ivanti

Reset drücken

Ein Bericht zum Stand der Cybersicherheit im Jahr 2023

Unternehmen liefern sich ein Wettrennen, um sich vor Cyberangriffen zu schützen. Doch die Branche kämpft mit einer reaktiven Checklisten-Mentalität.

Die Schokoriegel-Wette

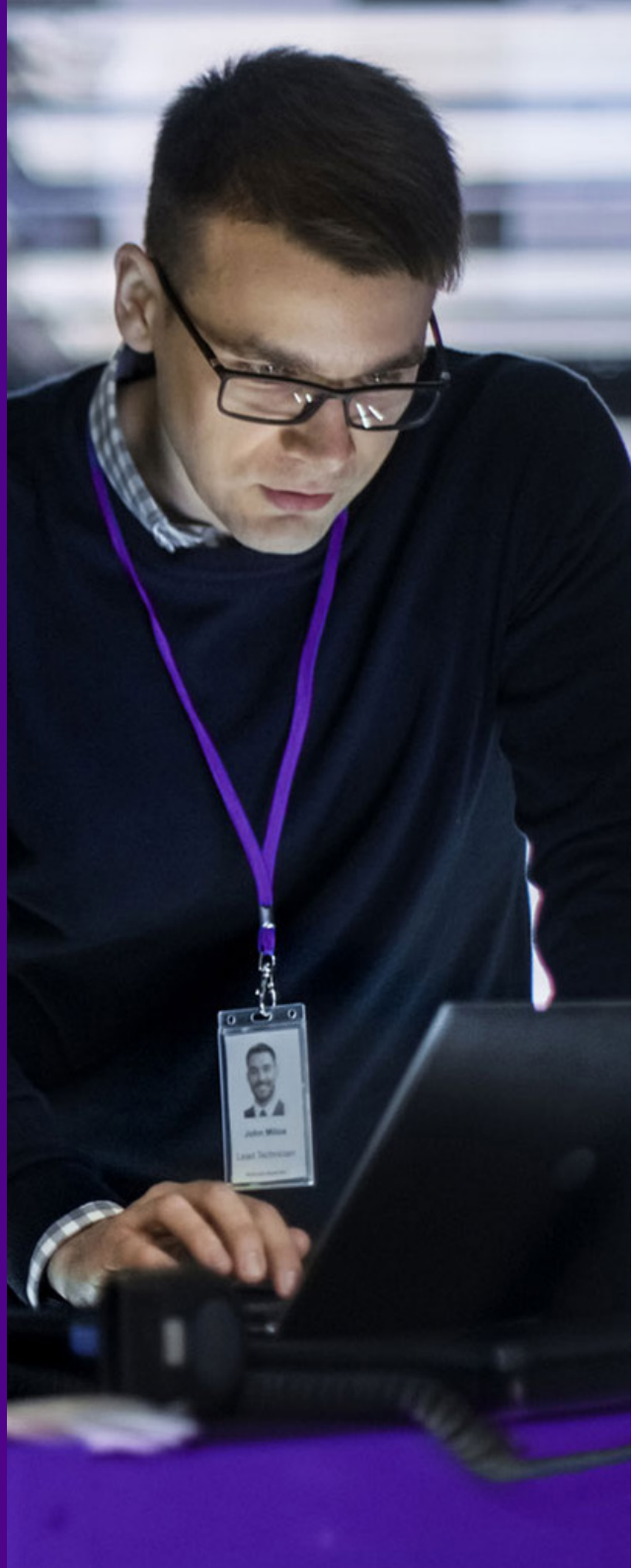
Wir befragten 1.356 Führungskräfte und Sicherheitsexperten über die Fähigkeit ihrer Unternehmen, eine schädliche Sicherheitsverletzung abzuwehren.

Würden Sie einen Schokoriegel auf die von Ihnen eingeführten Schutzmaßnahmen wetten?

1 von 5

befragten Fachleuten antwortete mit „Nein".

ivanti



Ist der Zustand der Cybersicherheit in Unternehmen so schlecht, dass 20 % nicht bereit wären, den Wert eines Schokoriegels – etwa 2 Euro – auf die Lage Ihrer Cybersicherheit zu setzen?

Was stimmt nicht, wenn ein Unternehmen die richtigen Mitarbeiter einstellt, die richtige Technologie kauft und alle richtigen Prozesse und Verfahren einführt, aber nicht bereit wäre, eine einfache Wette auf die Stärke seiner IT-Sicherheit einzugehen? Es ist vielleicht an der Zeit, unseren Ansatz für eine wirksame Cybersicherheit institutionell neu zu definieren.

Für unsere Forschungsreihe State of Cybersecurity Preparedness haben wir über 6.550 Fachleute befragt, um ein besseres Verständnis für die ernsthaften Probleme zu erhalten, mit denen Unternehmen konfrontiert sind – von neu auftretenden Cybersicherheits-Bedrohungen und knappen Budgets bis hin zu den verschiedenen Technologien und Prozessen, die Unternehmen zum Schutz einsetzen.

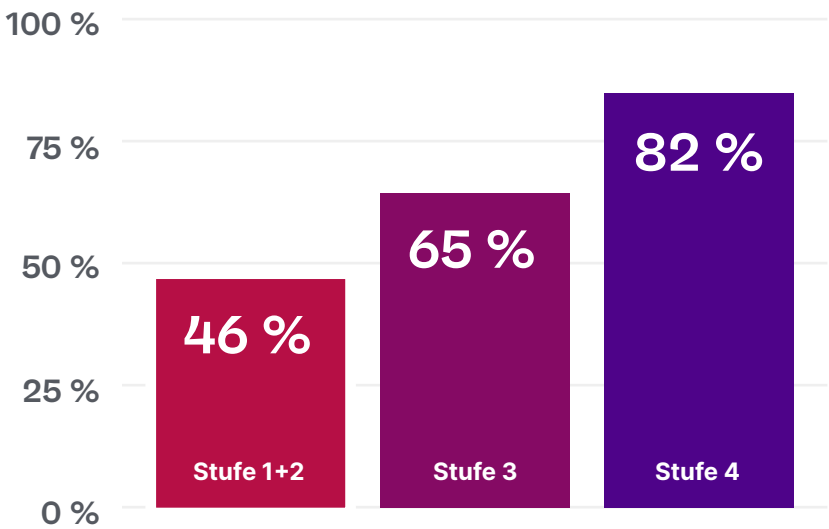
Außerdem betrachten wir das Problem aus drei Blickwinkeln – Unternehmensführung, Sicherheitsexperten und Wissensarbeiter – und nehmen uns etwas Zeit für die schockierenden Schwachstellen, die wir in der Chefetage gefunden haben.

Unser Ziel: Wir wollen der Frage auf den Grund gehen, warum Sicherheitsverantwortliche zwar optimistisch in Bezug auf ihre eigene Bereitschaft sind (denn das sind sie), aber gleichzeitig nicht bereit sind, einen Kit Kat®-Riegel darauf zu wetten – und wie sie ihren Ansatz für eine effektive, proaktive Cybersicherheitsstrategie und -praxis ändern können.

Inhalt:

Führungskräfte sind optimistisch, was die Abwehrbereitschaft angeht

F: Fühlen Sie sich im Vergleich zu vor einem Jahr mehr oder weniger gut auf die Abwehr von Cybersicherheitsangriffen vorbereitet?



„Ich fühle mich besser auf die Verteidigung vorbereitet als noch vor einem Jahr."

Die Reifegradgruppen für Cybersicherheit werden auf Seite 24 erläutert.

01

Sicherheit in einer hypervernetzten Welt

Eine kürzlich durchgeführte Umfrage von PwC ergab, dass „ein katastrophaler Cyberangriff das wichtigste Szenario in den Plänen für die Resilienz im Jahr 2023 ist", und dass zwei von drei Führungskräften Cyberkriminalität für die größte Bedrohung im nächsten Jahr halten.[1]

Was genau bedeutet es, in einer Welt zunehmender Verwundbarkeit und sogar völlig unbekannter Bedrohungen vorbereitet zu sein? Beginnen wir mit einer Einschätzung der Cybersicherheitslandschaft im Jahr 2023.

ivanti

Die Budgets für Cybersicherheit wachsen, um größeren und schädlicheren Bedrohungen gerecht zu werden

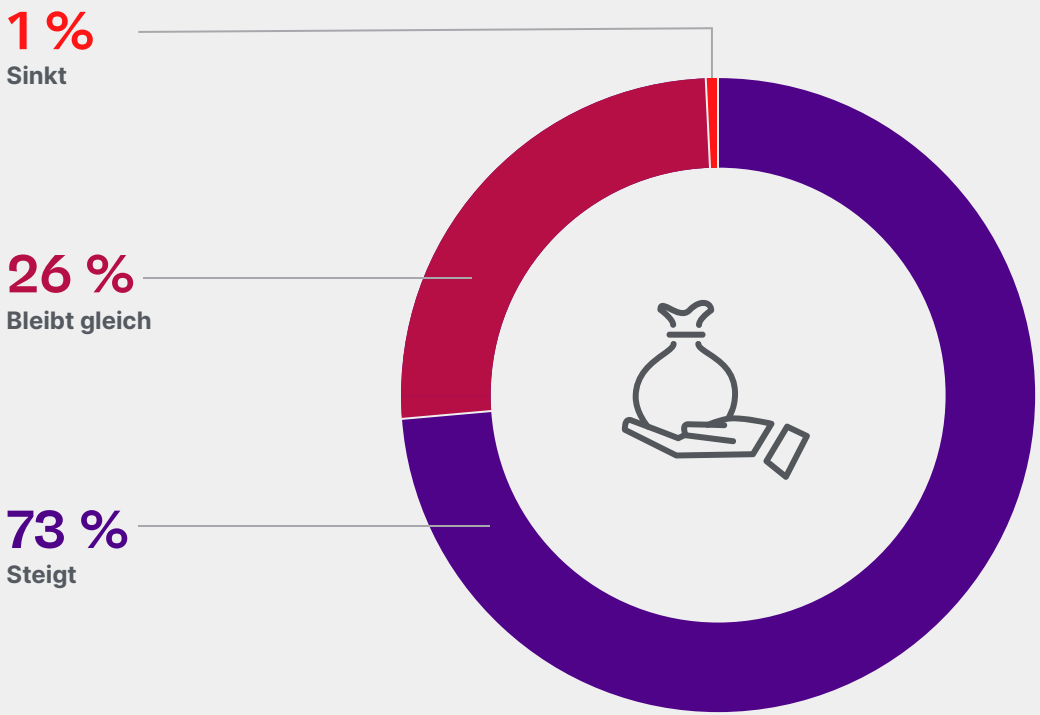
Von den von uns befragten Sicherheitsexperten und Führungskräften sagen 71 % eine Erhöhung ihres Cybersicherheitsbudgets im Jahr 2023 voraus – im Durchschnitt eine Steigerung von 11 %. Das ist etwa das Dreifache des erwarteten Budgetwachstums bei der Vergütung im Jahr 2023, so die Society for Human Resource Management.[2]

Lesley Salmon, Global Chief Information Officer bei Kellogg, sagte dem Wall Street Journal: „Wenn ich ein Budgetproblem habe, dann nicht im Bereich Cyber[sicherheit].“[3]

Der durchschnittliche Haushaltsanstieg für 2023 wird mit 11 % veranschlagt und liegt damit deutlich über der für denselben Zeitraum prognostizierten Inflation.

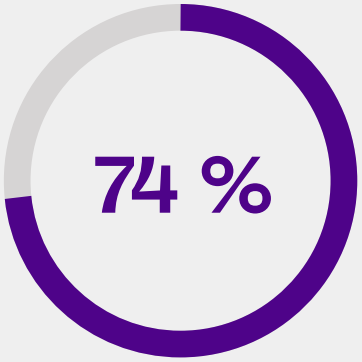
Die Budgets für Cybersicherheit steigen

F: Wird Ihr Budget für Cybersicherheit im Jahr 2023 im Vergleich zu 2022 steigen oder sinken?

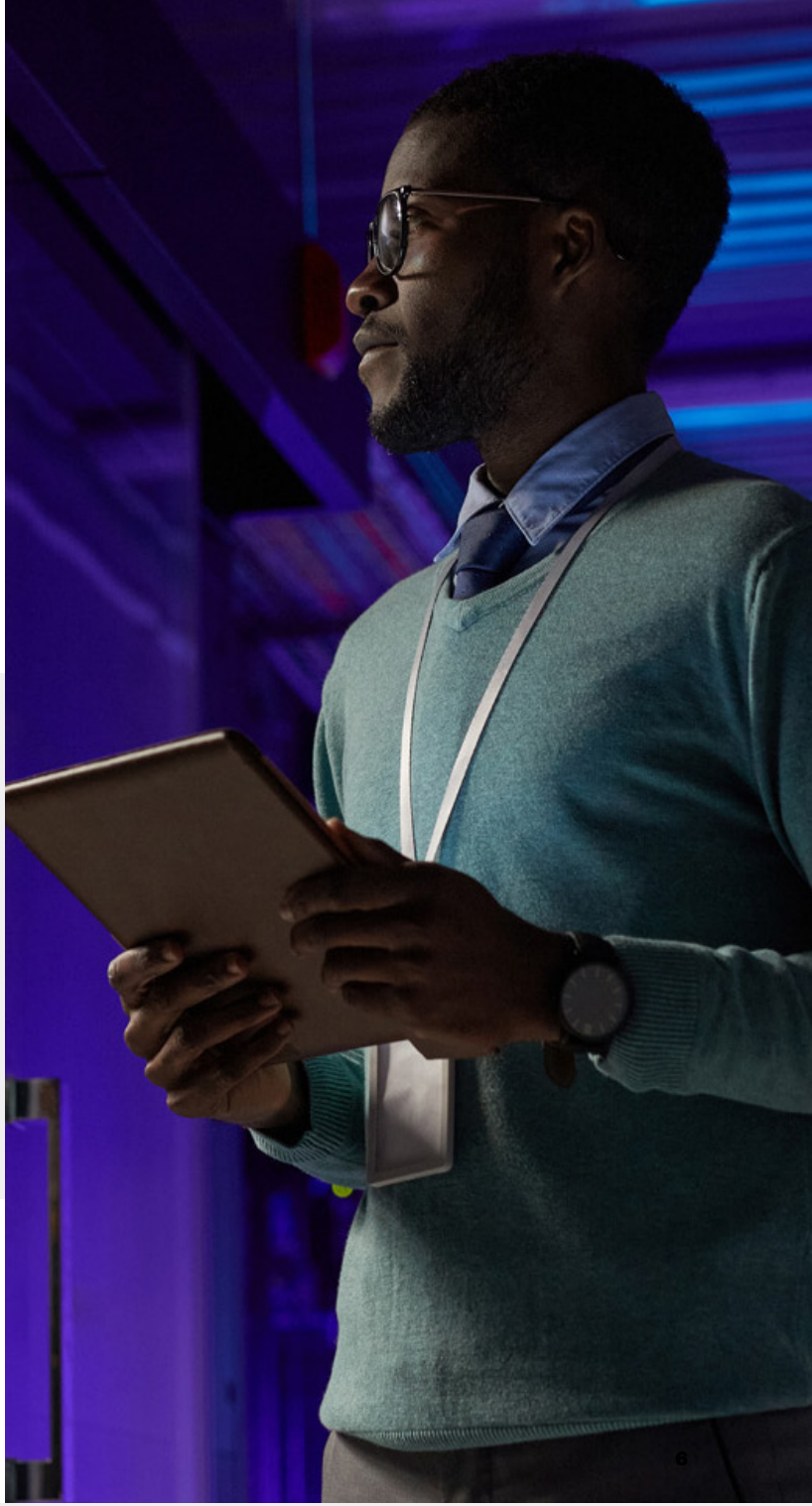


Fast drei von vier der von Ivanti befragten Sicherheitsexperten stellen Mittel für Sicherheitsverletzungen zur Verfügung, und das Budget für den „Notfallfonds" für Sicherheitsverletzungen macht etwa 16 % des gesamten Cybersicherheitsbudgets aus – eine beträchtliche Summe.

Der IBM-Bericht „Cost of a Data Breach 2022" stellt fest, dass die Kosten für die Wiederherstellung nach einer Datenschutzverletzung leicht siebenstellige Beträge erreichen können; im Durchschnitt gibt ein Unternehmen 4,35 Euro für die Wiederherstellung aus – und Branchen wie das Gesundheitswesen und das Bankwesen verzeichnen die höchsten Ausgaben für die Wiederherstellung.[4]



geben an, dass sie ein Budget für Sicherheitsverletzungen haben – und im Durchschnitt macht ein „Notfallfonds" für Sicherheitsverletzungen 16 % des gesamten Cybersicherheitsbudgets aus.



ivanti

Sicherheit wird durch große Lücken in der Sicherheitskompetenz und eine komplexe technische Ausstattung beeinträchtigt

„Die Komplexität des technischen Stacks" und „fehlende Sicherheitsfähigkeiten" sind die größten Hindernisse, die von Sicherheitsexperten und -leitern genannt werden – weit vor einem „unzureichenden Budget".

Komplexität des Tech-Stacks

Sicherheitsexperten geben an, dass sie im Durchschnitt sechs verschiedene Cybersicherheits-Tools und -Programme verwenden.

Charlie Bell, Sicherheitschef bei Microsoft, sagt, dass die Anhäufung von zu vielen Sicherheitsplattformen zu dem führt, was er eine „Art Frankenstein-Lösung" nennt. Bell erklärt: „Das Problem ist, dass es überall dort, wo man Dinge zusammenklebt, Nahtstellen gibt[,] und diese Nahtstellen werden zu Orten, an denen Menschen angreifen."[5]

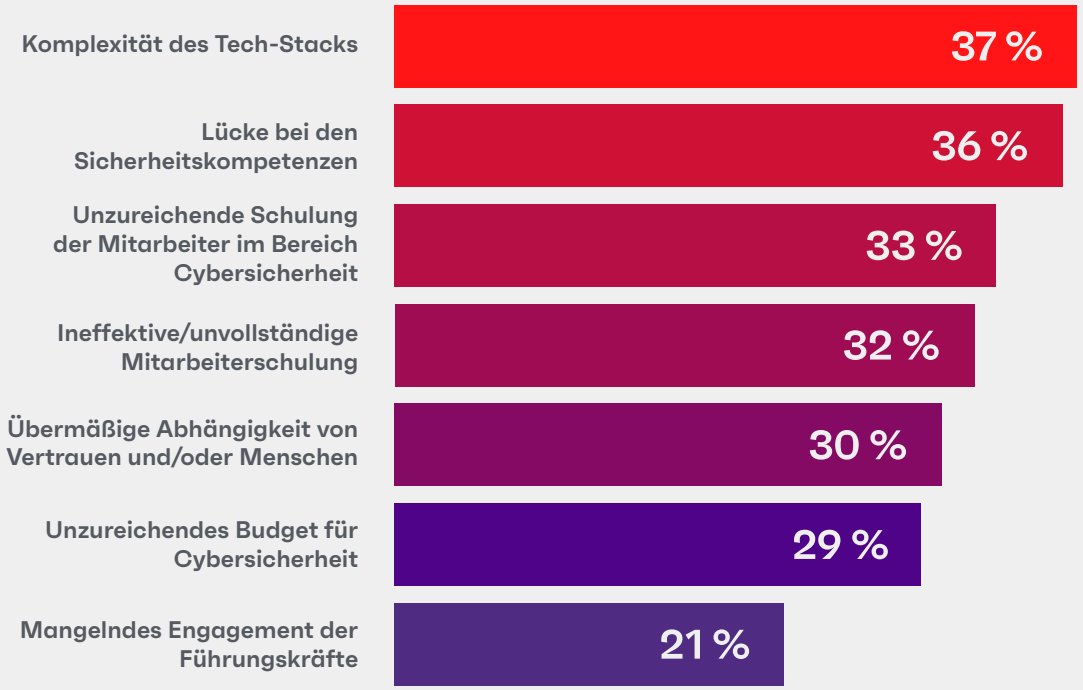
Lücke bei den Sicherheitskompetenzen

Für Sicherheitsexperten ist die „Qualifikationslücke" die mit Abstand größte Herausforderung, die von 39 % der befragten Sicherheitsexperten genannt wurde.

Diese Lücke untermauert die Ergebnisse zahlreicher anderer Studien, darunter ein aktueller Bericht des ISC2, der feststellt, dass die globale Lücke bei den Cybersicherheitsmitarbeitern im Jahr 2022 im Vergleich zu 2021 um 26,2 % gestiegen ist und 3,4 Millionen mehr Mitarbeiter benötigt werden, um Assets effektiv zu schützen.[6]

Komplexität und Talent stellen die größten Herausforderungen dar

F: Welches sind die größten Hindernisse für herausragende Cybersicherheit in Ihrem Unternehmen?



Der Wettlauf um das Risiko in der Lieferkette

Die digitale Transformation von Unternehmen – und all die Effizienz, die sich aus einer hochgradig vernetzten Lieferkette ergibt – bringt ein übergroßes Lieferkettenrisiko mit sich.

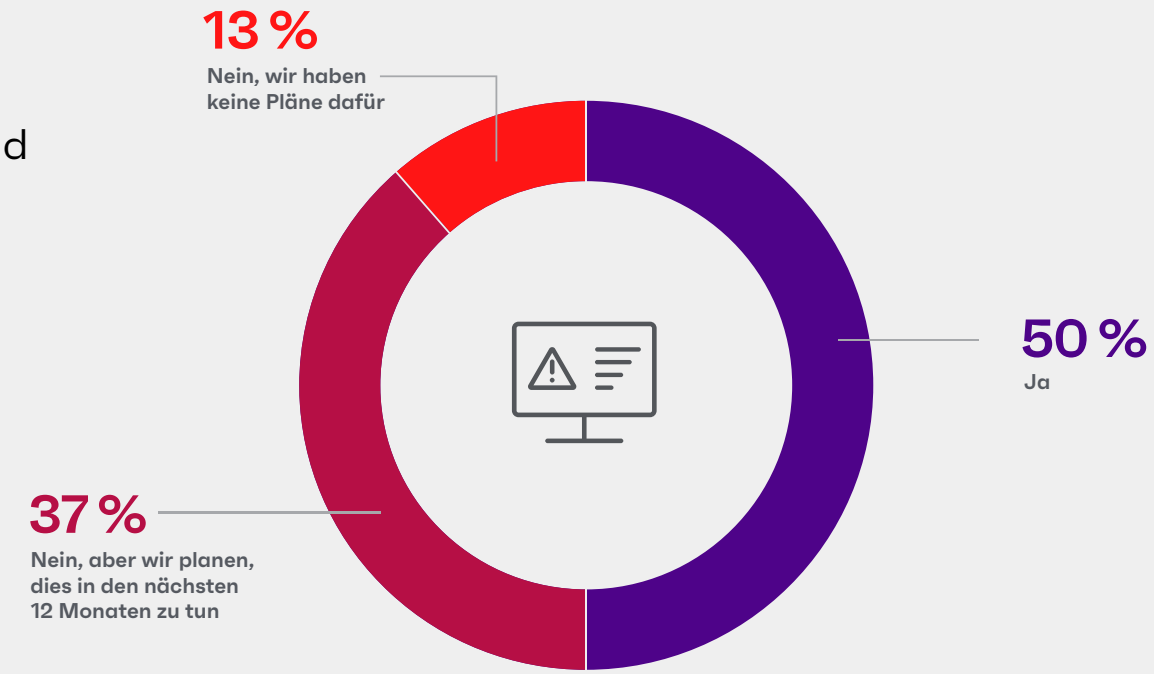
„Da die heutigen Lieferketten in hohem Maße miteinander verbunden sind, stellt eine Bedrohung eines Partners (z. B. eines Drittanbieters) eine Bedrohung für die gesamte Lieferkette dar", sagt Shaun McAlmont, Chief Executive Officer von Ninjio.[7]

CISOs und ihre Sicherheitsorganisationen beeilen sich, Schwachstellen in der Lieferkette zu erkennen und zu beheben, aber die meisten hinken immer noch hinterher.

In der Ivanti-Studie gaben weniger als die Hälfte (47 %) an, dass sie die Systeme und Komponenten von Drittanbietern, die in ihrer Software-Lieferkette am anfälligsten sind, bereits identifiziert haben, aber 35 % planen, dieses Risiko in den nächsten 12 Monaten anzugehen. Und 46 % stufen die Bedrohungen der Lieferkette für 2023 als „hoch" oder „kritisch" ein.

Risiken in der Lieferkette geben zunehmend Anlass zur Sorge

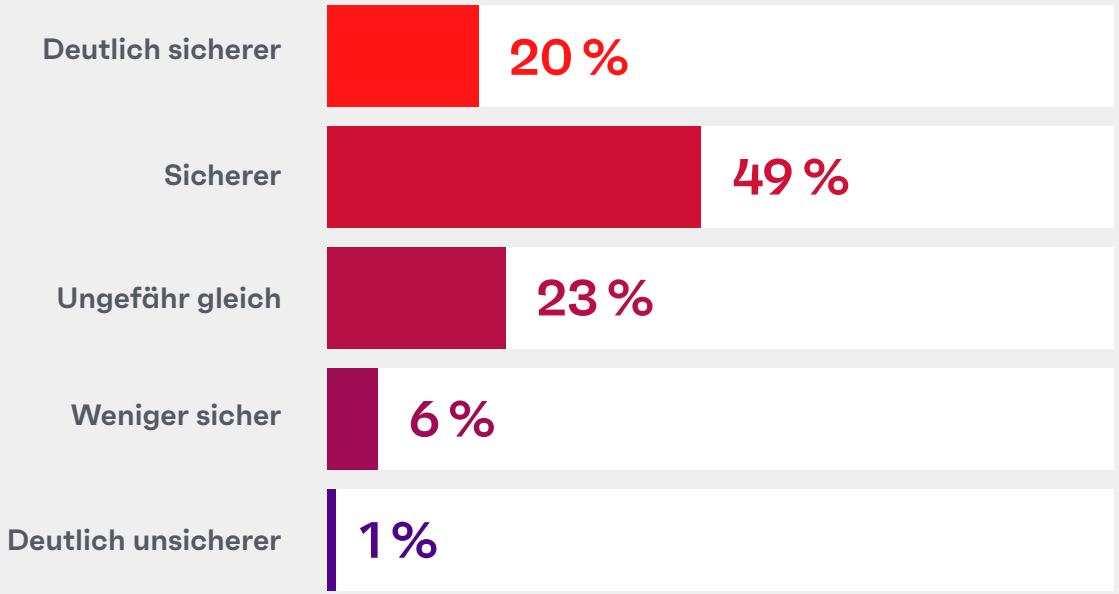
F: Hat Ihr Team die Systeme/Komponenten von Drittanbietern identifiziert, die in Ihrer Software-Lieferkette am verwundbarsten sind und im Falle einer Kompromittierung die größten Auswirkungen auf das Unternehmen haben werden?



Cloud-basiertes Risiko überbewertet?

Cloud-basierte Systeme sind ein Gewinn an Sicherheit

F: Betrachten Sie sowohl die Sicherheitsrisiken als auch die Chancen einer Cloud-Umgebung. Sind Sie der Meinung, dass Ihre Systeme durch die Einführung von Cloud-basierten Systemen und/oder Speichersystemen sicherer oder unsicherer werden?



Mehr als zwei von drei Unternehmen (68 %) geben an, dass ihre Systeme durch die Einführung von Cloud-basierten Systemen und/oder Speicherlösungen sicherer geworden sind.

Mit anderen Worten: Trotz der falschen Annahme, dass Cloud-basierte Systeme Unternehmen nicht zu vertretenden Sersicherheitsrisiken aussetzen, sind die von uns befragten Führungskräfte und Sicherheitsexperten der Meinung, dass die Cloud-basierte Umgebung nach Abwägung der Risiken und Chancen mehr Sicherheit bietet.

„Die Gewährleistung einer positiven und sicheren digitalen Mitarbeitererfahrung ist der neue Eckpfeiler für moderne IT-Führungskräfte", sagt Andy Stone, Chief Technology Officer bei Pure Storage. „Durch die sichere und effektive Nutzung der Cloud können Unternehmen ihren Mitarbeitern die Möglichkeit geben, an jedem beliebigen Ort und mit jedem beliebigen Gerät zu arbeiten. In einer digitalisierten Welt stagniert das Wachstum eines Unternehmens weitgehend, wenn es nicht gelingt, sicher auf die Cloud umzusteigen."

02

Hotspots für Cybersicherheit im Jahr 2023

Was sehen Cybersicherheits-Insider als die größten Bedrohungen für 2023? Und wie bereiten sich die Unternehmen auf bekannte und unbekannte Angriffe vor?

ivanti

Abwehrbereitschaft und Erfahrungslücken

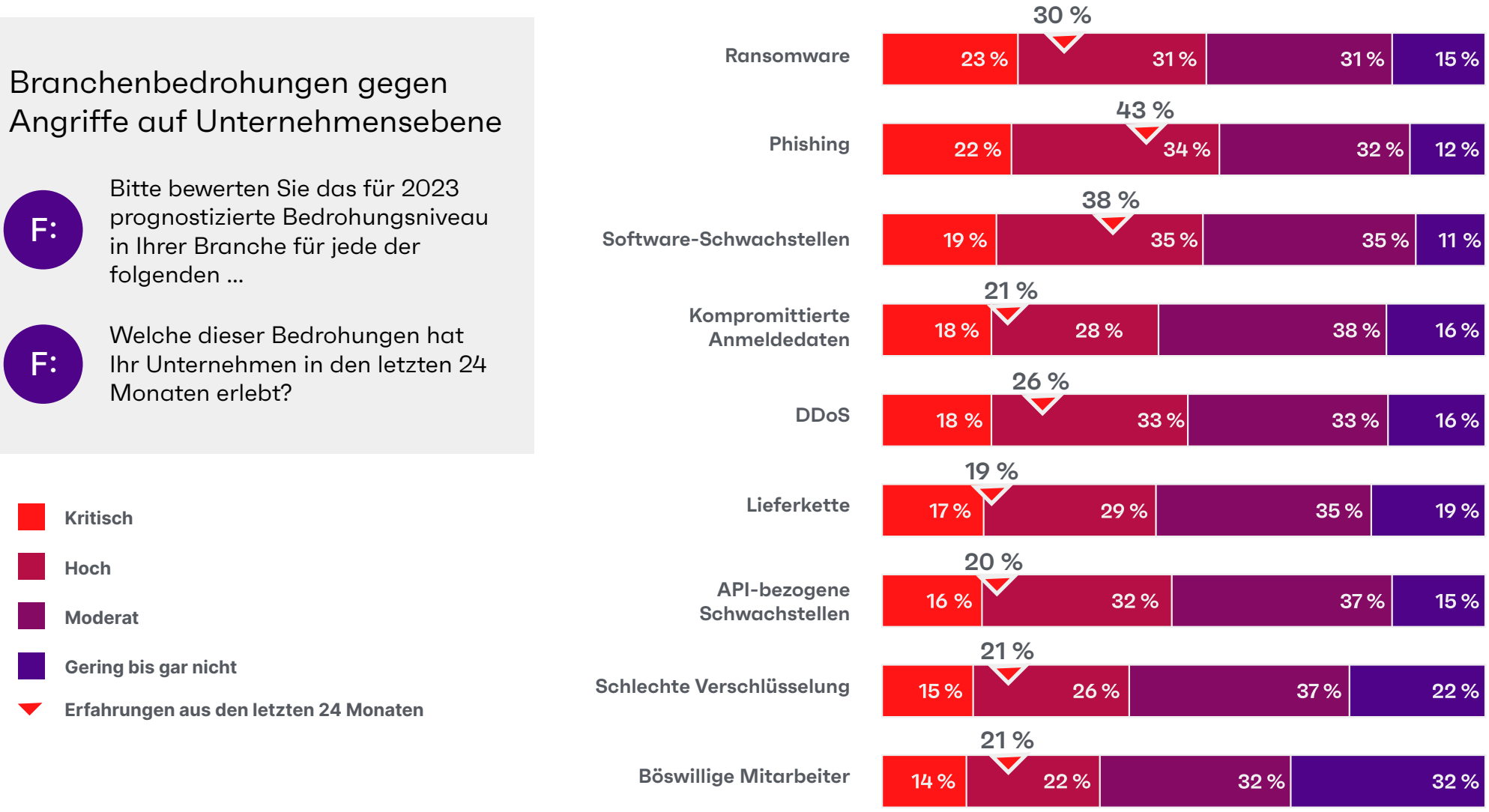
Die von uns befragten Fachleute nennen Phishing, Ransomware und Softwareschwachstellen als die größten Bedrohungen auf Branchenebene.

Vergleicht man die tatsächlichen Angriffe, denen Unternehmen ausgesetzt waren, so übertreffen Phishing und Software-Schwachstellen andere Risiken um ein Vielfaches.

Branchenbedrohungen gegen Angriffe auf Unternehmensebene

F: Bitte bewerten Sie das für 2023 prognostizierte Bedrohungsniveau in Ihrer Branche für jede der folgenden ...

F: Welche dieser Bedrohungen hat Ihr Unternehmen in den letzten 24 Monaten erlebt?



Ein Umfrageteilnehmer berichtet:

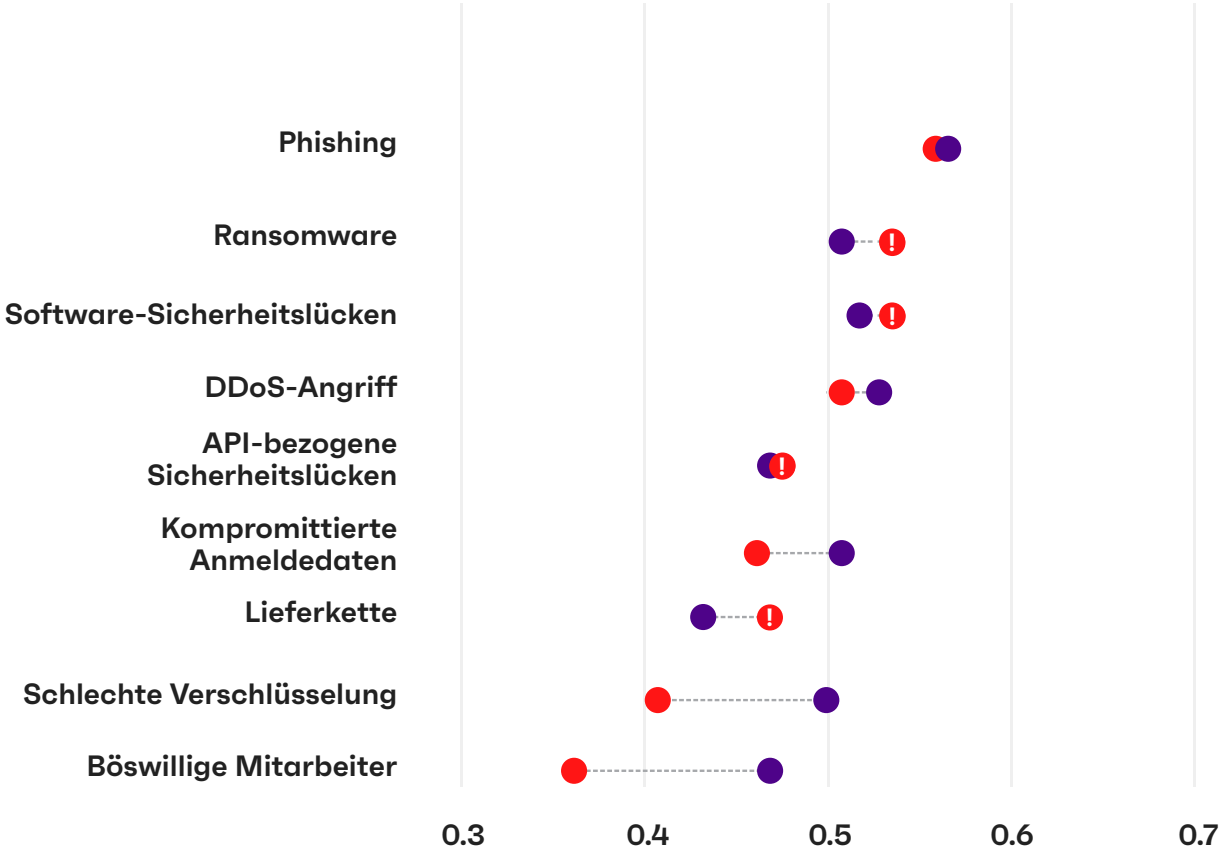
„Wir haben ein paar fortgeschrittene Phishing-Versuche erlebt, und die Angestellten wussten gar nicht, dass sie angegriffen wurden. Diese Art von Angriffen ist in den letzten zwei Jahren sehr viel raffinierter geworden – selbst unsere erfahrensten Mitarbeiter fallen ihnen zum Opfer."

Trotz der Vielfalt der Bedrohungen gibt ein großer Teil der Befragten an, dass sie auf die wachsende Bedrohungslandschaft vorbereitet sind. Etwa die Hälfte gibt an, „sehr gut" auf die zahlreichen Bedrohungen vorbereitet zu sein, darunter Ransomware, schlechte Verschlüsselung, böswillige Mitarbeiter und Software-Schwachstellen.

Ein Hotspot: Schwachstellen in der Lieferkette. Nur 42 % geben an, dass sie sehr gut auf die Bedrohungen in der Lieferkette vorbereitet sind, obwohl 46 % diese Bedrohung als sehr hoch einstufen.

Dieses Risiko war nur eine von mehreren „umgekehrten" Bedrohungen, bei denen der Bereitschaftsgrad hinter dem geschätzten Bedrohungsniveau zurückbleibt.

Sicherheitsbedrohungen versus Sicherheitsvorkehrungen



F: Bitte bewerten Sie das für 2023 prognostizierte Bedrohungsniveau in Ihrer Branche für jede der folgenden ...

F: Wie gut ist Ihr Unternehmen auf jede der hier aufgeführten Arten von Bedrohungen vorbereitet?

- Hohe + kritische Bedrohung
- „Sehr gut vorbereitet"
- Umgekehrte Bedrohung

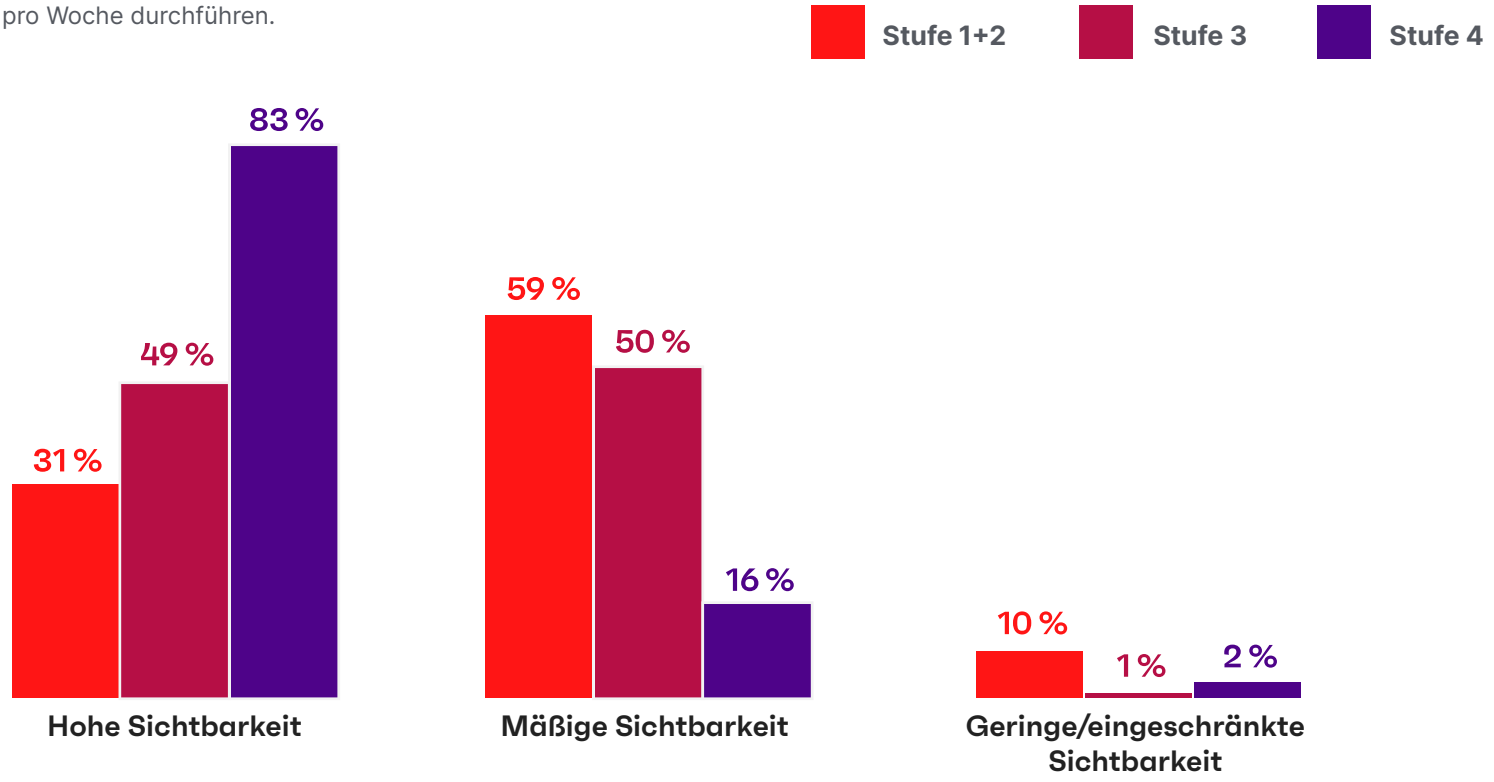
Erwartete Sicherheitsvorkehrungen wurden als ernsthaft unzureichend eingestuft

Etwas mehr als die Hälfte der Führungskräfte und Sicherheitsexperten (52 %) geben an, dass sie einen “sehr guten Blick” auf jeden Benutzer, jedes Gerät, jede Anwendung und jeden Dienst in ihrem Netzwerk haben.

Und nur 48 % geben an, dass sie ihr Asset-Discovery-Programm mindestens einmal pro Woche durchführen.

Erstklassige Unternehmen berichten über eine hohe Transparenz ihrer Assets

F: Welchen Grad an Transparenz hat Ihr Unternehmen in Bezug auf jeden Benutzer, jedes Gerät, jede Anwendung und jeden Dienst in Ihrem Netzwerk? (Dargestellt nach Reifegrad der Cybersicherheit.)

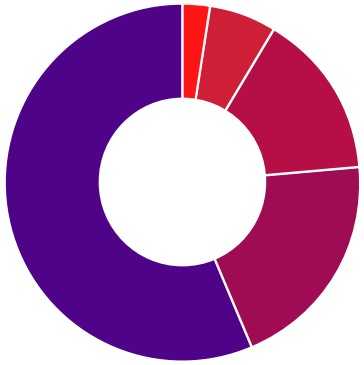


Fast alle geben an, dass sie über ein formelles Verfahren für die Deprovisionierung verfügen, und die große Mehrheit (68 %) gibt an, dass die Deprovisionierung für ausscheidende Mitarbeiter innerhalb von drei Werktagen erfolgt. (Bei externen Anbietern geben 81 % an, dass der Vorgang innerhalb von 5 Werktagen abgeschlossen ist).

Sicherheitsexperten berichten uns jedoch auch, dass die Deprovisioning-Anleitung in einem Drittel der Fälle ignoriert wird – ein erstaunliches Eingeständnis angesichts der damit verbundenen Gefahr.

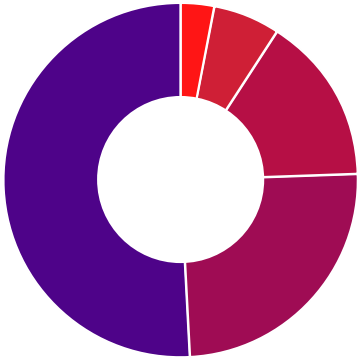
Mit Deprovisionierung, guten Protokollen, aber gemischten Ergebnissen

F: Wie schnell können Sie die Berechtigungsnachweise eines Mitarbeiters nach dessen Ausscheiden aus dem Unternehmen entziehen?



- 2 % Wir haben kein offizielles Verfahren für den Entzug von Berechtigungsnachweisen
- 5 % Weiß nicht
- 12 % Mehr als 7 Tage
- 16 % 4-7 Tage
- 45 % 2-5 Arbeitstage

F: Wie schnell können Sie die Berechtigungsnachweise von Drittanbietern, Beratern und/oder Auftragnehmern nach Ablauf eines Vertrags oder nach Beendigung einer Dienstleistung entziehen?



- 2 % Wir haben kein offizielles Verfahren für den Entzug von Berechtigungsnachweisen
- 4 % Weiß nicht
- 10 % Mehr als 7 Tage
- 16 % 4-7 Tage
- 33 % 2-3 Arbeitstage

Die Epidemie der Zombieberechtigungen

Noch eklatanter: 45 % der Befragten gaben an, den Verdacht zu haben, dass ehemalige Mitarbeiter und Auftragnehmer immer noch aktiven Zugang zu Unternehmenssystemen und -dateien haben – sei es, weil die Anweisungen zur Deprovisionierung nicht korrekt befolgt wurden oder weil Anwendungen von Drittanbietern auch nach der Deaktivierung der Anmeldedaten einen versteckten Zugang bieten.

„Große Unternehmen versäumen es oft, das riesige Ökosystem von Anwendungen, Plattformen und Diensten von Drittanbietern zu berücksichtigen, die weit über das Ausscheiden eines Mitarbeiters hinaus Zugriff gewähren", sagt Dr. Srinivas Mukkamala, Chief Product Officer bei Ivanti. „Wir nennen das Zombie-Berechtigungen, und eine schockierend große Anzahl von Sicherheitsexperten – und sogar Führungskräfte – haben immer noch Zugang zu den Systemen und Daten ihrer früheren Arbeitgeber."

45 %

der Sicherheitsexperten geben an, dass sie entweder vermuten oder wissen, dass ehemalige Mitarbeiter und Auftragnehmer immer noch aktiven Zugang zu Systemen oder Dateien in Form von noch aktiven Benutzernamen, Kennwörtern und Anmeldeinformationen haben.

Die Anleitung zur Deprovisionierung wird nur in 68 % der Fälle befolgt.

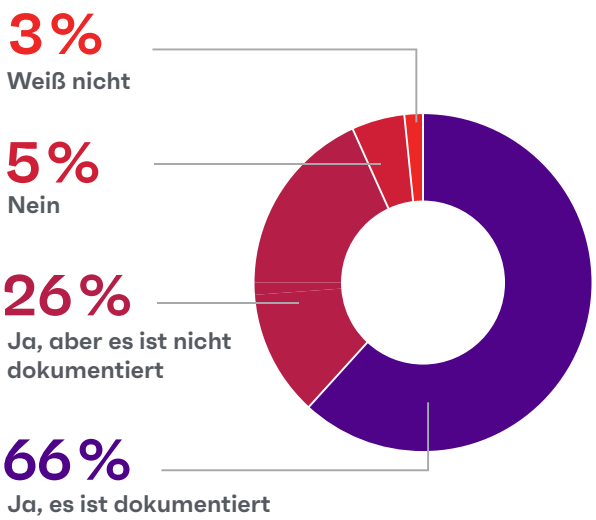
ivanti

Wenn jeder Patch eine Priorität ist, wird kein Patch priorisiert

92 % geben an, dass sie über eine Methode zur Priorisierung der zu patchenden Schwachstellen verfügen, obwohl mehr als ein Viertel der Befragten angibt, dass diese Methoden in keiner Weise dokumentiert sind.

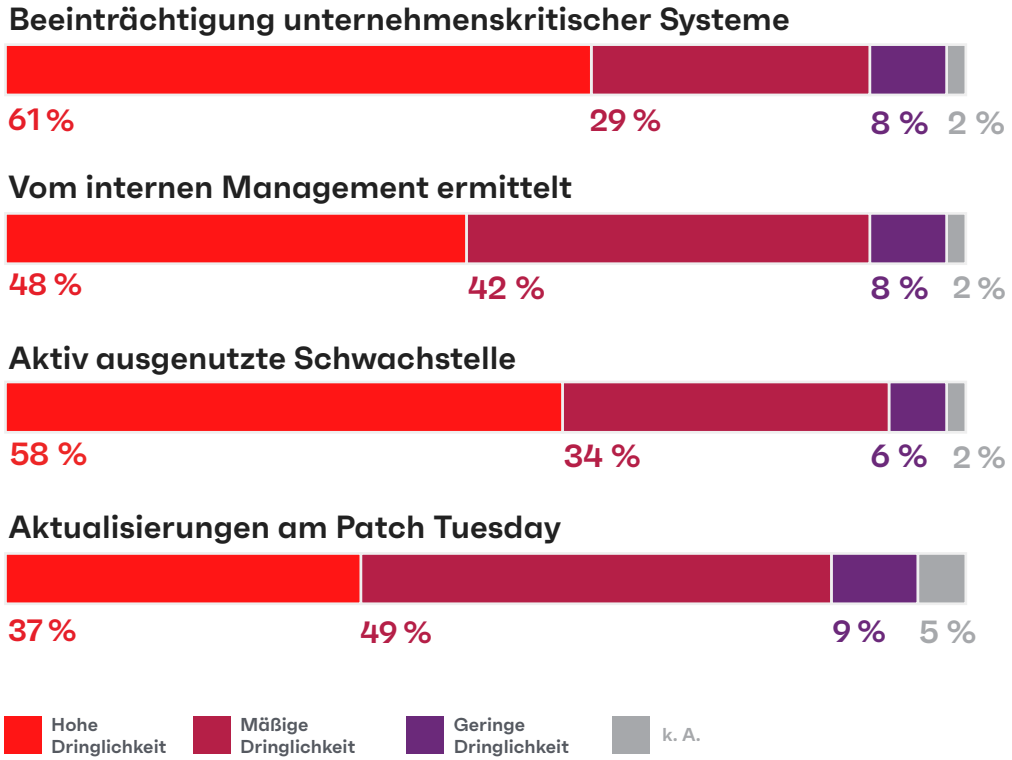
Auf die Frage, welche Arten von Patches Vorrang haben, sagen uns die Sicherheitsexperten, dass alle Arten von Patches einen hohen Stellenwert haben – was bedeutet, dass es keine gibt.

F: Verfügt das Cybersicherheitsteam über eine Methode zur Priorisierung der zu flickenden Schwachstellen?



Patch-Management leidet unter dem Motto „alles ist dringend".

F: Wie setzen Sie Prioritäten bei der Auswahl der zu patchenden Schwachstellen?



Diese „Alles ist dringend"-Mentalität bringt nicht nur die Prioritäten des Sicherheitsteams durcheinander, sondern kann auch zu einem hohen Maß an Stress und Burnout führen.

Eine von IBM durchgeführte weltweite Umfrage unter 1.100 Incident Respondern ergab, dass 68 % der Befragten angaben, dass es üblich sei, gleichzeitig mit zwei oder mehr Vorfällen betraut zu sein. In der Studie heißt es: „Die Arbeit scheint ihren Tribut zu fordern: Eine ähnliche Zahl, nämlich 64 %, gab an, wegen Schlaflosigkeit, Burnout und Angstzuständen psychologische Hilfe in Anspruch genommen zu haben." [8]

Eine frühere Umfrage von Ivanti deckte ähnliche Herausforderungen auf: Auf die Frage, was die Fluktuation fördert, nannten IT-Fachleute vor allem eine hohe Arbeitsbelastung (41 %) und unrealistische Erwartungen an das Team (34 %).[9]

03

Die Gefahren des Whale-Phishings

Whale-Phishing bedeutet, dass Cyberbedrohungen maßgeschneiderte Spear-Phishing-Techniken einsetzen, um „Wale" zu jagen – wichtige, hochrangige Ziele wie CEOs, Politiker oder hohe Regierungsbeamte.

Ist ein „Wal" erst einmal kompromittiert, können Angreifer Zugang zu sensiblen Informationen erhalten, Überweisungen genehmigen und sogar Mitarbeiter zu bestimmten Handlungen zwingen, denen sie normalerweise nie zustimmen würden – aber wenn der Chef sagt „spring" ...!

ivanti

Führungskräfte geben an, dass sie sich der Cybersicherheitsrisiken bewusst sind, aber dennoch riskante Verhaltensweisen an den Tag legen

Fast 9 von 10 Führungskräften (z. B. CEOs, Vizepräsidenten und Direktoren) geben an, dass sie darauf vorbereitet sind, Bedrohungen wie Malware und Phishing bei der Arbeit zu erkennen und zu melden.

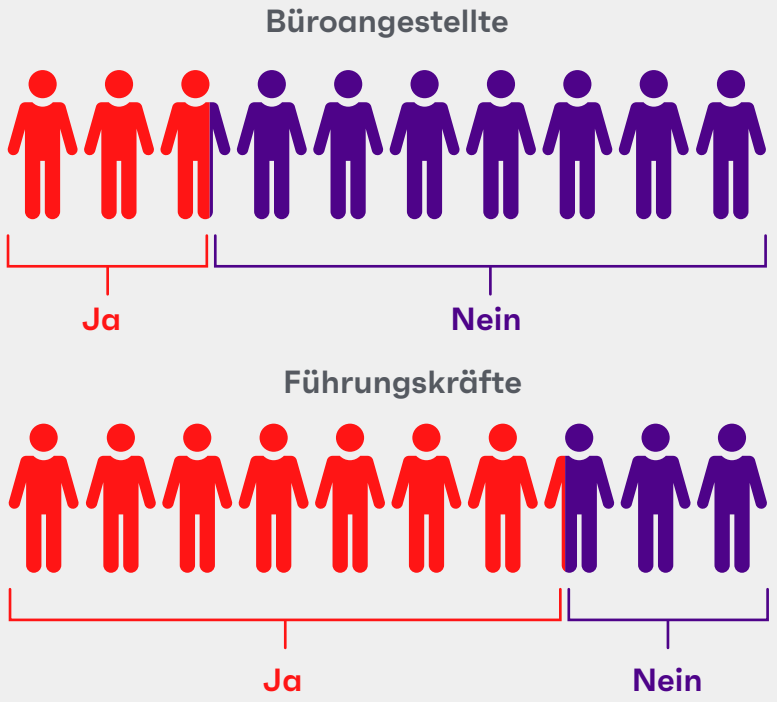
Und im Vergleich zu anderen von uns befragten Mitarbeitern geben sie deutlich häufiger an, dass sie sich mit einer Frage oder einem Anliegen an das Sicherheitsteam gewandt haben.

Dies sind gute Anzeichen. Unsere Untersuchungen zeigen jedoch, dass Führungskräfte viel häufiger über negative Interaktionen mit dem Sicherheitsteam berichten und 1,3-mal häufiger sagen, dass sie sich bei der Meldung von Sicherheitsmängeln „nicht sicher fühlen".

Darüber hinaus sind ihre Handlungen – die alltäglichen Gewohnheiten, zu denen sich die Leiter von Organisationen bekennen – sogar noch besorgniserregender.

Führungskräfte sagen, dass sie sich für die Sicherheit engagieren

F: Haben Sie sich schon einmal mit einer Sicherheitsfrage oder einem Anliegen an einen Mitarbeiter für Cybersicherheit an Ihrem Arbeitsplatz gewandt?



Führungskräfte zeigen häufiger gefährliche Verhaltensweisen

Fachleute wie CEOs, Vizepräsidenten und Direktoren – Personen, die wir in unserer Umfrage als „Führungskräfte" bezeichnet haben – praktizieren mit größerer Wahrscheinlichkeit ein unsicheres Sicherheitsverhalten als andere Wissensarbeiter.

- Mehr als ein Drittel der befragten Führungskräfte hat schon einmal auf einen Phishing-Link geklickt – viermal so häufig wie andere Büroangestellte!
- Fast jede vierte Führungskraft verwendet leicht zu merkende Geburtstage als Teil ihres Passworts
- Die Wahrscheinlichkeit, dass Führungskräfte Passwörter jahrelang aufbewahren, anstatt sie regelmäßig zu aktualisieren, ist viel größer als bei anderen Arbeitnehmern; jeder Vierte tut dies.
- Bei den befragten Führungskräften ist die Wahrscheinlichkeit, dass sie ihr Passwort an Personen außerhalb des Unternehmens weitergeben, fünfmal höher.

Eine erfolgreiche Whale-Phishing-Kampagne stellt eine viel größere Schwachstelle dar als herkömmliche Phishing-Versuche, doch viele Unternehmen behandeln sie noch immer nicht als einzigartige, übergroße Bedrohung.

Bedenken Sie dies: Führungskräfte – also Personen, auf die besonders raffinierte Phishing-Kampagnen abzielen – werden viermal häufiger Opfer von Phishing als alle anderen Büroangestellten.

(Wiederholen wir das für den Fall, dass Sie im Schnelldurchlauf lesen: Es ist viermal wahrscheinlicher, dass Ihre wertvollsten Mitarbeiter eine Handlung vornehmen, die die Sicherheitstüren für böswillige Akteure öffnet).

Allein dieses Risiko bedeutet, dass Unternehmen maßgeschneiderte Schulungsprogramme und technische Maßnahmen für CEOs und andere hochrangige Führungskräfte entwickeln müssen – zusätzliche Schutzschichten für diese hochgradig gefährdeten Ziele.

Mehr als 1 von 3 Führungskräften – wie CEOs, VPs und Geschäftsführer – sind Opfer von Phishing-Betrügereien geworden, indem sie entweder auf einen betrügerischen Link geklickt oder Geld geschickt haben.

04

Wie Unternehmen für das Jahr 2023 – und darüber hinaus – zukunftssicher gemacht werden können

Im Rahmen der Ivanti-Studie untersuchte das Forschungsteam Unternehmen, die sich selbst als fortschrittliche Cybersicherheitsunternehmen einstufen – Stufe 4 auf der Reifegradskala für Cybersicherheit. Wir wollen wissen: Welche Wegweiser zeichnen diese Gruppe aus? Und wie können andere Unternehmen von ihnen lernen?

ivanti

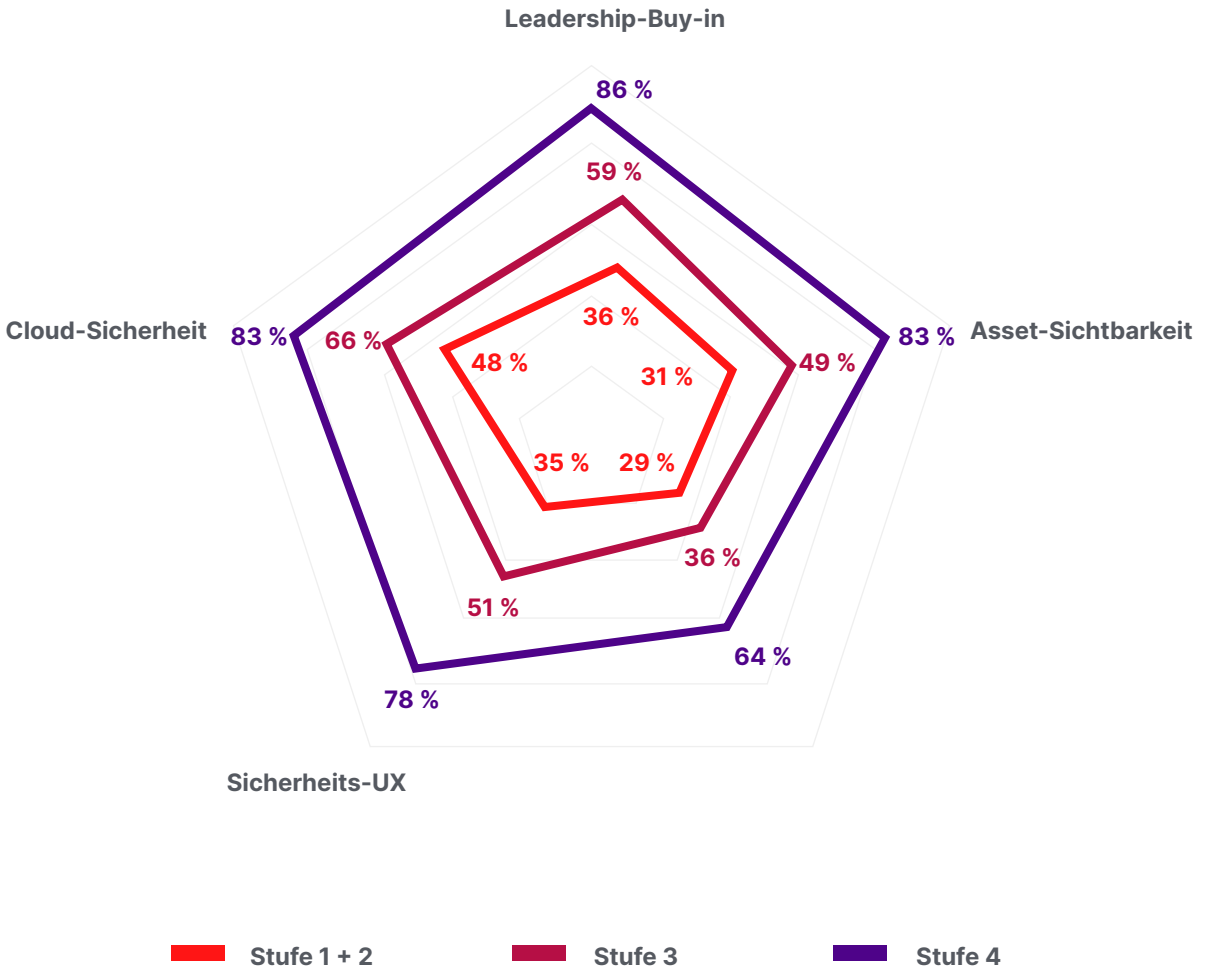
Die Reifegradskala der Cybersicherheit

Wir haben die Umfrageteilnehmer, die im Bereich der Cybersicherheit tätig sind, gebeten, den Grad der Vorbereitung der Cybersicherheit ihres Unternehmens zu bewerten – von grundlegend (Stufe 1) bis erstklassig (Stufe 4). Anschließend verglichen wir diese Kohorten, um mehr über die Praktiken und Verhaltensweisen von Unternehmen der Stufe 4 zu erfahren.

Ausgereiftere Cybersicherheitsunternehmen berichten von einer stärkeren Zustimmung, erhöhter Aufmerksamkeit für Transparenz und UX

Die Diagramme zeigen den prozentualen Anteil der Befragten, die Folgendes angaben:

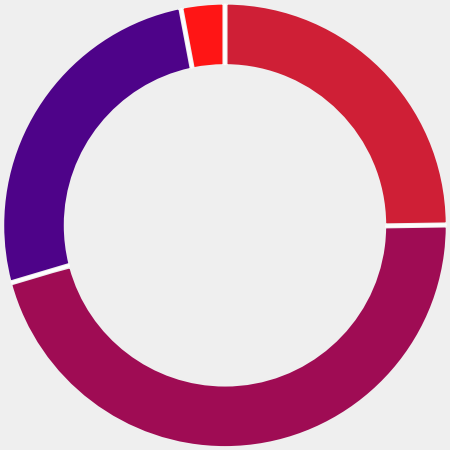
- Sehr unterstützende Führungskräfte („Leadership-Buy-in")
- Hoher Einblick in Nutzer, Geräte, Anwendungen und Dienste in ihren Netzwerken („Asset-Sichtbarkeit")
- Sehr gut auf Bedrohungen der Lieferkette in ihrer Branche vorbereitet („Steigende Bereitschaft")
- Hoher Stellenwert der Benutzerfreundlichkeit für Endnutzer bei technischen Maßnahmen im Bereich der Cybersicherheit („Sicherheits-UX")
- Mehr Sicherheit bei ihren Cloud-basierten Systemen und/oder bei der Einführung von Speicherlösungen („Cloud-Sicherheit")



Hinweis: Die Erhebung von Informationen durch Selbstauskunft hat ihre Grenzen, da die Menschen bei der Bewertung ihrer eigenen Bemühungen voreingenommen sein können. Die Selbstauskunft ist möglicherweise zum Teil für die außergewöhnlich geringe Zahl der Antworten der Stufe 1 verantwortlich, die wir für diesen Bericht mit der Stufe 2 zusammengefasst haben.

Wir sind der Meinung, dass die folgenden, auf diesem Reifegradmodell basierenden Erkenntnisse nützliche Signale für den Bereich der Cybersicherheit liefern, bitten die Leser jedoch, die Grenzen der Forschung zu beachten.

Antworten von Cybersicherheitsfachleuten nach Stufen



4 %

Stufe 1: Grundlegende Cybersicherheitshygiene

25 %

Stufe 2: Fortgeschrittene Cybersicherheitshygiene mit etablierten Verfahren und Richtlinien

42 %

Stufe 3: Umfassende und proaktive Cybersicherheitshygiene

29 %

Stufe 4: Expertenniveau; nachgewiesene Fähigkeit, komplexe Bedrohungen abzuwehren

Wodurch unterscheiden sich Unternehmen der Stufe 4 im Bereich Cybersicherheit?

Leadership-Buy-in: Die große Mehrheit der Unternehmen der Stufe 4 (86 %) gibt an, dass sie von ihren Vorgesetzten unterstützt werden. Die Zustimmung kann auf verschiedene Weise erfolgen, von der finanziellen Unterstützung für den Aufbau einer stärkeren Verteidigung bis hin zur Autonomie, um proaktive Strategien zu entwickeln, anstatt ohne Rücksicht auf den Kosten-Nutzen-Faktor der neuesten CEO-Priorität nachzujagen.

Transparenz der Ressourcen: Die meisten Level-4-Unternehmen (83 %) haben ein hohes Maß an Transparenz in Bezug auf Benutzer, Anwendungen und Geräte in ihrem Unternehmen. Die Wahrscheinlichkeit, dass sie dies tun, ist im Vergleich zu Unternehmen der Stufe 3 sogar um 70 % höher. Da die Zahl der Geräte und Apps explodiert, wird die Sichtbarkeit im Jahr 2023 ein wichtiger Schwerpunkt sein.

Die CISA hat diese Notwendigkeit kürzlich unterstrichen, als sie Ende 2022 eine neue Richtlinie herausgab (BOD 23-01). CISA-Direktorin Jen Easterly erklärt: „Zu wissen, was sich in Ihrem Netzwerk befindet, ist für jedes Unternehmen der erste Schritt zur Risikominderung."

Resilienz in der Lieferkette: Wenn es um die Bereitschaft in der Lieferkette geht, sind die Unternehmen der Stufe 4 im Vergleich zu allen anderen von uns befragten Unternehmen besser vorbereitet. 64 % sagen, dass sie auf Bedrohungen in der Lieferkette „sehr gut vorbereitet" sind, verglichen mit nur 36 % der Unternehmen der Stufe 3.

„Die Vorbereitung auf die Lieferkette ist ein Bereich, in dem die meisten Unternehmen noch Schwierigkeiten haben, sich anzupassen – zum großen Teil, weil das Problem enorm komplex sein kann", erklärt Michael Montoya, SVP & CISO bei Equinix. „Wir gehen davon aus, dass die Verringerung von Risiken in der Lieferkette 2023 ein großer Investitionsbereich sein wird – von der Implementierung von Software Bill of Materials (SBOMs) bis hin zum Einsatz von Zero-Trust-Lösungen und umfassenden Zugangskontrollen."

UX zur Risikominderung: Die besten Unternehmen wissen, dass eine hervorragende Benutzerfreundlichkeit ein wesentlicher Bestandteil der Sicherheit ist – ein wirksames Gegenmittel gegen schlechte Compliance und riskante Umgehungslösungen. Die meisten Unternehmen der Stufe 4 (71 %) geben an, dass die Benutzerfreundlichkeit für Endbenutzer eine „hohe Priorität" oder „entscheidend" ist – 20 Prozentpunkte mehr als bei Unternehmen der Stufe 3.

Sicherheit in der Cloud: Unternehmen der Stufe 4 geben viel häufiger an, dass ihre Cloud-basierten Systeme sicherer sind. Sie sind sogar dreimal häufiger der Meinung, dass die Cloud-Umgebung „viel sicherer" ist als die der Stufe 3.

„Der derzeitige Inflationsdruck und die makroökonomischen Bedingungen haben einen Push- und Pull-Effekt auf die Cloud-Ausgaben. Cloud Computing wird auch in Zukunft ein Bollwerk der Sicherheit und Innovation sein und aufgrund seiner Flexibilität, Elastizität und Skalierbarkeit das Wachstum in unsicheren Zeiten unterstützen." – Sid Nag, Vizepräsident und Analyst bei Gartner®[11]

Eines ist sicher: Eine rein defensive Taktik wird 2023 nicht mehr funktionieren. Michael Levin, Senior Vice President für Global Cyber Risk and Defense bei der UnitedHealth Group, erläuterte dieses Konzept gegenüber dem Wall Street Journal: „Viele Unternehmen konzentrieren sich immer noch auf die früheren Checklisten und die Einhaltung von Vorschriften nach dem Motto „Ich habe alles getan, was man mir gesagt hat, also bin ich sicher“, im Gegensatz zur Überlegung ‚Wie kann ich sicher sein?‘[12]

Zur Erinnerung: Die überwältigende Mehrheit der Sicherheitsexperten und Führungskräfte sagte uns, dass ihre Unternehmen heute genauso gut oder besser vorbereitet sind als vor einem Jahr – erstaunliche 97 % sagten dies! Dennoch würde jeder Fünfte nicht einen Schokoriegel darauf wetten. Optimismus und Realität.

Um mit den sich schnell verändernden und noch unbekannten Bedrohungen fertig zu werden, müssen Unternehmen über eine reaktive, regelbasierte Haltung hinausgehen (d. h. „Ich habe alles getan, was von mir verlangt wurde”).

Reifende Cybersicherheitsteams sollten auch Folgendes berücksichtigen:

Automatisierung: Setzen Sie Automatisierung ein, um die Transparenz von Assets zu erhöhen und eine risikobasierte Priorisierung von Patches vorzunehmen – beides Grundvoraussetzungen für sichere Unternehmen im Jahr 2023 – und nutzen Sie eine intelligente Benutzeroberfläche, um Mitarbeiter zu einem guten Sicherheitsverhalten zu zwingen (d. h., machen Sie Ausnahmen und Umgehungslösungen zu einem Problem, das sie nicht wert sind).

Resilienz: Entwickeln Sie Reaktions- und Wiederherstellungspläne, um Ausfälle zu verkürzen und die Auswirkungen zu begrenzen, denn Sie wissen, dass einige Angriffe unweigerlich durchschlagen werden.

Befähigung: Geben Sie dem Cybersicherheitsteam mehr Unabhängigkeit, um die Sicherheitsagenda festzulegen – keine gedankenlosen Reaktionen mehr auf die neueste Bedrohung, die in den Nachrichten auftaucht, oder Bestrafung von Teams für die Nichterfüllung endloser Listen von ständig wechselnden Prioritäten!

Ganzheitliches Risikomanagement: Denken Sie an die Sicherheit über das Unternehmen hinaus – von der Arbeit von überall aus (WFE) und hybriden Mitarbeitern bis hin zu Drittanbietern und Lieferanten. Verfolgen Sie bei diesen Akteuren einen Risiko-Ertrags-Ansatz und schenken Sie den „Walen” in Sachen Sicherheit, wie z. B. den Führungskräften in der Führungsetage oder den hochintegrierten Softwareanbietern, überdurchschnittliche Aufmerksamkeit.

Wenn sich die Bereitschaft zur Cybersicherheit von reaktionär und defensiv auf zukunftsorientiert und widerstandsfähig umstellt, werden unserer Meinung nach viel mehr Unternehmen bereit sein, die Wette mit dem Schokoriegel einzugehen.

05

Methodologie

Ivanti befragte im Oktober 2022 über 6.500 Führungskräfte, Cybersicherheitsexperten und Büroangestellte. Unser Ziel: die heutigen Bedrohungen zu verstehen – sowohl aus der Sicht von Sicherheitsexperten als auch von allen anderen Büroangestellten – und herauszufinden, wie sich Unternehmen auf noch unbekannte zukünftige Bedrohungen vorbereiten.

Die Studie wurde von Ravn Research durchgeführt, und die Panelists wurden von MSI Advanced Customer Insights rekrutiert. Die Umfrageergebnisse sind nicht gewichtet. Weitere länderspezifische Einzelheiten sind auf Anfrage erhältlich.

Umfrage-Stichprobe

Büroangestellte
5.202

Sicherheitsfachkräfte
902

Führungspersonal
454

Branchen

6 %
Bildung

12 %
Finanzdienstleistungen

12 %
Regierung

13 %
Herstellung/Verarbeitung

3 %
Gemeinnützige/karitative Einrichtungen

18 %
Sonstiges, bitte angeben

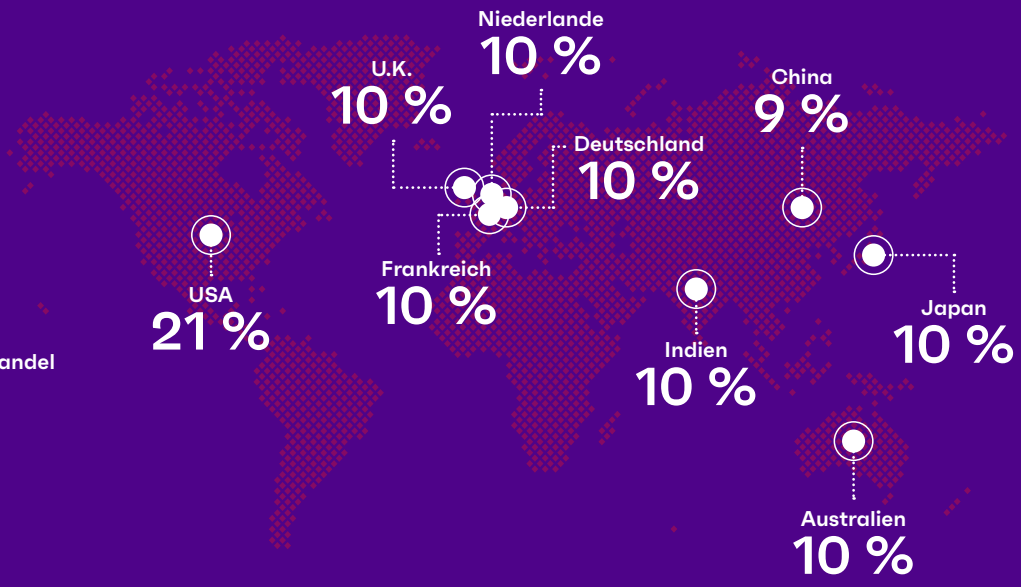
8 %
Professionelle Dienstleistungen

11 %
Einzelhandel, E-Commerce, Großhandel

14 %
Technologie

3 %
Telekommunikation

Länder



Referenzen

Alle Diagramme in diesem Bericht wurden aus Umfragedaten erstellt, die im Rahmen der Ivanti-Reihe State of Cybersecurity Preparedness 2023 erhoben wurden (siehe Methodik).

1. PwC: „A C-suite united on cyber-ready futures: Findings from the 2023 Global Digital Trust Insights," Sept. 2022. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html

2. SHRM: „2023 Salary Budgets Projected to Stay at 20-Year High but Trail Inflation," Sept. 2022. https://www.shrm.org/resourcesandtools/hr-topics/compensation/pages/2023-salary-increase-budgets-stay-trail-inflation.aspx

3. The Wall Street Journal: „Cybersecurity Tops the CIO Agenda as Threats Continue to Escalate," Okt. 2022. https://www.wsj.com/articles/cybersecurity-tops-the-cio-agenda-as-threats-continue-to-escalate-11666034102

4. IBM: „Cost of a data breach 2022: A million-dollar race to detect and respond," Juli 2022. https://www.ibm.com/reports/data-breach

5. The Wall Street Journal: „Microsoft's New Security Chief Says It Is Time to Take Shelter in the Cloud," Feb. 2022. https://www.wsj.com/articles/microsofts-new-security-chief-says-it-is-time-to-take-shelter-in-the-cloud-11645624800

6. InfoSecurity Group: „Cybersecurity Workforce Gap Grows by 26% in 2022," Okt. 2022. https://www.infosecurity-magazine.com/news/cybersecurity-workforce-gap-grows/

7. Supply Chain Brain: „Why Cybersecurity Has Never Been More Important for the Supply Chain Sector," Okt. 2022. https://www.supplychainbrain.com/blogs/1-think-tank/post/35798-why-cybersecurity-has-never-been-more-important-for-the-supply-chain-sector

8. The Wall Street Journal: „Rise in Cyberattacks Stretches and Stresses Defenders," Okt. 2022. https://www.wsj.com/articles/rise-in-cyberattacks-stretches-and-stresses-defenders-11664962202

9. Ivanti: „State of IT in 2021," Dez. 2021. https://www.ivanti.com/company/press-releases/2021/new-ivanti-study-finds-the-biggest-challenge-for-it-departments-is-keeping-up-with-digital-transformation-and-keeping-talent-in-technical-roles

10. CISA: „CISA Directives Federal Agencies to Improve Cybersecurity Asset Visibility and Vulnerability Detection," Okt. 2022. https://www.cisa.gov/news/2022/10/03/cisa-directs-federal-agencies-improve-cybersecurity-asset-visibility-and

11. Gartner-Pressemitteilung: „Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023," Okt. 2022.. https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023. GARTNER ist ein eingetragenes Warenzeichen und Dienstleistungsmarke von Gartner, Inc. und/oder seinen Tochtergesellschaften in den USA und international und werden hier mit Genehmigung verwendet. Alle Rechte vorbehalten.

12. The Wall Street Journal: „Cybersecurity Tops the CIO Agenda as Threats Continue to Escalate," Okt. 2022. https://www.wsj.com/articles/cybersecurity-tops-the-cio-agenda-as-threats-continue-to-escalate-11666034102

Zusätzliche Informationen zur Karte

S. 3 – Befragte aus dem Bereich Sicherheit und Führungskräfte; n=1.356

S. 5 – Befragte aus dem Bereich Sicherheit und Führungskräfte; n=1.356

S. 7 – Befragte aus dem Bereich Sicherheit und Führungskräfte; n=1.356

S. 8 – Befragte aus dem Bereich Sicherheit; n=902

S. 9 – Befragte aus dem Bereich Sicherheit und Führungskräfte; n=1.341

S. 11 – Befragte aus dem Bereich Sicherheit; n=902

S. 13 – Befragte aus dem Bereich Sicherheit; n=902

S. 14 – Befragte aus dem Bereich Sicherheit und Führungskräfte; n=1.356

S. 15 („Legitimation eines Mitarbeiters") – Befragte aus dem Bereich Sicherheit; n=902

S. 15 („die Anmeldeinformationen eines Drittanbieters […]") – Befragte im Bereich Sicherheit; n=882

S. 17 („wie setzen Sie Prioritäten") – Befragte aus dem Bereich Sicherheit; n=902

S. 17 („eine Methode zur Prioritätensetzung") – Befragte aus dem Bereich Sicherheit; n=886

S. 20 – Befragte Führungskräfte und Büroangestellte; n=5.656

S. 21 („mehr als ein Drittel") – Befragte Führungskräfte und Büroangestellte; n=1.949

S. 21 („Fast jeder Vierte") – Befragte Führungskräfte und Büroangestellte; n=5.656

S. 21 („Führungskräfte sind viel mehr") – Befragte Führungskräfte und Büroangestellte; n=5.373

S. 21 („Befragte Führungskräfte") – Befragte Führungskräfte und Büroangestellte; n=5.656

S. 24 („Leadership buy-in") – Befragte aus dem Bereich Sicherheit und Führungskräfte; n=1.356

S. 24 („Asset-Sichtbarkeit") – Befragte aus dem Bereich Sicherheit und Führungskräfte; n=1.356

S. 24 („Steigende Bereitschaft") – Befragte aus dem Bereich Sicherheit; n=902

S. 24 („Security UX") – Befragte aus dem Bereich Sicherheit; n=902

S. 24 („Cloud-Sicherheit") – Sicherheit und führende Befragte; n=1.341

Reset drücken

Ein Bericht zum Stand der Cybersicherheit 2023

Unternehmen liefern sich ein Wettrennen, um sich vor Cyberangriffen zu schützen, doch die Branche kämpft mit einer reaktiven Checklisten-Mentalität.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com