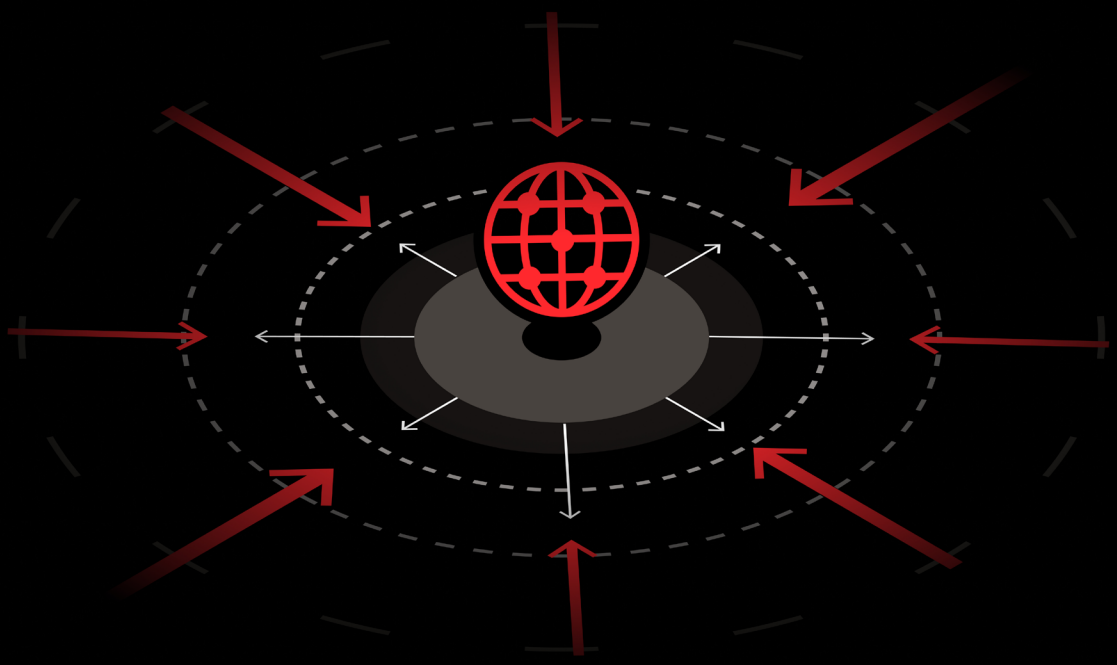
Weltweite Studie zum Thema Security

Die KI-Temposteuer

Warum sich die schnellsten Unternehmen am langsamsten erholen



fastly

Inhalt

Zusammenfassung

Unternehmen rasen aufgrund der massiven Skalierung der KI-Einführung in Organisationen auf eine selbst verursachte Cybersicherheitskrise zu. Indem sie KI-Innovationen nutzen, ohne darüber nachzudenken, wie sie ihre Sicherheit stärken und einen strategischen Plan zur Umsetzung ganzheitlicher Lösungen entwickeln können, entdecken Unternehmen, die sich unbedingt als „KI-Vorreiter“ bezeichnen wollen, dass glänzende neue Funktionen ohne Infrastrukturschutz mehr Probleme schaffen als lösen.

Um zu verstehen, was Unternehmen in der realen Welt erleben, hat Fastly seit September 2025 eine Partnerschaft mit der Forschungsagentur Sapio geschlossen, um 2.000 IT-Entscheidungsträger in 21 Regionen zu befragen, die im Bereich Cybersicherheit tätig sind. Die Ergebnisse zeigen eine unangenehme Wahrheit auf: Die Organisationen, die am aggressivsten bei der Einführung von KI sind, haben am meisten mit Sicherheitsstörungen zu kämpfen.

Das sind die Ergebnisse:

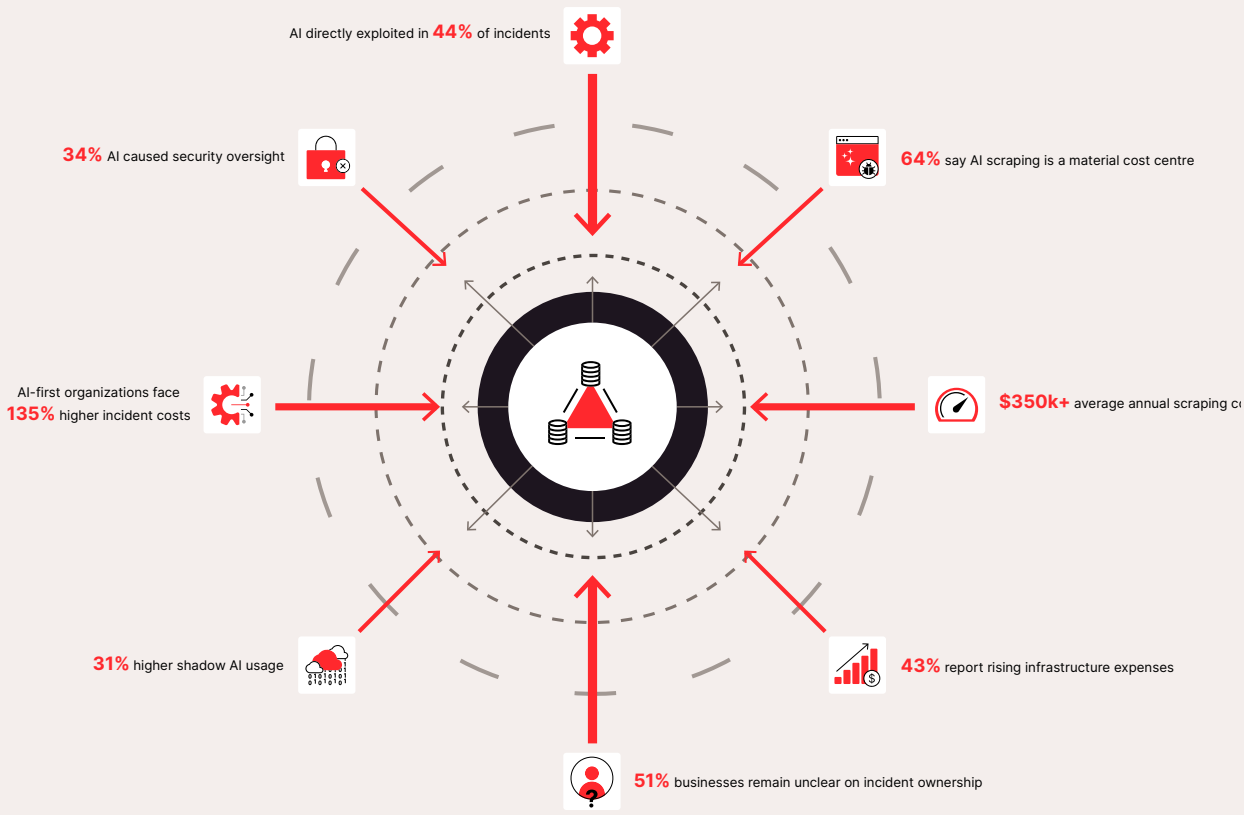
Unternehmen zahlen eine hohe KI-Steuer.

Mehr als 75 % der Unternehmen, die sich als KI-orientiert bezeichnen (d. h. sie haben KI von Anfang an, ob öffentlich oder informell, in ihre Kernprozesse integriert), benötigen im Durchschnitt 80 Tage länger, um sich von Sicherheitsvorfällen zu erholen, als vergleichbare Unternehmen. Bei KI-orientierten Unternehmen dauert die Erholung im Durchschnitt über alle Regionen hinweg 6,8 Monate, bei allen anderen 3,9 Monate.

Die finanziellen Auswirkungen sind für KI-Unternehmen ebenfalls schmerzhafter: Störungen kosten KI-orientierte Unternehmen 135 % mehr als vergleichbare Unternehmen und belaufen sich auf 3,13 % des Jahresumsatzes, verglichen mit 1,33 % bei Unternehmen, die nicht KI-orientiert sind – das entspricht einem Umsatzverlust in Milliardenhöhe. Fast die Hälfte (44 %) berichtet, dass KI in ihrem jüngsten Vorfall direkt ausgenutzt wurde.

Fortsetzung auf der nächsten Seite

Die sich ausweitende Angriffsfläche: Die KI breitet sich schneller aus, als die Sicherheit mithalten kann



Die Infrastruktur wird schneller erweitert, als die Abwehr mithalten kann. Auch die Schatten-KI hat in den letzten 12 Monaten stark zugenommen. Mehr als ein Drittel (34%) der KI-orientierten Unternehmen geben an, dass die direkte Ausnutzung von KI zu ihrer letzten Störung beigetragen hat. Weitere 30 % geben an, dass der Einsatz von KI zu einem Versehen geführt hat, das zu der Störung beigetragen hat. In der Zwischenzeit hat sich das KI-Scraping für mehr als zwei Drittel (64 %) der Unternehmen zu einem wesentlichen Kostenfaktor entwickelt, wobei die durchschnittlichen jährlichen Infrastrukturkosten um fast 350.000 US-Dollar gestiegen sind. Darüber hinaus berichteten 43 % der Befragten über steigende Infrastrukturkosten. Das ist nicht nur ein finanzielles Problem: 40 % hatten auch mit betrieblichen Störungen zu kämpfen und 29 % berichteten über verschlechterte Kundenerlebnisse.

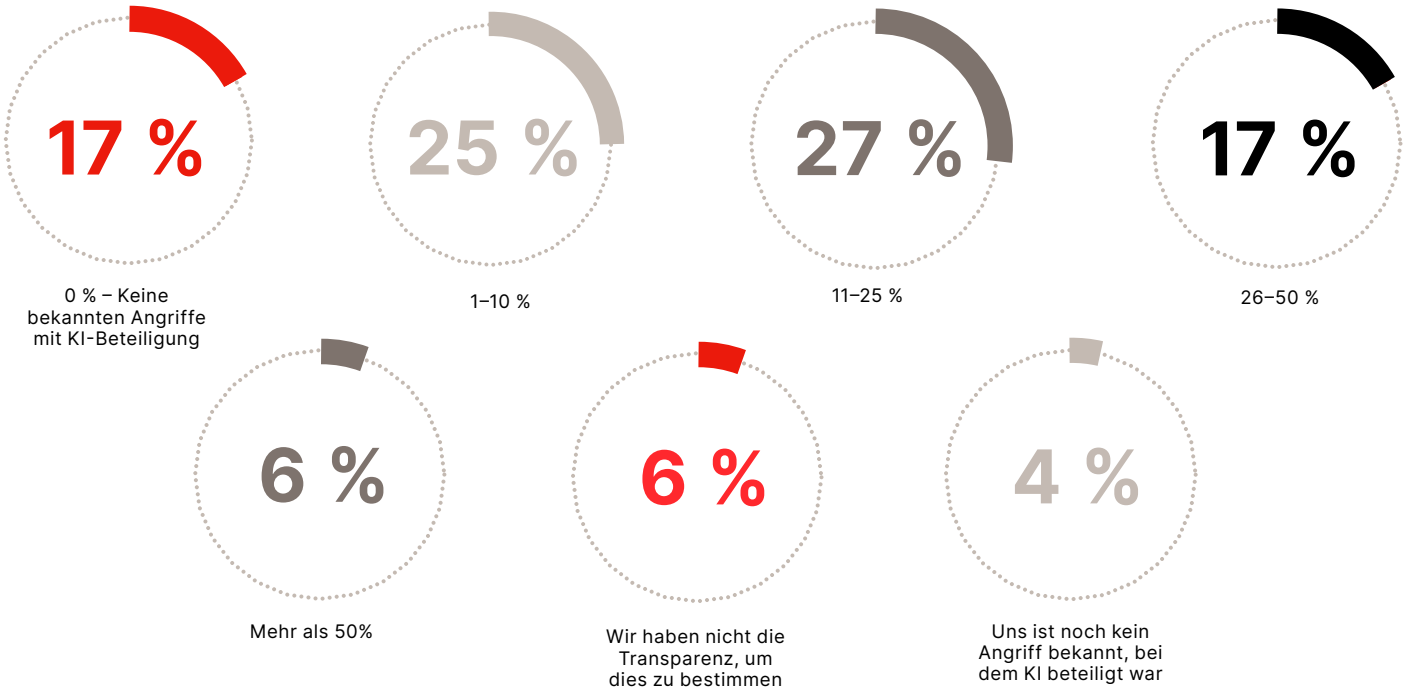
Niemand weiß, wer tatsächlich verantwortlich ist, wenn etwas schiefgeht. Die Hälfte der KI-orientierten Unternehmen (51 %) berichtet von Verwirrung darüber, wer die Störungsreaktion übernimmt, verglichen mit 23 % der Unternehmen, die KI nicht als oberste Priorität haben. Die traditionelle Verantwortlichkeitsstruktur verliert rapide an Bedeutung, da Teams heute sowohl Menschen als auch selbst denkende, selbst lernende und selbstständig handelnde KI-Agenten umfassen können.

Es gibt einen Lichtblick in den Daten. Das Gesamtvolumen der Störungen für alle Unternehmen ist mit durchschnittlich 41 Störungen pro Unternehmen gleich geblieben, und die Erholungsmöglichkeiten haben sich verbessert. Die durchschnittliche Erholungszeit sank um mehr als einen Monat von 7,34 Monaten im letzten Jahr auf 6,08 Monate. Die durch Störungen verursachten Umsatzeinbußen sanken von 2,98 % auf 2,68 % des Jahreseinkommens. Unternehmen, die in die Nachbereitung von Störungen (52 %) und die Reaktionsautomatisierung (43 %) investiert haben, dürften zu denjenigen gehören, die positive Ergebnisse verzeichnen.

Die Investitionsprioritäten verlagern sich hin zur Bewältigung KI-spezifischer Risiken. Agentische Tools zur Erkennung führen mit 56 % die Sicherheitsausgaben für agentenbasierte KI-Infrastruktur an, gefolgt von API-Sicherheit (55 %) und Webanwendungs-Firewalls (54 %). Drei Viertel (75 %) befürchten DDoS-Angriffe auf KI-Agenten, während 53 % einräumen, dass ihnen KI-spezifisches Sicherheits-Know-how fehlt.

Der Pfad in die Zukunft erfordert einen Mentalitätswandel. Unternehmen müssen die Aktivitäten von KI-Crawlern überwachen, die Einführung von Schatten-KI antizipieren und die Perimeterverteidigung verstärken, bevor sie die Angriffsfläche erweitern. Dies führt auch zu einem Umdenken bei Lösungen für den Web-App- und API-Schutz. Unternehmen beginnen, diese als geschäftskritische Infrastruktur und nicht als Nischenlösungen zu betrachten.

Unternehmen, die auf KI setzen, leiden häufig unter KI-bezogenen Kompromissen



Das AI-first-Paradoxon

Künstliche Intelligenz birgt das Potenzial, die Produktivität zu steigern, doch wie bei jeder Schlüsseltechnologie bedarf es eines strategischen Gleichgewichts zwischen Innovation und Sicherheit. Organisationen, die sich als „KI-Vorreiter“ positionieren und um die Integration künstlicher Intelligenz wetteifern, müssen dieses Gleichgewicht finden, um die Vorteile der KI wirklich nutzen zu können. Derzeit benötigen diese Unternehmen durchschnittlich 6,8 Monate, um sich von Cybersicherheitsstörungen zu erholen. Das sind 80 Tage länger als bei vergleichbaren Unternehmen, die nicht auf KI setzen und sich in nur etwa 4 Monaten erholen. Vor ihnen liegt noch ein steiniger Weg.

> „Die KI-Tools selbst werden zu privilegierten Bestandteilen Ihrer Infrastruktur, und genau das birgt das Risiko.“
>
> **– Marshall Erwin, CISO bei Fastly**

Innovation ist ein entscheidender Wettbewerbsvorteil. Jene Organisationen, die robuste Sicherheitsmaßnahmen zum Schutz von KI-Daten, Infrastruktur und Prozessen schaffen, werden besser für Innovationen aufgestellt sein als diejenigen, die Sicherheit als zweitranging ansehen. Störungen verursachen bei KI-orientierten Unternehmen 135 % höhere Kosten als bei Unternehmen ohne diesen Fokus. Die Erholungslücke führt direkt zu Umsatzeinbußen, verlängerten Ausfallzeiten und anhaltendem Reputationsschaden.

KI schafft ihre eigene Angriffsfläche

KI bringt mehr Komplexität, mehr Code und mehr Infrastruktur mit sich, die Unternehmen schützen müssen. Fast die Hälfte (44 %) der AI-first-Organisationen gibt an, dass KI bei ihrer jüngsten Sicherheitsstörung direkt ausgenutzt wurde, verglichen mit nur 6 % bei Organisationen, die KI nicht als oberste Priorität haben.

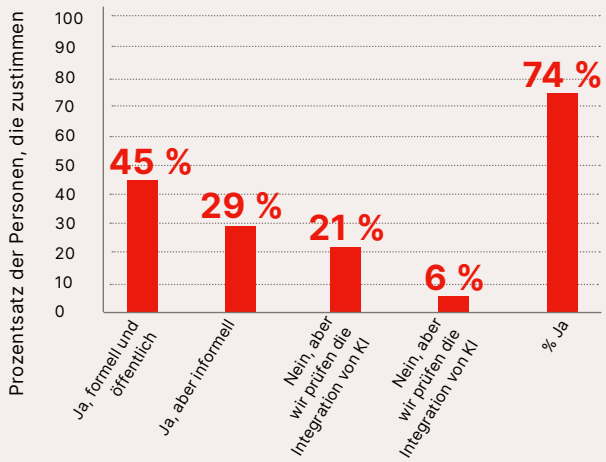
Eine offensichtliche Ursache liegt darin, dass das Sicherheitsteam nicht alles sehen kann. Schatten-KI (unautorisierte Tools, die Mitarbeiter ohne Genehmigung der IT-Abteilung einsetzen) ist bei einem Viertel der Mitarbeiter in KI-orientierten Unternehmen um 31 % höher, vermutlich weil die Kultur Innovation mit KI fördert. Für Marshall Erwin, CISO bei Fastly, sind offiziell eingeführte KI-Tools jedoch mindestens genauso problematisch wie Schatten-KI.

Genehmigte KI-Tools erhalten häufig weitreichende automatisierte Berechtigungen. Unternehmen, die bereits vor der Einführung von KI mit der Identitäts- und Zugriffsverwaltung zu kämpfen hatten, sehen sich nun mit einer Eskalation dieses Problems konfrontiert. „Diese Tools werden potenzielle Zugriffsrisiken erweitern“, warnt Erwin. „Die KI-Tools selbst werden zu privilegierten Bestandteilen Ihrer Infrastruktur, und genau das birgt das Risiko.“

Die Zahlen belegen diese Schlussfolgerung. Mehr als ein Drittel (34 %) der KI-orientierten Organisationen nennen den Einsatz von KI als einen Faktor für Sicherheitslücken, die zu ihrer letzten Sicherheitsverletzung beigetragen haben. Demgegenüber stehen 20 % in traditionellen Organisationen.

Stellen Sie sich KI-Tools als maschinelle Entitäten vor, die ihre eigene Identitätsverwaltung benötigen. Automatisierte Berechtigungen ermöglichen automatisierte Angriffe. Je eigenständiger diese Tools werden (d. h. je komplexer ihre autonomen Aufgaben), desto größer wird das Risiko.

Unternehmen, die sich selbst als KI-orientiert bezeichnen, benötigen länger, um sich von Sicherheitsstörungen zu erholen, als solche, die diesen Fokus nicht haben.



1 (Mitarbeiter, die nicht genehmigte KI-Tools verwenden)

Wie sich KI-Scraper auf das Geschäftsergebnis auswirken

Schatten-KI birgt die Gefahr des unbeabsichtigten Missbrauchs von KI innerhalb einer Organisation, aber es bestehen auch Risiken durch Dritte, die KI einsetzen. Diese böswilligen Akteure können die Inhalte einer Organisation mithilfe von Scraper-Bots angreifen. KI-Scraping kostet Unternehmen viel Geld, da es ihre Infrastruktur belastet.

Etwa zwei Drittel der Unternehmen (64 %) geben an, dass KI-gestütztes Web-Scraping zu einem wesentlichen Kostenfaktor geworden ist, wobei die Ausgaben im Durchschnitt jährlich über 348.000 US-Dollar betragen. Das belastet die Infrastrukturkosten und die Betriebsbudgets erheblich. Mehr als vier von zehn Unternehmen haben beobachtet, dass die Infrastrukturkosten mit der Zunahme der KI-Aktivitäten steigen. Weitere 40 % berichten von Betriebsstörungen, während 29 % mit Problemen bei der User Experience zu kämpfen haben. Langsame Ladezeiten, kaputte Funktionen und eine schlechtere Performance sind die Art von Problemen, die Kunden zu anderen Anbietern führen, wenn sie andauern.

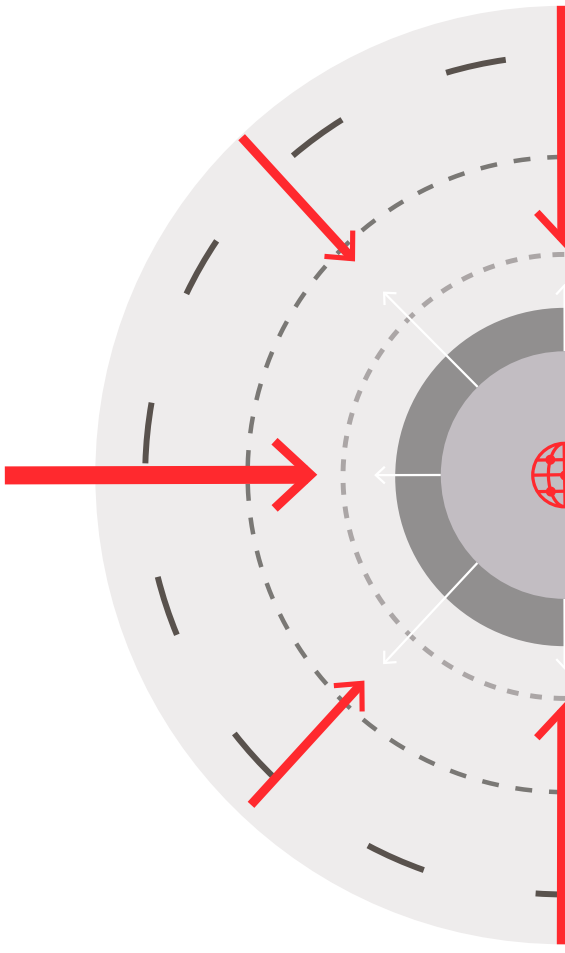
Altmodische externe Angriffstechniken können der KI-Infrastruktur erheblichen Schaden zufügen. Drei Viertel der Befragten in der Fastly-Umfrage befürchten, dass DDoS-Angriffe KI-Agenten treffen könnten. Das bedeutet, dass auch Unternehmen, die KI nicht intern einsetzen, darauf achten sollten, wie andere sie instrumentalisieren könnten.

Keines dieser Risiken sollte Unternehmen davon abhalten, KI einzusetzen, aber die Gewinner werden diejenigen sein, die innovativ sind und gleichzeitig ihre Sicherheitshaltung entsprechend anpassen. Das bedeutet entweder, die Fähigkeiten dafür zu finden (53 % geben zu, dass ihre Sicherheitsteams nicht über die KI-spezifische Expertise verfügen, um mit diesen Bedrohungen umzugehen) oder mit einem Drittanbieter zusammenzuarbeiten, der bei der Bewältigung der Risiken hilft.

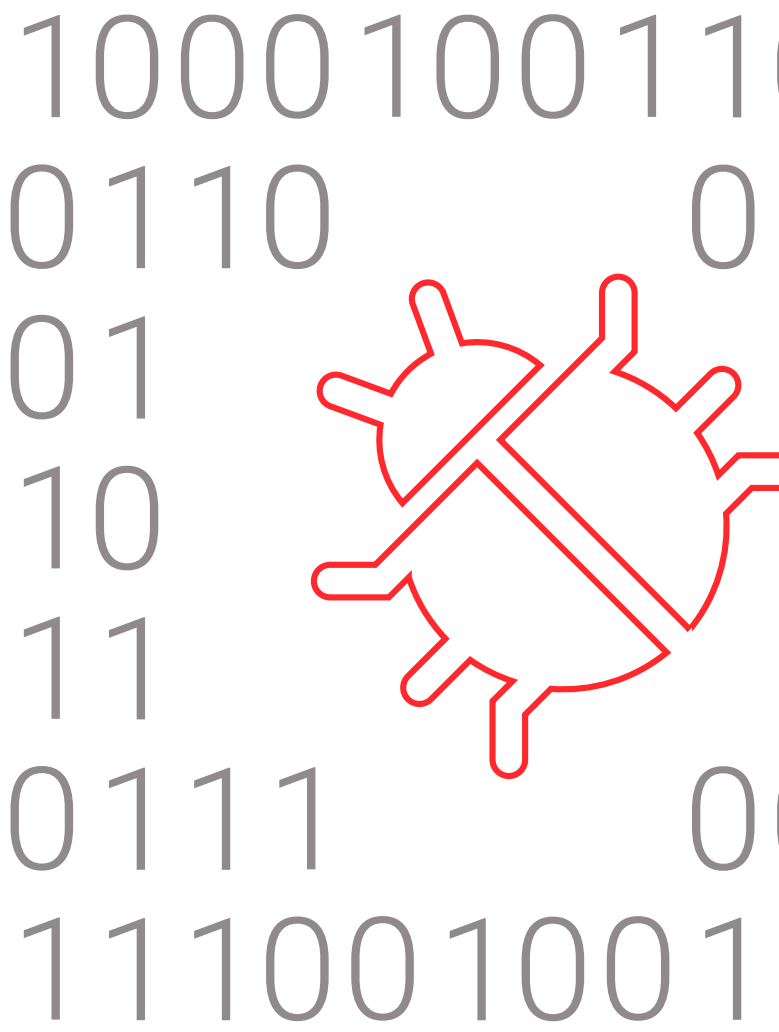
Web-App- und API-Schutz wird unerlässlich

Diese Gegebenheiten verändern die Art und Weise, wie Organisationen über ihre Sicherheitsmaßnahmen nachdenken. Web-App- und API-Schutz stand für einige Organisationen vielleicht einst weiter unten auf der Liste der Sicherheitstools, doch mittlerweile wird er zu einem wesentlichen Bestandteil ihrer Kerninfrastruktur. Er ist der Kontroll-Layer für die Verwaltung der Kosten und die Sicherung der APIs, die moderne digitale Services sowohl innerhalb als auch außerhalb einer Organisation unterstützen.

Unternehmen entscheiden mit ihren Ausgaben. Bei Investitionen in den Schutz der agentenbasierten Infrastruktur legen Organisationen den Schwerpunkt auf die Erkennbarkeit von Agenten (56 %), API-Sicherheit (55 %) und Web Application Firewalls (WAFs, 54 %). Diese nicht traditionellen Sicherheitskategorien sind eine direkte Antwort auf architektonische Muster, die vor zwei Jahren kaum existierten.



Wenn Bugs Sicherheitsverletzungen überwinden



Unsere Untersuchungen ergaben, dass die Zahl der Sicherheitsstörungen im Jahr 2025 unverändert blieb. Organisationen waren im Durchschnitt mit 41 bekannten Störungen konfrontiert, nur einer mehr als im Jahr 2024. Aber diese allgemeine Zahl hat kaum Aussagekraft. Was tatsächlich passiert, erzählt eine realistischere Geschichte.

Software-Bugs lösten 40 % der Sicherheitsvorfälle aus, gegenüber 33% im Jahr 2024. Damit rückte dieser Bereich vom zweiten auf den ersten Platz vor und verdrängte die bisherige Hauptursache (externe Angreifer) auf den zweiten Platz (39 %). Fehlkonfigurationen belegten mit 29 % den dritten Platz, gegenüber dem vierten Platz mit 25 % im letzten Jahr. Mehr denn je ringen Unternehmen mit Sicherheitsfehlern, die nichts mit ausgeklügelten Bedrohungsakteuren zu tun haben, sondern mit der Art und Weise, wie sie ihren Code schreiben oder ihre Infrastruktur konfigurieren (was zunehmend auch mit Code geschieht).

Neunzig Prozent der Organisationen waren von

Software-Bugs haben 40 % der Störungen ausgelöst, gegenüber 33 % im Jahr 2024.

mindestens einer Cybersicherheits-Störung betroffen, doch es ist klar, dass diese auf Entwicklungsprobleme, Prozessprobleme und möglicherweise auch auf kulturelle Probleme im Unternehmen zurückzuführen sind. Natürlich dürfen Organisationen die äußeren Gegebenheiten nicht aus den Augen verlieren, aber es ist an der Zeit, dass sie ihren Fokus stärker auf die Budgetverteilung und die Teamstruktur richten, anstatt sich ausschließlich auf externe Bedrohungen zu konzentrieren.

Skalierung verstärkt all diese Probleme. Bei großen Unternehmen mit mehr als 10.000 Mitarbeitern lag der Durchschnitt bei 57 Störungen, fast 40 % über dem Mittelwert von 40. Ausgedehnte Angriffsflächen und komplexe Entwicklungspipelines bieten mehr Möglichkeiten für Störungen. Kleinere Organisationen sind mit denselben Problemen in geringerem Umfang konfrontiert, was zwar hilfreich ist, das Problem jedoch nicht vollständig beseitigt.

Ein Silberstreif am Horizont bei der Erholung von Sicherheitsvorfällen

Die Fastly-Umfrage enthüllte einige wirklich gute Nachrichten: Unternehmen werden immer besser darin, sich von Angriffen zu erholen. Die durchschnittliche Recovery-Dauer sank von 7,34 Monaten im Vorjahr auf 6,08 Monate im Jahr 2025. Das ist mehr als ein Monat weniger Erholungszeit, was eine bedeutende Verbesserung darstellt. Denn jeder Tag Ausfallzeit kostet Geld und untergräbt das Vertrauen der Kunden.

Auch die Kluft zwischen Erwartungen und Realität schließt sich zunehmend. Die Unternehmen rechnen nun mit einer Erholungszeit von 5,89 Monaten, und die tatsächliche Zeitspanne von 6,08 Monaten liegt bemerkenswert nahe. Diese Ausrichtung deutet darauf hin, dass Unternehmen realistischere Pläne zur Störungsbehebung entwickeln, die auf tatsächlichen Erfahrungen und nicht auf Wunschdenken basieren.

Die finanziellen Auswirkungen entwickeln sich ebenfalls in die richtige Richtung. Die Umsatzverluste beliefen sich im Durchschnitt auf 2,68 % des Jahreseinkommens, gegenüber 2,98 % im Vorjahr. Das ist zwar immer noch schmerzhaft (ein Mittelstandsunternehmen, das fast 3 % seines Umsatzes verliert, muss einen schweren Schlag einstecken), aber die Entwicklung ist wichtig. Die Organisationen können den Schaden heute besser eindämmen als noch vor zwölf Monaten.

Schließlich scheinen Kunden nachsichtiger zu sein, sobald sie sehen, dass ein Unternehmen Anstrengungen unternimmt, seine Cybersicherheitsprobleme zu beheben. Die Wiederherstellung des Rufs dauert im Durchschnitt 4,73 Monate und ist damit schneller als die 6,08 Monate, die für die vollständige Wiederherstellung von Systemen und Betriebsabläufen benötigt werden. Das Krisenmanagement und die Aufrechterhaltung der Kundenkommunikation können das Vertrauen also selbst dann wieder aufbauen, wenn die technischen Teams noch mit der Beseitigung der Auswirkungen beschäftigt sind.

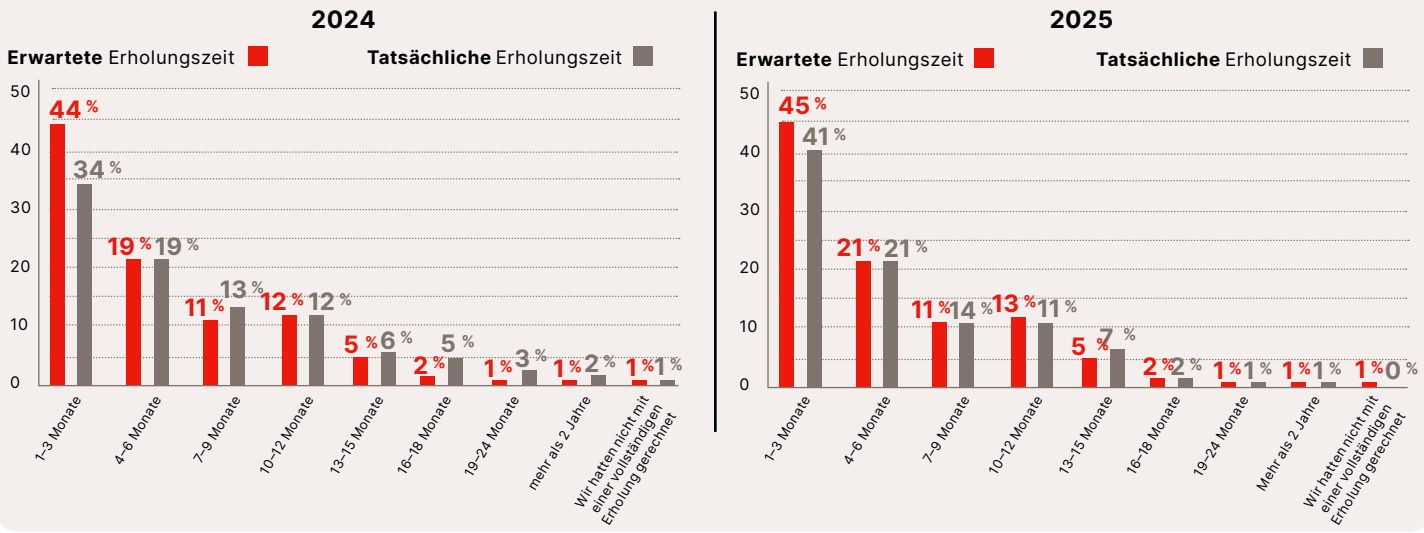
Investitionen in Reaktionsfähigkeiten zahlen sich aus

Organisationen investieren ihr Geld dort, wo es wirklich zählt. Über die Hälfte (52 %) investierte in Überprüfungen nach Störungen, um systematisch zu analysieren, was schiefgelaufen ist und wie dies in Zukunft verhindert werden kann. Weitere 43 % haben die Reaktionsautomatisierung eingeführt und nutzen Technologie, um Eindämmungs- und Wiederherstellungsmaßnahmen zu beschleunigen, die zuvor ein manuelles Eingreifen erforderten.

Doch in diesen positiven Entwicklungen sind erhebliche Vorwarnungen verborgen. Trotz der Verbesserungen haben 30 % der Unternehmen immer noch keine regelmäßig getesteten Playbooks für die Reaktion auf Störungen. Der Druck wächst, die tatsächlichen Erholungszeiten weiter zu verkürzen.

Und während sich Unternehmen zwar schneller erholen können, schlägt der Blitz häufig zweimal oder sogar öfter ein. Bei zwei Dritteln (66 %) der Organisationen kam es innerhalb von drei Monaten zu erneuten Störungen, da möglicherweise noch immer zugrunde liegende Probleme bestehen könnten.

Die Erwartungen bezüglich der Erholung werden immer realistischer



Investitionsprioritäten: Wohin die Sicherheitsbudgets wirklich fließen

Fragt man Sicherheitsteams, was ihnen schlaflose Nächte bereitet, stehen Datensicherheitsverletzungen natürlich mit 45 % an erster Stelle. Social Engineering folgt mit 40 % an zweiter Stelle. Das ergibt Sinn, wenn man bedenkt, dass Phishing-E-Mails nach wie vor der Ausgangspunkt für die meisten erfolgreichen Angriffe sind. Eine ausgeklügelte Technologie kann einen gestressten Mitarbeiter nicht davon abhalten, an einem späten Freitagnachmittag auf einen überzeugenden Link zu klicken.

Ransomware (die oft mithilfe von Social-Engineering-Angriffen eingesetzt wird) rangiert mit 28 % weit oben, nach generativer KI und mangelnden technischen Fähigkeiten. Nach Jahren voller Schlagzeilen – das sollte niemanden überraschen – fallen Unternehmen immer noch diesem Übel zum Opfer. Nur weil die Strategie mittlerweile gut bekannt ist, heißt das nicht, dass sie leichter zu stoppen ist.

Diese Risiken existieren nicht isoliert. Account-Übernahme (19 % geben dies als Sorge an) beginnt in der Regel ebenfalls mit Phishing.

Jedoch verdienen die Drittanbieter-Risiken besondere Aufmerksamkeit. Der Angriff im September auf das npm-Software-Repository zeigte, wie ein einziger Angriff Hunderte von Paketen infizieren und so Schadsoftware in unzählige Nutzerumgebungen einschleusen kann. Wenn Ihre Sicherheit teilweise von der Sicherheit eines anderen abhängt, gehen Sie ein Risiko ein, das Sie nicht direkt kontrollieren können.

Angesichts zunehmender Risiken ist es kein Wunder, dass Datenschutz und Privatsphäre mit 37 % die Investitionsprioritäten anführen Die Verlagerung hin zum Datenschutz spiegelt den zunehmenden regulatorischen Druck und die Erkenntnis wider, dass Datensicherheitsverletzungen Konsequenzen über die unmittelbare technische Behebung hinaus haben. Compliance-Verstöße, Klagen von Kunden und Markenschäden resultieren alle aus unsachgemäß gehandhabten Daten.

Cyberversicherung war mit 34 % die zweitbeliebteste Investitionskategorie, gefolgt von API-Sicherheit mit 33 %. Der zweite Platz der Cyberversicherungen ist ein Zeichen der Akzeptanz. Organisationen erkennen, dass eine perfekte Verteidigung unmöglich ist, deshalb übertragen sie das Risiko. Es ist nicht möglich, jede Sicherheitsverletzung zu verhindern? Stellen Sie zumindest sicher, dass Sie nicht den gesamten finanziellen Schaden tragen müssen, wenn es zu einer solchen kommt.

Angesichts zunehmender Risiken ist es kein Wunder, dass Datenschutz und Privatsphäre mit 37 % die Investitionsprioritäten anführen

Investitionen in die API-Sicherheit sind sinnvoll, wenn man bedenkt, dass jede neue App für Mobilgeräte, jede Integration von Drittanbietern und jeder Microservice einen weiteren potenziellen Angriffspunkt darstellt. APIs waren früher interne Infrastruktur. Jetzt sind sie dem Internet ausgesetzt und die Angreifer haben es bemerkt.

Die echte Investitionsverlagerung zeigt sich in der KI. Die Umfrage ergab, dass sich Unternehmen auf Bedrohungen durch agentische Infrastrukturen vorbereiten. Unter denjenigen, die in diesen Bereich investieren, steht die Agentenauffindbarkeit mit 56 % an erster Stelle, gefolgt von der API-Sicherheit mit 55 % und den WAFs mit 54 %. Diese nicht traditionellen Sicherheitskategorien sind eine Antwort auf architektonische Muster, die vor zwei Jahren kaum existierten.

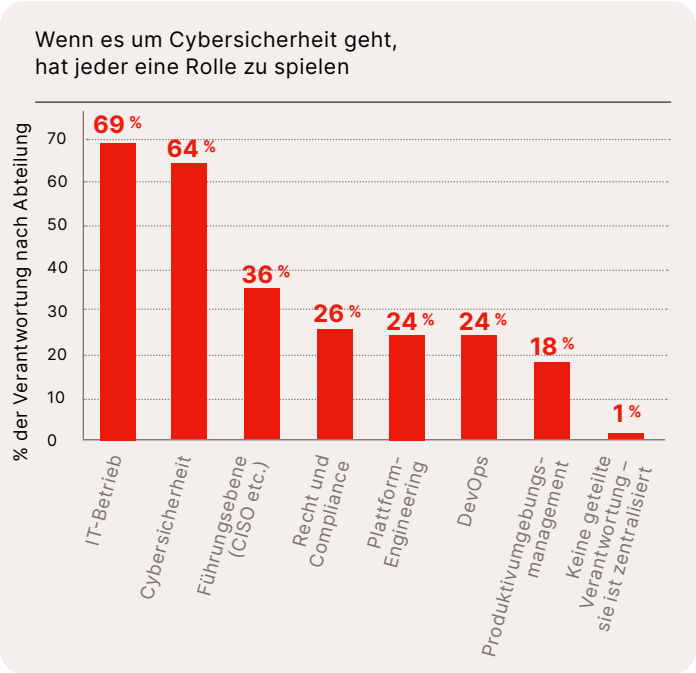
Drei Viertel der Unternehmen befürchten DDoS-Angriffe auf KI-Agenten, und mehr als die Hälfte gibt zu, dass ihren Teams die KI-spezifische Expertise fehlt, um mit diesen Bedrohungen umzugehen. Dennoch rangiert der DDoS-Schutz mit 30 % nur an fünfter Stelle der Investitionsprioritäten. Es besteht eine Diskrepanz zwischen den geäußerten Bedenken und den tatsächlichen Ausgaben, was entweder auf falsch gesetzte Prioritäten oder auf begrenzte Budgets hindeutet, die unangenehme Kompromisse erfordern.

2 „Widespread Supply Chain Compromise Impacting Npm Ecosystem | CISA.“ Cybersecurity and Infrastructure Security Agency CISA, 23. September 2025, www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem

CISOs tragen mehr Verantwortung, erhalten aber nur unzureichende Unterstützung

Der Stuhl des CISO wird immer heißer. Fast drei Viertel (73 %) der Unternehmen geben mittlerweile an, dass der CISO letztendlich die Verantwortung trägt, wenn es zu Sicherheitsverletzungen kommt. Der regulatorische Druck zeigt zunehmend, dass Sicherheitsleiter für Versäumnisse persönlich haftbar gemacht werden können. So erlaubt beispielsweise die NIS2-Richtlinie der EU von 2022 vorübergehende Suspendierungen von Führungskräften, die als unfähig angesehen werden, ihre Cybersicherheitsaufgaben zu erfüllen, sowie Schadensersatz gegen Geschäftsführer und CEOs.

Die Beteiligung des CISO an der Antwort auf Sicherheitsstörungen hat ebenfalls deutlich zugenommen: 82 % gaben eine aktive Beteiligung an, und 74 % verzeichneten im vergangenen Jahr ein verstärktes Engagement des CISO. Auf dem Papier sieht es so aus, als würde die Sicherheit die Aufmerksamkeit der Geschäftsführung erhalten, die sie verdient. In der Praxis war die Antwort weniger beeindruckend.



Richtlinienänderungen greifen daneben

Die meisten Organisationen (94 %) haben Richtlinienänderungen als Antwort auf die zunehmende Verantwortlichkeit der CISOs vorgenommen. Doch wenn man genauer hinsieht, was diese Veränderungen konkret bedeuten, wird das Bild unübersichtlich. Viele Maßnahmen sind defensiv, wobei 42 % eine verstärkte Prüfung der Sicherheitsoffenlegungsdokumentation versprechen (mit anderen Worten, die Regeln richtig zu lesen). Von den befragten Personen bieten 45 % jetzt mehr rechtliche Unterstützung für ihre Mitarbeiter im Bereich Cybersicherheit an.

Diese sind umgangssprachlich als „CYA-Richtlinien (Cover Your Ass)“ bekannt. „Diese Maßnahmen sind zwar schön und gut, aber sie dienen fast ausschließlich der Selbsterhaltung“, sagt Erwin. „Ihr Beitrag zur Verbesserung der Sicherheitslage ist gering.“

Eine der häufigsten Maßnahmen, die von 44 % genannt wird, ist, dem CISO einen Platz am Tisch für strategische Entscheidungen zu geben (das liegt fast gleichauf mit zusätzlicher rechtlicher Unterstützung und Ressourcen für Cybersicherheitsteams, die jeweils bei 45 % liegen). Das gibt ihnen zumindest eine Art Stimme, aber das allein reicht nicht aus, um den Verfall aufzuhalten. Sicherheitsverantwortliche benötigen die Befugnis und die Ressourcen, um notwendige Sicherheitsmaßnahmen umzusetzen, und nicht nur die Verantwortung, wenn etwas schiefgeht.

Niemand weiß, wer verantwortlich ist

Die Verwirrung erstreckt sich nicht nur auf technische Schwachstellen, sondern auch auf die Organisationsstruktur. Über die Hälfte der AI-first-Unternehmen berichten von mangelnder Klarheit darüber, wer für die Reaktion auf Störungen verantwortlich ist, verglichen mit nur 23 % der Organisationen, bei denen KI nicht an erster Stelle steht. Wenn es jedoch zu Sicherheitsverletzungen kommt, wird die Schuld nach oben verlagert: 79 % der AI-first-Unternehmen geben an, dass der CISO letztendlich verantwortlich gemacht wird, während es bei den traditionellen Unternehmen nur 57 % sind.

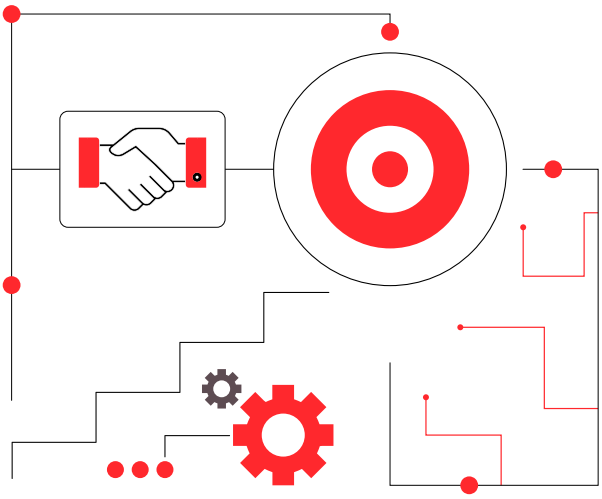
Da Unternehmen, die auf KI setzen, schneller neue Risiken schaffen, als sie sie bewältigen können, wird dieses Thema für Sicherheitsverantwortliche in den Mittelpunkt rücken. Sie werden die Schuld für die unvermeidlichen Sicherheitsverletzungen tragen müssen, die aus diesen Risiken folgen.

Verwirrung verursacht nicht nur Probleme an der Spitze. Unsere Studie zeigt, dass 43 % der Menschen in Unternehmen der Meinung sind, dass es Klarheit darüber gibt, wer für Störungen verantwortlich ist – der gleiche Prozentsatz ist der Meinung, dass es keine Klarheit gibt (der Rest ist unentschlossen).

3 PricewaterhouseCoopers. „What You Need to Know about NIS2 - PwC.“ PwC, 2023, www.pwc.de/en/cyber-security/european-nis2-directive-implications-for-businesses-and-institutions.html.

Die Lösung des Fachkräftemangels

Das Talentproblem wird immer schlimmer, nicht besser. Mehr als die Hälfte (53 %) der Sicherheitsteams verfügt nicht über das KI-spezifische Fachwissen, um auf neue Bedrohungen zu reagieren. Dabei geht es nicht mehr nur um allgemeine Fähigkeiten im Bereich der Cybersicherheit. Die rasante Verbreitung von KI-Infrastruktur hat eine Nachfrage nach spezialisiertem Wissen geschaffen, die der Markt nicht decken kann.



KI-orientierte Unternehmen sind besonders auf der Suche nach Talenten. Sie arbeiten schnell und entwickeln neue Systeme. Sie stellen außerdem fest, dass sich herkömmliche Sicherheitsexpertise nicht ohne Weiteres auf den Schutz von KI-Agenten, die Verwaltung der agentenbasierten Infrastruktur oder die Abwehr von KI-gestützten Angriffen übertragen lassen. Der Fachkräftemangel ist zu einem Engpass geworden, der einschränkt, wie schnell sie ihre expandierenden technologischen Infrastrukturen sichern können.

Frischgebackene Absolventen im Bereich Cybersicherheit stehen vor einer steilen Lernkurve. Sie müssen technische Fähigkeiten erlernen, die speziell auf das Toolset und den Workflow eines Unternehmens zugeschnitten sind, sowie die kulturellen Besonderheiten der Organisation. Es bedarf erheblicher Zeit und Mühe, bis ein unerfahrener Neuzugang produktiv wird. Mit der Skalierung von Unternehmen verstärkt sich diese Herausforderung, insbesondere bei der Arbeit in größeren, sich ständig verändernden Umgebungen.

Alternativen zur externen Personalsuche

Vielleicht sollten Unternehmen stattdessen nach innen schauen. Mehrere Optionen verdienen Beachtung. Bestehende Mitarbeiter für neue Aufgaben weiterzubilden bedeutet, dass sie bereits mit Ihrer Unternehmenskultur vertraut sind und die spezifischen Systeme und Prozesse des Unternehmens zumindest teilweise beherrschen. Diese Personen verstehen den geschäftlichen Kontext, der bei Sicherheitsentscheidungen unter Druck genauso wichtig ist wie technische Fähigkeiten.

Mentoring bietet praxisnahe Schulungen durch erfahrene Mitarbeiter, festigt die Fähigkeiten von Nachwuchskräften und bereitet sie auf den Erfolg vor. Das ist zwar langsamer als die Einstellung einer Person mit zehn Jahren Berufserfahrung, aber solche erfahrenen Kandidaten sind immer schwerer zu finden und teuer in der Rekrutierung.

Die abteilungsübergreifende Zusammenarbeit zwischen der Sicherheitsabteilung und anderen Teams wie der IT-Abteilung, der Compliance-Abteilung, dem Support und der Produktentwicklung kann dazu führen, dass die Mitarbeiter ein Gefühl dafür bekommen, wie sich das Thema Sicherheit auf andere Funktionen auswirkt. Hier gibt es Möglichkeiten, Mitarbeiter zeitweise in anderen Abteilungen einzusetzen.

Die interne Suche nach Fachkräften – insbesondere aus verschiedenen Funktionen – bietet gleich mehrere Vorteile: Sie fördert die Vorstellung, dass jeder für die Sicherheit verantwortlich ist. Darüber hinaus unterstützt sie die Bemühungen um die digitale Transformation, indem sie Sicherheitsexpertise in der gesamten Organisation verankert, anstatt sie in einem einzigen Team zu konzentrieren, das zu einem Engpass wird.

Wie Bedrohungen je nach Sektor variieren

Die aggregierten Daten erzählen eine Geschichte, aber eine Aufschlüsselung nach einzelnen Sektoren zeigt, wie ungleich die Belastung durch die Cybersicherheit auf die verschiedenen Branchen verteilt ist. Einige sehen sich mit existenziellen Bedrohungen für ihr Kerngeschäft konfrontiert, während andere mit geopolitischen Risiken oder dem betrieblichen Chaos bei der Sicherung ausgedehnter digitaler Bestände zu kämpfen haben. Hier ist die Aufschlüsselung der Bedrohungslandschaft nach Sektoren.

Finanzwesen

Im Finanzwesen gibt es durchschnittlich 54 Sicherheitsverletzungen pro Jahr. Phishing macht immer noch **39 %** der Unternehmen Sorgen, und Datenschutzverletzungen machen **42 % zu schaffen, aber die alarmierendste Zahl sind 442.232 US-Dollar**. Das sind die durchschnittlichen jährlichen Infrastrukturkosten, die allein durch KI-Scraping entstehen, und es sind die höchsten über alle Sektoren hinweg. Vielleicht ist das der Grund, warum die generative KI **41 %** der Finanzinstitute beunruhigt. Nur Tech-Unternehmen sind noch besorgter darüber.

Medien und Unterhaltung

Dieser Sektor fällt völlig aus dem Rahmen. Hier gibt es mit 24 die geringste Anzahl von Sicherheitsverletzungen in allen Sektoren. Allerdings stellt das Scraping von Inhalten eine Bedrohung für das Geschäftsmodell dar. Jedes fünfte dieser Unternehmen sieht darin ein großes Problem, während es in anderen Branchen nur**5–16 %** sind. Dies zeigt sich in den **51 %** der Medienunternehmen, die unter erhöhten Infrastrukturkosten durch KI-Scraping leiden, in den **47 %**, die von Betriebsunterbrechungen betroffen sind, und in den **39 %**, die von Problemen beim Kundenerlebnis berichten – all dies sind branchenübergreifende Höchstwerte. Nur **11 %** berichten von keinen Auswirkungen.

Staatliche Organe

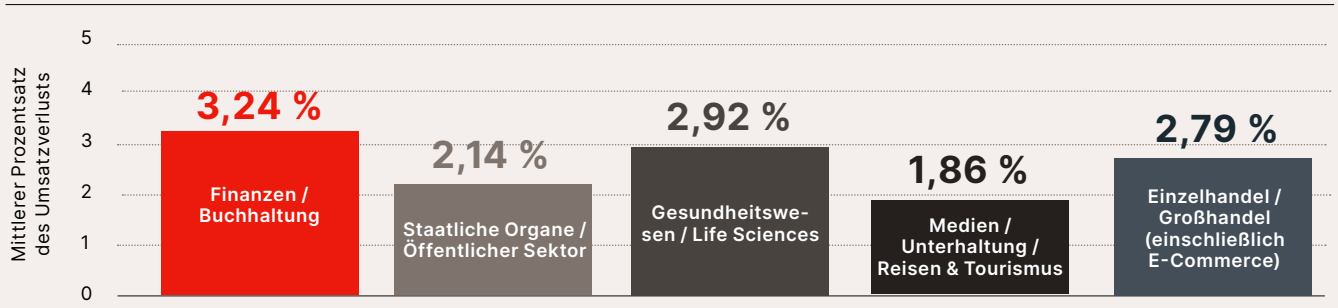
Angriffe auf den Staat sind verständlicherweise das größte Problem für die befragten Behörden. **21 %** der Sicherheitsteams machen sich diesbezüglich Sorgen (deutlich mehr als der Prozentsatz in den Wirtschaftssektoren). Der Prozentsatz, der sich über Datenschutzverletzungen sorgt, erreicht mit **52%** den höchsten Wert überhaupt.

Einzelhandel

Einzelhändler scheinen von allen Seiten unter Druck zu stehen. DDoS-Angriffe bereiten **25 %** von ihnen Sorgen (die höchste Rate aller Branchen), während die Angst vor Ransomware bei Einzelhändlern bei **32 %** mit der im Finanzsektor übereinstimmt. Und eine branchenweit höchste Qualifikationslücke von **32 %** bedeutet, dass Zahlungssysteme und Kundendaten nicht ausreichend geschützt sind.

Branchenspezifische Unterschiede können zu unterschiedlichen Bewertungen in verschiedenen Aspekten der Cybersicherheit führen, doch eines ist universell: Sie alle tragen die Kosten für KI. Die Kosten für Web-Scraping belaufen sich branchenübergreifend auf jährlich fast **300.000 bis 450.000 US-Dollar**. Herkömmliche Bedrohungen wie Identitätsdiebstahl und Datenschutzverletzungen bestehen weiterhin, aber KI hat zusätzliche, obligatorische Kosten für den Betrieb digitaler Systeme verursacht.

Finanzunternehmen haben bei ihrer größten Sicherheitsstörung im Jahr 2025 im Durchschnitt am meisten verloren



Der Pfad in die Zukunft: Sicherheit durch Design in einer KI-beschleunigten Welt

Angesichts der Tatsache, dass interne Fehler mittlerweile ebenso viele Sicherheitsverletzungen verursachen wie externe Angriffe und Softwarefehler 40 % der Vorfälle auslösen, könnte man meinen, dass dies zu einem grundlegenden Umdenken in Bezug auf die Art und Weise führen würde, wie Organisationen Software entwickeln. Aber das ist nicht der Fall.

> „Ich kann nicht warten, bis jemand zu mir kommt, um meine Zustimmung zu erhalten, denn wenn das passiert, dann habe ich wahrscheinlich schon versagt."
>
> **— Marshall Erwin, CISO bei Fastly**

Nur 37 % haben die Sicherheitsverantwortung auf Platform-Engineering- oder DevOps-Teams verlagert.

Die Teilnahme an Gesprächen, bevor Architekturentscheidungen getroffen werden, ist von entscheidender Bedeutung. „Ich kann nicht warten, bis jemand zu mir kommt, um meine Zustimmung zu erhalten, denn wenn das passiert, dann habe ich wahrscheinlich schon versagt", sagt Erwin.

DevOps-Automatisierung hilft, aber nur bei taktischen Problemen. Ihre CI/CD-Pipeline (Continuous Integration/Continuous Delivery) erkennt keine architektonischen Fehler, wie beispielsweise die Vergabe übermäßiger Berechtigungen an einen KI-Agenten, die Ihre Infrastruktur für Angriffe anfällig machen. Hierfür ist menschliches Urteilsvermögen während der Planung erforderlich.

Die Automatisierungsgrenze

Automatisierung ist ein wichtiger Teil der Sicherheitsgleichung, da sie hilft, die Talentlücke zu schließen. Doch selbst Unternehmen, die sich der Automatisierung verschrieben haben, stoßen an ihre Grenzen. „Das Volumen potenzieller Sicherheitslücken, die Sie sich ansehen und beheben müssen, ist heute für fast jedes etablierte Unternehmen im Technologiebereich hoch", bemerkt Erwin. Kombiniert man ein hohes Volumen mit einer hohen Rate an False Positives, kommt man mit Automatisierung nur bedingt weit.

Erwin empfiehlt Automatisierung für die Bewältigung weniger schwerwiegender Probleme und die Beauftragung von Experten für schwerwiegende Störungen. Überlassen Sie es den Maschinen, routinemäßige Sicherheitslücken zu schließen. Sparen Sie sich menschliches Fachwissen für die kniffligen Dinge auf, die Kontext und Urteilsvermögen erfordern.

Zwei Probleme, eine Lösung

KI schafft sowohl externe als auch interne Sicherheitsherausforderungen. Auf der einen Seite steht das Problem der betrieblichen Kosten durch externe KI-Bedrohungen. KI-Scraping belastet die Infrastrukturbudgets so stark, dass 64 % der Organisationen es mittlerweile als wesentlichen Kostenfaktor betrachten. Das liegt daran, dass Bots ihre Websites crawlen, Bandbreite verbrauchen, die Performance beeinträchtigen und ihre Cloud-Rechnungen erhöhen (ganz zu schweigen von der widerrechtlichen Aneignung wertvollen geistigen Eigentums).

Auf der anderen Seite steht das Problem der Angriffsfläche, mit dem die eigene KI-Infrastruktur von Unternehmen konfrontiert ist. Agentenbasierte Infrastruktur und privilegierte KI-Tools schaffen neue Vektoren für Angreifer. Diese hochprivilegierten Tools können Angreifern im Erfolgsfall tiefgreifenden Zugriff auf die Infrastruktur ermöglichen.

Beide Probleme laufen am gleichen Punkt zusammen: Webanwendungen und APIs. Lösungen für Web-App- und API-Schutz schützen beide Fronten. Derselbe Layer, der Scraper einschränkt, die Ihr Infrastrukturbudget belasten, schützt auch die APIs, die agentenbasierten Systemen zugrunde liegen. Webanwendungs-Firewalls, die Layer-7-Angriffe blockieren, funktionieren unabhängig davon, ob es sich bei dem Ziel um herkömmliche Infrastrukturen oder KI-Agenten handelt. Organisationen, die in agentische Sicherheit investieren, verstehen das.

> „Das Volumen potenzieller Sicherheitslücken, die Sie sich ansehen und beheben müssen, ist heute für fast jedes etablierte Unternehmen im Technologiebereich hoch."
>
> **– Marshall Erwin, CISO bei Fastly**

Wie man die Sicherheit vorab sicherstellt

KI-orientierte Unternehmen müssen den Wert eines überlegten Vorgehens erkennen. Wenn sie schnell handeln und dabei Dinge kaputt machen, brauchen sie länger, um die Scherben aufzusammeln. Deshalb erhöhen KI-Organisationen ihre Ausgaben für Sicherheit und fühlen sich dennoch verwundbarer.

Das ist auch der Grund, warum „Security by Design“ von einem ehrgeizigen Ziel zu einer Überlebensvoraussetzung geworden ist. Die 81 %, die sagen, dass Investitionen in Netzwerkstabilität ihre Innovation sicher beschleunigt haben, haben dies bereits herausgefunden.

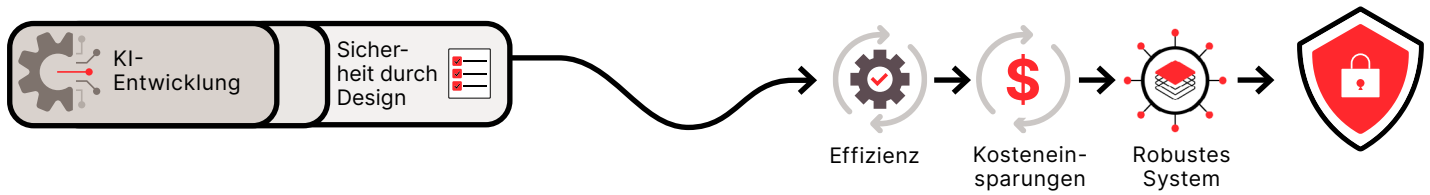
Die von Anfang an in die Systeme integrierte Sicherheitsarchitektur beseitigt Unsicherheiten und ermöglicht es den Teams, schneller und mit Zuversicht zu handeln. Die Alternative ist das, was wir jetzt sehen: Organisationen geben mehr aus, erholen sich langsamer und wundern sich, warum der Kauf weiterer Tools nichts gebracht hat. Es ist kein Zufall, dass 72 % der Organisationen die Markteinführungsgeschwindigkeit gegenüber dem Aufbau von Netzwerkstabilität in Systemen priorisieren.

KI verändert Geschäftsabläufe in einem Tempo, das den ein Jahrzehnt währenden Übergang der Wirtschaft zur Cloud als gemächlich erscheinen lässt. Unternehmen, die diese neue Infrastruktur aufbauen, ohne dass Sicherheitsarchitekten von Anfang an dabei waren, werden sich der großen Gemeinschaft der AI-first-Unternehmen anschließen, bei denen KI bei ihrer letzten Sicherheitsverletzung direkt ausgenutzt wurde.

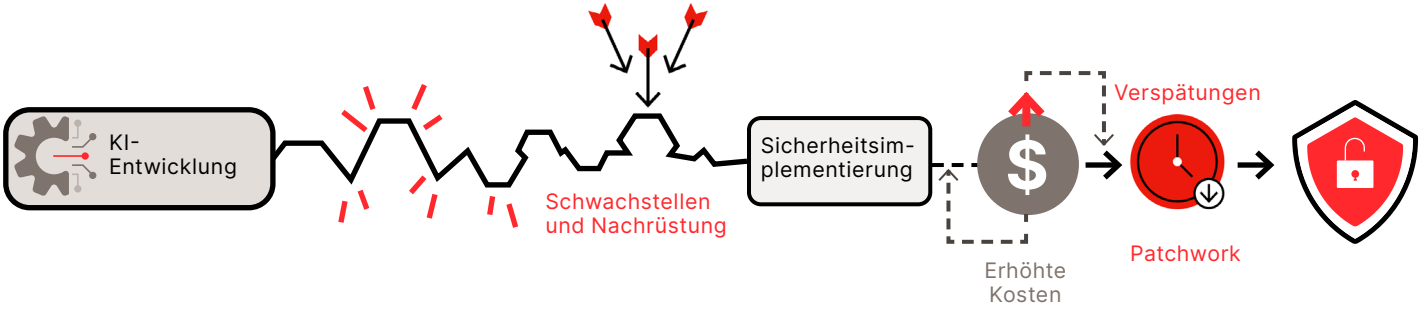
Es wird eine klare Trennlinie geben zwischen denen, die Sicherheit von Anfang an in ihre KI-Strategie integriert haben, und denen, die sie erst später hinzugefügt haben. Die gute Nachricht ist, dass Sie die Kontrolle darüber haben, auf welcher Seite Sie stehen.

Sicherheitsvorteile durch die Implementierung von KI von Anfang an

Frühe Implementierung



Implementierung während des laufenden Prozesses



Über die Studie

Für diese Studie haben wir branchenübergreifend 2.000 wichtige IT-Entscheider großer Unternehmen aus Nord-, Mittel- und Südamerika, Europa, dem Asien-Pazifik-Raum und Japan befragt, die Einfluss auf die Cybersicherheit haben. Die Befragungen wurden von Sapio Research im 4. Quartal 2025 per Onlineumfrage mittels E-Mail-Einladung durchgeführt. Bei jeder Stichprobe unterliegen die Ergebnisse gewissen Stichprobenabweichungen.

Das Ausmaß der Abweichung ist messbar und wird durch die Anzahl der Befragungen und die Höhe der Prozentsätze aus den Ergebnissen beeinflusst. In dieser speziellen Studie stehen die Chancen 95 zu 100, dass ein Umfrageergebnis nicht um mehr als 2,6 Prozentpunkte von dem Ergebnis einer Befragung aller Personen innerhalb der Grundgesamtheit abweicht, die durch die Stichprobe repräsentiert wird.

Über Sapio

Als Finalist im Rennen um den Titel als beste neue Agentur ist Sapio versiert in der Durchführung von Meinungsumfragen (wir haben Zugang zu 80 Millionen Nutzern auf der ganzen Welt), Fokusgruppen, persönlichen Interviews, Telefoninterviews, Online-Forschung, Desk Research, statistischer Modellierung und vielem mehr. Wir sind spezialisiert auf B2B-Forschung und -Beratung. Unser Geschäft basiert auf partnerschaftlichen Prinzipien, die von sozialen Unternehmen inspiriert sind.

Über Fastly, Inc.

Die leistungsstarke und programmierbare Edge-Cloud-Plattform von Fastly unterstützt weltweit führende Marken dabei, schnelle, sichere und ansprechende Online-Erlebnisse zu bieten. Dies wird durch Edge-Compute-, Bereitstellungs-, Sicherheits- und Observability-Angebote ermöglicht, die die Performance von Websites verbessern, die Sicherheit erhöhen und Innovationen auf globaler Ebene vorantreiben. Im Vergleich zu anderen Anbietern ermöglicht die leistungsstarke, hochmoderne Plattformarchitektur von Fastly Entwicklern die Bereitstellung sicherer Websites und Apps mit schneller Markteinführung und nachweislich branchenführenden Kosteneinsparungen. Organisationen auf der ganzen Welt vertrauen auf Fastly, um ihr Interneterlebnis zu verbessern, darunter Reddit, Neiman Marcus, die Universal Music Group und SeatGeek. Erfahren Sie mehr über Fastly unter https://www.fastly.com und folgen Sie uns unter @fastly.