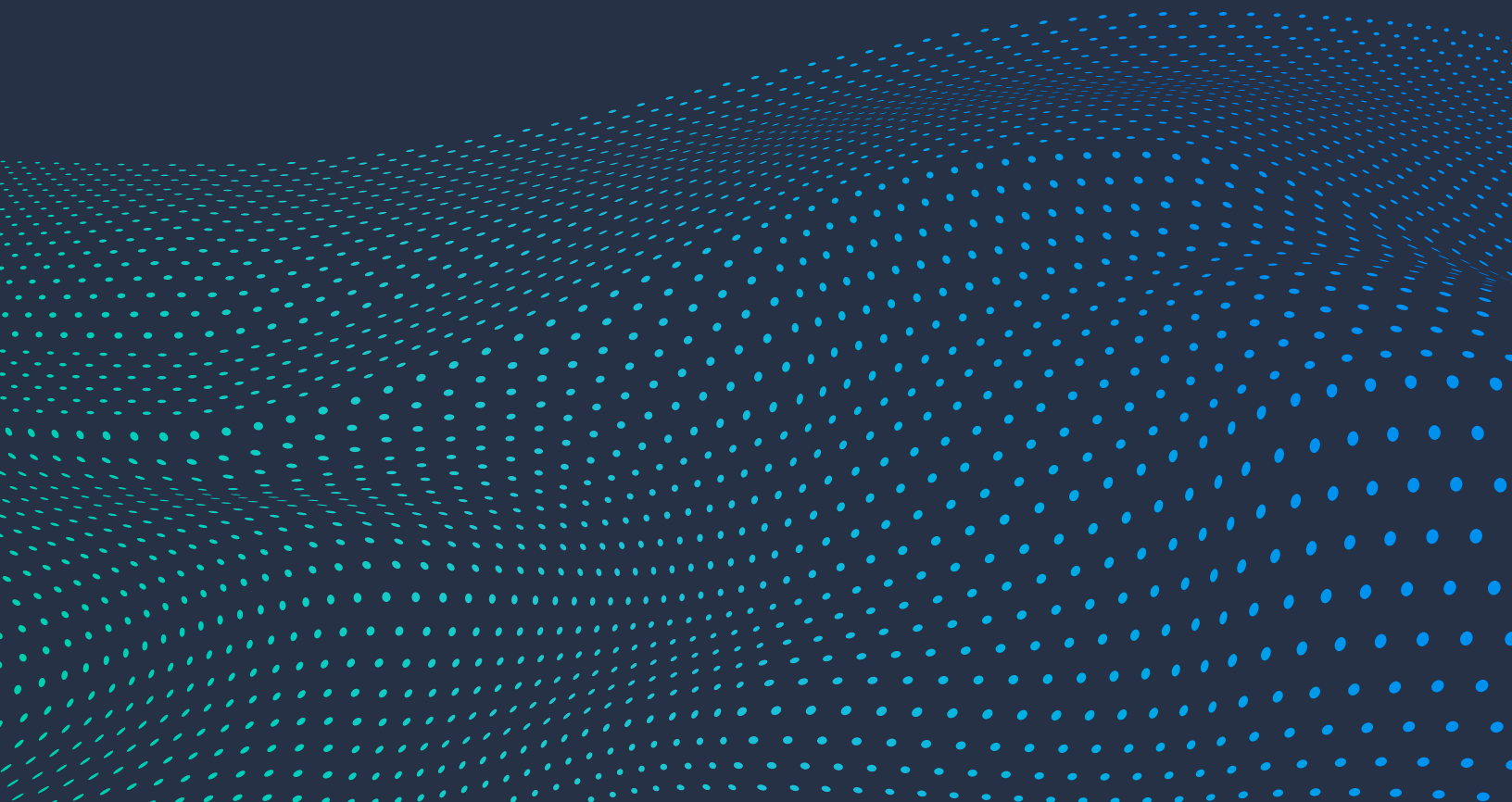
Barracuda
Your journey, secured.

APRIL 2024

Der CIO-Bericht: So steuern Sie Ihr Unternehmen durch Cyberrisiken



Inhaltsverzeichnis

Einleitung

Durch den zunehmenden Einsatz von neuen Technologien wie Künstlicher Intelligenz (KI) ist es wichtiger denn je, dass Führungskräfte in Unternehmen wissen, wie sie die Implementierung dieser effektiv und sicher verwalten können.

Für viele Unternehmen kann dies ein schwieriger Prozess sein. Die Cyber-Risikolandschaft ist komplex und entwickelt sich unentwegt weiter. Die Sprache der Cyberbedrohungen kann zutiefst technisch, jargonreich und undurchsichtig sein. Darüber hinaus ist die Risikobereitschaft von Unternehmen unterschiedlich. Was für die einen ein akzeptables Risiko darstellt, kann für die anderen ein Gräuel sein. Und angesichts konkurrierender Prioritäten bei den Unternehmensressourcen müssen häufig Kompromisse eingegangen werden.

Das ultimative Sicherheitsziel für alle Organisationen sollte Cyber-Resilienz sein. Wirksame Präventions- und Erkennungsmaßnahmen sind nach wie vor ein wichtiger Eckpfeiler von Sicherheitsstrategien, aber Unternehmen sollten sich nicht lediglich darauf beschränken. Die Statistiken legen nahe, dass die Wahrscheinlichkeit, von einem Sicherheitsvorfall betroffen zu sein, nahezu unvermeidlich ist. Viele Unternehmen werden wiederholt Opfer von Angriffen, vor allem, wenn sie die eigentliche Ursache des ersten Vorfalls oder die Faktoren, die ihn ermöglicht haben, nicht behoben haben.

Entscheidend ist, wie Sie sich auf einen Vorfall vorbereiten, ihn überstehen, darauf reagieren und sich davon erholen. Das bedeutet Cyber-Resilienz.

Und während fortschrittliche Defense-in-Depth-Sicherheitslösungen schon sehr viel Sicherheit bieten, hängt der Erfolg Ihrer Sicherheit letztendlich von den Menschen ab – der Unternehmensleitung, den IT-Sicherheitsexperten und den Mitarbeitenden im Allgemeinen.

Unsere Cybernomics 101-Studie in Zusammenarbeit mit dem Ponemon Institute, zeigt, wie personelle Sicherheitsherausforderungen, mangelnde Unterstützung auf Vorstandsebene oder Fachbereichsleitung, der Fachkräftemangel und die inkonsistente Umsetzung von Sicherheitsrichtlinien im gesamten Unternehmen die Cyberresistenz untergraben können. Viele Unternehmen sorgen sich um die Sicherheit ihrer Lieferkette und darum, wer außerhalb des Unternehmens Zugriff auf ihre sensiblen oder vertraulichen Daten haben könnte – beides Bereiche mit erheblichem Risiko und Hauptziele von Cyberangriffen.

Die meisten Unternehmen wissen, wie exponiert sie sind. Nur 43 % bewerten die eigenen Sicherheitsvorkehrungen als sehr wirksam. Das ist jedoch nicht zwangsläufig so besorgniserregend, wie es scheint. Die Überzeugung, dass Sie mehr für Ihre Sicherheit tun können, kann dazu beitragen, Ihre Aufmerksamkeit und Ressourcen auf die Bereiche zu konzentrieren, in welchen sie benötigt werden, und so letztlich für mehr Sicherheit zu sorgen.

In diesem Bericht befassen wir uns eingehender mit den Forschungsergebnissen zum Thema Cyber-Resilienz und schlagen Ihnen eine Anleitung, wie Sie Ihren Weg in eine stärkere, widerstandsfähigere Zukunft finden, vor.

Siroui Mushegian, CIO, Barracuda Networks Inc

Methodik

Das Ponemon Institute befragte im September 2023 insgesamt 1917 IT-Sicherheitsexperten aus den USA (522), dem Vereinigten Königreich (372), Frankreich (329), Deutschland (425) und Australien (269). Die letzte Stichprobe der Befragten repräsentierte Unternehmen mit einer Mitarbeiterzahl zwischen 100 und 5.000. Alle Befragten sind an der Verwaltung der IT-Sicherheitsfunktionen oder -aktivitäten ihres Unternehmens beteiligt.

In diesem Bericht werden die Ergebnisse nach Anzahl der Mitarbeiter der Unternehmen und für eine Reihe von Branchen untersucht, die für alle untersuchten Länder konsolidiert wurden.

Wie Unternehmen ihre Sicherheitslage bewerten

Wir wollten von den Befragten wissen, wie überzeugt sie von ihrer Fähigkeit sind, mit Cyberrisiken, -schwachstellen und -angriffen wirksam umzugehen. Dabei bewerteten wir die Antworten auf einer Skala von 1 bis 10, wobei 1 für sehr unwirksam und 10 für vollkommen wirksam steht.

Mit deutlichem Abstand sind Finanzdienstleister am zuversichtlichsten, was ihre Fähigkeiten angeht. Mehr als die Hälfte (55 %) stufen ihre Sicherheitsvorkehrungen als sehr wirksam ein. Die kleinsten befragten Unternehmen waren am wenigsten optimistisch. Etwa die Hälfte (48 %) sah die eigene Sicherheitslage am unteren Ende der Skala.

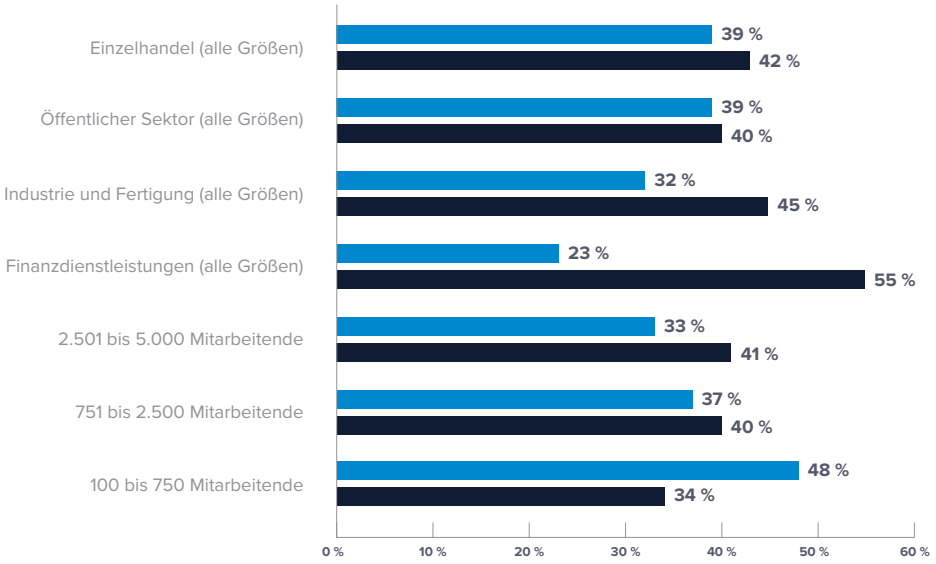


ABBILDUNG 1

Wie würden Sie die Sicherheitslage Ihres Unternehmens hinsichtlich der Wirksamkeit bei der Bekämpfung von Risiken, Schwachstellen und Angriffen auf einer Skala von 1 bis 10 bewerten?

Nicht sehr wirksam (1 bis 4)

Sehr wirksam (7 bis 10)

n=1.917

Die Kategorie „durchschnittlich wirksam“ (5 bis 6) ist in der Tabelle nicht enthalten.

Herausforderungen in puncto Governance

Fehlen einer einheitlichen unternehmensweiten Sicherheit

Für kleinere und mittelgroße Unternehmen ist die größte Herausforderung für die Unternehmensführung das Fehlen einheitlicher unternehmensweiter Sicherheitsrichtlinien und -programme. Die Hälfte (48 % bzw. 50 %) bezeichnet dies als eine der größten Herausforderungen, verglichen mit nur einem Viertel (27 %) der Unternehmen mit 2.501 bis 5.000 Mitarbeitenden. Das ist auch die größte Herausforderung für Finanzdienstleister (49 %), den Einzelhandel (49 %) und den öffentlichen Sektor (40 %).

Die Umsetzung einheitlicher Richtlinien kann für Sicherheitsteams ein organisatorisches Problem darstellen. Führungskräfte zögern oft, Sicherheitsmaßnahmen durchzusetzen, die unbequem oder einschränkend erscheinen. Mancher Mitarbeitende mag sich gegen Kontrollen wie den „Just-in-Time"-Zugang oder den „Least Privilege"-Zugriff zu bestimmten Anwendungen oder Daten sträuben, vor allem, wenn diese zuvor offen zugänglich waren.

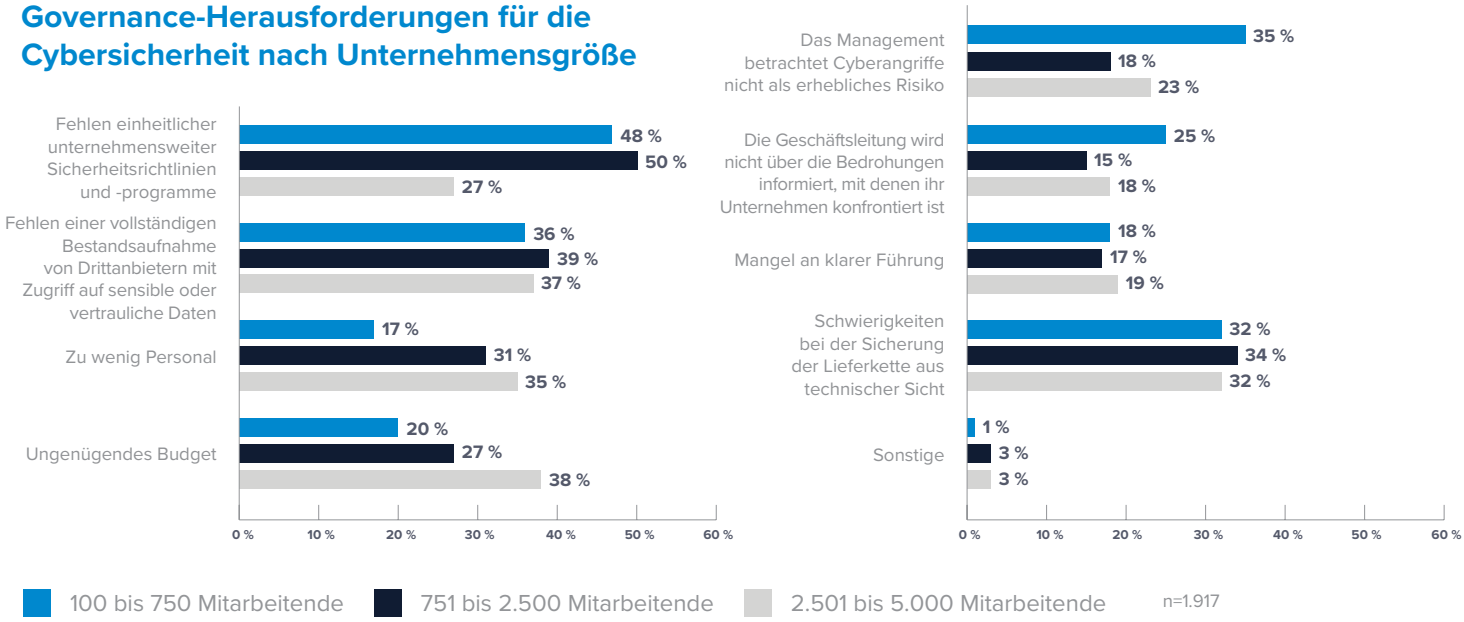
Einige Beschäftigte kennen die Sicherheitsrichtlinien vielleicht nicht, wissen nicht, ob sie für ihre Systeme oder Tätigkeiten gelten, oder glauben, dass ihr Arbeitsbereich ausgenommen werden sollte.

Derartige Missverständnisse können zu Verwirrung und Unmut führen und letztlich einer wirksamen Umsetzung im Wege stehen, was wiederum das organisatorische Risiko erhöht.

Je offener und transparenter Sie mit Ihren Beschäftigten über die Richtlinien diskutieren können, für wen sie gelten und warum sie wichtig sind, desto einfacher wird es. Diese Gespräche fördern das Verständnis und die Zusammenarbeit, vor allem, wenn sie durch regelmäßige Schulungen unterstützt werden. Es ist wichtig, auf Änderungen zu reagieren und die Sicherheitsrichtlinien regelmäßig zu überprüfen und zu aktualisieren, damit sie an die sich entwickelnden Bedrohungen und Geschäftsanforderungen angepasst sind.

ABBILDUNG 2

Governance-Herausforderungen für die Cybersicherheit nach Unternehmensgröße



Mangelnde Unterstützung und Verständnis seitens der Führungsebene

Die befragten kleineren Unternehmen machen sich große Sorgen über Herausforderungen auf Führungsebene. Knapp über ein Drittel (35 %) berichten, dass die Führungskräfte Cyberangriffe nicht als erhebliches Risiko sehen. Das hat nichts mit einem Versagen der Unternehmensführung zu tun. Man kann sich nur schwer für etwas interessieren oder sich für etwas einsetzen, das man nicht versteht. Ein Viertel der kleineren Unternehmen gibt zu, dass die Geschäftsleitung nicht über Bedrohungen informiert wird, mit denen das Unternehmen konfrontiert ist. Es liegt in der Verantwortung der Sicherheitsexperten, in einer Sprache zu sprechen, die die Führungskräfte des Unternehmens verstehen. Sie müssen in der Lage sein, ein Narrativ aufzubauen und zu erklären, wie man den Ruf einer Marke durch proaktive, vielschichtige Abwehrprogramme schützen kann.

Das Risikomanagement-Menü

Ein nützliches Instrument, das Führungskräften hilft, die Risiken und Sicherheitsentscheidungen zu verstehen, die sie treffen müssen, ist die Präsentation eines einfachen Menüs mit Optionen. Mithilfe dieses Ansatzes können Sie besser erkennen, welche Herausforderungen vorrangige Aufmerksamkeit erfordern und wie hoch Ihre allgemeine Risikobereitschaft ist.

Anhand der nachstehenden vier Schritte können Sie sich ein Bild von den Risiken machen, denen Ihr Unternehmen derzeit ausgesetzt ist:

1. **Bedrohungen:** Die Umstände oder Ereignisse, die organisatorische Abläufe, Vermögenswerte, Einzelpersonen oder andere Organisationen schädigen könnten
2. **Schwachstellen:** Die Schwachstellen, die das Unternehmen oder die Ressource in Gefahr bringen
3. **Wahrscheinlichkeit:** Die Wahrscheinlichkeit, dass ein Risikoszenario eintritt
4. **Risiko:** Das Potenzial für ein negatives Ergebnis

Sobald Sie das Risikoniveau verstanden haben, können Sie entscheiden, welches Sicherheitsniveau Sie benötigen und haben wollen:

- „Hohe Sicherheit“ bedeutet zum Beispiel, dass fast alles gesperrt wird. Dies bietet nahezu vollständige Sicherheit, kann aber auch Einschränkungen mit sich bringen, die zu Komplexität, Verzögerungen und Unmut führen können.
- Am anderen Ende der Skala bedeutet „geringe Sicherheit“, dass der Zugang weitgehend uneingeschränkt, offen und bequem ist – und dadurch eben auch stark offen für Angriffe.

Nicht jedes Unternehmen verfügt vom ersten Tag an über alle erforderlichen Sicherheitsressourcen, Tools und Prozesse. Wenn Sie die Sicherheit wie ein Menü betrachten, können Sie einen Ablaufplan aufstellen, wie Sie dieses Ziel erreichen und welche Risiken Sie auf dem Weg bewältigen müssen.

Mithilfe dieses Ansatzes können Sie besser erkennen, welche Risiken vorrangige Aufmerksamkeit erfordern und wie hoch Ihre allgemeine Risikobereitschaft ist. Mithilfe eines zentralen Risikoregisters können Sie die Risiken Ihres Unternehmens im Auge behalten und fundierte Entscheidungen zu deren Bewältigung oder Eindämmung treffen.

Mangel an Fähigkeiten sowie Sichtbarkeit und Kontrolle durch Dritte

Die größten befragten Unternehmen machen sich mit 38 % bzw. 35 % die meisten Sorgen über den Mangel an Geld und qualifiziertem Sicherheitspersonal.

Risiken in der Lieferkette stellen für alle Unternehmen, unabhängig von ihrer Größe, eine große Herausforderung dar. Dazu gehören die fehlende Erfassung von Dritten, die Zugang zu sensiblen oder vertraulichen Daten haben, und die technische Herausforderung, die Lieferketten zu sichern – jeweils etwa ein Drittel der Befragten nannte beides als größte Herausforderung.

Diese Bedenken rühren wahrscheinlich daher, dass ein großer Teil der Lieferkette außerhalb der Sicherheitsbereiche eines Unternehmens liegt. Je weiter Sie sich von der eigenen Kontrollmöglichkeit entfernen, desto größer ist das Risiko – vor allem, wenn es sich um Anbieter in Märkten mit geringeren Sicherheitsvorschriften handelt.

Schatten-IT ist zu einem großen Problem geworden. Der unkontrollierte Einsatz von Softwareanwendungen stellt ein Sicherheitsrisiko dar, da sie häufig nicht den IT-Richtlinien entsprechen. Sogar zugelassene Softwaretools können Risiken mit sich bringen, da sich viele zu Plattformen entwickelt haben, die Marktplätze für Apps und Plug-ins von Drittanbietern anbieten. Diese Ergänzungen können unbefugten Vierten Zugriff auf vertrauliche Daten außerhalb des Sicherheitsbereichs des Unternehmens verschaffen.

Zwar sind generative Open-Source-KI-Tools wertvoll für Innovation und Produktivität, doch sie speichern und trainieren ihre Modelle auch anhand der ihnen zur Verfügung gestellten Daten. Der unkontrollierte Einsatz von generativen KI-Tools kann zur Preisgabe von sensiblen Daten jenseits der Sicherheitsgrenzen des Unternehmens führen.

Momentaufnahme: Finanzdienstleistungen

Finanzdienstleister vertrauen auf die Stärke ihrer Sicherheitsplanung. Lediglich 3 % verfügen über keinen Incident-Response-Plan.

Das ist natürlich nicht verwunderlich. Die Finanzbranche unterliegt strengen Vorschriften und bei Verstößen auch erheblichen Strafen. Die Mitarbeitenden haben Verständnis dafür, dass sie innerhalb von Regeln, Prozessen und Verfahren arbeiten müssen. Die Zustimmung des Vorstands und der Geschäftsleitung zu Sicherheitsmaßnahmen in Verbindung mit ausreichenden Finanzmitteln bedeutet, dass Strategien für die Geschäftskontinuitätsplanung (Business Continuity Planning, BCP) und Notfallwiederherstellung (Disaster Recovery, DR) vorhanden sind, damit das Unternehmen nach einem Angriff möglichst schnell wieder arbeitsfähig ist.

Dennoch steht auch diese Branche vor Herausforderungen betreffend der Sicherheit. Viele Finanzinstitute sind sehr groß. Sie haben sich durch Übernahmen zu riesigen globalen Organisationen entwickelt, die in Silos existieren. Die Implementierung globaler und belastbarer Sicherheitsprozesse für alle diese Systeme ist daher enorm schwierig.

Momentaufnahme: Einzelhandel

Einzelhändler sind nicht so zuversichtlich wie Finanzdienstleister, wenn es um ihre allgemeine Sicherheitslage geht: 39 % stufen sie als relativ unwirksam ein. Allerdings schätzen 42 % ihre Sicherheitsvorkehrungen als sehr wirksam ein. Dies unterstreicht die komplexe, zweigeteilte Natur der Branche in Fragen der Sicherheit.

Auf der Unternehmensseite gibt es die Hauptniederlassung mit modernster Ausrüstung, Unternehmenssoftware, Rechenzentren und Sicherheitsvorkehrungen. Auf der anderen Seite stehen die Vertriebs- und Versandzentren, die Produktionslieferketten und die eigentlichen Einzelhandelsgeschäfte. Möglicherweise arbeiten sie mit völlig unterschiedlichen Technologien. Dabei kann es sich zum großen Teil um Altgeräte handeln, die sich nur schwer oder mit großem Aufwand ausmustern lassen, und die IT-Teams müssen dann versuchen, alles so gut wie möglich auf einen Nenner zur bringen.

Am häufigsten nannten Einzelhandelsunternehmen die fehlende Erfassung von Dritten, die Zugang zu sensiblen und vertraulichen Daten haben, als eine der größten Herausforderungen für die Unternehmensführung (46 %) sowie Schwierigkeiten bei der Sicherung der Lieferkette aus technischer Sicht (35 %).

Momentaufnahme: Öffentlicher Sektor

Auch bei Einrichtungen im öffentlichen Sektor herrscht häufig wenig Vertrauen in die eigene Sicherheitslage: 39 % stufen diese als relativ wirkungslos ein. Ein unzureichendes Budget (39 %) ist dabei die größte Herausforderung, gefolgt von einem Mangel an einheitlichen Sicherheitsrichtlinien und -programmen

(40 %). Knapp eine Institution von zehn (12 %) hat keinen Incident-Response-Plan.

Sicherheit im öffentlichen Sektor ist schwer zu erreichen. Es gibt viele Ämter und Angestellte, die abgesichert werden müssen, die Budgets sind immer knapp bemessen und die Aufmerksamkeit der Verantwortlichen, vor allem der politischen, ist oft auf andere Dinge ausgerichtet. Viele Institutionen im öffentlichen Sektor sind mit schwankenden Budgets und Finanzierungen konfrontiert, die sich je nach Regierungspartei schnell ändern können. Unter diesen Umständen kann die Planung langfristiger Sicherheit schwierig sein.

Einsatzbereitschaft für die Incident Response

Die gute Nachricht ist, dass etwa die Hälfte aller befragten Organisationen – unabhängig von Branche oder Mitarbeiterzahl – über einen Incident-Response-Plan verfügt, der in der gesamten Organisation einheitlich angewendet wird – und mehr als die Hälfte gibt an, dass der Plan mindestens einmal im Jahr formal getestet wird.

Das war es dann auch mit den guten Nachrichten. Etwa ein Viertel (23 %) der größten Unternehmen hat ihren Vorfallreaktionsplan noch nie getestet. Dies liegt möglicherweise daran, dass dies in einem großen Unternehmen ein komplexer, zeitaufwändiger und störender Prozess sein kann. Außerdem kann die Einrichtung eines BCP/DR-Prozesses für Unternehmen kostspielig sein, wenn hierfür große Datenmengen oder Systemsicherungen erforderlich sind.

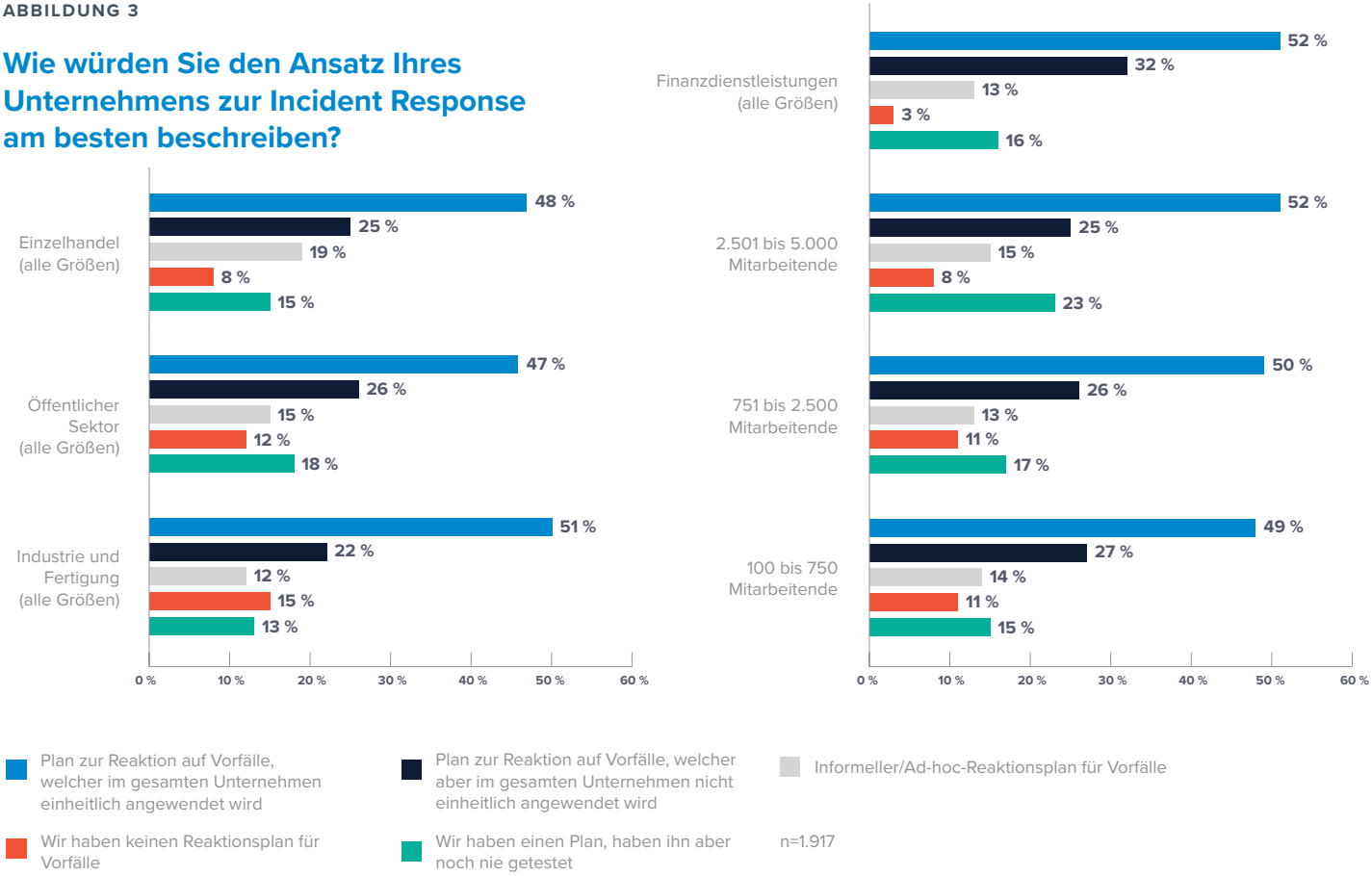
Darüber hinaus gibt etwa jeder Zehnte zu, dass er keinen Incident-Response-Plan hat.

Wenn ein Unternehmen keinen Plan hat, was im Falle eines Sicherheitsvorfalls zu tun ist, besteht die Gefahr, dass es nicht weiß, wie es auf die Ereignisse reagieren soll, und deshalb nichts oder das Falsche tut.

Ein „Purple-Team"-Ansatz kann dazu beitragen, die Reaktionsfähigkeit eines Unternehmens zu stärken. Die „violetten Teams" verwalten und koordinieren Simulationen zur Incident Response. Sie erstellen Szenarien, in denen ein „rotes Team" einen Vorfall simulieren kann, auf den dann ein „blaues Team" dann reagiert. Mithilfe solcher Simulationen können Unternehmen Sicherheitsvorfälle besser erkennen, darauf reagieren, ihre Auswirkungen eindämmen und aus ihnen lernen.

ABBILDUNG 3

Wie würden Sie den Ansatz Ihres Unternehmens zur Incident Response am besten beschreiben?



Checkliste zur Cyber-Resilienz

Die folgende Checkliste für Cyberresistenz stützt sich auf das Cybersicherheits-Framework des US National Institute of Standards and Technologies (NIST).

ZIEL	STRATEGISCHE AUSRICHTUNG FÜR FÜHRUNGSKRÄFTE – WAS SIE WISSEN MÜSSEN	FORTSCHRITT
VORBEREITUNG	**Organisieren** • Einhaltung der gesetzlichen Auflagen Welche gesetzlichen Vorschriften und Compliance-Verpflichtungen haben Sie in jedem der Märkte, in denen Sie tätig sind?	☐
	• Einbindung und Zuständigkeit des Managements Wer im Führungsteam muss an Entscheidungen zu Cyber-Resilienz und zu Risiken beteiligt sein?	☐
	• Cyberversicherung Welche Art von Versicherung benötigen Sie und sind Sie bereit bzw. in der Lage, in diese zu investieren?	☐
	Identifizieren • Asset-Management Welche Assets haben Sie, wo befinden sie sich, wer hat Zugriff darauf? Was sind Ihre wichtigsten Ressourcen, um die Geschäftskontinuität und den Betrieb aufrechtzuerhalten?	☐
	• Risikomanagement und Strategie Welches sind Ihre am stärksten gefährdeten Assets? Welchen Risiken sind diese ausgesetzt? Wie groß sind die möglichen Auswirkungen eines Angriffs hinsichtlich der Schäden, Störungen oder Verluste?	☐
STANDHALTEN	**Schützen** • Sicherheitsprozesse, -richtlinien und -technologien Wie können Sie Assets, Infrastruktur und Mitarbeiter im Rahmen Ihrer verfügbaren Ressourcen am besten schützen?	☐
	• Schulungen zum Thema Cybersicherheit Wie schulen und unterstützen Sie Ihre Mitarbeiter?	☐
	• Wartung und Kontrolle – Patchen usw. Sind die grundlegenden Sicherheitsmaßnahmen vorhanden? Patching, robuste Authentifizierung und Zugriffskontrollen (Multifaktor-Authentifizierung/Zero Trust) usw.?	☐
	Erkennen • Technologien und Verfahren zur Erkennung Können Ihre Sicherheitssysteme neue und neu aufgetretene Bedrohungen erkennen und blockieren?	☐
	• Security Operations Center Ist Ihre Sicherheitsüberwachung zuverlässig und kontinuierlich? Können Sie den gesamten IT-Bereich rund um die Uhr überwachen und managen? Haben Sie Zugang zu den Tools, den Kompetenzen und dem Personal, um Warnsignale und Anomalien zu untersuchen?	☐
REAGIEREN	**Schadensbegrenzung** • Planung und Reaktionsprozesse bei Vorfällen Haben Sie einen Incident Response-Plan, der für das gesamte Unternehmen gilt? Wird dieser regelmäßig getestet und ist auf dem neuesten Stand? Wie können Sie Zwischenfälle eindämmen und neutralisieren? Welche Dauer der Ausfallzeiten können Ihre kritischen Systeme aushalten? Können Sie bei Bedarf auf manuelle Prozesse zurückgreifen? Falls Ihre Kunden ebenso davon betroffen sind, wie hoch ist der vereinbarte Servicelevel? Befindet sich Ihr System On-Premises oder in der Cloud? (Handelt es sich um ein Security-as-a-Service (SaaS) Unternehmen, ein Geschäftssystem usw.?) Wen müssen Sie im Hinblick auf die Compliance informieren und wann?	☐
	• Interne und externe Kommunikation	☐
	• Analyse von Vorfällen und Schadensbegrenzung	☐
WIEDERHERS-TELLUNG	**Wiederherstellen** • Recovery-Planung Haben Sie einen Geschäftskontinuitätsplan/Disaster Recovery Plan? Haben Sie bei Ihrem Cloud-Anbieter eine „Hohe Verfügbarkeit“ eingerichtet? Benötigen Sie Unterstützung durch Dritte, um alle Lücken aufzudecken und zu schließen?	☐
	• Interne und externe Kommunikation	☐
	• Verbesserungen Welche Lektionen haben Sie gelernt? Welche Schritte unternehmen Sie/sollten Sie unternehmen, um Ihre Sicherheit zu erhöhen?	☐

Fazit

Cyber-Resilienz liegt in der Verantwortung aller, die Hauptlast tragen jedoch die Sicherheitsexperten. Wir unterstützen Sie dabei und bieten Ihnen sowohl grundlegende als auch praktische Möglichkeiten, um die Einhaltung eines Mindestmaßes an Compliance sicherzustellen.

Mithilfe der Checklistenvorlage können Sie dafür sorgen, dass Ihr Team und Ihr Unternehmen auf Kurs bleibt und die Verantwortung übernimmt. Passen Sie das Dokument an die Realität Ihres Geschäftsumfelds an und verwandeln Sie es in eine Roadmap und einen Plan mit Meilensteinen, Leistungen und Verantwortlichen.

Weitere Informationen

Es stehen zahlreiche hilfreiche Tools, Frameworks und Leitfäden zur Verfügung, die Sie auf dem Weg zur Cyber-Resilienz unterstützen. Hier sind ein paar Vorschläge, die Ihnen den Einstieg erleichtern sollen:

- Cyber Governance Code of Practice (UK)
- National Association of Corporate Directors (USA)
- Australian Institute of Company Directors (Australien)
- Cybersecurity Framework 2.0 (USA)

Über Barracuda

Wir von Barracuda wollen die Welt sicherer machen. Wir sind der Meinung, dass jedes Unternehmen Zugang zu Cloud-basierten Sicherheitslösungen auf Unternehmensebene verdient, die einfach zu erwerben, bereitzustellen und zu nutzen sind. Wir schützen E-Mails, Netzwerke, Daten und Anwendungen mit innovativen Lösungen, die mit unseren Kunden wachsen und sich anpassen. Mehr als 200.000 Unternehmen weltweit vertrauen auf den Schutz durch Barracuda – während sie sich oftmals der Vielzahl der Gefahren, vor welchen sie beschützt werden, unbewusst sind.

Weitere Informationen finden Sie unter de.barracuda.com.

Barracuda
Your journey, secured.