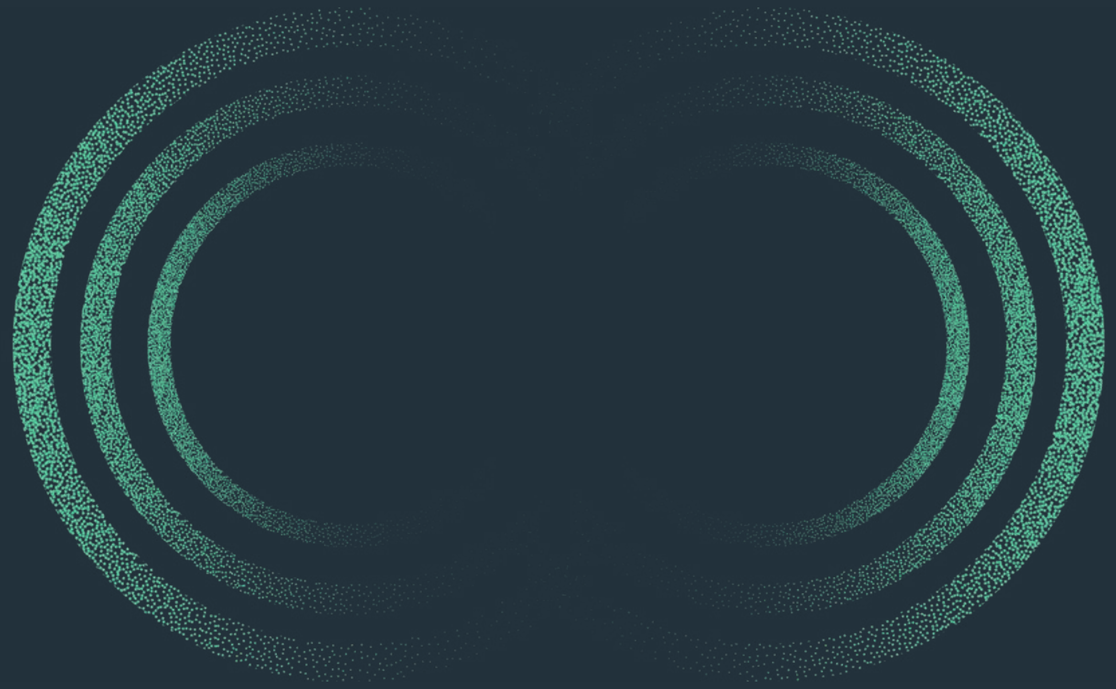
WithSecure™ Pulse 2023

Alles, was Sie über die neuesten IT- und Cybersicherheitstrends wissen müssen

WITH secure

Inhalt



Zusammen-fassung

Einleitung

In unserer globalen Marktforschungsstudie haben wir Tausende von IT-Fachleuten zu ihren Aufgaben, ihren Unternehmen und den Prioritäten für das kommende Jahr befragt. Die gewonnenen Daten liefern Ihnen die Grundlage für Ihre IT- und Sicherheitsstrategien im Jahr 2023 und darüber hinaus.

Pulse 2023 erreichte 3.072 Befragte in 12 Ländern: Großbritannien, Frankreich, Deutschland, Belgien, Niederlande, Dänemark, Finnland, Norwegen, Schweden sowie die USA, Kanada und Japan. Die Teilnehmer waren Entscheidungsträger und Meinungsführer in den Bereichen IT, Netzwerke und Cloud, verantwortlich für den Kauf von IT-Sicherheitsprodukten und -dienstleistungen für ihre Unternehmen.

Sicherheits-Prioritäten für 2023

Die Teilnehmer unserer Umfrage haben uns ihre wichtigsten geschäftlichen und technischen Prioritäten für die kommenden 12 Monate mitgeteilt. Die fünf Top-Prioritäten für Führungskräfte im Bereich Cybersicherheit sind:

Unser vertiefender Beitrag zu den Sicherheitsprioritäten (ab Seite 10) enthält einen Überblick zu den Trends, die wir in unserer Pulse 2023-Umfrage beobachtet haben.

Größte technische Sicherheitsherausforderungen (Top 5)

34% Verhinderung von Datenpannen

29% Gewährleistung des Schutzes vor Malware und Ransomware

27% Verhinderung hochentwickelter E-Mail-basierter Bedrohungen, z. B. Phishing oder Kompromittierung von Geschäfts-E-Mails (BEC)

27% Gewährleistung der Sicherheit von Cloud-basierten Collaboration-Anwendungen, z. B. Office 365 und Salesforce

26% Gewährleistung der Sicherheit eines immer vielfältigeren Pools von Geräten, Services und Software

“Der springende Punkt ist, dass gerade die Optionen, die niemand als Prioritäten wählt, den größten Unterschied bei der Sicherheitslage ausmachen; erfahrungsgemäß sind das eben die Kompetenzen und Praktiken, die vielen Unternehmen fehlen.”

Peter Page, WithSecure™ Head of Solution Consulting

Ausgaben für die Sicherheit

Zwischen dem ganzen Wirbel um Cybersicherheit ist die wohl wichtigste Frage für Unternehmen die Kostenbilanz. Wie viel sollen wir für Sicherheit eigentlich investieren? Ist überhaupt ein Betrag "genug"? Kommt es darauf an, wie viele Arbeitsplätze wir haben, wo unser Standort ist oder in welcher Branche wir tätig sind? Sorgen sich meine Mitbewerber ebenfalls über ihre Ausgaben - und wie viel von ihrem Budget setzen sie dafür ein?

Unsere Studie hat interessante Erkenntnisse über die Ausgaben von Unternehmen für Cybersicherheit zutage gefördert. Die Daten zeigen, dass mit der Weiterentwicklung ihrer Strategie der Kostenfaktor in den Hintergrund tritt.

86% der Befragten geben an, dass sich ihr Budget für Sicherheit in den kommenden 12 Monaten erhöhen wird.

“Ich sage immer, man sollte beim absoluten Minimum von 5 % anfangen. Das gilt natürlich ohne Gewähr: Je zentraler die Sicherheit für den Kunden ist, desto höher der Prozentsatz. Und umgekehrt."

Teemu Myllykangas, Director, B2B Product Management bei WithSecure™

“Unternehmen müssen sich entscheiden, wie viel Sicherheit sie wollen. Sie müssen vereinbaren, wie viel Risiko sie akzeptieren wollen, wie viel Störungen des Geschäftsbetriebs sie tolerieren können und wie risikofreudig sie sind. Auf Basis dieser Entscheidung können rationale Kostenentscheidungen für Sicherheitsmaßnahmen getroffen werden.”

Paul Brucciani, Head of Product Marketing bei WithSecure™

Datenresidenz

Unsere Studie Pulse 2023 hat gezeigt, dass IT-Mitarbeiter durchaus klare Meinungen dazu haben, wo die Daten ihres Unternehmens gespeichert und verarbeitet werden. Das überrascht nicht: Regeln und Vorschriften für den Umgang mit Daten - und viele Beispiele für Datenmissbrauch - machen diesen Komplex für viele zu einem brisanten und emotionalen Thema.

Die Ansichten unterschieden sich tendenziell je nach Größe der Organisationen, Region des Standorts und Branche.

Wie kann bei so viel Meinungsverschiedenheiten über den richtigen Umgang mit Daten ein Konsens erzielt werden? Beeinflusst die Politik zur Datenresidenz eines Unternehmens die Beziehung zu seinen Kunden? Oftmals üben hier auch Regulierungsbehörden und Datenschützer einen starken Einfluss aus.

Die vielleicht wichtigste Frage ist, warum es überhaupt solche Meinungsverschiedenheiten gibt. Uneinigkeit und Missverständnisse können zu Problemen führen, besonders zwischen IT-Meinungsführern und Entscheidern in derselben Organisation. Wenn es um den Schutz der Privatsphäre geht, gibt es keinen Raum für Fehler.

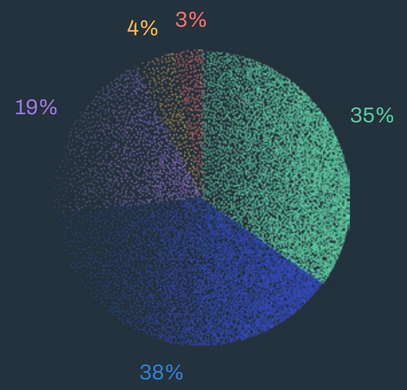
“Datenresidenz ist etwas, das Sie heute als Unternehmen in Betracht ziehen müssen. Sie haben nämlich möglicherweise Kunden, denen die nationale Sicherheit am Herzen liegt, und Sie als Start-up haben z. B. Ihr Software-as-a-Service-Produkt über amerikanische Cloud-Service-Anbieter bereitgestellt. Können Sie das weiterhin tun, können Sie weiterhin mit demselben Tempo innovativ sein wie bisher, oder müssen Sie eine alternative Lösung dafür finden? Das ist etwas, das Sie bedenken müssen.”

Albert Koubov Gonzalez, Berater, WithSecure™

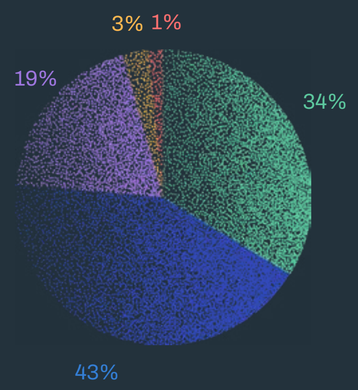
Wo die Daten gespeichert werden

Wie wichtig ist der geografische Standort für die Datenverarbeitung in Ihrer Position?

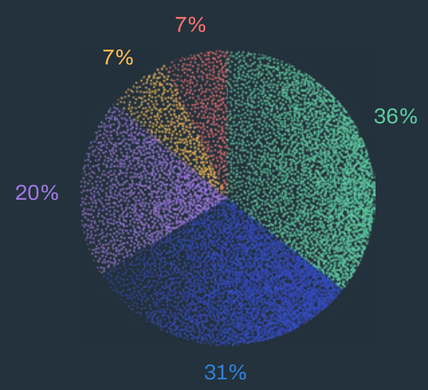
Insgesamt



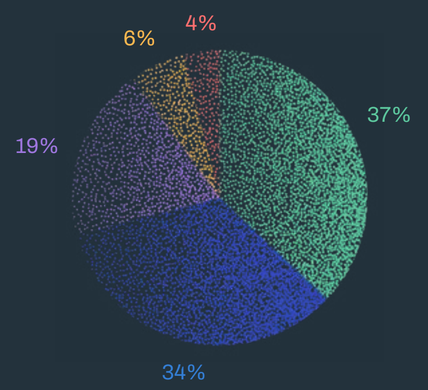
IT-Entscheider



IT-Meinungsführer



Top-Management



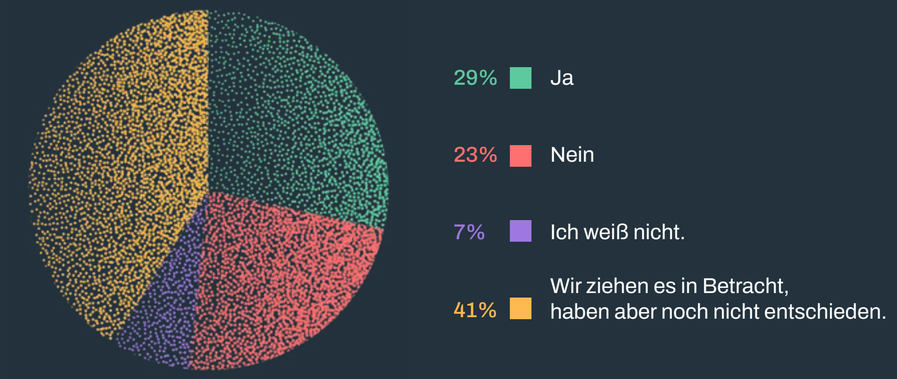
- Die Daten müssen in dem Land verarbeitet werden, wo wir tätig sind.
- Die Daten müssen in derselben Region (z. B. EU, Nordamerika, APAC) verarbeitet werden, in der wir tätig sind.
- Es ist unwichtig, wo wir unsere Endkundendaten verarbeiten, solange alle geltenden rechtlichen und Compliance-Anforderungen erfüllt werden.
- Wir verarbeiten keine Daten für Endkunden.
- Ich weiß nicht.

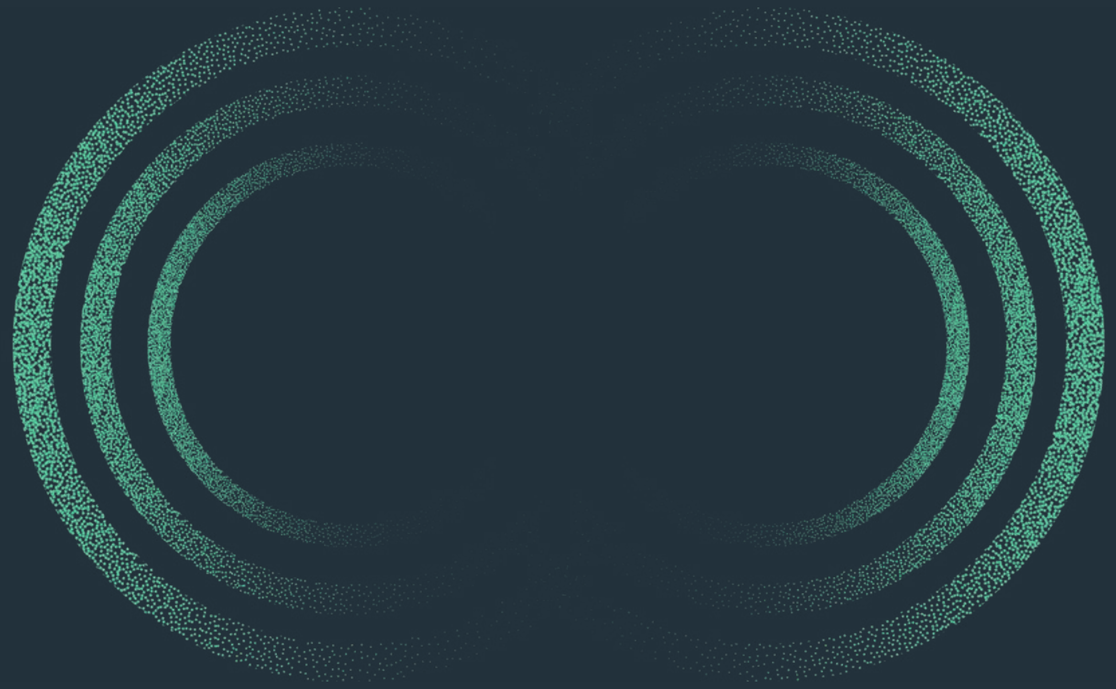
Anbieterwechel

Der Wechsel des Anbieters von Sicherheitslösungen ist ein anspruchsvolles Vorhaben. Denn damit sind enorme Investitionen in Zeit und Ressourcen verbunden. Trotzdem zeigt unsere Pulse 2023-Umfrage, dass mehr als 30 % der Befragten ihren Anbieter in den letzten sechs Monaten gewechselt haben. Ebenso viele planen, ihren Anbieter in den kommenden sechs Monaten zu wechseln.

Dies ist ein Hinweis, dass eine massive Umstellungswelle im Gange ist. Die Frage ist, warum und mit welchen Kosten.

Plant Ihr Unternehmen/Ihre Organisation in den nächsten sechs Monaten einen Wechsel Ihrer IT-Sicherheitslösung/ des Anbieters?

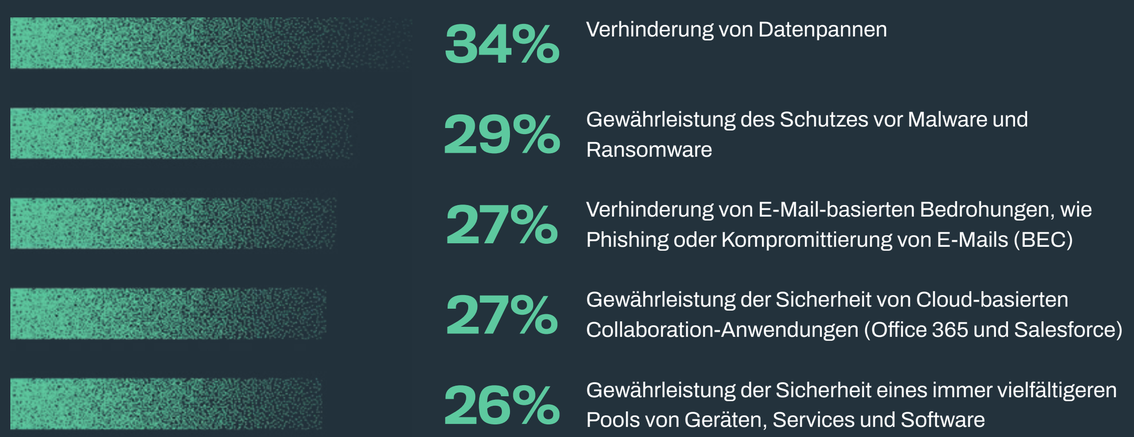




1. Sicherheit: Prioritäten für 2023

Technische Prioritäten für die Sicherheit

Oberste technische Sicherheitsprioritäten



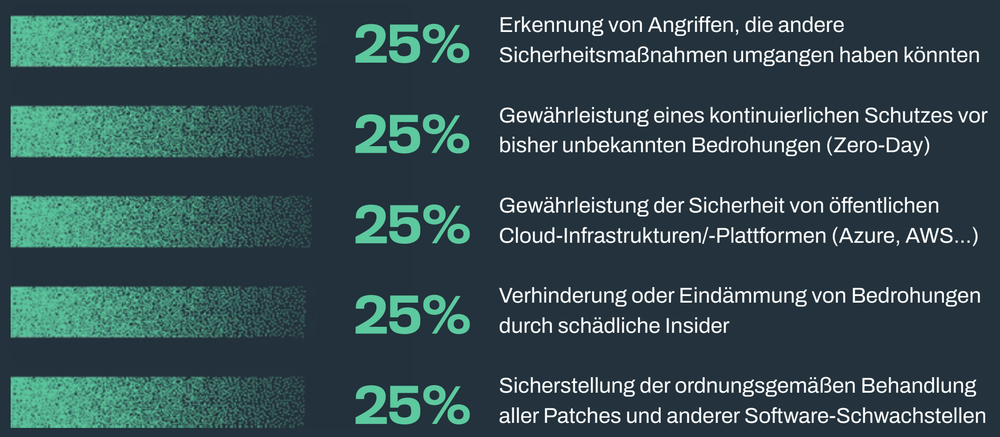
34% Verhinderung von Datenpannen

29% Gewährleistung des Schutzes vor Malware und Ransomware

27% Verhinderung von E-Mail-basierten Bedrohungen, wie Phishing oder Kompromittierung von E-Mails (BEC)

27% Gewährleistung der Sicherheit von Cloud-basierten Collaboration-Anwendungen (Office 365 und Salesforce)

26% Gewährleistung der Sicherheit eines immer vielfältigeren Pools von Geräten, Services und Software



25% Erkennung von Angriffen, die andere Sicherheitsmaßnahmen umgangen haben könnten

25% Gewährleistung eines kontinuierlichen Schutzes vor bisher unbekannten Bedrohungen (Zero-Day)

25% Gewährleistung der Sicherheit von öffentlichen Cloud-Infrastrukturen/-Plattformen (Azure, AWS...)

25% Verhinderung oder Eindämmung von Bedrohungen durch schädliche Insider

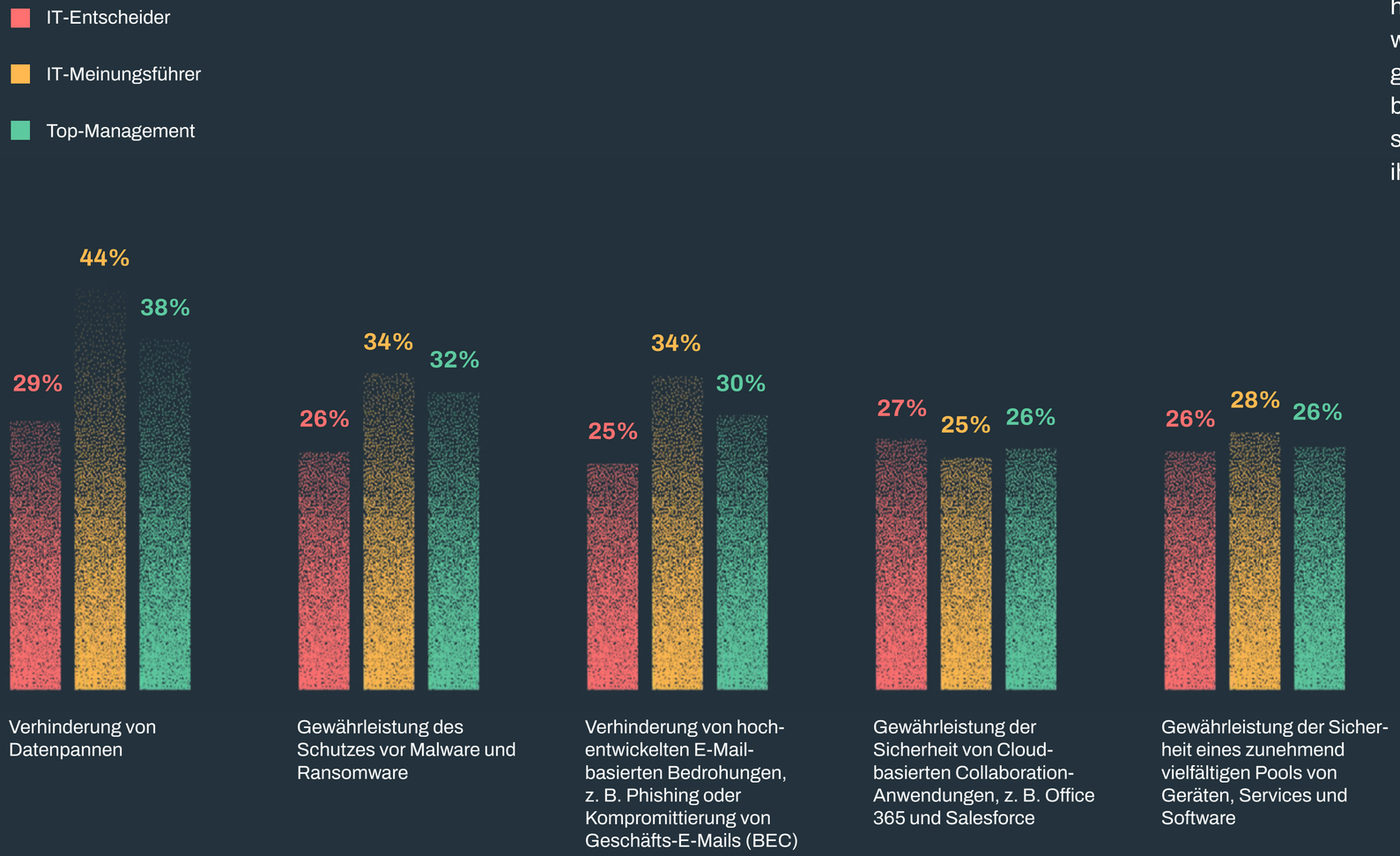
25% Sicherstellung der ordnungsgemäßen Behandlung aller Patches und anderer Software-Schwachstellen

Die Ergebnisse belegen einen breiten Konsens darüber, welche technischen Prioritäten besonders besorgniserregend sind. Die größte Herausforderung ist eindeutig die "Verhinderung von Datenpannen" (33,7 %). Die Verhinderung von E-Mail-basierten Bedrohungen und die Gewährleistung der Sicherheit von Cloud-basierten Collaboration-Anwendungen wie Office 365 und Salesforce stehen ebenfalls ganz oben auf der Liste. Die anderen genannten Prioritäten gehören im Allgemeinen zum Thema Detection and Response bei Bedrohungen.

”Interessant ist, dass die wichtigsten Sicherheitsfaktoren bei den obersten Prioritäten fehlen: nämlich erfahrungsgemäß die Kompetenzen und Praktiken, die in vielen Unternehmen fehlen. Jeder ist besorgt über die Abwehr von Angriffen durch Lösungen wie EDR und Beratung, aber beides ist entscheidend. EDR muss für eine wassserdichte Lösung zusätzlich zu EPP eingesetzt werden. Außerdem werden die Maßnahmen, die wirklich dauerhaft wirken, übersehen, weil sie intern durchgeführt werden müssen und oft viel schwierige Arbeit bedeuten - den Aufbau einer Sicherheitskultur kann man nicht auslagern.”

— Peter Page, Head of Solution Consulting bei WithSecure

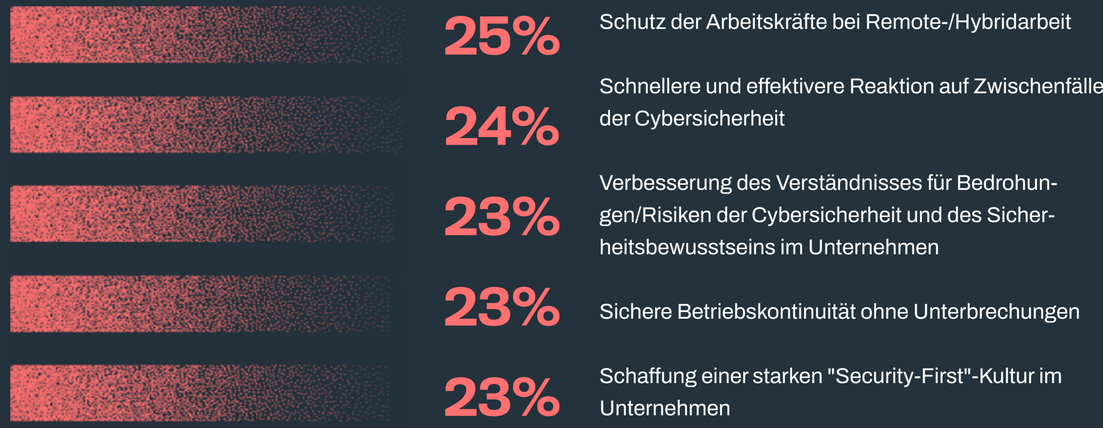
Die 5 größten technischen Herausforderungen 2022/23 nach Funktion



Diese Daten zeigen den jeweiligen Anteil der IT-Entscheider, IT-Meinungsführer und des Top-Managements, die ihre fünf wichtigsten technischen Prioritäten für 2023 angeben. Auch hier scheinen sich die Befragten weitgehend über die derzeit wichtigsten Prioritäten einig zu sein. Wenn es Diskrepanzen gibt (z. B. zwischen IT-Entscheidern und IT-Meinungsführern beim Thema "Verhinderung von Datenpannen"), könnte es sich lohnen, nachzufragen und sicherzustellen, dass alle in ihrem Sicherheitsteam die gleiche Auffassung vertreten.

Ergebnisse für die Sicherheit von Unternehmen

Größte Herausforderungen für Unternehmen



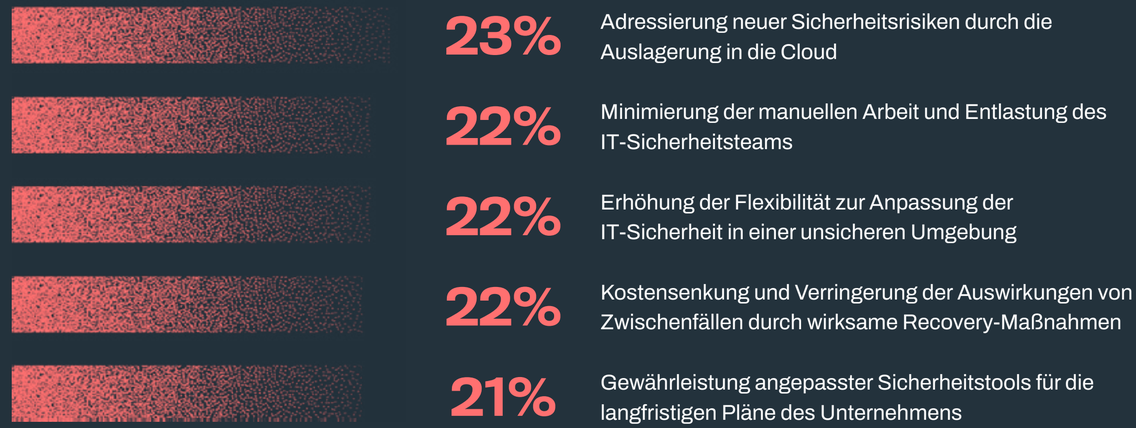
25% Schutz der Arbeitskräfte bei Remote-/Hybridarbeit

24% Schnellere und effektivere Reaktion auf Zwischenfälle in der Cybersicherheit

23% Verbesserung des Verständnisses für Bedrohungen/Risiken der Cybersicherheit und des Sicherheitsbewusstseins im Unternehmen

23% Sichere Betriebskontinuität ohne Unterbrechungen

23% Schaffung einer starken "Security-First"-Kultur im Unternehmen



23% Adressierung neuer Sicherheitsrisiken durch die Auslagerung in die Cloud

22% Minimierung der manuellen Arbeit und Entlastung des IT-Sicherheitsteams

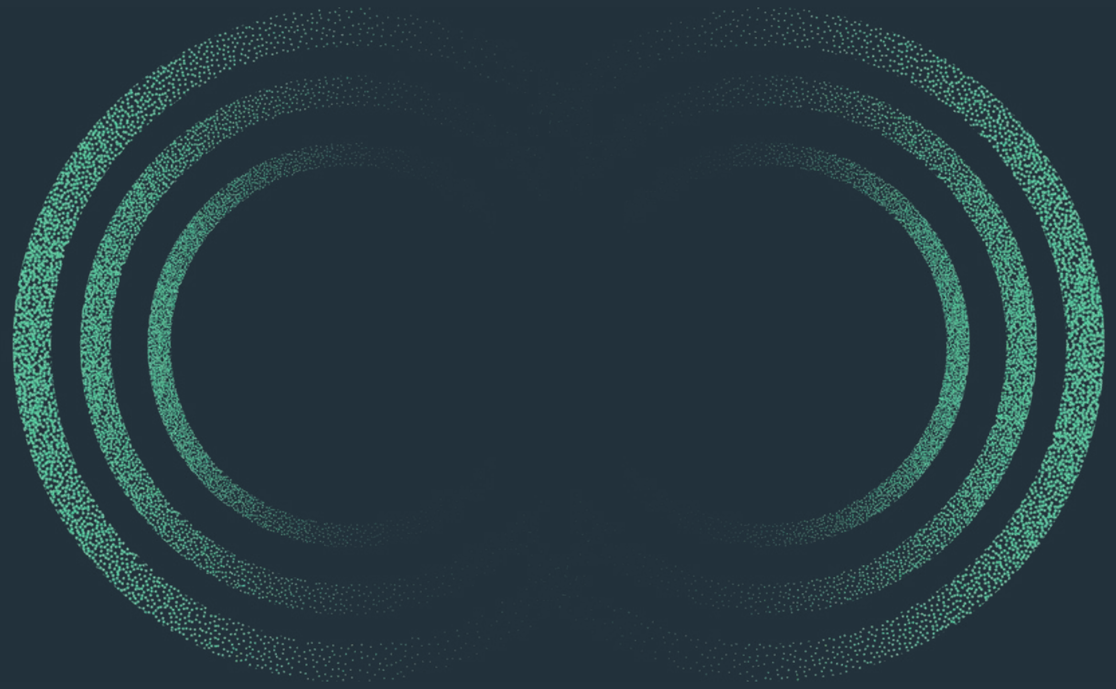
22% Erhöhung der Flexibilität zur Anpassung der IT-Sicherheit in einer unsicheren Umgebung

22% Kostensenkung und Verringerung der Auswirkungen von Zwischenfällen durch wirksame Recovery-Maßnahmen

21% Gewährleistung angepasster Sicherheitstools für die langfristigen Pläne des Unternehmens

“Es überrascht nicht, dass die Leute am meisten über die Herausforderung der Sicherung von Remote-Arbeitskräften besorgt sind. Im Jahr 2020 hat sich die Arbeitsweise massiv verändert; es gab hier viele Anleitungen und Ratschläge, um Unternehmen bei der Anpassung zu helfen. Für viele bedeutete dies groß angelegte Projekte, die eine Änderung der IT-Architektur (z. B. die Migration in die Cloud) und Umschulungen der Mitarbeiter erforderten. Aber auch wenn dies derzeit offenbar ein verbreitetes Problem ist, hoffe und erwarte ich, dass die meisten Unternehmen bis zur nächsten Umfrage im Jahr 2024/25 auf einem stabilen Stand sind, wo sie sich angepasst haben und alle mit den neuen Arbeitsweisen vertraut sind.”

— Peter Page, Head of Solution Consulting bei WithSecure



2. Ausgaben für Sicherheit

Wie viel sollte ich für Sicherheit investieren?

Diese Frage stellen sich weltweit tausende Unternehmen. Aber wie viel von Ihrem IT-Budget sollten Sie tatsächlich für Cybersicherheit verwenden?

Der weltweite Markt für Informationssicherheit wird bis 2024 voraussichtlich 174,7 Mrd. US-Dollar erreichen. Das ist eine beeindruckende Zahl; sie zeigt die wachsende Bedeutung der Cybersicherheit in einer zunehmend veränderlichen Welt. Es deutet auch darauf hin, dass Unternehmen auf die verstärkte Bedrohung reagieren und mehr in ihre Sicherheit investieren.

Angesichts mehrerer Faktoren, z. B. raffiniertere Angreifer, anhaltende Remote-Arbeit und die globale geopolitische Lage, stellt sich die Frage, wie viel Sicherheit "genug" ist und wie viel Unternehmen dafür ausgeben sollten.

Die Untersuchung von WithSecure ergab, dass 87,9 % der in der EU ansässigen Unternehmen planen, ihr Sicherheitsbudget in den nächsten 12 Monaten zu erhöhen. Überraschender ist vielleicht, dass 8,3 % der Meinung sind, dass sie ausreichend abgedeckt sind oder aktiv nach einer Reduzierung ihrer Ausgaben für Cybersicherheit suchen.

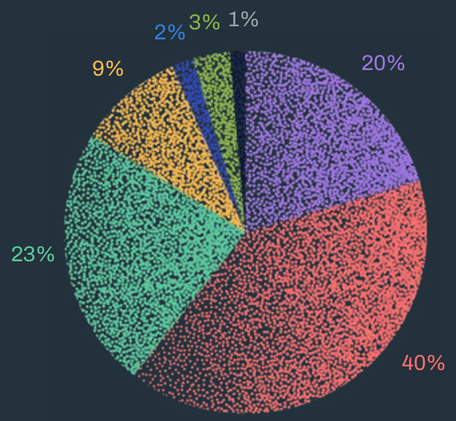
Auch bei der Frage, wie das Budget für das nächste Jahr aussehen wird, scheinen die Gruppen uneins zu sein: Während IT-Entscheider und Top-Management weitgehend übereinstimmen, haben die IT-Meinungsführer teils deutlich andere Budgeterwartungen. Eine frühzeitige und klare Kommunikation mit Ihren Stakeholdern zu diesem Thema ist entscheidend, um Verwirrung oder Entscheidungen in letzter Minute zu vermeiden.

Teemu Myllykangas, Director, B2B Product Management bei WithSecure™, kennt sich in diesem Bereich sehr genau aus. *“Wenn man ein Unternehmen fragt, ob es genug ausgibt, ist die Antwort schwierig. Bei einem Ja wird eine Datenpanne auf das Unternehmen zurückfallen, da die Leute wissen wollen, wie sie trotz der zu ihrem Schutz getätigten Investitionen geschädigt wurden. Bei einem Nein sollten sich dieselben Leute fragen, ob sie ihre Arbeit richtig machen und das Unternehmen schützen. Es gibt keine einfache Antwort auf diese Frage.”*

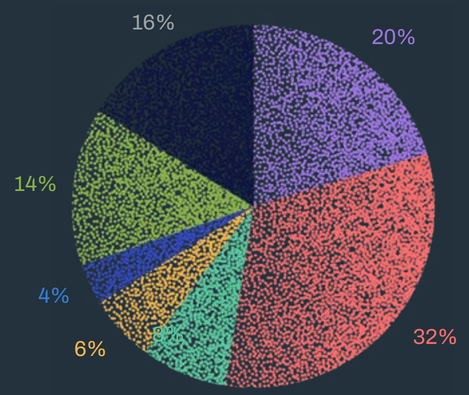
Die Branche geht allgemein davon aus, dass Unternehmen jährlich zwischen 3 % und 15 % ihres Budgets für Sicherheit ausgeben. Auf die Frage von Kunden, wo sie in dieser Kategorie einzuordnen sind, ist Myllykangas vorsichtig. *“Ich sage immer, man sollte mit einem absoluten Minimum von 5 % anfangen. Das gilt natürlich unter Vorbehalt: Je wichtiger die Sicherheit für den Kunden ist, desto höher ist der Prozentsatz. Und umgekehrt. Generell unterscheide ich drei Schritte: Beginnen Sie mit einer Risikobewertung und einer Bedrohungsmodellierung, um den ROI zu definieren; entscheiden Sie, wie Sie das Geld adäquat einsetzen, indem Sie ein bekanntes, grundlegendes Sicherheitskonzept verwenden; überprüfen Sie diese beiden Zahlen jährlich, um den Schwellenwert für die Rentabilität zu ermitteln und Ihr Budget zu verwalten.”*

Budgetpläne für die IT-Sicherheit nach Funktion

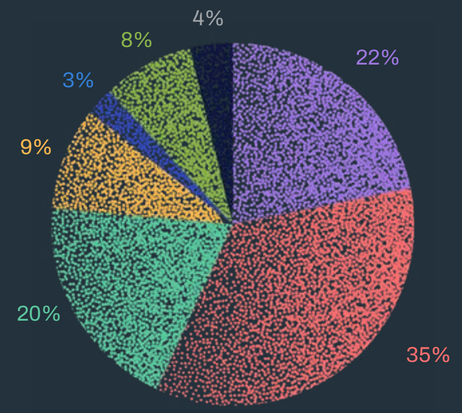
IT-Entscheider



IT-Meinungsführer



Top-Management



- In den kommenden 12 Monaten wird unser Budget um 1-5 % steigen.
- In den kommenden 12 Monaten wird unser Budget um 6-10 % steigen.
- In den kommenden 12 Monaten wird unser Budget um 11-15 % steigen.
- In den kommenden 12 Monaten wird unser Budget um mehr als 15 % steigen.
- In den kommenden 12 Monaten wird unser Budget sinken.
- In den kommenden 12 Monaten wird unser Budget weder steigen noch sinken.
- Ich weiß es nicht.

Risikobewertung ist entscheidend

“Es ist sehr schwierig, eine Faustregel dafür aufzustellen, ob die Ausgaben für Sicherheit ausreichen. Es gibt zu viele Variablen. Der Anteil des IT-Budgets kann je nach den Umständen um das Zehnfache variieren. Vor etwa fünf Jahren lag der Prozentsatz der Sicherheitsausgaben bei etwa 10 % des IT-Budgets eines Unternehmens, ist aber seitdem angestiegen. Unternehmen, für die Sicherheit von entscheidender Bedeutung ist, geben etwa 12–15 % ihres IT-Budgets für Sicherheit aus,” sagt Paul Brucciani, Head of Product Marketing bei WithSecure™.

Ihre erste Frage muss lauten: Welche Gefahren drohen? Wenn der Worst Case eintritt, was wären dann die Folgen? Sie müssen herausfinden, wie hoch die jährliche Verlusterwartung (Annual Loss Expectancy: ALE) ist und mit welcher Wahrscheinlichkeit dieser Fall eintritt.

Hier kommt WithSecure™ ins Spiel. Denn im Allgemeinen kennt ein Unternehmen die Antwort auf diese Frage nicht. Dank unserer langjährigen Erfahrung in der Incident Response können wir die ALE den Risikofaktoren gegenüberstellen und herausfinden, wie viel das Unternehmen für Sicherheit aufwenden sollte.

“Wenn Sie Ihr Risiko ermittelt haben, müssen Sie entscheiden, wie Sie damit umgehen wollen. Es gibt drei Möglichkeiten: Erstens können Sie die Risiken auslagern, was zum Beispiel den Abschluss einer Cyberversicherung bedeuten würde. Zweitens können Sie das Risiko verringern, indem Sie geeignete Sicherheitskontrollen, Technologien und Services einsetzen. Und schließlich kann man es einfach akzeptieren, damit leben und sich damit befassen, wenn es soweit ist,” sagt Brucciani weiter.

“Im Wesentlichen geht es darum, wie stark Sie das Risiko senken können, und damit um die Frage, wie viel von Ihrem Budget Sie für die Sicherheit zurückstellen müssen. Sie müssen entscheiden, wie viel Risiko Sie zu akzeptieren bereit sind und wie hoch Ihre Risikotoleranz ist.” so Brucciani weiter.

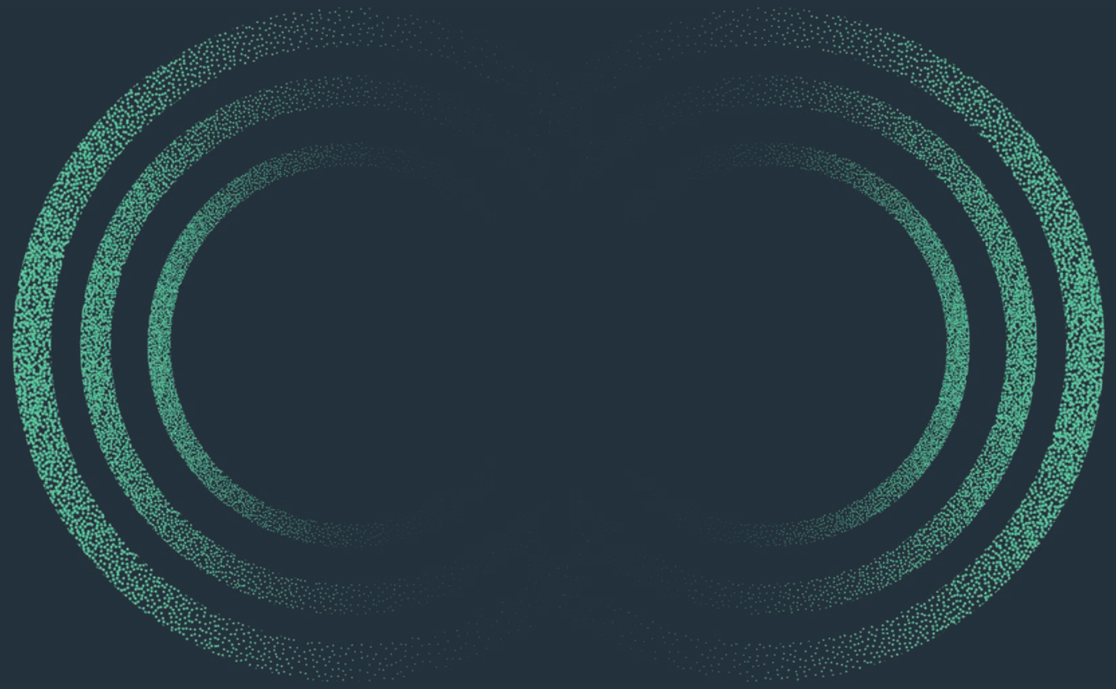
Dies sind Fragen, über die der CFO entscheiden muss. Erst danach können Sie Budgets, Beträge für unerwartete Ausgaben und den Umgang mit Risiken bestimmen.

Kosten sind nicht alles

Es ist wichtig zu unterstreichen, dass die Absicherung Ihres Unternehmens weit mehr ist als nur eine Kostenfrage. Es gibt hier etliche Faktoren, und die Untersuchungen von WithSecure haben genau diesen Punkt belegt. Nur 13,2 % der Befragten gaben in der WithSecure-Umfrage an, dass der niedrigste Preis der wichtigste Aspekt bei der Auswahl eines Anbieters ist. Mehr als ein Fünftel (21,8 %) hält hingegen den 24/7-Support für den wichtigsten Aspekt, und weiteren 16,7 % geht es um das Vertrauen in den Anbieter.

Es gibt zwar kein Patentrezept für die Entscheidung, wie viel Sie für Sicherheit ausgeben sollten, aber WithSecure™ kann Ihnen einen plausiblen, vertretbaren Weg aufzeigen, wie Sie einen optimalen Schutz Ihres Unternehmens gewährleisten können. Auch wenn der Kostenfaktor eine wichtige Rolle spielt und immer spielen wird, geht der Sicherheitsaspekt weit über das Geschäftsergebnis hinaus.

WithSecure™ Elements kann Ihnen helfen, Risiken, Komplexität und Ineffizienz zu reduzieren. Es kombiniert leistungsstarke prädiktive, präventive und reaktionsschnelle Sicherheitsfunktionen, die alle über ein einziges Sicherheitszentrum verwaltet und überwacht werden.



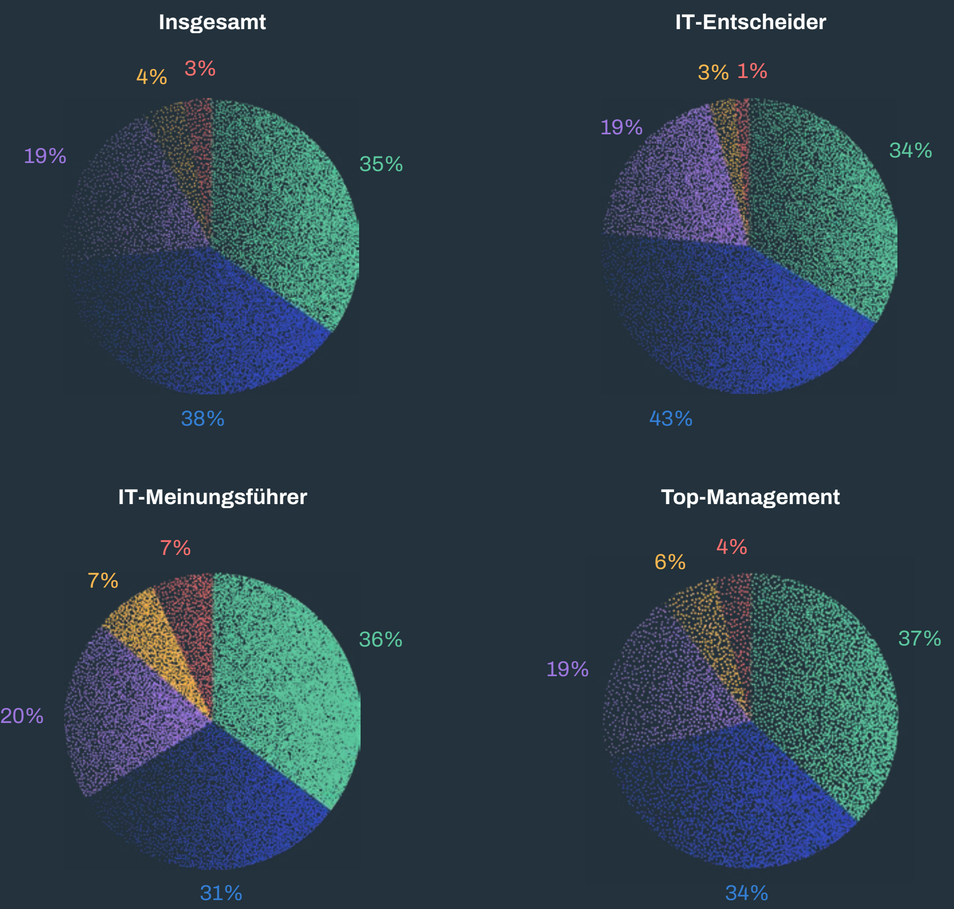
3. Daten-residenz

Wissen Sie, wo Ihre Daten liegen?

Die Menschen interessiert es brennend, wo ihre Daten gespeichert und verarbeitet werden.

Unsere Umfrage Pulse 2023 belegt ein starkes Interesse dafür, wo Daten gespeichert und verarbeitet werden. Fast 73 % der Befragten äußerten, dass ihre Daten in dem Land oder der Region verarbeitet werden müssen, wo sie tätig sind. Nicht einmal ein Fünftel sagte hingegen, dies sei nicht wichtig.

Wie wichtig ist der geografische Standort für die Datenverarbeitung in Ihrer Funktion?



- Die Daten müssen in dem Land verarbeitet werden, in dem wir tätig sind.
- Die Daten müssen in derselben Region (z. B. EU, Nordamerika, APAC) verarbeitet werden, in der wir tätig sind.
- Es spielt keine Rolle, wo wir unsere Endkundendaten verarbeiten, solange alle relevanten rechtlichen und Compliance-Anforderungen erfüllt sind.
- Wir verarbeiten keine Daten für Endkunden.
- Ich weiß nicht.

Uneinigkeit bezüglich der Datenresidenz

Bei der Aufschlüsselung dieser Antworten zeigte sich eine Diskrepanz. 42,8 % der IT-Entscheider halten die regionale Verarbeitung für erforderlich, aber nur 30,9 % der IT-Meinungsführer. Das lässt darauf schließen, dass die Frage regionaler versus nationaler Verarbeitung nicht ganz klar ist oder dass die Gruppen unterschiedliche Prioritäten haben.

Bestimmte Unternehmensgrößen (500-999 und über 5.000 Beschäftigte) bevorzugen die regionale Verarbeitung, wobei mehr Befragte meinen, es sei unwichtig, wo die Kundendaten landen.

Diese Einschätzung variiert je nach Unternehmensgröße: Befragte aus größeren Unternehmen waren eher der Meinung, dass die Daten in der Region verarbeitet werden müssen, als dass sie dies für unwichtig hielten.

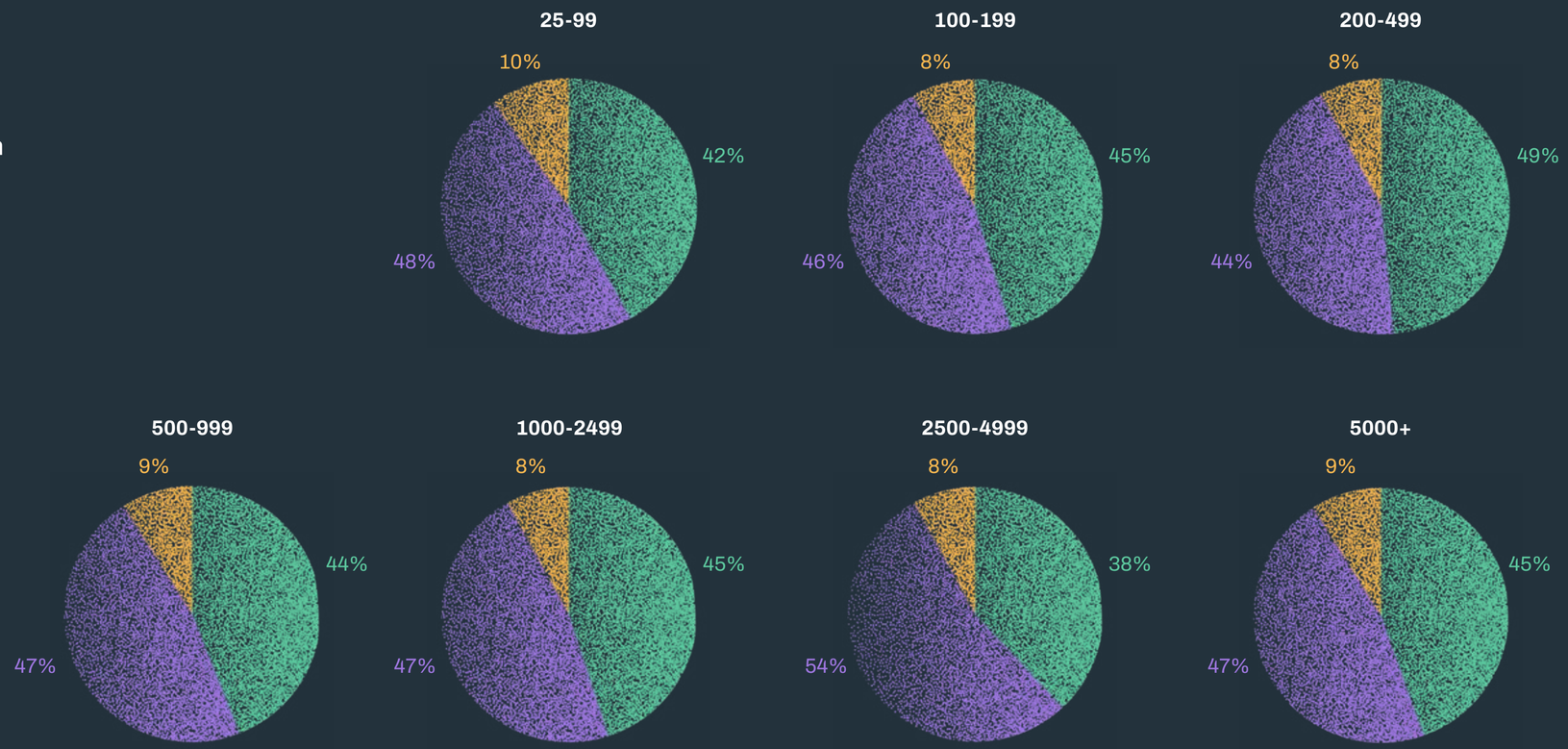
Die Bevorzugung einer starken Datenresidenz kann das Ergebnis erheblicher Umwälzungen und Veränderungen sein, sowohl in Bezug auf Vorschriften als auch in Bezug auf physische Ereignisse. Daten-Souveränität - die Regeln, nach denen die einzelnen Länder mit der Verfügungshoheit von Individuen über ihre Daten umgehen - steht im Spannungsfeld zwischen konkurrierenden Kräften wie der Globalisierung der Datenverarbeitung, regionaler Regulierung, Geopolitik und politischen Umwälzungen und dem daraus resultierenden Wunsch nach Risikominderung. All dies führt dazu, dass man sich intensiv damit beschäftigt, wo sich die eigenen Daten befinden und wohin oder durch wen sie sich bewegen.

Wo Sie die Daten verarbeiten

An diesem Punkt wird es etwas paradox: Ständig hören wir, dass die Cloud alles verändert - und doch scheint diese Technologie die Einstellung der Befragten nicht zu beeinflussen.

Unabhängig davon, ob Anwendungen in einem Unternehmen eher intern oder in der Cloud gehostet werden, blieben die Einstellungen gleich. Organisationen mit mehr als 2.500 Mitarbeitern (und Organisationen in Nordamerika) hosten Anwendungen eher vor Ort, während die Dänen, Schweden, Deutschen und Briten eher zur Cloud als zu On-Premise tendieren. Jene Organisationen, die ausschließlich auf die Cloud setzen, liegen weit darunter.

IT-Umgebung nach Beschätigtenanzahl



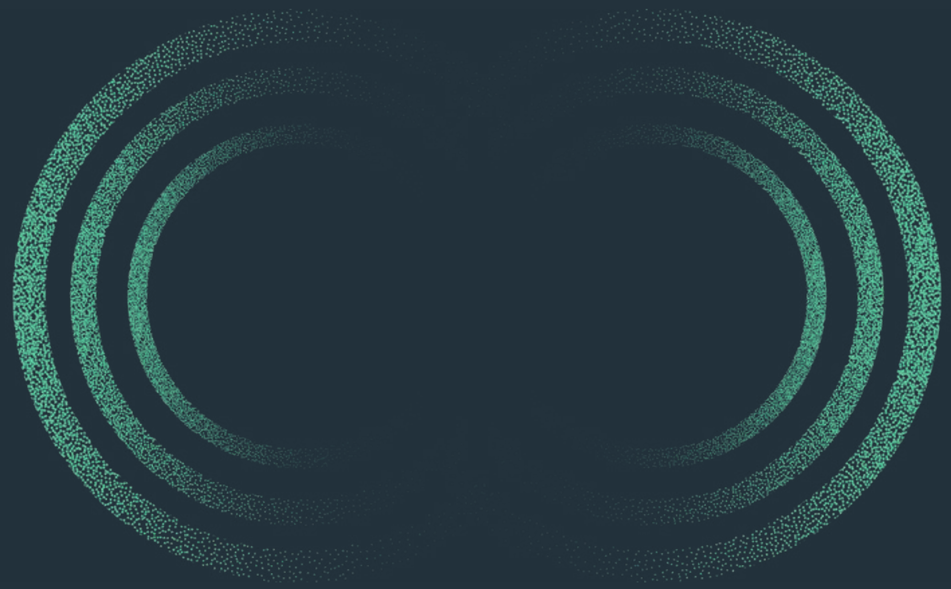
- Alle oder fast alle IT-Anwendungen/-Services werden intern auf den Servern des Unternehmens gehostet.
- Einige der IT-Anwendungen/-Dienste werden intern auf den Servern des Unternehmens gehostet, aber viele sind Cloud-basiert oder werden von einem externen Anbieter gehostet.
- Alle IT-Anwendungen und -Services sind Cloud-basiert oder werden von einem externen Anbieter gehostet.

Fazit und Empfehlungen

Die Datenresidenz zählt. Das ist ein Punkt, den unsere Countercept MDR-Kunden im letzten Jahr so vehement vorgetragen haben, dass wir für Europa eine spezielle Version von Countercept eingeführt haben, um ihren Wünschen zu entsprechen. Die Hebel und Treiber für diesen Wunsch sind komplex - aber es ist interessant, dass es dazu einen breiten Konsens unter den Befragten jeglicher Richtung gibt.

Letztlich ist es Sache der einzelnen Unternehmen, sowohl die regulatorischen Anforderungen zu erfüllen als auch einen guten Service für ihre Kunden zu gewährleisten. Die praktische Umsetzung kann, gelinde gesagt, komplex sein. Ein Wechsel von der Cloud zur lokalen Datenspeicherung und -verarbeitung ist mit einem entsprechenden Aufwand für Compliance, Sicherheit und Technik verbunden. Unsere Berater empfehlen, zunächst die nationalen Datenschutzvorschriften zu beachten und dann die Bedenken bzw. Anforderungen der Kunden einzubeziehen.

Der einzige Bereich, in dem eventuell erheblicher Handlungsbedarf besteht, ist die interne Kommunikation: Zwischen den IT-Entscheidern und den eher strategisch ausgerichteten Meinungsführern sowie dem Top-Management gibt es eine gewisse Diskrepanz in Bezug auf die regionale Datenverarbeitung. Das Verständnis für die Unterschiede zwischen nationalen und regionalen Anforderungen - und warum es diese unterschiedlichen Meinungen in den Organisationen zu geben scheint - sollte ein Bereich sein, den Sie umgehend analysieren sollten.



4. Cybersicherheit: Anbieterwechsel

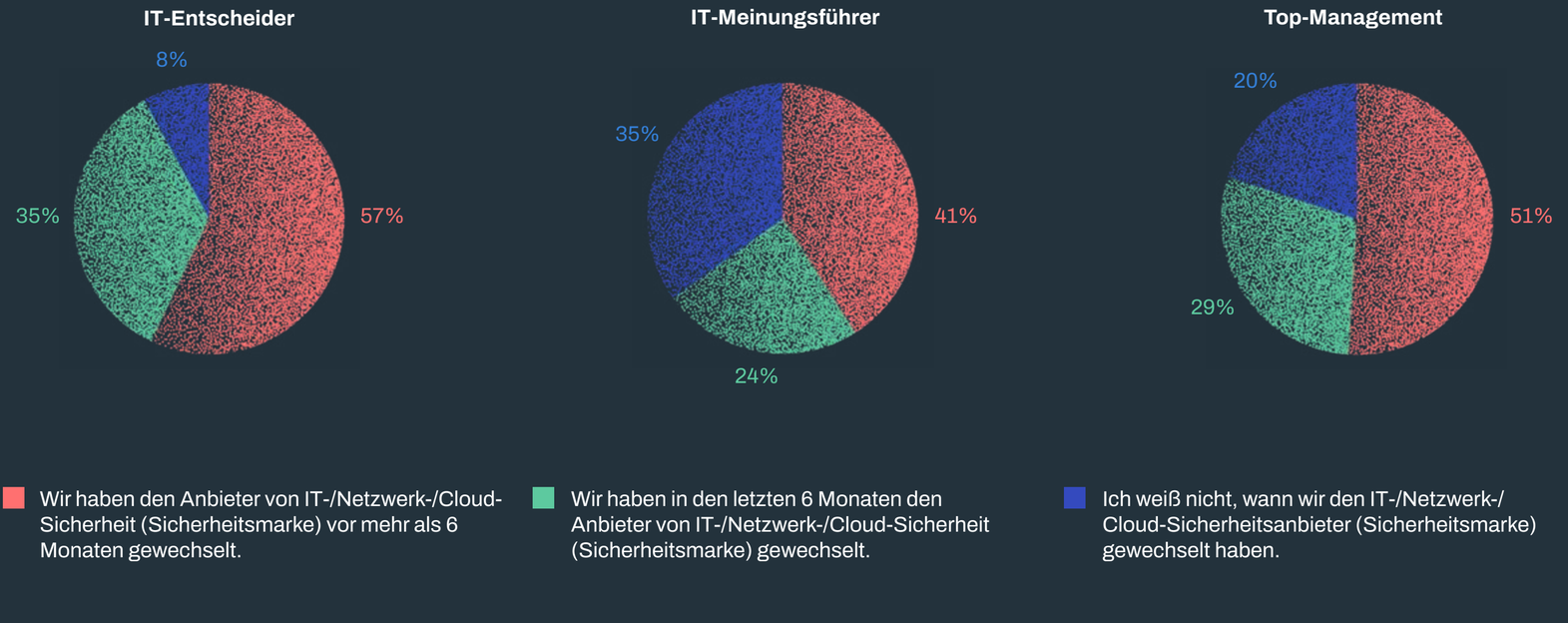
Anbieterwechsel ist die Regel

Für Sicherheitsunternehmen ist alles im Wandel - genauer gesagt für ihre Lieferanten und für ihre Anbieter.

Unsere Umfrage zeigt, dass fast ein Drittel (31,9 %) in den letzten sechs Monaten ihren Anbieter von Sicherheitslösungen gewechselt hat, und 32 % erwarten einen Wechsel der IT-Sicherheitslösung oder des Anbieters in den nächsten sechs Monaten.

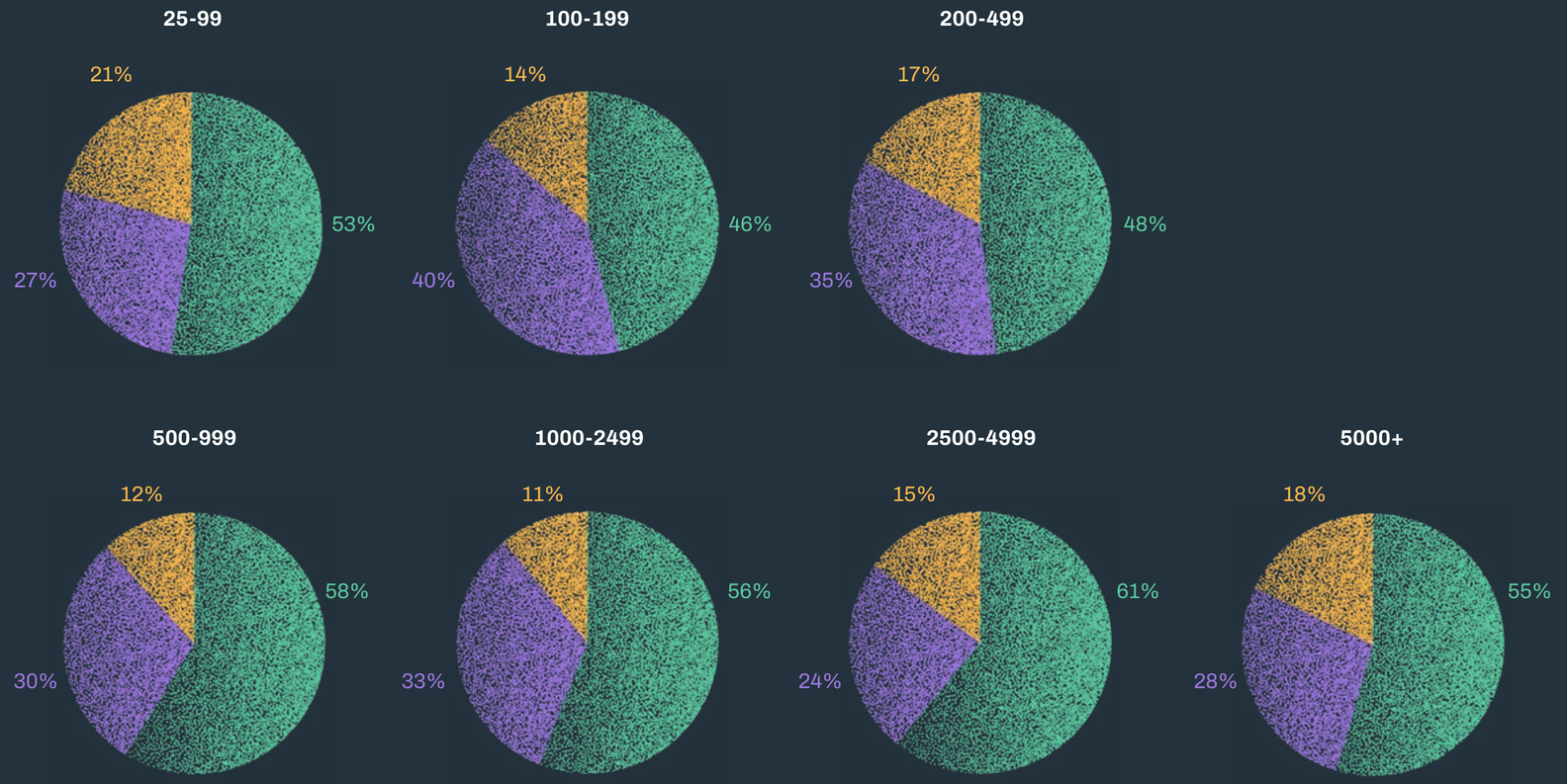
Vor allem Befragte aus dem Finanz- und Versicherungssektor sowie aus dem Bereich IT-Services und Technologie haben den Anbieter in den letzten sechs Monaten gewechselt (59,4 % bzw. 58,4 %) und erwarten eher einen Wechsel in den nächsten sechs Monaten (45 % bzw. 41,1 %).

Absichten und Kriterien für den Wechsel des Markenanbieters nach Funktion



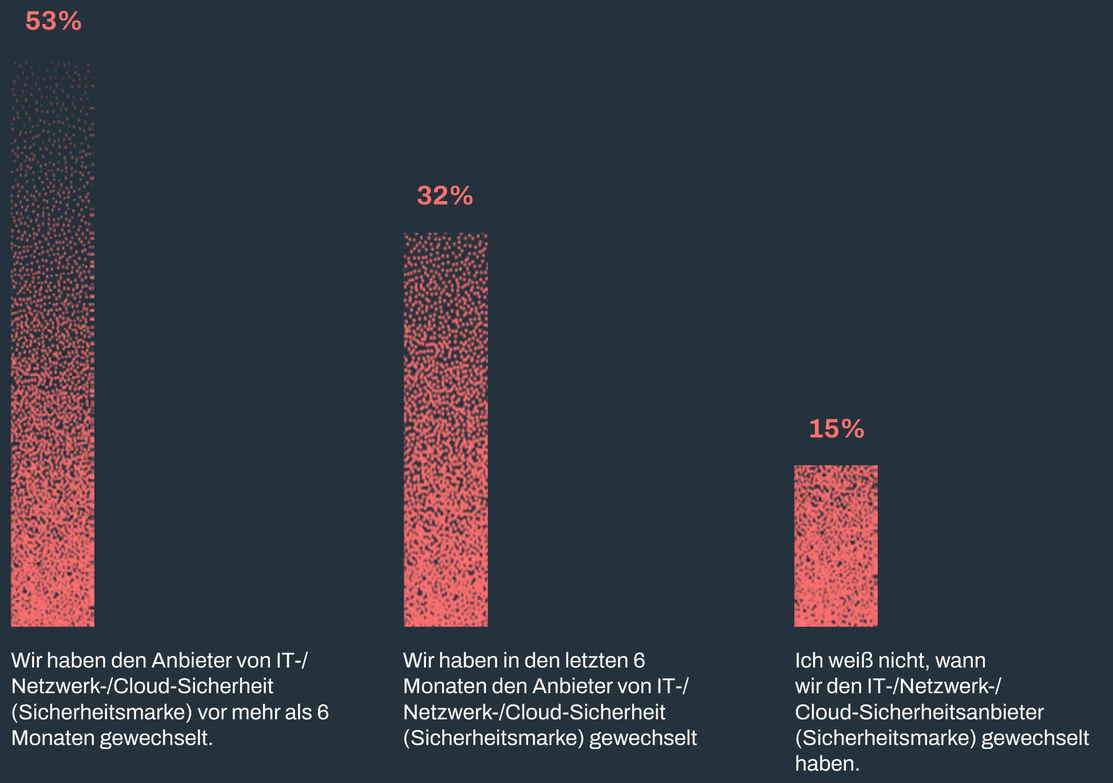
Betrachtet man dies aus der Sicht der Unternehmensgröße (n=1.800), so zeigt sich in kleinen bis mittelgroßen Unternehmen viel mehr Bewegung als in größeren Organisationen.

Absichten und Kriterien für den Wechsel des Markenanbieters nach Beschäftigtenanzahl

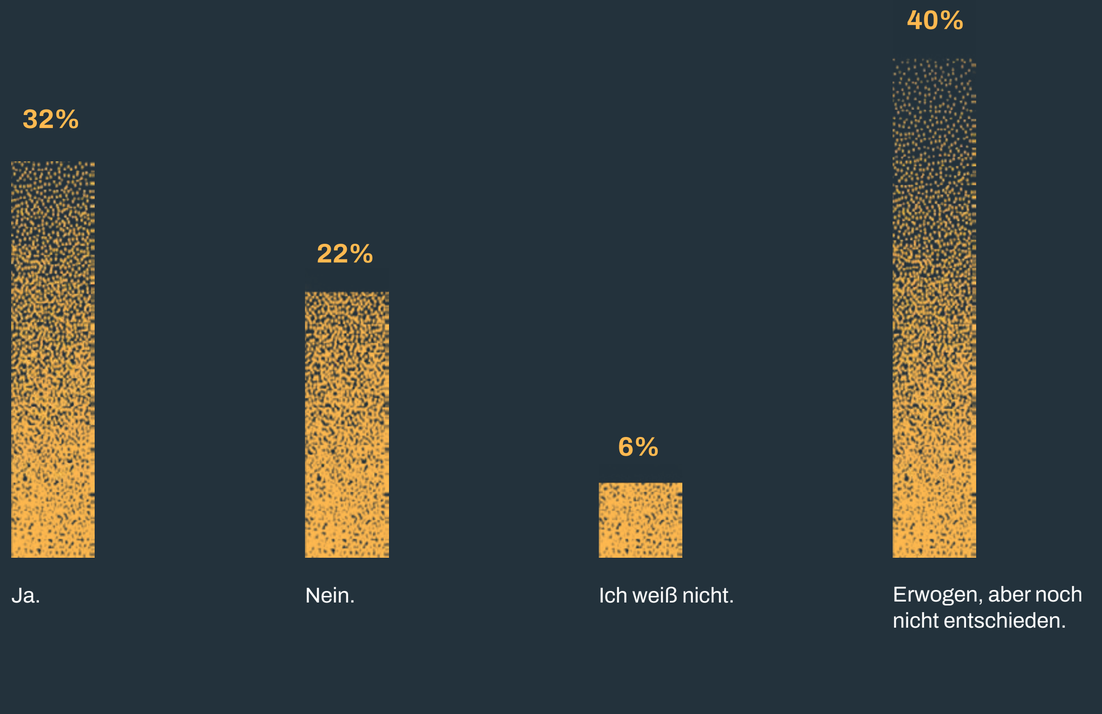


Für viele Unternehmen ist der ständige Wechsel zwischen verschiedenen Anbietern zwar die Norm, doch dieser Prozess ist kompliziert und zeitaufwändig. Wir haben Peter Page, Head of Solution Consulting bei WithSecure, gebeten, uns seine Gedanken zum Umgang von Unternehmen mit Anbieterwechseln zu erläutern. Außerdem haben wir untersucht, wie man das Vertrauen zwischen Anbietern und Kunden aufbauen und erhalten kann.

Bezüglich eines Wechsels des IT-/Netzwerk-/Cloud-Sicherheitsanbieters (Sicherheitsmarke)



Plant Ihr Unternehmen in den nächsten 6 Monaten einen Wechsel des IT-Sicherheitsanbieters?



Was fürchten Kunden am meisten bei Umstellungsprojekten?

Begrenzte oder eingeschränkte Ressourcen sind bekannte Stolpersteine - und sie machen den Wechsel von einem Anbieter zu einem anderen für viele Unternehmen zu einer gewaltigen Belastung. Einfach ausgedrückt: Manchmal ist es zu aufwändig, einen leistungsschwachen Anbieter loszuwerden. Doch das ist nicht mehr der Fall, wenn man den Aussagen der Befragten folgt.

“Sicherheitsteams sind oft nicht diejenigen, die neue Dienste implementieren”, sagt Page. “Sie müssen Projektmanagement- (und) IT-Teams in Anspruch nehmen, um die Software bereitzustellen, sie müssen sich auf das Netzwerkteam verlassen, da die Änderungen, die sie vornehmen, mehr Bereiche des Unternehmens betreffen, als sie selbst verantworten können, und sie müssen die Zustimmung von allen Akteuren einholen.”

Macht der Trend zu Cloud-Services den Wechsel leichter?

Wir haben bereits erwähnt, dass die Cloud sich ändernde Sicherheitsbedüfnisse und andere Herausforderungen mit sich bringt. Der Anbieterwechsel wird immer leichter, aber nicht wegen der Cloud: Die Nutzer sind mit dem Wechsel zwischen Cloud-Diensten genauso vertraut wie mit dem Wechsel zwischen lokalen Diensten.

Für Page kommt es auf die Menschen an: “*Es gibt jetzt einen großen Pool von Talenten, die über Fähigkeiten zur Entwicklung, Implementierung und Absicherung der Cloud verfügen. Sicherheitsanbieter brauchen diese Fähigkeiten ebenso. Aber wenn sich Ihre Umgebung ändert, ändert sich auch Ihr Sicherheitsservice. Es geht darum, Kunden zu helfen, dieses Risiko zu verstehen, und hier kommen Dinge wie Cloud Security Posture Management ins Spiel.”*

Warum werden Vertragslaufzeiten immer kürzer?

Kurzfristigere Verträge sind wohl das Resultat von zwei Faktoren: der Entwicklung der Produkte und Services auf dem Cybersicherheitsmarkt und kürzeren Vertragszeiten für Chief Information Security Officers (CISOs). Diese leitenden IT-Sicherheitsmanager bleiben meist weniger als zwei Jahre im selben Unternehmen.

Der Wechsel von CISOs kann zu ständig neuen Anforderungen und Entscheidungen führen und trägt wahrscheinlich teilweise zu dieser Instabilität auf dem Markt und dem daraus folgenden häufigen Anbieterwechsel bei.

“Es gibt auch einen ständigen Drang nach dem ‚Neuen' oder dem ‚Nächstbesten', und so steuert der Markt das Verhalten,” sagt Page. “*Manchmal wären die Mittel für den Kauf des Neuesten und Besten besser bei Basics oder für die Optimierung des Vorhandenen angelegt.”*

“*Wegen des starken Rauschens auf dem Markt ist der beste Ansatz schwer zu bestimmen. Ein CISO, der sich auf einen teuren, mehrjährigen Service einlässt, muss sicher sein, die Resultate zu kriegen, die er braucht - und die sein Vorstand sucht.”*

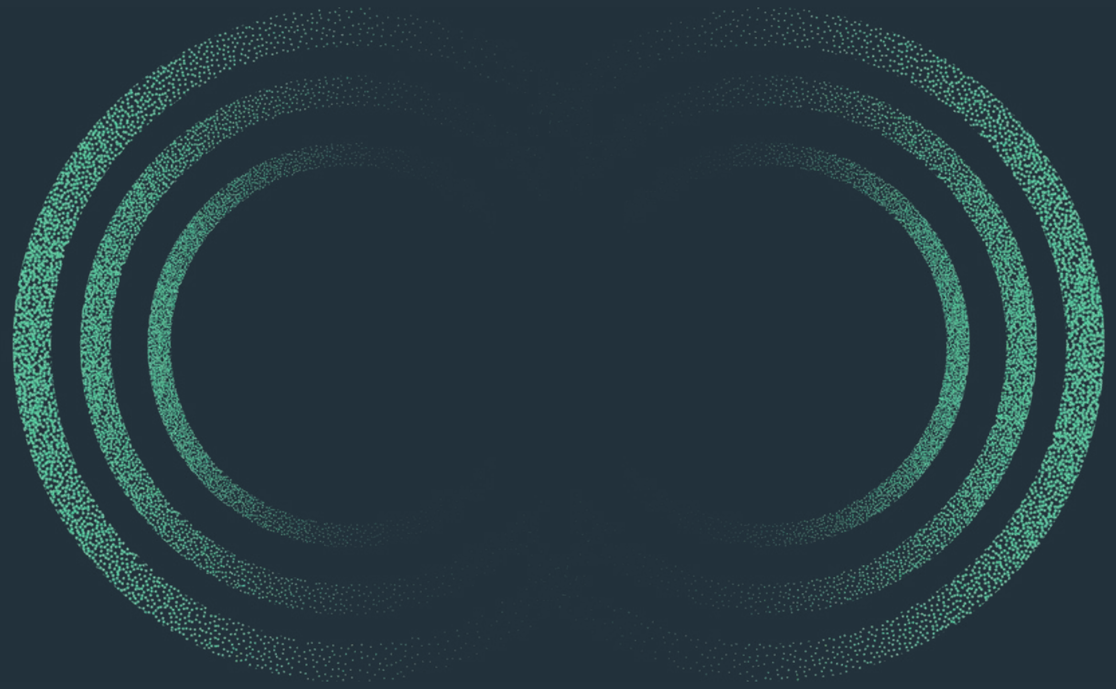
Wird es für CISOs schwieriger oder leichter, die Entscheidung für einen Wechsel zu treffen?

“Früher war es für CISOs schwierig, die Zustimmung des Vorstands für hohe Investitionen in die Cybersicherheit zu erhalten. Das ist jetzt leichter: Vorstände, CFOs und CEOs sehen die Sicherheitsverstöße und Ransomware-Infektionen in Unternehmen und können die finanziellen und ergebnisbezogenen Auswirkungen einschätzen.

“Aber aufgrund der Marktlage gibt es viele verschiedene Möglichkeiten für CISOs, das Problem anzugehen: Wo investieren sie? Sollen sie insourcen oder outsourcen? Was ist mit MDR oder EDR oder SIEM oder etwas anderem? Es ist also fast wie eine "Analyse-Paralyse". Es gibt zu viele Optionen, und das bedeutet, dass sie einen Großteil ihrer Zeit damit verbringen, Ausschreibungen zu erstellen und mit Anbietern zu sprechen - es wird zu einem Vollzeitjob, allein das zu tun.”

Der Faktor Zeit ist das Wesentliche

Trotz der Geschwindigkeit auf dem aktuellen Markt für Cybersicherheit ist Page überzeugt, dass im Interesse der Sicherheit jede Entscheidung besser ist als keine: *“Wenn man von nichts zu etwas übergeht, muss man eine Entscheidung treffen, denn man hat keine Transparenz und keinen Überblick über den Bestand. Bei Managed Services ist jedoch das Ende des Vertrags der Stichtag. Die Frage ist also: Wie zeitnah sollten Sie mit alternativen Anbietern sprechen? CISOs sind gut beraten, wenn sie 12 Monate vor Vertragsende über ihre Optionen nachdenken - da sehen wir die besten Ergebnisse.”*



5. Fazit

Es braucht etwas Zeit, die Ergebnisse der diesjährigen Umfrage zu verdauen. Klar ist, dass die Entscheidungsträger in Sachen Cybersicherheit unterschiedliche Meinungen und Erwartungen haben. Es ist daher nicht ganz leicht, die Daten zu sortieren, um herauszufinden, was verwertbar und was nur irgendwie interessant ist. Deshalb haben wir nachfolgend die unserer Meinung nach wichtigsten Erkenntnisse festgehalten. Einige dieser Erkenntnisse sind dem kundigen Leser sicherlich bereits bekannt, aber sie sind es wert, wiederholt zu werden, und unsere Daten stützen diese Schlussfolgerungen ebenfalls.

1) Die gefühlten Prioritäten sind nicht unbedingt die mit dem größten Einfluss auf die Sicherheitslage. Prüfen Sie, welche Praktiken und Kompetenzen in Ihrem Unternehmen fehlen, und vergleichen Sie das mit den angenommenen Prioritäten. Suchen Sie nach Unstimmigkeiten.

2) Sicherheitsausgaben sind Ansichtssache. Unsere Umfrage hat große Unterschiede in der Wahrnehmung der Sicherheitsbudgets für das kommende Jahr aufgezeigt, und uneinheitliche Erwartungen führen ja gerne zu Verwirrung, Konflikten und übereilten Entscheidungen. Das Rezept für ruhige und besonnene Entscheidungen ist Klarheit - und dass jeder Beteiligte weiß, was er mit einem gewissen Budget ändern, kaufen oder erreichen kann, wenn das Budget noch nicht fixiert ist.

3) Die Datenresidenz ist ein heißes Thema, und für mehr als 70 % unserer Befragten ist sie absolut entscheidend. Genauso wichtig sind aber auch die Folgen aus dem Tausch einer Cloud-basierten Anwendung, die die Datenresidenz nicht garantieren kann, gegen eine Alternative: Ist eine lokale oder interne Lösung genauso sicher oder bietet sie die benötigten Funktionen?

4) Wenn Sie den Anbieter wechseln wollen, sollten Sie sich rechtzeitig entscheiden. Es ist auffällig, dass erfolgreiche Anbieterwechsel meist mindestens 12 Monate vor dem Auslaufen oder der Erneuerung des Vertrags eingeleitet werden. Und: sich überhaupt zu entscheinden, ist wahrscheinlich die zentrale Entscheidung. Lassen Sie sich nicht von der Analyse-Paralyse einfangen.

Schließlich: Unsere Daten zeigen eine signifikante Übereinstimmung und einen Konsens zwischen den befragten Gruppen - was auf eine gute organisatorische Harmonie hinweist. Es gibt jedoch auch Punkte, bei denen die Meinungen von Entscheidern, Meinungsführern und Management deutlich auseinandergehen. Dies sind die Bereiche, die uns alle beschäftigen sollten und in denen eine klare und offene Kommunikation das wirksamste Instrument für das kommende Jahr wird.

Methodik

Die B2B-Marktforschungsstudie 2022 von WithSecure erreichte 3.072 Befragte (davon 2.098 aus Europa) durch eine Online-Umfrage im Mai 2022 in 12 Ländern, darunter neun europäische Länder: Großbritannien, Frankreich, Deutschland, Belgien, Niederlande, Dänemark, Finnland, Norwegen, Schweden sowie die USA, Kanada und Japan. Bei allen Befragten handelt es sich um IT-/Netzwerk-/Cloud-Sicherheits-Entscheidungsträger und Meinungsführer für den Kauf von IT-/Netzwerk-/Cloud-Sicherheitsprodukten und -Services in ihren Unternehmen.

Über WithSecure™

WithSecure™, ehemals F-Secure Business, ist der zuverlässige Partner für Cybersicherheit. IT-Dienstleister, Managed Security Services Provider und andere Unternehmen vertrauen WithSecure™ – wie auch große Finanzinstitute, Industrieunternehmen und führende Kommunikations- und Technologieanbieter. Mit seinem ergebnisorientierten Ansatz der Cybersicherheit hilft der finnische Sicherheitsanbieter Unternehmen dabei, die Sicherheit in Relation zu den Betriebsabläufen zu setzen und Prozesse zu sichern sowie Betriebsunterbrechungen vorzubeugen. WithSecure™ nennt diesen Ansatz „Outcome-based Cyber Security“. KI-gesteuerte Sicherheitsmaßnahmen sichern Endgeräte und die Zusammenarbeit in der Cloud mit intelligenten Erkennungs- und Reaktionsmechanismen. Die Detection & Response-Experten von WithSecure™ identifizieren Geschäftsrisiken, indem sie proaktiv nach Bedrohungen suchen und bereits laufende Angriffe abwehren – dabei arbeiten sie eng mit Instituten, großen Unternehmen und innovativen Tech-Firmen zusammen. Sie haben mehr als 30 Jahre Erfahrung in der Entwicklung von Technologien, die sich an den Bedürfnissen der Unternehmen orientieren. Das Portfolio von WithSecure™ eröffnet durch flexible Vertriebsmodelle die Möglichkeit, gemeinsam mit Partnern zu wachsen.

WithSecure™ Corporation wurde 1988 gegründet und ist an der NASDAQ OMX Helsinki Ltd. gelistet.

W / T H®
secure