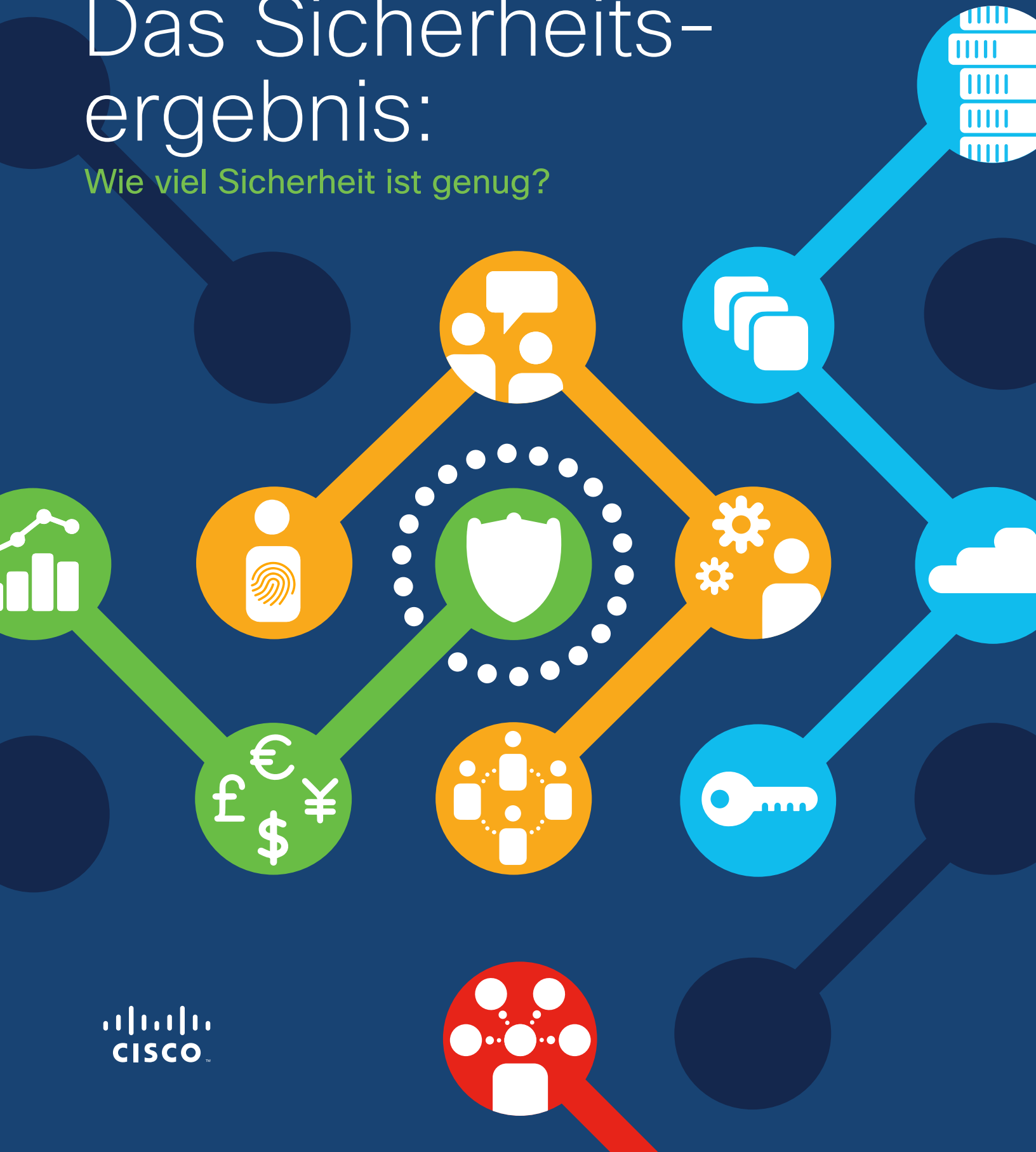
Das Sicherheits-ergebnis:

Wie viel Sicherheit ist genug?



CISCO

Inhalt

Einleitung – Das Sicherheitsergebnis 3

Übersicht – Die Zahlen lügen nicht 4

Faktoren zur Bestimmung einer erfolgreichen Sicherheit 5

- Budget 5
- Know-how 7
- Fähigkeiten 7
- Einfluss 11

Wichtigste Erkenntnisse 12

Empfehlungen für mehr Sicherheit 13

Methodik 15

Über die Cisco Reihe zur Cybersicherheit 16

Einleitung: Das Sicherheitsergebnis

Wenn Unternehmen Dutzende von Sicherheitsprodukten installieren und es dennoch zu Sicherheitsverletzungen kommt, dann wirft dies eine wichtige Frage auf: *Wie viel Sicherheit ist genug?* Wie viele Produkte benötigt ein Unternehmen? Um welche Lösungen handelt es sich? Wie viel sollte für die Sicherheit ausgegeben werden? Mit anderen Worten: *Welches Ergebnis wird mit Sicherheit angestrebt?*

Unternehmen können in dem Versuch, Angreifer in Schach zu halten, enorme Summen in Sicherheit investieren. Aber wie viel *müssen* sie ausgeben und was *müssen* sie tun, um ihre Sicherheit zu gewährleisten?

Es geht dabei nicht nur um Geld. Vielleicht verfügt ein Unternehmen über ein umfangreiches Sicherheitsbudget, beschäftigt aber nicht die richtigen Experten, um seine Vision umsetzen zu können. Oder vielleicht verfügt ein Unternehmen zwar nur über ein reduziertes Sicherheitsbudget, hat es aber sorgfältig in die richtigen Mitarbeiter investiert – und in seine anfälligsten oder kritischsten Ressourcen. Manchmal wird ein Großteil der Sicherheit eines Unternehmens von einem Drittanbieter verwaltet, sodass das Unternehmen keinen Einfluss auf erforderliche Änderungen oder Upgrades ausüben kann.

Ja, das Budget ist wichtig, wenn es um Sicherheit geht. Doch es ist nicht alles. Wie ist Ihr Unternehmen in Sachen Sicherheit aufgestellt? Verfügen Sie über die richtigen Mitarbeiter, Prozesse und Technologien, um Ihre Umgebung proaktiv zu schützen? Bleiben Sie hinter Ihren Sicherheitsanforderungen zurück oder übertreffen Sie diese?

In diesem Bericht erläutern wir die wichtigsten Faktoren für eine erfolgreiche Sicherheit, die von unseren Branchenexperten sowie einer Gruppe von etwa 80 Teilnehmern in einer kürzlich von Cisco durchgeführten Doppelblindbefragung von Sicherheitsexperten festgelegt wurden. Und natürlich wäre es nicht fair, wenn wir Ihnen nicht wenigstens eine kleine Hilfestellung geben würden, wie Sie Ihre Sicherheit stärken können.

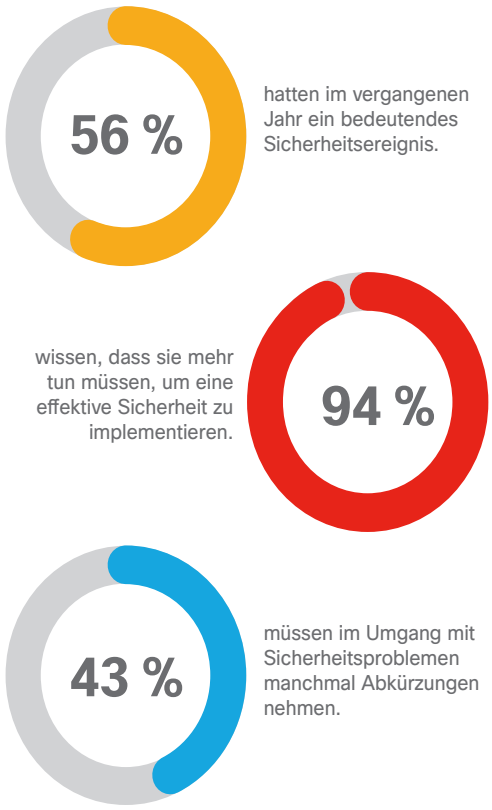
„Die Sicherheitsherausforderungen sind mit zahlreichen Dynamiken verbunden, die über reines Geld hinausgehen.“

Wendy Nather, Leiterin von Advisory CISOs, Cisco

Die Zahlen lügen nicht

Ein bezeichnendes Ergebnis unserer kürzlich durchgeführten Umfrage war, dass es bei 56 Prozent der Teilnehmer (mehr als die Hälfte) im vergangenen Jahr zu einem bedeutenden Sicherheitsereignis gekommen war (Sicherheitsverletzung, unbefugter Netzwerkzugriff, Malware-Infektion usw.). 94 Prozent der Befragten gaben an zu wissen, dass sie mehr tun müssen, um eine effektive Sicherheit zu implementieren. Und 43 Prozent räumen ein, dass sie im Umgang mit Sicherheitsproblemen teilweise Abkürzungen nehmen müssen – beispielsweise, indem sie einen infizierten Endpunkt vollständig entfernen, anstatt die Malware korrekt zu beseitigen (siehe Abbildung 1).

Abbildung 1 Wie sind die heutigen Unternehmen in Sachen Sicherheit aufgestellt?
Prozentsatz der Befragten, N=79



Quelle: Cisco Security Bottom Line-Umfrage 2019

Aber es gibt nicht nur schlechte Neuigkeiten. 95 Prozent der Befragten gaben an, dass sie effizient ermitteln können, welche Daten und Systeme in ihrem Unternehmen das höchste Maß an Schutz benötigen – definitiv ein guter Anfang! Warum haben sie also immer noch Schwierigkeiten? Geht es um Feld? Oder sind andere Faktoren im Spiel?

Wendy Nather, Leiterin von Advisory CISOs bei Cisco, nennt die folgenden vier Faktoren, die sich auf eine erfolgreiche Sicherheit auswirken können:

- Budget
- Know-how
- Fähigkeiten
- Einfluss

Als Gesprächseinstieg prägte Nather vor einigen Jahren den Begriff „Security Poverty Line“ (etwa „Sicherheitsarmutsgrenze“). Darüber hinaus verfasste sie in ihrer Funktion als Research Director bei **451 Research** zwei Berichte zu dem Thema: „Living Below the Security Poverty Line“ im Jahr 2011 und „The Real Cost of Security“ im Jahr 2013.

„Anhand meiner vorherigen Erfahrungen als CISO im öffentlichen und privaten Sektor weiß ich, dass viele Unternehmen Schwierigkeiten beim Thema Sicherheit haben“, sagt Nather. „Die Sicherheitsherausforderungen sind mit zahlreichen Dynamiken verbunden, die über reines Geld hinausgehen. So kann ein Unternehmen, das Millionen ausgibt, weiterhin schwache Sicherheitsergebnisse erzielen, während ein Unternehmen mit kleinerem Budget basierend auf seinen konkreten Anforderungen ausreichende Verteidigungsmaßnahmen haben kann.“

Faktoren zur Bestimmung einer erfolgreichen Sicherheit

Außer Geld können sich noch weitere Faktoren auf das Sicherheitsergebnis auswirken. Neben dem Budget gibt es noch Know-how, Fähigkeiten und Einfluss.

Budget

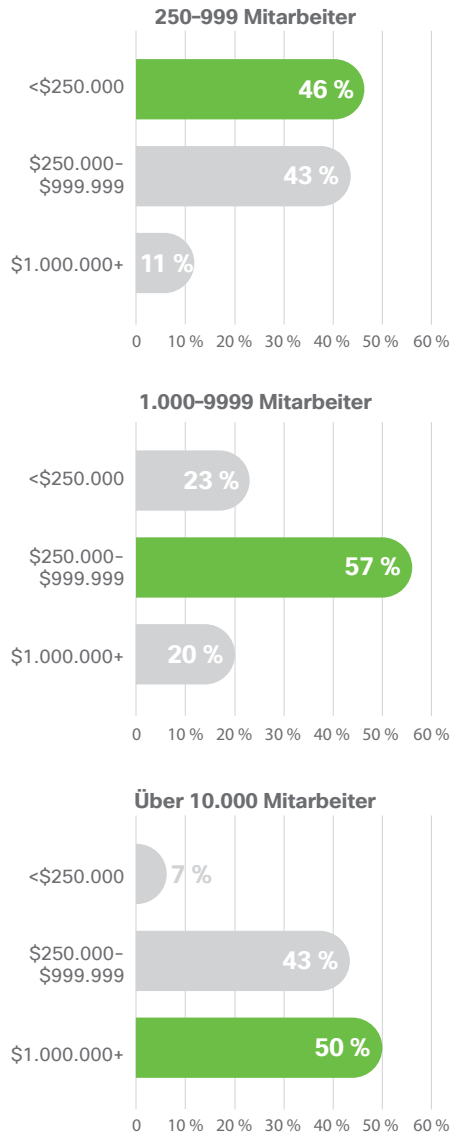
Wie viel geben Unternehmen für Sicherheit aus?

Bei Sicherheitsausgaben gibt es keine „magische Zahl". Der Betrag, den ein Unternehmen für seine Sicherheit aufwenden sollte, hängt von verschiedenen Faktoren ab, unter anderem: Größe, Branche, Risikoneigung, Grad der Gefährdung usw. Als groben Maßstab für andere Unternehmen haben wir allerdings die jährlichen Ausgaben unserer Umfrageteilnehmer (nach Unternehmensgröße) aufgeteilt. Abbildung 2 zeigt:

- Unter den **mittelständischen Unternehmen (250–999 Mitarbeiter)** geben 46 % jährlich 250.000 US-Dollar für Sicherheit aus, 43 Prozent geben jährlich 250.000 bis 999.999 US-Dollar aus (nur 11 Prozent geben jährlich 1 Million US-Dollar oder mehr aus).
- Die Mehrheit (57 Prozent) der **großen Unternehmen (1.000–9.999 Mitarbeiter)** geben jährlich 250.000 bis 999.999 US-Dollar für Sicherheit aus (nur 20 Prozent geben jährlich 1 Million US-Dollar oder mehr aus, 23 Prozent geben jährlich weniger als 250.000 US-Dollar aus).
- 50 Prozent der **Großkonzerne (mehr als 10.000 Mitarbeiter)** geben jährlich 1 Million US-Dollar oder mehr für Sicherheit aus, 43 Prozent geben 250.000 bis 999.999 US-Dollar aus und nur sieben Prozent geben weniger als 250.000 US-Dollar aus.

Diese Zahlen liefern zwar einige grundlegende Einblicke in das Verhältnis zwischen Unternehmensgröße und Sicherheitsausgaben, es muss aber beachtet werden, dass beim Thema Sicherheit die Größe eines Unternehmens nicht alles ist. Die reine Mitarbeiterzahl hängt nicht zwangsläufig mit der Höhe der Umsätze oder den verfügbaren Finanzmitteln oder auch nur dem Risikograd eines Unternehmens zusammen. Beispielsweise kann ein Hedge-Fonds Milliarden von Dollar mit einem kleinen Team verwalten, während eine große Behörde mit zahlreichen Angestellten ggf. nur über ein schmales und schwankendes Budget verfügt.

Abbildung 2 Wie viel gibt Ihr Unternehmen jährlich für Sicherheit aus?



Quelle: Cisco Security Bottom Line-Umfrage 2019

Ein weiterer beliebter Maßstab für die Bewertung von Sicherheitsausgaben ist der prozentuale Anteil am IT-Budget. Allerdings sind prozentuale Anteile nicht hilfreich, wenn die betroffenen Zahlen sehr groß oder sehr klein sind. Wenn eine Bank es sich leisten kann, 10 Prozent eines IT-Budgets in Milliardenhöhe für Sicherheit auszugeben, kann sie natürlich viel mehr kaufen als ein Startup, das 10 Prozent eines IT-Budgets von 50.000 US-Dollar für Sicherheit ausgeben kann. Wenn Unternehmen ihre Sicherheitsausgaben festlegen, sind sie besser beraten, die Preise für die konkreten Sicherheitsfunktionen zu ermitteln, die sie benötigen, als einfach einen zufälligen Prozentsatz ihres IT-Budgets zu bestimmen.

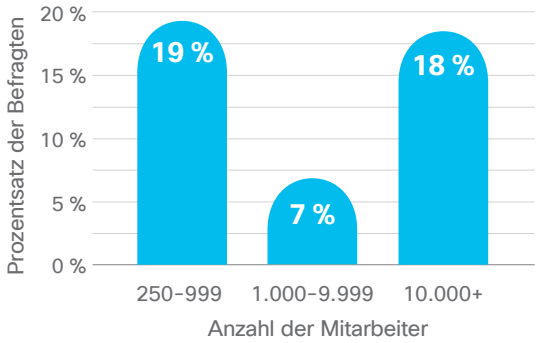
Können Unternehmen sich die Sicherheit leisten, die sie benötigen?

Erstaunliche 84 Prozent der Umfrageteilnehmer gaben an, dass sie sich einen Teil der *Mindestmenge* an Sicherheit leisten können, die sie zum Schutz ihrer Infrastruktur benötigen, jedoch nicht alles. Interessanterweise fanden wir heraus, dass Unternehmen mit 1.000–9.999 Mitarbeitern die größten Schwierigkeiten haben, wenn es darum geht, was sie sich leisten können – nur sieben Prozent dieser Unternehmen gaben an, dass sie sich das Mindestmaß an Sicherheit, das sie benötigen, leisten könnten (siehe Abbildung 3).

Im Vergleich dazu gaben 19 Prozent der kleineren Unternehmen (250–999 Mitarbeiter) und 18 Prozent der größeren Unternehmen (über 10.000 Mitarbeiter) an, sie könnten sich das gesamte *Mindestmaß* an Sicherheit leisten, das sie benötigen. Scheinbar können Sicherheitsbudgets nicht immer proportional mit dem Wachstum eines Unternehmens ansteigen (bis eine sehr große Anzahl von Mitarbeitern erreicht wird).

„Die interessante Frage lautet, warum es nicht die kleinsten Unternehmen sind, die sich am häufigsten nicht in der Lage fühlen, sich das Mindestmaß an Sicherheit zu leisten, das sie benötigen", sagt Nather. „Liegt es daran, dass sie den Eindruck haben, ein weniger lohnenswertes Ziel für Angriffe zu sein, und deshalb nicht so viel Sicherheit brauchen? Nimmt das wahrgenommene Sicherheitsrisiko im Relation zu anderen Wachstumsfaktoren eines Unternehmens zu? Oder erscheint ein Unternehmen auf dem Radar der Angreifer, nachdem es sich ein gewisses Profil erarbeitet hat, nur um dann festzustellen, dass es seine eigenen Sicherheitsvorgaben nicht erfüllen konnte?"

Abbildung 3 Mein Unternehmen kann sich das nötige Mindestmaß an Sicherheit leisten.
Prozentsatz der Befragten, die zustimmen



Quelle: Cisco Security Bottom Line-Umfrage 2019

Sorgt ein größeres Budget für mehr Vertrauen in die Sicherheit/bessere Fähigkeiten?

27 Prozent der Unternehmen, die jährlich 1 Million US-Dollar oder mehr für Sicherheit ausgeben, gaben an, sie könnten sich das gesamte erforderliche Minimum an Sicherheit leisten. Dem gegenüber stehen nur neun Prozent der Unternehmen, die jährlich 250.000 bis 999.999 US-Dollar für Sicherheit ausgeben. Die logische Schlussfolgerung scheint also zu sein, dass höhere Ausgaben bei Sicherheitsfähigkeiten durchaus einen Unterschied machen.

Allerdings haben Unternehmen mit sämtlichen Sicherheitsbudgets weiterhin den Eindruck, dass sie mehr für die Implementierung von effektiver Sicherheit tun müssen. 94 Prozent der Unternehmen, die jährlich 1 Million US-Dollar oder mehr ausgeben, 95 Prozent der Unternehmen, die jährlich 250.000 bis 999.999 US-Dollar ausgeben, und 92 Prozent der Unternehmen, die jährlich weniger als 250.000 US-Dollar ausgeben, gaben an, sie müssten mehr tun.

Unter den Unternehmen mit 1.000–9.999 Mitarbeitern gaben nur 23 Prozent an, dass sie sich in Sachen Sicherheits-Know-how am meisten auf interne Mitarbeiter verlassen. Dies betont wiederum die Erkenntnis, dass Unternehmen dieser speziellen Größe die größten Schwierigkeiten haben, wenn es darum geht, sich die nötigen Sicherheitsfunktionen leisten zu können.

Budget ist also zwar auf jeden Fall hilfreich, ist allerdings beim Thema Sicherheit nicht alles. Welche anderen Faktoren spielen eine Rolle?

Know-how

Verfügen die Unternehmen über die nötigen Mitarbeiter und Fähigkeiten, um ihre Umgebungen effektiv zu schützen?

Bei der Frage, auf wen sie sich in Sachen Sicherheits-Know-how *am stärksten* verlassen, nannten nur 37 Prozent interne Mitarbeiter. Knapp genauso viele Befragte (28 Prozent) gaben an, sich überwiegend auf professionelle Netzwerke zu verlassen. Dies betont den weit verbreiteten Mangel an Fachkräften in der Cybersicherheit. Laut der **Untersuchung von (ISC)²** mangelt es uns heute weltweit an knapp 3 Millionen Cybersicherheitsexperten.

Es ist zwar gut, dass die Unternehmen das Gefühl haben, sich an externe Ressourcen wenden zu können, wenn sie Sicherheits-Know-how benötigen, doch es gibt wichtiges Unternehmenswissen, bei dem sie sich auf ihre internen Sicherheitsmitarbeiter verlassen können sollten. Dazu zählt das Wissen rund um Benutzerfreundlichkeit und Prozessdesign, Risikoanalyse und die Reaktion auf Vorfälle.

„Es müssen zahlreiche Entscheidungen zu Sicherheitsrisiken getroffen werden und ein wesentlicher Teil der Reaktionen auf Vorfälle ist nur dann möglich, wenn man über tiefgreifende Kenntnisse eines Unternehmens verfügt", sagte Nather. „Auch wenn man externe Incident-Responder beauftragt, müssen diese sich weiterhin auf interne Experten verlassen können, die wissen, was im Netzwerk geschieht."

Darüber hinaus haben wir aufgedeckt, dass 34 Prozent der Befragten aus den Medien von den Sicherheitsschwachstellen erfahren, die sich auf ihr Unternehmen auswirken. Dies unterstreicht den bestehenden Bedarf an zuverlässigen Journalisten und fachkundigen Bloggern, die die Bewusstseinslücke vieler Unternehmen beim Thema Cybersicherheit schließen.

Fähigkeiten

Welche zusätzlichen Faktoren hindern Unternehmen daran, eine hohes Maß an Sicherheit zu erzielen?

Selbst wenn ein Unternehmen über das nötige Know-how verfügt, um zu wissen, was es im Rahmen seines Sicherheitsprogramms tun muss, bedeutet das nicht zwangsläufig, dass es auch über die nötigen Fähigkeiten verfügt, um dies umzusetzen. Beispielsweise herrscht landläufig die Meinung, dass Netzwerksegmentierung eine wichtige Cybersicherheitskontrolle darstellt, doch ein komplexes Legacy-Netzwerk, das von verschiedenen Anbietern betrieben wird, ist möglicherweise zu schwierig und kostspielig, um es nur mit den vorhandenen Ressourcen zu entwirren.

Außerdem können Sicherheitsteams ihre Anforderungen nicht immer als Vorgaben für externe Gruppen oder Unternehmen heranziehen. Muss ein Hersteller beispielsweise Dutzende von landesspezifischen Betriebsstandards und Vorschriften erfüllen, kann es Jahre dauern, bis er ein Software-Update für eine Kontrollsysteme freigeben und verteilen kann.

Fähigkeiten sind ein wichtiger Faktor für das Ergebnis. Fähigkeiten, manchmal auch als „Sicherheitsreifegrad“ bezeichnet, basieren auf grundlegenden Funktionen, die Unternehmen benötigen, bevor sie sich an komplexere Projekte wagen können. Dies umfasst (siehe Abbildung 4):

Abbildung 4 Reifegrad-Pyramide

1. **Wissen, was Sie haben und wofür es gut ist.** Die Pflege einer Bestandsaufnahme ist in der heutigen dynamischen Umgebung nicht so einfach, wie sie klingt. Viele Anwendungsökosysteme sind so komplex, dass keine Einzelperson wissen kann, welche Daten zu welchen Zwecken und über welche Schnittstellen geteilt werden. In Benutzer-Audits werden in der Regel Accounts aufgedeckt, die kritisch, aber nicht dokumentiert sind.
2. **Die Fähigkeit, Änderungen an Ressourcen anzustoßen (und zu verhindern).** Wenn Sie nicht die Kontrolle über eine Ressource haben, müssen Sie in der Lage sein, den Verantwortlichen dazu zu bringen, diese rechtzeitig zu verändern, um Schwachstellen beheben zu können. Ebenso müssen Sie sicherstellen, dass Änderungen nur dann durchgeführt werden, wenn sie genehmigt wurden, und dass dabei auch technologische Abhängigkeiten berücksichtigt werden.
3. **Verstehen Ihrer Sicherheitsrisiken.** Was sind Ihre kritischsten Ressourcen und welchen Wert haben sie für Kriminelle? Sie sollten wissen, welche Arten von Bedrohungen mit höchster Wahrscheinlichkeit auf Ihre Ressourcen abzielen, wie Sie sie erkennen und blockieren können. Andernfalls stecken Sie vielleicht Zeit und Geld in Ressourcen, die keine Rolle spielen, und übergehen dabei wichtigere Ressourcen.
4. **Die Fähigkeit, Sicherheitstechnologie zu installieren und zu betreiben.** Sobald Sie die ersten drei Fähigkeiten gemeistert haben, können Sie Produkte und Services effektiv nutzen.

Welche Technologien werden am häufigsten in Sicherheitsprogrammen verwendet?

Dies sind die 15 wichtigsten Sicherheitstechnologien, die von unseren Umfrageteilnehmern verwendet werden:

1. **Firewalls/Management von Sicherheitsrichtlinien**
2. **E-Mail-Sicherheit**
3. **Netzwerk-Malware-Schutz**
4. **Erkennung/Schutz von Cloud-Bedrohungen und -Workloads**
5. **Schutz vor Datenverlust**
6. **Verschlüsselung**
7. **VPN**
8. **Sicheres Internet-/Web-Gateway**
9. **Security Information & Event Management (SIEM)**
10. **Netzwerkzugriffskontrolle**
11. **Cloud Access Security Broker**
12. **Endpunktsicherheit/EDR**
13. **Firewall für Web-Anwendung**
14. **Netzwerkbedrohungserkennung/ Netzwerkdatenverkehrsanalyse**
15. **Threat-Intelligence-Plattformen**

„Je mehr Produkte Sie haben, desto mehr müssen Sie dafür tun, um alle diese Informationen miteinander zu verbinden. Beim Thema Sicherheit benötigen Sie einen ganzheitlichen Ansatz statt einer Strategie mit starren Säulen ... Mit integrierter Sicherheit können Sie anfangen, Maßnahmen zu ergreifen, ohne Ihr Team wesentlich zu vergrößern.“

Marisa Chancellor, Senior Director, Information Security, Cisco

Für sich selbst genommen bilden die 15 oben aufgeführten wichtigen Technologien ein umfangreiches Portfolio, das nach einer großen Anzahl von Personen mit umfassendem Know-how verlangt, um diese Technologien zu konfigurieren, zu warten und zu überwachen. Die Konsequenz ist, dass die Personalkosten des Sicherheitsergebnisses höher sind, als vielen Unternehmen klar ist, wenn sie versuchen, ihre Bedürfnisse zu planen.

„In meiner vorherigen Rolle als Branchenanalytikerin habe ich Sicherheitsexperten befragt, welche Technologien CISOs ihrer Meinung nach kaufen müssen, um ihre Unternehmen richtig zu schützen", sagte Nather. „Darauf erhielt ich die unterschiedlichsten Antworten, was bedeutet, dass es keine standardmäßige Vorgehensweise gibt. Einigen führten nur vier Technologien an, andere hingegen über 31 verschiedene Tools."

Nather führt fort: „Viele Teilnehmer dieser Umfrage gaben einfach an, dass die Bedürfnisse eines Unternehmens von verschiedenen Faktoren abhängen – über welche Arten von Daten es verfügt, in welcher Branche es tätig ist, ob es geografisch verteilt ist und so weiter. Wenn wir es nicht schaffen, eine einheitliche Lösung für den CISO zu entwickeln – und hier verfügen wir höchstens über einen Compliance-Standard für einen eng bemessenen, wohlverstandenen Risikofall wie PCI-DSS –, können wir auch nicht erwarten, dass alle Unternehmen mit Sicherheit wissen, was sie tatsächlich brauchen. Und wenn ein Unternehmen nicht weiß, was es braucht, dann weiß es auch nicht, ob es sich Sicherheit überhaupt leisten kann."

Es gibt zwar einige Technologien, für die sich die meisten Unternehmen entscheiden, wie Firewalls und Endpunktsicherheit, aber der Rest hängt von der konkreten Situation eines Unternehmens ab. Möglicherweise sind umfangreiche Recherchen und ein Cybersicherheits-Audit erforderlich, bevor ein Unternehmen genau bestimmen kann, was es benötigt oder sich leisten kann.

Kelley Misata, PhD, ist Gründerin und CEO von Sightline Security. Sightline ist ein neues Cybersicherheitsunternehmen und eine gemeinnützige Organisation nach 501(c)(3), das zusammen mit anderen gemeinnützigen Organisationen deren Sicherheit bewertet, priorisiert und verbessert.

Cybersicherheit für gemeinnützige Organisationen

Warum wird eine Organisation wie Sightline heute benötigt?

Misata: Es gibt mehrere Gründe, aber hier sind die drei wichtigsten. Erstens: Gemeinnützige Organisationen wissen noch nicht, was sie brauchen. Sie navigieren die Cybersicherheitslandschaft ohne Karte. Da die Sicherheit heute so komplex ist, ist das äußerst schwierig – insbesondere, wenn man nur wenig Zeit, Personal und Geld hat. Und erst recht, wenn man sich vollständig auf seine Mission konzentriert, anderen zu helfen!

Zweitens: Kommerzielle Sicherheitslösungen sind nicht auf gemeinnützige Zwecke ausgelegt. Ja, gemeinnützige Organisationen haben ähnliche Geschäftsfunktionen, doch sie haben auch Nuancen, durch die ihr Sicherheitsmanagement anders wird.

Drittens: Gemeinnützige Organisationen sind mit dem Thema Sicherheit nicht gut vertraut, und ehrlich gesagt können Sicherheitsexperten es Menschen, die nicht vom Fach sind, teilweise schwer machen, zu verstehen, wovon wir sprechen. Gemeinnützige Organisationen nehmen an Sicherheitskonferenzen teil und stellen fest, dass sie zum Gesagten keine Verbindung herstellen oder die angebotenen Lösungen nicht an ihrem Geschäft ausrichten können. Sightline dient als Brücke, Übersetzer und Fürsprecher für diese Organisationen. Wir erstellen Bewertungstools und eine Sicherheits-Community ausschließlich für gemeinnützige Organisationen.

Einfluss

Können Unternehmen effektiv Einfluss auf Anbieter, Partner und sonstige Dritte ausüben, damit sie die nötige Sicherheit bereitstellen?

Die Sicherheit einer Lieferkette aus Drittanbietern ist heute ein wichtiges Anliegen für CISOs. Wenn Services, Hardware und Software aus Dutzenden oder Hunderten verschiedenen Quellen stammen, haben die Unternehmen keine Chance, die vollständige Kontrolle über ihre Sicherheit zu übernehmen.

Und es ist nicht überraschend, dass Unternehmen mit zunehmenden Mitarbeiterzahlen und Budgets eher in der Lage sind, Anbieter und Partner zu beeinflussen, damit diese sie bei ihrer Sicherheit unterstützen. Beispielsweise erfahren 86 Prozent der Unternehmen mit über 10.000 Mitarbeitern von den betroffenen Anbietern/Partnern von Sicherheitsschwachstellen und Vorfällen, die sich auf ihren Betrieb auswirken können, noch bevor diese öffentlich bekannt werden. Dem gegenüber stehen nur 60 Prozent der Unternehmen mit weniger als 1.000 Mitarbeitern.

Darüber hinaus gaben 38 Prozent der Unternehmen, die jährlich 1 Million US-Dollar oder mehr für Sicherheit ausgeben, an, dass sie immer in der Lage waren, sicherheitsbezogene Geschäftsbedingungen zu einem Anbieter-/Partnervertrag hinzuzufügen. Dem gegenüber stehen nur 17 Prozent der Unternehmen, die jährlich weniger als 250.000 US-Dollar für Sicherheit ausgeben. Dies deutet darauf hin, dass größere Unternehmen mit höherer Kaufkraft besser in der Lage sind, mit externen Parteien zu verhandeln.

Was bleibt für kleinere Unternehmen, die vielleicht noch stärker von externen Partnern abhängig sind? „Ihre vielleicht beste Option lautet, mit ihren Kollegen zusammenzuarbeiten, um mehr Einfluss auf gemeinsame Anbieter und Lieferanten zu nehmen“, sagt Nather. „Beispielsweise machen es Branchenverbände, regionale Cybersicherheitsforen oder Zentren zum Austausch und zur Analyse von Informationen (ISACs) ihren Mitgliedern möglich, Anfragen und Antworten auf Sicherheitsprobleme zu organisieren. Diesen Einfluss zu finden oder zu schaffen, ist heute Teil der Arbeit des CISO, was die Vernetzung mit Kollegen noch wichtiger macht.“

(Cybersicherheit für gemeinnützige Organisationen, Forts.)

Können Sie einige spezielle Sicherheitsherausforderungen nennen, mit denen gemeinnützige Organisationen konfrontiert sind?

Misata: Erstens: Die Geschäftsprozesse von gemeinnützigen Organisationen sind sehr schlank. Das heißt, sie können weder Zeit noch Geld für Lösungen verschwenden, die ihre Mission nicht direkt unterstützen. Viele gemeinnützige Organisationen betrachten Cybersicherheit als kostspielig, überwältigend und unnötig, bis etwas Schlimmes passiert.

Zweitens: Viele gemeinnützige Organisationen haben noch nicht ermittelt, welche ihrer Ressourcen eventuell für Angreifer attraktiv sind. Woher sollen sie also wissen, was sie schützen müssen? Viele gemeinnützige Organisationen werden heute dazu verleitet, Geld für Lösungen auszugeben, noch bevor sie verstehen, was sie überhaupt brauchen.

Drittens: Eine der größten Herausforderungen für gemeinnützige Organisationen besteht darin, dass sich keine Person in der Organisation ausschließlich auf Sicherheit konzentriert. Obwohl sie äußerst aktiv sind und wissen, dass Sicherheit (insbesondere Cybersicherheit) wichtig ist, wird ihre Aufmerksamkeit an vielen verschiedenen Stellen benötigt.

Die gute Nachricht ist, dass die gemeinnützigen Organisationen trotz alledem zur Tat schreiten und sich nicht mehr als immun gegen einen Angriff sehen. Sie erkennen, dass sie über wertvolle Ressourcen und Daten verfügen. Doch sie haben oft nur minimalen Einfluss auf Anbieter und Service-Provider und geraten ins Hintertreffen. Durch unsere Zusammenarbeit mit den Mitgliedern von Sightline können wir jetzt Daten und Erkenntnisse über den Sicherheitsstatus bei gemeinnützigen Organisationen sammeln, um sie auf den neuesten Stand zu bringen.

Wichtigste Erkenntnisse

Insgesamt haben die Unternehmen nicht den Eindruck, dass sie sich die nötige Sicherheit leisten können, und zwar unabhängig davon, wie groß sie sind oder wie viel sie derzeit ausgeben.

Mittelgroße Unternehmen mit 1.000 bis 9.999 Mitarbeitern haben die größten Schwierigkeiten, ihre Umgebungen ausreichend zu schützen.

Es gibt keine allgemeingültige Antwort darauf, welche Sicherheitsprodukte ein Unternehmen nutzen sollte oder wie viel für Sicherheit ausgegeben werden sollte. Dies hängt weitestgehend von der Größe und Art des Unternehmens, der Bedeutung seiner Ressourcen sowie der Frage ab, was es sich tatsächlich leisten kann. Dadurch wird es den Unternehmen erschwert, herauszufinden, was in ihren Sicherheitsprogrammen enthalten sein sollte.

Höhere Sicherheitsausgaben führen nicht immer zu besseren Sicherheitsfähigkeiten. Es müssen auch andere Faktoren berücksichtigt werden, zum Beispiel Know-how und Einfluss.

Die Unternehmen müssen sicherstellen, dass ihre internen Mitarbeiter sich kontinuierlich Know-how aneignen, sowohl in Bezug auf die allgemeine Sicherheit als auch auf ihre konkrete Umgebung und ihr Risikoprofil. Es gibt einige Aspekte der Sicherheit, für die nur Insider gerüstet sind.

Fähigkeiten sind ein wichtiger Faktor für das Sicherheitsergebnis. Faktoren wie die Frage, ob ein Sicherheitsteam die Kontrolle über bestimmte Ressourcen hat, haben ggf. eine große Wirkung auf seine Fähigkeit, eine Verteidigungsstrategie umzusetzen – selbst wenn das erforderliche Budget und Know-how vorliegen.

Je größer ein Unternehmen ist, desto einfacher ist es, Drittanbieter zu beeinflussen, die sich auf seinen Sicherheitsstatus auswirken. Kleinere Unternehmen müssen sich möglicherweise auf Verbände stützen, um das gleiche Maß an Einfluss und Skaleneffekten zu erzielen.

Empfehlungen für mehr Sicherheit

Unabhängig davon, wie Ihr Unternehmen im Hinblick auf das Sicherheitsergebnis abschneidet, finden Sie hier einige Empfehlungen, um die wichtigsten in diesem Bericht behandelten Herausforderungen zu überwinden.

1. Finden Sie heraus, was für Ihr Unternehmen das Richtige ist

Unternehmen sollten sich genauer ansehen, was mit ihren Sicherheitsausgaben geschieht. In dieser Branche herrscht großer Druck, mit der Konkurrenz mitzuhalten. *„Was kaufen alle anderen? Brauche ich diese neue Technologie?“* Natürlich ist es immer gut, die Branche im Auge zu behalten und auszuwerten, was andere unternehmen, um ihre Abwehrmaßnahmen zu verbessern. Doch wie wir in diesem Bericht betont haben, gibt es keine allgemeingültige Lösung für Sicherheit.

Bevor Sie neue Technologien kaufen, betrachten Sie Ihr Know-how in Bezug auf die Reifegrad-Pyramide im Abschnitt „Fähigkeiten“. Denn Sie können nichts schützen, von dem Sie nicht wissen, dass Sie es haben. Und ein Schwachstellenscanner kann Ihnen nicht helfen, wenn Sie seine Befunde nicht beheben können.

Wenn Sie wissen, welche Bedrohungen nicht nur möglich, sondern *wahrscheinlich* sind, können Sie sich auf die richtigen Prioritäten konzentrieren, wenn Sie sich nicht mit allem befassen können. Ziehen Sie die Durchführung einer **Cyber-Risikobewertung** in Betracht, entweder intern oder über einen Drittanbieter, um auf den richtigen Weg zu gelangen.

2. Holen Sie mehr aus Ihren Investitionen heraus

Ein bedauerlicher Trend im Laufe der Jahre war es, sich immer die neuesten und besten Sicherheitsprodukte herauszusuchen. In der Theorie ist das gut, um sicherzustellen, dass Sie vor sich ständig weiterentwickelnden Bedrohungen geschützt sind. Doch bei vielen Unternehmen entstand dadurch ein komplexes Durcheinander aus isolierten Einzellösungen, die schwierig – wenn nicht gar unmöglich – zu verwalten sind. Wenn Sie zu viele Warnungen von unterschiedlichen Technologien erhalten und den ganzen Tag damit verbringen müssen, zwischen verschiedenen Anwendungen hin und her zu wechseln, um herauszufinden, was in Ihrer Umgebung geschieht, leidet Ihre Sicherheit darunter.

Investieren Sie stattdessen in Sicherheitstechnologien, die für Sie arbeiten – nicht umgekehrt. Cisco nutzt einen **plattformbasierten Sicherheitsansatz**. Das bedeutet, dass wir nicht nur Firewalls oder E-Mail-Sicherheitslösungen oder Anti-Malware-Technologie verkaufen. Wir bieten ein offenes und umfassendes Portfolio von Sicherheitstechnologien, die alle zusammenarbeiten, um Ihr Netzwerk zu schützen. Wird eine Bedrohung in einem Bereich erkannt, bieten wir Ihnen die Möglichkeit, sie in allen anderen Bereichen automatisch zu blockieren. Automatisierung und Integration können viel dazu beitragen, die Komplexität zu verringern und zu gewährleisten, dass Sie Ihre Sicherheitstechnologien und -mitarbeiter optimal einsetzen.

„Ich betrachte Sicherheit als Ökosystem. Je mehr Dinge zusammenarbeiten, desto besser. Wenn ich Zeit und Energie aufwenden muss, um selbst Technologien zu integrieren, habe ich weniger Zeit für tatsächliche Sicherheitsaufgaben.“

Steve Martino, SVP/CISO, Cisco

Und was Ihre Anbieter betrifft, sollten Sie sich alles zunutze machen, was sie anbieten – vieles davon zu geringen Kosten oder sogar kostenlos. Nehmen Sie an kostenlosen Webinaren teil. Rufen Sie den technischen Support an. Besuchen Sie die Veranstaltungen Ihrer Anbieter. Treten Sie Kundenberatungsgruppen bei. Nehmen Sie an Anbieterschulungen teil. Auf alle Fälle sollten Ihre Sicherheitsmitarbeiter wissen, wie sie die Technologie, in die Sie investiert haben, effektiv nutzen können.

3. Nutzen Sie bei Sicherheit einen Zero-Trust-Ansatz

Ihr Unternehmen wird heute von allen Seiten bedroht. Die Bedrohungen zielen auf Ihre Benutzer, Ihre Anwendungen, Ihr Netzwerk, die Cloud, IoT-Geräte usw. ab. Aufgrund dieser erweiterten Angriffsfläche ist es entscheidend, dass die Unternehmen bei Sicherheit einen **Zero-Trust-Ansatz** nutzen.

Zero Trust erfordert, dass die Unternehmen:

- Transparenz in allen Bereichen des Netzwerks gewährleisten
- Kontrollmaßnahmen ergreifen, um sicherzustellen, dass nur die richtigen Personen, Geräte und Anwendungen Zugriff auf die Umgebung des Unternehmens erhalten
- Eine effektive Möglichkeit haben, verdächtiges Verhalten zu blockieren, um die Ausbreitung von Angriffen zu verhindern

Mit diesen Maßnahmen können Unternehmen ihre Mitarbeiter, Workloads und Arbeitsplätze effektiver schützen.

Indem Sie über die grundlegenden Sicherheitsmaßnahmen hinausgehen und einen mehrschichtigen, ganzheitlichen Sicherheitsansatz verfolgen, wird es für Angreifer schwieriger und teurer, Ihre Ressourcen zu kompromittieren – was sicherlich zu Ihrem Sicherheitsergebnis beiträgt!

4. Weiten Sie Ihre Schulungen aus

Da viele unserer Befragten sich in Sachen Sicherheits-Know-how auf externe Quellen verlassen, scheinen mehr Schulungen angebracht zu sein. Gewährleisten Sie, dass Sie nach der Einstellung Ihrer Talente kontinuierlich in ihre Fähigkeiten und ihr Verständnis Ihrer Umgebung investieren.

Ermöglichen Sie ihnen die Teilnahme an Konferenzen und Workshops. Führen Sie interne Schulungen durch. Bringen Sie sie dazu, kostenlose Ressourcen wie den **Cisco Security Blog** und die **Seite von Cisco Talos Threat Intelligence** zu nutzen, um im Hinblick auf aktuelle Bedrohungen auf dem neuesten Stand zu bleiben. Lassen Sie sie mehr Zertifizierungen einholen. Kurz gesagt: Stellen Sie sicher, dass sie nicht einfach nur ihre Aufgaben erledigen, sondern dabei zu echten Experten werden – nicht nur Sicherheitsexperten, sondern auch Experten für Ihr Unternehmen. Ein Dritter wird Ihre speziellen Sicherheitsanforderungen und Einschränkungen niemals so gut verstehen wie Ihre eigenen Mitarbeiter.

5. Ziehen Sie Outsourcing in Erwägung

Wenn Sie mehrere Altsysteme betreiben, ist es wahrscheinlich, dass Ihr IT-Team zu viel Zeit damit verbringt, diese zu verwalten und zu aktualisieren. Darunter leidet die Effektivität Ihrer Sicherheit. Die Migration von komplexen Legacy-Systemen zu ausgelagerten SaaS-Anwendungen für bekannte Funktionen außerhalb Ihres Kerngeschäfts, zum Beispiel E-Mail, Office-Anwendungen oder Lohnbuchhaltung, kann die Sicherheit in diesen Bereichen erheblich verbessern, sodass Sie sich darauf konzentrieren können, Ihre wichtigsten Ressourcen und Prozesse zu schützen.

Für Sicherheitsprodukte, die mehr dedizierte Mitarbeiter erfordern, als Ihnen (kostenbedingt) zur Verfügung stehen, ist das Outsourcing der Verwaltung dieser Technologien über einen MSSP ebenfalls eine Option. Erkennen Sie, dass es manchmal am besten – und am kostenwirksamsten – ist, für Ihre Sicherheit Unterstützung einzuholen, statt zu versuchen, alles selbst zu erledigen.

6. Bündeln Sie Ihre Kräfte

Wie der Abschnitt „Einfluss“ zeigt, ist Zusammenarbeit beim Thema Sicherheit oft hilfreich. Wenn Ihr Unternehmen zu klein ist, um Einfluss auf Ihre Lieferanten auszuüben, denken Sie darüber nach, sich über professionelle Netzwerke oder Branchengruppen mit anderen Unternehmen zusammenzutun, um mehr Einfluss zu gewinnen. Die Möglichkeit, rechtzeitig Fehlerbehebungen und Updates von Ihren Anbietern und Partnern zu erhalten, ist für eine effektive Sicherheit entscheidend. Und zu 50 kleinen Unternehmen können sie nicht so leicht Nein sagen wie zu einem einzigen.

Auf cisco.com/go/security erfahren Sie, wie wir Ihnen helfen können, IHRE Umgebung zu schützen.

Methodik

Unsere Daten in diesem Bericht basieren auf einer Online-Doppelblindstudie unter etwa 80 IT-Entscheidungsträgern in den USA, die zu Sicherheitsbudgets und -planung befragt wurden. Bei den Befragten handelt es sich um Vollzeitmitarbeiter in mittelständischen Unternehmen (250–999 Mitarbeiter), größeren Unternehmen (1.000–9.999 Mitarbeiter) und Großkonzernen (über 10.000 Mitarbeiter), die in einer gewinnorientierten, behördlichen oder Hochschulorganisation mit formeller IT-Abteilung beschäftigt sind. Sie sind gut über Sicherheitsrichtlinien und -verfahren informiert, beteiligen sich an der Erarbeitung einer Sicherheitsstrategie und verbringen mindestens 40 Prozent ihrer Arbeitszeit mit Sicherheit.

Über die Cisco Reihe zur Cybersicherheit

Im vergangenen Jahrzehnt hat Cisco eine Fülle an maßgeblichen Sicherheits- und Bedrohungsinformationen für Sicherheitsexperten veröffentlicht, die sich für den aktuellen Stand der globalen Cybersicherheit interessieren. Diese umfassenden Berichte enthielten detaillierte Beschreibungen von Bedrohungslandschaften und ihren organisatorischen Auswirkungen sowie Best Practices zum Schutz vor den negativen Folgen von Datensicherheitsverletzungen.

In seinem neuen Ansatz für seine Vordenkerposition veröffentlicht Cisco Security eine Reihe von forschungsbasierten, datengesteuerten Publikationen unter folgendem Namen: Cisco Reihe zur Cybersicherheit. Wir haben die Anzahl der Titel um unterschiedliche Berichte für Sicherheitsexperten mit verschiedenen Interessenbereichen erweitert, darunter die Data Privacy Benchmark Study, Threat Report, CISO Benchmark Study und vieles mehr.

Weitere Informationen und Zugriff auf alle Berichte und archivierte Kopien finden Sie unter www.cisco.com/go/securityreports.

Hauptgeschäftsstelle Nord- und Südamerika
Cisco Systems, Inc.
San Jose, CA

Hauptgeschäftsstelle Asien/Pazifik
Cisco Systems (USA) Pte.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV Amsterdam,
Niederlande

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen mit Telefon- und Faxnummern finden Sie auf der Cisco Website unter **www.cisco.com/go/offices**.

Veröffentlicht im Oktober 2019 BTTM_01_1019

© 2019 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten.

Cisco und das Cisco Logo sind Marken oder eingetragene Marken von Cisco und/oder Partnerunternehmen in den Vereinigten Staaten und anderen Ländern. Eine Liste der Cisco Marken finden Sie unter **www.cisco.com/go/trademarks**. Die genannten Marken anderer Anbieter sind Eigentum der jeweiligen Inhaber. Die Verwendung des Begriffs „Partner“ impliziert keine gesellschaftsrechtliche Beziehung zwischen Cisco und anderen Unternehmen. (1110R)