Allianz

Khozinul / Adobe Stock

ALLIANZ COMMERCIAL

Cybersicherheit und -resilienz 2025

Schaden- und Risikomanagement-Trends

commercial.allianz.com

Melinda Nagy / Adobe Stock

Contents

Zusammenfassung

Die Cyberrisiko- und Cyberversicherungslandschaft im Jahr 2025 ist geprägt von einem komplexen und sich wandelnden Bedrohungsumfeld. Versicherte Unternehmen, insbesondere größere Firmen, sind immer besser gegen Attacken gewappnet, sehen sich aber mit wachsenden Herausforderungen durch Angriffs- und „Nicht-Angriffs"-Ereignisse konfrontiert. Wir sehen ermutigende Anzeichen dafür, dass sich die Stärkung der Cybersicherheit und Abwehrbereitschaft auszuzahlen beginnt. Dadurch konnten auch die Auswirkungen großer Cyber-Versicherungsschäden im bisherigen Jahresverlauf 2025 gemindert werden. Durch die Abhängigkeit von digitalen Lieferketten, die Auswirkungen weitreichenderer Datenschutzbestimmungen und immer ausgeklügeltere Social-Engineering-Angriffe auf Mitarbeitende steigt jedoch das potenzielle Ausmaß der Schäden.

Schadentrends

Eine Analyse von Cyber-Versicherungsschäden durch **Allianz Commercial** zeigt, dass sich die Zahl der Schadensfälle im ersten Halbjahr 2025 auf dem Niveau des ersten Halbjahres 2024 bewegte (rund 300 Schadensfälle), nachdem sie im Jahr 2023 im Vergleich zum Vorjahr deutlich gestiegen war. In den ersten sechs Monaten des Jahres 2025 hat sich das Gesamtvolumen der Cyber-Versicherungsschäden mehr als halbiert. Die Anzahl der großen Schadensfälle (> 1 Million Euro) ist um rund 30 Prozent gesunken. Die Risikolandschaft wird jedoch vielfältiger und umfasst nicht mehr nur direkte Cyberangriffe. Der diesjährige Bericht identifiziert Rückwirkungsschäden, technische Fehler und Rechtsstreitigkeiten im Zusammenhang mit Datenschutzverletzungen als wesentliche Schadenursachen: Vorfälle wie die unrechtmäßige Erhebung oder Verarbeitung von Daten und IT-Ausfälle waren 2024 für 28 Prozent der Kosten großer Schadensfälle verantwortlich – so viel wie nie zuvor.

Ransomware-Angriffe verlagern sich auf mittelgroße und weniger gut geschützte Unternehmen

Gemessen an den Fallzahlen und Kosten bleibt Ransomware der Haupttreiber von Cyber-Versicherungsschäden: Im ersten Halbjahr 2025 waren Ransomware-Attacken für rund 60 Prozent des Umfangs großen Schadensfälle (>1 Million Euro) verantwortlich. Schlagzeilenträchtige Angriffe in vielen Branchen verdeutlichen die anhaltende Bedrohungslage, obwohl sich die stärkere Zusammenarbeit der internationalen Strafverfolgungsbehörden und Maßnahmen großer Unternehmen zur Verbesserung ihrer Cyberresilienz sichtlich auszahlen. Die Zahl der aktiven Ransomware-Gruppen wächst jedoch weiter, allein im ersten Halbjahr 2024 um 50 Prozent. Außerdem wenden diese Akteure immer ausgefeiltere Taktiken an. Mithilfe künstlicher Intelligenz (KI) nutzen sie Schwachstellen in der Sicherheitskette – insbesondere Mitarbeitende und Lieferanten – aus, um sich Zugang zu den Systemen von Unternehmen zu verschaffen.

Zugleich verlagern die Angreifer ihren Fokus: Anstelle gut geschützter Großunternehmen – insbesondere in den USA und Europa, wo die Hürden für einen erfolgreichen Angriff mittlerweile viel höher sind – nehmen sie zunehmend mittlere und kleine Firmen mit weniger ausgereiften Abwehrsystemen sowie Unternehmen in Regionen wie Asien oder Lateinamerika ins Visier. Verizon zufolge war Ransomware zuletzt bei 88 Prozent der von kleinen und mittleren Unternehmen verzeichneten Datensicherheitsverletzungen im Spiel, bei größeren Unternehmen dagegen nur in 39 Prozent der Fälle. Auch im jüngste **Allianz Risk Barometer** bezeichneten kleinere Unternehmen Cybervorfälle als ihr größtes Geschäftsrisiko.

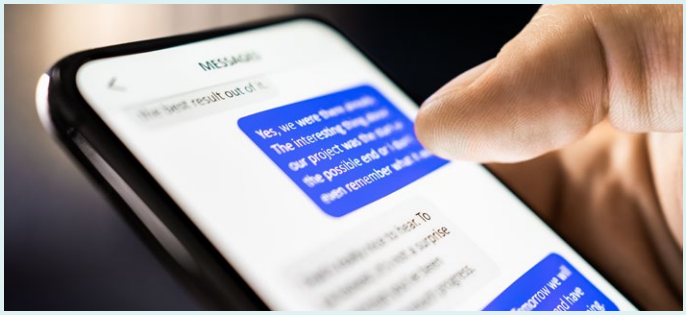
Artem / Adobe Stock

Datenexfiltration als wesentliche Schadenursache

Mit der Verbesserung der Reaktionsfähigkeit großer Unternehmen ist seit einigen Jahren ein Trend von Ransomware-Angriffen mit einfachen Lösegeldforderungen hin zu doppelten Erpressungsangriffen einschließlich Datenexfiltration zu beobachten. Im ersten Halbjahr 2025 spielte Datendiebstahl bei 40 Prozent der großen Cyber-Versicherungsschäden (>1 Million Euro) eine Rolle –ein

deutlicher Sprung gegenüber 25 Prozent im Gesamtjahr 2024. Die von derartigen Angriffen verursachten Schäden waren doppelt so hoch wie die von Angriffen ohne Datenexfiltration.

Datendiebstähle sind für Angreifer einfacher und schneller zu bewerkstelligen als Systemverschlüsselungen und erhöhen die Erfolgswahrscheinlichkeit ihrer Lösegeldforderungen. Im Jahr 2024 erreichten die durchschnittlichen Kosten eines Datenlecks weltweit einen neuen Rekordwert (fast fünf Millionen US-Dollar), was auf Faktoren wie den Einfluss strengerer Datenschutzgesetze zurückzuführen war. Unterdessen ist der Anteil der Angriffe, bei denen es zu Systemverschlüsselungen kam, auf den niedrigsten Stand seit sechs Jahren gefallen.



terovesalainen / Adobe Stock

Angriffe mit ausgefeilten Social-Engineering-Taktiken und Zugangsdaten auf dem Vormarsch

Die jüngsten Cyberangriffe weisen Gemeinsamkeiten auf, wie die Verwendung ausgefeilter Social-Engineering-Methoden und kompromittierter Anmeldedaten, um Zugang zu Netzwerken zu erhalten. Beispielsweise geben sich Angreifer als Mitarbeitende aus, denen der Systemzugriff verweigert wurde. Viele Angreifer versuchen auch, über Lieferanten oder IT-Lieferketten Zugang zu sensiblen Informationen zu erhalten. Verizon zufolge spielte der Faktor Mensch bei rund 60 Prozent der Datensicherheitsverletzungen im Jahr 2024 eine Rolle. Der Anteil der Sicherheitsverletzungen, an denen Dritte beteiligt waren, verdoppelte sich gegenüber dem vorherigen Berichtszeitraum auf 30 Prozent. Angreifer nutzen immer häufiger kompromittierte Zugangsdaten, die sie sich durch Phishing-Attacken aneignen oder über das Darknet beschaffen, von sogenannten Access Brokern – spezialisierten Agenten, von denen es immer mehr gibt.

Scattered Spider, eine Hackergruppe, die hinter den jüngsten Angriffen auf Casinos, Einzelhändler, Fluggesellschaften und Versicherungen steckt, nutzt kompromittierte Zugangsdaten sowie Social-Engineering- und Phishing-Taktiken, um sich schnell Zugang zu den Systemen von Unternehmen zu verschaffen. Allein im ersten Halbjahr 2025 wurden der Gruppe mehr als zehn Angriffe zugeschrieben. Mittlerweile gibt es mehr Angriffe mit gestohlenen Anmeldedaten als mit Schadsoftware. Nach Angaben des Cybersecurity-Unternehmens CrowdStrike erfolgten rund 80 Prozent der Angriffe im zurückliegenden Jahr malwarelos – verglichen mit 40 Prozent im Jahr 2019. Diese Zahlen spiegeln auch den zunehmenden Einsatz generativer KI für ausgeklügeltere Social-Engineering-Strategien wie personalisierte Phishing-E-Mails oder -Anrufe (Vishing) wider.

Am meisten betroffen: produzierende Unternehmen, Dienstleister und Einzelhändler

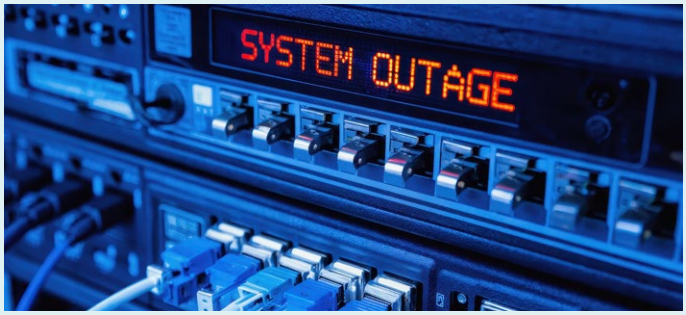
Im ersten Halbjahr 2025 führten Einzelhändler die Liste der Top-Angriffsziele von Cyberkriminellen an. Wie eine Analyse der Auswirkungen großer Cyber-Schadensfälle (>1 Million Euro) seit 2020 zeigt, ist der Handel zudem der am drittstärksten von Cybervorfällen betroffene Sektor nach dem verarbeitenden Gewerbe und den Dienstleistungen: Die Kosten der analysierten Großschäden durch Cybervorfälle entfielen zu 33 Prozent auf produzierende Unternehmen, zu 18 Prozent auf Dienstleister/ Beratungsunternehmen und zu 9 Prozent auf Einzelhändler.

Viele Einzelhändler haben hohe Umsätze, verarbeiten große Mengen an persönlichen Daten und sind anfällig für Betriebsstörungen – alles Faktoren, die Erpresser als Druckmittel nutzen können. Außerdem haben sie in der Regel eine große Anzahl von Beschäftigten, Lieferanten und IT-Systemen, was eine große Angriffsfläche schafft. Gleichzeitig sind ihre Cybersicherheitssysteme zumeist weniger ausgereift als in Branchen wie dem Bankwesen.

Risiken aufgrund der Abhängigkeit von Lieferketten

Schadensfälle im Zusammenhang mit der zunehmenden Abhängigkeit von IT-Lieferketten sind ein bedeutender neuer Trend. Wie Untersuchungen von **Allianz Commercial** zeigen, waren Rückwirkungsschäden in Lieferketten im ersten Halbjahr 2025 für 15 Prozent der Kosten großer Cyber-Versicherungsschäden (>1 Million Euro) verantwortlich – verglichen mit 6 Prozent im Jahr 2024. Derartige Schäden können durch Angriffe oder technische Fehler verursacht werden, die zu Unterbrechungen kritischer Dienste wie Software oder Cloud-Services führen. CrowdStrike zufolge nahm die Zahl der Cloud-Angriffe im ersten Halbjahr 2025 im Vergleich zum Gesamtjahr 2024 um 136 Prozent zu. Störungen in der IT-Lieferkette können Auswirkungen auf physische Produkte haben, wenn der Lieferant eines Versicherungsnehmers nicht in der Lage ist, die für die Produktion erforderlichen Waren zu liefern, und können auch Datensicherheitsverletzungen zur Folge haben.

Viele Unternehmen haben ihre Cybersicherheitsinfrastruktur gestärkt. Das Risiko von Datenschutzverletzungen bei ihren IT-Dienstleistern und Partnern ist jedoch schwieriger zu kontrollieren. Umso wichtiger ist ein gutes Management von Dienstleistern und Lieferanten – nicht nur durch eine entsprechende Vertragsgestaltung, sondern auch durch Zugangskontrollen, Monitoring und Lieferanten-Audits.



aznan / Adobe Stock

‚Nicht-Angriffs'-Vorfälle führen zu einem breiteren Spektrum an potenziellen Schadensereignissen

Schäden durch Cyberattacken sind weiterhin die größte Ursache von Cyber-Versicherungsschäden. Der Anteil der Versicherungsansprüche, die auf technische Fehler und Datenschutzverstöße zurückzuführen sind, ist jedoch gestiegen: Im Jahr 2024 belief sich dieser auf rekordhohe 28 Prozent der analysierten Großschäden (>1 Million Euro).

Mit einem Anteil von rund 10 Prozent am Gesamtvolumen tauchten Betriebsunterbrechungen aufgrund technischer Fehler 2024 erstmals in der Großschäden-Statistik von **Allianz Commercial** auf. Mit dafür verantwortlich war einer der größten IT-Ausfälle aller Zeiten bei CrowdStrike. Derartige Ausfälle können durch technische Fehler oder menschliches Versagen verursacht werden.

rookielion / Adobe Stock

Datenschutzgesetze und Rechtsprechung weiter in der Entwicklung

Datensicherheitsverletzungen und Datenschutzklagen, zum Beispiel im Zusammenhang mit der unrechtmäßigen Erhebung und Verarbeitung personenbezogener Daten, haben in den vergangenen Jahren an Bedeutung gewonnen. Den Analysen von Allianz Commercial zufolge betrug ihr Anteil am Gesamtwert großer Schadensfälle (>1 Million Euro) im Jahr 2024 rekordhohe 18 Prozent – dreimal so viel wie drei Jahre zuvor.

Unterdessen machten IT-/Media-Vermögenshaftpflichtschäden im ersten Halbjahr 2025 ein Viertel des Volumens großer Cyber-Schadensfälle aus, verglichen mit 21 Prozent im Jahr 2024. Viele dieser Versicherungsansprüche stehen im Zusammenhang mit rechtlichen Schritten gegen Technologieunternehmen aufgrund von Servicedefiziten, technischen Fehlern und angeblichen Verstößen gegen Datenschutzbestimmungen und Geheimhaltungspflichten. Sie können aber auch auf Angriffe zurückzuführen sein.

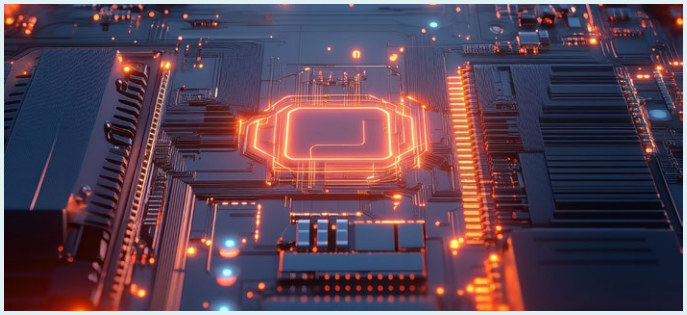
Die Zahl der Sammelklagen wegen Verstößen gegen Datenschutzgesetze hat in den letzten Jahren erheblich zugenommen. Mit rund 1.500 Datenschutzklagen allein in den USA erreichte die Zahl der Rechtsstreitigkeiten im Jahr 2024 ein beispielloses Ausmaß. Die Einhaltung vieler unterschiedlicher, sich ständig weiter entwickelnder Regelwerke stellt Unternehmen vor große Herausforderungen, insbesondere angesichts der technologischen Fortschritte in Bereichen wie KI und Biometrie. KI-Systeme können zu Datensicherheitsverletzungen durch eine unrechtmäßige Erhebung/Verarbeitung von Daten führen.

kaliel / Adobe Stock

Erkennung, Reaktion und Schulung zur Senkung der Kosten von Schadensereignissen

Die jüngsten Cyberangriffe haben verdeutlicht, wie wichtig eine effektive Cyberhygiene, Früherkennung und Reaktionsfähigkeit sind und wie sie helfen können, die potenziellen Kosten von Schadensereignissen zu minimieren. Analysen zeigen, dass die Entscheidungen der versicherten Unternehmen bei mehr als 80 Prozent der großen Schadensfälle erheblichen Einfluss auf die Schadenshöhe haben und dass viele Vorfälle durch grundlegende Sicherheitsmaßnahmen wie Patching, Segmentierung, Backups und Multi-Faktor-Authentifizierung (MFA) verhindert werden könnten. Eine effektive Bedrohungserkennung und Cyberreaktion können die Kosten von Schadensfällen um den Faktor 1.000 reduzieren. Ihre Bedeutung zeigt sich auch im Wachstum des globalen Marktes für MDR-Dienstleistungen (Managed Detection and Response), der sich in den nächsten zehn Jahren voraussichtlich vervierfachen wird.

Seventyfour / Adobe Stock



narin_nonthamand / Adobe Stock

Wachsende Lücke: Unternehmen mit Cyberversicherungen werden resilienter

Der stabile Trend bei der Gesamtanzahl der Cyber-Versicherungsschäden seit Jahresanfang 2025 steht im Gegensatz zur allgemeinen Entwicklung der Bedrohungslandschaft. So wurden dem Internet Crime Complaint Center des FBI (IC3) im vergangenen Jahr mehr finanzielle Verluste durch Internetkriminalität gemeldet als je zuvor: insgesamt 16,6 Milliarden US-Dollar.

Was die Cyberresilienz angeht, wird die Kluft zwischen versicherten und nicht versicherten Unternehmen größer. In Deutschland zum Beispiel sind die Cyber-Versicherungsansprüche innerhalb von vier Jahren um lediglich rund 70 Prozent gestiegen, während die Cyberkriminalität laut FBI im gleichen Zeitraum um insgesamt 250 Prozent zugenommen hat.

Diese Resilienzlücke spiegelt das gestiegene Risikobewusstsein der Cyberversicherten sowie ihre Maßnahmen zur Minderung von Cyberrisiken wider. Viele dieser Maßnahmen sind eine Voraussetzung für die Gewährung von Deckungsschutz. Die größere Cyberresilienz der versicherten Unternehmen verdeutlicht aber auch die Effektivität der von den Versicherern bereitgestellten Beratungs- und Support-Dienstleistungen zur Risikominimierung und Unterstützung im Ernstfall. Regelmäßige Tabletop Exercises und Krisentrainings helfen, die Cyberabwehr zu stärken, und können so Betriebsunterbrechungen minimieren, die für mehr als 50 Prozent der Kosten von Cyber-Versicherungsschäden verantwortlich sind. Betriebsunterbrechungsschäden stehen im direkten Zusammenhang mit der Früherkennung, Eindämmung und Reaktion auf Vorfälle, und eine gute Geschäftskontinuitätsplanung kann die Kosten von Cybervorfällen erheblich senken. Dagegen können eine schlechte Kommunikation, mangelnde Koordination und Unentschlossenheit die Auswirkungen eines Vorfalls verlängern.

Transformatives Potenzial der KI-gestützten Bedrohungserkennung

KI ist ein heißes Thema für Versicherungsnehmer, die in einem sich wandelnden regulatorischen Umfeld unter Wettbewerbsdruck stehen, KI-Tools einzuführen. Angreifer nutzen KI, um Ransomware-Attacken zu automatisieren und zu skalieren, ausgeklügelte Schadsoftware zu entwickeln und überzeugende Phishing-Kampagnen zu konzipieren. Gleichzeitig hebt KI die Cybersicherheit auf eine neue Ebene, indem sie eine schnellere und automatisierte Erkennung von und Reaktion auf Bedrohungen ermöglicht und die Cyberresilienz von Unternehmen stärkt. IBM zufolge waren die Kosten durch Datensicherheitsverletzungen bei Unternehmen, die KI-basierte Sicherheits- und Automatisierungslösungen nutzen, zuletzt um durchschnittlich 2,2 Millionen US-Dollar niedriger als bei Unternehmen, die keine derartigen Lösungen einsetzen.

Regulierung erhöht Anforderungen an Cyberresilienz

Neue Regelwerke wie die EU-Verordnung über die digitale operationale Resilienz im Finanzsektor (DORA) und die EU-Richtlinie zur Sicherung von Netzwerk- und Informationssystemen (NIS2) sollen die Cybersicherheitsstandards in kritischen Sektoren einschließlich der zugehörigen Lieferketten anheben. Sie enthalten Vorgaben für ein verbessertes Risikomanagement, Vorfallmeldungen und Resilienztests. Damit werden sie vor allem mittelgroßen Unternehmen mit ihrer derzeit noch unterentwickelten Cybersicherheitsinfrastruktur zugutekommen.

Ausblick für den Versicherungsmarkt

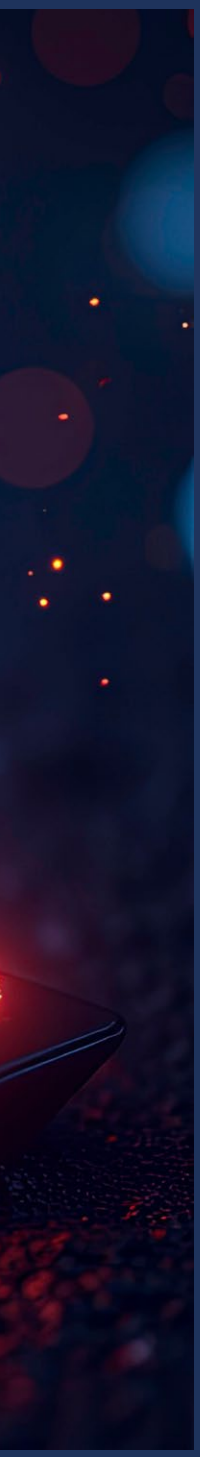
Cyberversicherte haben bereits gute Fortschritte bei der Minderung großer Cyberschäden gemacht, indem sie ihre Cybersicherheit und ihre Abwehrbereitschaft verbessert haben. Angesichts der sich wandelnden Bedrohungslandschaft und des anhaltenden Regulierungsdrucks müssen sie jedoch wachsam bleiben und weiterhin in ihre Cyberresilienz investieren. Cyberversicherungen bleiben ein wichtiger Aspekt des Managements dieser Risiken. Neben finanziellem Schutz bieten sie Unternehmen Zugang zu wichtiger Expertise in Bezug auf die Stärkung ihrer Cyberresilienz. Angetrieben durch die fortschreitende Digitalisierung und das zunehmende Risikobewusstsein der Unternehmen wird der globale Versicherungsmarkt bis zum Ende des Jahrzehnts voraussichtlich auf fast 30 Milliarden US-Dollar anwachsen – mehr als das Doppelte des derzeitigen Marktvolumens. Cyberversicherungen sind zwar noch relativ wenig verbreitet, aber die Nachfrage wächst, insbesondere unter mittelständischen Unternehmen und in Regionen mit einer traditionell geringen Verbreitung derartiger Policen.

Schadentrends

Spirit / Adobe Stock

SCHADENTRENDS

Cyberversicherte gewinnen die Kontrolle zurück und sind besser für Angriffe gewappnet, stehen aber weiter vor Herausforderungen



Wir sehen ermutigende Anzeichen dafür, dass sich die Maßnahmen versicherter Unternehmen zur Stärkung ihrer Cybersicherheit und Abwehrbereitschaft auszuzahlen beginnen. Diese Maßnahmen haben auch dazu beigetragen, die Auswirkungen großer Cyber-Versicherungsschäden im bisherigen Jahresverlauf 2025 zu mindern.

Eine Analyse der bei der Allianz im Zusammenhang mit Cyberversicherungen, Vermögensschadenversicherungen für Technologieunternehmen und Medienhaftpflichtversicherungen eingegangenen Schadensmeldungen zeigt, dass sich die Zahl der Schadensfälle in den ersten sechs Monaten des Jahres 2025 auf dem Niveau des ersten Halbjahres 2024 bewegte (mit rund 300 Fällen), nachdem sie 2023 im Vergleich zum Vorjahr deutlich gestiegen war. Im ersten Halbjahr 2025 ist das Gesamtvolumen der Cyber-Versicherungsschäden um mehr als 50 Prozent gesunken. Die Anzahl der großen Cyber-Schadensfälle (>1 Million Euro) ist um rund 30 Prozent zurückgegangen.

„Der positive Trend, den wir im Jahr 2025 insbesondere bei großen Schadensfällen beobachten, lässt insbesondere auf die Investitionen der Versicherungsnehmer in Cybersicherheit zurückführen. Vor allem die Verbesserungen in der Erkennung und Reaktion auf Angriffe trägt zu niedrigeren Schadenvolumen bei“, sagt **Michael Daum, Global Head of Cyber Claims bei Allianz Commercial.**

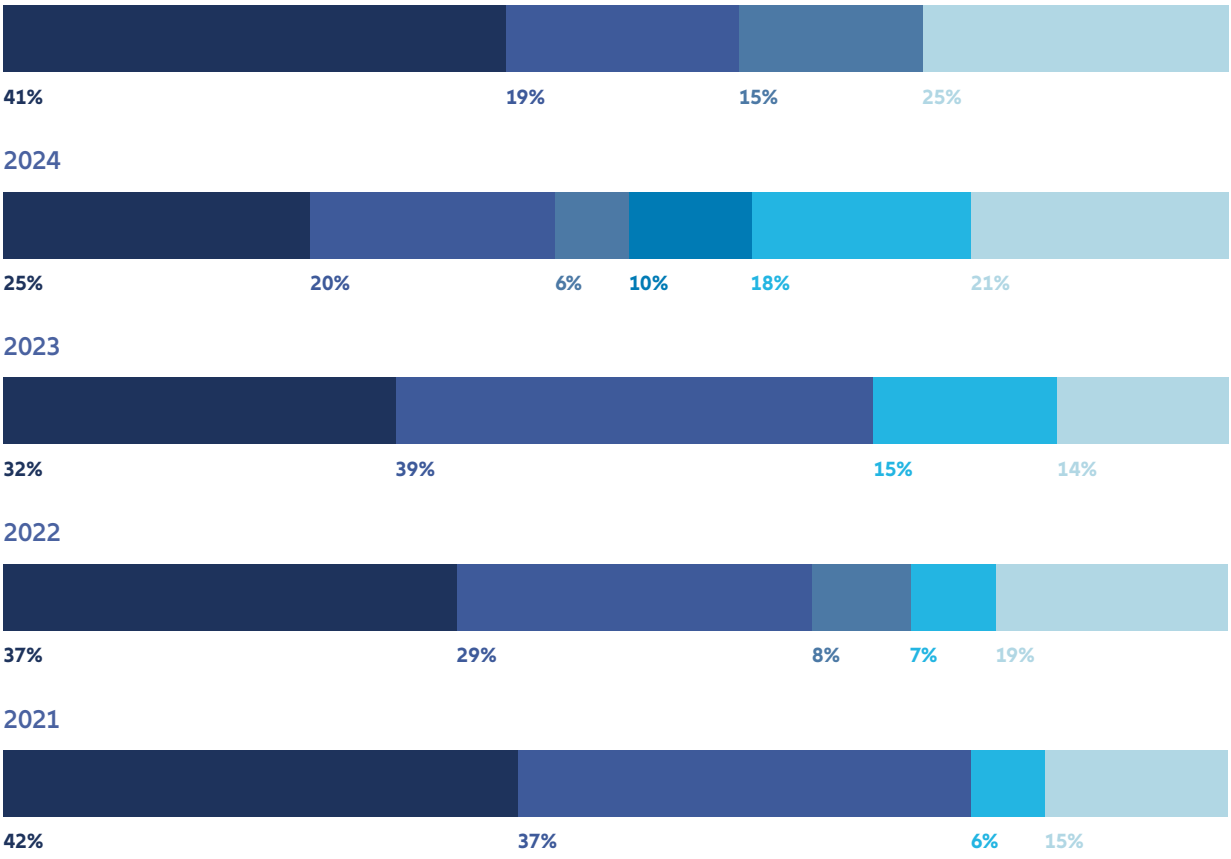
„Dieses Jahr gab es mehrere Ransomware-Attacken, die für Schlagzeilen sorgten. Dennoch sind die durch solche Angriffe verursachten Versicherungsschäden im bisherigen Verlauf des Jahres 2025 rückläufig. Die verbesserten Erkennungs- und Abwehrmechanismen der Versicherungsnehmer tragen dazu bei, Angriffe frühzeitig zu stoppen. Denn je weiter ein Angreifer in ein System eindringt und je länger er sich darin aufhält, desto exponentiell größer werden die Auswirkungen. Die Kosten eines Ransomware-Angriffs, bei dem Daten gestohlen und Systeme verschlüsselt werden, können leicht um Faktor 1000 höher sein als bei einem Vorfall, der frühzeitig erkannt und eingedämmt wird.“

Gleichzeitig führt eine vielfältigere Risikolandschaft auch zu einem breiteren Spektrum an potenziellen Schadensereignissen für Unternehmen. So waren Vorfälle, die nicht in Verbindung mit Cyberangriffen standen, im Jahr 2024 für 28 Prozent der Kosten von großen Schadensfällen verantwortlich – ein neuer Rekord. Beispiele für derartige Vorfälle sind die unrechtmäßige Erhebung und Verarbeitung von Daten oder technische Fehler. Ransomware ist zwar nach wie vor die Hauptursache aller analysierten Schadensfälle. Unternehmen sehen sich jedoch mit immer neuen Herausforderungen und Bedrohungen im Cyberspace konfrontiert. Dazu zählen ihre zunehmende Abhängigkeit von digitalen Lieferketten, die Auswirkungen strengerer Datenschutzbestimmungen sowie die steigende Zahl von Social-Engineering-Angriffen, die auf das schwächste Glied in jedem gut geschützten Unternehmen abzielen: die Mitarbeitenden.

> “
> Eine vielfältigere Risikolandschaft führt auch zu einem breiteren Spektrum an potenziellen Schadensereignissen für Unternehmen

Analyse von Cyber-Versicherungsschäden: Die Risikolandschaft wird vielfältiger – Vorfälle nach Schadenskategorie

Nach Anteil am Gesamtwert der Schäden in % – nur Großschäden (>1 Million Euro)



LEGENDE

- Schäden durch Cyberangriffe (mit Datenexfiltration)
- Schäden durch Cyberangriffe (ohne Datenexfiltration)
- Rückwirkungsschäden (Lieferkette)
- Betriebsunterbrechungen durch technische Fehler
- Nicht im Zusammenhang mit Cyberangriffen stehende Datensicherheitsverletzungen (z. B. unrechtmäßige Erhebung und Verarbeitung von Daten)
- IT-/Media-Vermögenshaftpflichtschäden (z. B. Rechtsstreitigkeiten im Zusammenhang mit der Leistungserbringung usw.)

Quelle: Allianz Commercial. Die Analyse umfasst nur große Versicherungsschäden (>1 Million Euro) im Zeitraum 2021 bis 2025 (erste 6 Monate) mit einem Gesamtwert von über 400 Millionen Euro im Datensatz

Trends

↑ **Anteil der Berufshaftpflichtschäden bei Technologie-/Medienunternehmen nimmt zu**

↑ **Versicherungsschäden aufgrund von Datensicherheitsverletzungen, die nicht im Zusammenhang mit Cyberangriffen stehen, sondern durch die unrechtmäßige Erhebung/Verarbeitung personenbezogener Daten verursacht werden, haben in den letzten Jahren zugenommen. Im ersten Halbjahr 2025 wurden jedoch keine derartigen Vorfälle beobachtet.**

↑ **2024 wurden erstmals Betriebsunterbrechungsschäden aufgrund technischer Fehler verzeichnet – nicht nur im Zusammenhang mit dem CrowdStrike-Vorfall**

↑ **Zusätzliche Versicherungsmodule für Rückwirkungsschäden, die auch Lieferkettenrisiken abdecken, wurden 2024 wieder relevant**

↓ **Seit 2021, als Cyberangriffe für über 80 Prozent der Schadensfälle verantwortlich waren, ist ihr Anteil im Trend gesunken**

SCHADENTRENDS

Bessere Cybersecurity-Infrastruktur von Großunternehmen führt zu Verlagerung von Ransomware-Angriffen auf mittelgroße und weniger gut geschützte Unternehmen

Ransomware-Angriffe haben weiterhin den höchsten Anteil an der Anzahl und den Kosten von Cyber-Versicherungsansprüchen. Die Analysen von **Allianz Commercial** zeigen, dass die durch derartige Angriffe verursachten Schäden in der ersten Jahreshälfte 2025 rund 60 Prozent des Gesamtvolumens großer Cyber-Versicherungsschäden (>1 Million Euro) ausmachten.

In diesem Jahr hat es eine ganze Reihe disruptiver Cyberangriffe auf Einzelhändler in Europa und den USA gegeben, darunter Marks & Spencer, Co-op und United Natural Foods. Im Juli bestätigte die australische Airline Qantas[1], dass sich Hacker Zugang zu wichtigen Daten von bis zu sechs Millionen Kunden verschafft hatten.

Während die Bedrohung durch Ransomware kaum nachzulassen scheint, gibt es Hinweise darauf, dass sich die engere Zusammenarbeit der internationalen Strafverfolgungsbehörden und die bessere Cybersecurity-Infrastruktur großer Unternehmen positiv auf die Cyber-Versicherungsschäden auswirken.

Anfang 2024 erlitten die Aktivitäten zweier führender Ransomware-as-a-Service-Gruppen (RaaS) – LockBit und Noberus – durch eine koordinierte internationale Strafverfolgungsaktion einen schweren Rückschlag. Im Juli 2025 verhaftete die britische National Crime Agency[2] vier Personen (im Alter zwischen 19 und 20 Jahren) im Zusammenhang mit Cyberangriffen auf britische Einzelhändler im Jahr 2025, die Berichten zufolge von der Ransomware-Gruppe Scattered Spider durchgeführt wurden.

Was ist RaaS?

Ransomware-as-a-Service (RaaS) ist ein Geschäftsmodell von Cyberkriminellen, bei dem Ransomware-Entwickler Ransomware-Code oder Malware an andere Hacker, sogenannte „Affiliates", verkaufen, die den Code dann für ihre eigenen Ransomware-Angriffe nutzen.

Allerdings haben auch die Ransomware-Aktivitäten wieder zugenommen, da sich die Angreifer und ihre Partner neu formiert haben oder durch andere Gruppen wie RansomHub (derzeit inaktiv), Akira, Qilin oder DragonForce ersetzt worden sind. Im Jahr 2024 identifizierte das Cybersecurity-Unternehmen CrowdStrike[3] 26 neue Cyberangriffsgruppen, womit die Zahl der von ihm beobachteten Gruppen auf 257 anstieg. Laut BlackFog[4] wurden noch nie zuvor so viele Ransomware-Angriffe gemeldet wie im ersten Quartal 2025, mit einem Plus von 45 Prozent gegenüber dem gleichen Quartal des Vorjahres.

„Unternehmen mit hohen Umsätzen, vielen personenbezogenen Daten und einer schwachen Informationssicherheit sind ideale Ziele für Hacker. Solche Ziele sind jedoch zunehmend schwerer zu finden, weshalb Angreifer nun vermehrt kleinere und weniger gut geschützte Unternehmen ins Visier nehmen" , sagt **Michael Daum, Global Head of Cyber Claims bei Allianz Commercial.** *„Unsere Incident-Response-Partner haben alle Hände voll zu tun – vor allem mit Vorfällen, die nicht versicherte und kleinere Unternehmen betreffen."*

Ransomware-Angriffe betreffen mittlerweile überdurchschnittlich häufig kleine und mittlere Unternehmen. Verizon[5] zufolge war Ransomware zuletzt bei 88 Prozent der von diesen Unternehmen verzeichneten Datenschutzverletzungen im Spiel, verglichen mit 39 Prozent bei größeren Unternehmen. Laut einer Umfrage des World Economic Forum[6] hat sich die Zahl kleiner Unternehmen, die Handlungsbedarf bei ihren Cyberabwehrmaßnahmen sehen, seit 2022 versiebenfacht. Dagegen hat sich die Zahl großer Unternehmen, die ihre Cyberresilienz als unzureichend bezeichnen, im gleichen Zeitraum fast halbiert. Auch im jüngsten **Allianz Risk Barometer** bezeichneten kleinere und mittlere Unternehmen Cybervorfälle als ihr größtes Geschäftsrisiko.

„Die Hürden für einen erfolgreichen Angriff auf ein gut geschütztes Unternehmen sind mittlerweile deutlich höher. Zwar sind auch gut aufgestellte Unternehmen nicht gegen Cyber Angriffe immun, doch der Schwerpunkt erfolgreicher Angriffe hat sich von Großunternehmen in den USA und Europa zunehmend auf kleinere und mittlere Unternehmen sowie auf Unternehmen in anderen Regionen wie Asien und Lateinamerika verlagert", so **Daum.**

SCHADENTRENDS

Datenexfiltration ist eine wesentliche Schadenursache

Vor dem Hintergrund der verbesserten Reaktionsfähigkeit großer Unternehmen ist seit einigen Jahren ein Trend von Ransomware-Angriffen mit einfachen Lösegeldforderungen hin zu doppelten Erpressungsangriffen einschließlich Datenexfiltration zu beobachten.

Bei rund 40 Prozent der im ersten Halbjahr 2025 verzeichneten großen Cyber-Versicherungsschäden (>1 Million Euro) kam es zu Datenexfiltration. Im Gesamtjahr 2024 traf dies nur auf 25 Prozent der Fälle zu. Wie analysen von **Allianz Commercial** zeigen, waren auch die Schäden mehr als doppelt so hoch wie bei Angriffen ohne Datenexfiltration.

„Bei Ransomware-Angriffen beobachten wir weiterhin einen Trend hin zu Angriffen mit Datenexfiltration. Es ist viel einfacher, Daten zu stehlen, als sie zu verschlüsseln – es erfordert weniger Vorbereitung und Aufwand seitens der Angreifer", erklärt **Caitlin Ewing, Complex Claims Analyst bei Allianz Commercial.**

Im diesjährigen **Allianz Risk Barometer,** waren Datensicherheitsverletzungen das Cyberrisiko, das Unternehmen weltweit am meisten Sorgen bereitet. Wie der Cost of a Data Breach Report 2024 von IBM[7] zeigt, erreichten die durchschnittlichen Kosten eines Datenlecks im Jahr 2024 ein Rekordhoch von fast 5 Millionen US-Dollar (4,88 Millionen US-Dollar) pro Fall. Der Anstieg war auf eine Reihe von Faktoren zurückzuführen, darunter der Einfluss strengerer Datenschutzbestimmungen.

Was ist Datenexfiltration?

Datenexfiltration, ist Datendiebstahl: die vorsätzliche unbefugte und verdeckte Übertragung von Daten von einem Computer oder einem anderen Gerät. Datenexfiltration ist mittlerweile ein gängiges Merkmal von Ransomware-Angriffen, um die Wahrscheinlichkeit zu erhöhen, dass die Opfer ein Lösegeld zahlen.

Nach Angaben der Cyber-Sicherheits-Firma Sophos[8] ist der Anteil der Ransomware-Angriffe, die eine Datenverschlüsselung zur Folge haben, auf ein Sechs-Jahres-Tief gesunken: Zuletzt sah sich nur die Hälfte der Opfer eines Cyberangriffs mit einer Datenverschlüsselung konfrontiert – 2024 waren es noch 70 Prozent.

Im Jahr 2024 wurde der Telekommunikationskonzern AT&T Opfer von zwei Datenlecks, bei denen personenbezogene Daten einer zweistelligen Millionenanzahl von Kunden und ehemaligen Kunden rechtswidrig kopiert und im Darknet[9] zum Verkauf angeboten wurden. Im August 2025 wurde berichtet[10], dass das Unternehmen einzelnen Kunden und ehemaligen Kunden im Rahmen eines Vergleichs über 177 Millionen US-Dollar zur Beilegung einer Sammelklage zu beiden Datenpannen möglicherweise bis zu 7.500 US-Dollar zahlen muss.

Artem / Adobe Stock

SCHADENTRENDS

Social Engineering auf dem Vormarsch – Angreifer nehmen Mitarbeitende als schwächstes Glied der Sicherheitskette ins Visier

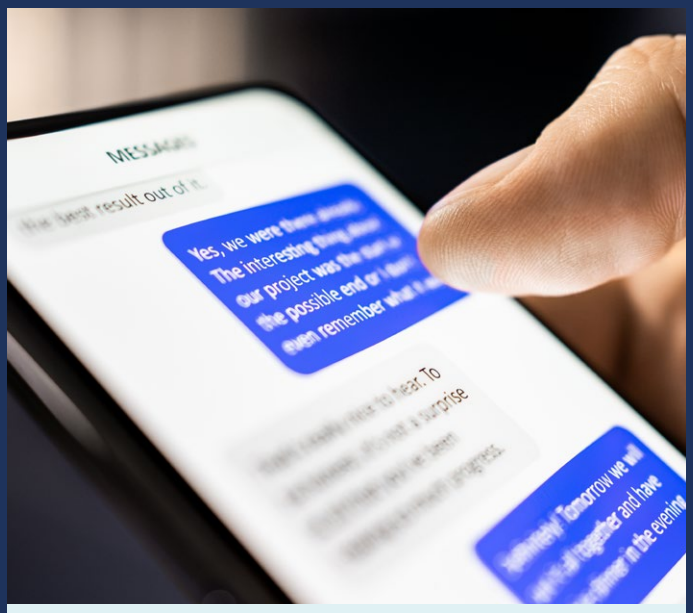
Die jüngsten Cyberangriffe weisen mehrere Gemeinsamkeiten auf, darunter den Einsatz ausgefeilterer Social-Engineering-Methoden und kompromittierter Zugangsdaten, um Unternehmensnetzwerke zu infiltrieren. Viele Angreifer nehmen auch den Umweg über Lieferanten oder IT-Lieferketten, um die ansonsten robusten Abwehrsysteme der betroffenen Unternehmen zu durchbrechen.

Verizon[11] zufolge spielte der Faktor Mensch bei rund 60 Prozent der Datensicherheitsverletzungen im Jahr 2024 eine Rolle. Der Anteil der Sicherheitsverletzungen, an denen Dritte beteiligt waren, verdoppelte sich gegenüber dem vorherigen Berichtszeitraum auf 30 Prozent. Laut Cybereason[12] ist Business E-Mail Compromise (BEC) die häufigste Form des Cybervorfalls, während Phishing und Social Engineering mit einem Anteil von 46 Prozent an allen analysierten Attacken die am häufigsten genutzten initialen Angriffsvektoren sind.

Da Unternehmen ihre Abwehrmaßnahmen verstärkt haben, nehmen Cyberkriminelle nun Mitarbeitende ins Visier, die anfällig für Social Engineering sind, berichtet **Caitlin Ewing, Complex Claims Analyst bei Allianz Commercial.**

„Social Engineering ist für Hacker zu einer gängigen Methode geworden, um durch die Ausnutzung menschlicher Interaktionen an sensible Informationen zu gelangen. Menschen werden als schwächstes Glied der Cybersicherheitskette angesehen, und Angreifer versuchen, dies auszunutzen“, so **Ewing.** *„Social Engineering ist zu einer wesentlichen Ursache von Cyberschäden geworden. Für Cyberkriminelle ist es leichter umzusetzen, vor allem mithilfe von KI. Früher waren derartige Manipulationsversuche einfacher zu erkennen, da häufig Fehler gemacht oder auffällige Formulierungen verwendet wurden. Heute gibt es weniger offensichtliche Warnsignale.“*

> Social Engineering ist zu einer wesentlichen Ursache von Cyberschäden geworden



terovesalainen / Adobe Stock

Die vier Hauptphasen von Social-Engineering-Angriffen

- **Informationen sammeln:** Im Vorfeld von Angriffen nutzen Cyberkriminelle häufig Informationen aus sozialen Medien, wie beispielsweise den Jobtitel oder die Aufgabenbereiche eines Beschäftigten, um dessen Identität überzeugend zu fälschen.
- **Vertrauen aufbauen oder ein Gefühl der Dringlichkeit erzeugen:** Hacker können entweder Zeit investieren, um eine Beziehung aufzubauen und das Vertrauen einer Person zu gewinnen, oder ein Gefühl der Dringlichkeit erzeugen, indem sie einen vorgetäuschten Notfall inszenieren, um ihr Opfer zum Handeln zu bewegen.
- **Schwachstellen ausnutzen:** Wenn die Opfer ihnen vertrauen oder auf einen vorgetäuschten Notfall reagieren, bringen Hacker sie dazu, sensible Informationen preiszugeben.
- **Spuren verwischen:** Haben sie ihr Ziel erreicht, versuchen die Hacker, jegliche Hinweise auf ihre Aktivitäten auszulöschen.

SCHADENTRENDS

Der goldene Schlüssel: Zugangsdaten überholen Malware

Im Zusammenhang mit Social Engineering und Phishing steht auch die zunehmende Verwendung von Zugangsdaten wie Benutzername und Passwort für den Erstzugriff bei Cyberangriffen. Laut Verizon[13] sind kompromittierte Anmeldedaten mittlerweile zum häufigsten Angriffsvektor geworden.

Ransomware-Gruppen nutzen Zugangsdaten, die sie sich durch Phishing- oder Cyberattacken aneignen, darunter auch Daten von IT-Dienstleistern oder im Darknet zum Verkauf angebotene Daten. Darüber hinaus verschaffen sich spezialisierte Agenten, sogenannte Access Broker, Zugang zu Unternehmen und verkaufen die erlangten Zugangsdaten an andere Bedrohungsakteure wie Ransomware-Gruppen. Das Cybersecurity-Unternehmen CrowdStrike[14] berichtet über eine starke Zunahme der Aktivitäten dieser Akteure im Jahr 2024, mit fast 50 Prozent mehr Anzeigen von Access Brokern, die gültige gestohlene Zugangsdaten verkaufen, als 2023.

Scattered Spider, eine Hackergruppe, die hinter den jüngsten Angriffen auf Casinos, Einzelhändler, Fluggesellschaften und Versicherungen vermutet wird, verschafft sich mithilfe kompromittierter Zugangsdaten und ausgeklügelter Social-Engineering- und Phishing-Taktiken Zugang zu den Systemen von Unternehmen. So viel Medienaufmerksamkeit wie 2025 hat die Gruppe noch nie erhalten: In den ersten sechs Monaten des Jahres wurden ihr bereits mehr als zehn gemeldete Angriffe zugeschrieben. Ein Angriff kann zum Beispiel so ablaufen: Die Hacker kontaktieren den IT-Helpdesk eines Unternehmens und geben sich als legitime Mitarbeitende aus, um ein Passwort und/oder die Multi-Faktor-Authentifizierung (MFA) zurückzusetzen. Sobald sie sich Zugang zum IT-System verschafft haben, versuchen sie, Ransomware einzuschleusen, Daten zu verschlüsseln und personenbezogene Daten zu exfiltrieren. Bei einem Vorfall im Jahr 2025 wechselten die Angreifer lau CrowdStrike[15] innerhalb von nur 24 Stunden von der Kontoübernahme zum Einsatz von Ransomware – 32 Prozent schneller als im Jahr 2024. Wie Analysten festgestellt haben, besteht eine der größten Stärken der Hackergruppe Scattered Spider darin, dass ihre Mitglieder größtenteils englische Muttersprachler sind, die sich überzeugend als amerikanische oder britische Mitarbeitende ausgeben und so echte Zugangsdaten zu den IT-Systemen eines Zielunternehmens erbeuten können.

Die stärkere Konzentration auf identitätsbasierte Angriffsversuche ist Teil einer allgemeinen Abkehr von Malware. Im Jahr 2024 beobachtete CrowdStrike[16] eine Zunahme der interaktiven Angriffskampagnen um 35 Prozent gegenüber dem Vorjahr. Anstelle von Schadsoftware setzen Cyberkriminelle bei diesen Angriffen auf „Hands-on-Keyboard"-Aktionen, um normales Verhalten legitimer Benutzer oder Administratoren nachzuahmen. Im vergangenen Jahr waren rund 80 Prozent der Angriffe malwarelos – verglichen mit 40 Prozent im Jahr 2019.

Social Engineering bleibt ein beliebtes Einfallstor für Cyberkriminelle, da es schneller und einfacher als das Hacken eines gut geschützten Systems ist, erläutert **Rishi Baviskar, Global Head of Cyber Risk Consulting at Allianz Commercial.**

„Anmeldedaten zu verwenden ist einfacher als Hacken. Haben sie erst einmal den ‚goldenen Schlüssel', können sich Hacker schnell Zugang zu einem System verschaffen, ihre Zugriffsrechte erweitern und sich dann frei im System bewegen."

Die Abwehr von Social-Engineering-Versuchen und Angriffen mit gestohlenen Anmeldedaten ist eine Frage der grundlegenden Cyberhygiene, meint **Baviskar:**

„Multi-Faktor-Authentifizierung (MFA), strenge Zugriffskontrollen und Schulungen tragen dazu bei, die Risiken derartiger Angriffe zu reduzieren. Und wenn der Benutzerzugriff auf wesentliche Geschäftszwecke beschränkt ist, wird es für Hacker noch viel schwieriger. Da die Angreifer ihre Taktiken ändern, müssen sich die Unternehmen anpassen und Abwehrmaßnahmen für verschiedene Szenarien entwickeln."

Während Cyberkriminelle versuchen, Cybersicherheitsmaßnahmen zu umgehen, bleibt MFA eine unverzichtbare Sicherheitskontrolle. Cybereason[17] zufolge hatten nur 36 Prozent der Unternehmen, die Opfer eines Business Email Compromise (BEC)-Angriffs wurden, MFA für ihre kompromittierten Konten aktiviert.

„Die Multi-Faktor-Authentifizierung (MFA) hat sich als echter Game Changer erwiesen. Mit MFA ist es viel schwieriger, sich unbefugt Zugang zu einem System zu verschaffen. Wir sehen zwar einige Fälle, in denen Angreifer versuchen, die Authentifizierung durch Abfangtechniken oder MFA-Fatigue zu umgehen – eine Angriffstaktik, bei der Benutzer mit wiederholten Multi-Faktor-Authentifizierungsanfragen bombardiert werden, bis ihre Wachsamkeit nachlässt. Eine komplett fehlende MFA wäre jedoch ein viel größeres Problem", betont **Baviskar.**

SCHADENTRENDS

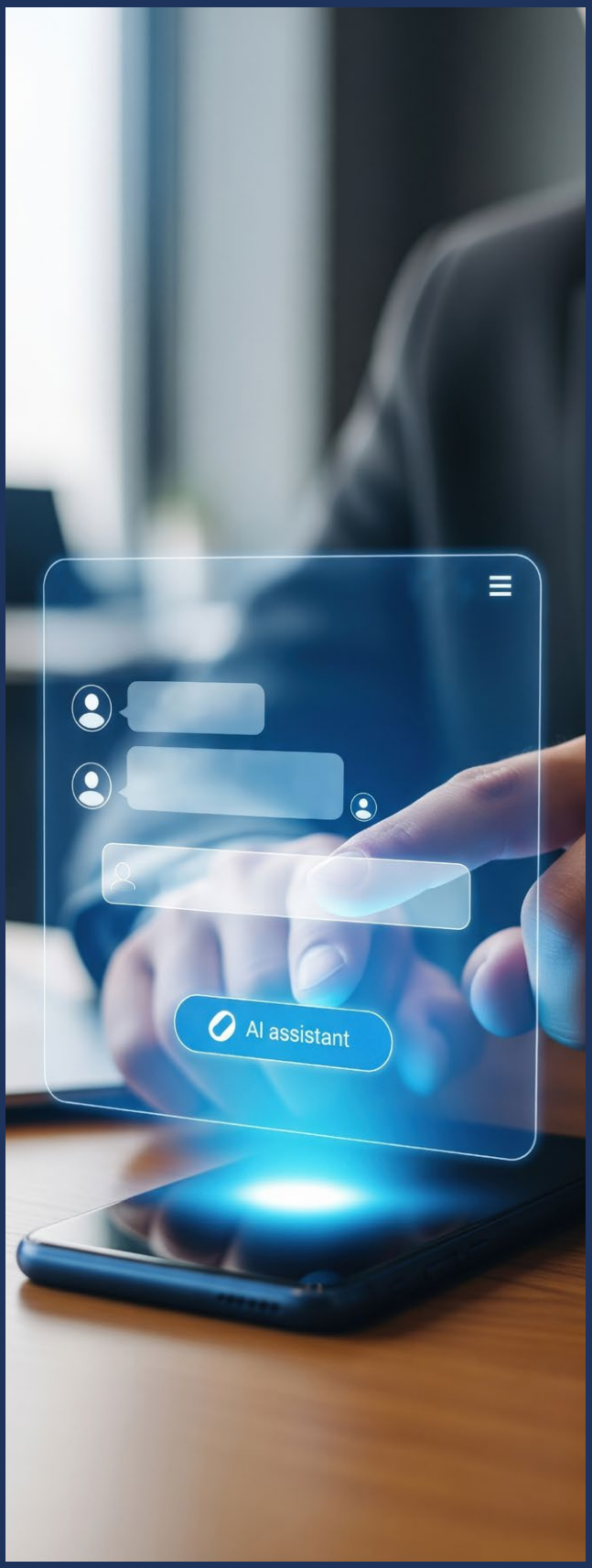
Effektivere Social-Engineering- und Malware-Angriffe durch KI

Cyberkriminelle und staatliche Hackergruppen machen regen Gebrauch von künstlicher Intelligenz (KI), die ihre Produktivität und die Raffinesse ihrer Angriffe steigert. Mithilfe von KI können Cyberkriminelle zum Beispiel schneller umfangreichere Ransomware-Angriffe durchführen und Angriffstools oder natürlicher aussehende Malware-Codes entwickeln, die für Antivirensoftware schwieriger zu erkennen sind.

Generative KI hat erhebliche Auswirkungen auf Social Engineering, da sie überzeugendere und personalisierte Social-Engineering-Taktiken, Phishing-E-Mails und Websites zum Abgreifen von Zugangsdaten ermöglicht. Untersuchungen[18] haben gezeigt, dass die Klickrate für KI-generierte Phishing-E-Mails mit der für von Menschen erstellte Inhalte vergleichbar ist. Kriminelle nutzen KI auch, um Unternehmen mithilfe von Deepfakes zu betrügen oder sich Zugang zu Anmeldedaten zu verschaffen.

„Angreifer nutzen KI, um die verschiedenen Schritte, die hinter Cyberangriffen stehen, zu automatisieren und zu beschleunigen. Tatsächlich nehmen sowohl Ausmaß als auch Häufigkeit der Angriffe zu. Damit rückt die Notwendigkeit einer guten Abwehr wieder in den Vordergrund. Wenn man nur eine schwache Cybersicherheitsinfrastruktur hat und nicht in Prozesse und Technologien zur Erkennung von und Reaktion auf Cyberbedrohungen, Sicherheitsverletzungen und Cyberangriffe investiert, kommen die Angreifer wahrscheinlich durch. Dafür braucht es nur einen erfolgreichen Angriff“, warnt **Rishi Baviskar, Global Head of Cyber Risk Consulting, Allianz Commercial.**

> Angreifer nutzen KI, um Angriffe zu automatisieren und zu beschleunigen. Damit rückt die Notwendigkeit einer guten Abwehr wieder in den Vordergrund



photchara / Adobe Stock

SCHADENTRENDS

Einzelhandel wird zum Hauptangriffsziel

Im ersten Halbjahr 2025 führten Einzelhändler die Liste der Top-Angriffsziele von Cyberkriminellen an. Wie eine Analyse der Auswirkungen großer Cyber-Schadensfälle (>1 Million Euro) seit 2020 zeigt, ist der Handel zudem der am drittstärksten von Cybervorfällen betroffene Sektor nach dem verarbeitenden Gewerbe und den Dienstleistungen. In diesem Zeitraum entfielen die Kosten der analysierten Großschäden durch Cybervorfälle zu 33 Prozent auf produzierende Unternehmen, zu 18 Prozent auf Dienstleister/ Beratungsunternehmen und zu 9 Prozent auf Einzelhändler.

In Großbritannien führten Hacker in den letzten zwölf Monaten mehrere erfolgreiche Angriffe auf Einzelhändler durch, darunter Harrods, Marks & Spencer und die Co-operative Group. Nach einem Ransomware-Angriff auf seinen US-Betrieb wurde Ahold Delhaize, eine der größten Supermarktketten der Welt, im vergangenen Jahr ebenfalls Opfer eines Datenlecks. Die französische Luxusmarke Louis Vuitton[19] war in diesem Jahr bereits von mehreren Cyberangriffen betroffen.

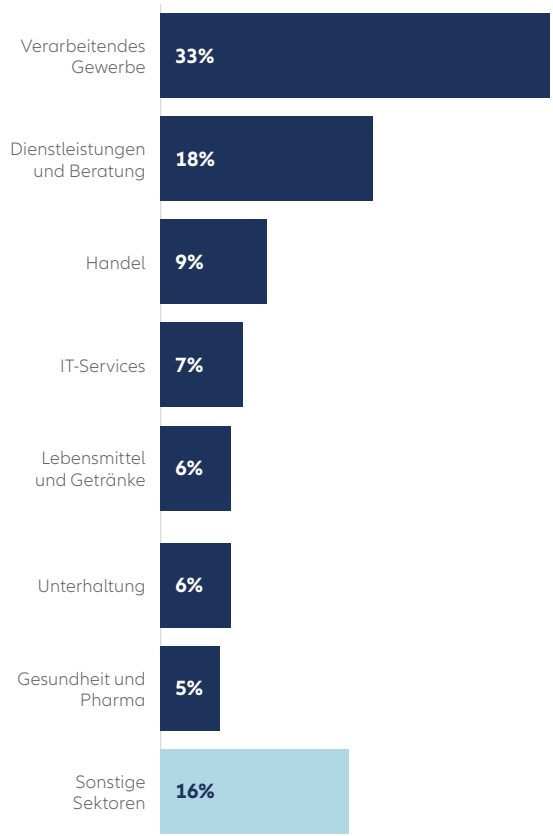
Viele der Angriffe auf Einzelhändler werden der Ransomware-Gruppe Scattered Spider zugeschrieben und weisen mehrere Gemeinsamkeiten auf, zum Beispiel die Anwendung doppelter Erpressung und ausgeklügelter Social-Engineering-Techniken.

Einzelhändler sind aus mehreren Gründen attraktive Ziele für Cyberkriminelle: Sie haben hohe Umsätze, verarbeiten große Mengen an personenbezogenen Daten und sind anfällig für betriebliche Störungen – alles Faktoren, die bei Erpressungsforderungen als Druckmittel dienen können. Einzelhändler haben in der Regel eine große Belegschaft und eine Vielzahl unterschiedlicher Lieferanten und IT-Systeme. Das schafft eine große Angriffsfläche. Gleichzeitig sind ihre Cybersicherheitssysteme zumeist weniger ausgereift als in Branchen wie dem Bankwesen.

Cyberangriffe auf bestimmte Branchen können zu Risikoakkumulationen in den Portfolios der Versicherer führen, erklärt **Tresa Stephens, Head of Cyber, North America bei Allianz Commercial:** *„Im vergangenen Jahr gab es mehrere Angriffe, die auf bestimmte Branchen wie den Einzelhandel abzielten; davor standen das Gesundheitswesen und das Bildungswesen im Fokus. Wenn Angreifer eine bestimmte Branche ins Visier nehmen, unterstreicht das die Notwendigkeit für Versicherer, ihre Risikoexpositionen zu steuern und sicherzustellen, dass ihr Portfolio ausreichend diversifiziert ist"*, so **Stephens.**

Am stärksten betroffene Branchen nach großen Cyberschäden (>1 Million Euro)

Anteil am Schadenvolumen in %



Quelle: Allianz Commercial. Die Analyse umfasst nur große Versicherungsschäden (>1 Million Euro) im Zeitraum 2020 bis 2025 (erste 6 Monate) mit einem Gesamtwert von über 450 Millionen Euro im Datensatz

Im September 2025 wurde der britische Luxusautohersteller Jaguar Land Rover Ziel eines schwerwiegenden Cyberangriffs. Nach Angaben des Unternehmens wurden dessen Vertriebs- und Produktionsaktivitäten dadurch „erheblich beeinträchtigt"[20]. Der Angriff wurde mit Mitgliedern der Gruppe „Scattered Spider" sowie anderen Hackern in Verbindung gebracht.

SCHADENTRENDS

Rückwirkungsschäden in der IT-Lieferkette als zentrale Gefahr

Ein wichtiger Trend in den letzten 18 Monaten war das Aufkommen von Schadensfällen im Zusammenhang mit der zunehmenden Abhängigkeit von IT-Lieferketten. Wie Untersuchungen von **Allianz Commercial** zeigen, waren Rückwirkungsschäden in IT-Lieferketten im ersten Halbjahr 2025 für 15 Prozent der Kosten großer Cyber-Versicherungsschäden (>1 Million Euro) verantwortlich – verglichen mit 6 Prozent im Jahr 2024. Besonders besorgniserregend sind Rückwirkungsschäden dadurch, dass sie sowohl durch Cyberattacken als auch durch technische Fehler verursacht werden können.

Im vergangenen Jahr gab es mehrere bedeutende Fälle von Rückwirkungsschäden aufgrund von Cybervorfällen in IT-Lieferketten. CDK Global, ein Anbieter von Software für die Automobilindustrie, wurde 2024 Opfer eines Ransomware-Angriffs, von dem Tausende von Autohäusern in den USA betroffen waren. Ein erfolgreicher Ransomware-Angriff auf Blue Yonder, einen Anbieter von Supply-Chain-Software, im November 2024 führte zu Betriebsstörungen bei mehreren Kunden, darunter die großen britischen Supermarktketten Morrisons und Sainsbury's.

„Rückwirkungsschäden sind ein deutlicher Trend. Wenn es zu einem Zwischenfall bei einem Geschäftspartner kommt, kann das erhebliche Auswirkungen auf Ihr Unternehmen haben, selbst wenn Sie gut vorbereitet sind", betont **Caitlin Ewing, Complex Claims Analyst at Allianz Commercial.**

Lieferketten entwickeln sich zu einem wesentlichen Treiber von Cyber-Versicherungsschäden und bergen ein bedeutendes Risiko für Rückwirkungsschäden. Wie ein vor Kurzem vom World Economic Forum veröffentlichter Bericht[21] zeigt, betrachtet mehr als die Hälfte der Großunternehmen (54 Prozent) lieferkettenbezogene Herausforderungen als größtes Hindernis für den Aufbau von Cyberresilienz.

Ein Cyberangriff oder ein technischer Fehler, der sich auf die IT-Systeme einer Drittpartei auswirkt, kann Unterbrechungen kritischer Dienste – wie Software oder Cloud-Services – bei Versicherten zur Folge haben. Dem Cybersecurity-Unternehmen CrowdStrike[22] zufolge ist die Zahl der Cloud-Angriffe im ersten Halbjahr 2025 im Vergleich zum Gesamtjahr 2024 um 136 Prozent gestiegen. Störungen in der IT-Lieferkette können auch Auswirkungen auf physische Produkte haben, wenn der Lieferant eines Versicherungsnehmers aufgrund eines IT-Ausfalls oder Cyberangriffs nicht in der Lage ist, die für die Produktion erforderlichen Waren zu liefern.

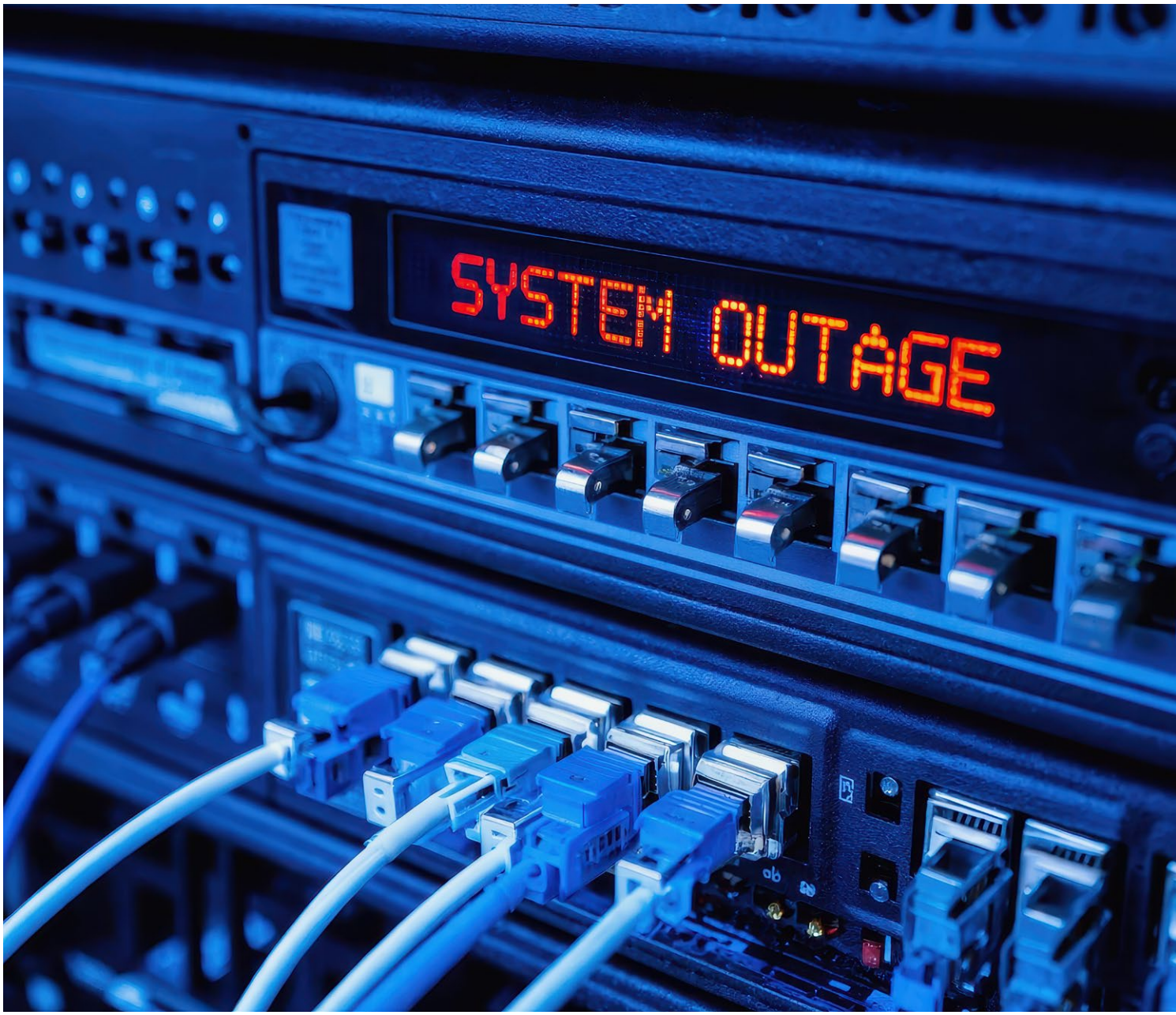
„Die meisten Unternehmen nutzen heute externe Anbieter für wichtige digitale Dienstleistungen wie Software, Cybersicherheit oder Datenspeicherung und -verarbeitung. Unternehmen müssen diese kritischen Abhängigkeiten verstehen und sich darüber im Klaren sein, welche Auswirkungen es haben kann, wenn diese Dienste durch einen Ausfall, einen technischen Fehler oder einen Cyberangriff lahmgelegt werden", sagt **Tresa Stephens, Head of Cyber, North America bei Allianz Commercial.**

Im Kontext von Cyberversicherungen sind Lieferkettenrisiken derzeit das wichtigste neue Bedrohungsthema, sagt **Michael Daum, Global Head of Cyber Claims bei Allianz Commercial.** Neben potenziellen Rückwirkungsschäden können Cybervorfälle bei Lieferanten auch zu Datenschutzverletzungen wie der Kompromittierung von Zugangsdaten oder personenbezogenen Daten führen.

„Viele Unternehmen haben ihre eigene Cybersicherheit und vor allem ihre Erkennungs- und Reaktionsmechanismen erheblich verbessert und dadurch die Schäden aus Cybervorfällen erfolgreich gesenkt. Dennoch bleibt ein erhebliches Risiko über ihre IT-Dienstleister und Partner bestehen, welches deutlich schwerer zu kontrollieren ist. Zukünftig wird das Cyber Management von Dienstleistern und Lieferanten noch größere Bedeutung erlangen, etwa über sorgfältige Vertragsgestaltung, Monitoring und Audits", so **Daum.**

> Das Risiko von Datenschutzverletzungen bei IT-Dienstleistern und Partnern ist viel schwieriger zu kontrollieren

Mehr ‚Nicht-Angriffs'-Cyberschäden in einer vielfältigeren Risikolandschaft



aznan / Adobe Stock

MEHR ‚NICHT-ANGRIFFS'-CYBERSCHÄDEN IN EINER VIELFÄLTIGEREN RISIKOLANDSCHAFT

Erstmals große Schäden durch technische Fehler und Ausfälle

Obwohl Cyberangriffe weiterhin die Hauptursache von Cyber-Versicherungsschäden sind, ist der Anteil technischer Fehler und Datenschutzverletzungen gestiegen – im Jahr 2024 waren sie für rekordhohe 28 Prozent der Kosten analysierter Großschäden (>1 Million Euro) verantwortlich.

Betriebsunterbrechungen aufgrund technischer Fehler tauchten 2024 erstmals in den Daten von **Allianz Commercial** zu großen Cyber-Schadensfällen auf, mit einem Anteil von rund 10 Prozent am Gesamtwert dieser Schäden. Ein Grund dafür war der IT-Ausfall beim Cybersecurity-Unternehmen CrowdStrike, einer der größten IT-Ausfälle aller Zeiten, von dem weltweit schätzungsweise 8,5 Millionen Windows-Systeme betroffen waren. Die durch ein fehlerhaftes Software-Update verursachten Systemausfälle führten zu erheblichen Störungen im Gesundheitswesen, im Einzelhandel, im Finanzwesen und im Gastgewerbe und hatte Tausende von Flugausfällen sowie mehrere Hafenschließungen in den USA und Europa zur Folge.

Systemausfälle können durch verschiedene technische Fehler oder menschliches Versagen verursacht werden. Der Modehändler H&M[23] war nach einem Ausfall seiner IT-Systeme Anfang dieses Jahres vorübergehend nicht in der Lage, Zahlungen in seinen Filialen abzuwickeln. Beim deutschen Autohersteller VW[24] führte eine Fehlkonfiguration des Cloud-Speichersystems Ende 2024 zu einer Datenpanne, bei der die Daten von 800.000 E-Auto-Besitzern kompromittiert wurden.

Technische Fehler sind keine Seltenheit, sagt **Rishi Baviskar, Global Head of Cyber Risk Consulting:**

„Der Ausfall einer wichtigen Software oder eines wichtigen Dienstleisters kann erhebliche Betriebsunterbrechungen und Schäden für Unternehmen und ihre Versicherer zur Folge haben, deren Ausmaß mit dem von Ransomware-Angriffen vergleichbar ist. Ob Softwarefehler, fehlerhaftes Update, Fehlkonfiguration oder Systemausfall – derartige Ereignisse können einen Dominoeffekt auslösen und eine große Zahl von Versicherten in Mitleidenschaft ziehen."

Darüber hinaus sind die Rechenzentren, in denen Cloud-Services und ausgelagerte IT-Dienste untergebracht sind, anfällig für Naturkatastrophen wie Überschwemmungen, Stromausfälle und extreme Wetterereignisse wie Hitzewellen oder Wasserknappheit. Ein Ausfall ihrer Kühlsysteme kann dazu führen, dass Systeme in den Failsafe-Modus wechseln, was ebenfalls Betriebsunterbrechungen zur Folge haben kann.

Auch durch Ausfälle kritischer Versorgungsinfrastruktur wie der Stromversorgung kann es zu Datenverlusten und Unterbrechungen von IT-Diensten kommen. Der wirtschaftliche Schaden für den öffentlichen und privaten Sektor durch den großflächigen Stromausfall in Spanien und Portugal im April 2025 wird auf 1,6 Milliarden Euro[25] geschätzt. In diesem Jahr ist es in Spanien, Frankreich, der Tschechischen Republik und Indien zu Ausfällen von Kommunikationsnetzen gekommen. In der ersten Jahreshälfte 2025 registrierte die Allianz mehr als zehn großflächige Stromausfälle.

> Der Ausfall einer wichtigen Software oder eines wichtigen Dienstleisters kann erhebliche Betriebsunterbrechungen und Schäden für Unternehmen und ihre Versicherer zur Folge haben

MEHR ‚NICHT-ANGRIFFS'-CYBERSCHÄDEN IN EINER VIELFÄLTIGEREN RISIKOLANDSCHAFT

Datenschutzgesetze und Rechtsprechung weiter in der Entwicklung

„Nicht-Angriffs"-Datenschutzverletzungen und -klagen, zum Beispiel im Zusammenhang mit der unrechtmäßigen Erhebung und Verarbeitung personenbezogener Daten, haben in den vergangenen Jahren an Bedeutung gewonnen. Wie die Schadenstatistik von **Allianz Commercial** zeigt, betrug ihr Anteil am Gesamtwert der großen Cyber-Schadensfälle (>1 Million Euro) im Jahr 2024 rekordhohe 18 Prozent – dreimal so viel wie drei Jahre zuvor.

IT-/Media-Vermögenshaftpflichtschäden machten im ersten Halbjahr 2025 ein Viertel des Volumens großer Schadensfälle aus, verglichen mit 21 Prozent im Jahr 2024. Viele dieser Versicherungsansprüche stehen im Zusammenhang mit rechtlichen Schritten gegen Technologieunternehmen aufgrund von Servicedefiziten, technischen Fehlern und angeblichen Verstößen gegen Datenschutzgesetze und Geheimhaltungspflichten. Sie können aber auch auf Angriffe zurückzuführen sein.

rookielion / Adobe Stock

In den USA haben Sammelklagen wegen der Verletzung von Datenschutzvorschriften in den vergangenen Jahren deutlich zugenommen. Viele Bundesstaaten sind noch dabei, derartige Vorschriften zu entwickeln und umzusetzen. Wie die Anwaltskanzlei Duane Morris[26] berichtet, erreichte die Zahl der diesbezüglichen Rechtsstreitigkeiten mit rund 1.500 Klagen im Jahr 2024 ein beispielloses Ausmaß.

„Datensicherheitsverletzungen, die nicht im Zusammenhang mit Cyberangriffen stehen, und IT-/Media-Vermögenshaftpflichtschäden sind zu bedeutenden Faktoren geworden, da Unternehmen mehr Daten zu einzelnen Personen erheben und sich die regulatorischen und rechtlichen Rahmenbedingungen ändern. In den USA befinden sich die Datenschutzgesetze auf Ebene der Bundesstaaten weiterhin in der Entwicklung. In diesem Umfeld gehen die Klägeranwälte äußerst unternehmerisch vor und finden immer wieder neue Möglichkeiten, Sammelklagen gegen Unternehmen wegen potenzieller Datenschutzverletzungen einzureichen", berichtet **Caitlin Ewing, Complex Claims Analyst bei Allianz Commercial.**

Die Erfassung biometrischer Daten hat in den letzten Jahren zu einer Welle von Sammelklagen geführt und gezeigt, wie die Gerichte neue Datenschutzgesetze wie den Illinois Biometric Information Privacy Act (BIPA), ein US-amerikanisches Gesetz, auslegen. Eine kürzlich erfolgte Klarstellung des BIPA hat den Umfang potenzieller Schadenersatzansprüche eingeschränkt. Zuletzt hat es jedoch auch Sammelklagen auf der Grundlage des Gesetzes zum Schutz genetischer Informationen des Bundesstaates Illinois (Illinois Genetic Information Privacy Act) gegeben, so **Ewing.**

Darüber hinaus wurden bereits mehrere hundert Sammelklagen gegen Unternehmen wegen der unbefugten Weitergabe und Nutzung von Daten im Zusammenhang mit neuen Technologien eingereicht, zum Beispiel Web-Tracking-Technologien wie Tracking Pixel oder Session-Replay-Software. Dabei berufen sich die Kläger sowohl auf staatliche Datenschutzgesetze als auch auf Gesetze zur telefonischen Überwachung.

In den USA werden weiterhin Sammelklagen im Zusammenhang mit Datenschutzthemen eingereicht, deren Ausgang jedoch

noch offen ist, sagt **Tresa Stephens, Head of Cyber, North America bei Allianz Commercial:** *„Die Kläger sind streitlustig und wollen die neuen Datenschutzbestimmungen zusammen mit bestehenden Gesetzen nutzen, um dagegen anzugehen, wie einige Unternehmen Technologie einsetzen, und sich gegen eine vermeintliche Überwachungskultur zu wehren."*

Beispielsweise wurden zahlreiche Klagen im Zusammenhang mit dem sogenannten Daniel's Law in New Jersey eingereicht, das die Offenlegung der privaten Adressen und Telefonnummern bestimmter Amtsträger einschränkt.

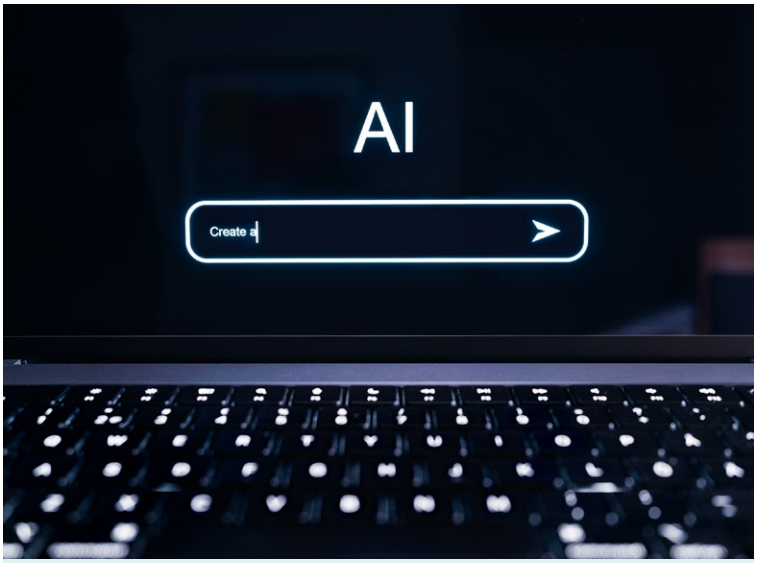
„Wir sehen gerade die erste Klagewelle im Zusammenhang mit dem Daniel's Law – als erstes Gesetz dieser Art hat es eine Menge Aktivität ausgelöst, und inzwischen erwägen auch andere Bundesstaaten die Einführung ähnlicher Gesetze", so **Ewing.**

Compliance-Vorgaben einzuhalten, ist herausfordernd, meint **Stephens:**

„Unternehmen sammeln in mehreren Ländern und Bundesstaaten mit jeweils eigenen Datenschutzgesetzen und -vorschriften Daten über Personen. Mit den Vorschriften in Echtzeit Schritt zu halten, ist eine große Herausforderung, insbesondere angesichts der Fortschritte in Bereichen wie künstliche Intelligenz und Biometrie."

Laut der Anwaltskanzlei BakerHostetler[27] wird bis 2026 etwa die Hälfte der US-Bevölkerung durch umfassende bundesstaatliche Datenschutzgesetze geschützt sein. Die US-Bundesstaaten sind weiter dabei, Datenschutzgesetze in Bereichen wie Datenerhebung und -nutzung, Biometrie, Schutz der Daten von Kindern und Datenbroker zu erlassen oder bestehende Gesetze anzupassen.

Die Einhaltung von Vorschriften, wie beispielsweise Meldepflichten bei Datenschutzverletzungen, kann für Unternehmen eine Herausforderung darstellen, insbesondere während eines Cyberangriffs. Cyberversicherungen sind jedoch in der Regel mit einer professionellen Krisenberatung durch erfahrene Experten verbunden. Dadurch erhalten die Unternehmen schnell Unterstützung bei der Umsetzung geeigneter Reaktionsmaßnahmen, erläutert **Stephens.**



terovesalainen / Adobe Stock

Haftpflicht- und Rechtsverfolgungsrisiken durch KI

Künstliche Intelligenz (KI) ist ein heißes Thema für Versicherungsnehmer, die in einem sich wandelnden regulatorischen Umfeld unter Wettbewerbsdruck stehen, KI-Tools einzuführen.

„Um das Thema KI führt kein Weg mehr herum und es entwickelt sich zu einem interessanten neuen Bereich für Risiko- und Haftungsfragen. Fast alle Unternehmen prüfen den Einsatz von KI, um ihre Effizienz zu steigern. Niemand möchte den Anschluss verlieren und in der nächsten Phase der technologischen Revolution zurückbleiben," sagt **Tresa Stephens, Head of Cyber, North America bei Allianz Commercial.**

„Die Underwriter werden von den Unternehmen genau wissen wollen, wie sie KI nutzen. Dabei wird der Fokus auf Anwendungen mit höherem Risiko liegen, zum Beispiel KI-basierten Kundeninteraktionen oder KI-gestützten Diensten, die Kunden angeboten werden. Wir möchten wissen, wie derartige Anwendungen aussehen und welche Maßnahmen ergriffen werden, um die Risiken zu mindern."

Neben ihrer Rolle in der Cybersicherheit dürfte KI auch zu höheren Haftungsrisiken und Versicherungsschäden führen. Beispielsweise können KI-Systeme zu Datensicherheitsverletzungen durch eine unrechtmäßige Erhebung und Verarbeitung von Daten führen.

„Das Risiko ist da. Datenschutzklagen im Zusammenhang mit dem Einsatz von KI könnten sich zu einem potenziellen Treiber von Cyber-Versicherungsschäden entwickeln", sagt **Caitlin Ewing, Complex Claims Analyst bei Allianz Commercial.**

Erkennung, Reaktion und Schulung

kaliel / Adobe Stock

ERKENNUNG, REAKTION UND SCHULUNG

Die Kosten von Schadensfällen reduzieren

Die jüngsten Cyberangriffe haben den Wert einer guten Cyberhygiene und einer effektiven Bedrohungserkennung und Cyberreaktion sowie die Notwendigkeit von Schulungsprogrammen zur Sensibilisierung der Mitarbeitenden für potenzielle Bedrohungen verdeutlicht. Alle diese Maßnahmen können die Auswirkungen eines Cybervorfalls nachweislich erheblich begrenzen.

„Eine wichtige Erkenntnis des diesjährigen Berichts ist, dass Cyberhygiene zwar nach wie vor von entscheidender Bedeutung ist, die Vorbereitung auf Bedrohungsszenarien aber genauso wichtig ist. Hier kann eine Cyberversicherung sehr hilfreich sein. Mit einer solchen Deckung erhalten Kunden Zugang zu einer Vielzahl von Experten und einem breiten Spektrum von Dienstleistungen, die ihnen helfen können, sich für etwaige Vorfälle zu rüsten und diese besser zu bewältigen. Das kann die finanziellen und geschäftlichen Auswirkungen sowie den potenziellen Reputationsschaden erheblich mindern“, sagt **Tresa Stephens, Head of Cyber, North America bei Allianz Commercial.**

> Eine effektive Bedrohungserkennung und Cyberreaktion können die Kosten von Schadensfällen um den Faktor 1.000 reduzieren

Eine Analyse der von **Allianz Commercial** bearbeiteten Schadensfälle zeigt, wie grundlegende Sicherheitsmaßnahmen – wie Patching, Segmentierung, Backups und die Verwendung von Multi-Faktor-Authentifizierung (MFA) – entscheidend dazu beitragen können, Cyberschäden zu verhindern und zu mindern. Bei mehr als 80 Prozent der von **Allianz Commercial** analysierten großen Schadensfälle (>1 Million Euro) hatten die Entscheidungen des versicherten Unternehmens erheblichen Einfluss auf die Höhe des Schadens, und die meisten Vorfälle hätten leicht vermieden oder begrenzt werden können.

Eine effektive Bedrohungserkennung und Cyberreaktion können die Kosten von Schadensfällen um den Faktor 1.000 reduzieren.

20.000 oder 20 Millionen Euro? Früherkennung und Reaktionsfähigkeit können den Ausschlag gebene

PROFILE: Ein produzierendes Unternehmen mit 2.000 Beschäftigten.

Cybervorfall - Szenario 1: Eine oder mehrere Computer von Mitarbeitenden werden erfolgreich gehackt. Der Angriff wird frühzeitig erkannt und eingedämmt (zum Beispiel, bevor sich die Angreifer Administratorrechte sichern können).

Kosten: Die Gesamtkosten für die IT-Forensik zur Aufklärung des Sachverhalts und für die Wiederherstellung von Daten und Systemen belaufen sich auf etwa 20.000 Euro.

Cybervorfall - Szenario 2: Die Situation ist die gleiche, aber der Angriff bleibt unentdeckt und wird nicht frühzeitig gestoppt, sodass die Angreifer das IT-System des Unternehmens erfolgreich infiltrieren und ihr Hauptziel erreichen (d.h. Administratorrechte für die Domain). Den Angreifern gelingt es, die Systeme des Unternehmens zu verschlüsseln und das Unternehmen zu erpressen.

Kosten: Der Gesamtverlust durch die Betriebsunterbrechung (zwei Wochen), die Lösegeldzahlung, die vollständige Systemwiederherstellung und Schadenersatzansprüche von Dritten aufgrund kompromittierter persönlicher Daten summiert sich auf rund 20 Millionen Euro (1.000 mal so viel wie in Szenario 1).

Ihre zunehmende Bedeutung zeigt sich auch im Wachstum des globalen Marktes für MDR-Dienstleistungen (Managed Detection and Response). Nach Schätzungen von Precedence Research[28] wird sich das Volumen dieses Marktes von knapp 3 Milliarden US-Dollar im Jahr 2024 bis 2034 auf 12 Milliarden US-Dollar vervierfachen.

Die zunehmende Abhängigkeit von Technologien und externen Dienstleistern macht die Früherkennung und Vorbereitung auf etwaige Cybervorfälle noch wichtiger, betont **Rishi Baviskar, Global Head of Cyber Risk Consulting bei Allianz Commercial.**

„Die Frage ist nicht, ob, sondern wann es zu einem Cybervorfall kommt – daher ist die Resilienz entscheidend. Unternehmen müssen die Kosten von Betriebsunterbrechungen durch Maßnahmen zur Identifizierung und Eindämmung von Sicherheitsproblemen kontrollieren – sie müssen vorbereitet sein, regelmäßige Tests durchführen und Incident-Response-Experten in Bereitschaft haben. Kürzere Betriebsunterbrechungen und die Eindämmung von Datenschutzverletzungen führen schnell zu erheblichen Kosteneinsparungen."

Dieser positive Trend sollte Unternehmen davon überzeugen, in einer sich verändernden Cyberrisikolandschaft in Cybersicherheit zu investieren, meint **Stephens:**

„Die Risikolandschaft verändert sich ständig, und wir wissen nie, welche neuen Herausforderungen auf uns zukommen werden. Neue Technologien wie künstliche Intelligenz (KI), die zunehmende Abhängigkeit von IT-Lieferketten und ausgelagerten Dienstleistungen sowie ein sich wandelndes regulatorisches und rechtliches Umfeld können in relativ kurzer Zeit neue Risiken und Schadensszenarien hervorbringen."

Fortschritte in der Cybersicherheit wie KI-gestützte Erkennungstechnologien schaffen neue Möglichkeiten, Cyberkriminellen einen Schritt voraus zu bleiben, sagt **Michael Daum, Global Head of Cyber Claims bei Allianz Commercial.**

„Bis vor kurzem war es für Unternehmen sehr schwierig, ihre Cyberabwehr so auszubauen, dass die Wahrscheinlichkeit eines erfolgreichen Angriffs minimiert wird. In der Vergangenheit waren die Cyberkriminellen im Vorteil. Jetzt gibt es Werkzeuge und Prozesse, mit denen jedes Unternehmen sein Schicksal besser selbst in die Hand nehmen kann", so **Daum.**

„Das Risiko lässt sich zwar nicht vollständig ausschalten, doch es gab nie einen besseren Zeitpunkt, um in erfolgreiche Abwehrmaßnahmen zu investieren. Unternehmen haben heute mehr Möglichkeiten denn je, ihre Cyberrisiken aktiv zu beeinflussen und zu mindern."

Maximusdn / Adobe Stock

> In der Vergangenheit waren die Cyberkriminellen im Vorteil. Jetzt gibt es Werkzeuge und Prozesse, mit denen jedes Unternehmen sein Schicksal besser selbst in die Hand nehmen kann

ERKENNUNG, REAKTION UND SCHULUNG

Wachsende Lücke: Unternehmen mit Cyberversicherungen werden resilienter

Der stabile Trend bei den Cyber-Versicherungsschäden seit Jahresanfang 2025 steht im Gegensatz zur allgemeinen Bedrohungslandschaft. Im Jahr 2024 setzte sich der Aufwärtstrend bei Ransomware-Angriffen fort. IBM[29]. zufolge stieg die Zahl der aktiven Ransomware-Gruppen in den ersten sechs Monaten des Jahres 2024 um 56 Prozent. Im vergangenen Jahr wurde auch ein neuer Rekord bei den dem Internet Crime Complaint Center des FBI (IC3) gemeldeten Verlusten durch Internetkriminalität verzeichnet – 16,6 Milliarden US-Dollar[30].

Was die Cyberresilienz angeht, wird die Kluft zwischen versicherten und nicht versicherten Unternehmen immer größer. Wie Zahlen aus der Versicherungsbranche zeigen, sind die Cyber-Versicherungsansprüche zum Beispiel in Deutschland innerhalb von vier Jahren um rund 70 Prozent gestiegen – und damit deutlich weniger stark als die Cyberkriminalität insgesamt, die laut BITKOM im gleichen Zeitraum[31] um 250 Prozent zugenommen hat.

Die wachsende Kluft zwischen versicherten und nicht versicherten Unternehmen spiegelt das gestiegene Bewusstsein der Versicherungsnehmer für Cyberrisiken sowie ihre Maßnahmen zur Minderung dieser Risiken wider. Viele dieser Maßnahmen sind eine Voraussetzung für die Gewährung von Deckungsschutz. Gleichzeitig verdeutlicht diese Kluft die Effektivität der von den Versicherern bereitgestellten Beratungs- und Support-Dienstleistungen zur Risikominimierung und Unterstützung im Ernstfall, erläutert **Tresa Stephens, Head of Cyber, North America bei Allianz Commercial.**

„Unternehmen, die eine Cyberversicherung abschließen, sind in der Regel risikobewusst und eher bereit, in Cybersicherheit zu investieren. Cyberversicherungen bieten einen klaren Mehrwert, der über den Risikotransfer hinausgeht und sich auf Bedrohungsanalysen, Schadensverhütung, Schadensminderung und Reaktionsmaßnahmen im Ernstfall erstreckt, bereitgestellt durch Risikoberater und Schadenexperten. Die Allianz zum Beispiel bietet ihren Kunden Zugang zu subventionierten Tabletop Exercises – strategischen Notfallsimulationen, mit denen geprüft wird, wie gut eine Organisation auf bestimmte Cyberszenarien vorbereitet ist“, so **Stephens.**

Der WEF Global Cybersecurity Outlook 2025[32] bestätigt, dass eine Versicherung zu einer besseren Cyberresilienz von Unternehmen beiträgt: Unter den als hoch resilient eingestuften Unternehmen gaben nur 7 Prozent an, keine Cyberversicherung zu haben.

Seventyfour / Adobe Stock

JonoErasmus / Adobe Stock

ERKENNUNG, REAKTION UND SCHULUNG

Gut vorbereitet mit Tabletop Exercises

Ein von **Allianz Commercial** vor kurzem bearbeiteter Cyber-Schadensfall verdeutlicht den Wert von Tabletop Exercises. Der Versicherte wurde nur wenige Wochen nach der Teilnahme an einer Notfallsimulation Opfer eines Cyberangriffs. Dadurch war das Response-Team gut vorbereitet und konnte den Schaden erfolgreich eindämmen, berichtet **Caitlin Ewing, Complex Claims Analyst bei Allianz Commercial.**

„Tabletop Exercises bereiten Unternehmen auf Cybervorfälle vor und stärken ihr Vertrauen in ihre Notfallpläne. Unternehmen unterliegen einem ständigen Wandel und auch die Bedrohungslage verändert sich permanent. Regelmäßige Resilienztrainings und Vorbereitungen tragen dazu bei, dass die Betroffenen in Krisensituationen kompetent handeln können“, erklärt **Ewing.**

Tabletop Exercises sind ein besonders hilfreiches Instrument, um Unternehmen dabei zu unterstützen, sich auf Betriebsunterbrechungen durch einen Cybervorfall vorzubereiten und diese zu minimieren. Allerdings nutzen nicht alle Unternehmen dieses Instrument routinemäßig, sagt **Tresa Stephens, Head of Cyber, North America bei Allianz Commercial:**

„Eine gute Planung und Leitlinien für den Ernstfall sind unverzichtbar. Menschen verlassen Unternehmen; Systeme und Lieferanten ändern sich. Daher ist es wichtig, einen Notfallplan zu haben, diesen regelmäßig zu testen, zu aktualisieren und in die Unternehmenskultur zu integrieren. Das sollte Priorität haben.“

> Eine gute Planung und Leitlinien für den Ernstfall sind unverzichtbar. Menschen verlassen Unternehmen; Systeme und Lieferanten ändern sich. Daher ist es wichtig, einen Notfallplan zu haben, diesen regelmäßig zu testen, zu aktualisieren und in die Unternehmenskultur zu integrieren

ERKENNUNG, REAKTION UND SCHULUNG

Ransomware-Angriffe verdeutlichen Bedarf an Ausweichlösungen zur Sicherstellung der Betriebsfähigkeit

Die jüngsten Cyberangriffe auf Einzelhändler insbesondere in Großbritannien und den USA verdeutlichen die potenziell katastrophalen Auswirkungen von Betriebsunterbrechungen auf Unternehmen und die Notwendigkeit einer robusten Planung für die Aufrechterhaltung des Geschäftsbetriebs nach Cybervorfällen.

Wie die Schadensanalysen von Allianz Commercial zeigen, sind Betriebsunterbrechungen weiterhin der größte Treiber von Cyberschäden, mit einem Anteil von über 50 Prozent am Gesamtwert der Schadensfälle. Im diesjährigen **Allianz Risk Barometer** waren Cybervorfälle und Betriebsunterbrechungen die Geschäftsrisiken, die Unternehmen weltweit am meisten Sorge bereiten.

Die jüngsten Angriffe auf Einzelhändler ähnelten sich zwar alle, hatten jedoch unterschiedlich schwerwiegende Störungen des Geschäftsbetriebs zur Folge. Der Angriff auf Marks & Spencer im April 2025 wird den britischen Einzelhändler laut Ergebniserklärungen voraussichtlich rund 300 Millionen Pfund[33] an entgangenen Gewinnen durch monatelange Störungen seiner Lagerhaltungssysteme und seines Online-Vertriebs kosten. Beim Angriff[34] auf Coop wurden die Daten von rund sechs Millionen Kunden gestohlen. Außerdem wurden die Lieferketten der britische Supermarktkette erheblich gestört, was zu leeren Regalen in vielen Filialen führte. Berichten zufolge gelang es dem Unternehmen jedoch, den Angriff zu stoppen, bevor die Hacker seine Systeme verschlüsseln konnten.

Betriebsunterbrechungsschäden stehen in engem Zusammenhang mit der frühzeitigen Identifizierung von und Reaktion auf Bedrohungen sowie der Geschäftskontinuitätsplanung. Durch eine frühzeitige Identifizierung und Eindämmung von Sicherheitsvorfällen lassen sich die Kosten von Betriebsunterbrechungen deutlich reduzieren. Dagegen können eine schlechte Kommunikation, mangelnde Koordination und Unentschlossenheit die Auswirkungen eines Ransomware-Angriffs verlängern und zu größeren finanziellen Einbußen und Reputationsschäden führen. Betriebsunterbrechungen durch Cybervorfälle unterscheiden sich stark von traditionellen Sachschadenereignissen. Während diese in der Regel auf einen Standort beschränkt bleiben, kann ein Cyberangriff schnell auf eine gesamte Organisation übergreifen. Zudem haben Kunden und Geschäftspartner in der Regel weniger Verständnis für Cybervorfälle als für Naturkatastrophen.

Bei der Incident-Response-Planung müssen sich Unternehmen mit den potenziellen Auswirkungen von Systemverlusten und Lieferketten- oder Vertriebsstörungen sowie möglichen Eindämmungsmaßnahmen beschäftigen, erklärt **Michael Daum, Global Head of Cyber Claims bei Allianz Commercial.**

„Unternehmen sollten im Rahmen ihrer Incident-Response- und Geschäftskontinuitätsplanung Strategien entwickeln, um auch nach einem Cybervorfall den Betrieb aufrechtzuerhalten und ihre Kunden weiter zu bedienen. Es ist sinnvoll, diese Strategien im Voraus festzulegen und sich durch Übungen, Simulationen und Schulungen auf mögliche Betriebsunterbrechungen vorzubereiten" so **Daum.**

„Für die Incident-Response-Planung ist es auch hilfreich, sich einen guten Überblick über bestehende Abhängigkeiten zu verschaffen und für den Fall, dass es zu Lieferunterbrechungen kommt, entsprechende Pläne bereitzuhalten – oder zumindest mögliche Maßnahmen zur Minderung der Auswirkungen in Betracht zu ziehen. Eine frühzeitige Vorbereitung auf mögliche Betriebsunterbrechungen – und ein gutes Verständnis aller Versicherungsanforderungen – kann dazu beitragen, die Auswirkungen derartiger Ereignisse zu minimieren und die Kosten zu begrenzen", ergänzt **Caitlin Ewing, Complex Claims Analyst bei Allianz Commercial.**

Viele Unternehmen tun sich immer noch schwer damit, ihr Cyberrisiko zu quantifizieren, insbesondere in Bezug auf Betriebsunterbrechungen.

„Durch die Vielschichtigkeit der Cyberproblematik und die vielen zusammenwirkenden Faktoren und Variablen kann dieses Risiko nur schwer zu beziffern sein. Makler, Versicherer und externe Dienstleister können die Unternehmen jedoch mit Daten zu wahrscheinlichen Schäden und Erfahrungswerten unterstützen", sagt **Tresa Stephens, Head of Cyber, North America bei Allianz Commercial.**

Der Mangel an IT-Fachkräften und die wachsende Cyberkompetenzlücke machen es schwerer, die potenziellen Auswirkungen eines Cybervorfalls zu verstehen und zu quantifizieren. Die International Data Corporation[35] prognostiziert, dass bis 2026 neun von zehn Unternehmen weltweit vom IT-Fachkräftemangel betroffen sein werden, was Verluste in Höhe von 5,5 Billionen US-Dollar zur Folge haben könnte.

ERKENNUNG, REAKTION UND SCHULUNG

Transformative Kraft der KI-gestützten Bedrohungserkennung

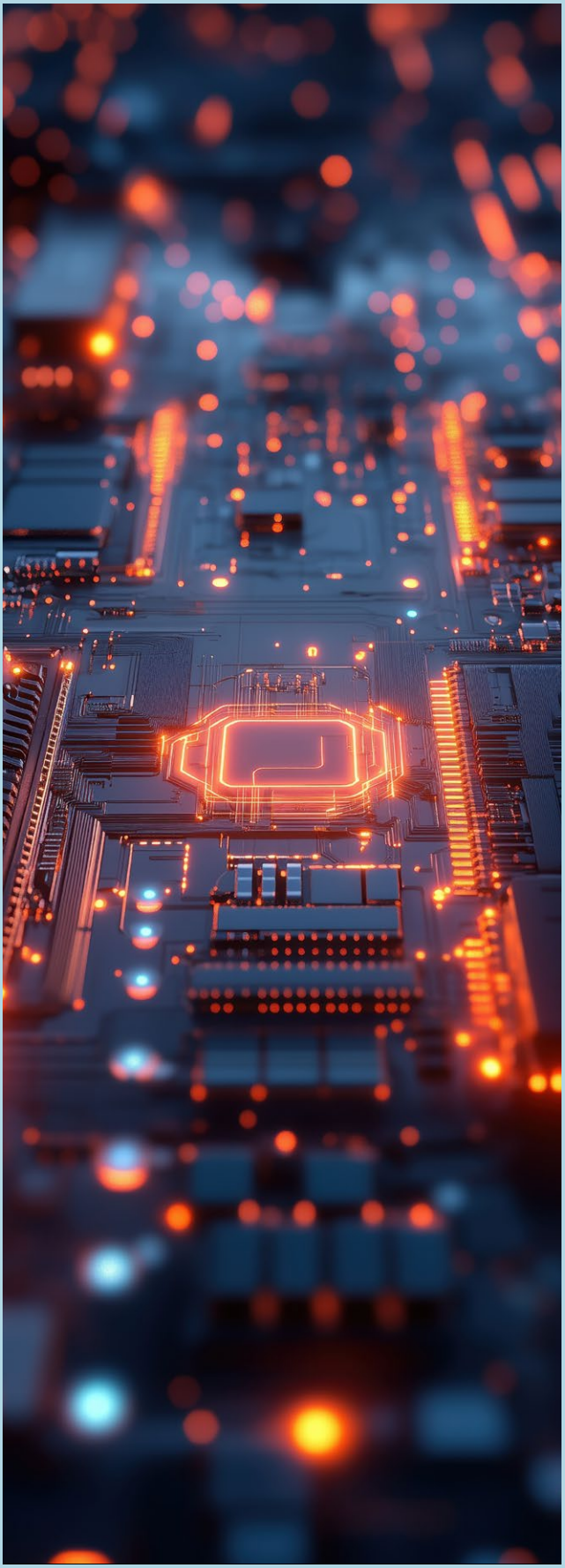
Künstliche Intelligenz (KI) hebt die Cybersicherheit auf eine neue Ebene, indem sie die Erkennung und Reaktion auf Bedrohungen beschleunigt und automatisiert und Unternehmen hilft, Schwachstellen zu identifizieren und ihre Cyberresilienz zu stärken.

Wie der Cost of a Data Breach Report 2024 von IBM[36] zeigt, hatten Unternehmen, die KI-basierte Sicherheits- und Automatisierungslösungen nutzen, im Schnitt 2,2 Millionen US-Dollar weniger an Schadenskosten als Unternehmen, die keine derartigen Lösungen einsetzen. Die Umfrage kam zu dem Ergebnis, dass zwei von drei Unternehmen im Jahr 2024 KI-basierte Sicherheits- und Automatisierungslösungen für die IT-Sicherheit nutzten.

„KI verschafft Unternehmen in der Verteidigung gegen Angriffe derzeit einen Vorteil. Sie müssen dafür allerdings in KI-gestützte Erkennungstools investieren. Tun sie das nicht, liegt der KI-Vorteil bei den Angreifern“, warnt **Michael Daum, Global Head of Cyber Claims bei Allianz Commercial.**

Auch **Rishi Baviskar, Global Head of Cyber Risk Consulting bei Allianz Commercial,** ist der Ansicht, dass KI eine zunehmend wichtige Rolle in der Cybersicherheit spielt:

„Angreifer nutzen KI für ihre Cyberangriffe, aber auch Unternehmen setzen sie zunehmend zum Schutz ihres Betriebs ein, zum Beispiel, um den Inhalt potenzieller Phishing-E-Mails zu analysieren oder Muster in Code und Metadaten zu erkennen. KI kann Anomalien im Softwarecode oder potenzielle Malware erkennen und ungewöhnliches Verhalten identifizieren. KI-gestützte Lösungen wie SOAR-Tools (Security Orchestration, Automation and Response) ermöglichen es Unternehmen, schneller auf Sicherheitsbedrohungen zu reagieren, wodurch die Zeit zwischen Erkennung und Eindämmung verkürzt wird und Betriebsunterbrechungen reduziert werden.“



narin_nonthamand / Adobe Stock

ERKENNUNG, REAKTION UND SCHULUNG

Regulierung erhöht Anforderungen an Cyberresilienz

Neue Vorschriften sollen die Cyberresilienz erhöhen, was die IT-Lieferketten stärken und die Auswirkungen von Ransomware-Angriffen verringern dürfte.

Datenschutzgesetze wie die Datenschutz-Grundverordnung (DSGVO) der EU sind mittlerweile in den meisten wichtigen Märkten fest etabliert, und Unternehmen setzen diese Vorschriften im Allgemeinen gut um. Nun möchte die EU ihre digitale Strategie jedoch stärken und dabei den Schwerpunkt auf Cybersicherheit sowie auf neue Bereiche wie künstliche Intelligenz (KI) legen.

Zusammen mit DORA (Digital Operational Resilience Act), das die digitale operationale Resilienz im Finanzsektor durch Vorgaben für ein robustes IT-Risikomanagement, Vorfallmeldungen und Resilienztests stärken soll, legt die überarbeitete Network and Information Security Directive (NIS2) die Latte für die Cybersicherheit in der EU deutlich höher. Die Richtlinie, die derzeit von den Mitgliedstaaten umgesetzt wird, schafft einen gemeinsamen Rahmen für Cybersicherheit in 18 kritischen Sektoren, einschließlich der zugehörigen Lieferketten. Unternehmen, die unter die NIS2 fallen, müssen geeignete Maßnahmen zum Management von Cybersicherheitsrisiken ergreifen und die zuständigen nationalen Behörden über schwerwiegende Vorfälle informieren.

„NIS2 wird viele Unternehmen vor Herausforderungen stellen, aber ich sehe es als Chance. Wie DORA ist auch NIS2 ein hervorragendes Gesetz, das einen Paradigmenwechsel in der Art und Weise darstellt, wie EU-Regierungen mit Cyberrisiken umgehen“, sagt **Robin Kroha, Chief Information Security Officer & Head of Global Protection and Resilience bei Allianz Services.**

NIS2 wird die Cybersicherheitsstandards für viele Unternehmen erhöhen, darunter auch mittelständische Unternehmen, die derzeit nicht über angemessene Cybersicherheits- und Risikomanagementsysteme verfügen, so **Kroha:**

„Viele Unternehmen – insbesondere mittelständische Unternehmen – sind auf solche Vorschriften völlig unvorbereitet. Sie verfügen nicht über viele der bei Großunternehmen üblichen Risikomanagementsysteme wie Business Continuity Management, Krisenmanagement, Informationssicherheit und IT-Sicherheitsmanagement.“

ImageFlow/ Adobe Stock

Kroha zufolge wird die Ausweitung der Cybersicherheitsanforderungen im Rahmen von NIS2 die Cyberresilienz in Europa erheblich stärken. NIS2 verpflichtet Unternehmen zur Umsetzung vieler Best-Practice-Verfahren, die dazu beitragen, die Auswirkungen eines Cyberangriffs zu mindern, wie zum Beispiel Backup-Strategien, Maßnahmen für die Erkennung und Reaktion auf Bedrohungen sowie Business-Continuity-Planung.

„NIS2 wird sich sofort positiv auswirken. Das durchschnittliche mittelständische Unternehmen verfügt nicht über etablierte Managementsysteme im Cyberbereich. Am besten aufgestellt sind die Unternehmen, bei denen eine starke Cybersicherheit und digitale Resilienz fest in der Kultur verankert sind“, sagt **Kroha.**

ERKENNUNG, REAKTION UND SCHULUNG

Trends am Versicherungsmarkt

Der weltweite Cyberversicherungsmarkt wird sich mehr als verdoppeln, auf knapp 30 Milliarden US-Dollar.

„Cyberkriminelle werden immer wieder neue potenzielle Angriffsziele ins Visier nehmen, und je mehr Unternehmen Opfer derartiger Angriffe werden, desto größer wird die Nachfrage nach Cyberversicherungen sein, vor allem unter mittelständischen Unternehmen und in Teilen der Welt, in denen bislang noch nicht so viel in die Minderung von Cyberrisiken investiert wird. Im Zuge ihrer zunehmenden Digitalisierung werden Unternehmen ihre digitalen Risiken und Vermögenswerte natürlich ähnlich gut managen und schützen wollen wie ihre physischen Vermögenswerte“, sagt **Tresa Stephens, Head of Cyber, North America bei Allianz Commercial.**

Die Verbreitung von Cyberversicherungen ist nach wie vor relativ gering, spielt aber eine wichtige Rolle beim Aufbau von Resilienz in Zeiten rascher technologischer und regulatorischer Veränderungen. Viele Unternehmen sind sich jedoch nach wie vor nicht bewusst darüber, wie umfassend der Deckungsschutz einer Cyberversicherung ist, der auch die Kosten für die Reaktion auf Vorfälle, Betriebsunterbrechungen und Datenschutzverletzungen aufgrund einer Vielzahl von Cybervorfällen abdeckt, so **Stephens.**

Laut einer Umfrage[37] des World Economic Forum sind 71 Prozent der großen Unternehmen zuversichtlich, dass ihre Cyberversicherung potenzielle Schäden aufgrund von Cybervorfällen ausreichend abdeckt. Bei kleineren Unternehmen sind es nur 35 Prozent.

„Die Voraussetzungen für das fortgesetzte Wachstum des Cyberversicherungsmarktes und die Übernahme eines breiteren Spektrums von Risiken durch die Versicherer sind gut. Ein besseres Bewusstsein für und Investitionen in Cybersicherheit reduzieren die grundlegenden Risiken, während Cyber-Risikomodellierung und Rückversicherungsschutz Versicherern helfen, ihr Gesamtrisiko besser zu steuern“, sagt **Stephens.**

> Die Voraussetzungen für das fortgesetzte Wachstum des Cyberversicherungsmarktes und die Übernahme eines breiteren Spektrums von Risiken durch die Versicherer sind gut

Photographee.eu / Adobe Stock

Referenzen

1 Qantas, Qantas cyber incident, 2. Juli 2025
2 Reuters, UK police arrest four over cyber-attacks on M&S, Co-op and Harrods, 10. Juli 2025
3 CrowdStrike, CrowdStrike 2025 Global Threat Report
4 BlackFog, BlackFog report reveals record number of ransomware attacks from January to March, 9. April 2025
5 Verizon, 2025 Data Breach Investigations Report
6 World Economic Forum, Global Cybersecurity Outlook 2025
7 IBM, IBM Report: Escalating data breach disruption pushes costs to new highs, 30. Juli 2024
8 Sophos, The State of Ransomware 2025
9 CNN, AT&T says personal data from 73 million current and former account holders leaked onto dark web, 30. März 2024
10 CNN, AT&T may pay customers up to $7,500 in $177 million data breach settlement, 16. August 2025
11 Verizon, 2025 Data Breach Investigations Report
12 Cybereason, TTP Briefing: Januar - Mai 2025
13 Verizon, 2025 Data Breach Investigations Report
14 CrowdStrike, How to navigate the 2025 identity threat landscape, 31. März 2025
15 CrowdStrike, CrowdStrike 2025 Threat Hunting Report
16 CrowdStrike, 2025 Global Threat Report
17 Cybereason TTP Briefing: Januar - Mai 2025
18 Fred Heiding, Simon Lermen, Andrew Kao, Bruce Schneier, Arun Vishwanath, Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects, 30. November 2024
19 Computer Weekly, Luxury retailer LVMH says UK customer data was stolen in cyber-attack, 14. Juli 2025
20 BBC, Jaguar Land Rover production severely hit by cyber-attack, 2. September 2025
21 World Economic Forum, Global Cybersecurity Outlook 2025
22 CrowdStrike, CrowdStrike 2025 Threat Hunting Report: AI Becomes a Weapon and a Target, 4. August 2025
23 RetailTechInnovationHub, H&M all apologies as fashion and homeware retailer reports major IT outage affecting payments in stores, 4. Juni 2025
24 Europäisches Parlament, Data leak affecting owners of Volkswagen Group electric vehicles, 16. Januar 2025
25 Reuters, How warning signs hinted at Spain's unprecedented power outage, 2. Mai 2025
26 Duane Morris, DMCAR Trend #7 – Data breaches gives rise to an unprecedented number of class action filings, 21. Januar 2025
27 BakerHostetler, Comprehensive State Privacy Laws
28 Precedence Research, Managed Detection and Response (MDR) Market Size, Share and Trends 2025 to 2034
29 IBM, Research finds 56% increase in active ransomware groups, 18. November 2024
30 FBI, Federal Bureau of Investigation Internet Crime Report 2024
31 Bitkom, Wirtschaftsschutz 2024, Berlin, 28. August 2024
32 World Economic Forum, Global Cybersecurity Outlook 2025
33 M&S, Full Year Results for the 52 Weeks Ended 29 March 2025
34 BBC, Co-op boss confirms all 6.5m members had data stolen, 16. Juli 2025
35 International Data Corporation, IT skills shortage expected to impact nine out of ten organizations by 2026 with a cost of $5.5 trillion in delays, quality issues and revenue loss, according to IDC, 14. Mai 2024
36 IBM, Cost of a Data Breach Report 2024
37 World Economic Forum, Global Cybersecurity Outlook 2025

About Allianz Commercial

Allianz Commercial is the center of expertise and global line of Allianz Group for insuring mid-sized businesses, large enterprises and specialist risks. Among our customers are the world's largest consumer brands, financial institutions and industry players, the global aviation and shipping industry as well as family-owned and medium enterprises which are the backbone of the economy. We also cover unique risks such as offshore wind parks, infrastructure projects or film productions.

Powered by the employees, financial strength, and network of the world's #1 insurance brand, as ranked by Interbrand, we work together to help our customers prepare for what's ahead: They trust us to provide a wide range of traditional and alternative risk transfer solutions, outstanding risk consulting and multinational services as well as seamless claims handling.

The trade name Allianz Commercial brings together the large corporate insurance business of Allianz Global Corporate & Specialty (AGCS) and the commercial insurance business of national Allianz Property & Casualty entities serving mid-sized companies. We are present in over 200 countries and territories either through our own teams or the Allianz Group network and partners. In 2023, the integrated business of Allianz Commercial generated around €18 billion in gross premium globally.

Weitere Informationen und Ansprechpartner

Für weitere Informationen zu Cyberversicherungen wenden Sie sich bitte an Ihre regionalen Ansprechpartner bei Allianz Commercial.

commercial.allianz.com

Email: az.commercial.communications@allianz.com

Disclaimer & Copyright

Copyright © 2025 Allianz Commercial / Allianz Global Corporate & Specialty SE. All rights reserved.

The material contained in this publication is designed to provide general information only. While every effort has been made to ensure that the information provided is accurate, this information is provided without any representation or warranty of any kind about its accuracy and neither Allianz Global Corporate & Specialty SE, nor any other company of Allianz Group can be held responsible for any errors or omissions.

All descriptions of insurance coverage are subject to the terms, conditions and exclusions contained in the individual policy. Any queries relating to insurance cover should be made with your local contact in underwriting and/or broker. Any references to third-party websites are provided solely as a convenience to you and not as an endorsement by Allianz of the content of such third-party websites. Neither Allianz Global Corporate & Specialty SE, nor any other company of Allianz Group is responsible for the content of such third-party websites and neither Allianz Global Corporate & Specialty SE, nor any other company of Allianz Group does make any representations regarding the content or accuracy of materials on such third-party websites.

Allianz Global Corporate & Specialty SE, Königinstraße 28, 80802 Munich, Germany.

Commercial Register: Munich, HRB 208312

September 2025