Delinea

WHITEPAPER

Identitätssicherheit ist entscheidend für den Abschluss und die Aufrechterhaltung einer Cyberversicherung

Bericht zur Untersuchung der Cyberversicherung 2024

Zusammenfassung

Die Cyberversicherung ist ein wichtiger Bestandteil eines Cyber-Risikomanagementprogramms, damit die Widerstandsfähigkeit und Wiederherstellung gewährleistet sind. Jetzt, da der Abschluss einer Cyberversicherung für Unternehmen aller Art zum Standard geworden ist, hat sich der Schwerpunkt auf die Aufrechterhaltung der Versicherungsfähigkeit verlagert, auch wenn sich die Risikofaktoren ändern.

Da Cybervorfälle die Branche in Aufruhr versetzen, nehmen die Versicherer detaillierte Risikobewertungen vor und es wird für Führungskräfte im Bereich Cybersicherheit immer schwieriger, den Wert ihres Sicherheitsprogramms nachzuweisen und eine robuste Deckung zu erhalten. Die Organisationen müssen entsprechende Nachweise erbringen, um sicherzustellen, dass ihre Versicherung fortbesteht und bei Bedarf erhöht oder angepasst wird. Für komplexe, hybride Organisationen mit wechselnden Risikoprofilen kann das Erfassen genauer, aktueller Informationen eine unglaublich mühsame und zeitaufwendige Arbeit sein.

In dieser Forschungsstudie mit 300 Entscheidungsträgern analysieren wir, wie Unternehmen diese Herausforderungen angehen, damit sie eine Cyberversicherung abschließen und aufrechterhalten können. Wir untersuchen insbesondere, wie Unternehmen neuere Technologien wie künstliche Intelligenz einsetzen, um die Effizienz zu steigern, schnell zu skalieren und Kosten zu senken.

Die wichtigsten Erkenntnisse:

1. **Lücken in der Identitätssicherheit sind die häufigste Ursache für Cybervorfälle, die zu Versicherungsansprüchen führen. Identitäts- und Privilegienkompromittierungen sind für 47 % der Angriffe verantwortlich, die zu Versicherungsansprüchen führen.**

2. **Versicherungsgesellschaften wollen einen Nachweis der Identitätssicherheit, bevor sie eine Police ausstellen. Mehr als 40 % der Versicherungsgesellschaften verlangen vor Abschluss dem Gewähren einer Police Least-Privilege-Zugriffskontrollen/-autorisierung. Nahezu alle (95 %) der US-Unternehmen mussten in Identitätssicherheitslösungen investieren, bevor sie eine Police abschließen konnten.**

3. **Obwohl die Gesamtkosten für Cyberversicherungen steigen, bietet KI den Versicherungsnehmern einen Vorteil. Die Hälfte der US-Unternehmen nutzt KI-gestützte Bedrohungserkennung und -überwachung, um ihre Cyberversicherungsbeiträge zu senken.**

47 %

Identitäts- und Privilegien-kompromittierungen sind für 47 % der Angriffe ver-antwortlich, die zu Versicherungsansprüchen führen

Lesen Sie weiter, um Ihre eigenen Identitätssicherheitspraktiken und Cyberversicherungsstrategien zu bewerten. Die Informationen werden Ihnen helfen, sich auf Ihre nächste Bewertung der Cyberversicherung vorzubereiten und innovative Möglichkeiten zur Reduzierung Ihres Aufwands und Ihrer Kosten zu ermitteln.

Wichtigste Erkenntnis 1

Lücken in der Identitätssicherheit sind die häufigste Ursache für Cybervorfälle, die zu Versicherungsansprüchen führen.

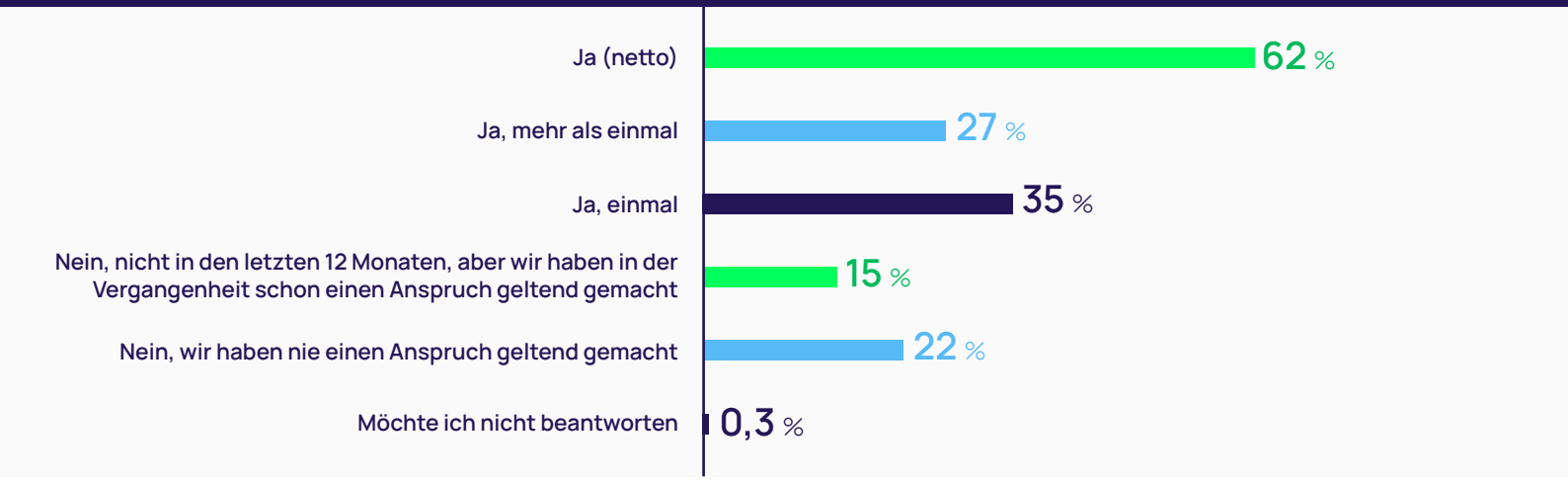
Die Häufigkeit von Cyberversicherungsansprüchen ist nach wie vor hoch.

Wenn Unternehmen eine Cyberversicherung haben, nutzen sie diese auch.

Die Daten zeigen, dass 77 % der Unternehmen, die eine Versicherung abgeschlossen haben, bereits einen Schadensfall gemeldet haben. Dies deckt sich mit den Ergebnissen der Delinea-Umfrage von 2023, in der 79 % der Befragten angaben, in der Vergangenheit eine Cyberversicherung abgeschlossen zu haben.

Allein in den letzten 12 Monaten haben 62 % der Unternehmen einen Schadensfall gemeldet. Ein besonders schlechtes Jahr war es für mehr als 27 % der Unternehmen, die in den letzten 12 Monaten mehr als einmal einen Schadensfall gemeldet haben.

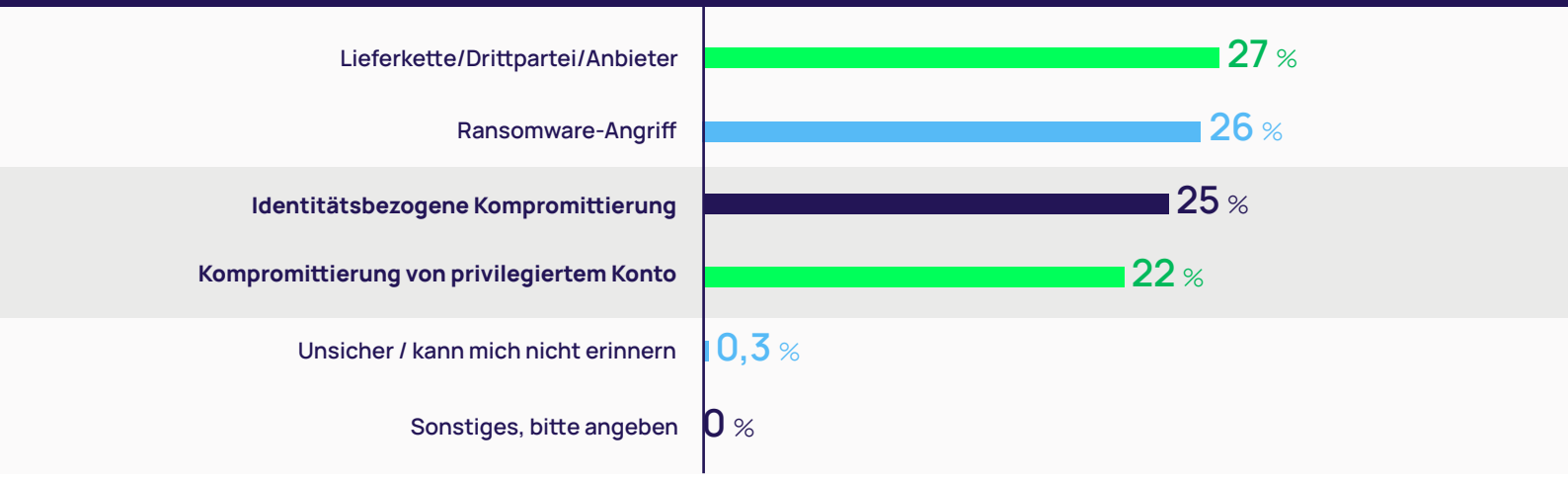
Abbildung 1 | Hat Ihr Unternehmen in den letzten 12 Monaten einen Cyberversicherungsanspruch geltend gemacht?



Bei den Angriffstechniken werden Identitäten und privilegierte Konten missbraucht.

Die beiden Vektoren für Identitätsangriffe, d. h. die Kompromittierung von Identitätsdaten und die Kompromittierung von privilegierten Konten, verursachen zusammen über 47 % der Angriffe, die zu Versicherungsansprüchen führen.

Abbildung 2 | Was war die Ursache für den Cybervorfall im Zusammenhang mit dem Cyberversicherungsanspruch?



Heutzutage müssen die meisten Cyberangreifer nicht mehr wirklich einbrechen – sie melden sich einfach an. Identitätsbezogene Angriffe beginnen in der Regel damit, dass ein Angreifer gültige Zugangsdaten verwendet, die er gestohlen oder erworben hat. Er kann diese Zugangsdaten dann verwenden, um sich als eine autorisierte Identität auszugeben oder ein privilegiertes Konto zu nutzen, um den Zugriff auf geschützte Ressourcen zu ermöglichen. Je nach dem Umfang des Zugriffs, der mit dieser Identität oder diesem privilegierten Konto verbunden ist, ist der Angreifer möglicherweise in der Lage, Malware herunterzuladen, Daten zu manipulieren, Systeme herunterzufahren und noch mehr. All das kann zu einem potenziellen Anspruch gegenüber der Versicherung führen.

Als Teil der Lieferkette haben Dritte, wie Auftragnehmer, Anbieter und Partner, oft Zugang zu sensiblen Daten und IT-Systemen. IT-Betriebsteams lagern beispielsweise häufig Aufgaben wie die Fehlerbehebung aus und Entwicklungsteams skalieren in der Regel mit externen Entwicklern. Diese Benutzer können über ein gemeinsames privilegiertes Konto oder eine individuelle Identität auf Ressourcen zugreifen. Allzu oft arbeiten diese Arten von Nutzern ohne ausreichende Aufsicht und der Zugang bleibt noch lange nach Abschluss der Projekte bestehen. So bleiben Schwachstellen zurück, die von Angreifern ausgenutzt werden können, was dazu führt, dass ein Anspruch gegenüber der Versicherung geltend gemacht wird.

Ransomware gelangt oft durch Social Engineering oder Phishing in das System. Dabei werden Benutzer mit lokalen Rechten dazu verleitet, auf einen Link zu klicken, über den Malware heruntergeladen wird. Wenn Sie erst einmal in das System eingedrungen sind, können Angreifer Daten verschlüsseln und ein Lösegeld für den Verschlüsselungscode verlangen oder Daten exfiltrieren und damit drohen, sie freizugeben, wenn keine Lösegeldzahlung erfolgt.

Unternehmen schließen eine Cyberversicherung ab, um ihre Compliance-Anforderungen zu erfüllen und die Geschäftskontinuität sicherzustellen.

Wir haben die Unternehmen gefragt, warum sie sich *zu dem jeweiligen Zeitpunkt* um Versicherungsschutz bemüht haben. Zu den Gründen gehören die Einhaltung gesetzlicher Vorschriften, Anweisungen der Unternehmensführung oder des Vorstands sowie Reaktionen auf jüngste Cyberangriffe, die entweder in der Branche oder direkt im Unternehmen stattgefunden haben.

Die Befragten gaben an, dass die Einhaltung von Compliance-Anforderungen / gesetzlichen Anforderungen der *wichtigste Grund für* den Abschluss einer Cyberversicherung ist. Es geht hier nicht darum, dass Vorschriften wie PCI, HIPAA und andere Compliance-Regelungen den Abschluss einer Cyberversicherung für versicherte Unternehmen vorschreiben. Es geht auch nicht darum, dass eine Cyberversicherung eine wirksame Strategie ist, um für Bußgelder bei Nichteinhaltung von Vorschriften aufzukommen, zumindest nicht für die meisten Unternehmen. Die Realität ist, dass Bußgelder der ***seltenste*** Kostenpunkt ist, für die eine Cyberversicherung aufkommt.

Abbildung 3 A | Was waren die Hauptgründe für die Beantragung der Cyberversicherung zum Zeitpunkt, als Sie diese abgeschlossen haben?

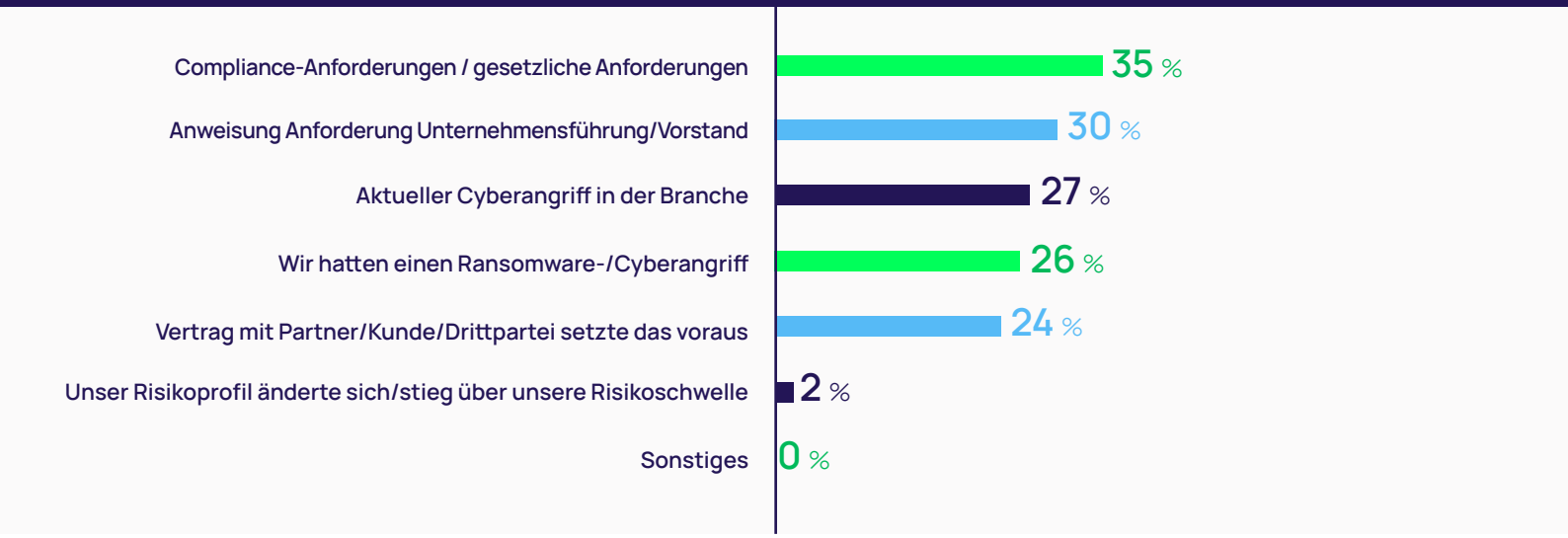
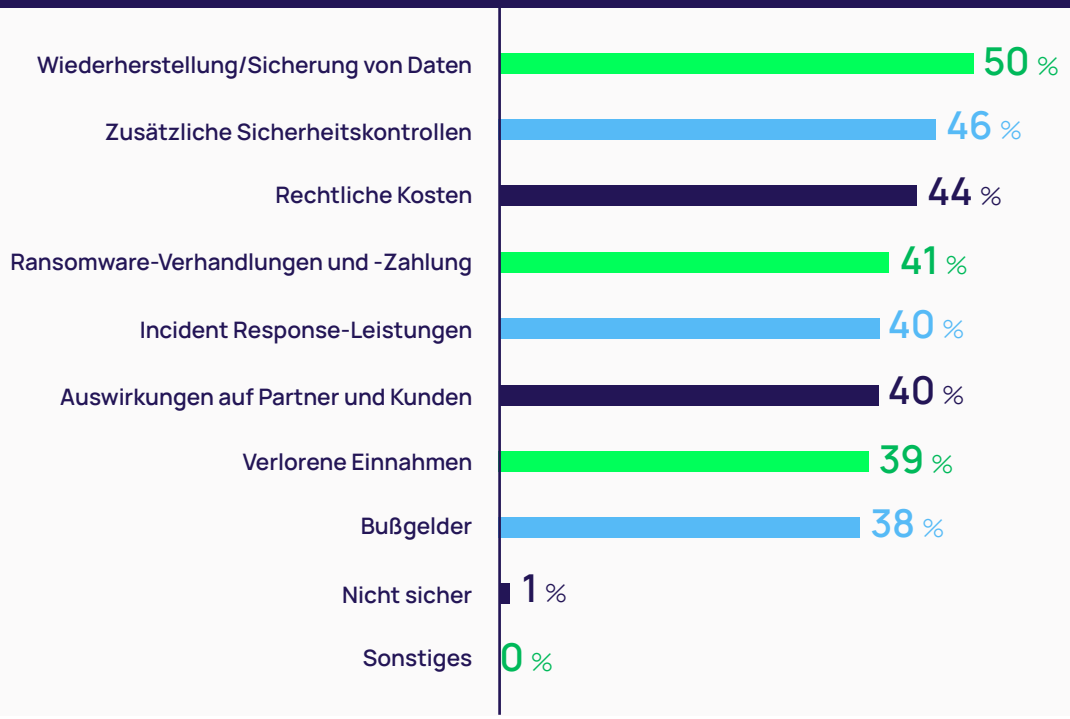


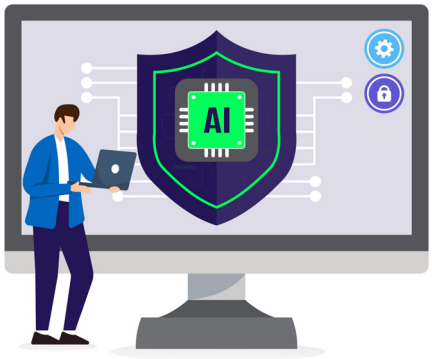
Abbildung 3 B | Wofür würde Ihre Cyberversicherung aufkommen?



Wahrscheinlicher ist, dass Unternehmen, die den Vorschriften der Branche unterliegen, bei Nichteinhaltung der Datenschutzbestimmungen mit hohen Geldstrafen rechnen müssen. Eine schnelle Wiederherstellung und Sicherung kann dazu beitragen, Geldstrafen und andere Kosten zu vermeiden, die mit der Nichteinhaltung von Vorschriften nach einer Datenschutzverletzung verbunden sind, da es so möglich ist, die Daten schnell wiederherzustellen und zu sichern.

Cyberversicherungen legen den absoluten Schwerpunkt auf Dienste zur Datenwiederherstellung und Datensicherung, da diese für die Minimierung von Ausfallzeiten und finanziellen Verlusten nach einem Cybersicherheitsvorfall von entscheidender Bedeutung sind. Durch die Abdeckung dieser Leistungen ermöglichen die Versicherer eine schnelle Wiederherstellung und die Widerstandsfähigkeit des Unternehmens, was sowohl dem Versicherten als auch dem Versicherer zugutekommt.

Es ist außerdem zu beachten, dass eine Versicherung eine Strategie für das Risikomanagement und nicht für die Cybersicherheit ist. Viele Unternehmen nutzen Compliance- oder Cybersicherheits-Frameworks wie NIST, um ihre Sicherheitsprogramme anzuleiten, auch wenn sie nicht versicherte Unternehmen sind. Diese Frameworks verlangen den Nachweis von Sicherheitskontrollen, ebenso wie die Versicherungsgesellschaften, da diese nachweislich das Risiko verringern. Wenn Sie diese Kontrollen einrichten, stellen Sie sowohl die Aufsichtsbehörden als auch die Versicherungsgesellschaften zufrieden. Auch wenn Sie nicht an Vorschriften gebunden sind, die bei Nichteinhaltung Geldbußen nach sich ziehen, können Sie diesen Teil nicht einfach ignorieren und erwarten, dass Sie bei der nächsten Prüfung oder Bewertung durch die Versicherung bestehen werden.



Die Hälfte der US-Unternehmen nutzt KI-gestützte Bedrohungserkennung und -überwachung, um ihre Cyberversicherungsbeiträge zu senken

Wichtigste Erkenntnis 2

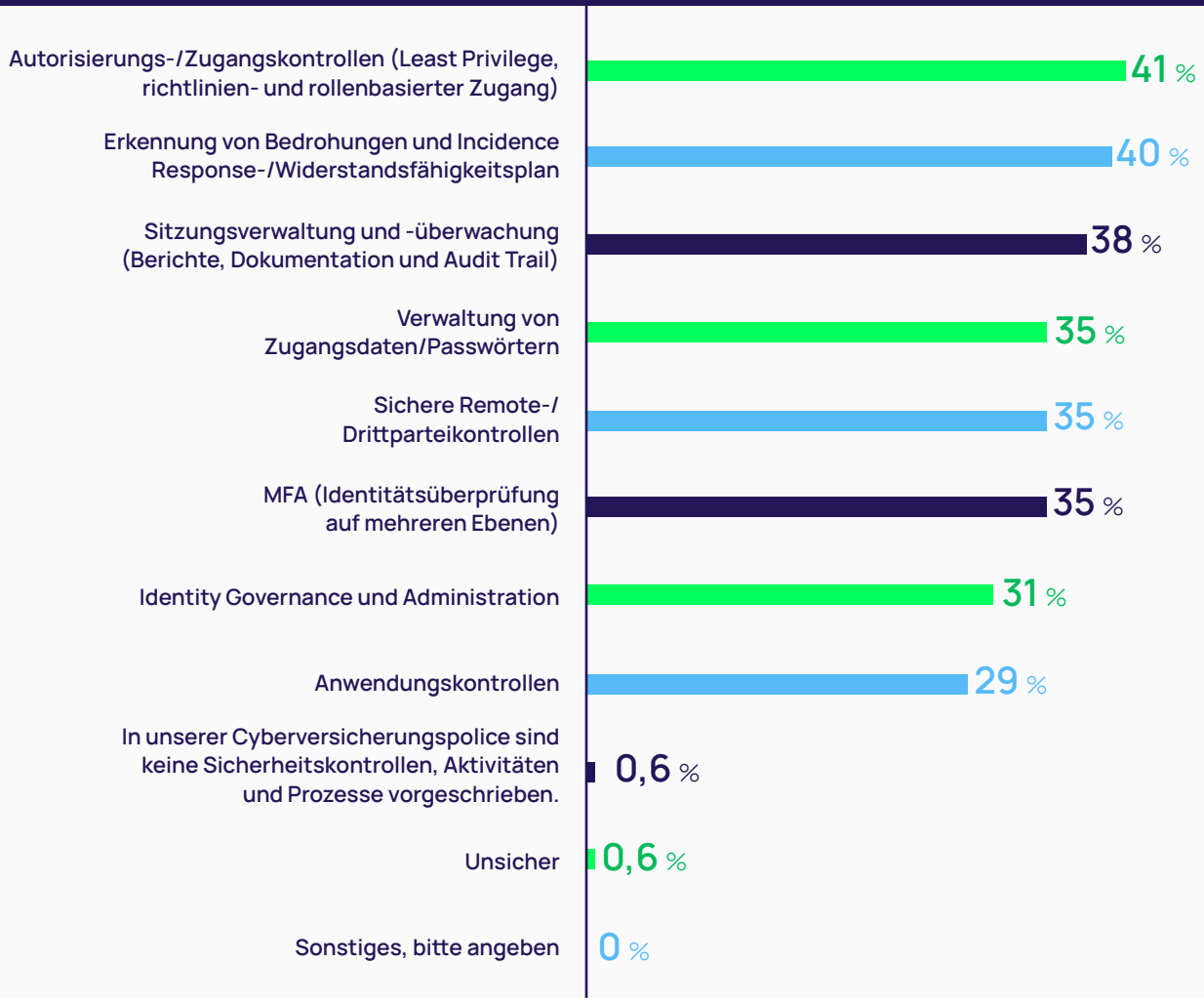
Versicherungsgesellschaften wollen einen Nachweis der Identitätssicherheit, bevor sie eine Police ausstellen. Davon setzen 41 % Autorisierungskontrollen voraus.

Die Versicherer verlangen Identitätssicherheitskontrollen, Aktivitäten und Prozesse.

Da nun mehr historische Daten vorliegen, die auf die Ursache von Cyberangriffen hindeuten, verlangen viele Versicherungsgesellschaften von ihren Versicherungsnehmern, die Wahrscheinlichkeit und die Auswirkungen von Cybervorfällen zu minimieren, was die Höhe der potenziellen Auszahlungen bei Schadensfällen verringert. Fast alle Befragten haben eine Form von Identitätssicherheitsanforderung, die vom Anbieter Ihrer Cyberversicherung vorgeschrieben wird. Die meisten der Befragten gaben an, dass Cyberversicherungspolicen mehrere Identitätssicherheitskontrollen erfordern.

Die Versicherer verlangen in der Regel von den Versicherungsnehmern, dass sie Kontrollen in Bezug auf die Autorisierung/Least-Privilege-Zugang einrichten, dicht gefolgt von der Erkennung von und Reaktion auf Bedrohungen.

Abbildung 4 | Welche Sicherheitskontrollen, Aktivitäten und Prozesse sind in Ihrer Cyberversicherungspolice vorgeschrieben?



Diese Kontrollen entsprechen den Best Practices der Branche und den gesetzlichen Anforderungen. Wirksame Sicherheitskontrollen tragen nicht nur zur Vorbeugung von Vorfällen bei, sondern sorgen auch dafür, dass Unternehmen schnell und effektiv reagieren können, um Ausfallzeiten und finanzielle Verluste zu verringern. Indem sie umfassende Sicherheitskontrollen vorschreiben, können die Versicherer potenzielle Verluste besser verwalten und vorhersagen, was zu stabileren und vorhersehbaren Beiträgen für die Versicherungsnehmer führt.

Definition der erforderlichen Identitätssicherheitskontrollen

Zugangskontrollen/-autorisierung	Zugriffskontrollen legen fest, auf welche Systeme und Daten eine Identität zugreifen kann und was sie mit diesem Zugriff tun kann. Unternehmen verwalten die Autorisierung in der Regel über Richtlinien wie rollenbasierte Zugriffskontrollen oder attributbasierte Zugriffskontrollen. Least-Privilege-Best-Practices setzen voraus, dass Identitäten nur die Berechtigungen haben, die zur Erfüllung ihrer Aufgaben erforderlich sind, und zwar nur dann, wenn sie diese benötigen.
Anwendungskontrollen	Anwendungskontrollen helfen Ihnen dabei, ein Gleichgewicht zwischen Least-Privilege-Best-Practices und der Produktivität der Benutzer herzustellen. Vertrauenswürdige Anwendungen werden zur automatischen Installation oder Ausführung zu den Zulassungslisten hinzugefügt, während bekannte bösartige Anwendungen (Malware) zu den Ablehnungslisten hinzugefügt und blockiert werden. Unbekannte Anwendungen können so lange isoliert werden, bis sie geprüft und genehmigt wurden.
Verwaltung von Zugangsdaten/ Passwörtern	Zu den Zugangsdaten gehören Benutzernamen, Kennwörter, Token und andere Secrets, die den Zugriff auf Ihre Systeme und Daten ermöglichen. Cyberangreifer verwenden Methoden wie das Credential Stuffing und das Passwort-Cracking, um Zugangsdaten zu stehlen. Es ist auch möglich, dass Sie die Zugangsdaten von Zugangsbrokern im Dark Web kaufen. Um einen Diebstahl zu verhindern, sollten die Zugangsdaten schwer zu erraten und jederzeit gesichert sein. Sie können Zugangsdaten in einem militärisch verschlüsselten Vault speichern. Die kontinuierliche Verwaltung der Zugangsdaten, wie Rotation und Ablauf, stellt sicher, dass die Zugangsdaten nur eine begrenzte Lebensdauer haben.
Identity Governance and Administration (IGA)	IGA steuert die Berechtigungen für Identitäten während ihres gesamten Lebenszyklus, einschließlich des Beitretens, des Wechsels oder des Abgangs von Benutzern und ermöglicht die Überwachung aller Identitäten in Ihrem Unternehmen (Menschen und Maschinen), was den Nachweis dieser Überwachung gegenüber Auditoren, Cyberversicherungsgesellschaften und Compliance-Organisationen erleichtert.
Multi-Faktor-Authentifizierung (MFA)	Bei der Multi-Faktor-Authentifizierung wird die Identität von Personen überprüft, indem sie etwas vorweisen müssen (z. B. einen Code auf einem Telefon oder einen Fingerabdruck) oder etwas angeben müssen (z. B. Antwort auf eine Frage). Best Practices erfordern eine Identitätsüberprüfung bei jeder Interaktion, die ein hohes Risiko birgt, einschließlich der ersten Anmeldung und der Berechtigungserhöhung.
Sichere Remote-/ Drittparteikontrollen	Diese Kontrollen ermöglichen es externen Mitarbeitern und Dritten, sicher auf genau die Ressourcen zuzugreifen, die sie für ihre Arbeit benötigen, während sie gleichzeitig genau überwacht werden.
Sitzungsmanagement und Überwachung	Durch Sitzungsmanagement und die kontinuierliche Überwachung werden ungewöhnliche Vorgänge bei Identitätsaktivitäten und -ereignissen erkannt. Zudem werden die proaktive Vorbeugung von Vorfällen und eine schnelle Reaktion ermöglicht. Anhand von Audit Trails lassen sich Muster erkennen, die für die Vorhersage von Risiken und die Beschleunigung der forensischen Analyse nach einem Vorfall nützlich sind. Darüber hinaus können Sie mit Hilfe von detaillierten Berichten Verbesserungen Ihrer Identitätssicherheit nachverfolgen, die Rechenschaftspflicht sicherstellen und den Nachweis von Kontrollen gegenüber Cyberversicherungsgesellschaften erbringen.
Bedrohungserkennung und Incident Response	Eine effektive Bedrohungserkennung und Incident Response sind entscheidend für die Cyberresilienz und Geschäftskontinuität. Zu den Kontrollen gehören Mechanismen zur Bedrohungserkennung und ein strukturierter Reaktionsplan zur proaktiven Risikominderung und zur Eindämmung und Behebung laufender Vorfälle. Dazu gehören Redundanzen, die sicherstellen, dass es bei einem Vorfall zu minimalen oder gar keinen Ausfällen kommt.

Die Wichtigkeit der Identitätssicherheit wird auch von Sicherheits- und Cyberversicherungsexperten hervorgehoben

CJ Dietzman
Senior Vice President von Alliant Insurance Service

Wenn ich an die Erwartungen von Versicherungsträgern und Versicherern denke, steht die Identitätssicherheit inzwischen sehr auf dem Spiel. Cyberversicherungsgesellschaften messen das Risiko anhand von Vorfällen, Gesetzen und Schadensfällen. Beim Reverse Engineering von Cyberangriffen wurden oft Schwachstellen im Identitätsmanagement festgestellt. „Sie müssen eine gute Darstellung der integrierten Kontrollen und einen ganzheitliche Ansatz haben, wie Sie das Risiko des unbefugten Zugriffs mindern und Identitäten schützen."

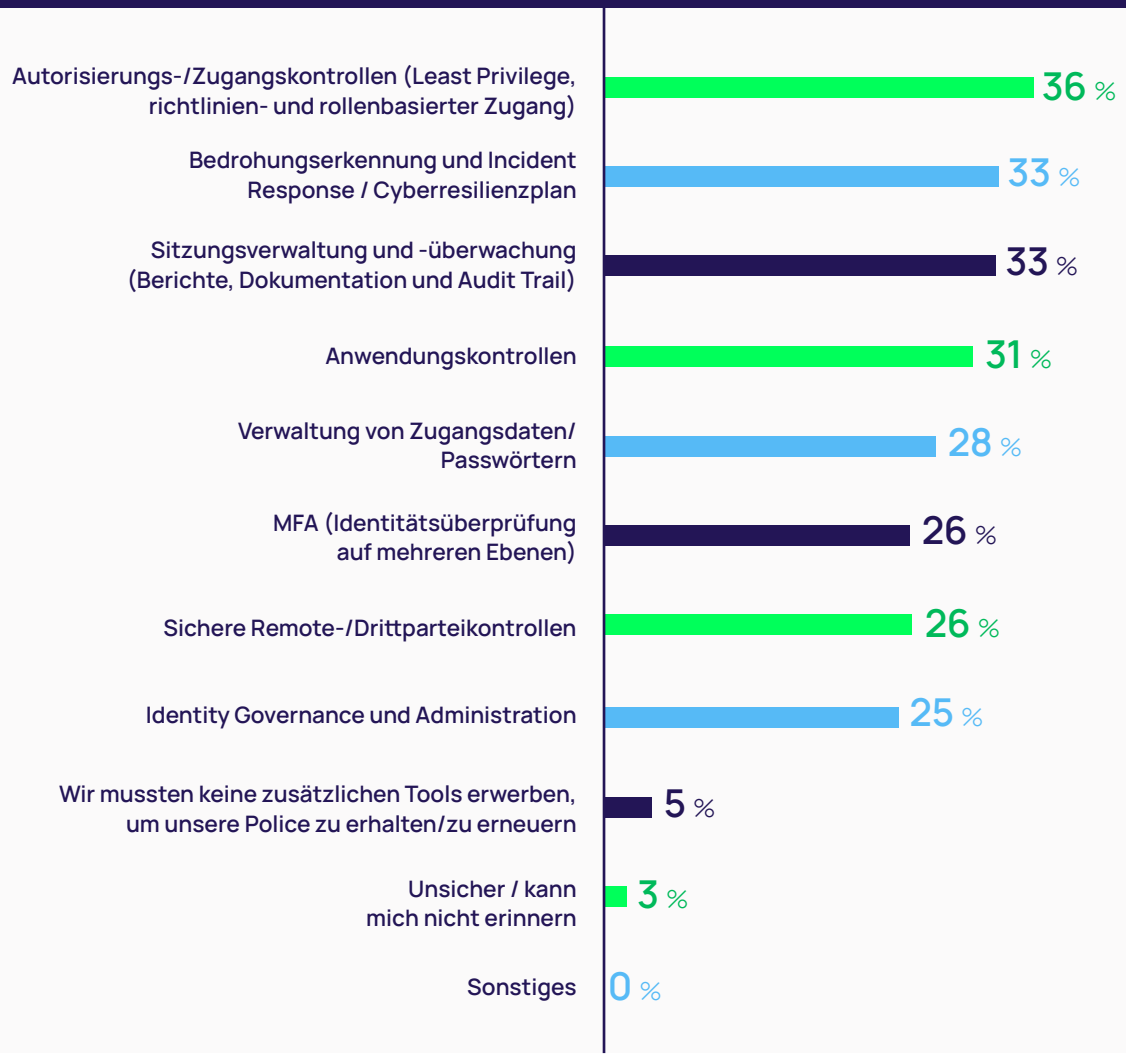
„Der größte Teil der Vorfälle im Bereich der Cybersicherheit, die zu einem Schadensfall führen, ist auf das Abgreifen von Zugangsdaten, die Kompromittierung eines Mitarbeiters, die Nutzung eines Dritten, der Zugang zu Ihren Systemen hatte, usw. zurückzuführen."

Myrna Soto
CEO von Apogee Executive Advisors und Expertin für Cybersicherheit und Risikomanagement

Die Mehrheit der befragten Unternehmen musste in Identitätssicherheitslösungen investieren, bevor sie ihre Police abschließen oder erneuern konnten.

Um die oben genannten Sicherheitsanforderungen zu erfüllen, können Unternehmen potenziellen Versicherungsanbietern nicht einfach manuelle Prozesse vorlegen und erwarten, dass sie eine Police erhalten. Stattdessen mussten sie Identitätssicherheitslösungen als Teil ihres Sicherheitstechnologie-Stacks erwerben.

Abbildung 5 | Welche zusätzlichen Tools mussten Sie erwerben, um Ihre Police zu erhalten/zu erneuern?

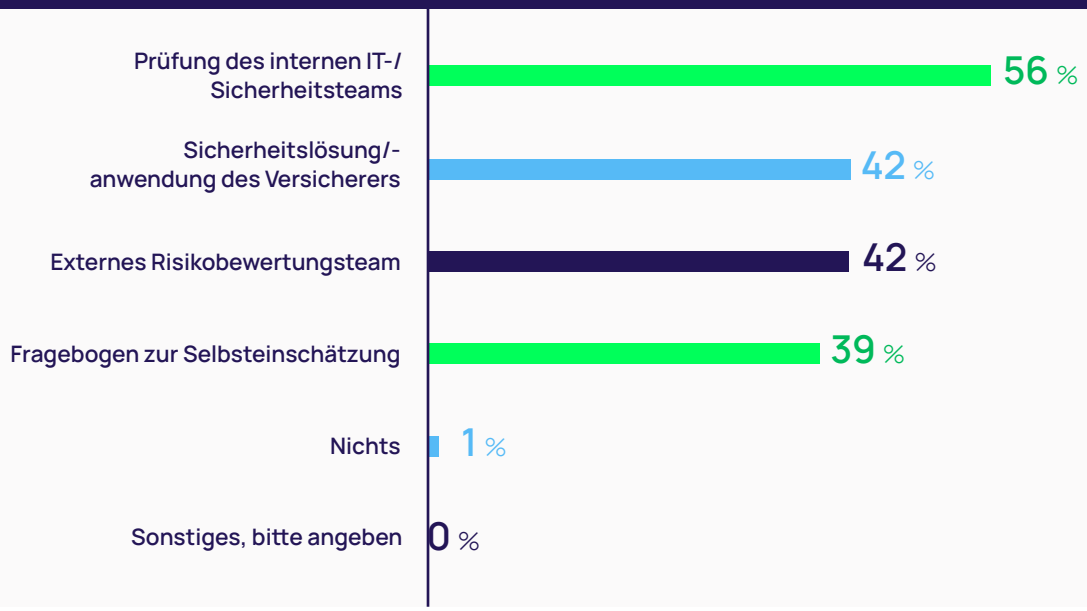


Diese Ergebnisse verdeutlichen die unterschiedlichen Sicherheitsbedürfnisse der Unternehmen und den unterschiedlichen Stand der Vorbereitungen in Bezug auf die Cybersicherheitsinfrastruktur.

Durch Bewertungen wird die Sicherheitslage beurteilt, bevor Policen gewährt werden.

Angesichts der zunehmenden Reife der Cyberversicherungsbranche verlangen die Versicherer jetzt detaillierte Bewertungen der Sicherheitslage. Die meisten Befragten entscheiden sich dafür, diese Bewertungen selbst durchzuführen. Andere ziehen ein externes Risikobewertungsteam hinzu, um ihre internen Fähigkeiten zu ergänzen und einen unvoreingenommenen Blick auf die Sicherheitslage des Unternehmens zu erhalten.

Abbildung 6 | Welche Arten von Bewertungen mussten Sie durchführen, um Ihre Cyberversicherungspolice zu erhalten?



Unabhängig davon, ob Sie diese Bewertungen selbst durchführen oder sich auf einen externen Anbieter verlassen, müssen Sie damit rechnen, dass sie qualifizierte IT- und Sicherheitsteammitglieder von ihrer täglichen Arbeit und strategischeren Projekten abziehen.

41 %

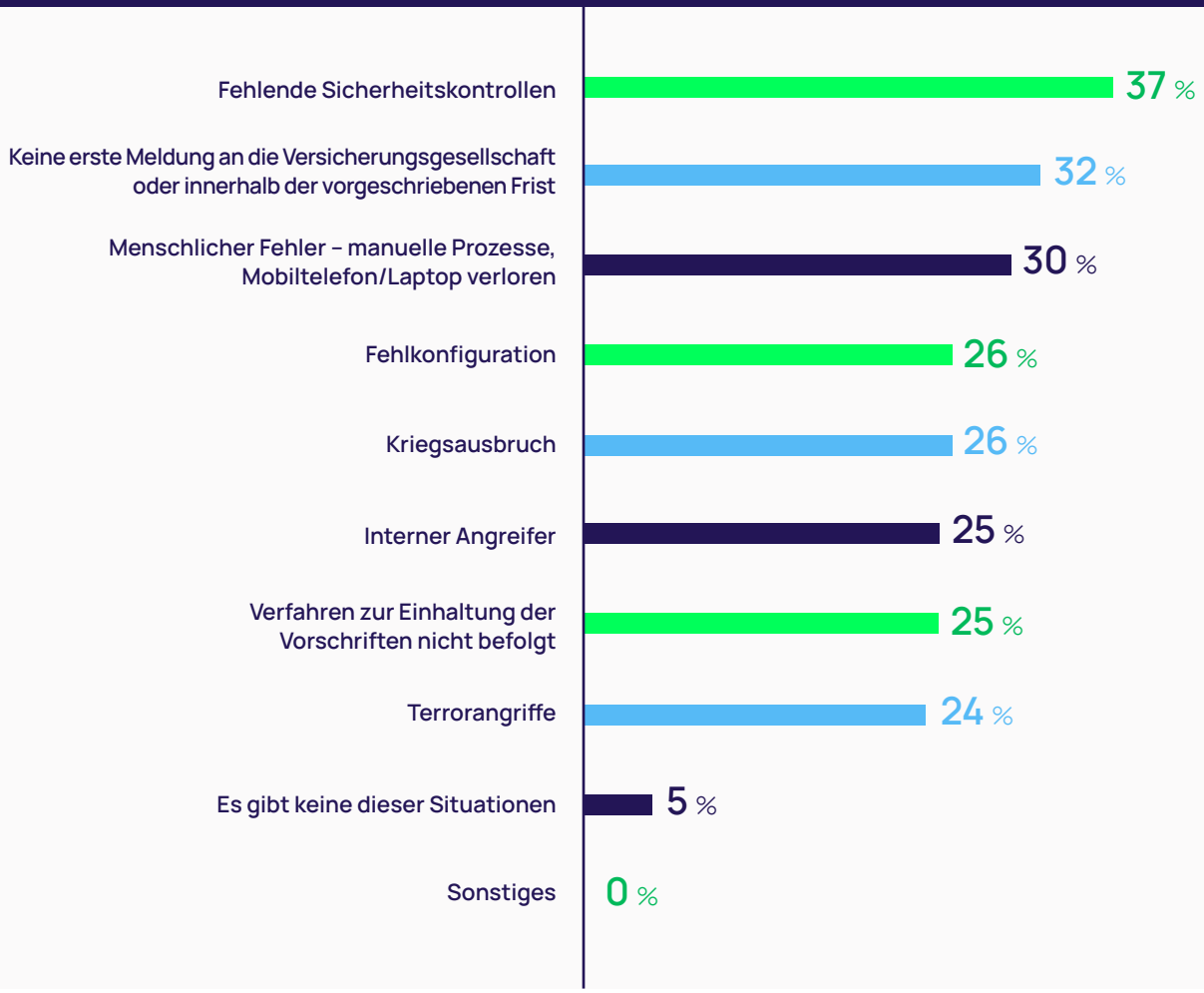
41 % der Versicherungsgesellschaften verlangen vor Abschluss einer Police eine Least-Privilege-Zugriffskontrollen/-autorisierung

Die Anforderungen hören nicht auf, wenn die Policen genehmigt sind. Sie müssen wirksame Sicherheitskontrollen durchführen, wenn Sie erwarten, dass die Kosten für Ihre gemeldeten Schadensfälle gedeckt werden.

Gute Nachrichten: Sie haben Identitätssicherheitslösungen erworben, Sie haben Kontrollen nachgewiesen und Sie haben eine positive Bewertung erhalten. Ihre Versicherungspolice ist genehmigt worden!

Die Ergebnisse dieser Umfrage zeigen jedoch, dass ein Versicherungsanspruch mit hoher Wahrscheinlichkeit abgelehnt wird, wenn Sie diese Sicherheitskontrollen nicht einhalten und ordnungsgemäß anwenden. Wie auch die Befragten müssen Sie sicherstellen, dass die Sicherheitskontrollen auf Ihre sich verändernde Organisation angewendet werden, korrekt konfiguriert sind und wie erwartet funktionieren.

Abbildung 7 | In welchen Situationen, wenn überhaupt, wäre Ihr Cyberversicherungsschutz ungültig?



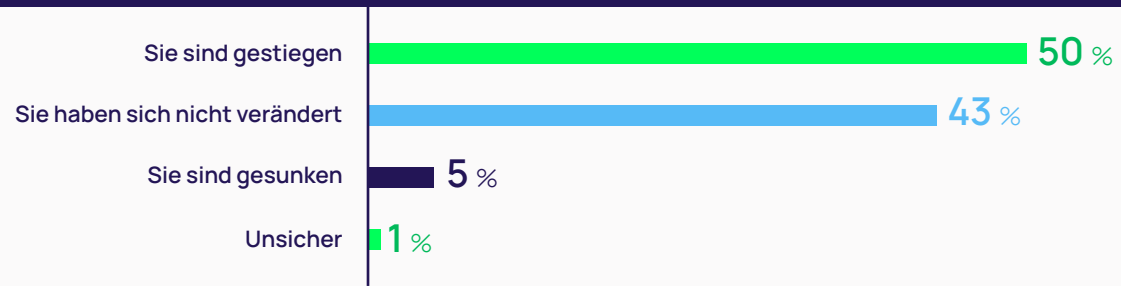
Ihre Sicherheitslage sollte nicht auf „Einstellen und dann vergessen“ basieren. Ihr Risiko ändert sich ständig, da Ihre IT-Umgebung immer komplexer wird und Mitarbeiter hinzukommen, ihre Rollen wechseln und das Unternehmen verlassen. Die Wahrheit ist, dass Unternehmen sich nicht immer an die Richtlinien halten, die sie einem Versicherungsanbieter in ihrem Antrag stolz mitteilen.

Wichtigste Erkenntnis 3

Obwohl die Gesamtkosten für Cyberversicherungen steigen, verringern neue Technologien wie KI die Beiträge.

Die Versicherungskosten steigen für viele Unternehmen stetig an.

Abbildung 8 | Wie, wenn überhaupt, haben sich Ihre Cyberversicherungskosten verändert, seit Sie die Versicherung beantragt oder zuletzt erneuert haben?



Obwohl mehr als die Hälfte einen Anstieg meldet, zeigt ein Vergleich mit dem Vorjahr, dass sich der Kostenanstieg verlangsamt. Im vergangenen Jahr gaben 79 % der Unternehmen an, dass die Versicherungskosten seit ihrem letzten Antrag oder ihrer letzten Erneuerung gestiegen sind.

Warum gibt es nur bei einigen einen Anstieg?

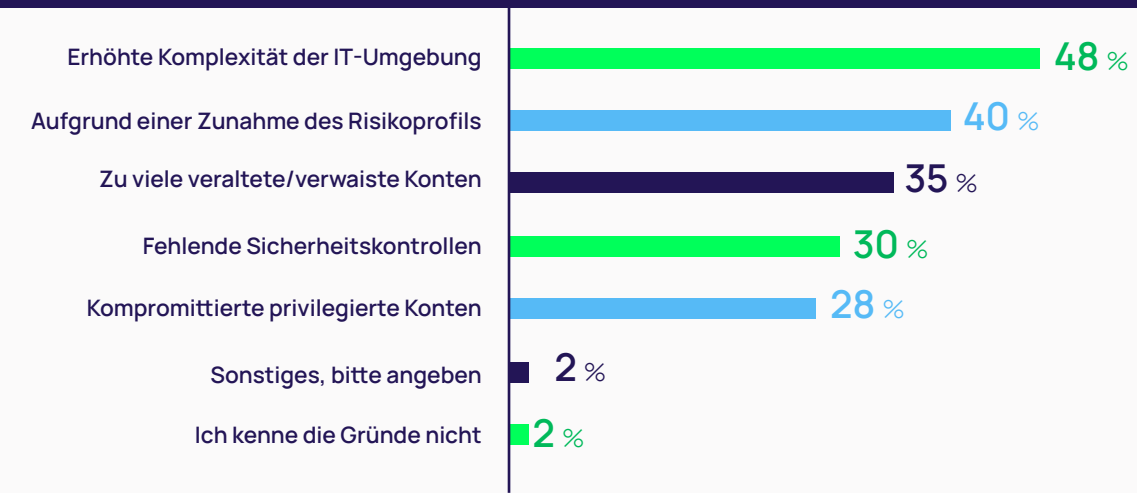
Bedenken Sie die Gesamtkosten der Ressourcen, die erforderlich sind, um Versicherungsbewertungen durchzuführen, Lücken zu schließen und den Nachweis einer effektiven Cybersicherheit in einer modernen, hybriden IT-Umgebung zu erbringen.

Die Befragten nennen die Komplexität der IT als einen treibenden Faktor für die steigenden Kosten. Je größer die Zahl der Identitäten, desto mehr Ressourcen werden für die Erfüllung dieser Aufgaben benötigt. Die Komplexität der IT-Umgebung erschwert die Bewertung der Sicherheit von Cyberversicherungen und unzusammenhängende Prüfungs- und Berichterstattungslösungen machen die Zusammenstellung der Einzelheiten und die Risikomessung komplex.

Steigende Kosten könnten dazu führen, dass Versicherungsnehmer aufgrund eines erhöhten Risikoprofils höhere Deckungssummen beantragen. Sie sind sich der geschäftlichen Auswirkungen bewusst, die sie im Falle eines Cyberangriffs zu tragen haben und wollen dieses Risiko übertragen.

Je nach IT-Komplexität und Risikoprofil können Versicherungsgesellschaften die Preise für alle Versicherungsnehmer anheben, um eine ausreichende Liquidität sicherzustellen, falls mehrere Schadensfälle gleichzeitig eintreten.

Abbildung 9 | Warum sind die Kosten gestiegen?



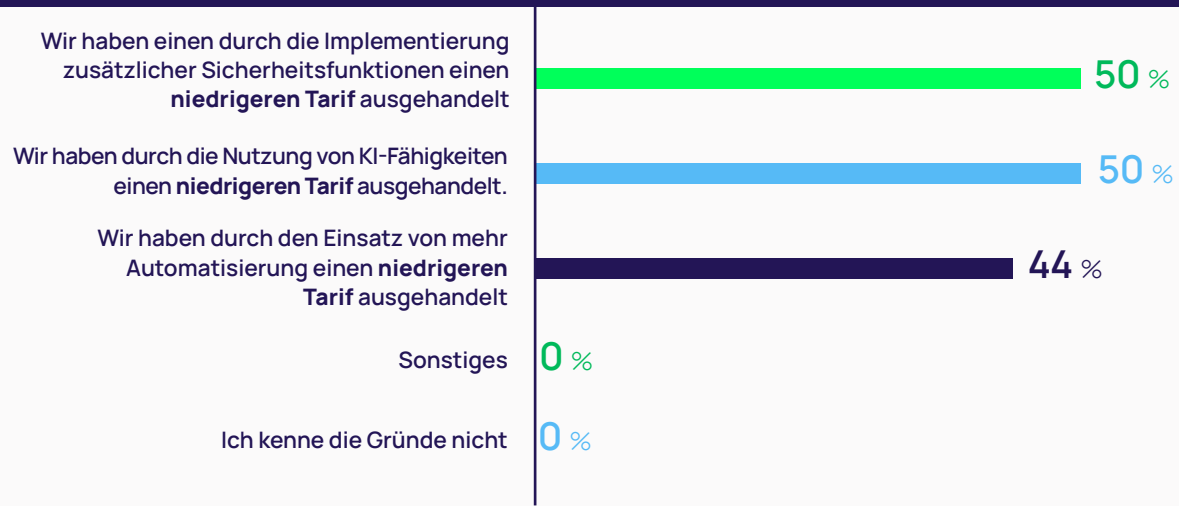
Cybersicherheitslösungen, die eine komplexe IT-Umgebung schnell und umfassend bewerten und risikobasierte Berichte liefern, die Sie mit Versicherungsanbietern teilen können, sind ein wirksames Mittel zur Senkung Ihrer Cyberversicherungskosten.

KI und Sicherheitskontrollen haben vorausschauenden Unternehmen geholfen, ihre Versicherungsbeiträge zu senken.

Nicht jedes Unternehmen erhält den gleichen Versicherungstarif. Ihr Tarif richtet sich danach, wie risikoreich die Versicherungsgesellschaft Sie einschätzt – Ihr Risikoprofil. Bei Cyberversicherungen wird Ihr Risiko durch Faktoren wie Ihren Technologie-Stack, Sicherheitskontrollen und Ihre Historie beeinflusst. Wenn Sie Transparenz und Kontrollen nachweisen können, die Sie zu einem geringeren Risiko machen, können Sie möglicherweise erfolgreich Ihre Tarife und damit Ihre Kosten senken.

Die Umfrageergebnisse zeigen, dass vorausschauende Unternehmen die Vorteile von KI nutzen, um niedrigere Tarife und damit Kosten zu vereinbaren. Die Mehrheit muss sich jedoch noch darauf konzentrieren, die Grundlagen einer starken Identitätssicherheit einzuführen und umzusetzen.

Abbildung 10 | Warum sind Ihre Versicherungskosten gesunken?

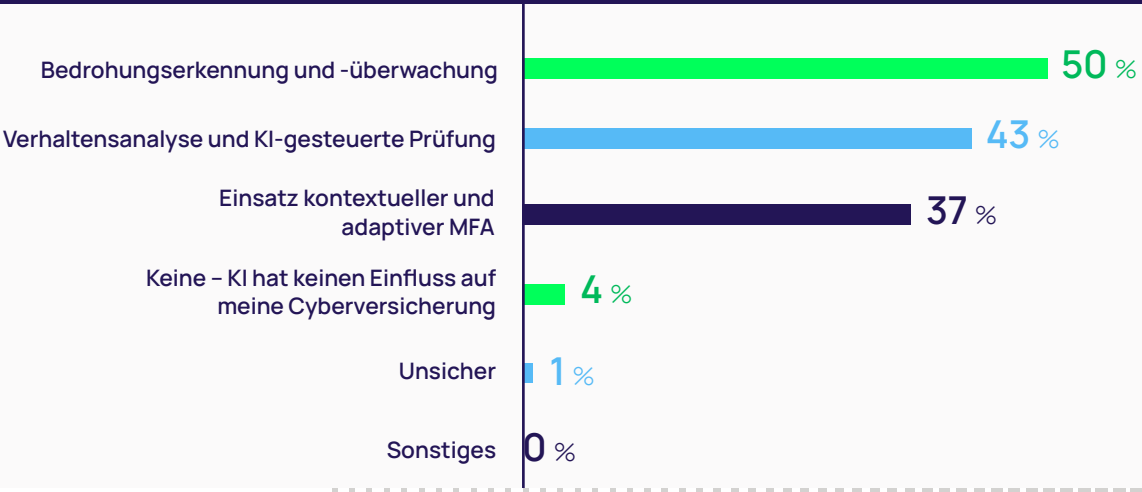


Künstliche Intelligenz, insbesondere für die Erkennung und Überwachung von Bedrohungen, ist ein wirksames Mittel zur Senkung der Cyberversicherungsbeiträge

Die Beiträge, d. h. der Betrag, den ein Unternehmen für die Fortführung eines Versicherungsvertrags zahlt, hängen unter anderem von der Art der Versicherung, den Versicherungsgrenzen und dem Selbstbehalt ab. Je mehr Vertrauen Sie in Ihre Sicherheitsvorkehrungen und -kontrollen haben, desto besser können Sie die für Sie richtige Versicherung auswählen und niedrigere Beiträge aushandeln.

Unternehmen setzen künstliche Intelligenz (KI) ein, um sicherzustellen, dass Cybersicherheitslösungen und -richtlinien wie erwartet funktionieren und um laufende Vorfälle einzudämmen, damit sie die Verweildauer von Angreifern und den Aktionsradius von Angriffen verringern können, was wiederum Ihr Risikoprofil senken kann.

Abbildung 11 | Welche KI-Funktionen setzen Sie gegebenenfalls ein, um Ihre Cyberversicherungsbeiträge zu senken?



Fazit

Eine Versicherung ist zwar ein wichtiges Instrument für die Cyberresilienz, aber Sie werden nie in der Lage sein, alle Risiken an diese zu übertragen. Die Cyberversicherung muss mit robusten, angemessenen und vertretbaren Cybersicherheitskontrollen und -prozessen einhergehen.

Insbesondere erwarten die Versicherungsanbieter Identitätssicherheitsmaßnahmen und wirksame Lösungen, bevor sie eine Police genehmigen. Sie müssen Nachweise für funktionierende Identitätssicherheitskontrollen vorlegen und sicherstellen, dass Sie diese Kontrollen aufrechterhalten, wenn sich Ihre Angriffsfläche ändert und Ihr Risikoprofil zunimmt.

KI hilft Unternehmen dabei, das Wissen von Fachleuten zu erfassen und als „SOC-Assistent" identitätsbezogene Bedrohungen schneller zu erkennen, was letztlich die Verweildauer verkürzt, den Aktionsradius eines Angriffs begrenzt und das Risiko verringert. Die Ergebnisse dieser Umfrage zeigen, dass KI bei der Aushandlung von Verträgen zwischen Unternehmen und Versicherungsträgern noch größere Vorteile bringen wird.

Im Rahmen ihrer Risikobewertungen wollen die Versicherer wissen, wie Sie KI in Ihre Bemühungen zur digitalen Transformation einbinden, einschließlich Produktentwicklung, Codierung, Entwicklung, QA-Tests usw. Sie sollten auch Fragen erwarten, mit denen geprüft wird, wie Ihr Sicherheitsteam KI für Elemente wie Identitätsmanagement, Autorisierung, Erkennung und Reaktion einsetzt. Alle KI-basierten Kontrollen müssen leicht erklärbar sein, damit Ihr Team, die Auditoren und die Versicherungsanbieter wissen, wie sie zur Risikominderung beitragen.

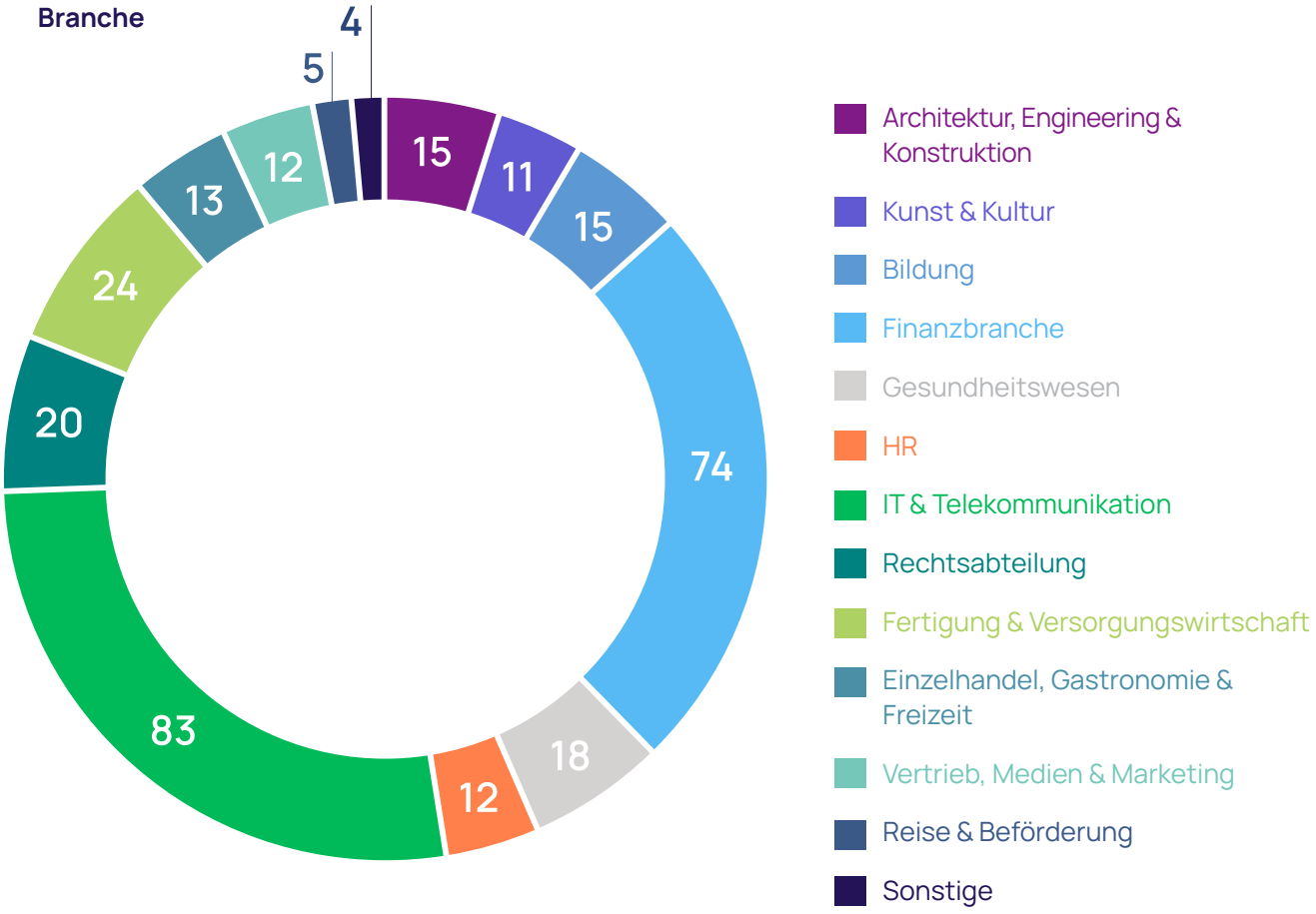
Die meisten befragten US-Unternehmen mussten in Identitätssicherheitslösungen investieren, bevor sie eine Police abschließen konnten.

Untersuchungsmethode

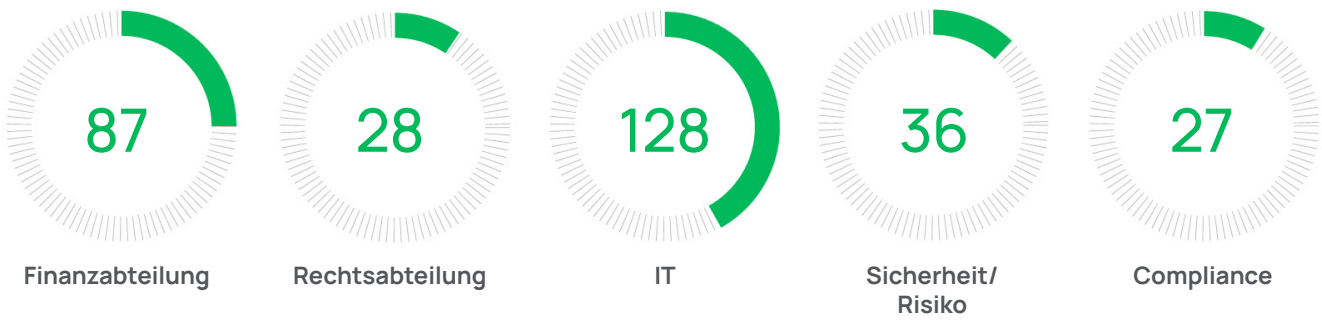
Diese Online-Umfrage wurde im Auftrag von Delinea von Censuswide durchgeführt, das im Juni 2024 306 Führungskräfte befragte, die am Antrags- oder Erneuerungsprozess der Cyberversicherung ihres Unternehmens beteiligt sind. Allen Befragten wurden dieselben Fragen vorgelegt und die Antwortmöglichkeiten wurden randomisiert. Die Ergebnisse wurden nicht gewichtet.

Auflistung der 306 Befragten nach Anzahl

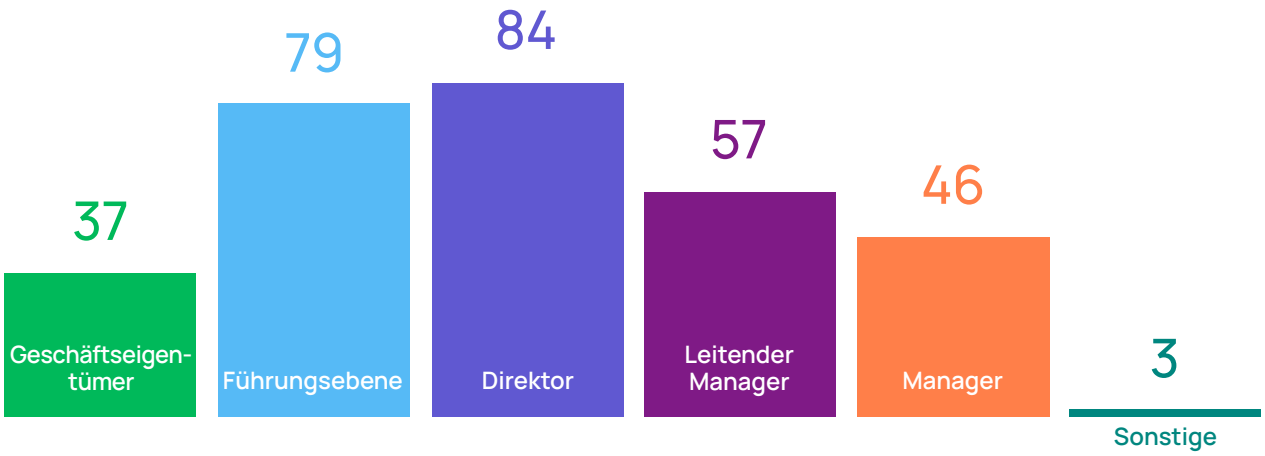
Branche



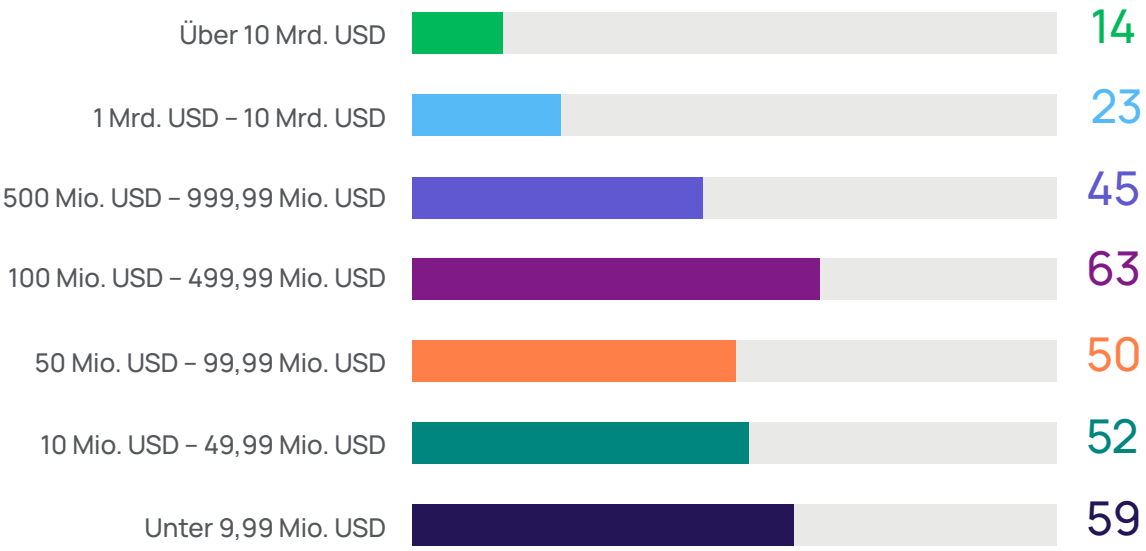
Rollen



Titel



Unternehmensgröße



Zugehörige Ressourcen

WEBINAR

Die Zukunft der Cyberversicherung: Steuerung der Auswirkungen von KI auf Versicherungsnehmer

Hören Sie sich an, was Cyberssicherheits- und Versicherungsexperten zur Prüfung der Vertragsbedingungen sagen, um sicherzustellen, dass Sie Ihren Versicherungsschutz und die Ausschlüsse verstehen und wissen, was Sie im Falle eines Vorfalls von Ihrem Versicherungsanbieter erwarten können.

Jetzt ansehen

WHITEPAPER

Einblicke in die erweiterten Anforderungen an die Cyberversicherung

Dieser Bericht gibt einen Überblick über die Fragebögen führender Versicherungsunternehmen und hebt die häufigsten Fragen hervor. Insbesondere werden die immer strengeren Anforderungen der Versicherer an die Identitätssicherheit untersucht, einschließlich der Multi-Faktor-Authentifizierung (MFA), der Passwortverwaltung, der Zugriffskontrolle, der Berechtigungserhöhung, dem Sitzungsmanagement, Least Privilege und der Zero-Trust-Richtlinien.

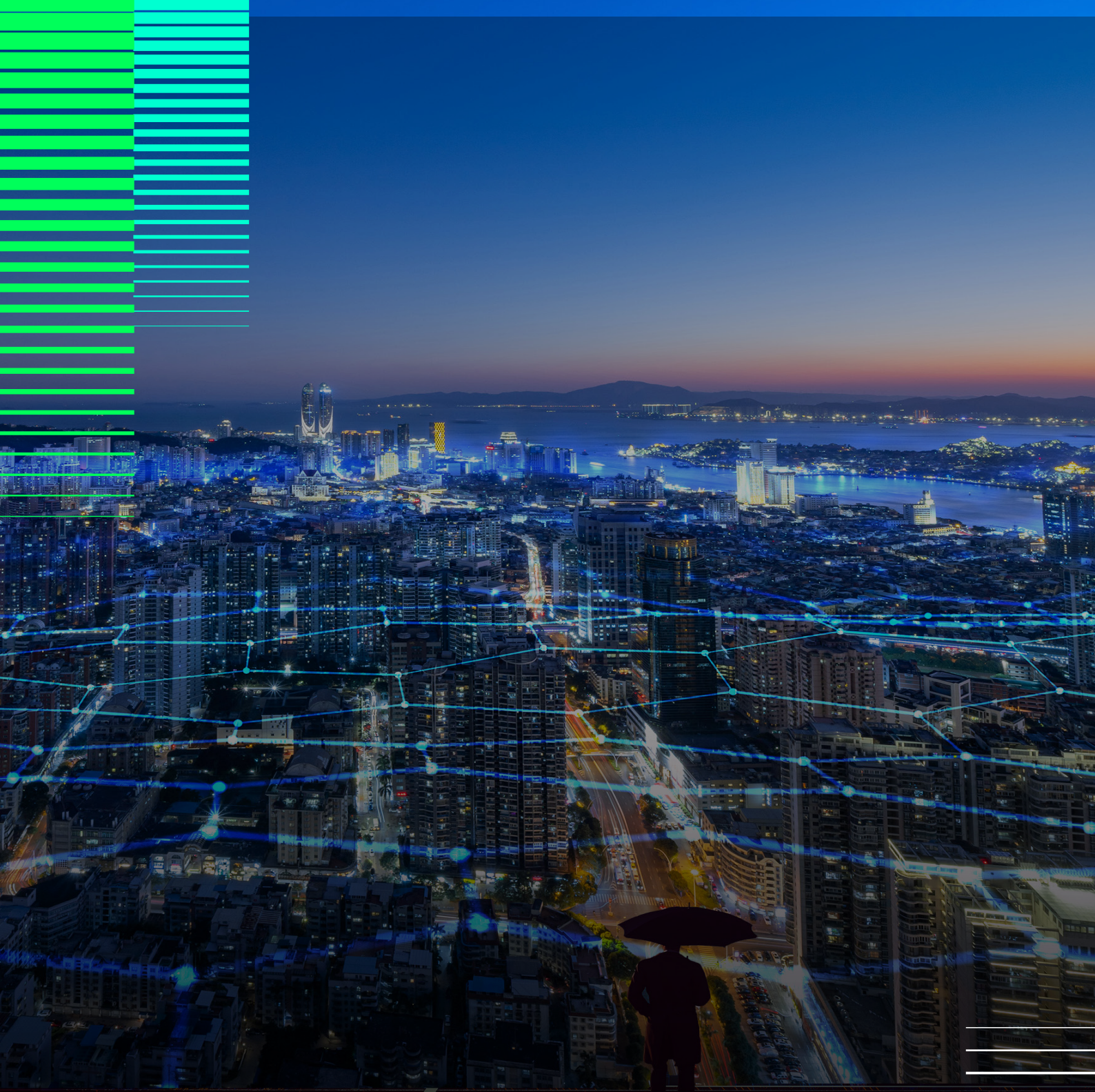
Jetzt herunterladen

PODCAST

Cyberversicherungstrends für das Risikomanagement mit Joe Carson von Delinea und Dara Gibson von Optiv

Erfahren Sie, wie Sie mit Ihrem Vorstand Gespräche über Cyberversicherungen führen können.

Jetzt anhören



Delinea

Securing identities at every interaction

Delinea ist ein Vorreiter in der Sicherung von Identitäten durch zentralisierte Autorisierung. Dabei werden dank der nahtlosen Verwaltung der Interaktionen innerhalb des gesamten modernen Unternehmens die Organisationen sicherer. Mit Delinea können Organisationen über den gesamten Lebenszyklus der Identität hinweg diese für Cloud- und traditionelle Infrastruktur, Daten und SaaS-Anwendungen mit Kontext und Intelligenz ausstatten, um auf diese Weise Bedrohungen in Zusammenhang mit Identitäten auszuräumen. Dank der intelligenten Autorisierung bietet Ihnen Delinea als einzige Plattform die Möglichkeit, alle Identitäten aufzudecken, angemessene Zugriffsebenen zuzuweisen, Unregelmäßigkeiten zu erkennen und unverzüglich in Echtzeit auf Bedrohungen in Bezug auf Identitäten zu reagieren. Delinea verkürzt die Einarbeitungszeit Ihrer Teams von Monaten auf Wochen und fördert die Produktivität mit - im Vergleich zu direkten Mitbewerbern - 90 % weniger Verwaltungsressourcen. Mit einer Verfügbarkeit von 99,99 % ist die Delinea Plattform eine der zuverlässigsten Lösungen für Identitätssicherheit auf dem Markt. Mehr über Delinea erfahren Sie auf **delinea.com**, **LinkedIn**, **X** und **YouTube**.