Weltweite Studie zum Thema Security

Cybersicherheit am Scheideweg

Gründe für das Cybersicherheitsdilemma in Unternehmen und mögliche Lösungen

fastly

Inhalt

Zusammenfassung

Im vergangenen Jahr hat das Thema Cybersicherheit weiter an Bedeutung gewonnen. Angreifer stahlen die Anrufdaten fast aller AT&T Kunden.[1] Bei einem Angriff auf UnitedHealth wurden persönliche Gesundheitsdaten „eines beträchtlichen Teils der amerikanischen Bevölkerung“ preisgegeben.[2] Die chinesische Hacker-Gruppe Salt Typhoon soll Donald Trump und seine Mitarbeiter ins Visier genommen haben, indem sie sich in die US-Telekommunikationsnetze hackte.[3] Die Welt erlebte den bisher wohl größten Cyberausfall, als durch eine Fehlkonfiguration bei einem CrowdStrike Update Millionen von Windows PCs vom Netz gingen.

Wie dieses Beispiel zeigt, ist der Bedarf an mehr Cybersicherheit und digitaler Widerstandsfähigkeit größer denn je. Dennoch befinden sich die Sicherheitsbemühungen vieler Unternehmen bis dato nach wie vor in einer prekären Lage. Der Gegenwind, den Initiativen im Bereich der Cybersicherheit zu spüren bekommen, hat sich im Vergleich zum Vorjahr verschärft. Die Gründe dafür sind größtenteils nicht technischer Natur und betreffen Themen wie die Einhaltung immer knapperer Budgets und Unklarheiten bezüglich der Verantwortung für die Cybersicherheit in Unternehmen.

Die Cybersicherheit befindet sich an einem Scheideweg. Um genauere Einblicke in den Umgang mit wichtigen Cybersicherheitsthemen in Unternehmen zu gewinnen und zu erfahren, in welche Richtung sich die Branche entwickelt, hat Fastly im September 2024 gemeinsam mit dem Marktforschungsunternehmen Sapio 1800 IT-Entscheider mit Einfluss auf die Cybersicherheit befragt. Dieser Bericht liefert tiefe Einblicke in die Herausforderungen, vor denen Unternehmen im Bereich Cybersicherheit stehen, und wie sie diese bewältigen wollen. Hier die wichtigsten Erkenntnisse im Überblick:

- **Viele Sicherheitsinitiativen stehen auf Messers Schneide.** Immer mehr Menschen (87 %) rechnen im nächsten Jahr mit steigenden Investitionen in die Cybersicherheit. Allerdings dürfte die Wirkung dieser Ausgaben sehr genau unter die Lupe genommen werden. Sicherheitsteams haben einen schweren Stand beim Versuch, Führungskräfte davon zu überzeugen, die benötigten Mittel bereitzustellen. Dies ist der Tatsache geschuldet, dass sich die Chefetage mit vielen weiteren Prioritäten befassen muss, insbesondere in Bereichen wie der digitalen Transformation und der IT-Modernisierung. Und Initiativen zur Cybersicherheit bremsen den Fortschritt in diesen Bereichen aus ihrer Sicht aus.
- **Unternehmen haben mit der Skalierung ihrer Cybersicherheitsmaßnahmen zu kämpfen.** Während sie mit dem Vorstand um die Rechtfertigung ihrer Funktion ringen, gibt es auch besorgniserregende Anzeichen für Ineffizienzen bei der Cybersicherheit. Über ein Drittel der Befragten hatte keine klare Vorstellung davon, wo sie ihre Ressourcen für die Cybersicherheit einsetzen sollten, was mit einem Gefühl der Überinvestition einhergeht.
- **Der Markt bietet nicht die Fachkräfte, die Unternehmen brauchen.** Hinzu kommt, dass Unternehmen scheinbar nicht in der Lage sind, ihre Bemühungen im Bereich Cybersicherheit nicht in demselben Maße zu skalieren, in dem die Anforderungen an die Kapazität und Komplexität steigen. Hinzu kommen Anzeichen, dass Unternehmen nicht in der Lage sind, ihre Bemühungen im Bereich Cybersicherheit nicht in demselben Maße zu skalieren, wie die Anforderungen an die Kapazität und Komplexität steigen. Es ist also ein Umdenken im Hinblick auf den Umgang mit Kompetenzen gefragt, um den immer neuen Anforderungen an die Cybersicherheit gerecht zu werden.
- **Die technologische Komplexität behindert die Bemühungen im Bereich der Cybersicherheit.** Die Technologie, die Unternehmen zur Bekämpfung von Cyberbedrohungen einsetzen, ist ebenfalls ein wichtiger Faktor bei der Ausweitung von Cybersicherheitsinitiativen. Außerdem haben Unternehmen nach wie vor mit komplexen, überlappenden Tools zu kämpfen, die Cybersicherheitsmaßnahmen wie die Reaktion auf Vorfälle erschweren. Der CrowdStrike Ausfall im Jahr 2024 hat Sicherheitsprodukte und -services ins Rampenlicht gerückt, und Sicherheitsverantwortliche beginnen, die Risiken und Vorteile ihrer Cybersicherheitstools zu hinterfragen.

---

1 Whittaker, Zack. „AT&T says criminals stole phone records of ‘nearly all’ customers in new data breach | TechCrunch.“ TechCrunch, 12. Juli 2024, techcrunch.com/2024/07/12/att-phone-records-stolen-data-breach.

2 UnitedHealth Group. „UnitedHealth Group Updates on Change Healthcare Cyberattack.“ UnitedHealth Group, 22. April 2024, www.unitedhealthgroup.com/newsroom/2024/2024-04-22-uhg-updates-on-change-healthcare-cyberattack.html.

3 Barrett, Devlin. „What to Know About the Chinese Hackers Who Targeted the 2024 Campaigns.“ N.Y. Times, 26. Oktober 2024, www.nytimes.com/2024/10/26/us/politics/salt-typhoon-hack-what-we-know.html.

Die Kluft zwischen Realität und Erwartungen bei der Wiederherstellung nach Cybersicherheitsvorfällen

2024 war ein Rekordjahr für Cyberangriffe. Der CrowdStrike Vorfall, der weltweit etwa 8,5 Mio. Windows Systeme zum Absturz brachte, führte zu Ausfällen in verschiedensten Branchen – vom Finanzwesen über den Flugverkehr bis hin zu Industrieunternehmen.[4] Derartige Ausfälle sind unvermeidlich, aber wie gut sind wir darauf vorbereitet?

Unternehmen fällt es schwerer, sich von Cyberangriffen zu erholen, als sie glauben. Die durchschnittliche erwartete Wiederherstellungszeit liegt bei 5,85 Monaten. In der Praxis dauert es aber mit 7,34 Monaten knapp 25 % länger.

Tatsächlich dauert die Wiederherstellung nach Cyberangriffen immer länger, während die Investitionen in die Cybersicherheit sinken. Unternehmen, die im kommenden Jahr weniger Geld ausgeben möchten, rechnen mit einem Anstieg der Wiederherstellungszeit auf mehr als 8 Monate. Die Diskrepanz zwischen Wahrnehmung und Realität nimmt ebenfalls zu: Bei Unternehmen, die weniger in die Cybersicherheit investieren wollen, dauert die Wiederherstellung mit fast 11 Monaten ein Drittel länger als erwartet. Unternehmen, die in die Cybersicherheit investieren, erholen sich schneller von Sicherheitsvorfällen als Unternehmen, die ihre Ausgaben für die Cybersicherheit kürzen wollen.

Vorbeugende Maßnahmen stehen ganz oben auf der Liste der Bemühungen um die Cybersicherheit.

Die beiden wichtigsten Maßnahmen, die als Reaktion auf Verletzungen der Cybersicherheit ergriffen wurden, nämlich die Einführung strengerer Sicherheitsmaßnahmen (43 %) und das Angebot zusätzlicher Mitarbeiterschulungen (41 %), fallen in die Kategorie „Lessons Learned“, also vorbeugende Maßnahmen zur Vermeidung künftiger Zwischenfälle. Die Befragten konzentrieren sich auch stärker auf Software-Patches: 86 % von ihnen änderten nach dem CrowdStrike Vorfall ihre Vorgehensweise beim Testen oder Bereitstellen von Patches.

Nur wenige Unternehmen nennen spezifische Aktivitäten, die zur Wiederherstellung nach Sicherheitsvorfällen beitragen, darunter die Wiederherstellung anhand von Backups (38 %) und die Kommunikation mit Stakeholdern (34 %). Forensische Analysen, die bei der juristischen Verfolgung böswilliger Angreifer von innen oder von außen oder bei der Meldung an Aufsichtsbehörden hilfreich sind, genießen mit 25 % den geringsten Zuspruch. Positiv ist, dass 32 % der Befragten zusätzliches Geld für Playbooks und unterstützende Tools für die Gefahrenabwehr bereitstellen. *(Abbildung 1)*

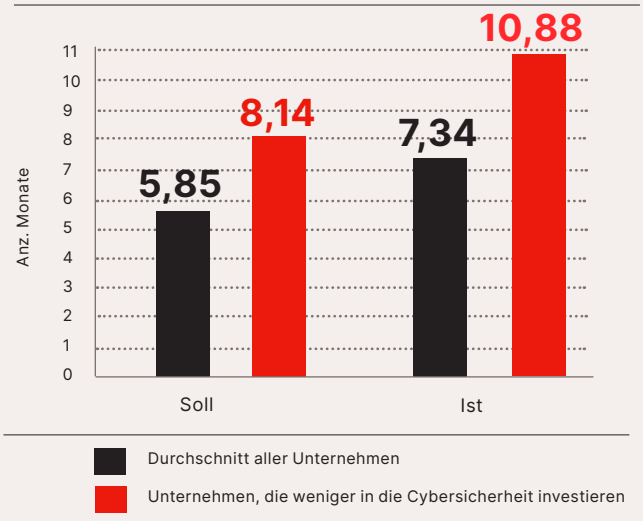
Unternehmen setzen bevorzugt auf interne Recovery-Teams. 61 % greifen auf ihre IT-Teams zurück und 39 % arbeiten mit externen Cybersicherheitsfirmen zusammen, um wieder auf Kurs zu kommen. Weniger als jeder dritte Befragte nannte Versicherungspolicen zur Deckung der Kosten als wichtige Maßnahme. Marktdaten deuten darauf hin, dass es immer schwieriger wird, eine Cyberversicherung abzuschließen, da die durchschnittlichen Kosten für eine Datenschutzverletzung inzwischen einen Höchststand von 4,88 Millionen Dollar erreicht haben.[5]

Außerdem stehen die Unternehmen Drittanbietern, die zu diesen Cybersicherheitsvorfällen beitragen, skeptisch gegenüber. Nach dem weltweiten IT-Ausfall im vergangenen Sommer ziehen 29 % der Befragten einen Anbieterwechsel in Betracht, wenn es zu öffentlichkeitswirksamen Sicherheitsvorfällen oder Problemen mit der Softwarequalität kommt. Fast die Hälfte (48 %) überdenkt die Art und Weise, wie sie ihre bestehenden Cybersicherheitstools einsetzen.

Der Fokus auf Prävention zeigt ein gesteigertes Bewusstsein dafür, dass Vorsorge besser ist als Nachsicht – und dass Cybersicherheit eine proaktive Maßnahme sein sollte. Eine koordinierte und finanziell gut abgesicherte Verteidigung ist aber dennoch unerlässlich, um Angriffe abzuwehren, die diese Abwehrmaßnahmen durchbrechen.

Abbildung 1

Wiederherstellungszeit nach Cybersicherheitsvorfällen



4 Weston, David. „Helping our customers through the CrowdStrike outage“. Microsoft, 20. Juli 2024, https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/

5 „Cost of a data breach 2024 | IBM“. 4. November 2024, www.ibm.com/reports/data-breach.

Wie sehr verlassen sich Unternehmen auf ihre Sicherheitsinfrastruktur und wie sehr sollten sie sich darauf verlassen?

Kaum ein Unternehmen war von Cybersicherheitsvorfällen verschont. Im Durchschnitt waren die Unternehmen im letzten Jahr von fast 40 bekannten Cyberangriffen betroffen, und weniger als eines von zehn Unternehmen war von keinerlei Angriffen betroffen. Die meisten Vorfälle gab es mit durchschnittlich einem Angriff pro Woche bei Unternehmen in den USA. Größere Unternehmen schnitten mit durchschnittlich 64 Vorfällen pro Jahr noch schlechter ab, was auf ihre große Angriffsfläche zurückzuführen ist.

Viele Bedrohungen entstehen durch einfache Fehler. Bei 25 % der Befragten waren falsch konfigurierte IT-Ressourcen die Ursache. Zu den weiteren Problemen zählen Softwarefehler (33 %). Allerdings kommen die Patches und andere IT Updates zum Stoppen von Angriffen oft nicht schnell genug, was bei 18 % der Unternehmen zu Sicherheitsproblemen führt. Secure DevOps (SecDevOps) kann Abhilfe schaffen, indem es Bugs verhindert und IT Updates beschleunigt, um etwaige Schwachstellen zu beheben.

Besonders auffällig ist das Spannungsverhältnis zwischen manuellen Prozessen und Automatisierung. Bei 24 % der Sicherheitsvorfälle spielen manuelle Prozesse eine Rolle. Viele Unternehmen verlassen sich nach wie vor darauf, dass ihre Mitarbeiter manuelle Sicherheitsprozesse und -richtlinien befolgen, anstatt Sicherheit diese direkt in technologische Lösungen zu integrieren. Dies hat bei 16 % der Befragten Probleme verursacht.

Cybersicherheitsvorfälle richten erheblichen Schaden an

Cybersicherheitsvorfälle verursachten im Jahr 2024 bei fast einem Viertel (23 %) der Befragten Umsatzeinbußen von durchschnittlich 3 %. Ausfälle, gefolgt von Datenverlusten, sind ebenfalls schwerwiegende Folgen.

Auch Geldbußen und rechtliche Schritte sind Risiken, die mit Cybersicherheitsvorfällen verbunden sind. Compliance-Verstöße waren für 17 % der Befragten ein Problem, und 19 % mussten feststellen, dass Nutzerkonten kompromittiert wurden, was möglicherweise Verstöße gegen die Datenschutzgesetze darstellt.

Ein weiterer wesentlicher Faktor ist der Reputationsschaden, von dem 22 % der Unternehmen betroffen sind: 18 % bzw. 19 % der Unternehmen berichten von Vertrauensverlusten und sinkender Kundenzufriedenheit. Dies wirkt sich auch auf die Kundenbindung aus, denn 14 % der Befragten haben nach einem Vorfall eine stärkere Kundenabwanderung festgestellt.

Vorbereitung auf ein weiteres Jahr voller Bedrohungen

Die Besorgnis über Cyberbedrohungen ist ungebrochen. Die zu erwartende Zunahme automatisierter Angriffe bereitet 42 % der Befragten Kopfzerbrechen. Viele der Befragten machen sich Sorgen, dass ihre eigenen Cybersicherheitstechnologien nicht Schritt halten können. 29 % beklagen einen Mangel an automatisierten Abwehrmaßnahmen und ein Viertel ärgert sich über ein langsames Änderungsmanagement. Die Automatisierung der Cybersicherheit ist mit 21 % die zweithöchste Sicherheitspriorität der Befragten für die nächsten 12 Monate.

Die Sorge um die Cyberabwehr beeinträchtigt die Bemühungen um mehr Innovation in anderen Bereichen. Die digitale Transformation bringt Wachstumschancen mit sich, aber 40 % der Befragten befürchten, durch die zusätzliche Software und digitale Infrastruktur anfälliger für Angreifer zu werden, zumal 32 % glauben, nicht genug Erfahrung in der Absicherung moderner komplexer Softwarearchitekturen zu haben.

Etwa die Hälfte (52 %) glaubt, nicht auf den Umgang mit modernen Bedrohungen vorbereitet zu sein, und 46 % sind der Meinung, dass es ihnen im Unternehmen an zuverlässigen Cybersicherheitstechnologien mangelt.

DDoS im Fokus

Es gibt sie zwar schon seit einem viertel Jahrhundert, aber Distributed Denial of Service (DDoS)-Angriffe stellen nach wie vor eine ständige Bedrohung dar. **23 %** der Unternehmen machen sich Sorgen um DDoS-Angriffe im nächsten Jahr.

62 % der Unternehmen, die 2024 von DDoS-Angriffen betroffen waren, litten unter ausfallbedingten Verlusten. Mehr als die Hälfte (**52 %**) meldeten erhebliche Umsatzeinbußen, und **70 %** mussten einen Anstieg der Betriebskosten hinnehmen.

Paradoxerweise rangiert der DDoS-Schutz mit **25 %** nur an neunter Stelle der Investitionsprioritäten. Dennoch fühlen sich **45 %** derjenigen, die DDoS als Bedrohung für das nächste Jahr nennen, unvorbereitet. Möglichkeiten, um sich vor DDoS-Angriffen zu schützen, gibt es viele. Am beliebtesten ist mit **71 %** der Einsatz von cloudbasierten Lösungen zum Schutz vor DDoS, während sich **56 %** der Befragten auf ihre Internetanbieter verlassen. **54 %** stellen entsprechende Lösungen auf ihren eigenen Servern bereit. Web Application Firewalls (WAFs) können sowohl in der Cloud als auch vor Ort eingesetzt werden und sind mit **66 %** die beliebteste Maßnahme.

Kommen die Ausgaben für die Cybersicherheit zu kurz?

Nichts geht ohne angemessene Investitionen. Das gilt auch für die Cybersicherheit. Angesichts der immer größeren Zahl an Angreifern, die immer raffinierter vorgehen, müssen Unternehmen Mittel für den Schutz ihrer Ressourcen bereitstellen. Gute Absichten gibt es zwar genug, aber in der Praxis tauchen einige eklatante Probleme auf.

Im Jahr 2023 planten drei Viertel unserer Umfrageteilnehmer, mehr in die Cybersicherheit zu investieren. Ein Jahr später ist die Hälfte aller Unternehmen der Meinung, zu wenig in Schlüsselbereiche der Cybersicherheit investiert zu haben und befürchtet, dadurch anfällig für Angriffe geworden zu sein. Am stärksten ist diese Befürchtung mit 61 % bei Unternehmen in den USA ausgeprägt, was aufgrund der Tatsache, dass sie am häufigsten von Angriffen betroffen sind, nur allzu verständlich ist.

Unternehmen haben im Allgemeinen das Gefühl, in die richtigen Bereiche der Cybersicherheit zu investieren. 71 % der Befragten geben an, dass ihre Investitionen mit ihrer Cybersicherheitsstrategie übereinstimmen. Warum also haben so viele Unternehmen das Gefühl, dass sie immer noch zu wenig in die Sicherheit investieren?

Investitionen sind schwer zu rechtfertigen

Die Schwierigkeiten im Bereich der Cybersicherheit gehen über einen bloßen Mangel an Bewusstsein für diese Problematik hinaus, der leichter zu beheben wäre. Stattdessen wird die Cybersicherheit als Hindernis für andere Prioritäten betrachtet. So befürchten beispielsweise 45 % der befragten Führungskräfte, dass sie die Innovationskraft hemmt. Die IT-Modernisierung spielt bei den Bemühungen um die digitale Transformation eine wichtige Rolle. 43 % der Befragten sind allerdings der Meinung, dass Investitionen in die Cybersicherheit solche Initiativen behindern.

Cybersicherheitsexperten müssen ihre Kosten gegenüber der Führungsebene rechtfertigen, aber 44 % tun dies nicht. Während 72 % der Befragten der Meinung sind, dass ihre Investitionen zur Erreichung von Umsatz- und Wachstumszielen beigetragen haben, glauben nur 62 %, den ROI ihrer Ausgaben für die Cybersicherheit beziffern zu können. Ein Teil des Problems besteht darin, zu wissen, wofür man sein Geld überhaupt ausgeben soll. 36 % der Befragten gaben an, zu viel investiert zu haben, ohne einen genauen Plan für die Verwendung dieser Mittel zu haben.

Diejenigen, die Budgetkürzungen vornehmen, sollten dies oft am wenigsten tun

Positiv ist, dass mit 87 % sogar mehr Unternehmen als im letzten Jahr planen, ihre Investitionen in die Cybersicherheit zu erhöhen. Da aber 76 % der Unternehmen im letzten Jahr planten, mehr in die Cybersicherheit zu investieren, und die Hälfte in diesem Jahr immer noch das Gefühl hat, zu wenig zu investieren, decken sich die Absichten möglicherweise nicht mit der Realität.

Nur 4 % planen, ihre Investitionen in die Cybersicherheit zu senken, was laut Jay Coley, Director Technical Strategy bei Fastly, nicht unbedingt funktionelle Einschränkungen bedeuten muss. Er erklärt: „Es besteht auch die Möglichkeit, auf kostengünstigere Lösungen umzusteigen, Verträge aus Kosteneffizienzgründen zu konsolidieren oder sogar Open-Source-Optionen in Betracht zu ziehen."

Es ist nichts dagegen einzuwenden, seinen ROI maximieren zu wollen, aber die relativ schlechte Performance, was die Cybersicherheit in Unternehmen anbelangt, die die entsprechenden Budgets kürzen, gibt Anlass zur Sorge. Diese Unternehmen waren im vergangenen Jahr im Durchschnitt von 68 Sicherheitsvorfällen betroffen und liegen damit 70 % über dem Gesamtdurchschnitt von 40 Vorfällen.

Jeder Investition sollte eine Risikoanalyse vorausgehen

Unternehmen können viel erreichen, wenn sie in präventive und reaktive Maßnahmen investieren, die die gewünschte Wirkung zeigen. Dies erfordert einen durchdachten Ansatz bei der Risikoanalyse, um die größten Cyberrisiken für das jeweilige Unternehmen zu verstehen und gezielt in entsprechende Abwehrmaßnahmen zu investieren.

Risiko ist eine Sprache, die die Führungsebene versteht. Und Cybersicherheitsexperten können in dieser Sprache mit Entscheidern kommunizieren, indem sie ihnen die wichtigsten Metriken zur Risikominderung vorlegen und ihnen aufzeigen, wie Cybersicherheit Innovationen und Veränderungen im Unternehmen sicherer macht. Außerdem können sie gemeinsam mit Entwicklerteams schon früh im Entwicklungszyklus Sicherheitsmaßnahmen einführen und dabei gegebenenfalls Prozesse automatisieren, um diese Maßnahmen effektiver und reibungsloser zu gestalten.

Wer trägt nun eigentlich die Verantwortung?

Wer trägt im Falle eines Cyberangriffs die Verantwortung? Die Aufsichtsbehörden verweisen immer häufiger auf den Chief Information Security Officer (CISO). Im Oktober 2023 befasste sich die US-amerikanische Securities and Exchange Commission (SEC) nicht nur mit SolarWinds als Unternehmen, sondern auch mit dessen CISO Timothy G. Brown. Letzterer wurde wegen Betrugs und des Versagens interner Kontrollen angeklagt, die meisten Anklagepunkte wurden allerdings abgewiesen.[6] Die SEC und andere Aufsichtsbehörden haben inzwischen ihre Formulierungen angepasst, um die Haftung des CISO eindeutiger zu definieren.

Große Fragezeichen bei den Verantwortlichkeiten des CISO

Die Befragten sind sich der Verschiebung bei den Verantwortlichkeiten für die Cybersicherheit bewusst. 93 % haben sogar schon entsprechende Anpassungen vorgenommen. In den meisten Fällen sind diese Anpassungen aber nicht zielführend. Die am häufigsten genannte Maßnahme, nämlich den CISO endlich an strategischen Entscheidungen zu beteiligen (41 %), ist nicht gerade revolutionär.

Bei einigen Maßnahmen handelt es sich um reine Abwehrmaßnahmen oder Maßnahmen zur Erfüllung der Pflichten. Die 38 %, die eine „verstärkte Prüfung der Unterlagen zur Offenlegungspflicht gegenüber den Aufsichtsbehörden“ versprechen, verpflichten sich damit lediglich, die Vorschriften zu lesen. Der gleiche Anteil verspricht mehr juristische Unterstützung für seine Mitarbeiter im Bereich Cybersicherheit, um sie bei Konflikten mit diesen Behörden besser zu schützen. Nur knapp jeder fünfte Befragte (21 %) betont, dass der CISO die Verantwortung für die Einhaltung der Gesetze im Bereich der Cybersicherheit trägt.

„Diese Maßnahmen sind zwar schön und gut, aber sie dienen fast ausschließlich der Selbsterhaltung“, so Fastly CISO Marshall Erwin. „Ihr Beitrag zur Verbesserung der Sicherheitslage ist gering.“

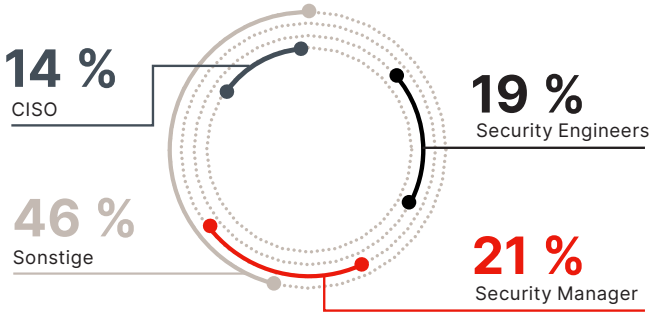
Und wer ist letztendlich wirklich zuständig?

Das Problem besteht zum Teil darin, dass nicht klar ist, wer für Vorfälle im Bereich der Cybersicherheit zuständig ist. Es gibt keine klare Führungspersönlichkeit, die verantwortlich ist, und verschiedene Rollen auf verschiedenen Ebenen fühlen sich auf gewisse Weise verantwortlich. Der CISO wird nach den Security Engineers (19 %) und den Security Managern (21 %) mit 14 % sogar erst an dritter Stelle genannt. (*Abbildung 2)*

Es gibt aber auch ermutigende Signale. Die zunehmende teamübergreifende Zuständigkeit von Anwendungsentwicklern (10 %), Platform Engineers (8 %) und Site Reliability Engineers (7 %) deutet darauf hin, dass die Verantwortung für Cybersicherheitsvorfälle nicht länger ausschließlich auf Sicherheitsexperten beschränkt ist.

In einer idealen Welt würden diese Zahlen bedeuten, dass alle eine gewisse Verantwortung tragen. In der Praxis bedeuten sie allerdings, dass niemand die eindeutige Verantwortung trägt. Gerade einmal 36 % der Befragten legen klare Rollen und Verantwortlichkeiten für die Cybersicherheit fest. Bei fast zwei Dritteln der Befragten ist die Verantwortung nicht eindeutig geklärt, und 46 % sind der Meinung, dass es keine klare Antwort darauf gibt, wer für Vorfälle im Bereich der Cybersicherheit verantwortlich ist. Letztendlich muss aber jemand die Verantwortung tragen.

Abbildung 2
Wer trägt die Verantwortung für Cybersicherheitsvorfälle?



Mitarbeiter im Fadenkreuz

Damit die Sicherheit wirklich zu einer unternehmensweiten Aufgabe wird, müssen sich alle Mitarbeiter dessen bewusst sein und die entsprechenden Befugnisse zur Richtlinienkonformität haben. Social-Engineering-Angriffe – mit **37 %** die von den Befragten am meisten gefürchtete Bedrohung für das kommende Jahr - zielen direkt auf Mitarbeiter ab. Die Zunahme hybrider Arbeitsformen hat auch Auswirkungen auf die Sicherheit: **70 %** der Unternehmen befürchten Angriffe auf Remote-Mitarbeiter.

Ein Großteil der Befragten (**77 %**) glaubt, die Bedeutung der Einhaltung von Cybersicherheitsvorschriften gegenüber der gesamten Belegschaft hinreichend zu kommunizieren. Diese Rechnung scheint auch wirklich aufzugehen, denn **70 %** der Nicht-IT-Mitarbeiter geben an, ihren Einfluss auf die Cybersicherheit zu verstehen, und 69 % sagen, dass alle Mitarbeiter sich an die Vorschriften zur Cybersicherheit halten. Allerdings gibt es auch einige Vorbehalte. **55 %** geben an, dass es zu wenig interne Schulungen über Best Practices im Bereich der Cybersicherheit gibt.

Die Regeln zu kennen ist das eine, ein weiterer Schritt ist es aber, über die nötigen Ressourcen zu verfügen, um sie zu befolgen. **72 %** der Unternehmen geben an, diese Ressourcen zur Verfügung zu stellen, was im Umkehrschluss bedeutet, dass mehr als ein Viertel dies nicht tun. Auch in Bezug auf die Meldeverfahren für Sicherheitsvorfälle gibt es Unklarheiten. Zwar geben **73 %** der Befragten an, dass es ein klares und allgemein zugängliches Verfahren für die Meldung von Vorfällen gibt, aber nur **63 %** sind der Meinung, dass Nicht-IT-Mitarbeiter in der Lage sind, potenzielle Bedrohungen sicher zu erkennen und darauf zu reagieren.

6 Becky Bracken, Senior Editor. „Sizable Chunk of SEC Charges Against SolarWinds Tossed Out of Court.“ Dark Reading, 18. Juli 2024, www.darkreading.com/application-security/solarwinds-charges-tossed-out-of-court-in-legal-victory-against-sec.

Der Fachkräftemangel in der Cybersicherheit erfordert ein Umdenken

Fachkenntnisse sind ein großer Stolperstein im Bereich der Cybersicherheit. 30 % der Befragten geben an, dass es ihren Unternehmen an den nötigen Kompetenzen fehlt, um modernen Sicherheitsbedrohungen zu begegnen. Fast die Hälfte (47 %) hat nicht genug in Neueinstellungen und Gehaltserhöhungen investiert, um qualifizierte Mitarbeiter im Bereich Cybersicherheit zu gewinnen und zu halten. Ausbildung und Talentakquise haben mit 28 % die höchste Priorität für das kommende Jahr.

Vielleicht suchen Unternehmen aber auch an den falschen Stellen nach qualifizierten Mitarbeitern. Die Hälfte der Befragten (51 %) ist der Ansicht, dass es dem Talentpool an den benötigten Kompetenzen fehlt. Tatsächlich sehen nur 13 % keine nennenswerten Probleme mit dem derzeitigen Angebot an Talenten für die Besetzung offener Stellen in der Cybersicherheit.

Es erfordert viel Zeit und Mühe, um aus unerfahrenen Neuzugängen produktive Mitglieder des Sicherheitsteams zu machen. Frischgebackene Cybersecurity-Absolventen benötigen zusätzliches technisches Wissen, zum Beispiel im Umgang mit den spezifischen Tools und Arbeitsabläufen eines Unternehmens, und müssen sich gleichzeitig mit der jeweiligen Unternehmenskultur auseinandersetzen.

Je größer das Unternehmen, desto größer auch die Herausforderung. Die Arbeit in einem solch komplexen und dynamischen Umfeld stellt für die Mitarbeiter ebenfalls eine Herausforderung dar. 17 % der Befragten nannten einen Mangel an Erfahrung im Umgang mit großen Technologien und Unternehmen als Problem.

Alternativen zur externen Personalsuche

Vielleicht sollten sich die Unternehmen angesichts der genannten Herausforderungen bei der Kompetenzentwicklung lieber im eigenen Hause umsehen? Folgende Optionen stehen dabei zur Verfügung:

- **Weiterbildung.** Bestehende Mitarbeiter auf neue Aufgaben vorzubereiten bedeutet, dass das entsprechende Personal bereits mit Ihrer Kultur vertraut ist die spezifischen Systeme und Prozesse des Unternehmens zumindest teilweise beherrscht.
- **Mentoring.** Die Vermittlung von praktischen Kompetenzen durch erfahrenere Mitarbeiter ist eine wertvolle Möglichkeit, die Qualifikationen von Nachwuchskräften auszubauen und sie auf Erfolgskurs zu bringen.
- **Funktionsübergreifende Zusammenarbeit.** Eine bessere Kommunikation 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 sogar die Möglichkeit, Mitarbeiter zeitweise in anderen Abteilungen einzusetzen. Idealerweise werden dadurch die Kompetenzen und die Verantwortung auf andere Teams ausgeweitet. Ein besseres Sicherheitsverständnis in der Produktentwicklung könnte beispielsweise die Umsetzung von Secure-by-Design-Prinzipien in der Entwicklungspraxis fördern.

Die interne Suche nach Fachkräften – insbesondere aus verschiedenen Funktionen – bietet gleich mehrere Vorteile: Einerseits trägt sie zu einem stärkeren Bewusstsein dafür bei, dass jeder für die Sicherheit verantwortlich ist. Andererseits unterstützt sie auch die digitale Transformation. Da 40 % der Unternehmen befürchten, durch Initiativen zur digitalen Transformation anfälliger für Angriffe zu werden, kann eine integrierte Sicherheitskultur zu mehr Sicherheit im gesamten Transformationsprozess beitragen.

Abbildung 3
Fachkräftemangel

Die richtigen Tools für ein neues Bedrohungsumfeld

Da sich Bedrohungen für die Cybersicherheit ständig weiterentwickeln, müssen sich auch die Tools, mit denen wir uns davor schützen, entsprechend anpassen.

Social Engineering ist mit 37 % für viele Unternehmen der besorgniserregendste Bedrohungsvektor. Dazu gehören auch andere weit verbreitete Bedrohungen wie Phishing, das ein entscheidender Schritt bei Angriffen wie der Kompromittierung von Geschäfts-E-Mails und Ransomware ist (letztere ist mit 34 % die am zweithäufigsten gefürchtete Bedrohung).

Viele Bedrohungen überschneiden sich auch, was zusätzlich zur Komplexität des Bedrohungsumfelds beiträgt. Account-Übernahme (Account Takeover, ATO), die von 20 % der Befragten als Bedrohung genannt wurde, ist oft eine direkte Folge von Phishing. Datenexfiltration, die 28 % der Befragten Kopfschmerzen bereitet, ist eine häufige Folge von Ransomware-Angriffen.

Die von 20 % der Befragten erwähnte Kompromittierung durch Dritte ist nach Vorfällen wie dem SolarWinds Hack aus dem Jahr 2020 und dem Kaseya Ransomware-Angriff aus dem Jahr 2021 zu einer besonderen Sorge für Unternehmen geworden. In jüngster Zeit gelangten Amex Kreditkartendaten durch eine Sicherheitslücke bei Dritten an die Öffentlichkeit, und die Datenschutzverletzung bei UnitedHealth brachte große Teile des US-amerikanischen Gesundheitswesens zum Stillstand. *(Abbildung 4)*

Investitionen in Schutzmaßnahmen

Unternehmen investieren auf breiter Front, um sich zu schützen. Sie kaufen einige wohlüberlegte Produkte und Services, um Bedrohungen abzuwehren. Wir freuen uns, dass moderne Authentifizierungsfunktionen mit 35 % zu den beiden wichtigsten Investitionen gehören. Der Einsatz von Tools aus Bereichen wie Identitäts- und Zugriffsmanagement sowie Multi-Faktor-Authentifizierung wird dazu beitragen, Social-Engineering-Angriffe, die die Grundlage für viele andere Bedrohungen bilden, zu entschärfen.

Die zunehmende Bedrohung durch API-Missbrauch hat viele Unternehmen dazu veranlasst, in die Sicherheit ihrer API Gateways zu investieren (29 %). Derselbe Prozentsatz – also mehr als die 21 %, die die Exploits von Webanwendungen als Grund zur Sorge angaben – hat auch in Web Application Firewalls investiert, obwohl WAF-Produkte auch eine gängige Form der Verteidigung gegen andere Angriffe wie niedrigvolumige DDoS-Angriffe sind. Im Durchschnitt geben Unternehmen jährlich 1,58 Millionen US-Dollar für die Sicherheit ihrer Webanwendungen und APIs aus.

Überraschenderweise liegen Investitionen in den DDoS- und Bot-Schutz mit 25 % bzw. 15 % auf dem neunten respektive letzten Platz. Bots sind ein gängiges Mittel für Credential-Stuffing-Angriffe, die häufig zur Account-Übernahme eingesetzt werden.

Die Befragten investierten auch in Services zur Abwehr von Cyberbedrohungen. Ein Ansatz besteht dabei im Risikotransfer. Ein Ansatz besteht dabei im Risikotransfer. Cyberversicherungen liegen bei den Investitionen mit einem Spitzenwert von 35 % gleichauf mit moderner Authentifizierung. Eine weitere Möglichkeit ist das Outsourcing der Prävention und Reaktion auf Cyberbedrohungen an ein Unternehmen, das Managed Security Services anbietet. Diese Optionen nehmen 29 % der Befragten in Anspruch.

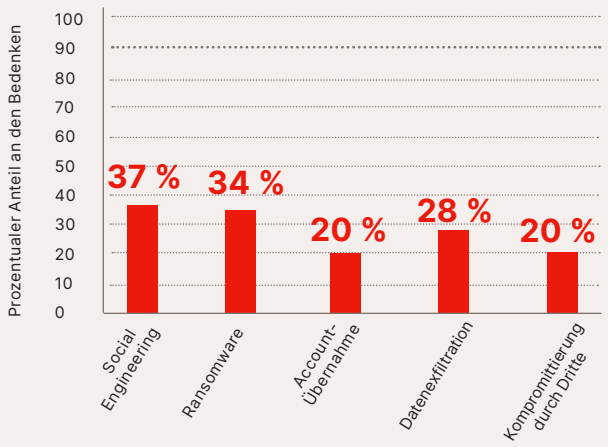
Unternehmen, die ihre Sicherheitsfunktionen outsourcen, greifen häufig auf mehrere Anbieter zurück. 27 % aller Befragten haben diesen Ansatz gewählt, während 32 % ihre Sicherheitsmaßnahmen von einem einzigen externen Serviceanbieter verwalten lassen. 17 % ziehen es vor, ihre Sicherheitsmaßnahmen im eigenen Haus zu bündeln, während 18 % eine Mischung aus beiden Ansätzen bevorzugen.

Die Toolsets sind nach wie vor fragmentiert

Überschneidungen bei den verwendeten Tools stellen für die Befragten ein Problem dar. Im Durchschnitt kommen in Unternehmen 7,85 Lösungen für die Netzwerk- und Anwendungssicherheit zum Einsatz, in Skandinavien sogar 9,4. Weit mehr als ein Drittel (37,7 %) dieser Tools überschneiden sich, obwohl sich die Lage im Vergleich zum Vorjahr (41 %) etwas gebessert hat.

Abbildung 4

Hauptgründe für die Konsolidierung von Tools



Höchste Zeit für Konsolidierung, Zentralisierung und von Anfang an integrierte Sicherheit

Mit Abstand die wichtigste Erkenntnis aus unserer Umfrage für das Jahr 2024 lautet: Es besteht ein Spannungsfeld zwischen zunehmenden Cyberbedrohungen und eingeschränkten Investitionen in die Cybersicherheit. 75 % der Befragten sind der Überzeugung, dass Cybersicherheit unverzichtbar ist, aber 50 % fühlen sich aufgrund unzureichender Investitionen in Schutzmaßnahmen gefährdet. Während viele von ihnen mehr in den Schutz investieren möchten, zeigt die Erfahrung, dass dieses Vorhaben nicht immer in die Tat umgesetzt wird. Dies liegt zum Teil daran, dass es schwierig ist, die Kosten gegenüber der Unternehmensleitung zu rechtfertigen, da Führungskräfte oft der Meinung sind, dass das Geld anderswo besser aufgehoben sei.

Die Abhängigkeit von fragmentierten und überlappenden Toolsets verschärft dieses Problem, da unnötig große Cybersicherheits-Stacks sowohl kostspielig als auch komplex zu integrieren sind. Außerdem sind solche Stacks eine natürliche Folge reaktiver Cybersicherheitsstrategien, die sich im Laufe der Zeit stückweise weiterentwickeln, um sich den Veränderungen im Bedrohungsumfeld anzupassen.

Zeit für „Security by Design“

Unternehmen müssen den wachsenden Cyberrisiken mit mehr Effizienz und innovativen Lösungen begegnen und gleichzeitig verhindern, dass Kosten und Komplexität überhandnehmen. Dies erfordert einheitliche Mechanismen zur Identifizierung und Abwehr von Bedrohungen, die auf das gesamte Unternehmen übertragbar sind.

Die Konsolidierung von Toolsets ist ein wesentlicher Bestandteil solcher Mechanismen, da sie zu einer geringeren Komplexität bei gleichzeitiger Kostensenkung beiträgt. Dies erfordert ein ausgereiftes Risikomanagement, bei dem die Funktionen der Tools anhand der möglichen Auswirkungen und der Wahrscheinlichkeit ihres Auftretens den einzelnen Risiken zugeordnet werden. Dies hängt wiederum von Faktoren wie Branche und Unternehmensgröße ab (siehe „Branchenspezifische Einblicke“).

Außerdem braucht es eine Reihe von universellen Sicherheitsgrundsätzen und den Willen, diese bei der Entwicklung von Produkten und Services für den Kunden bis hin zu internen Arbeitsabläufen anzuwenden, um die Sicherheit von innen heraus zu stärken.

Die Integration eines Sicherheitskonzepts, das bereits beim Design ansetzt („Secure by Design“) in die Softwarearchitektur steht nur bei 18 % der Befragten auf der Prioritätenliste und insgesamt an sechster Stelle unter den Abwehrmaßnahmen. Da dafür sowohl ein kultureller als auch ein technischer Wandel notwendig ist, die schwer unter einen Hut zu bringen sind, ist dies nur zu verständlich.

Es gibt aber auch noch ein weiteres Problem: 34 % unserer Befragten halten Cybersicherheit für eine Verschwendung von Zeit und Geld, die besser an anderer Stelle eingesetzt werden sollten. Diese Personen sind auch eher bereit, ihre Investitionen in die Cybersicherheit zu verringern (55 %).

Fastly CISO Marshall Erwin sieht ein weiteres Problem in der mangelnden Transparenz in Bezug auf die Cybersicherheit unter Führungskräften: „Ein effektives Sicherheitsprogramm mindert viele Risiken und verringert die Wahrscheinlichkeit von Sicherheitsverletzungen oder Zwischenfällen. Allerdings bleibt der direkte Mehrwert den Führungskräften meist verborgen.“

Die ablehnende Haltung gegenüber Cybersicherheitslösungen zu ändern, dürfte sich schwierig gestalten, aber eine direkte Verbindung zwischen Investitionen in Cybersicherheit und quantifizierbaren, risikobasierten Ergebnissen ist ein guter erster Schritt.

Branchenspezifische Einblicke

Bedrohungen der Cybersicherheit sind weit verbreitet, aber sie sind nicht gleichmäßig verteilt. Jede Branche hat mit eigenen Schwerpunktrisiken zu kämpfen. Dieses Jahr haben wir uns anstatt wie letztes Jahr vier, sechs Branchen angesehen.

Finanzwesen Zwei von fünf Cybersicherheitsexperten (41%), die in den Bereichen Finanzdienstleistungen und Buchhaltung tätig sind, erwarten, dass Social-Engineering-Angriffe wie Phishing und Smishing die größte Bedrohung für ihre Branche darstellen werden. Entscheider im Finanzwesen betrachten solche Angriffe mit einer um 10,8 % höheren Wahrscheinlichkeit als große Bedrohung als der Durchschnitt der anderen Branchen.

Öffentlicher Sektor Staatliche Behörden sind besonders von DDoS-Bedrohungen betroffen. Bei 15 % von ihnen kommt es aufgrund solcher Angriffe im Zuge der Zunahme geopolitischer Spannungen zu Serviceunterbrechungen. Das bedeutet aber nicht, dass es Angreifer nicht auch auf die Daten von Behörden abgesehen haben. Fast die Hälfte der Befragten (47 %) berichtete von Ausfallzeiten und mehr als ein Drittel (35 %) von Datenverlusten als Hauptfolgen von Sicherheitsvorfällen.

Fortsetzung auf der nächsten Seite

Branchenspezifische Einblicke *Fortsetzung*

Healthcare Während Kriminelle es bei Angriffen auf Finanzunternehmen direkt auf das Geld abgesehen haben, geht es im Gesundheitswesen um Patientendaten, mit denen sich im Dark Web viel Geld verdienen lässt. Aus diesem Grund haben 39 % der Unternehmen im Bereich Gesundheit / Life Sciences bereits Datenverluste durch Sicherheitsvorfälle erlitten – 7 % mehr als der Durchschnitt aller Branchen. Es ist also nicht verwunderlich, dass die Datenexfiltration in den nächsten 12 Monaten eine der größten Bedrohungen für Unternehmen im Gesundheitswesen darstellt.

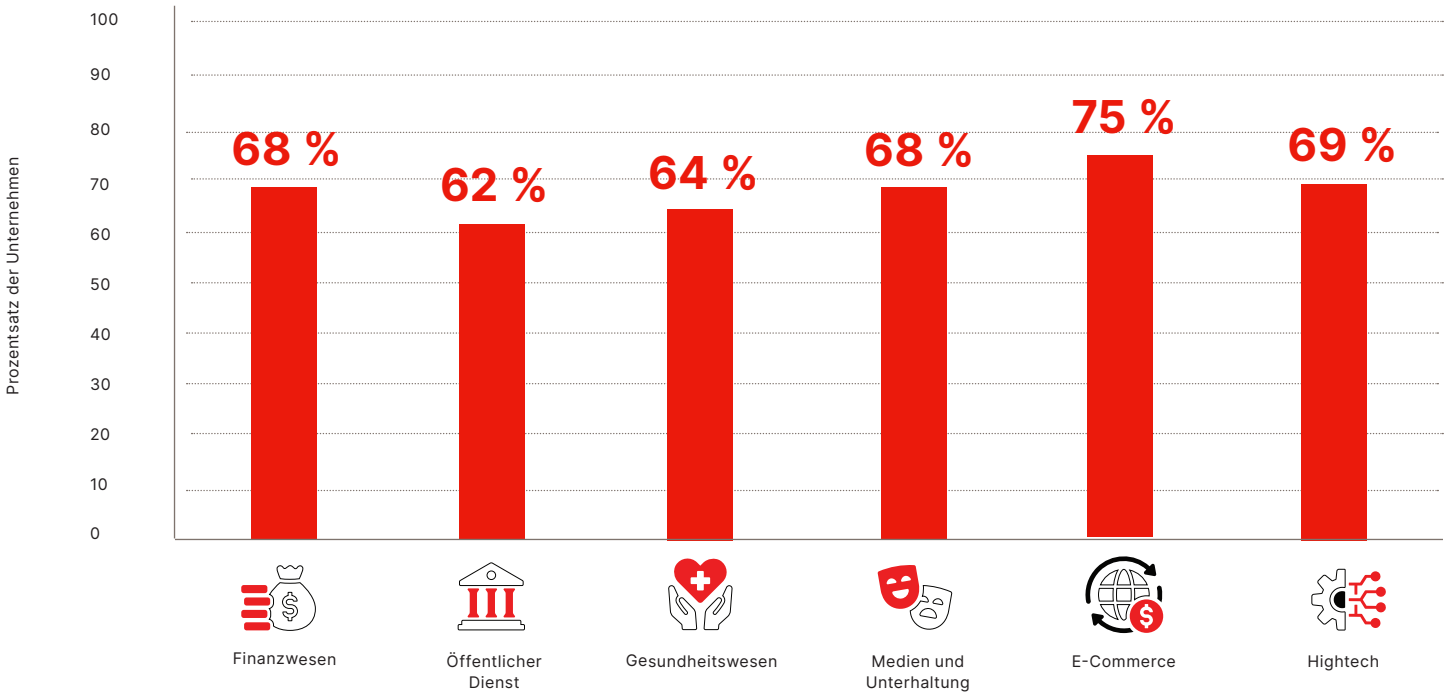
Medien und Unterhaltung Das wichtigste Gut dieser Branche ist Content. Cybersicherheitsexperten aus der Medien- und Unterhaltungsbranche befürchten im Vergleich zu anderen Branchen um 36 % häufiger, dass unautorisiertes Scraping urheberrechtlich geschützter Inhalte in den nächsten 12 Monaten zu den größten Bedrohungen gehören wird.

E-Commerce Einzelhändler sind mit Angriffen an mehreren Fronten konfrontiert, von gestohlenen Kreditkartendaten bis hin zu Versandbetrug und der Übernahme von Kundenkonten. Mehr als jeder fünfte Einzelhändler (22 %) rechnet damit, dass Account-Übernahmen die größte Bedrohung für die Cybersicherheit darstellen werden. Dies verdeutlicht wiederum die Notwendigkeit sicherer Authentifizierungslösungen.

Hightech Geistiges Eigentum ist der heilige Gral für Black-Hat-Hacker, die es auf Hightech-Unternehmen abgesehen haben. Nutzerkonten lassen sich jedoch auch leicht zu Geld machen, weshalb 22 % der Unternehmen in diesem Sektor Account-Übernahmen als größte Bedrohung für die Cybersicherheit in den nächsten 12 Monaten ansehen. Mitarbeiter aus dem Technologiebereich sind weniger besorgt darüber, dass Ransomware und Erpressung in den nächsten 12 Monaten zu den Hauptbedrohungen gehören werden.

Obwohl jede Branche mit ihren eigenen Risiken zu kämpfen hat, ist sich die Hälfte aller Befragten (52 %) in einem Punkt einig: Angesichts des immer komplexeren Bedrohungsumfelds sind sie schlecht auf zukünftige Angriffe vorbereitet.

Prozentsatz der Unternehmen, die in den letzten 12 Monaten von einem Sicherheitsvorfall betroffen waren



Über die Studie

Für diese Studie haben wir branchenübergreifend 1.800 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 September 2024 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. 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 mit ihren Edge-Computing-, Delivery-, Security- und Observability-Produkten bei der Auslieferung schneller, sicherer und ansprechender Onlineerlebnisse, indem sie ihnen eine bessere Website-Performance, mehr Sicherheit und Innovationen im globalen Maßstab ermöglicht. Im Vergleich zu anderen Anbietern sorgt Fastlys leistungsstarke, hochperformante und moderne Plattformarchitektur dafür, dass Entwickler sichere Websites und Anwendungen in kürzester Zeit bereitstellen und dabei nachweislich branchenführende Kosteneinsparungen erzielen können. Unternehmen weltweit vertrauen auf Fastly, wenn es darum geht, das von ihnen bereitgestellte Interneterlebnis zu verbessern, darunter Reddit, Neiman Marcus, Universal Music Group und SeatGeek. Weitere Informationen über Fastly erhalten Sie unter https://www.fastly.com/de oder unter @fastly.