erpressung konfrontiert ist (54 %) als der Gesamtdurchschnitt (48 %).

## Die Studie

Im Dezember 2023 und im Januar 2024 wurden 1650 Sicherheitsverantwortliche befragt, und zwar in Australien, Deutschland, Frankreich, Großbritannien, Indien, Japan, Neuseeland, Singapur und den USA. Vertreten sind damit 16 Branchen: Luft- und Raumfahrt inklusive Verteidigung, Business Services, Konsumgüter, Bildung, Finanzdienstleistungen, öffentliche Hand (Bund, Länder und Kommunen), Gesundheitswesen, Biowissenschaften, Fertigung, Technologie, Medien, Öl/Gas, Einzelhandel/Großhandel, Telekommunikation, Transport und Logistik sowie Versorgungsunternehmen.

## Kommunikation und Medien

Die Befragten aus **Kommunikation und Medien** bezeichnen ihre Cybersicherheitsprogramme häufiger (57 %) als „extrem fortgeschritten“ als alle Branchen im Gesamtdurchschnitt (47 %). Trotzdem ist offenbar noch Luft nach oben: Die Security-Teams der Branche finden am häufigsten (16 %), dass sie nicht die nötigen Ressourcen oder Befugnisse haben, um Herausforderungen anzugehen; der Gesamtdurchschnitt liegt bei 8 %.

Die Kommunikations- und Medienunternehmen sind gekennzeichnet durch die Probleme, mit denen sie – anders als die übrigen Branchen – am meisten zu kämpfen haben:

- **82 % finden es wegen häufiger Änderungen und der wachsenden Angriffsfläche schwierig, Cyberhygiene und Security Posture Management aktuell zu halten; das finden zwar alle Branchen, aber im Durchschnitt nur 71 %.**
- **62 % sagen, dass ihr SOC zu viele verschiedene Sicherheitstools und Management-Konsolen hat, zwischen denen das Team hin- und herwechselt; im Gesamtdurchschnitt ist dieser Anteil geringer, nämlich 43 %.**
- **47 % geben an, dass sie selbst oder andere aus dem Team, schon mehrfach erwogen haben, der Cybersecurity den Rücken zu kehren, weil es unmöglich ist, Leute mit den richtigen Skills zu finden oder zu halten; im Durchschnitt sagen dies 36 %.**
- **74 % sagen von sich, dass sie von neuen Compliance-Vorgaben betroffen sind; im Durchschnitt sind es 62 %.**

Möglicherweise liegt es an diesen Schwierigkeiten, dass bei Kommunikation und Medien eine ganze Reihe von Incidents häufiger vorkommt als im Gesamtvergleich: Insider-Angriffe (55 %, Durchschnitt: 42 %), Digital Asset Fraud (59 %, Durchschnitt: 43 %), Angriffe über die Software-Lieferkette (57 %, Durchschnitt: 43 %) sowie gezielte Angriffe (54 %, Durchschnitt: 44 %). Auch fehlkonfigurierte Systeme sind für diese Branche ein größeres Problem: 44 % der Befragten nennen sie als Fehler-Ursache der letzten beiden Jahre.

Die Cybersecurity-Teams der Kommunikations- und Medienunternehmen sollten sich um Unterstützung aus der Geschäftsleitung bemühen, damit sie den Reifegrad ihrer Sicherheitsprogramme weiter erhöhen können. Wenn die Teams

genügend Ressourcen und Befugnisse haben, um Probleme zu lösen, werden sie vermutlich bessere Ergebnisse bei der Bedrohungsbekämpfung erzielen.

## Technologie

Die Befragten aus Technologieunternehmen haben offenbar mit komplexen Umgebungen zu kämpfen. Daraus ergeben sich etliche Probleme:

- **Die Komplexität des Security-Stacks wird häufiger (36 %) als Grund dafür genannt, dass die Teams Schwierigkeiten haben, auf der Höhe der Cybersecurity-Anforderungen zu bleiben, als im Durchschnitt (26 %).**
- **Technologieunternehmen klagen häufiger (37 %) als der Durchschnitt (26 %) über zu viele separate Security-Tools und über zu wenig Personal für die nötige Handarbeit.**
- **Bekannte Software-Lücken (34 %) und Schwachstellen in eigenen Anwendungen (34 %) sind im Technologiesektor häufiger die Fehler-Ursachen von Incidents als im Durchschnitt der Branchen.**

Der Veränderungen im regulatorischen Umfeld sind ein weiteres Hindernis. 41 % der Befragten aus Technologieunternehmen geben an, dass diese Entwicklungen ein Grund dafür sind, dass es ihnen schwerfällt, Schritt zu halten. Im Gesamtdurchschnitt teilen nur 28 % diese Wahrnehmung.

Hinzu kommen noch die geopolitischen Konflikte, die Technologieunternehmen stärker treffen als andere. Die Befragten der Branche stimmen zu 42 % voll und ganz zu, dass internationale Konflikte dazu beitragen, dass ihr Unternehmen stärker ins Fadenkreuz der Gegner rückt. In der Gesamtheit der Branchen haben nur 29 % diesen Eindruck.

Positiv zu vermerken ist, dass die Sicherheitsbudgets der Tech-Branche sich offenbar an der Wirklichkeit orientieren. Die Befragten erwarten viel häufiger (63 %) einen signifikanten Anstieg der Ausgaben für Cybersecurity als der Durchschnitt (48 %).

Für die Technologieunternehmen, die mit Komplexität zu kämpfen haben, ist Vereinfachung die Devise. Auch weil die Branche anscheinend unter dem Shiny-Object-Syndrom leidet und fasziniert von den Möglichkeiten des jeweils neuesten Trends ist, dürfte eine konsequente Tool-Konsolidierung zu den wirksamsten Maßnahmen gehören.

## Gesundheitswesen

Das Gesundheitswesen hat die bedenklichsten Erkennungszeiten aller Branchen. 31 % der Befragten sagen, dass sie die Mean Time to Detect (MTTD) in Monaten messen – im Gesamtdurchschnitt ist das nur bei 19 % der Unternehmen der Fall. Das Gesundheitswesen hat auch häufiger mit Ransomware-Angriffen zu kämpfen (56 %) als der Durchschnitt (45 %). Die Befragten aus dem Gesundheitssektor nennen ferner öfter Accounts mit allzu großzügigen Rechten (33 %) als die häufigste Fehler-Ursache von Incidents.

Die Branche hat außerdem mehr Probleme bei der Personalbeschaffung als andere:

- **44 % der Befragten aus dem Gesundheitswesen sagen, dass schon Teammitglieder ohne die entsprechende Erfahrung Projekte leiten sollten; der Vergleichswert des Gesamtdurchschnitts liegt bei 39 %.**
- **44 % geben an, dass sich bei ihnen kritische Projekte oder Vorhaben aufgrund von Schwierigkeiten bei der Personalgewinnung verzögert haben; der Durchschnitt liegt bei 37 %.**

Im Gesundheitswesen sind auch die meisten Befragten (67 %) von neuen Compliance-Vorgaben betroffen. Dass diese Veränderungen dazu führen, dass mehr Verantwortliche in leitender Position Tag für Tag rund um die Uhr in Rufbereitschaft sind, ist eine Aussage, der im Gesundheitswesen 44 % zustimmen – das ist der höchste Wert aller Branchen. Der Vergleichsdurchschnitt liegt hier bei 35 %.

Die Befragten aus Unternehmen des Gesundheitswesens machen sich am wenigsten Hoffnung, was generative KI angeht. 52 % gehen davon aus, dass die Gegner am meisten profitieren werden; im Durchschnitt sind es 45 %. Diesen Vorteil wiederum mit KI zu kontern, daran hat die Branche weniger Interesse. Nur 37 % der Gesundheitsunternehmen nennen KI als Handlungsfeld mit hoher Priorität, im Durchschnitt der Branchen sind es 44 %.

In Anbetracht der Schwierigkeiten, die das Gesundheitswesen bei der Bedrohungserkennung, bei der Abwehr von Ransomware und der Personalgewinnung hat, könnte es ratsam sein, sich auf die Grundlagen der Cyberhygiene zu besinnen. Dies wäre ein gangbarer Pfad nach vorne, auf dem die Unternehmen mit weniger mehr erreichen könnten.

## Öffentliche Hand

Die Befragten des öffentlichen Sektors legen mehr Wert auf Security Awareness Training (24 %) als der Durchschnitt (17 %). Entsprechend nennen 28 % mangelnde Cybersecurity-Kenntnisse und mangelndes Engagement vonseiten der Führungsebene als größte Herausforderung; der Durchschnitt liegt bei 20 %.

Und während die Befragten der öffentlichen Hand im letzten Jahr noch bezweifelten, dass KI das Sicherheitsteam entlasten könne, zeigen sie sich 2024 zuversichtlicher, wenn es um die neue generative KI geht:

- **Dass generative KI als Game Changer für die eigene Organisation wirken könnte, findet bei der öffentlichen Hand die meiste Zustimmung (55 %). Im Durchschnitt sind 47 % dieser Ansicht. Die Befragten der öffentlichen Hand erhoffen sich auch am meisten Nutzen für das Security-Team (55 %). Der Vergleichswert liegt hier bei 46 %.**
- **Die Sicherheitsteams des öffentlichen Sektors sind auch Vorreiter bei der Aufstellung von Richtlinien für den internen KI-Einsatz: 77 % haben bereits derartige Regelwerke, der Durchschnitt liegt bei 66 %.**
- **Optimistischer als der Durchschnitt ist dieser Sektor auch in Bezug auf Security Use Cases für generative KI: bei der Bedrohungserkennung (46 %, Durchschnitt: 35 %), bei Penetrationstests (42 %, Durchschnitt: 29 %) und bei der Schulung der Sicherheitsteams (44 %, Durchschnitt: 34 %).**

Die öffentliche Hand ist außerdem stärker an der SecOps-Automatisierung interessiert als die übrigen Branchen. Die Befragten nennen als Einsatzfelder die Verwaltung von SSL-Zertifikaten (43 %, Durchschnitt: 31 %), der Orchestrierung von Aktionen über Security-Tools hinweg (53 %, Durchschnitt: 38 %) und die Anreicherung von Warnmeldungen (47 %, Durchschnitt: 32 %). Bei den Grundlagen werden Fehlkonfigurationen öfter als Hauptbedrohungsvektor genannt: 42 % geben an, dass dies die häufigste Fehler-Ursache ist. Auch Seitwärtsbewegungen werden von den Befragten der öffentlichen Hand mehr gefürchtet als in den übrigen Branchen: 39 % nennen dies als ihre Hauptsorge.

Wenig Wissen und viel KI-Begeisterung könnte sich als toxische Kombination erweisen. Organisationen des öffentlichen Sektors sollten bei der Einführung generativer KI mit Bedacht vorgehen und sich gründlich über die Risiken informieren, bevor sie auf den Zug aufspringen.

# Länder-Highlights

Schlaglichter auf 8 Weltregionen.

## Australien

Die Daten zeichnen ein beunruhigendes Bild. Die australischen Unternehmen stimmen häufiger (44 %) als der weltweite Durchschnitt (29 %) voll und ganz der Aussage zu, dass geopolitische Spannungen die Angriffslage verschärfen. Und 56 % der australischen Befragten hatten bereits mit nationalstaatlichen Angriffen zu tun – deutlich mehr als der Gesamtdurchschnitt (39 %). Auch sonst haben australische Unternehmen überdurchschnittlich häufig Incidents zu verzeichnen, das gilt u. a. für Datenkompromittierungen (63 %, Durchschnitt: 52 %), Compliance-Verstöße (53 %, Durchschnitt: 43 %), Insider-Angriffe (55 %, Durchschnitt: 42 %) und CEO-Fraud (59 %, Durchschnitt: 49 %).

Möglicherweise sind diese Befunde auf mangelnde Transparenz zurückzuführen. 72 % der Befragten klagen, dass sie zu viel zwischen einzelnen Security-Tools hin- und herwechseln (Durchschnitt: 43 %). Die australischen Unternehmen haben auch öfter Probleme, ihre Angriffsfläche zu überschauen (35 %), als der Durchschnitt (20 %). Entsprechend dürftig fällt die Erkennung aus: Ganze 50 % der australischen Befragten sagen, dass sich die MTTD bei ihnen über Monate hinzieht; der Durchschnitt liegt deutlich niedriger: bei 19 %.

Die Befragten aus Australien haben im weltweiten Vergleich außerdem mehr mit Personalproblemen zu kämpfen:

- **52 % der Befragten sagen, dass schon Teammitglieder ohne die entsprechende Erfahrung Projekte leiten sollten (Durchschnitt: 39 %).**
- **50 % geben an, dass sie selbst oder andere schon mehrfach erwogen haben, der Cybersecurity den Rücken zu kehren (Durchschnitt: 36 %).**
- **52 % sagen, dass sich bei ihnen kritische Projekte oder Vorhaben verzögert haben (Durchschnitt: 37 %).**

Allerdings liegt Australien sowohl bei der Einführung von generativer KI als auch bei der Richtlinienerstellung in der Leader-Region: 69 % der Befragten geben an, dass die Leute in ihren Teams öffentliche generative KI für die Arbeit verwenden (Durchschnitt: 54 %), und 73 % sagen, dass sie Sicherheitsrichtlinien für den Einsatz generativer KI eingeführt haben (Durchschnitt: 66 %).

## Deutschland

Den Daten zufolge sind sich die deutschen Befragten der Risiken generativer KI stärker bewusst als die Teams in anderen Ländern:

- **41 % der deutschen Befragten stimmen voll und ganz der Aussage zu, dass generative KI die Angriffsfläche in besorgniserregendem Ausmaß vergrößert (weltweiter Durchschnitt: 31 %).**
- **38 % stimmen voll und ganz zu, dass generative KI ihre bestehende Angriffsfläche anfälliger macht (Durchschnitt: 29 %).**

Die deutschen Unternehmen haben offenbar vor allem Probleme bei der Personalgewinnung. 33 % geben an, dass die Cybersicherheitsanforderungen im vergangenen Jahr schwieriger zu erfüllen waren, weil sie nicht genügend qualifizierte Leute einstellen konnten; der Durchschnitt liegt bei 25 %.

Tool-Komplexität ist ein weiteres Hindernis. Die deutschen Teams klagen häufiger (53 %) als der Durchschnitt (43 %) darüber, dass sie zu oft zwischen separaten Sicherheitstools hin- und herwechseln müssen. Es könnte sein, dass es sich dabei öfter um Cloud-Tools handelt, denn Angriffe auf Cloud-Infrastrukturen zählen zu den Incidents, die in Deutschland am meisten Sorgen bereiten (23 %).

Die Schwierigkeiten bei Fachkräften und Tools könnten auch erklären, warum die MTTD deutscher Unternehmen etwas länger ist als anderswo. Im weltweiten Durchschnitt messen 35 % ihre MTTD in Wochen, in Deutschland sind es 40 %.

Trotz dieser Hindernisse zeichnen sich deutsche Unternehmen dadurch aus, dass sie bei Ransomware-Angriffen gut in der Lage sind, ihre Daten und Systeme zu retten. Damit waren in den letzten beiden Jahren 58 % erfolgreich – dies ist der höchste Prozentsatz im Ländervergleich, der Durchschnitt liegt bei 44 %.

Nicht zuletzt sind die Befragten aus Deutschland noch mehr (94 %) als der Durchschnitt (86 %) der Ansicht, dass die derzeitige geopolitische Lage ihr Unternehmen stärker in die Schusslinie der Cyberangreifer rückt.

## Frankreich

Die Befragten aus Frankreich hatten im letzten Jahr öfter Schwierigkeiten (56 %), mit den Cybersicherheitsanforderungen Schritt zu halten, als der weltweite Durchschnitt (46 %). Dazu passt, dass sie den Reifegrad ihrer Cybersicherheit auch niedriger einschätzen. Nur 37 % bezeichnen ihre Programme als „extrem fortgeschritten“, im weltweiten Durchschnitt sind es 47 %.

Auf die Frage, warum es schwieriger sei, die Cybersicherheitsanforderungen zu erfüllen, sagen 33 % der Befragten in Frankreich, dass die Anzahl der Tools und Anbieter ihres Security-Stacks zu groß geworden ist (Durchschnitt: 26 %). Und weil ein überkomplexer Stack zu Fehlkonfigurationen führt, erstaunt es nicht, dass 40 % der französischen Unternehmen fehlkonfigurierte Systeme als Grund zur Sorge nennen.

In Bezug auf generative KI zeigt sich die Lage in Frankreich etwas verwackelt: Bei der umfassenden Einführung von Cybersicherheitstools mit KI- und ML-Funktionen fallen die französischen Unternehmen mit 27 % hinter den weltweiten Durchschnitt (37 %) zurück. Einerseits sagen die Befragten häufiger (56 %) als der Durchschnitt (44 %), dass sie ihre Bemühungen auf generative KI konzentrieren, andererseits haben sie seltener (52 %) als der Durchschnitt (66 %) bereits Richtlinien für den KI-Einsatz etabliert.

Positiv zu vermerken ist, dass die französischen Unternehmen in den letzten beiden Jahren weniger Incidents der folgenden Angriffsarten erlitten haben als der weltweite Durchschnitt:

- **Kompromittierte Daten: 44 %**
- **Compliance-Verstöße: 37 %**
- **DDoS-Angriffe: 37 %**
- **Ransomware: 40 %**

## Großbritannien

Die Daten aus dem Vereinigten Königreich ergeben im weltweiten Vergleich ein insgesamt positives Bild. Deutlich wird insbesondere, dass die Unternehmen auf den Britischen Inseln häufiger die Zusammenarbeit suchen und auf diese Weise Resilienz aufbauen:

- **66 % der Befragten aus Großbritannien sagen, dass die Teams von Security und Software-Entwicklung enger zusammenarbeiten (weltweiter Durchschnitt: 54 %).**
- **56 % sagen, dass die Teams von Security und Engineering Operations enger zusammenarbeiten (Durchschnitt: 46 %).**

Auch in puncto Automatisierung liegen die britischen Unternehmen im Ländervergleich vorne. Vor allem bei der allgemeinen Prozessautomatisierung (40 %) und beim Schwachstellenmanagement (35 %) ist der Automatisierungsgrad hoch.

Und offenbar trifft der Fachkräftemangel britische Unternehmen weniger heftig. Dass Teammitglieder ohne die entsprechende Erfahrung mit der Leitung von Projekten betraut wurden, kommt im weltweiten Durchschnitt (39 %) öfter vor als in Großbritannien (30 %). Und nur 23 % der britischen Befragten sagen, dass kritische Sicherheitsprojekte aufgrund von Fachkräftemangel mehrfach gescheitert sind – im weltweiten Durchschnitt haben 33 % dergleichen erlebt.

Diese Erfolge könnten der Grund dafür sein, dass britische Unternehmen relativ selten von den folgenden Incidents betroffen sind:

- **Compliance-Verstöße: 35 % (Durchschnitt: 43 %)**
- **Insider-Angriffe: 37 % (Durchschnitt: 42 %)**
- **CEO-Fraud: 38 % (Durchschnitt: 49 %)**
- **DDoS-Angriffe: 38 % (Durchschnitt: 46 %)**
- **Kontenübernahmen: 34 % (Durchschnitt: 42 %)**
- **Ransomware: 37 % (Durchschnitt: 45 %)**
- **Angriffe über die Software-Lieferkette: 35 % (Durchschnitt: 43 %)**

## Indien

Indien hat den höchsten Prozentsatz von Unternehmen (66 %), die ihre Sicherheitsprogramme als „extrem fortgeschritten“ einstufen; der weltweite Durchschnitt liegt bei 47 %. Auch die Zusammenarbeit der internen Teams ist stärker ausgeprägt: 58 % der Security-Teams arbeiten enger mit der Software-Entwicklung zusammen, 52 % mit den Engineering Operations und 78 % mit der IT.

Auffällig ist auch, dass die indischen Unternehmen besonders auf die Cloud-Sicherheit fokussiert sind: 48 % der Befragten nennen dies als eins der wichtigsten Handlungsfelder, im weltweiten Durchschnitt sind es nur 35 %. Dazu passt, dass die Befragten aus Indien im Vergleich am häufigsten Angriffe auf Cloud-Infrastrukturen als Hauptsorge nennen (25 %). Noch mehr Sorgen bereiten jedoch Cyber-Erpressungen, die in Indien häufiger (37 %) als im Durchschnitt (24 %) als zentrales Problem genannt werden.

Compliance-Vorgaben mit Meldepflichten bei erheblichen Verstößen sind in Indien offenbar hochrelevant: Die Befragten sagen deutlich öfter (81 %) als der Durchschnitt (62 %), dass sie von regulatorischen Änderungen betroffen sind. Und 54 % der Befragten aus Indien sind voll und ganz der Überzeugung, dass Compliance eine Aufgabe ist, die sich alle im Sicherheitsteam zu eigen machen sollten; im weltweiten Durchschnitt haben nur 42 % diese Einstellung.

Was die Auswirkungen generativer KI angeht, so sind die indischen Unternehmen im Vergleich am optimistischsten. 51 % gehen davon aus, dass die Verteidigung den größeren Vorteil aus generativer KI ziehen kann – deutlich mehr als der weltweite Durchschnitt (43 %). In Indien werden auch häufiger mögliche Use Cases generativer KI identifiziert. Dazu gehören u. a. diese:

- **Erkennung und Priorisierung von Bedrohungen: 52 % (Durchschnitt: 35 %)**
- **Training und Ausbildung: 50 % (Durchschnitt: 34 %)**
- **Analyse von Bedrohungsinformationen: 55 % (Durchschnitt: 39 %)**
- **Erstellung von Erkennungsregeln: 44 % (Durchschnitt: 30 %)**
- **Zusammenfassung von Security-Infos: 54 % (Durchschnitt: 34 %)**

Dazu gehört auch, dass Indien bei der Einführung von Richtlinien zum Einsatz generativer KI seiner Zeit voraus ist: 82 % der Unternehmen haben dort bereits Regelwerke für End-User eingeführt, weltweit sind es erst 66 %.

## Japan

Das Land der aufgehenden Sonne zeigt sich selbstkritisch. Die Befragten aus Japan sagen häufiger (54 %) als der weltweite Durchschnitt (46 %), dass es immer schwieriger wird, mit den Cybersicherheitsanforderungen Schritt zu halten. Die Gegenprobe: 27 % finden, dass Security einfacher geworden ist – weltweit sind jedoch 41 % dieser Ansicht. Von den Befragten dieser Gruppe wiederum meinen in Japan nur 5 %, dass Security viel einfacher geworden ist; weltweit sind es 17 %.

Woher rühren diese Schwierigkeiten? Die folgenden Hindernisse werden von den Befragten aus japanischen Unternehmen häufiger genannt als im weltweiten Durchschnitt:

- **36 % finden, dass ihre Security Stacks zu unübersichtlich geworden sind (Durchschnitt: 26 %).**
- **29 % sind nicht in der Lage, alle sicherheitsrelevanten Daten effektiv zu analysieren (Durchschnitt: 21 %).**
- **27 % haben nur eine eingeschränkte Transparenz ihrer Angriffsfläche (Durchschnitt: 20 %).**

Ein weiterer Grund könnte in der mangelnden Ausgabenbereitschaft liegen. In Japan gehen nur 38 % davon aus, dass Ihre Security-Budgets deutlich aufgestockt werden.

Was die Vorteile von generativer KI für die Fachleute im SOC betrifft, so sind die japanischen Befragten eher skeptisch. Nur 37 % sind voll und ganz der Meinung, dass generative KI zur Entwicklung ihrer Skills beitragen kann. Der weltweite Durchschnitt ist mit 43 % optimistischer.

Von allen Ländern ist Japan am stärksten auf den Schutz vor Ransomware fixiert. 21 % bezeichnen dies als eines der wichtigsten Handlungsfelder. Und es gibt Anzeichen, dass sich diese Bemühungen bereits in Form kürzerer Erkennungszeiten bezahlt machen: Die japanischen Befragten sagen häufiger (43 %) als die Befragten im weltweiten Durchschnitt (33 %), dass bei ihnen die MTTD in Tagen gemessen wird.

## Singapur

Die Daten aus Singapur zeigen, dass dort einiges im Argen liegt. Die Cybersicherheitsprogramme haben insgesamt einen niedrigeren Reifegrad als die Programme in anderen Ländern. Konkret zeigt sich das an diesen Befunden:

- **Singapur hat den höchsten Prozentsatz an Befragten, die ihre Cybersicherheitsprogramme als „im Aufbau befindlich“ bezeichnen: 14 % (weltweiter Durchschnitt: 7 %).**
- **Die Teams haben seltener die nötigen Befugnisse und Ressourcen, um Cybersecurity-Herausforderungen anzugehen: 77 % (Durchschnitt: 91 %).**
- **Nur 28 % der Befragten rechnen damit, dass die Ausgaben für Cybersicherheit steigen – das ist der niedrigste Wert im gesamten Ländervergleich.**
- **26 % der Befragten kennen ihre MTTR nicht, 25 % führen im Nachgang eines Incidents keine Analysen durch, um die MTTD zu bestimmen.**

Damit korreliert die Beobachtung, dass die Unternehmen in Singapur die Business-Vorteile digitaler Resilienz tendenziell eher ausblenden. Die Befragten sind deutlich seltener (23 %) als der Durchschnitt (33 %) der Ansicht, dass digitale Resilienz die Kundenbindung verbessern kann, und sie glauben auch weniger (25 %) als der Durchschnitt (35 %), dass digitale Resilienz hilft, erhebliche Betriebsunterbrechungen zu vermeiden.

Die Unternehmen aus Singapur sind anscheinend auch weniger an einer Zusammenarbeit von Security, Rechtsabteilung und Compliance-Teams interessiert. Verstärkten Security-Schulungen der Compliance-Teams können nur 29 % voll und ganz zustimmen – der weltweite Durchschnitt liegt bei 42 %. Und ebenfalls nur 29 % können voll und ganz bestätigen, dass Compliance in die Workflows der Security-Teams integriert ist – auch hier liegt der weltweite Durchschnitt bei 42 %.

Unsere Daten deuten generell darauf hin, dass der Reifegrad von Sicherheitsprogrammen mit der KI-Priorisierung korreliert. Von daher ist es kaum überraschend, dass nur 36 % der Befragten in Singapur eine Konzentration auf KI melden (Durchschnitt: 44 %); auch ist der Anteil von Unternehmen mit Richtlinien für den Einsatz generativer KI geringer, er liegt bei nur 48 %. Und im weltweiten Vergleich macht sich Singapur am wenigsten Gedanken über KI-gestützte Angriffe: Nur 23 % nennen dies als größte Sorge.

## USA

Die Daten aus den USA weichen nur selten vom weltweiten Durchschnitt ab. Ein Bereich allerdings, in dem die Werte darüber liegen, betrifft die Richtlinien für den Einsatz generativer KI – hier haben 72 % bereits Regelwerke eingeführt, während der Durchschnitt bei 66 % liegt. Dazu passt, dass die Befragten von US-Unternehmen im weltweiten Vergleich sich am wenigsten um den Missbrauch generativer KI sorgen; nur 18 % nennen dies als Fehler-Ursache.

Auffällig ist auch, dass die Unternehmen in den USA mit längeren Erkennungszeiten zu kämpfen haben. Die Befragten sagen öfter (40 %) als der Durchschnitt (35 %), dass sie die MTTD in Wochen messen. Der Anteil derjenigen, bei denen die MTTD Monate dauert, liegt mit 22 % ebenfalls höher als der Durchschnitt von 19 %. Und dies sind offenbar bereits verbesserte Werte, denn 30 % geben an, dass sie die MTTD durch Prozessautomatisierung optimiert haben (Durchschnitt: 25 %).

Was die Prioritäten für die Zukunft betrifft, so haben die US-Unternehmen eher vor, den Fachkräftemangel anzugehen. 21 % der Befragten sagen, dass sie mehr Cybersicherheitspersonal einstellen wollen (Durchschnitt: 18 %), und 25 % haben vor, Security-Operations-Schulungen anzubieten (Durchschnitt: 23 %).

# Über Splunk

Splunk macht Unternehmen digital resilienter. Führende Unternehmen nutzen unsere Plattform für einheitliche Security und Observability, um ihre digitalen Systeme sicher und zuverlässig zu halten. Unternehmen vertrauen auf Splunk, um zu verhindern, dass sich Sicherheits-, Infrastruktur- und Anwendungsprobleme zu größeren Vorfällen entwickeln, um Beeinträchtigungen durch digitale Störungen zu reduzieren und um die Transformation zu beschleunigen.

Bleiben Sie dran und reden Sie mit:



**splunk**>

Splunk, Splunk> und Turn Data Into Doing sind Marken und eingetragene Marken von Splunk Inc. in den Vereinigten Staaten und anderen Ländern. Alle anderen Markennamen, Produktnamen oder Marken gehören den entsprechenden Inhabern. © 2024 Splunk Inc. Alle Rechte vorbehalten.

24-492903-Splunk-State-of-Security-113\_GER

