CISCO
SECURE

Security Outcomes-Studie

Teil 2

Optimale Umsetzung der fünf wichtigsten Sicherheitspraktiken

Inhalt

Die „großen Fünf“

Mit der Cisco Security Outcomes-Studie 2021 wollten wir messen, was beim Cybersicherheitsmanagement am wichtigsten ist. Zu diesem Zweck haben wir 25 allgemeine Sicherheitspraktiken untersucht und überprüft, wie jede davon mit der Erreichung von 11 Ergebnissen auf Programmebene korreliert. Sie können diese Korrelationen bei Praxisergebnissen über eine interaktive Visualisierung auf der Website der Cisco Security Outcomes-Studie 2021 anzeigen oder den vollständigen Bericht herunterladen.

Bei den Tests haben wir festgestellt, dass sich fünf der 25 Verfahren in Bezug auf den Gesamtbeitrag zum Erfolg des Sicherheitsprogramms bei allen gemessenen Ergebnissen von den anderen abheben.

Auf den folgenden Seiten konzentrieren wir uns auf diese „großen Fünf“ Faktoren für den Erfolg von Sicherheitsprogrammen, um Strategien zur Maximierung ihrer Effektivität zu identifizieren. Die „großen Fünf“ sind:

Proaktive Technologie-aktualisierung	Das Unternehmen verfügt über eine Strategie zur proaktiven technischen Modernisierung, um mit den besten verfügbaren IT- und Sicherheitstechnologien auf dem neuesten Stand zu bleiben.
Gut integrierte Technologie	Sicherheitstechnologien sind gut integriert und arbeiten effizient zusammen.
Rechtzeitige Incident Response	Incident Response-Funktionen ermöglichen eine zeitnahe und effektive Untersuchung und Behebung von Sicherheitsereignissen.
Genaue Bedrohungs-erkennung	Bedrohungserkennungsfunktionen ermöglichen eine präzise Erkennung potenzieller Sicherheitsereignisse ohne signifikante „blinde Flecken“.
Schnelle Disaster Recovery	Wiederherstellungsfunktionen minimieren die Auswirkungen von Angriffen und gewährleisten die Ausfallsicherheit von Geschäftsfunktionen, die von Sicherheitsvorfällen betroffen sind.

Die breite Wirksamkeit dieser Praktiken wirft die Frage auf: „Warum?“ Was macht sie so entscheidend für den Erfolg? Welche Faktoren machen sie mehr oder weniger effektiv? Wie sollten Unternehmen diese Praktiken implementieren, um die Ergebnisse zu maximieren? Das sind die Fragen, die wir in dieser Iteration der Security Outcomes-Studie untersuchen möchten.

Auf den folgenden Seiten konzentrieren wir uns auf diese „großen Fünf“ Faktoren für den Erfolg von Sicherheitsprogrammen, um Strategien zur Maximierung ihrer Effektivität zu identifizieren. Dazu haben wir eine unabhängige Doppelblindstudie unter mehr als 5.100 IT- und Sicherheitsexpert:innen weltweit durchgeführt. Wir analysieren die Daten, extrahieren wichtige Erkenntnisse und teilen bewährte Erkenntnisse, um Ihrem Unternehmen neue Höchstleistungen zu ermöglichen.

Wichtigste Ergebnisse

Wir haben über 5.100 IT- und Sicherheitsfachleute in 27 Ländern zu den Ansätzen ihrer Unternehmen befragt, die Sicherheitsarchitektur zu modernisieren und zu integrieren, Bedrohungen zu erkennen und darauf zu reagieren und im Katastrophenfall widerstandsfähig zu bleiben. Die Befragten haben von unterschiedlichsten Einblicken, Schwierigkeiten, Strategien und Erfolgen berichtet. Wir haben jede Antwort auf vielerlei Art analysiert, die wichtigsten Ergebnisse extrahiert und im Folgenden aufgeführt.

Modernisierung und Integration der Architektur

- Moderne, gut integrierte IT trägt mehr zum Gesamterfolg des Programms bei als jede andere Sicherheitspraxis oder -kontrolle.
- Neuere, Cloud-basierte Architekturen lassen sich viel einfacher regelmäßig aktualisieren, um mit dem Unternehmen Schritt zu halten.
- Unternehmen, die hauptsächlich von einem einzigen Anbieter beziehen, verdoppeln ihre Chancen, einen integrierten Technologie-Stack aufzubauen.
- Integrierte Security-Technologien führen mit siebenmal höherer Wahrscheinlichkeit zu einem hohen Maß an Prozessautomatisierung.

Erkennung von und Reaktion auf Cyberbedrohungen

- SecOps-Programme, die auf starken Mitarbeiter:innen, Prozessen und Technologien basieren, erzielen eine 3,5-fach höhere Leistung als Programme mit schwächeren Ressourcen.
- Ausgelagerte Erkennungs- und Reaktionsteams werden als überlegen empfunden, aber interne Teams erzielen eine schnellere mittlere Reaktionszeit (6 Tage vs. 13 Tage).
- Teams, die Threat-Intelligence intensiv nutzen, melden mit doppelt so hoher Wahrscheinlichkeit starke Erkennungs- und Reaktionsfähigkeiten.
- Durch Automatisierung lässt die Leistung von weniger erfahrenen Mitarbeiter:innen mehr als verdoppeln, und starke Teams erzielen fast sicher (95 %) SecOps-Erfolge.

Bleiben Sie bei einem Notfall widerstandsfähig

- In Unternehmen, die Business Continuity und Disaster Recovery auf Vorstandsebene überwachen, ist die Wahrscheinlichkeit am höchsten (11 % über dem Durchschnitt), dass starke Programme vorhanden sind.
- Die Wahrscheinlichkeit, die Business Resiliency aufrechtzuerhalten, steigt erst dann, wenn die Business-Continuity- und Disaster-Recovery-Funktionen mindestens 80 % der kritischen Systeme abdecken.
- Unternehmen, die ihre Funktionen für Business Continuity und Disaster Recovery regelmäßig auf verschiedene Arten testen, haben eine 2,5-mal höhere Wahrscheinlichkeit, die Business Resiliency aufrechtzuerhalten.
- Unternehmen, die Chaos Engineering zum Standard machen, erreichen mit doppelt so hoher Wahrscheinlichkeit eine hohe Widerstandsfähigkeit.

Über die Befragung

Sampling	Teilnehmer:innen	Analyse
Cisco hat das Umfrageforschungsunternehmen YouGov Mitte 2021 beauftragt, eine vollständig anonyme Umfrage unter Verwendung einer geschichteten Zufallsstichprobe durchzuführen.	5.123 aktive IT-, Sicherheits- und Datenschutzfachleute aus 27 Ländern haben geantwortet. Demografische Daten finden Sie im Anhang.	Das Cyentia Institute hat die Umfragedaten für Cisco unabhängig analysiert und alle in dieser Studie dargestellten Ergebnisse generiert.

5.123 aktive IT-, Sicherheits- und Datenschutzfachleute aus **27** Ländern haben geantwortet

„Wir müssen uns sicher sein, dass wir alles in unserer Macht Stehende tun, um die Sicherheit zu gewährleisten. Wir wissen, wie fortschrittlich die Angreifer sind. Sie entwickeln sich weiter und verfügen jeden Tag über neue Techniken. Wir möchten unsere Geräte, unsere Benutzer und unser Unternehmen schützen. Deshalb möchten wir die Angriffsfläche für mögliche Sicherheitsverletzungen verkleinern.“

– Eric J. Mandela, Assistant Director
of Technology Infrastructure bei der Allied Beverage Group

Weiterlesen

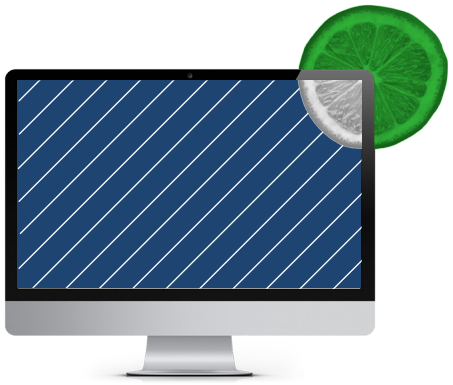
Strategien für proaktive technische Modernisierung

Unsere vorherige Studie ergab, dass ein proaktiver Ansatz zur Modernisierung und Wartung erstklassiger IT- und Sicherheitstechnologien mehr zu einem erfolgreichen Cybersicherheitsprogramm beiträgt als jede andere Maßnahme. Das ist insofern bemerkenswert, als alle 25 von uns getesteten Verfahren weithin als „Best Practices“ gelten. Deshalb wollten wir in dieser Folgestudie untersuchen, was diese Praxis so effektiv macht.

Um tiefer in die Strategien zur technischen Modernisierung einzutauchen, testen wir zunächst kurz die Aktualität der vorhandenen Infrastruktur. Wir haben die Teilnehmer:innen gefragt, welcher Anteil ihrer aktiven Sicherheitstechnologien veraltet ist. Im Durchschnitt gelten 39 % der von Unternehmen verwendeten Sicherheitstechnologien als veraltet. Fast 13 % der Befragten geben an, dass mindestens 80 % der von ihnen verwendeten Sicherheitstools Alterserscheinungen zeigen.

Diese Tatsache allein kann viele der Vorteile erklären, die eine proaktive Strategie zur technischen Modernisierung mit sich bringt. Neuere Technologien bieten angeblich erweiterte Funktionen gegen eine immer weiter wachsende Horde von Cyberbedrohungen. Aber das ist noch nicht alles. Sehen wir uns also die Fragen an, die wir anhand der Daten beantworten wollten.

Im Durchschnitt gelten 39 % der von Unternehmen verwendeten Sicherheitstechnologien als veraltet.



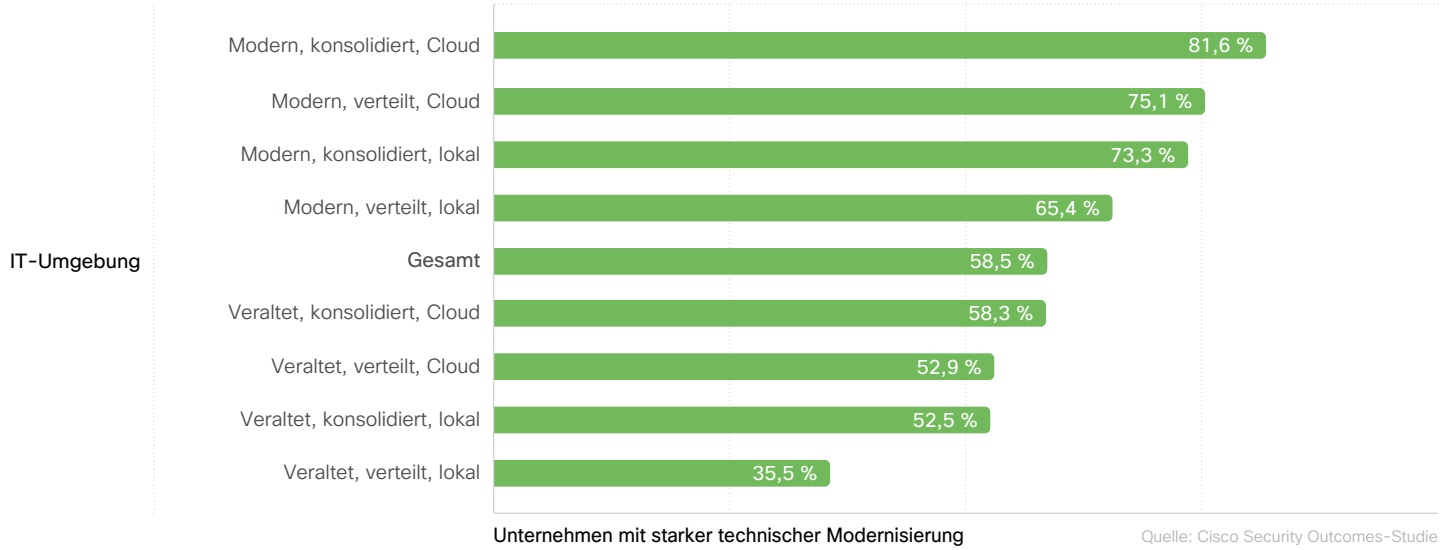
Haben Infrastrukturmerkmale Auswirkungen auf Modernisierungsinitiativen?

In der ursprünglichen Studie spekulierten wir, dass modernere, Cloud-basierte Architekturen effektiver sein könnten, weil sie einfacher zu verwalten sind und native Sicherheitsmaßnahmen integriert haben. Als Schritt zum Testen dieser Hypothese haben wir die Teilnehmer:innen gebeten, ihre Technologieinfrastruktur anhand einer Reihe skalierter Deskriptoren allgemein zu beschreiben, darunter:

- Cloud vs. lokal
- Modern vs. veraltet
- Konsolidiert vs. verteilt

Tragen diese unterschiedlichen Architekturmerkmale zur Wirksamkeit von Funktionen zur technischen Modernisierung bei? Sehr sogar, wie Abbildung 1 zeigt. **Bei Unternehmen mit modernen, konsolidierten, Cloud-basierten Architekturen ist die Wahrscheinlichkeit, dass sie über leistungsstarke Funktionen zur technischen Modernisierung verfügen, mehr als doppelt so hoch wie bei Unternehmen, die veraltete, verteilte, lokale Technologien verwenden.** Bevor Sie das Diagramm im nächsten Meeting zur Cloud-Migrationsstrategie präsentieren, sollten Sie jedoch beachten, dass Unternehmen mit überwiegend lokalen Umgebungen nach wie vor eine deutlich überdurchschnittliche Leistung zeigen, sofern sie ihre IT modernisiert haben.

Ein Cloud-nativer Ansatz macht es natürlich einfacher, Ihre Strategie zur technischen Modernisierung erfolgreich umzusetzen. Veraltete Infrastruktur ist dabei jedoch das drängendere Problem. Wenn es schwierig wird, ältere Infrastrukturen auf dem neuesten Stand zu halten, können Sie die Migration zu einer neuen Architektur vorantreiben, anstatt die alte fortwährend aufzurüsten. Das ist bei lange Jahre genutzten oder kritischen Infrastrukturen natürlich nicht immer möglich oder kostengünstig, aber das allgemeine Prinzip gilt weiterhin.



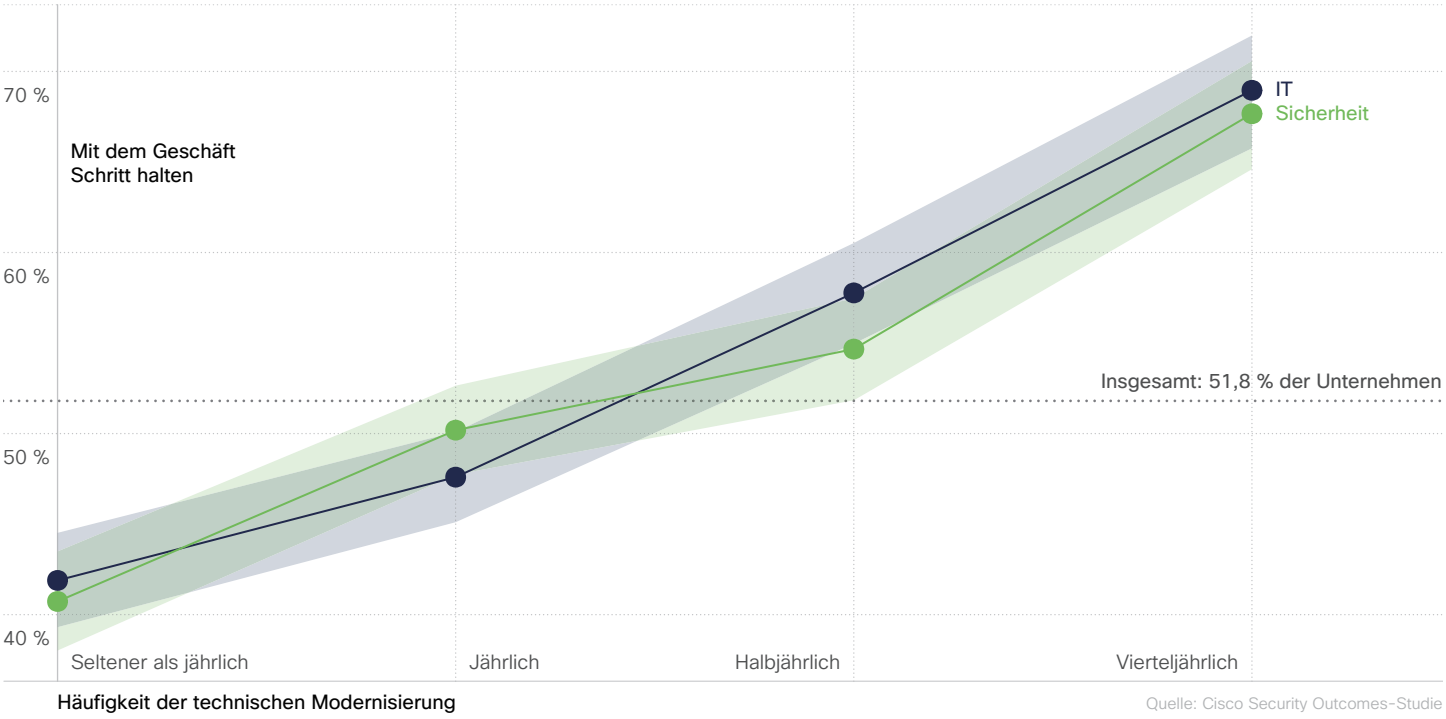
Quelle: Cisco Security Outcomes-Studie

Abbildung 1: Auswirkung der Merkmale der IT-Architektur auf die Leistung der technischen Modernisierung

81,6 % der Unternehmen mit modernen, konsolidierten, Cloud-basierten Architekturen berichten von leistungsstarken Technologieaktualisierungsfunktionen

Tragen häufige Upgrades dazu bei, dass die Sicherheit mit dem Geschäft Schritt hält?

Laut der Security Outcomes-Studie 2021 war das Ergebnis, das am stärksten mit einer Strategie zur proaktiven technischen Modernisierung korrelierte, die Fähigkeit des Sicherheitsprogramms, mit den Anforderungen und dem Wachstum des Unternehmens Schritt zu halten. Tatsächlich war dies die stärkste Korrelation von Maßnahme und Ergebnis in der gesamten Studie.



Quelle: Cisco Security Outcomes-Studie

Abbildung 2: Auswirkung der Häufigkeit der technischen Modernisierungen auf die Fähigkeit des Sicherheitsprogramms, mit dem Geschäft Schritt zu halten[1]

Wir haben Unternehmen nach der Häufigkeit ihrer IT- und Sicherheits-Upgrades befragt und diese Antworten mit der Fähigkeit ihres Sicherheitsprogramms verglichen, mit dem Unternehmen Schritt zu halten. Besteht ein Zusammenhang zwischen diesen beiden Variablen? Ja, tatsächlich. Wir konnten bei diesem wichtigen Ergebnis eine stetige Verbesserung feststellen, wenn die Zahl der Upgrades anstieg. **Insgesamt ist bei Unternehmen, die vierteljährlich IT- und Sicherheitstechnologien aktualisieren, die Wahrscheinlichkeit, dass sie mit dem Geschäft Schritt halten, um 30 % höher als bei Unternehmen, die nur alle paar Jahre ein Upgrade durchführen.** Klingt nach einer guten Motivation für gestresste IT-Teams: auf dem Laufenden bleiben und immer weitermachen.

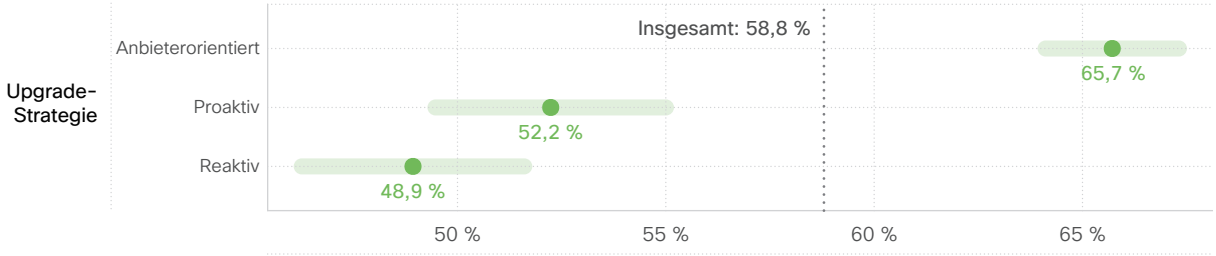
[1] Im gesamten Bericht werden die Zahlen mit dem „Gesamtwert" für eine bestimmte Maßnahme oder ein bestimmtes Ergebnis gekennzeichnet. Dieser Wert stellt den Durchschnittswert aller Befragten dar, die diese bestimmte Reihe von Fragen beantwortet haben. Er wird als Referenz angegeben und soll Ihnen helfen, zu verstehen, wer überdurchschnittliche Ergebnisse erzielt und wer nicht auf der Höhe der Zeit ist. Unsicherheit wird in einigen Diagrammen durch Fehlerbalken oder schattierte Bereiche dargestellt. Wenn sich diese Bereiche mit der Gesamtlinie überschneiden, können wir nicht ableiten, dass ein bestimmter Aspekt eines Sicherheitsprogramms Auswirkungen auf das Ergebnis oder die Maßnahme hat, das bzw. die wir untersuchen.

Was (oder wer) sollte Bemühungen zur technischen Modernisierung fördern?

Wir haben festgestellt, dass häufige Upgrades zur Förderung des Geschäfts beitragen. Aber was – oder wer – sollte den Prozess zur Durchführung dieser Upgrades vorantreiben? Wir haben die Teilnehmer:innen gebeten, die wichtigsten Faktoren ihres Unternehmens für die Modernisierung von Sicherheitstechnologien auszuwählen. Ihre Antworten lassen sich in drei große Kategorien einteilen:

- **Anbieterorientiert:** Der Zeitplan wird von einem SaaS-Anbieter festgelegt oder ist Teil einer größeren Anbieterkonsolidierungsinitiative (häufigster Faktor)
- **Proaktiv:** nach einem vorher festgelegten Zeitplan oder wenn neue Funktionen oder Anwendungsfälle ein Upgrade erfordern (zweithäufigster Faktor)
- **Reaktiv:** Reaktion auf einen Vorfall, wenn Technologie veraltet ist, oder um Compliance-Anforderungen zu erfüllen (seltenster Faktor)

Diese Faktoren sind an und für sich interessant, aber wir möchten wirklich wissen, ob diese Motive mit einem stärkeren Ansatz zur technischen Modernisierung korrelieren. Die Antwort ist in Abbildung 3 zu finden, die im Wesentlichen besagt, dass Initiativen zur technischen Modernisierung erfolgreicher sind, wenn Anbieter sie handhaben (oder zumindest aktiv daran beteiligt sind). **Weniger als die Hälfte der Unternehmen mit einem reaktiven Ansatz gibt an, dass sie über starke Aktualisierungsfunktionen verfügen, verglichen mit fast zwei Dritteln derer, die ihre Updates mit den Aktualisierungszyklen des Anbieters synchronisieren.**



Quelle: Cisco Security Outcomes-Studie

Abbildung 3: Auswirkung der primären Treiber für Upgrades auf die Leistung bei der Modernisierung von Sicherheitstechnologien

Wir verstehen schon – das alles klingt wirklich verdächtig, wenn es von einem Anbieter von IT- und Sicherheitsprodukten kommt. Aber wir hatten tatsächlich keinen Einfluss auf diese Erkenntnis. Die Umfrage wurde von einem renommierten unabhängigen Forschungsunternehmen durchgeführt. Die Befragten wussten nicht, dass Cisco die Umfrage gesponsert hat, und das angesehene Cyentia Institute hat die Daten analysiert, um das abzuleiten, was Sie in Abbildung 3 sehen. Außerdem werden wir bei der Interpretation dieser Ergebnisse besonders vorsichtig sein.

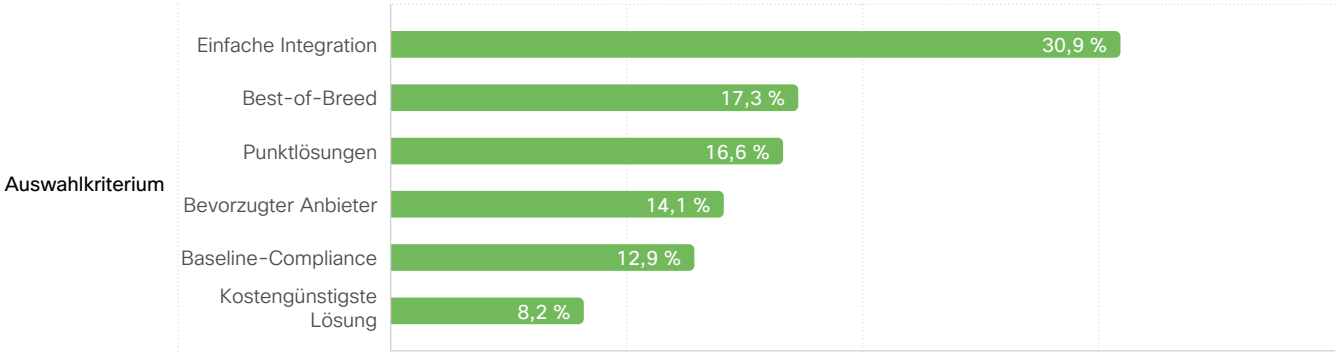
Wir vermuten, dass ein Großteil der Verbesserungen, die anbieterorientierten Ansätzen zugeschrieben werden, darauf zurückzuführen sind, dass Cloud-/SaaS-Architekturen besser mit häufigen Updates zurechtkommen. Wir werden außerdem feststellen, dass es hier weniger darum geht, dass Anbieter großartig sind, sondern vielmehr darum, die internen Schwierigkeiten und politischen Hindernisse zu überwinden, die die Zeitpläne für technische Modernisierung behindern.

Um es mit den Worten von Rob Base und DJ EZ Rock zu sagen: „It takes two to make a thing go right. It takes two to make it outta sight." Wer hätte gedacht, dass die beiden Sicherheitsarchitekten waren? Machen Sie Ihre Modernisierungsstrategie „outta sight" – lassen Sie sie also unsichtbar im Hintergrund ablaufen –, indem Sie die Trägheit Ihrer Technologielösungspartner nutzen, um Ihre Geschäftsergebnisse zu verbessern.

65,7 % der Unternehmen, die Ihre Updates mit den Aktualisierungszyklen von Anbietern synchronisieren, geben an, dass sie über starke Technologieaktualisierungsfunktionen verfügen.

Führen Sie Upgrades wegen neuer Funktionen oder verbesserter Kompatibilität durch?

Im vorherigen Abschnitt ging es darum, welche Szenarien Unternehmen zur Modernisierung von Technologie veranlassen. Jetzt sehen wir uns an, warum sie eine Lösung gegenüber einer anderen bevorzugen. Abbildung 4 zeigt, was uns die Befragten über ihre Auswahlkriterien mitgeteilt haben. Eine gute Integration in vorhandene Technologie ist die klare Präferenz, gefolgt von Lösungen, die erstklassige Funktionen bieten oder bestimmte Anforderungen erfüllen. Vielleicht überraschend ist, dass die Minimierung der Kosten an letzter Stelle steht.



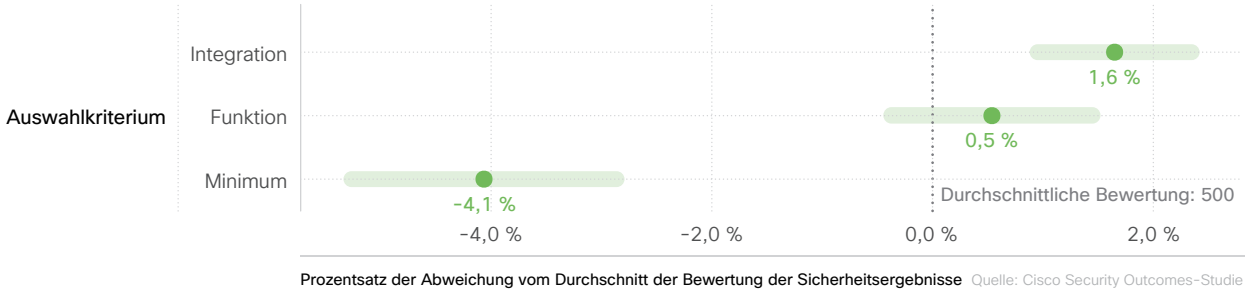
Quelle: Cisco Security Outcomes-Studie

Abbildung 4: Primäre Auswahlkriterien bei der Aktualisierung von Sicherheitsprodukten

Das ist alles ganz toll, aber hat es überhaupt mit dem Aufbau eines erfolgreichen Sicherheitsprogramms zu tun? Um diese Frage zu beantworten, haben wir die Auswahlkriterien aus Abbildung 4 in drei Kategorien eingeteilt:

- **Minimum:** kostengünstigste Lösung, Baseline-Compliance
- **Einfache Integration:** Integration mit vorhandener Technologie, Verwendung bevorzugter Anbieter
- **Fähigkeit**: Best-of-Breed; Punktlösungen

Anschließend haben wir diese Kategorien anhand einer aggregierten Bewertung getestet, die für jedes Unternehmen basierend auf ihrem Leistungsniveau in den 11 Sicherheitsergebnissen erstellt wurde. Der absolute Wert der Bewertung hat keine besondere Bedeutung, bietet aber einen Vergleichspunkt für die verschiedenen Strategien zu technischen Modernisierung. **Wie in Abbildung 5 dargestellt, verbessert die Priorisierung von Integration und Funktionen die Ergebnisse stärker als die Auswahl von Produkten auf Grundlage der Kostenminimierung oder der Erfüllung grundlegender Compliance-Anforderungen. Aber ein integrationsorientierter Ansatz ist der einzige, der den Durchschnitt deutlich übertrifft.**



Quelle: Cisco Security Outcomes-Studie

Abbildung 5: Auswirkung des Technologie-Auswahlkriteriums auf die Gesamtbewertung der Sicherheitsergebnisse

Beachten Sie, dass die Unterschiede hier in Bezug auf den Gesamterfolg des Programms ziemlich gering sind. Und wahrscheinlich erhalten wir hier tatsächlich einen Einblick in die umfassenderen Prioritäten und Praktiken des Sicherheitsprogramms. Dies deutet jedoch darauf hin, dass es sich lohnt, auch über weniger zentrale Fragen nachzudenken, z. B. warum wir ein Produkt einem anderen vorziehen. Und wenn Sie bei der Modernisierung oder Aktualisierung von Sicherheitslösungen Schwierigkeiten haben, Funktionen einzustufen, sollten Sie dies als vernünftige Rechtfertigung dafür betrachten, Kompatibilität und Funktionalität zu optimieren, anstatt nur Kosten zu senken.

Was bedeutet die Bewertung der Sicherheits-ergebnisse?

Wir haben die Teilnehmer:innen nach dem Erfolg ihres Unternehmens bei 12 verschiedenen Ergebnissen ihres Sicherheitsprogramms gefragt. In der ersten Ausgabe der Security Outcomes-Studie wurden diese im Detail analysiert, und einige davon haben wir auch in dieser Studie einzeln untersucht. Aber wir wollten auch eine aggregierte Bewertung erstellen, die den Leistungsstand jedes Unternehmens über alle 12 Ergebnisse erfasst und als Maß für die allgemeine Leistung des Sicherheitsprogramms dient. Wir nennen dies die „Bewertung der Sicherheitsergebnisse“ und werden den Begriff in diesem Bericht immer wieder verwenden.

Um die Bewertung zu erhalten, haben wir eine ausgeklügelte Statistik-Technik verwendet: die probabilistische Testtheorie. Mit dieser Technik können wir Unternehmen basierend auf ihrer Leistung in Bezug auf alle Ergebnisse bewerten und gleichzeitig berücksichtigen, dass einige Ergebnisse schwieriger zu erreichen sind als andere. Mit dieser bewährten Technik werden standardisierte Testergebnisse erstellt. Der absolute Wert der Bewertung hat keine besondere Bedeutung, bietet aber einen Vergleichspunkt zwischen den Programmen.

„CISOs müssen sowohl Influencer als auch Ausbilder sein. Wenn wir so effektiv wie möglich sein möchten, müssen wir bei den strategischen Entscheidungen, die in unseren Unternehmen getroffen werden, führend sein. Wir versuchen, die Leute davon zu überzeugen, dass Sicherheit wichtig ist, dass wir die richtigen Investitionen brauchen, um gut darin zu sein, und dass wir in jeden Aspekt des Unternehmens einbezogen werden sollten. Gleichzeitig müssen wir aber auch Wissen vermitteln. Die meisten Führungskräfte haben keinen Hintergrund im Bereich Sicherheit, deshalb müssen wir sie bei jedem Schritt über die Arten von Risiken informieren, die jede Entscheidung, die wir treffen, mit sich bringt.“

Helen Patton, Advisory CISO, Cisco @CisoHelen

Erfahren Sie in dieser spannenden Episode unseres Security Stories-Podcasts, wie Helen die Rolle des CISO weiterentwickelt

Gut integrierte Sicherheitstechnologien

Laut unserer letzten Security Outcomes-Studie tragen gut integrierte Sicherheitstechnologien, die effektiv mit einer breiteren IT-Infrastruktur zusammenarbeiten, zur Erfolgswahrscheinlichkeit aller Programmergebnisse bei. Wir haben eine Reihe von Fragen gestellt, um die Faktoren hinter dieser lobenswerten Leistung genauer zu untersuchen, angefangen bei den Absichten hinter sicherheitstechnischen Integrationen.

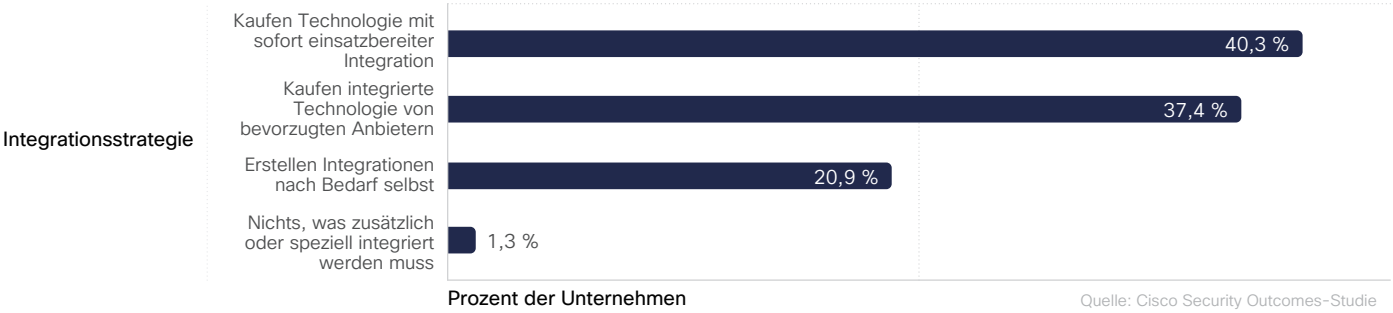
Den Befragten zufolge ist das häufigste Motiv für die Integration von Sicherheitstechnologien die Verbesserung der Effizienz von Überwachung und Audits. Damit können auch wir uns gut identifizieren, da wir mit der Mühe und Frustration vertraut sind, zahlreiche Konsolen oder Dashboards überprüfen zu müssen, um einen Eindruck von den Vorgängen im Netzwerk zu erhalten. Eine einfachere Zusammenarbeit und Automatisierung waren auch häufige Faktoren für die Integration von Sicherheitstechnologien (mehr dazu gleich). Wir haben diese Motivationen gegen die gemeldeten Stufen der technischen Integration und die Programmergebnisse getestet, aber die Korrelation war nicht so stark. Vielleicht ist das „Was“ oder „Wie“ bei der Integration von Sicherheitstechnologien wichtiger als das „Warum“? Mit den folgenden Fragen möchten wir uns noch etwas stärker auf diesen Aspekt konzentrieren.

Den Befragten zufolge ist das häufigste Motiv für die Integration von Sicherheitstechnologien die Verbesserung der Effizienz von Überwachung und Audits.

Gut integrierte Technologie kaufen oder selbst entwickeln?

Wir wissen aus der vorherigen Studie, dass die Integration von Sicherheitstechnologien zu Ergebnissen führt. Aber wie lässt sich am besten ein hochgradig integriertes Technologie-Stack erreichen? Fertig kaufen? Auf Ihre Anforderungen zuschneiden? Gleich ganz sein lassen? Lassen Sie uns sehen, ob wir das herausfinden können.

Wir haben Unternehmen nach ihrem typischen Ansatz für die Integration von Sicherheitstechnologien gefragt. Die Antworten sind in Abbildung 6 dargestellt. **Insgesamt würden mehr als drei Viertel der Unternehmen integrierte Lösungen lieber kaufen als selbst entwickeln.** Von diesen Unternehmen entscheiden sich über 40 % für Technologien, die ohne weitere Anpassung in ihre bestehende Infrastruktur integrierbar sind. Und mehr als 37 % gehen noch einen Schritt weiter und ziehen es vor, Lösungen von einem einzigen Anbieter zu beziehen, damit sie nativ gut integriert oder Teil einer größeren Plattform sind. Etwas mehr als 20 % sind bereit, Integrationen selbst zu entwickeln, sofern das Produkt ihren Anforderungen entspricht. Nur wenige verfolgen einen Laissez-faire-Ansatz.



Quelle: Cisco Security Outcomes-Studie

Abbildung 6: Gängige Ansätze zur Integration von Sicherheitstechnologien in allen Unternehmen

Insgesamt würden mehr als **3/4** der Unternehmen integrierte Lösungen lieber kaufen als selbst entwickeln.

Abbildung 7 untersucht, ob einer dieser Integrationsansätze einen Unterschied macht. Auch hier zeigen sich die Vorteile der Zusammenarbeit mit Anbietern, damit die Technologie stets modern und gut integriert ist. **Wie im Diagramm zu sehen, ist die Wahrscheinlichkeit, dass gut integrierte Sicherheitstechnologien erreicht werden, bei dauerhafter Zusammenarbeit mit einem bevorzugten Anbieter mehr als doppelt so hoch wie bei einem eigenständigen Ansatz (~ 69 % vs. ~ 31 %).** Darüber hinaus bleibt diese Erkenntnis unserer Studie zufolge über alle Unternehmensgrößen hinweg konsistent, obwohl die Vorteile der Verwendung eines bevorzugten Anbieters für kleine und mittelständische Unternehmen etwas größer sind als für große.

Und ja, wir wissen, dass dies ein weiteres verdächtig passendes Ergebnis ist, wenn es von einem Unternehmen mit einem umfangreichen, integrierten Sicherheitsportfolio stammt. Sicher, wir freuen uns, dass dieses Ergebnis die Strategie von Cisco unterstützt … aber denken Sie daran, dass dies eine Doppelblindstudie war und wir die Ergebnisse in keiner Weise manipuliert haben.

Es überrascht nicht, dass Unternehmen, die keine zusätzlichen Schritte zur Integration von Sicherheitstechnologien unternommen haben, zu einer sich selbst erfüllenden Prophezeiung wurden. **Aber natürlich gehen wir davon aus, dass manche überrascht sein werden, dass es praktisch keinen Unterschied zwischen denjenigen gibt, die Produkte mit vorgefertigten Integrationen kaufen, und denjenigen, die selbst für die Integration sorgen.** Jeweils knapp die Hälfte (~ 49 %) der Unternehmen, die einen dieser Ansätze nutzen, gibt ein hohes Integrationsniveau an.

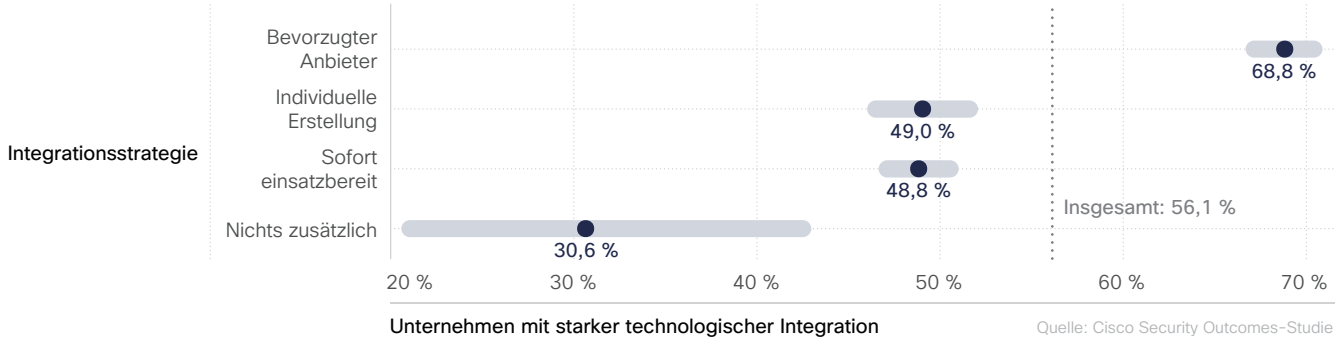


Abbildung 7: Auswirkung gängiger Integrationsansätze auf das Niveau der Integration von Sicherheitstechnologie

Wolkig mit Aussicht auf Integration

Wir haben von vielen Unternehmen gehört, die mit der Entscheidung hadern, ob sie ihre Integration von Sicherheitstechnologien in der Cloud oder in lokalen Umgebungen beginnen (oder erweitern) sollten. Wenn Ihnen das ähnlich geht, haben wir einige Daten, die Sie bei dieser Bewertung unterstützen könnten. Die gute Nachricht ist, dass viele der Befragten von guten Ergebnissen sowohl in lokalen als auch in Cloud-Umgebungen berichten. Allerdings scheint es in der Cloud deutlich einfacher zu sein, eine starke Technologieintegration zu erreichen.

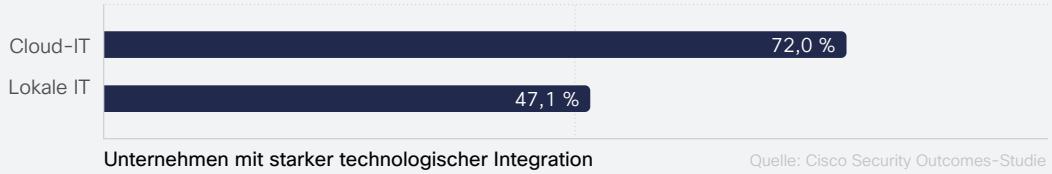


Abbildung 8: Auswirkungen von Cloud- und lokalen Umgebungen auf das Niveau der Integration von Sicherheitstechnologie

Hilft die Integration bei der Automatisierung?

Wie bereits erwähnt, ist Automatisierung nicht die häufigste Motivation für eine Technologieintegration. Aber 44 % der Unternehmen haben sie als Anreiz identifiziert. Abgesehen von der Motivation: Gibt es Belege dafür, dass gut integrierte Technologien tatsächlich eine bessere Automatisierung von Sicherheitsprozessen ermöglichen? Die in Abbildung 9 dargestellten Indizien deuten darauf hin, dass dies tatsächlich der Fall ist.

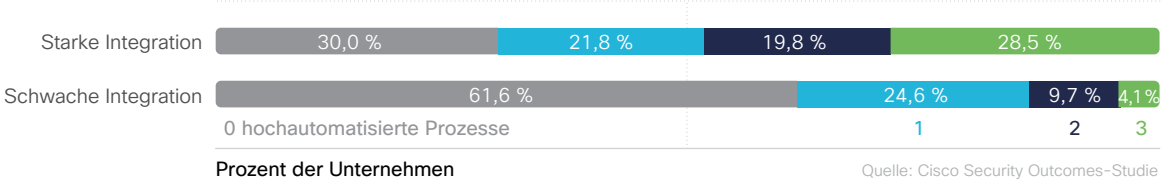


Abbildung 9: Auswirkungen der technischen Integration auf den Umfang der Automatisierung von Sicherheitsprozessen

Die beiden horizontalen Balken in Abbildung 9 unterscheiden Unternehmen nach ihrem Grad der Integration von Sicherheitstechnologie (stark vs. schwach). Die Farbsegmente stellen die Anzahl der wichtigsten Sicherheitsprozesse (Ereignisüberwachung, Vorfallsanalyse und Incident Response) dar, die von ausgereifter Automatisierung unterstützt werden. Der Anteil der Unternehmen ohne Automatisierung ist bei Unternehmen mit schwacher Integration mehr als doppelt so hoch. **Umgekehrt war es bei Unternehmen mit gut integrierten Sicherheitstechnologien fast siebenmal wahrscheinlicher, dass sie einen hohen Automatisierungsgrad für alle drei Prozesse erreichten (4,1 % gegenüber 28,5 %).** Das klingt nach einer überzeugenden Motivation!

Welche Funktionen sollten integriert werden?

Als Nächstes fragten wir die Teilnehmer:innen nach ihrem Integrationsgrad zwischen Technologien, die die fünf Kernfunktionen des NIST Cybersecurity Framework (CSF) unterstützen. Sie antworteten auf einer Skala von stark fragmentiert (Silo-Technologien, die größtenteils isoliert arbeiten) bis hochgradig integriert (aufeinander abgestimmte Technologien, die eine funktionale Einheit bilden). Anschließend haben wir ein Modell erstellt, um die Auswirkungen auf die Gesamtbewertung der Sicherheitsergebnisse für jedes Unternehmen zu bestimmen.

Die Ergebnisse in Abbildung 10 sind über die fünf Funktionen hinweg ziemlich konsistent. **Eine Bemühung zur Defragmentierung und Integration der NIST-CSF-Funktionsbereiche korreliert mit einer Steigerung des Erfolges des Sicherheitsprogramms (+ 11 % bis ~ 15 %).** Daher lautet die Antwort auf die Frage in der Überschrift dieses Abschnitts: alle. Aber wenn Sie sich fragen, wo Sie anfangen sollen: Eine hochgradig integrierte Identifizierungsfunktion bringt die größten Vorteile.

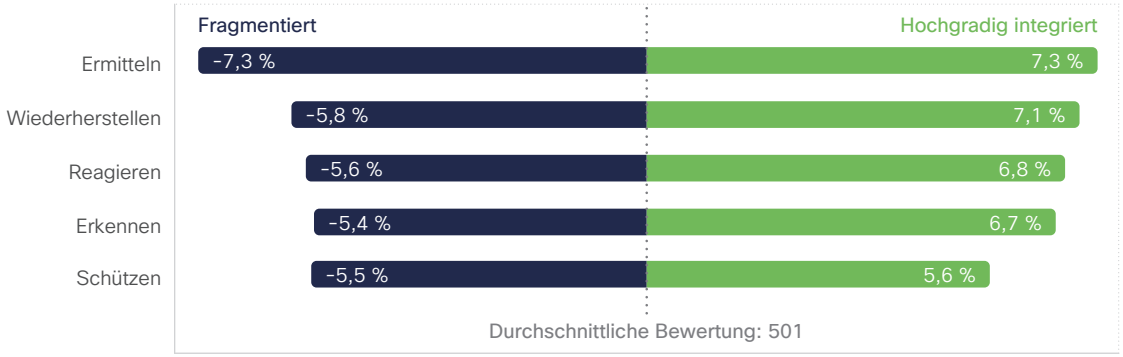


Abbildung 10: Auswirkung der Integration von NIST-CSF-Funktionen auf die Gesamtbewertung der Sicherheitsergebnisse

Wir können nicht umhin, einen Zusammenhang zwischen dieser Tatsache und dem zu sehen, was wir im vorherigen Abschnitt über Überwachung, Audits und Zusammenarbeit als die stärksten Faktoren für die Integration von Technologie gelernt haben. Zusammen erscheinen sie als starkes Indiz für die grundlegende Bedeutung einer guten Transparenz im gesamten Unternehmen. Es ist sicherlich naheliegend, dass ein fragmentierter Ansatz zur „Entwicklung eines organisatorischen Verständnisses für das Management von Cybersicherheitsrisiken für Systeme, Menschen, Ressourcen, Daten und Fähigkeiten“ (wie es im CSF formuliert ist) böse enden dürfte. Im Abschnitt „Bedrohungserkennung und Incident Response“ wird dieser Aspekt noch vertieft.

Zu Integration, Identifizierung und Information

Über das gerade besprochene Diagramm hinaus weisen die Daten in dieser Studie durchweg auf den entscheidenden Zusammenhang zwischen Integration, Identifizierung und Information hin. Wenn Sie eine Ressource oder Bedrohung nicht identifizieren können, wissen Sie nicht, dass sie vorhanden ist, und sind daher nicht besorgt genug, um eine fundierte Verteidigung aufzubauen, bis es zu spät ist.

Abbildung 11 illustriert dieses Konzept gut. Wir haben die gemeldete Integrationsstufe jedes Unternehmens innerhalb der NIST-CSF-Funktion „Identifizieren“ mit ihrer Fähigkeit verglichen, Bedrohungen rechtzeitig und präzise zu erkennen. **Unternehmen mit hochgradig integrierten Systemen zur Identifizierung kritischer Ressourcen und Risiken zeigten deutlich bessere Fähigkeiten bei der Bedrohungserkennung (+ 41 %).** Praktisch gesehen gehen also der Kampf gegen Fragmentierung und der Kampf gegen Angreifer Hand in Hand!

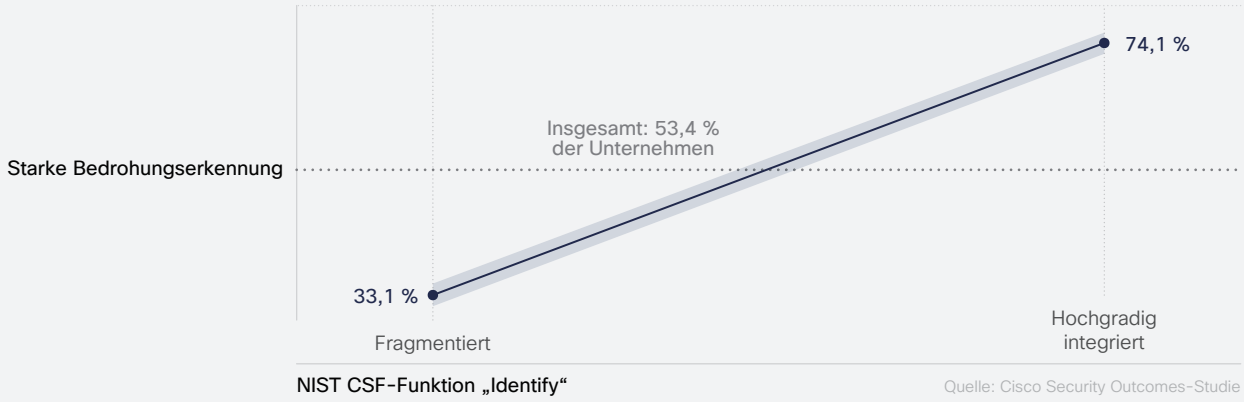


Abbildung 11: Auswirkung der Integration der NIST-CSF-Identifizierungsfunktion auf die Funktionen zur Bedrohungserkennung

der Unternehmen mit hochgradig integrierten Systemen zur Identifizierung kritischer Ressourcen und Risiken zeigten um

+41 %

bessere Fähigkeiten bei der Bedrohungserkennung

„Dank der Automatisierungsfunktionen können unsere Techniker rechtzeitig auf neue Bedrohungen reagieren. Anstatt ständig Regeln zu aktualisieren und das Netzwerk rund um die Uhr zu überwachen, können wir uns jetzt darauf konzentrieren, die richtigen Sicherheitskonzepte auszuarbeiten. Cisco geht bis ins kleinste Detail und filtert für uns die Informationen heraus, die wir für den zuverlässigen Schutz und die Verwaltung der Infrastruktur benötigen. So erhalten wir die perfekte Kombination aus maschineller und menschlicher Intelligenz.“

Steve Erzberger, CTO, Frankfurter Bankgesellschaft (Schweiz) AG

Weiterlesen

Entwicklung von Funktionen zur Bedrohungserkennung und Incident Response

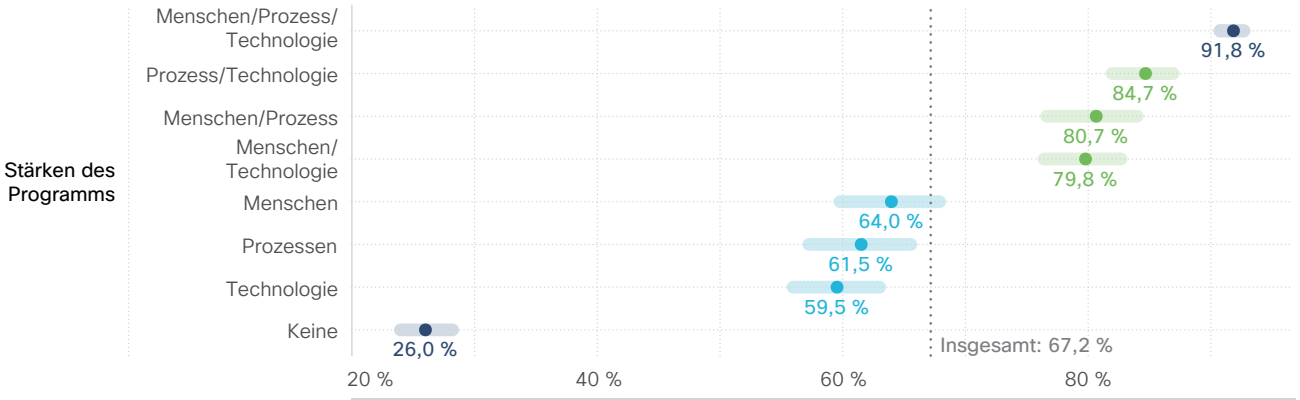
Dieser Abschnitt behandelt zwei separate Bereiche für Sicherheitspraktiken, die beide zu den „großen Fünf“ gehören. Aber da Bedrohungserkennung und Incident Response (IR) häufig Personen, Prozesse und Technologien unter dem Banner Security Operations (SecOps) zusammenbringen, haben wir in diesen Bereichen eine Reihe gemeinsamer Fragen gestellt. Daher ist es sinnvoll, sie für diese Studie im selben Abschnitt zu analysieren.

Fast alle Unternehmen (etwa 92 %) mit starken Mitarbeiter:innen, Prozessen und Technologien verfügen über erweiterte Funktionen zur Erkennung von und Reaktion auf Bedrohungen.

Priorisierung von Mitarbeiter:innen, Prozessen oder Technologie?

Apropos Mitarbeiter:innen, Prozesse und Technologie – beginnen wir doch hier mit der Untersuchung. Sicherheitsfunktionen werden häufig als eine Kombination aus allen drei Elementen beschrieben, insbesondere im Bereich der Bedrohungserkennung und Incident Response. Aber ist ein Teil dieser Security-Dreifaltigkeit wichtiger als die anderen? Sie wissen, worauf wir hinauswollen. Lassen Sie uns mit der Analyse beginnen.

Ausgehend von Abbildung 12 unten sehen wir, dass nur etwa ein Viertel der Programme, denen es in allen drei Bereichen an Stärke mangelt, Vertrauen in ihre SecOps haben. Wenn Sie in einem bestimmten Feld (Mitarbeiter:innen, Prozesse oder Technologie) an Stärke gewinnen, steigt dieser Anteil auf bis zu ca. 60–64 %, je Bereich. Starke Mitarbeiter:innen scheinen einen kleinen Vorteil zu gewähren, aber die überlappenden Konfidenzintervalle zeigen, dass Sie hier nicht zu viel hineininterpretieren sollten. Die wichtige Erkenntnis ist, dass jeder dieser Bereiche einen guten Ausgangspunkt für die Entwicklung besserer Erkennungs- und Reaktionsfunktionen bietet.



Quelle: Cisco Security Outcomes-Studie

Abbildung 12: Auswirkungen starker Mitarbeiter:innen, Prozesse und Technologien auf die Funktionen zur Bedrohungserkennung und Incident Response

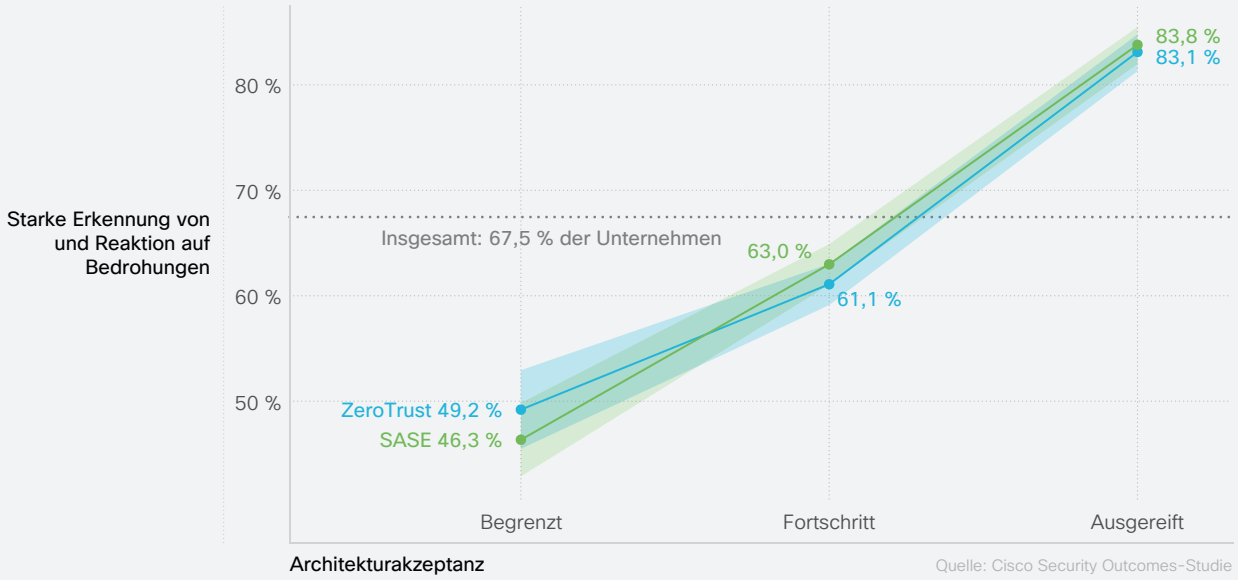
Gehen wir in Abbildung 12 weiter nach oben: Wenn bei zwei Aspekten gute Arbeit geleistet wird, rücken SecOps-Programme deutlich über den Durchschnitt und die Funktionen werden um etwa 15 bis 20 % besser als bei Unternehmen, die nur einen Bereich gut machen. Auch hier spielt es keine Rolle, welche Kombination aus Mitarbeiter:innen, Prozessen und Technologien Sie wählen. Sie müssen lediglich in zwei der drei Bereiche eine gute Leistung vorweisen. Es ist doch schön, zu sehen, dass Sie bei der Zusammenstellung der SecOps-Roadmap Ihres Unternehmens etwas Freiheit haben, oder?

Damit kommen wir zu den Elite-Programmen in Abbildung 12, die eine hervorragende Leistung in allen drei SecOps-Feldern erreichen. **Fast alle Unternehmen (etwa 92 %) mit starken Mitarbeiter:innen, Prozessen und Technologien verfügen über erweiterte Funktionen zur Erkennung von und Reaktion auf Bedrohungen.** Das ist 3,5-mal mehr als bei SecOps-Programmen, die in keinem der Bereiche gut aufgestellt sind! Beginnen Sie also, wo immer Sie können, aber stoppen Sie nicht, bis Sie Spitzenwerte auf allen drei Feldern erreichen.

Unternehmen mit starken Mitarbeiter:innen, Prozessen und Technologien verfügen über eine **3,5 x** bessere Bedrohungserkennung und -reaktion als die, die in all diesen Bereichen nicht gut genug aufgestellt sind

Ermöglichen Zero Trust und SASE bessere SecOps?

Wir wissen, dass abstrakte Deskriptoren wie „starke Technologie“ es schwierig machen, aus den obigen Erkenntnissen konkrete Erkenntnisse zu ziehen. Deshalb haben wir ein paar Nachfragen zu bestimmten Architekturen gestellt. Wir haben die Teilnehmer:innen über die Einführung von Zero Trust und Secure Access Service Edge (SASE) befragt, um besser zu verstehen, wie sich diese Ansätze auf Bedrohungserkennung und Incident Response (und damit auf die Ergebnisse des Sicherheitsprogramms) auswirken.



Quelle: Cisco Security Outcomes-Studie

Abbildung 13: Auswirkungen von Zero-Trust- und SASE-Architekturen auf die Funktionen zur Bedrohungserkennung und Incident Response

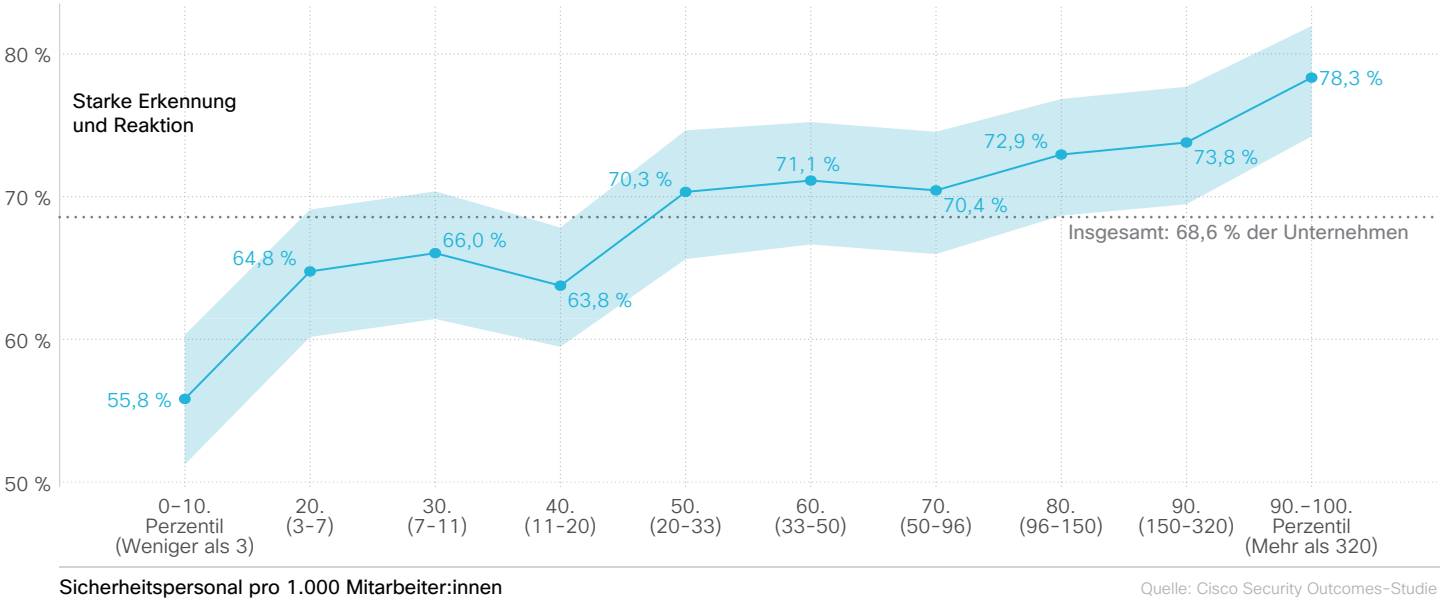
Unternehmen, die behaupten, ausgereifte Implementierungen von Zero Trust oder SASE zu haben, melden mit etwa 35 % höherer Wahrscheinlichkeit als Unternehmen mit neuen Implementierungen starke SecOps.

Diese Ergebnisse untermauern die oben vorgestellten Indizien in Bezug auf die vielen Vorteile, die moderne Architekturen für Cybersicherheitsprogramme bieten können.

Bedeuten mehr Köpfe weniger Kopfschmerzen?

Wir wissen, dass gute Mitarbeiter:innen für den Aufbau einer leistungsstarken Bedrohungserkennung und Incident Response wichtig sind. Aber ist es besser, sich darauf zu konzentrieren, mehr Mitarbeiter:innen einzustellen oder die Fähigkeiten der bestehenden zu erweitern? Das muss sich natürlich nicht gegenseitig ausschließen, aber die Frage bleibt: Gibt es Anzeichen dafür, dass Quantität oder Qualität bei der Entwicklung erfolgreicher SecOps-Teams wichtiger ist?

Um dies zu beantworten, haben wir zunächst für alle Unternehmen das Verhältnis der SecOps-Mitarbeiter:innen zur Gesamtbelegschaft berechnet. Anschließend haben wir dieses Verhältnis mit der angegebenen Stärke der Erkennungs- und Reaktionsfähigkeiten verglichen. Abbildung 14 zeigt das Ergebnis dieser Berechnungen, und obwohl dies die Frage nach Menge oder Qualität nicht vollständig beantwortet, bietet es einige Erkenntnisse.



Quelle: Cisco Security Outcomes-Studie

Abbildung 14: Auswirkung des Verhältnisses von Sicherheitspersonal auf die Funktionen zur Bedrohungserkennung und Incident Response

Erstens: Die relative Anzahl an Mitarbeiter:innen im Bereich Sicherheit korreliert mit einer besseren Erkennung von und Reaktion auf Bedrohungen. Bei Unternehmen mit den höchsten Quoten ist die Wahrscheinlichkeit, dass sie über stärkere Funktionen verfügen, um etwas mehr als 20 % höher als bei den Unternehmen mit der niedrigsten. ABER: Sehen Sie, wie die gepunktete Linie, die den Gesamtdurchschnitt markiert, einen Großteil des schattierten Konfidenzintervalls in Abbildung 14 durchquert? Das bedeutet im Wesentlichen, dass Unternehmen, die nicht am äußersten Ende der Personalskala stehen (die Mehrheit), gleichermaßen starke SecOps-Programme melden.

Was bedeutet das nun tatsächlich? Wir können mit Zuversicht sagen, dass Unternehmen mit großen Sicherheitsteams mit deutlich höherer Wahrscheinlichkeit starke Erkennungs- und Reaktionsfähigkeiten erzielen als Unternehmen mit einem rudimentären Team. Aber die Mitarbeiterzahl allein wird nicht alle Ihre SecOps-Kopfschmerzen beseitigen oder einen Erfolg garantieren. Darüber hinaus ist noch nicht einmal die Leistungssteigerung, die im vorherigen Abschnitt mit starken Mitarbeiter:innen in Zusammenhang gebracht wurde, allein durch die Unterschiede zwischen dem kleinsten und dem größten Mitarbeiterverhältnis erklärbar. **Daher müssen wir folgern, dass Qualität für den Aufbau starker Teams zur Erkennung und Reaktion auf Bedrohungen gleichermaßen wichtig ist wie Quantität – vielleicht sogar noch wichtiger.**

Sicherheitsteams sehen sich weiterhin mit einem erheblichen Personalmangel konfrontiert.

Angesichts knapper werdender Ressourcen und steigender Bedrohungen erleben viele Cybersicherheitsexperten extremen Stress und Burnout. Welche proaktiven Maßnahmen können wir ergreifen, um ihr Wohlergehen zu fördern? In diesem E-Book haben wir Branchenführer und Praktiker gebeten, ihre Erkenntnisse und Geschichten zum Umgang mit psychischer Gesundheit mitzuteilen.

SecOps-Personal: Outsourcing, Insourcing oder beides?

Bei SecOps geht es also nicht nur um die Mitarbeiterzahl, aber haben Personalmodelle Auswirkungen auf die Ergebnisse? Ist bei identischen Voraussetzungen Outsourcing, Insourcing oder ein gemischter Ansatz für die Erkennung von und Reaktion auf Bedrohungen am geeignetsten? Lassen Sie und untersuchen, wie die Daten diese Frage beantworten. Aber seien Sie gewarnt – in diesem Bereich gibt es keine eindeutigen Antworten.

Wir haben die Teilnehmer:innen nach ihren Personalmodellen gefragt und diese dann mit der Bewertung ihrer Erkennungs- und Reaktionsfähigkeiten verglichen. **Wie in Abbildung 15 zu sehen ist, war die Wahrscheinlichkeit, dass Unternehmen, die sich auf Insourcing oder Outsourcing konzentrieren, starke SecOps-Programme melden, höher (+ 20–30 %) als bei Unternehmen mit einem gemischten Personalmodell.** Da jedoch die meisten Unternehmen angaben, dass sie ein gemischtes Modell irgendeiner Art verwenden, hielten wir es für lohnenswert, dies aus einer anderen Perspektive zu betrachten, bevor wir sie alle zum Scheitern verurteilen, nur weil die Umfrage (scheinbar) auf dieses Ergebnis hinweist.

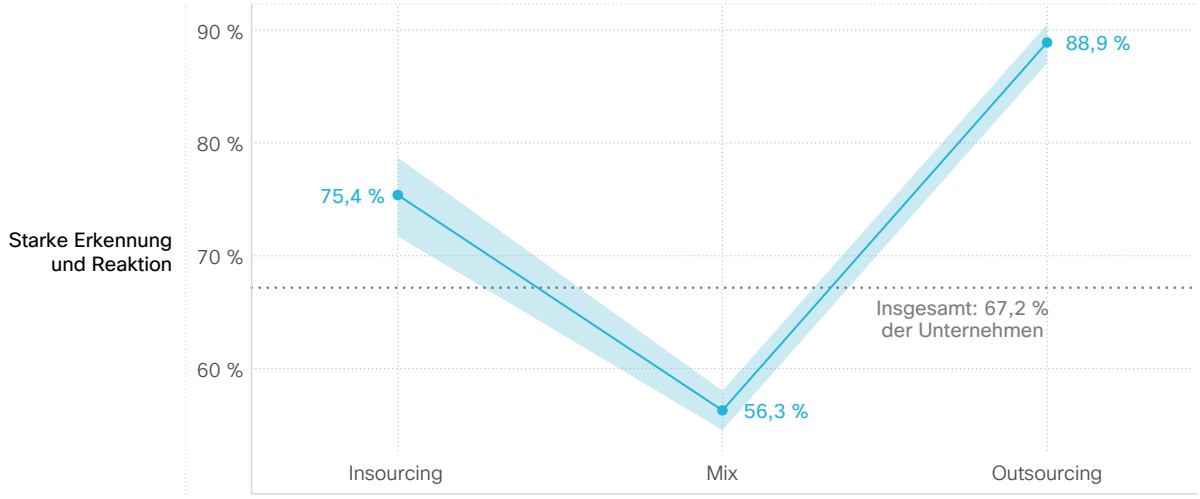


Abbildung 15: Auswirkungen von Personalmodellen auf die wahrgenommene Bedrohungserkennung und Incident Response

Die Wahrscheinlichkeit, dass Unternehmen, die sich auf Insourcing oder Outsourcing konzentrieren, starke SecOps-Programme melden ist

20 bis 30 %

höher als bei Unternehmen mit einem gemischten Personalmodell

Wir haben die Teilnehmer:innen nicht nur gebeten, die wahrgenommene Stärke der Erkennungs- und Reaktionsfähigkeiten zu bewerten, sondern auch versucht, objektivere Kennzahlen für den Vergleich zu erhalten. Eine davon ist die Mean Time to Respond (MTTR): die durchschnittliche Zeit bis zur Behebung oder Eindämmung eines Sicherheitsvorfalls. In unserer Hintergrundanalyse außerhalb dieses Berichts stimmen diese Kennzahlen oft tendenziell mit den subjektiven Bewertungen überein. Aber in diesem Fall widersprachen sich die beiden Perspektiven, wie aus Abbildung 16 hervorgeht.

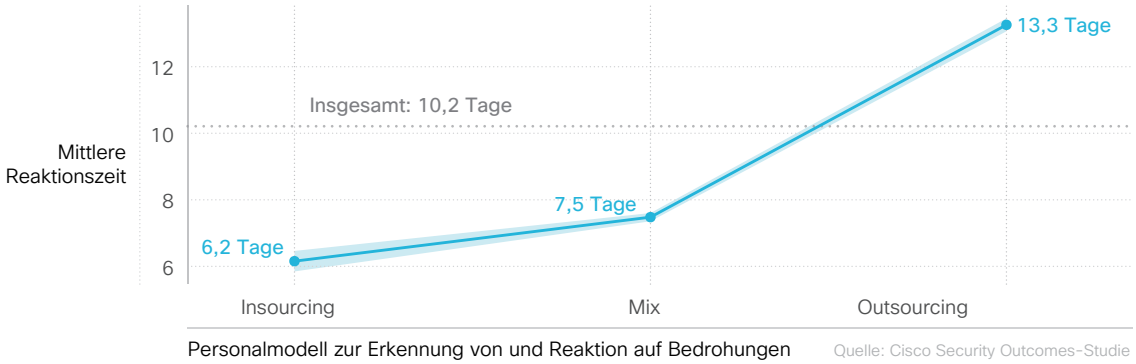


Abbildung 16: Auswirkungen von Personalmodellen auf die durchschnittliche Reaktionszeit auf Sicherheitsvorfälle[2]

Basierend auf Abbildung 16 beträgt die MTTR von Unternehmen mit internen Bedrohungserkennungs- und Reaktionsteams eine MTTR weniger als die Hälfte derjenigen, die Outsourcing-Modelle nutzen (etwa 6 Tage vs. 13 Tage). Diejenigen mit hybriden Personalmodellen landen in der Mitte (etwa 8 Tage) – ihre MTTRs sind nicht ganz so kurz wie bei internen Teams, aber wesentlich kürzer als bei den meisten Unternehmen, die diese Funktion outsourcen.

Natürlich haben wir es hier mit einem Dilemma zu tun. Welche Kennzahl (Perspektive vs. Metrik) ist die richtige und, noch wichtiger, auf welche Kennzahl sollten Sie achten, wenn Sie In-/Outsourcing-Entscheidungen treffen? Wir werden hier absichtlich uneindeutig sein und „beide“ und „keine“ sagen (nehmen Sie es uns bitte nicht übel, dass wir hier den widersprüchlichen Daten folgen).

Natürlich hat die Problembehebung viele Elemente und Abhängigkeiten. Das Unternehmen ist möglicherweise darauf angewiesen, dass ein Anbieter einen Patch/Bugfix herausbringt, um eine Schwachstelle vollständig zu beheben. Dieser Patch muss dann in seiner Umgebung im Labor getestet werden, bevor er in der Produktion bereitgestellt wird. Hier muss es genügen, zu sagen, dass viele Variablen zu berücksichtigen sind.

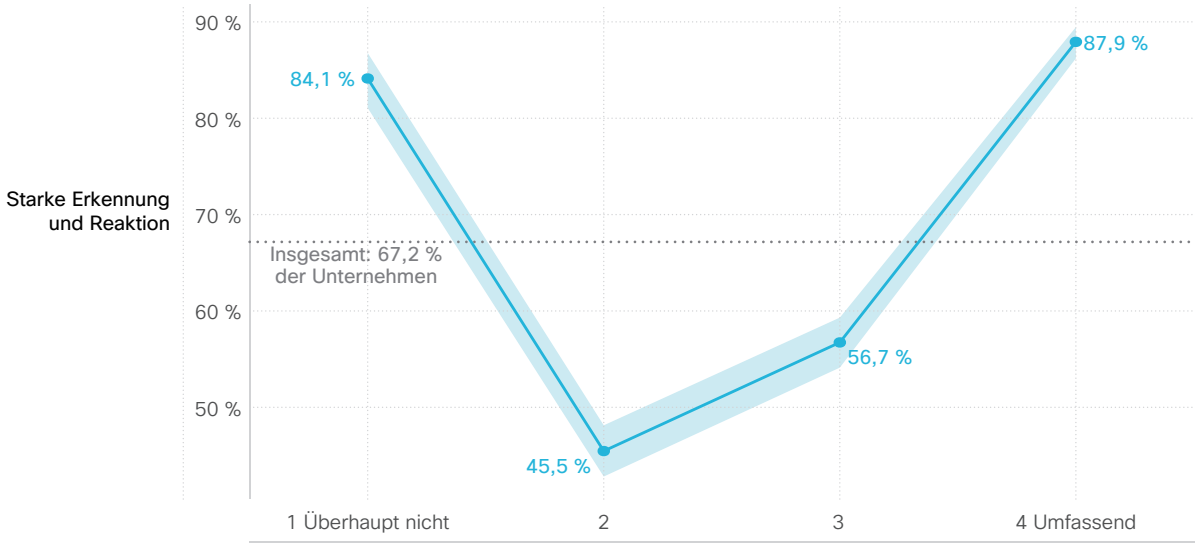
Tatsächlich ist es schwer zu sagen, was hier vor sich geht. Vielleicht ist der Versuch, Kennzahlen über eine Umfrage zu sammeln, irreführend. Vielleicht sind die MTTR- und Fähigkeitsbewertungen so unterschiedlich, dass es möglich ist, ein „starkes“ Erkennungs- und Reaktionsprogramm zu haben, aber eine langsamere Problembehebung. Vielleicht sind diese Programme langsamer, weil sie gründlicher sind. Vielleicht dauert die Abstimmung mit ausgelagerten Mitarbeiter:innen nur länger. Vielleicht gibt es ein Gefühl von Zuversicht, weil „wir die Experten dafür bezahlen und sie das schon hinkriegen werden.“ Vielleicht sehen wir eine SecOps-Version des Dunning-Kruger-Effekts. Wahrscheinlich trifft alles davon zu, und noch viel mehr. Aus diesem Grund empfehlen wir Ihnen, diesen Abschnitt zu nutzen, um Diskussionen anzuregen, anstatt Entscheidungen zu treffen.

[2] Wir verwenden das geometrische Mittel in diesem Diagramm, da es eher repräsentativ für einen „typischen“ Wert ist. Die angegebene MTTR betrug in der Regel weniger als 2–3 Wochen, aber gelegentlich gaben die Befragten Monate (oder Jahre!) an. Mit dem geometrischen Mittelwert gelingt es, „typisch“ besser darzustellen, ohne dass das Ergebnis von diesen extrem großen Werten verfälscht wird.

Ist die Nutzung von Intelligence sinnvoll?

Apropos Dunning-Kruger-Effekt – das ist der perfekte Einstieg in diesen Abschnitt. Wir haben die Teilnehmer:innen über die Verwendung von Cyber-Threat-Intelligence in ihrem SecOps-Programm befragt. Die meisten Unternehmen (85 %) geben an, dass sie Intelligence zu einem gewissen Grad verwenden, aber weniger als ein Drittel (31 %) nutzt sie umfassend. Führt diese Intelligence zu einer besseren, intelligenteren und schnelleren Bedrohungserkennung und -reaktion? Nun ... sehen wir uns Abbildung 17 an.

Seltsamerweise scheinen die meisten Unternehmen, die überhaupt keine Threat-Intelligence nutzen, der Meinung zu sein, dass es ihnen gut geht. Hier kommt das alte Sprichwort „Was ich nicht weiß, macht mich nicht heiß“ in den Sinn, insbesondere da diese Vorstellung offensichtlich zerstreut wird, sobald Unternehmen anfangen, Intelligence zu nutzen (das Vertrauen sinkt von etwa 84 % auf 46 %). **Unternehmen, die Threat-Intelligence umfassend nutzen, melden fast doppelt so häufig starke Erkennungs- und Reaktionsfähigkeiten wie Unternehmen mit geringerer Nutzung. Und in einem Beispiel, in dem Fähigkeitsbewertungen und Metriken übereinstimmen, erreichen diejenigen, die Intelligence stärker nutzen, etwa halb so lange MTTRs wie diejenigen, die keine Intelligence nutzen.**



Quelle: Cisco Security Outcomes-Studie

Abbildung 17: Auswirkungen der Nutzung von Cyber-Intelligence auf Funktionen zur Bedrohungserkennung und Incident Response

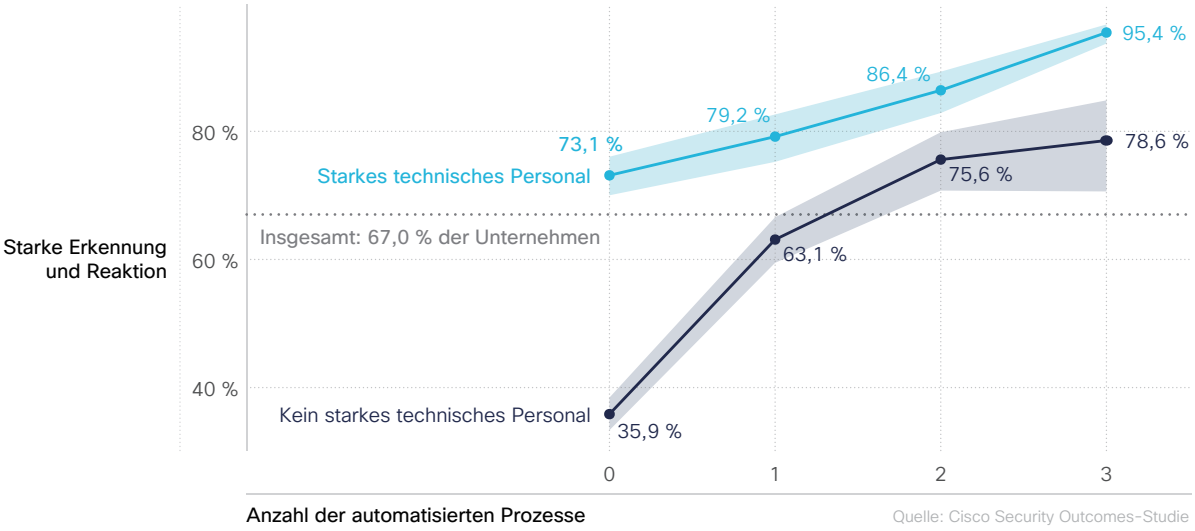
Der Psychologe und Bestsellerautor Daniel Kahneman sagte einmal: „Wir sind blind für unsere eigene Blindheit. Wir haben kaum eine Ahnung davon, wie wenig Ahnung wir haben.“ Abbildung 17 zeigt, dass Unternehmen, die ein wenig über die gegen sie gerichteten Bedrohungen Bescheid wissen, viele Dinge nicht wissen. Die umfassendere Nutzung von Threat-Intelligence beginnt, dieses Vertrauen wieder aufzubauen – nur sind Unternehmen dadurch nicht mehr so blind.

Unternehmen, die Threat-Intelligence umfassend nutzen, geben fast **2 X** häufiger an, dass sie über starke Erkennungs- und Reaktionsfähigkeiten verfügen

Ist Automatisierung ein Ersatz für Mitarbeiter:innen?

Nachdem Sie diesen Titel gelesen haben, nehmen Sie vielleicht an, dass es sich um eine rhetorische Frage handelt. Nicht so schnell. Auf die Gefahr hin, die gesamte Security-Community zu reizen, lehnen wir uns hier ein bisschen aus dem (Daten-) Fenster und behaupten, dass Automatisierung tatsächlich Mitarbeiter:innen ersetzen kann. ABER: Lesen Sie weiter, bevor Sie beschließen, diesen Bericht zu löschen und uns zu Ihrer Liste blockierter Kontakte hinzuzufügen. Tief durchatmen.

Abbildung 18 enthält Elemente, die Sie zuvor in separaten Diagrammen gesehen haben – Sicherheitspersonal und Automatisierung. Die beiden Kurven dienen zum Vergleich zweier unterschiedlicher Arten von SecOps-Programmen. Die erste (dunkelblaue Linie) stellt Unternehmen dar, die KEINE starken Personalressourcen haben, während diejenigen, die diesen Luxus genießen, durch die hellblaue Linie dargestellt werden. In beiden Szenarien zeigt die Bewegung von links nach rechts die Auswirkungen einer zunehmenden Automatisierung auf Bedrohungserkennung und IR-Funktionen.



Quelle: Cisco Security Outcomes-Studie

Abbildung 18: Auswirkung der Stärke von Personal und Automatisierung auf die Funktionen zur Bedrohungserkennung und Incident Response

Beginnen wir mit denjenigen ohne starkes Sicherheitspersonal. Nur etwa ein Drittel der Unternehmen, denen es an starkem Sicherheitspersonal mangelt und die keine wichtigen Prozesse automatisieren, berichten von starken Erkennungs- und Reaktionsfähigkeiten. Wenn einer der drei Prozessbereiche, nach denen wir gefragt haben (Bedrohungsüberwachung, Ereignisanalyse, Incident Response), automatisiert wird, steigt dieser Wert sprunghaft an. Die Automatisierung von zwei dieser Systeme steigert den Wert noch weiter, und bei Automatisierung von allen dreien wird die Leistung von weniger erfahrenen Mitarbeiter:innen mehr als verdoppelt. **Mehr als drei Viertel der SecOps-Programme, die nicht über ausreichende Personalressourcen verfügen, können durch ein hohes Maß an Automatisierung dennoch robuste Funktionen erreichen.**

Vergleichen Sie nun einmal den ganz rechten Punkt auf der dunkelblauen Linie mit dem untersten Punkt der hellblauen Linie. Haben Sie die Auswirkungen verstanden? **Ein SecOps-Programm mit schwächeren Mitarbeiter:innen, die jedoch fortschrittliche Automatisierung nutzen, zeigt eine ähnliche Leistung wie die Kombination aus starken Mitarbeitern und schlechter Automatisierung.** Oder anders ausgedrückt: Starke Automatisierung kann ein Ersatz für starke Mitarbeiter:innen sein. Sehen Sie – wir würden Sie nicht anlügen!

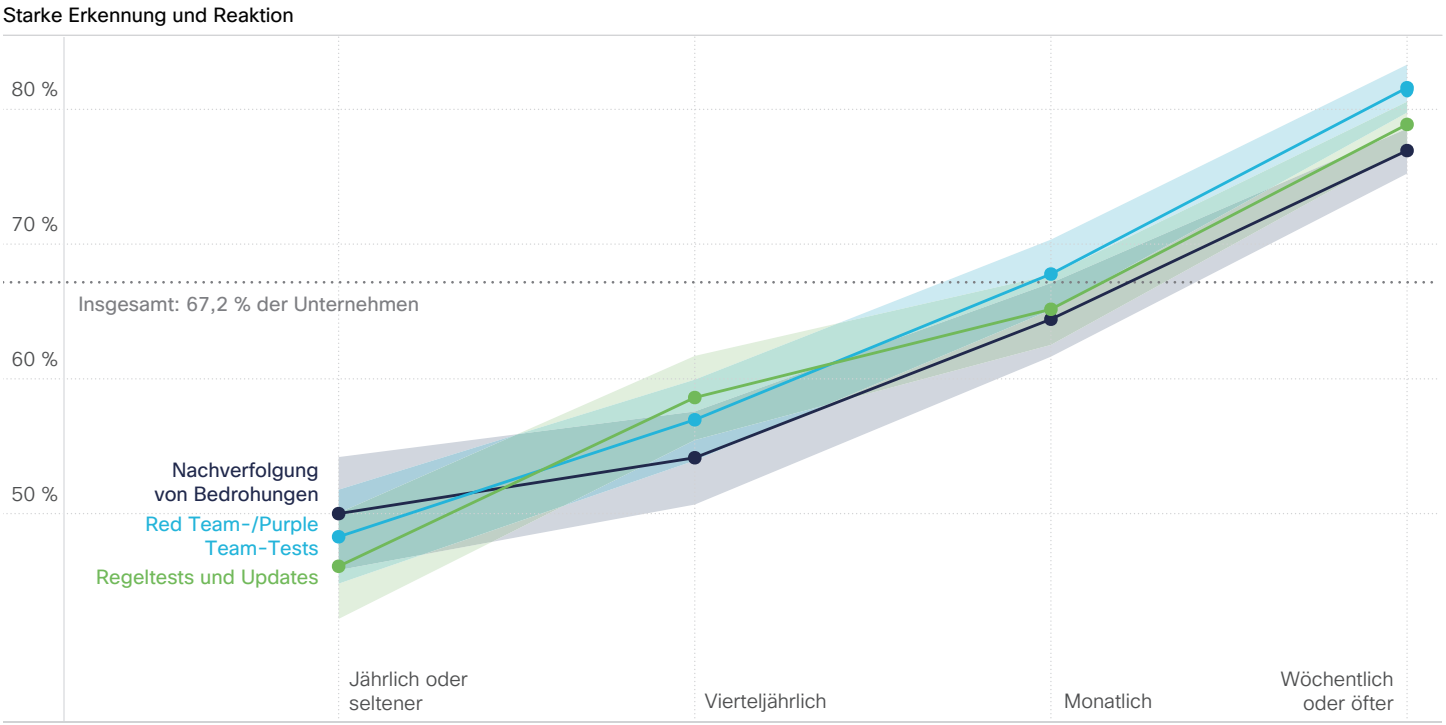
Aber Mensch gegen Maschine ist eigentlich nicht der wichtigste Punkt oder die wichtigste Lektion aus Abbildung 18. Wenn Sie der blauen Linie durch aufeinanderfolgende Automatisierungsstufen folgen, finden Sie eine überzeugende Begründung für die Verfolgung beider Ziele. Sicherheitsprogramme, die über ein starkes Team verfügen UND wichtige Bedrohungserkennungs- und -reaktionsprozesse automatisieren, erzielen mit großer Sicherheit (mehr als 95 %) SecOps-Erfolge. Verwenden Sie also Automatisierung nicht als Ersatz für eine talentierte Belegschaft. Nutzen Sie sie, um Ihre Talente zu stärken, indem Sie ihnen ermöglichen, sich auf Aktivitäten mit hoher Priorität zu konzentrieren.

Wie oft sollten wir optimieren, hacken und suchen?

Man könnte eine beliebige Anzahl wiederkehrender Aktivitäten nennen, die Programme zur Erkennung von und Reaktion auf Bedrohungen verbessern könnten. In einer informellen Umfrage zu diesem Thema wurden drei Maßnahmen häufiger empfohlen als alle anderen:

- Testen und Aktualisieren von Erkennungsregeln und Anwendungsfällen
- Proaktive Suche nach Anzeichen für schädliche Aktivitäten
- Durchführung von Red Team-/Purple Team-Tests

Wir haben die Teilnehmer:innen gefragt, wie oft ihr Unternehmen jede dieser Aktivitäten durchführen, und diesen Wert mit der gemeldeten Stärke der Funktionen zur Bedrohungserkennung und -reaktion verglichen. Der resultierende Trend in Abbildung 19 könnte nicht deutlicher sein.

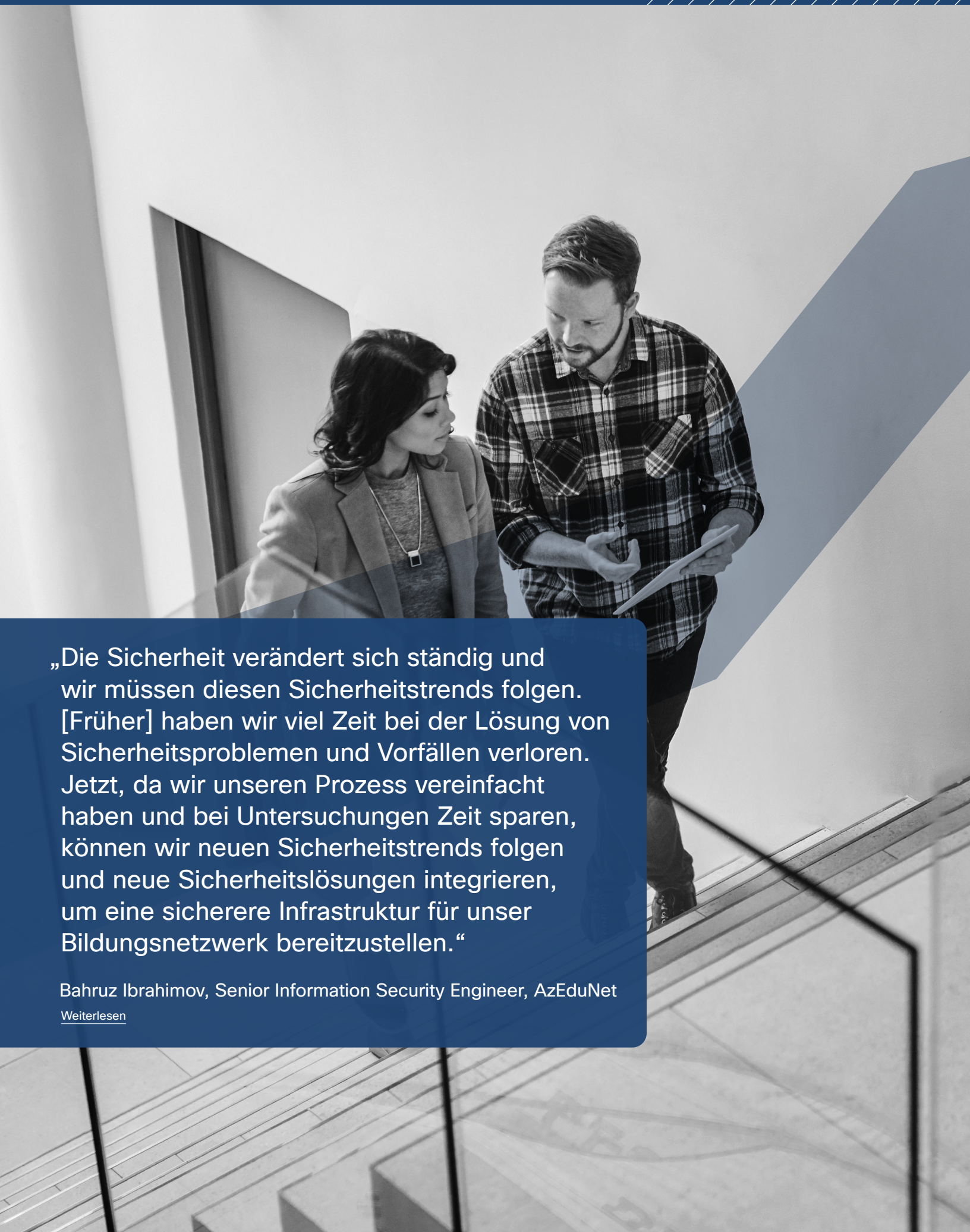


Quelle: Cisco Security Outcomes-Studie

Abbildung 19: Auswirkung der Aktivitätshäufigkeit auf die Funktionen zur Bedrohungserkennung und Incident Response

Regeloptimierungen, Red Team-/Purple Team-Tests und die Nachverfolgung von Bedrohungen folgen einem ähnlichen Weg. Je häufiger diese Maßnahmen durchgeführt werden, desto stärker profitieren SecOps-Programme davon. **Unternehmen, die diese Aktivitäten mindestens einmal pro Woche durchführen, verzeichnen eine Leistungssteigerung von etwa 30 % im Vergleich zu Unternehmen, die dies jährlich oder seltener tun.** Wie oft sollte Ihr Unternehmen sie durchführen? Die einfache Antwort lautet: „Je öfter, desto besser."

Unternehmen, die diese Aktivitäten mindestens einmal pro Woche durchführen, melden eine um **30 %** stärkere Performance



„Die Sicherheit verändert sich ständig und wir müssen diesen Sicherheitstrends folgen. [Früher] haben wir viel Zeit bei der Lösung von Sicherheitsproblemen und Vorfällen verloren. Jetzt, da wir unseren Prozess vereinfacht haben und bei Untersuchungen Zeit sparen, können wir neuen Sicherheitstrends folgen und neue Sicherheitslösungen integrieren, um eine sicherere Infrastruktur für unser Bildungsnetzwerk bereitzustellen.“

Bahruz Ibrahimov, Senior Information Security Engineer, AzEduNet

Weiterlesen

Gewährleistung von Widerstandsfähigkeit und schneller Disaster Recovery

Es ist interessant, wie sich die Priorisierung der verschiedenen Aspekte der Cybersicherheit im Laufe der Zeit verändert. Nachdem das Thema Business Continuity und Disaster Recovery (BCDR) einige Jahre lang hinter Datenschutzverstößen und Cyber-Spionage zurück stand, rückt es nun wieder in den Vordergrund. Und das aus gutem Grund. Die rasante Verbreitung von Ransomware, Ausfälle großer Hosting-Anbieter usw. haben starke Änderungen an den Strategien zur Gewährleistung der Widerstandsfähigkeit angesichts unerbittlicher Bedrohungen erzwungen.

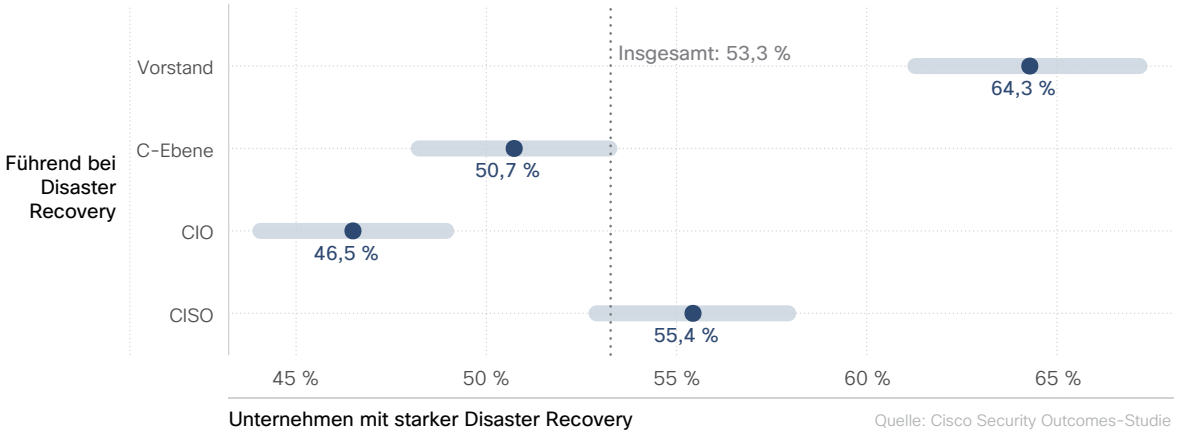
In der Security Outcomes-Studie 2021 wurde die schnelle Disaster Recovery als der viertstärkste Faktor beim Aufbau erfolgreicher Cybersicherheitsprogramme eingestuft. Sie zeigte signifikante Korrelationen mit allen 11 Ergebnissen außer einem (Sicherheitskultur). Lassen Sie uns vor diesem Hintergrund Strategien zur Maximierung der Effektivität dieser Praxis und zur Gewährleistung der Widerstandsfähigkeit betrachten.

Die rasante Verbreitung von Ransomware, Ausfälle großer Hosting-Anbieter usw. haben starke Änderungen an den Strategien zur Gewährleistung der Widerstandsfähigkeit angesichts unerbittlicher Bedrohungen erzwungen.

Sollte Disaster Recovery auf Vorstandsebene überwacht werden?

Wir wollten wissen, wer die ultimative Aufsicht über die Disaster-Recovery-Funktionen hatte. Dabei stellte sich heraus, dass die Verantwortung ziemlich gleichmäßig zwischen CIOs, CISOs und anderen Nicht-IT-Mitgliedern der C-Ebene verteilt ist. In jeweils etwa einem Viertel der befragten Unternehmen liegt die Verantwortung für BCDR-Prozesse bei einer dieser Personen. Die Überwachung dieser Aufgaben durch den Vorstand ist etwas weniger verbreitet, wird aber in immerhin 18 % der befragten Unternehmen angewendet.

Beim Vergleich dieser Antworten mit der Bewertung der Business Continuity und Disaster Recovery durch die Teilnehmer:innen wurde deutlich, dass die Frage der Verantwortung nicht nur eine Kuriosität ist. **Abbildung 20 zeigt, dass in Unternehmen, die BCDR auf Vorstandsebene überwachen, die Wahrscheinlichkeit am höchsten ist (11 % über dem Durchschnitt), dass starke Programme vorhanden sind.** Business-Continuity- und Disaster-Recovery-Funktionen, die ganz oben vom CIO verantwortet werden, weisen die niedrigsten Raten auf. Diese liegen sehr deutlich unter dem Durchschnitt.



Quelle: Cisco Security Outcomes-Studie

Abbildung 20: Auswirkung der obersten organisatorischen Aufsicht auf die Disaster-Recovery-Funktionen

Es gibt viele plausible Erklärungen für die Ergebnisse in Abbildung 20. Wir vermuten, dass Unternehmen, in denen der Vorstand für Disaster-Recovery-Fragen verantwortlich ist, wahrscheinlich größere Bedenken hinsichtlich Betriebsrisiken und Widerstandsfähigkeit haben. Diese Bedenken führen vermutlich zu einer strengeren Aufsicht, einer stärkeren Unterstützung und größeren Budgets. Wenn Ihr Unternehmen also Schwierigkeiten hat, die Disaster-Recovery-Funktionen zu verbessern, kann es sinnvoll sein, diese von oben nach unten statt von unten nach oben aufzubauen.

Was ist mit dem täglichen Betrieb der Disaster Recovery?

Neben der Aufsicht auf oberster Ebene haben wir auch gefragt, wer für die taktischeren Aspekte der Disaster Recovery verantwortlich ist. **Wenn die Verantwortung für den Betrieb innerhalb der Cybersicherheits- oder spezialisierter Business-Continuity-Teams liegt, ist die Leistung in der Regel am besten.** Von der IT verantwortete Programme lagen in der Regel dahinter. Interessanterweise scheint die Überwachung durch den Vorstand dafür zu sorgen, dass alle Programme besser werden. Die Erfolgsquoten waren statistisch gleich, unabhängig davon, wo die alltäglichen Verantwortlichkeiten lagen, solange die ultimative Kontrolle beim Vorstand lag.

Ist der Umfang der Disaster Recovery wichtig?

Sie werden wahrscheinlich nicht überrascht sein, dass Notfälle nicht nur dann eintreten, wenn Sie dafür bereit sind. Bei Cybersicherheitsvorfällen ist das nicht anders. Deshalb ist es gängige Praxis, sich auf alle Eventualitäten so gut wie möglich vorzubereiten. Das ist natürlich leichter gesagt als getan.

Dies wird dadurch bestätigt, dass weniger als drei von zehn Unternehmen angeben, dass ihre Disaster-Recovery-Funktionen mindestens 80 % der kritischen Systeme abdecken. Die Hälfte davon fällt in den Bereich von 50 % bis 79 %, und etwas weniger als 20 % geben an, dass die Abdeckungsraten niedriger sind. Auf den ersten Blick erscheint das nicht so schlimm. Schließlich ist bei den meisten Unternehmen die Mehrheit ihrer kritischen Systeme abgedeckt. Leider wird dabei nicht berücksichtigt, dass Notfälle die lästige Tendenz haben, an unerwarteten Orten aufzutreten. Unsere Daten deuten darauf hin, dass dies häufiger geschieht, als wir zugeben möchten.

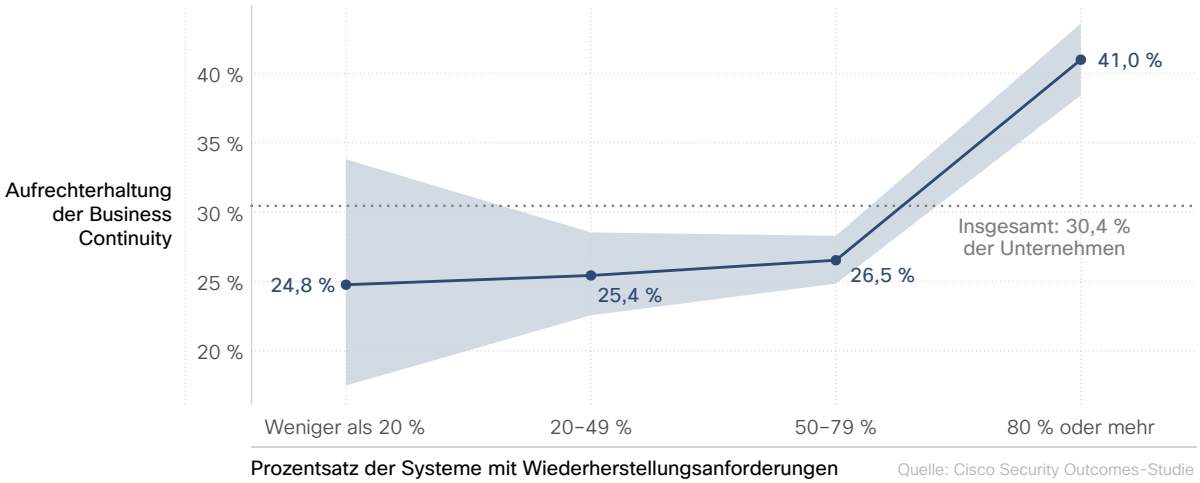


Abbildung 21: Auswirkung der Abdeckung kritischer Ressourcen auf die Disaster-Recovery-Funktionen

Abbildung 21 zeigt ein neues Ergebnis, das für diese Studie hinzugefügt wurde, um die Fähigkeit eines Unternehmens zu messen, die Business Continuity auch bei disruptiven Ereignissen aufrechtzuerhalten. Es stellt sich heraus, dass dies eines der drei Ergebnisse ist, mit denen die Befragten am meisten zu kämpfen haben. Umso wichtiger ist es, effektive Wege zu finden, um die Erfolgswahrscheinlichkeit zu erhöhen.

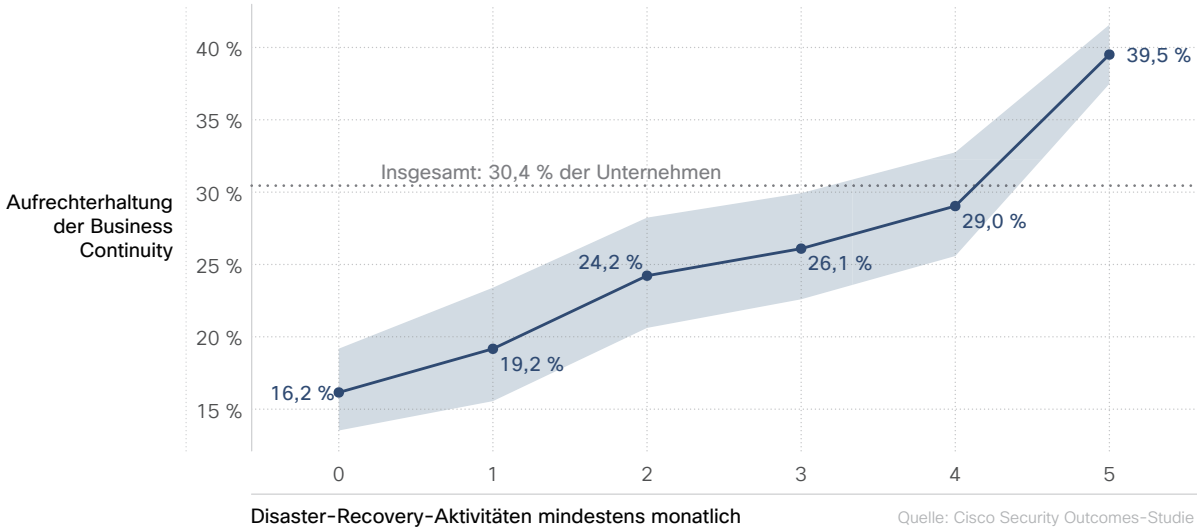
Abbildung 21 enthält eine wichtige Botschaft zur Aufrechterhaltung der Business Continuity. **Es gibt praktisch keine Verbesserung der Wahrscheinlichkeit, dieses Ergebnis zu erreichen, bis die BCDR-Funktionen mindestens 80 % der kritischen Systeme abdecken.**

Dies geht höchstwahrscheinlich auf die unschöne Neigung von Katastrophen zurück, dort zuzuschlagen, wo wir noch nicht bereit sind. Die Lektion dabei ist, dass wir nicht erwarten können, dass Investitionen in Business Continuity und Disaster Recovery zu unmittelbaren oder gleichwertigen Ergebnissen führen. Das ist wahrscheinlich keine angenehme Nachricht, aber andererseits sind Katastrophen ja niemals willkommen.

Macht Übung Sie zum Meister der Disaster Recovery?

Diese Frage beantworten wir direkt vorneweg: Nein, leider nicht. Aber sie macht Sie viel besser, als Sie ohne Übung wären. Wie viel besser? Lesen Sie weiter ...

Ein bekanntes Sprichwort beim Militär lautet: „Kein Plan überlebt die erste Feindberührung“. Diese Erkenntnis ist ziemlich gut auf das Cyber-Schlachtfeld übertragbar, und es gibt viele verschiedene Möglichkeiten, BCDR-Funktionen zu testen, darunter Plan-Walkthroughs, theoretische Planspiele, Live-Tests, parallele Tests und vollständige Produktionstests. Wir haben die Teilnehmer:innen gefragt, wie oft ihr Unternehmen solche Übungen durchführen, und diese mit ihrer Wahrscheinlichkeit verglichen, die Business Continuity aufrechtzuerhalten.



Quelle: Cisco Security Outcomes-Studie

Abbildung 22: Auswirkungen von Testübungen auf die Disaster-Recovery-Funktionen

Keine dieser Praktiken stand in Bezug auf die Wirksamkeit weit über den anderen, aber alle trugen gemeinsam zu einer besseren Widerstandsfähigkeit bei. **Bei Unternehmen, die regelmäßig alle fünf Arten von Disaster-Recovery-Tests durchführen, war die Wahrscheinlichkeit, dass die Business Continuity erfolgreich aufrechterhalten wurde, fast 2,5-mal höher als bei Unternehmen, die keine davon durchführen.** Das Fazit? Überlassen Sie Widerstandsfähigkeit nicht dem Zufall. Testen Sie Ihre Business-Continuity- und Disaster-Recovery-Funktionen regelmäßig aus verschiedenen Blickwinkeln.

Bei Unternehmen, die regelmäßig alle fünf Arten von Disaster-Recovery-Tests durchführen, war die Wahrscheinlichkeit,

2,5x

höher, dass die Business Continuity erfolgreich aufrechterhalten wurde

Sollten wir das Chaos von der Leine lassen?

Beim Thema Stresstests für Ihren Disaster-Recovery-Plan sollten Sie den Stress maximieren. Chaos Engineering bedeutet, dass Systeme regelmäßig (absichtlich) unterbrochen werden, um ihre Fähigkeit zu testen, unerwarteten Bedingungen und Ereignissen standzuhalten. Könnte Ihr Unternehmen widerstandsfähiger werden, wenn Sie absichtlich Störungen Ihrer IT- und Sicherheitssysteme verursachen? Nun, hier können Sie es herausfinden.

Wir haben die Teilnehmer:innen gefragt, inwieweit ihre Unternehmen Chaos Engineering betreiben, und erfahren, dass es häufiger ist als erwartet. Bemerkenswert ist, dass wir einen Zusammenhang zwischen dieser Vorgehensweise und der technischen Integration bemerkt haben. Abbildung 23 zeigt, dass über zwei Drittel der Unternehmen, bei denen Chaos Engineering Standard ist, von hochgradig integrierten Technologien berichten, die ihre Wiederherstellungsfunktionen unterstützen. Ob die Integration Chaos Engineering erfordert oder erst ermöglicht, ist unklar. Wie bei so vielen Dingen in diesem Bereich trifft wahrscheinlich beides zu. Behalten Sie diese neue Disziplin im Auge – insbesondere, wenn Sie für BCDR in einer komplexen und hochgradig integrierten IT-Umgebung verantwortlich sind.

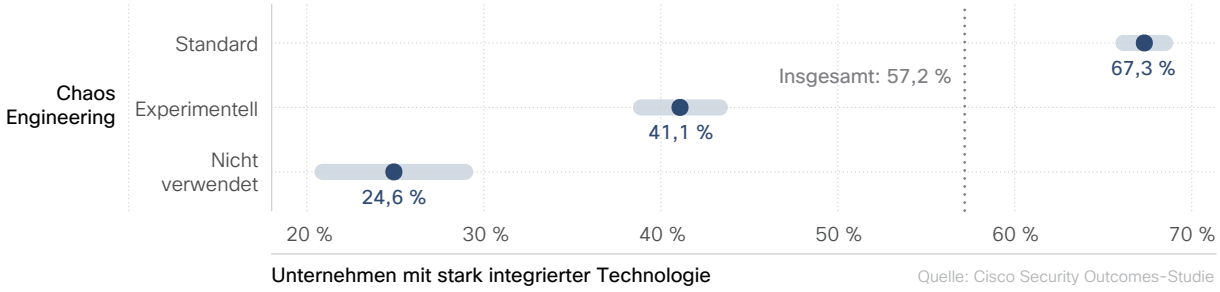


Abbildung 23: Zusammenhang zwischen Chaos Engineering und dem Grad der IT-Integration

Der Vergleich des Umfangs von Chaos Engineering mit dem Ergebnis der Aufrechterhaltung der Business Resiliency in Abbildung 24 ist ein überzeugender Grund, in Ihrem Netzwerk für etwas Chaos zu sorgen. **Unternehmen, die Chaos Engineering als Standard praktizieren, erzielen bei diesem Ergebnis doppelt so hohe Erfolgschancen wie Unternehmen, die es nicht nutzen.** Wenn Sie dieses Ergebnis schockiert, sind Sie nicht allein. Die gute Nachricht ist, dass Sie das Chaos beherrschen können, bevor es Sie beherrscht – lassen Sie Chaos Engineering für sich arbeiten.

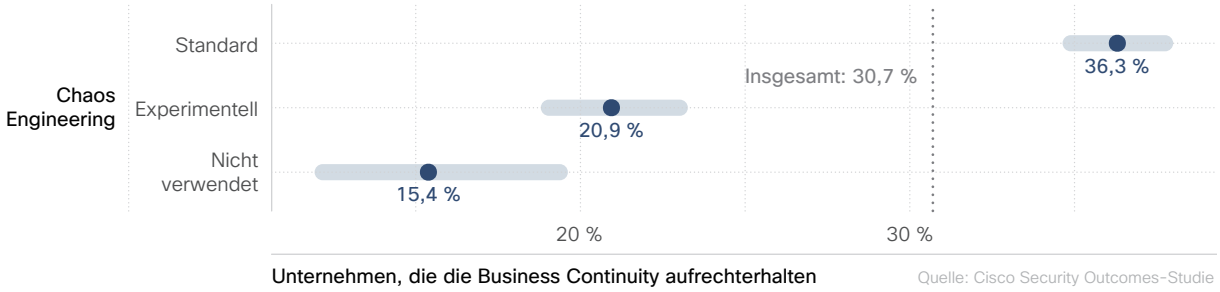


Abbildung 24: Auswirkungen von Chaos Engineering auf die Aufrechterhaltung der Business Resiliency

Fazit und Empfehlungen

Wir haben mit Sicherheitspraktiken begonnen, die in einer früheren Studie als sehr effektiv identifiziert wurden, haben in einer neuen Umfrage mehr Informationen gesammelt, um herauszufinden, was sie am effektivsten macht, und diese Lektionen mit Ihnen geteilt. Wir hoffen, dass Sie diesem Bericht einige praktische Tipps entnehmen konnten, wie Sie Ihr Cybersicherheitsprogramm erfolgreicher machen können.

Aber es schadet nie, über die Ergebnisse einer solchen Studie nachzudenken und zu hören, was andere daraus gelernt haben. Wir haben unser erfahrenes CISO Advisory Team gebeten, sich mit jedem der untersuchten Bereiche zu befassen. Nachfolgend finden Sie die wichtigsten Empfehlungen. Weitere Einblicke und Erkenntnisse finden Sie in unserer Blog-Reihe zur Security Outcomes-Studie.

Proaktive Technologieaktualisierung

„Das Verschuldungsproblem im Security-Bereich ist erheblich. Für den CISO besteht der beste Weg darin, eine „Buy, Hold, Sell"-Strategie zu entwickeln. Erkennen Sie, was Sie haben, definieren Sie eine anpassbare Architektur, reduzieren Sie das Abhängigkeitsrisiko und implementieren Sie eine Überprüfungsschleife für zukünftige Aktualisierungszyklen."

Richard Archdeacon, Advisory CISO, Cisco

Gut integrierte Technologie

„Wir wissen, dass eine moderne, gut integrierte IT zum Erfolg des Sicherheitsprogramms beiträgt. Hier sind einige Maßnahmen, die Sie ergreifen können, um Ihre Umgebung zu verbessern: Suchen Sie nach Cloud-basierten Sicherheitslösungen, untersuchen Sie Automatisierungsmöglichkeiten und stellen Sie sicher, dass die Beschaffungsanforderungen die Fähigkeit zur Technologieintegration umfassen."

Helen Patton, Advisory CISO, Cisco @CisoHelen

Rechtzeitige Incident Response

„Starke Mitarbeiter:innen verschaffen IR-Teams einen Vorteil. Dies ist ein guter Ausgangspunkt, muss aber in Verbindung mit anderen Elementen erfolgen. Wenn Unternehmen starke Mitarbeiter:innen, Prozesse und Technologien kombinieren, erhalten sie erweiterte Funktionen zur Bedrohungserkennung und -reaktion."

Dave Lewis, Advisory CISO, Cisco @gattaca

Genaue Bedrohungserkennung

„Wählen Sie die am besten qualifizierten Mitarbeiter:innen für Ihre SecOps-Teams aus, denn das ist wichtiger als ihre reine Anzahl. Wenn Sie nicht die nötigen Fachleute haben, können Sie durch Automatisierung die Lücken Ihrer Nachwuchskräfte schließen und Ergebnisse erzielen, die genauso stark sind, als wenn Sie erfahrenere Mitarbeiter:innen hätten."

Wendy Nather, Advisory CISO, Cisco @wendynather

Schnelle Disaster Recovery

„Die Ergebnisse in diesem Bericht unterstreichen den Wert der Funktionen für Business Continuity und Disaster Recovery. Führen Sie sie aber nicht isoliert von anderen Sicherheitsfunktionen aus. Die Priorisierung und Risikoeinstufung von Ressourcen sollte mit anderen Risikomanagementfunktionen geteilt werden. Ebenso sollten Sie Asset-Management und Threat-Management eng integrieren, um sicherzustellen, dass alle Teams nach demselben Leitfaden arbeiten."

Wolfgang Goerlich, Advisory CISO, Cisco @jwgoerlich

Informationen zu Cisco Secure

Cisco hat sich schon lange als weltweit führender Anbieter von Technologien etabliert, der das Internet am Laufen hält, und gleichzeitig ein offenes, integriertes Portfolio an Cybersicherheitslösungen entwickelt. Wir glauben, dass Sicherheitslösungen als Team agieren sollten. Sie sollten voneinander lernen. Sie sollten als koordinierte Einheit zuhören und antworten. Ist dies der Fall, wird die Sicherheit systematischer und effektiver. Unsere Kunden vertrauen uns seit Jahren als weltweit größter Anbieter von IT-Infrastruktur- und Netzwerkservices sowie als weltweit größtes Unternehmen im Bereich Cybersicherheit.

Cisco Secure basiert auf dem Prinzip „Nicht mehr, sondern bessere Sicherheit“. Es bietet einen schlanken, kundenorientierten Sicherheitsansatz, der eine einfache Bereitstellung, Verwaltung und Nutzung gewährleistet. Und natürlich muss alles zusammen funktionieren. Unsere Mitarbeiter:innen und Kunden stehen im Mittelpunkt unserer Arbeit stehen. Wir wissen, dass Kunden Komplexität und Rauschen reduzieren, auf ihre Sicherheit vertrauen und sich auf Ergebnisse konzentrieren möchten. Dies erfordert eine Vereinfachung, ohne dabei zu einfach zu sein. Unsere Cloud-native Plattform ist dabei ein großer Schritt nach vorne.

Wir bieten der Security-Community Zuverlässigkeit und das Vertrauen, dass sie mit der Cisco SecureX-Plattform jetzt und in Zukunft vor Bedrohungen geschützt ist. Wir unterstützen alle Fortune 100-Unternehmen mit der umfassendsten und am besten integrierten Plattform dabei, ihre Arbeit zu sichern – wo immer sie stattfindet. Weitere Informationen dazu, wie wir Erfahrungen vereinfachen, Erfolge beschleunigen und für Zukunftssicherheit sorgen, finden Sie unter cisco.com/go/secure.

Anhang: Demografische Daten der Umfrage

In diesem Anhang haben wir die demografischen Daten zu den 5.123 qualifizierten Antworten auf diese Umfrage zusammengestellt. Wir hoffen, dass dies dazu beiträgt, die Repräsentativität dieser Ergebnisse einzuordnen.

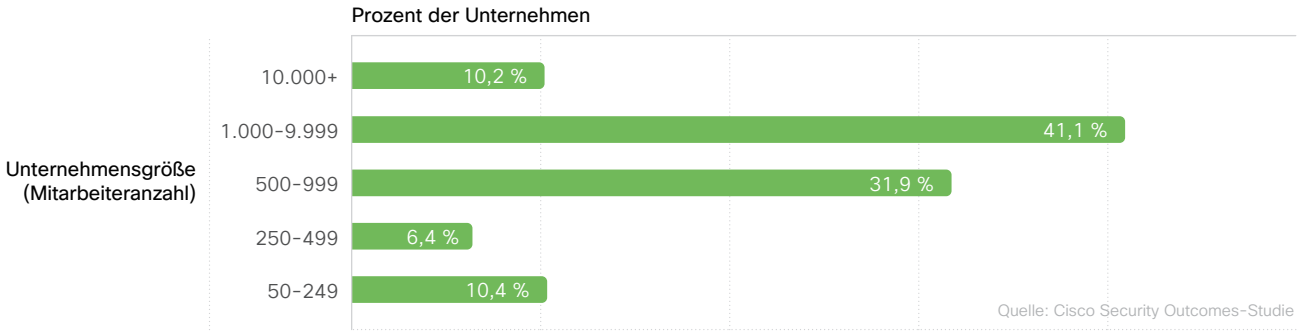


Abbildung A1: Anzahl der Mitarbeiter:innen in den teilnehmenden Unternehmen

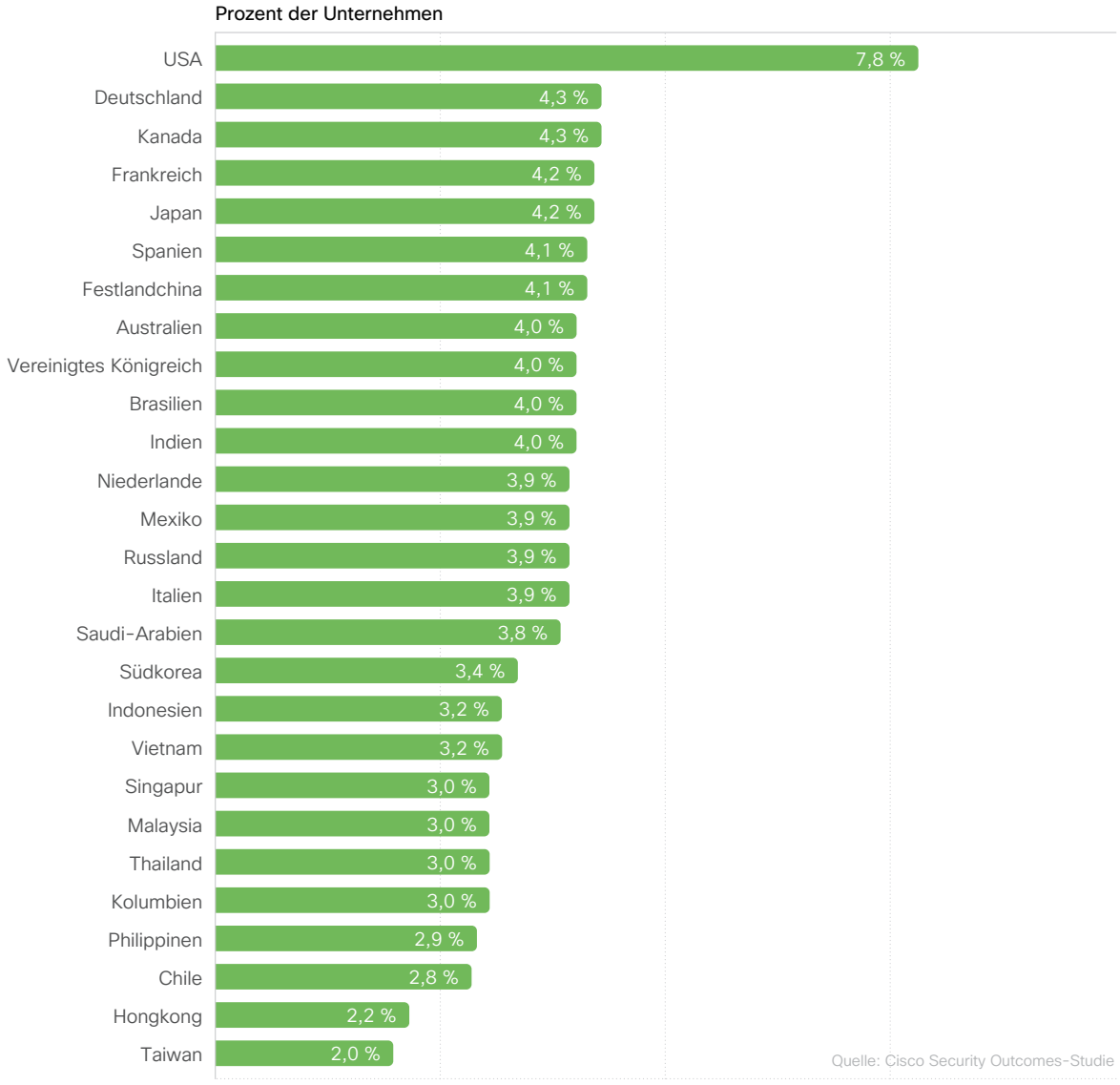


Abbildung A2: Märkte, in denen die teilnehmenden Unternehmen ihren Hauptsitz haben

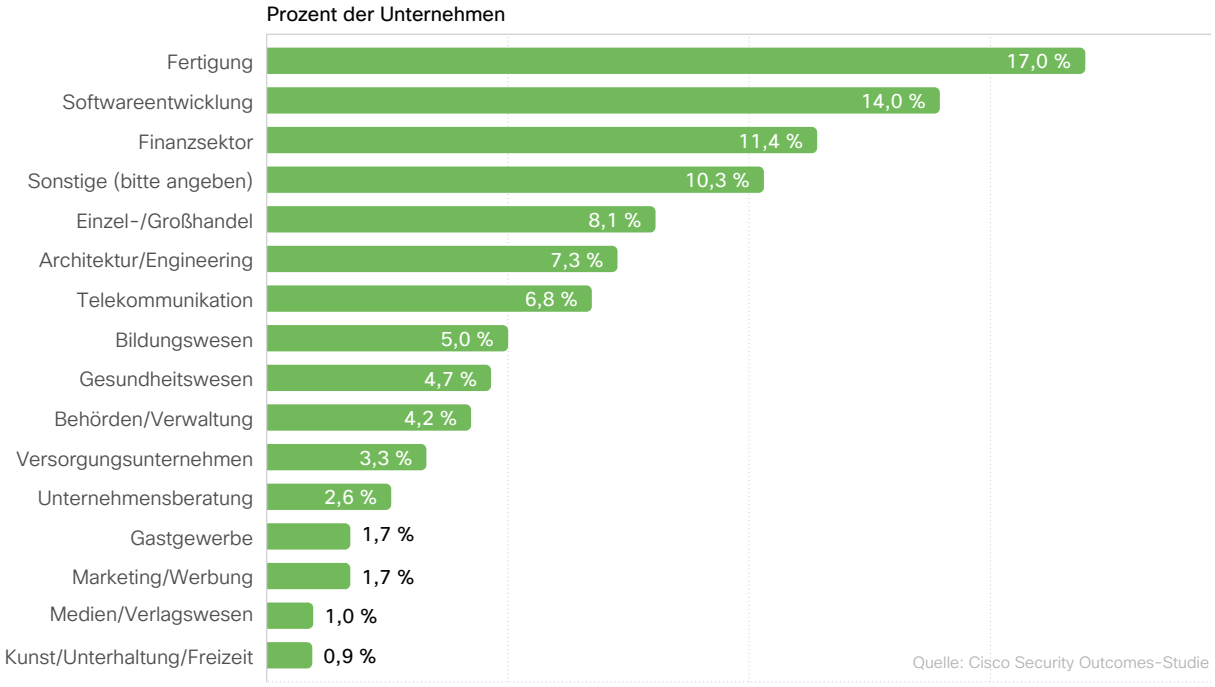


Abbildung A3: Branchen der teilnehmenden Unternehmen

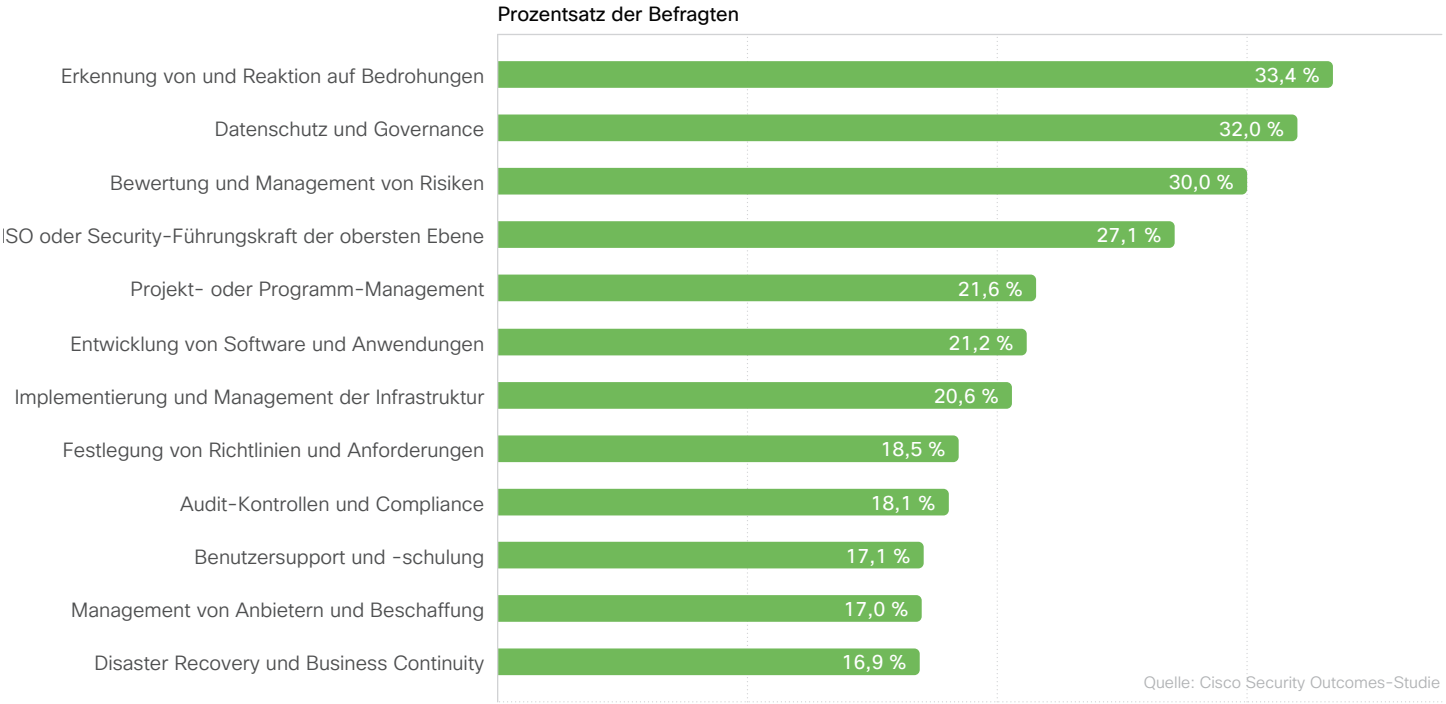


Abbildung A4: Hauptzuständigkeiten der Befragten

CISCO
SECURE

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

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

Hauptgeschäftsstelle Europa
Cisco Systems International BV
Amsterdam, Niederlande

Veröffentlicht im Dezember 2021