

Sicherheit jetzt und in der Zukunft

20 Überlegungen zur Cybersicherheit für 2020



Enthält
exklusive
Inhalte für
Deutschland.

Siehe Seite 23

Inhalt

Einleitung	3
20 Überlegungen zur Cybersicherheit für 2020	4
1. Wer sorgt in Ihrem Unternehmen für Unterstützung seitens der Führungskräfte und klare Fokussierung?	4
2. Wie können Sie entscheiden, welche Kennzahlen am wichtigsten sind? . . .	5
3. Welche primären Überlegungen stehen bei begrenzten Budgets hinter Ausgaben?	6
4. Wie sieht das optimale Verhältnis zwischen Ausgaben für die Überprüfung der Vertrauenswürdigkeit einerseits und für die Bedrohungserkennung andererseits aus?	8
5. Was können Sie an der Messung der geschäftlichen Auswirkungen von Sicherheitsverletzungen ablesen?	9
6. Warum werden heute mehr Sicherheitsverletzungen freiwillig offengelegt als jemals zuvor?	11
7. Können Sie die Vorteile der Zusammenarbeit zwischen Netzwerk und Sicherheit quantifizieren?	11
8. Welche Gründe sehen Sie außer Kostensenkungen für Outsourcing? . . .	11
9. Lohnt sich die Vorbereitung für Sie?	13
10. Wie wichtig ist das Patching für die Abwehr von Sicherheitsverletzungen?	13
11. Was verursacht Ausfallzeiten?	14
12. Wie schwierig ist es, mobile Mitarbeiter zu schützen?	14
13. Wie können Sie Zero Trust auf sichere Anwendungen ausweiten? . . .	14
14. Ist das Verteidigen der Netzwerkinfrastruktur immer noch eine Herausforderung?	16
15. Lassen sich die Auswirkungen der Anbieterkonsolidierung messen? . . .	17
16. Wo liegen bei Ihnen die Ursachen für Cybersicherheitsermüdung und -überdruß?	18
17. Welche Sicherheitsvorteile bietet das Hosting der Infrastruktur in der Cloud?	19
18. Welche Herausforderungen erwarten Sie für die Zukunft?	20
19. Wie viel Augenmerk sollten Sie auf die Reaktion auf Vorfälle legen? . . .	21
20. Was können Sie jetzt unternehmen, um Ihren Sicherheitsstatus zu verbessern?	22
Was in Deutschland anders ist.	23-25
Sicherheit jetzt und in der Zukunft	26
Über die Cisco Reihe zur Cybersicherheit	27

Einleitung

Sicherheitsverantwortliche begrüßen zwar das Unternehmenswachstum und die digitale Transformation, sehen sich dabei jedoch mit einer Vielzahl von Herausforderungen konfrontiert. Das wissen wir, weil Sie es uns sowohl in laufenden Gesprächen als auch im Rahmen unserer jährlichen Benchmark-Umfrage mitteilen. Einige Herausforderungen konzentrieren sich auf die Sicherheit, beispielsweise der Bedarf an mehr Transparenz oder Automatisierung oder auch das Streben nach einem unkomplizierteren Management und einfacheren Reaktionen. Einige hängen mit dem Erfolg des Unternehmens zusammen, beispielsweise das Ziel, Wachstum und Transformation zu unterstützen, unabhängig davon, welche Cloud-Anwendung benötigt wird oder welches Mobilgerät verwendet wird. Wieder andere Herausforderungen betreffen aktuelle Investitionen, die auch in Zukunft relevant bleiben, wenn sich Ihr Unternehmen verändert.

All das kommt zu den alltäglichen Routineanforderungen hinzu, die u. a. das Erkennen und Blockieren fortgeschrittener Bedrohungen umfassen. Es ist schwierig, raffinierte Angreifer und die ständig wachsende Angriffsfläche gleichzeitig im Griff zu behalten. Ihre Herausforderungen bestehen heute nicht mehr nur darin, das begrenzte Budget möglichst effektiv einzusetzen. Sie sind beispielsweise auch für den Erhalt der Markenreputation, das Vertrauen der Vorstandsmitglieder und Aktionäre und die Rekrutierung von Experten für die Taktiken, Techniken und Verfahren von Cyberangriffen verantwortlich.

Sie müssen Benutzern den benötigten Zugriff gewähren und parallel dazu diese Herausforderungen im Hinblick auf Sicherheit, Komplexität und Budget bewältigen. Außerdem müssen Sie den mit der Technologie verbundenen Aufwand senken, schwere Sicherheitsverletzungen verhindern, Bedrohungen aufspüren, bevor diese Ihr Netzwerk unterwandern und Daten ausschleusen, das Sicherheitsbudget intelligenter nutzen und mehr Kunden gewinnen.

Laut Weltwirtschaftsforum werden Cyberangriffe als das zweitgrößte globale Risiko (nach Finanzkrisen) wahrgenommen, das Führungskräfte in den hochentwickeltesten Volkswirtschaften beunruhigt.¹

Mit unserer sechsten jährlichen Umfrage unter 2.800 IT-Entscheidungssträgern aus 13 Ländern haben wir unsere jährliche Tradition fortgesetzt, uns Ihr Umfeld genau anzusehen, um wichtige Benchmark-Statistiken zu erstellen.² Wir haben auch ausführlich mit einem Gremium aus CISOs gesprochen, um die Ergebnisse zu analysieren und eine Liste mit 20 Überlegungen für 2020 zu erstellen. Der vorliegende Bericht enthält wertvolle Erkenntnisse und Daten, die Sie mit anderen Mitgliedern des Führungsteams oder mit dem Vorstand teilen können, um konkrete Empfehlungen zur Verbesserung des Sicherheitsstatus Ihres Unternehmens zu geben.

Da wir wissen, dass in dieser Branche nichts sicher ist außer der Unsicherheit, haben wir die Abschnittsüberschriften dieses Berichts als Fragen formuliert, die Sie sich vielleicht stellen, wenn Sie sich auf das kommende Jahr vorbereiten. Wenn diese Fragen bei Ihnen Anklang finden oder zu weiteren Fragen führen, können Sie uns unter security-reports@cisco.external.com Feedback zukommen lassen. In der Zwischenzeit hoffen wir, dass der Bericht Ihnen helfen wird, die Sicherheitsherausforderungen in diesem Jahr zu bewältigen.

Alle Berichte aus unserer Reihe zur Cybersicherheit finden Sie unter cisco.com/go/securityreports.

¹ „Diese Punkte betrachten CEOs auf der ganzen Welt als die größten Risiken für Unternehmen“, Weltwirtschaftsforum, 2019

² Die Umfragen wurden in Australien, Brasilien, China, Deutschland, Frankreich, Indien, Italien, Japan, Kanada, Mexiko, Spanien, den USA und dem Vereinigten Königreich durchgeführt.

20 Überlegungen zur Cybersicherheit für 2020

1. Wer sorgt in Ihrem Unternehmen für Unterstützung seitens der Führungskräfte und klare Fokussierung?

Im Laufe der Jahre haben wir in unserer Umfrage vier entscheidende Verfahren zur Förderung einer für beide Seiten vorteilhaften Beziehung zwischen Führungskräften und der Sicherheitsorganisation gemessen. In dieser Übung wird bewertet, wie sehr die Unternehmensführung hinter dem Thema Sicherheit steht. Gegenüber dem letzten Jahr zeigt sich ein leichter Abwärtstrend. Die Ergebnisse sehen wie folgt aus:

- 89 Prozent der Befragten geben an, **Sicherheit habe bei ihrer Unternehmensführung weiterhin hohe Priorität**. Gegenüber den vorangegangenen vier Jahren ist jedoch ein geringfügiger Rückgang (7 Prozent) zu verzeichnen.
- Der Anteil der Unternehmen, die **die Sicherheitsrollen und -zuständigkeiten innerhalb des Führungsteams** geklärt haben, schwankte in den letzten Jahren. In diesem Jahr sind es 89 Prozent. Angesichts der zunehmenden Sichtbarkeit der Cybersicherheit und des dringenden Bedarfs an Sicherheitsverantwortliche auf den obersten Unternehmensebenen ist der Klärung von Rollen und Verantwortlichkeiten weiterhin eine hohe Bedeutung beizumessen.
- Die Einbeziehung von Cyberrisikobewertungen in die allgemeinen Risikobewertungsprozesse ist gegenüber dem Vorjahr um 5 Prozent zurückgegangen, weist jedoch immer noch einen hohen Wert auf: 91 Prozent der Befragten gaben an, so zu verfahren.
- Der Anteil der Führungsteams, die klare Kennzahlen zur Bewertung der Effektivität von Sicherheitsprogrammen festlegen, ist zwar gegenüber dem letzten Jahr um 6 Prozent gesunken, liegt aber immer noch bei 90 Prozent der Befragten.

Innerhalb von vier Jahren ist dieser Wert leicht zurückgegangen, was auf Folgendes hindeuten kann: 1) Der Umfang der Sicherheitsverantwortung ändert sich. 2) Die Kommunikation mit dem Führungsteam ist nicht mehr so klar wie früher. 3) Die Geschäftsleitung setzt andere geschäftliche Prioritäten. 4) CISOs und Führungskräfte bewerten ihre Kennzahlen neu.

Obwohl die Zahlen gesunken sind, liegen sie immer noch sehr hoch. Vielleicht ist dies darauf zurückzuführen, dass die Sicherheit jetzt zwar in den Betrieb eingebunden ist, dafür aber mehr Unterstützung seitens der Unternehmensführung erfordert. **Die Tatsache, dass die Zahlen immer noch sehr hoch sind, deutet auf eine anhaltend starke Beziehung zwischen Führungskräften und Sicherheitsexperten hin.**

Das Führungsteam ist bei jedem Unternehmen anders zusammengesetzt, und es gibt viele verschiedene Führungsstile. Die Rolle des CISO besteht darin, Gespräche zu führen und die Geschäftsbereiche ins Boot zu holen, indem er den Mehrwert gut konzipierter Sicherheit für das Unternehmen aufzeigt.

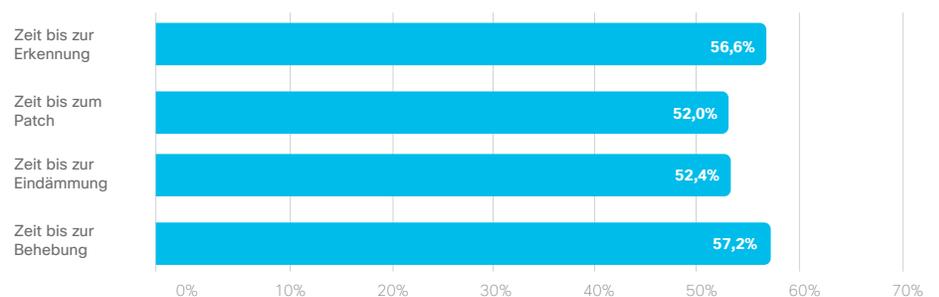
Mick Jenkins MBE, CISO der Brunel University London

2. Wie können Sie entscheiden, welche Kennzahlen am wichtigsten sind?

Wie bereits erwähnt gaben 90 Prozent der Befragten an, das Führungsteam ihres Unternehmens habe für die Messung der Effektivität seines Sicherheitsprogramms klare Kennzahlen festgelegt. Das Festlegen klarer Kennzahlen ist ein integraler Bestandteil eines Sicherheits-Frameworks. Dennoch ist es keine einfache Aufgabe, sich über mehrere Führungskräfte und Sicherheitsteams hinweg darüber einig zu werden, wie betriebliche Verbesserungen und Sicherheitsergebnisse gemessen werden sollen.

Die von uns befragten IT-Entscheidungsträger bewerteten die **Zeit bis zur Erkennung als die wichtigste Leistungskennzahl (KPI). Bei der Berichterstattung an die Mitglieder des Führungsteams oder den Vorstand wird jedoch die Zeit bis zur Behebung als ebenso wichtig erachtet**, da sie einen Anhaltspunkt für die Gesamtauswirkungen liefert, wobei Folgendes miteinfließen kann: Systemausfallzeit, betroffene Datensätze, Kosten der Untersuchung, Umsatzeinbußen, Kundenabwanderung, entgangene Geschäftschancen, Ex-Pocket-Ausgaben (Abbildung 1). Es kann sich auch um eine Näherungskennzahl für die Gesamteffektivität der IT-Abteilung handeln, da die Behebung viel Zusammenarbeit über mehrere Abteilungen hinweg erfordern kann.

Abbildung 1: Zum Melden einer ernststen Sicherheitsverletzung an die Mitglieder des Führungsteams oder den Vorstand verwendete Kennzahlen. (N=2.800) Die Prozentsätze wurden gerundet.

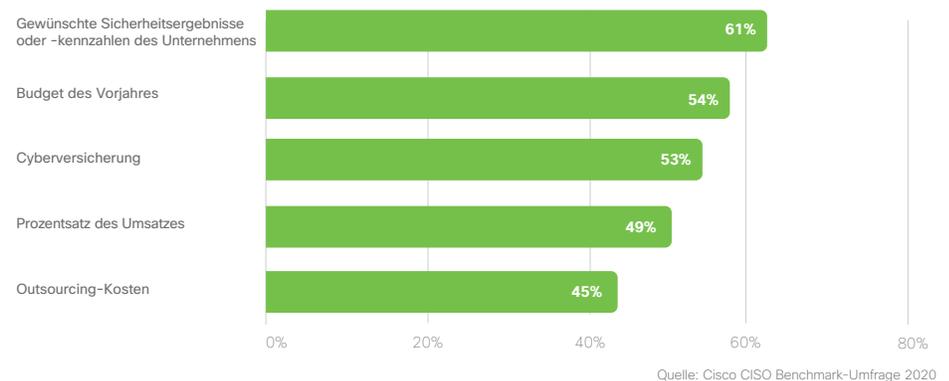


Quelle: Cisco CISO Benchmark-Umfrage 2020

3. Welche primären Überlegungen stehen bei begrenzten Budgets hinter Ausgaben?

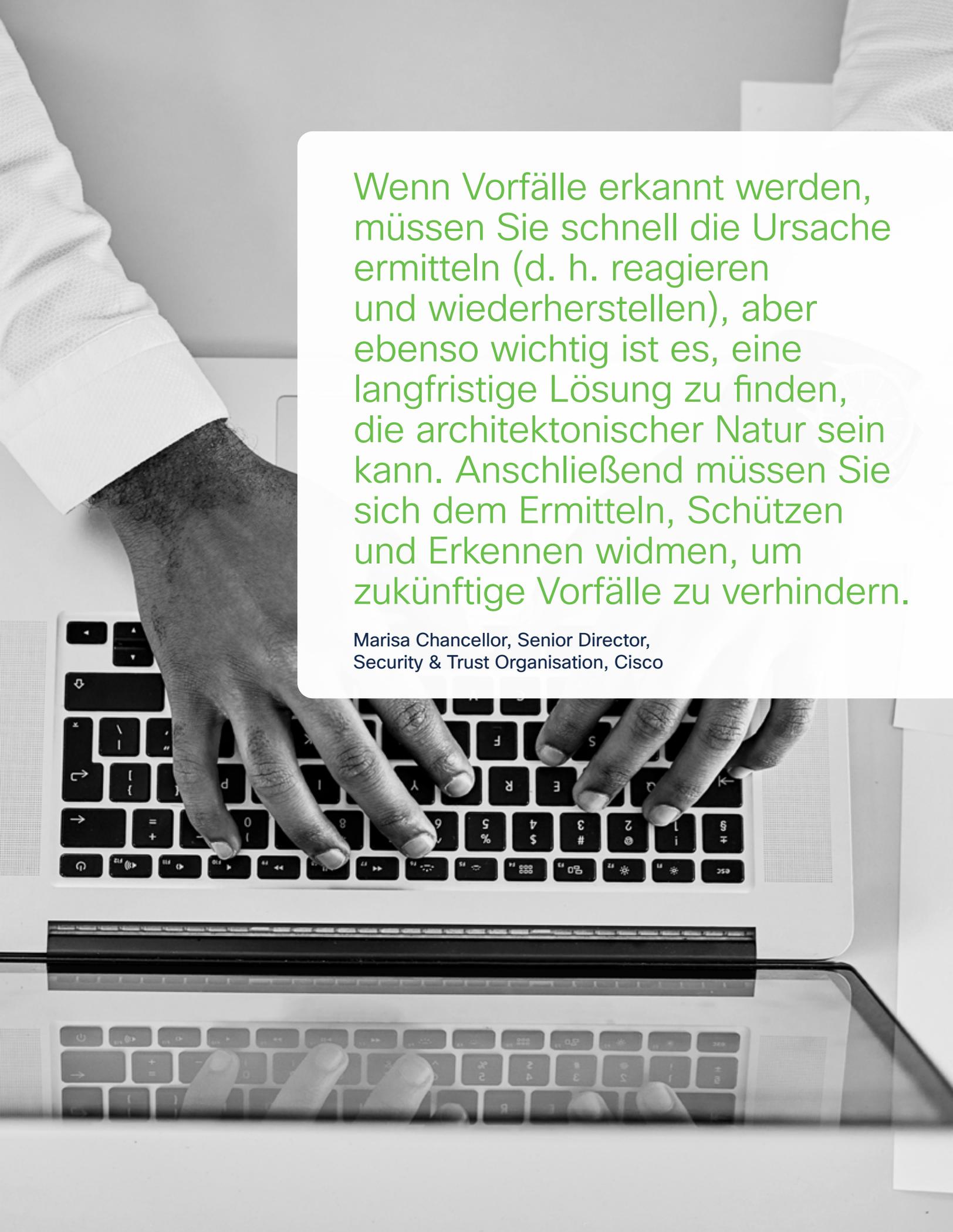
In den meisten Fällen haben wir gehört, dass die Verteilung von Sicherheitsausgaben anhand von ergebnisbasierten Zielen und Kennzahlen erfolgen sollte. 61 Prozent der Befragten nutzen diese Planungsmethode – eine Steigerung um 10 Prozent gegenüber dem Vorjahr und ein ermutigender Trend (Abbildung 2).

Abbildung 2: Welche Optionen nutzen Unternehmen, um die Ausgaben für die Sicherheit festzulegen und/oder zu kontrollieren? (N=2.799) Die Prozentsätze wurden gerundet.



Der Prozentsatz des Umsatzes und die Outsourcing-Kosten stehen auf der Liste der Faktoren zur Festlegung von Sicherheitsbudgets ganz unten. 54 Prozent der Befragten richten sich bei ihren Ausgaben nach dem Budget des Vorjahres. Auch wenn dies nicht wie eine präzise Möglichkeit zur Quantifizierung von Sicherheitskosten erscheint – insbesondere da die durchschnittlichen globalen Kosten einer Datensicherheitsverletzung (3,92 Mio. USD) selten berücksichtigt werden –, wird sich die Budgetprognose wahrscheinlich wenig ändern, wenn das Budget Jahr für Jahr gleich bleibt oder die SaaS-Abonnementkosten planbar sind.³

³ [2019 Cost of a Data Breach Report](#), Ponemon Institute



Wenn Vorfälle erkannt werden, müssen Sie schnell die Ursache ermitteln (d. h. reagieren und wiederherstellen), aber ebenso wichtig ist es, eine langfristige Lösung zu finden, die architektonischer Natur sein kann. Anschließend müssen Sie sich dem Ermitteln, Schützen und Erkennen widmen, um zukünftige Vorfälle zu verhindern.

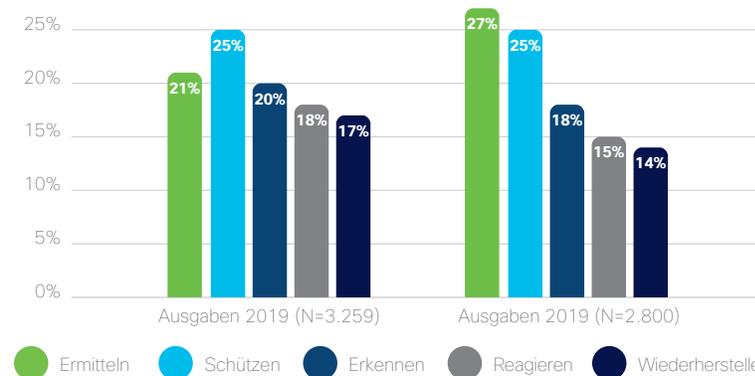
Marisa Chancellor, Senior Director,
Security & Trust Organisation, Cisco

4. Wie sieht das optimale Verhältnis zwischen Ausgaben für die Überprüfung der Vertrauenswürdigkeit einerseits und für die Bedrohungserkennung andererseits aus?

Bei der Untersuchung der Verwendung von Sicherheitsbudgets haben wir die Teilnehmer zu fünf Kategorien (Ermitteln, Schützen, Erkennen, Reagieren und Wiederherstellen) befragt, die den Lebenszyklus der Cybersicherheitsabwehr und des Managements von Sicherheitsverletzungen beschreiben.

- **In der Kategorie „Ermitteln“** ist der Anteil der Ausgaben von 21 Prozent im Jahr 2019 auf 27 Prozent im Jahr 2020 gestiegen.
- **Bei „Schützen“ und „Erkennen“** sind die Anteile mit 25 Prozent bzw. 18 Prozent im Wesentlichen gleich geblieben.
- **Die Ausgaben in den Kategorien „Reagieren“ und „Wiederherstellen“** sind im gleichen Zeitraum leicht zurückgegangen auf 15 Prozent bzw. 14 Prozent.

Abbildung 3: Sicherheitsausgaben nach Lebenszyklusategorie. Die Prozentsätze wurden gerundet.



Quelle: Cisco CISO Benchmark-Umfrage 2020

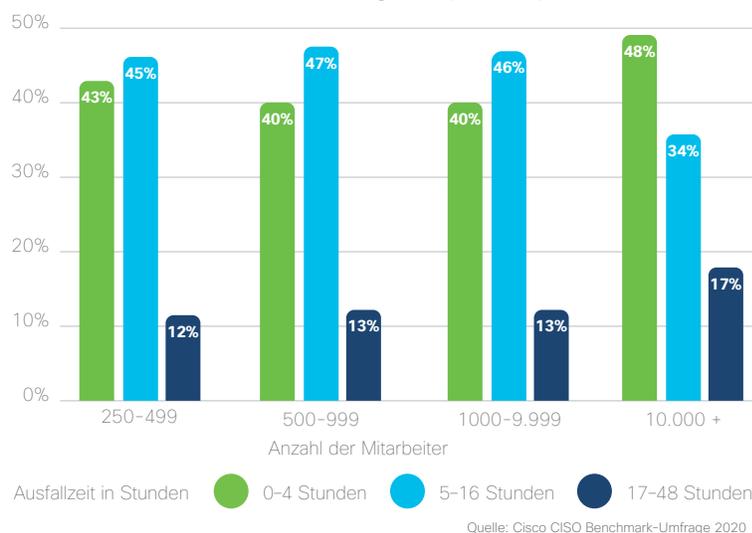
Dieser Trend zeigt, dass **Unternehmen mehr für Prävention ausgeben und eine weniger reaktive Cybersicherheitshaltung an den Tag legen**. Große Unternehmen versuchen immer, die richtige Balance zwischen Proaktivität, Reaktionsschnelligkeit und Ausfallsicherheit zu finden, wobei das Pendel mal in die eine und mal in die andere Richtung ausschlägt. Im vergangenen Jahr haben sich die Unternehmen möglicherweise auf die Grundlagen (Inventar, Ermittlung usw.) konzentriert. Theoretisch sollte das richtige Maß an Ausgaben in den Kategorien „Ermitteln“, „Schützen“ und „Erkennen“ auch dazu führen, dass bei „Reagieren“ und „Wiederherstellen“ weniger Ausgaben anfallen.

5. Was können Sie an der Messung der geschäftlichen Auswirkungen von Sicherheitsverletzungen ablesen?

In unserer Umfrage haben wir nach verschiedenen Auswirkungen von Sicherheitsverletzungen gefragt, beispielsweise Ausfallzeiten, betroffene Datensätze und Finanzen.

In welchem Umfang verzeichnen Unternehmen Ausfallzeiten bei schweren Sicherheitsverletzungen? Wir haben Unternehmen unterschiedlicher Größe miteinander verglichen, wobei die Ergebnisse insgesamt sehr ähnlich waren. Große Unternehmen (mindestens 10.000 Mitarbeiter) haben mit größerer Wahrscheinlichkeit weniger Ausfallzeit (0-4 Stunden), da sie wahrscheinlich über mehr Ressourcen für die Reaktion und Wiederherstellung verfügen. Bei kleinen bis mittelgroßen Unternehmen beträgt die Zeit bis zur Wiederherstellung meist 5 bis 16 Stunden. Katastrophale Ausfallzeiten von 17 bis 48 Stunden treten in Unternehmen aller Größen ähnlich selten auf (Abbildung 4).

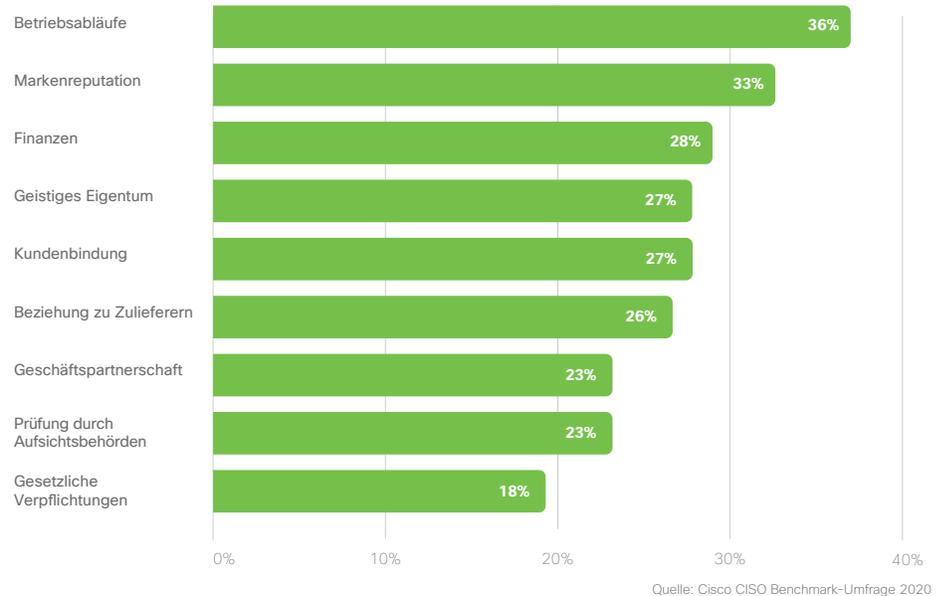
Abbildung 4: Bei der schwersten Sicherheitsverletzung, die im vergangenen Jahr bewältigt wurde, bestand ein Zusammenhang zwischen der Systemausfallzeit in Stunden und der Unternehmensgröße. (N=2.265) Die Prozentsätze wurden gerundet.



Der Anteil der Unternehmen, bei denen mehr als 100.000 Datensätze von der schwersten Datensicherheitsverletzung betroffen waren, ist von 15 Prozent im vergangenen Jahr auf über 19 Prozent in diesem Jahr gestiegen.

Darüber hinaus kann sich, wie Abbildung 5 zeigt, eine schwere Sicherheitsverletzung auf neun kritische Bereiche eines Unternehmens auswirken. **Die am stärksten betroffenen Bereiche des Unternehmens waren die Betriebsabläufe und die Markenreputation**, gefolgt von Finanzen, geistigem Eigentum und Kundenbindung.

Abbildung 5: Prozentsätze der Befragten, die von einer Sicherheitsverletzung beeinträchtigte Unternehmensbereiche angeben. (N=2.121) Die Prozentsätze wurden gerundet.



Mit Blick auf die vergangenen Jahre zeigt sich, dass der Anteil der Befragten, bei denen durch schwere Sicherheitsverletzungen die Markenreputation gelitten hat, **innerhalb von drei Jahren von 26 Prozent auf 33 Prozent gestiegen ist**. Der Anteil der Befragten, die Auswirkungen auf die Betriebsabläufe melden, bewegt sich dagegen konstant zwischen 36 und 38 Prozent. Der Anteil der Befragten mit Auswirkungen auf die Finanzen ist in den letzten drei Jahren nur um einen Prozentpunkt pro Jahr zurückgegangen und somit auch relativ stabil geblieben. Da die Auswirkungen auf die Marke insgesamt zunehmen, **ist es von entscheidender Bedeutung, die Planung der Krisenkommunikation in Ihren Gesamtplan zur Reaktion auf Vorfälle einzubeziehen**.

6. Warum werden heute mehr Sicherheitsverletzungen freiwillig offengelegt als jemals zuvor?

Mit 61 Prozent liegt der Anteil der Befragten, die im vergangenen Jahr freiwillig eine Sicherheitsverletzung offengelegt haben, auf dem höchsten Stand der letzten vier Jahre. Dies zeigt, dass Unternehmen insgesamt proaktiv Sicherheitsverletzungen melden, vielleicht als Folge neuer Rechtsvorschriften – oder möglicherweise aufgrund eines erhöhten sozialen Bewusstseins und des Wunsches, das Vertrauen der Kunden aufrechtzuerhalten.

Positiv ist zu bewerten, dass der Anteil der freiwilligen Offenlegungen bei Unternehmen, die eine Sicherheitsverletzung mit einer Dauer von mehr als 17 Stunden hatten, mehr als doppelt so hoch war wie der Anteil der unfreiwilligen oder nur wegen Meldevorschriften erfolgten Offenlegungen.

Bei mehr als der Hälfte (51 Prozent) aller Sicherheitsverletzungen geraten Unternehmen in die Defensive, weil ein solcher Vorfall von großem öffentlichem Interesse ist. Doch während die Anforderungen der behördlichen Meldepflichten gestiegen sind, ist der Anteil der unfreiwilligen Offenlegungen mit etwas mehr als einem Viertel (27 Prozent) weitgehend gleich geblieben. **Immerhin 61 Prozent der Befragten sind inzwischen der Meinung, dass ihre Glaubwürdigkeit zunimmt, wenn sie eine schwere Sicherheitsverletzung freiwillig offenlegen, und dass sie damit ihren Markenruf bewahren können.**

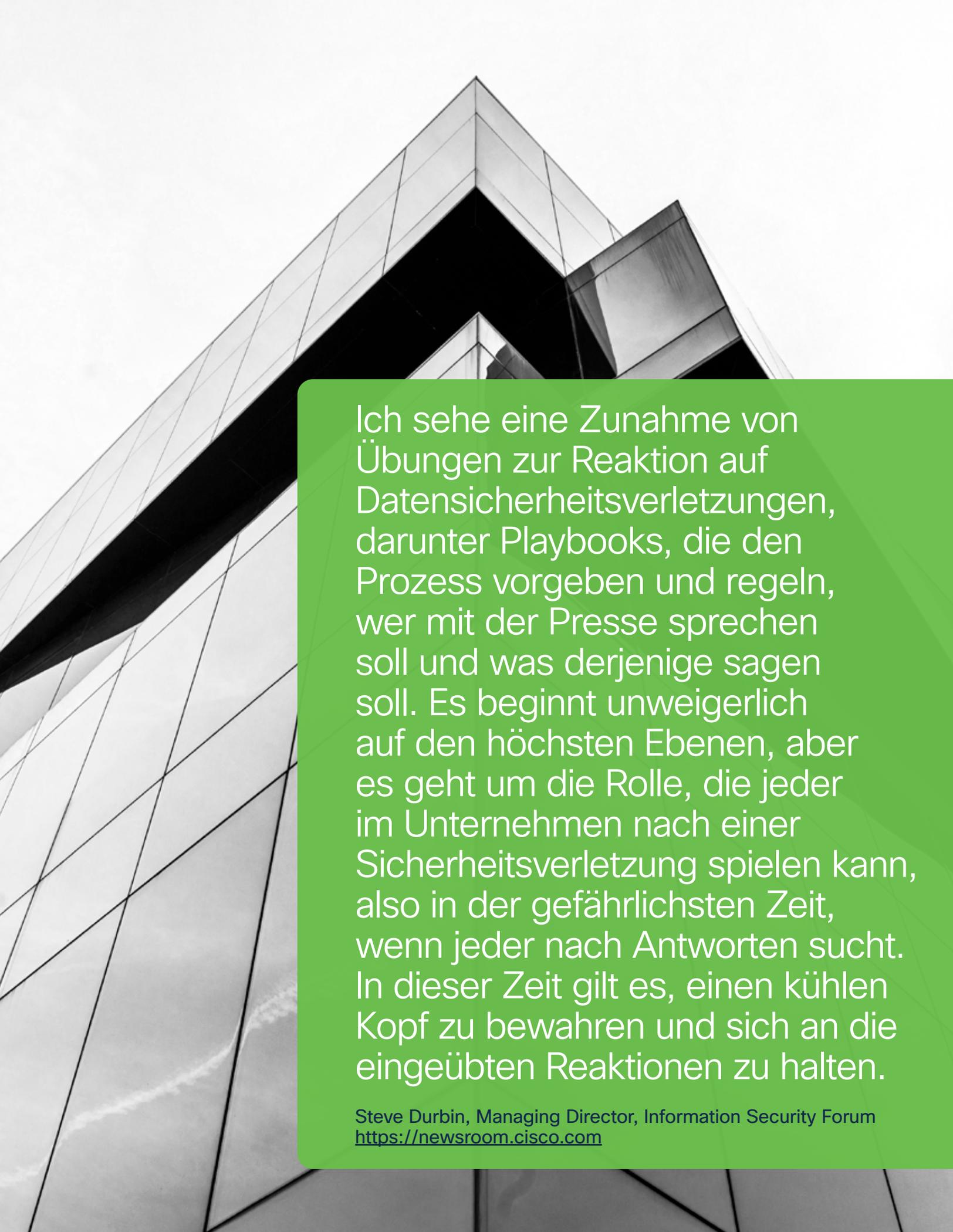
7. Können Sie die Vorteile der Zusammenarbeit zwischen Netzwerk und Sicherheit quantifizieren?

Die Zusammenarbeit zwischen den **Netzwerk- und Sicherheitsteams ist nach wie vor sehr gängig**: Mehr als 91 Prozent der Befragten haben in der diesjährigen Umfrage angegeben, sehr oder extrem kollaborativ zu sein. Auch die **Endpunkt- und Sicherheitsteams arbeiten mit 87 Prozent weiterhin stark zusammen**. Trotz des Rückgangs um einige Prozentpunkte in diesen Bereichen deutet der allgemeine Trend darauf hin, dass Sie weniger wahrscheinlich in Silos arbeiten.

8. Welche Gründe sehen Sie außer Kostensenkungen für Outsourcing?

Im Vergleich zum Bericht aus dem vergangenen Jahr hat das Outsourcing deutlich zugenommen, was möglicherweise auf einen historischen Trend hindeutet, da die Anbieterlandschaften zu komplex werden, um sie intern zu verwalten. Interessanterweise erwarten die Unternehmen nach eigenen Angaben, dass ihr Outsourcing in Zukunft abnehmen wird.

Unsere Befragten setzen aus vielerlei Gründen auf Outsourcing – es geht nicht nur um die Kosten. Die Kosteneffizienz als Grund liegt mit 55 Prozent nur knapp vorn. Dicht dahinter folgt das Argument, dass Sicherheitsteams zeitigere Reaktionen auf Vorfälle fordern (53 Prozent).



Ich sehe eine Zunahme von Übungen zur Reaktion auf Datensicherheitsverletzungen, darunter Playbooks, die den Prozess vorgeben und regeln, wer mit der Presse sprechen soll und was derjenige sagen soll. Es beginnt unweigerlich auf den höchsten Ebenen, aber es geht um die Rolle, die jeder im Unternehmen nach einer Sicherheitsverletzung spielen kann, also in der gefährlichsten Zeit, wenn jeder nach Antworten sucht. In dieser Zeit gilt es, einen kühlen Kopf zu bewahren und sich an die eingeübten Reaktionen zu halten.

Steve Durbin, Managing Director, Information Security Forum
<https://newsroom.cisco.com>

9. Lohnt sich die Vorbereitung für Sie?

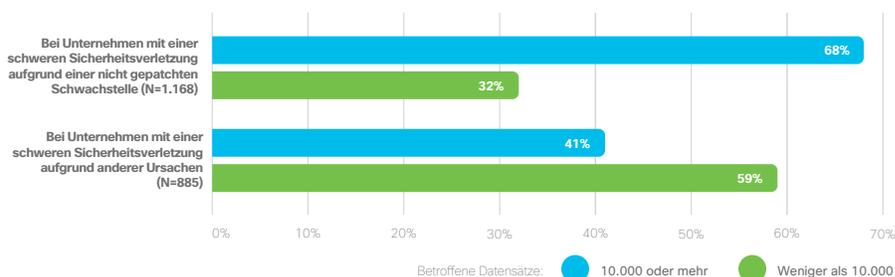
Aus den Antworten auf die Frage, welche Sicherheitsverfahren oder -richtlinien für das Unternehmen gelten, konnten wir schließen, dass **die mit schweren Sicherheitsverletzungen verbundenen Kosten bei den Befragten, die die unten aufgeführten Punkte beachten, häufig niedriger ausfallen**. Mit anderen Worten: Wenn die folgenden sechs Verfahren mit Ihrem Sicherheitsprogramm übereinstimmen, bleiben die Kosten bei Sicherheitsverletzungen in Ihrem Unternehmen mit höherer Wahrscheinlichkeit unter 100.000 US-Dollar.

- Wir prüfen und verbessern unsere Sicherheitsvorkehrungen regelmäßig, formell und strategisch.
- Die Verbindungsaktivität im Netzwerk wird regelmäßig geprüft, um sicherzustellen, dass Sicherheitsmaßnahmen planmäßig funktionieren.
- Sicherheit ist gut in die Ziele unseres Unternehmens und unsere Geschäftsprozesse integriert.
- Sicherheitsvorfälle untersuchen wir routinemäßig und systematisch.
- Unsere Sicherheitstechnologien sind gut integriert und arbeiten effizient zusammen.
- Unsere Funktionen zur Erkennung und Blockierung von Sicherheitsrisiken sind stets auf dem neuesten Stand.

10. Wie wichtig ist das Patching für die Abwehr von Sicherheitsverletzungen?

Ein wichtiger Aspekt für 2020 ist, dass 46 Prozent der Unternehmen (gegenüber 30 Prozent im Bericht vom letzten Jahr) einen Vorfall hatten, der durch eine nicht gepatchte Schwachstelle verursacht wurde. Darüber hinaus verzeichneten diejenigen **Unternehmen, bei denen im vergangenen Jahr eine schwere Sicherheitsverletzung aufgrund einer nicht gepatchten Schwachstelle aufgetreten war, höhere Datenverluste** (Abbildung 6). Beispielsweise haben 68 Prozent der Unternehmen mit Sicherheitsverletzungen wegen einer nicht gepatchten Schwachstelle im vergangenen Jahr mindestens 10.000 Datensätze verloren. Von denjenigen, die laut eigenen Angaben aufgrund anderer Ursachen eine Sicherheitsverletzung hatten, haben im selben Zeitraum nur 41 Prozent 10.000 Datensätze oder mehr verloren.

Abbildung 6: Die Umfrageteilnehmer wurden gefragt, ob sie im letzten Jahr einen Sicherheitsvorfall erlebt hätten, der auf eine nicht gepatchte Schwachstelle oder auf andere Ursachen zurückzuführen war. Sie sollten auch angeben, wie viele Datensätze sie verloren hatten. (N=2.053) Die Prozentsätze wurden gerundet.



Quelle: Cisco CISO Benchmark-Umfrage 2020

Es ist allgemein bekannt, dass das Patching schwierig sein kann und unter Umständen zu Störungen führt. Diese Ergebnisse zeigen jedoch, dass die Implementierung einer Mindestbasisrichtlinie für die zuletzt veröffentlichten Patches einen konkreten ROI verspricht. **Unternehmen sollten die Informationen zum Gerätebestand in ihrer Umgebung aktuell halten und eine Risikoanalyse für fehlende Patches durchführen. Danach können sie einen Change Management-Prozess erstellen, um die Versionskontrolle und -dokumentation durchzusetzen.**

11. Was verursacht Ausfallzeiten?

Wie bereits erwähnt sollten die Befragten ihre Ausfallzeit in Stunden angeben. Als häufigste Ursache für Ausfallzeit wurde Malware genannt, gefolgt von schädlichem Spam. Interessanterweise variiert die dritte Ursache je nach Dauer der Ausfallzeit. Bei Sicherheitsverletzungen mit Ausfallzeiten zwischen 0 und 4 Stunden ist Phishing die dritthäufigste Ursache. Bei Ausfallzeiten zwischen 4 und 24 Stunden ist es Spyware. Bei allem über 24 Stunden ist es [Ransomware](#).

Bezeichnenderweise trifft Ransomware alle Unternehmen gleichermaßen: Sie war bei kleinen wie auch bei großen Unternehmen die schwerwiegendste Bedrohung in Bezug auf Ausfallzeit. Die langen damit verbundenen Ausfallzeiten sind möglicherweise auf die eingehenden Untersuchungen zurückzuführen, die erforderlich sind, um den Schaden zu bewerten, zu versuchen, Sicherungen wiederherzustellen und die Angriffsvektoren zu beheben.

Wenn Sie an weiteren Informationen zum Umgang mit Angriffen verschiedener Art interessiert sind, abonnieren Sie den [Threat-Intelligence-Blog von Talos](#).

12. Wie schwierig ist es, mobile Mitarbeiter zu schützen?

Wir haben unsere Umfrageteilnehmer gebeten, uns mitzuteilen, wie schwierig es ist, verschiedene Aspekte ihrer Infrastruktur zu schützen. **Mehr als die Hälfte (52 Prozent) der Befragten sagte uns, dass mobile Geräte inzwischen sehr oder extrem schwierig zu schützen sind.** Dieser Aspekt hat damit das Benutzerverhalten überholt, das im letzten Bericht noch die größte Herausforderung war.

Mit einem [Zero-Trust-Framework](#) können Sie alle Personen und Geräte identifizieren und überprüfen, die versuchen, auf Ihre Infrastruktur zuzugreifen. Zero Trust ist ein pragmatisches und zukunftsicheres Framework, das dazu beitragen kann, effektive Sicherheit in Ihrer gesamten Architektur zu gewährleisten – für Mitarbeiter, Workloads und Arbeitsumgebungen.

Ein Zero-Trust-Framework erfüllt unter anderem diese drei Kriterien:

- Die Benutzer sind bekannt und authentifiziert.
- Die Geräte wurden überprüft und als adäquat eingestuft.
- Die Benutzer haben in Ihrer Umgebung nur beschränkten Zugriff.

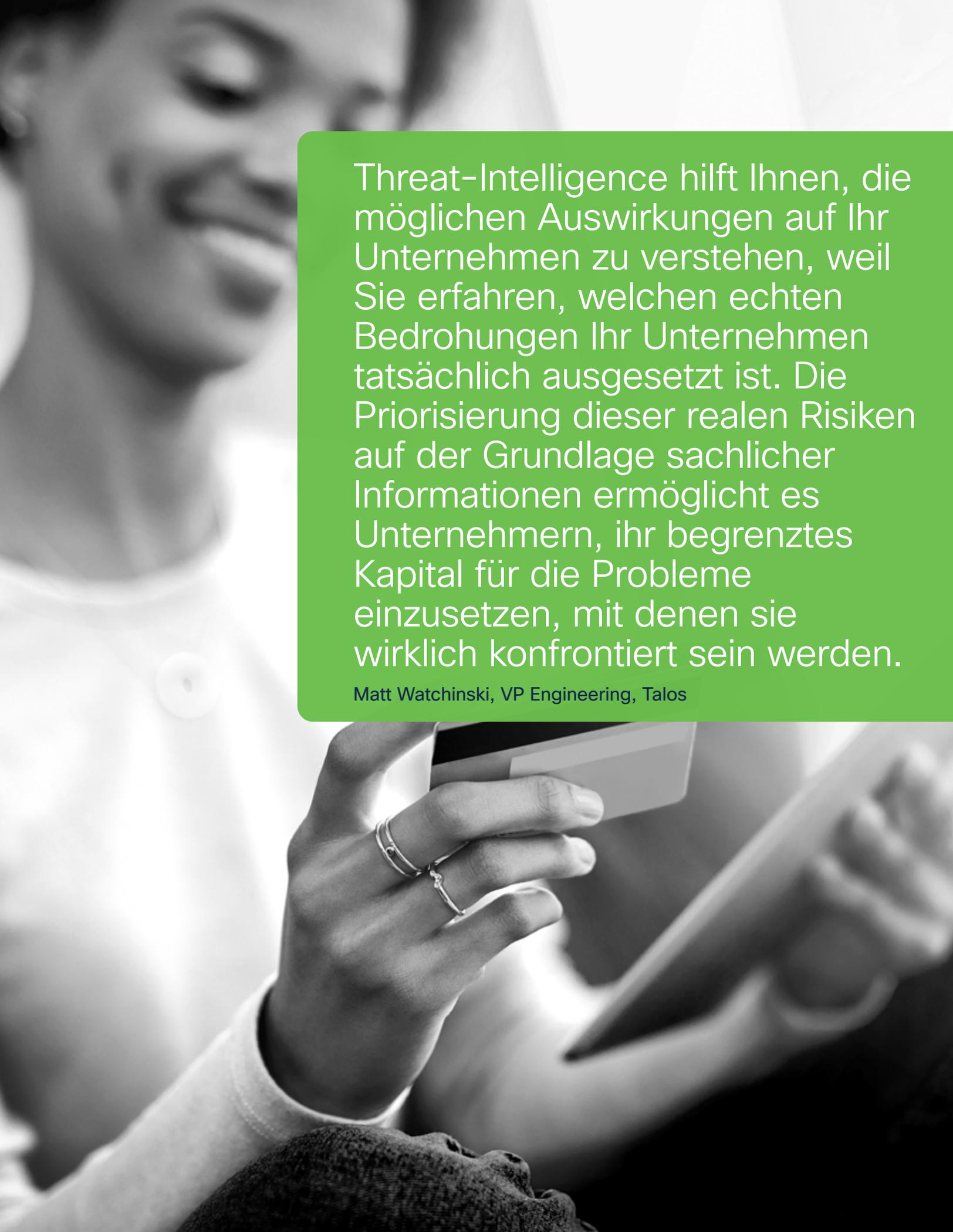
Durch Zero Trust entfällt ein Großteil des Rätselratens, wenn Sie Ihre Infrastruktur mitsamt Mobilgeräten vor allen potenziellen Bedrohungen schützen möchten.

13. Wie können Sie Zero Trust auf sichere Anwendungen ausweiten?

Bei der Workload-Sicherheit geht es darum, alle Benutzer- und Geräteverbindungen im gesamten Netzwerk zu sichern. Ein Zero-Trust-Framework kann die Abhängigkeiten innerhalb von und zwischen Datenbanken und Anwendungen identifizieren, damit Sie Mikrosegmentierung anwenden und die Ausbreitung von Bedrohungen verhindern können.

41 Prozent der befragten Unternehmen halten Rechenzentren für sehr oder extrem schwierig zu schützen. 39 Prozent geben an, große Schwierigkeiten mit dem Schützen von Anwendungen zu haben. Der problematischste Aspekt sind in der Public Cloud gespeicherte Daten: 52 Prozent der Befragten empfinden es als sehr oder extrem schwierig, diese zu schützen.

Ein Zero-Trust-Framework bietet Ihnen Einblick in die laufenden – und die kritischen – Vorgänge, indem Richtlinien im gesamten Netzwerk ermittelt und durchgesetzt werden. Dank kontinuierlicher Überwachung und Reaktion auf Anzeichen für Bedrohungen (Indicators of Compromise) werden Sie außerdem über Richtlinienverstöße benachrichtigt.



Threat-Intelligence hilft Ihnen, die möglichen Auswirkungen auf Ihr Unternehmen zu verstehen, weil Sie erfahren, welchen echten Bedrohungen Ihr Unternehmen tatsächlich ausgesetzt ist. Die Priorisierung dieser realen Risiken auf der Grundlage sachlicher Informationen ermöglicht es Unternehmern, ihr begrenztes Kapital für die Probleme einzusetzen, mit denen sie wirklich konfrontiert sein werden.

Matt Watchinski, VP Engineering, Talos

14. Ist das Verteidigen der Netzwerkinfrastruktur immer noch eine Herausforderung?

Die Private Cloud-Infrastruktur ist eine der größten Sicherheitsherausforderungen für Unternehmen. (50 Prozent der Unternehmen empfinden sie als sehr oder extrem schwierig zu schützen.) Die Netzwerkinfrastruktur erachten 41 Prozent als sehr oder extrem schwierig zu schützen.

Hier bietet ein Zero-Trust-Framework einen Mehrwert. Sie profitieren damit von softwarebasierter Zugriffskontrolle für alle Verbindungen innerhalb Ihrer Anwendungen sowie in der gesamten Multi-Cloud-Umgebung. Diese Kontrolle richtet sich nicht nach dem Standort, sondern nach dem Benutzer-, Geräte- und Anwendungskontext. Mit diesem Modell können Sie Risiken unabhängig von Verteilung und Standort in Ihrer gesamten Infrastruktur minimieren, erkennen und darauf reagieren. Unten sind die definierten Framework-Phasen zum Entwickeln eines Modells für Zero-Trust-Sicherheitsreife aufgeführt.

Entwickeln eines Modells für Zero-Trust-Sicherheitsreife

Wir bei Cisco setzen fünf Transformationsschritte ein, die unsere Kunden als Struktur übernehmen, um ein **Zero-Trust-Framework** für ihr Unternehmen zu implementieren:

Phase 1: Verfügen Sie über eine klare IAM-Strategie (Identity and Access Management, Identitäts- und Zugriffsmanagement), die auf Ihre Geschäftsanforderungen abgestimmt ist und zur vollständigen Implementierung und Integration einer MFA-Lösung (Multi-Factor Authentication, mehrstufige Authentifizierung) mit Unterstützung durch risikobasierte Richtlinien geführt hat?

Phase 2: Verfügen Sie über aktuelle Bestandsinformationen, bei denen zwischen verwalteten und nicht verwalteten Geräten unterschieden wird und die als Teil einer integrierten IT- und Sicherheitsfunktion gründlich überprüft werden?

Phase 3: Verfügen Sie über eine Richtlinie für vertrauenswürdige Geräte, die Benutzer auffordert, ihre Geräte innerhalb eines verwalteten Prozesses gegen gemessene Schwachstellen zu aktualisieren, und über Berichte zu nicht richtlinienkonformen Geräten?

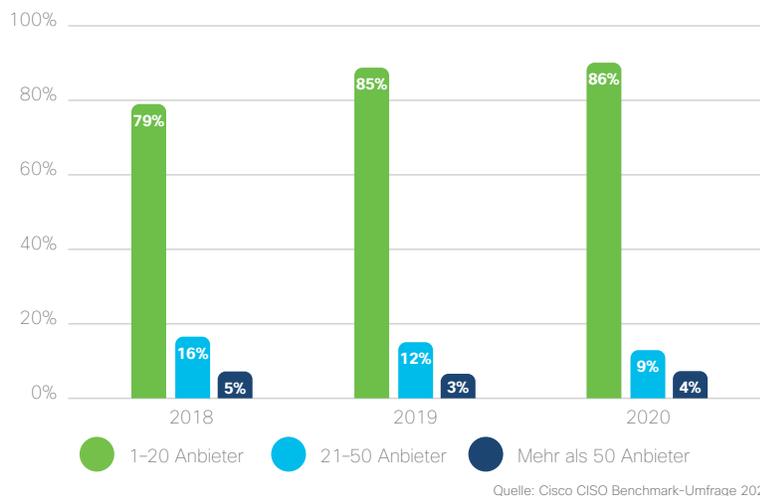
Phase 4: Steuern Sie den Benutzerzugriff über eine zentral verwaltete Richtlinie, die Ausnahmen identifiziert und darauf reagiert?

Phase 5: Verfügen Sie über eine geschäftsorientierte Zero-Trust-Strategie, unterstützt von einer Architektur und einer Reihe von Prozessen, die es Benutzern ermöglichen, nahtlos auf lokale und Cloud-Anwendungen zuzugreifen?

15. Lassen sich die Auswirkungen der Anbieterkonsolidierung messen?

Der Trend zur Reduzierung der Komplexität durch Anbieterkonsolidierung setzt sich fort: **86 Prozent der Unternehmen nutzen zwischen 1 und 20 Anbietern, nur 13 Prozent haben mehr als 20 Anbieter** (Abbildung 7).

Abbildung 7: Anzahl der in den Sicherheitsumgebungen der Befragten vertretenen unterschiedlichen Sicherheitsanbieter (d. h. Marken, Hersteller). (N=2.800) Die Prozentsätze wurden gerundet.



Seit 2017 hat sich nach Angaben der befragten Unternehmen verändert, wie sie mit einer mehrere Anbieter umfassenden Strategie zurechtkommen. **28 Prozent sind nun der Meinung, dass die Verwaltung einer solchen heterogenen Umgebung eine große Herausforderung darstellt. Dieser Wert ist seit 2017 um 8 Prozent gestiegen. 53 Prozent finden sie relativ herausfordernd.** Immer weniger Unternehmen (zuvor 26 Prozent, jetzt 17 Prozent) finden es einfach, eine heterogene Umgebung zu verwalten. Die meisten Unternehmen (81 Prozent) fallen jetzt in die Kategorien derjenigen, die diesen Punkt als Herausforderung empfinden. Das kann bedeuten, dass weniger Anbieter zu verwalten sind oder dass sie begonnen haben, Tools wie Analysemodule zu verwenden, um die Ergebnisse mehrerer unterschiedlicher Tools zu verbessern.

Wir haben uns auch Trends zum Zusammenhang zwischen Warnungen in einer heterogenen Umgebung und deren Auswirkungen auf die Cybersicherheitsermüdung (die wir im nächsten Thema etwas näher untersuchen) angesehen. **Definiert man Cybersicherheitsermüdung als den nahezu völligen Verzicht auf alle proaktiven Verteidigungsmaßnahmen gegen Angreifer, leiden 42 Prozent der Befragten daran.**

Unsere Daten zeigen, dass Unternehmen, die unter Cybersicherheitsermüdung leiden, eine heterogene Umgebung mit deutlich höherer Wahrscheinlichkeit als Herausforderung empfinden. Unseren Erkenntnissen zufolge entsteht Cybersicherheitsermüdung, wenn Unternehmen auf zu viele Warnungen reagieren müssen und Schwierigkeiten mit der Anbieterkomplexität haben, aber auch wenn eine Sicherheitsverletzung mit größeren Auswirkungen (in Bezug auf die Ausfallzeit in Stunden) auftritt. Da mehr als 96 der an Cybersicherheitsermüdung leidenden Unternehmen angeben, das Management einer heterogenen Umgebung sei eine Herausforderung, **scheint die Komplexität eine der Hauptursachen für den Überdross zu sein.**

Ich möchte nicht meine gesamte Arbeitszeit mit der Integration von Sicherheitsprodukten verbringen. Ich möchte Sicherheit einfach nutzen können. Ich sage meinem Team immer, dass ich bei einem neuen Produkt drei Dinge erwarte:

- Es muss funktionieren.
- Ich muss volle Transparenz haben. „Schwarze Löcher“ darf es nicht geben.
- Es muss in unsere übrige Sicherheitsumgebung integriert sein.

Steve Martino, SVP, Chief Information and Security Officer, Cisco

16. Wo liegen bei Ihnen die Ursachen für Cybersicherheitsermüdung und -überdruss?

Im vorherigen Abschnitt zeichnete sich ein Zusammenhang zwischen Umgebungen mit mehreren Anbietern und zunehmender Cybersicherheitsermüdung ab. Jetzt werfen wir einen Blick auf das durchschnittliche tägliche Aufkommen an Sicherheitswarnungen in Unternehmen.

Die Gesamtanzahl der Warnungen, mit denen Sie es pro Tag zu tun haben, hat in den vergangenen Jahren zugenommen. Im Jahr 2017 gingen bei 50 Prozent der Unternehmen höchstens 5.000 Warnungen pro Tag ein. Jetzt fallen nur noch 36 Prozent der Unternehmen in diese Kategorie. Dagegen hat der Anteil der Unternehmen, die täglich mindestens 100.000 Warnungen erhalten, von 11 Prozent im Jahr 2017 auf 17 Prozent im Jahr 2020 zugenommen (Abbildung 8).

Abbildung 8: Gemeldete Anzahl der eingegangenen Warnungen. (N=2.800) Die Prozentsätze wurden gerundet.



Quelle: Cisco CISO Benchmark-Umfrage 2020

Vielleicht aufgrund dieses Volumenzuwachses und der erforderlichen Verarbeitungsressourcen werden mit knapp 48 Prozent so wenige Warnungen untersucht wie seit mehr als vier Jahren nicht. (Der Anteil lag 2017 bei 56 Prozent und ist seither jedes Jahr zurückgegangen.) Die Quote der legitimen Vorfälle entspricht mit 26 Prozent dem Vorjahreswert und deutet darauf hin, dass viele Untersuchungen falsch-positive Meldungen ergeben.

Positiv ist zu vermerken, dass sich der Anteil der behobenen legitimen Bedrohungen seit dem Bericht vom letzten Jahr gesteigert hat. Mit 50 Prozent liegt er jetzt wieder auf dem Niveau von 2017. Somit bleibt jedoch immer noch die Hälfte aller wirklichen Vorfälle unbeachtet.

Die schier überwältigende Anzahl von Warnungen hat offensichtlich Einfluss auf die Cybersicherheitsermüdung: **Bei 93 Prozent der Befragten, die nach eigenen Angaben unter Cybersicherheitsermüdung leiden, gehen pro Tag mehr als 5.000 Warnungen ein.**

Um den zunehmenden Störungen und der steigenden Anzahl von Warnungen zu begegnen, plädieren wir für einen Ansatz, bei dem Automatisierung im Mittelpunkt steht. Durch Automatisierung können Richtlinien konsistenter, schneller und effizienter durchgesetzt werden. Wenn festgestellt wird, dass ein Gerät infiziert oder anfällig ist, wird es automatisch isoliert oder erhält keinen Zugriff, ohne dass ein Administrator eingreifen muss.

17. Welche Sicherheitsvorteile bietet das Hosting der Infrastruktur in der Cloud?

Durch unsere Studie haben wir herausgefunden, dass Aussichten auf erhöhte Effektivität, Effizienz und Transparenz einige der wichtigsten Antriebsfaktoren für Unternehmen sind, ihre Sicherheitsmaßnahmen (88 Prozent) und die Infrastruktur (89 Prozent) in die Cloud zu verlagern. Es verwundert wenig, dass **86 Prozent der Befragten angeben, durch Cloud-basierte Sicherheitsmaßnahmen habe sich die Transparenz ihrer Netzwerke erhöht.** Im Jahr 2020 verwalten gut 83 Prozent der Unternehmen mehr als 20 Prozent ihrer IT-Infrastruktur in der Cloud (intern oder extern).

Kunden sind zunehmend darauf angewiesen, dass Anbieter Vorfälle näher untersuchen und erweiterte Analysen und detaillierte forensische Berichte bereitstellen. Aus diesem Grund müssen IR-Anbieter hochgradig spezialisierte Kombinationen aus Produkten und Prozessen anbieten, um die mittlere Zeit bis zur Eindämmung (Mean Time to Contain, MTTC) und die mittlere Zeit bis zur Behebung (Mean Time to Remediate, MTTR) bei Vorfällen zu verkürzen.

Market Guide for Digital Forensics and Incident Response Services, Gartner, Dezember 2019⁴

⁴ Brian Reed, Toby Bussa, Market Guide for Digital Forensics and Incident Response Services, Gartner, 11. Dezember 2019

18. Welche Herausforderungen erwarten Sie für die Zukunft?

Die digitale Transformation bringt eine wahre Flut von Infrastrukturänderungen mit sich, die nicht immer leicht zu implementieren sind. Dennoch bietet sie IT- und Sicherheitsverantwortlichen immer noch die Chance, Innovationen zu schaffen und Wettbewerbsvorteile zu erzielen.

Sicherheitsverantwortliche setzen auf fortschrittliche Technologien und Ansätze – von künstlicher Intelligenz und maschinellem Lernen bis hin zur sicheren Implementierung von DevOps und Mikrosegmentierung. Wie wir alle wissen, sind Multi-Cloud-Umgebungen nach wie vor weit verbreitet.

Angesichts der Dynamik dieser Umgebungen müssen Sicherheitsexperten nicht nur die Grundlagen beherrschen, sondern auch bei neueren Technologien auf dem Laufenden bleiben. Einige dieser neueren Technologien sollten in jedem Fall zu einem festen Bestandteil Ihres Sicherheitsökosystems werden.

Wir sehen beispielsweise, dass im heutigen Zeitalter der allgegenwärtigen Digitalisierung **derzeit nur 27 Prozent der Unternehmen eine mehrstufige Authentifizierung (MFA) nutzen**. Für eine so wertvolle Zero-Trust-Technologie ist dieser Anteil sehr klein. MFA war bei den Befragten aus folgenden Ländern in dieser Reihenfolge am gängigsten: USA, China, Italien, Indien, Deutschland und Vereinigtes Königreich. Die Branchen mit der weitesten Verbreitung sind (in dieser Reihenfolge) Softwareentwicklung, Finanzdienstleistungen, Behörden, Einzelhandel, Fertigung und Telekommunikation.

Bei der digitalen Transformation ist nach der Cloud-Einführung die Automatisierung der große Gewinner. Viele Sicherheitsverantwortliche haben erkannt, dass Automatisierung eine hilfreiche Maßnahme gegen den Fachkräftemangel ist: Sie setzen auf Lösungen mit mehr [maschinellern Lernen und künstlicher Intelligenz](#).

Wie Abbildung 9 zeigt, **plant die Mehrheit (77 Prozent) unserer Umfrageteilnehmer, die Automatisierung auszubauen, um Reaktionen in ihren Sicherheitsumgebungen zu vereinfachen und zu beschleunigen**. Bei der Automatisierungsplanung sollten Sie strategisch definieren, in welchen Unternehmensbereichen eine Automatisierung am meisten bewirkt und den höchsten ROI bietet.

Abbildung 9: Anteil der Befragten, die für das kommende Jahr einen verstärkten Einsatz von Automatisierung in der Sicherheitsumgebung ihres Unternehmens planen. (N=2.800) Die Prozentsätze wurden gerundet.



Quelle: Cisco CISO Benchmark-Umfrage 2020

19. Wie viel Augenmerk sollten Sie auf die Reaktion auf Vorfälle legen?

Die Bedrohungslandschaft hat sich für Unternehmen weltweit zu einem komplexen, herausfordernden Umfeld entwickelt. Der Fachkräftemangel bei gleichzeitiger Zunahme der IT-Sicherheitsvorfälle hat den Sicherheitsstatus in den meisten Unternehmen geschwächt. Wer sich zurücklehnt und wartet, bis eine Warnung eingeht, riskiert empfindliche Strafen, gesteigerte Kontrollen, Datenverluste, [Probleme mit der Datensicherheit](#) und Umsatzeinbußen. Prävention durch Transparenz, proaktive Bedrohungssuche und die Einrichtung eines Zero-Trust-Frameworks ist also entscheidend für den Schutz Ihrer Infrastruktur.

In unserer Umfrage unter IT-Entscheidungsträgern **gaben 76 Prozent an, sie seien hinsichtlich der Reaktion auf Vorfällen sehr gut informiert. 23 Prozent sind nach eigenen Angaben einigermaßen informiert. Zusammen ergibt dies immerhin 99 Prozent.** Das ist die gute Nachricht. Doch wie unsere Umfrage ergab, führt die Komplexität der Sicherheitsmaßnahmen zu Cybersicherheitsermüdung, die wiederum Ihre schwer zu gewinnenden Ressourcen belasten könnte. Hier kann Outsourcing helfen.

Abbildung 10: Der Anteil der Befragten, die sehr gut oder einigermaßen über die Reaktion auf Vorfälle informiert sind, beträgt zusammen 99 Prozent. (N=2.800) Die Prozentsätze wurden gerundet.



Laut unserer Umfrage nutzen 34 Prozent der Befragten Outsourcing für Services zur Reaktion auf Vorfälle, und 36 Prozent setzen externe Services bzw. Services von Drittanbietern zur Analyse infizierter Systeme ein. Dieser Wert hat sich gegenüber letztem Jahr erhöht. Die Verwendung von Services zur Reaktion auf Vorfälle hat sich zu einem effizienten Ansatz zur Ressourcenschonung, Risikominderung und Aufrechterhaltung der Compliance entwickelt. Durch proaktive Planung und das nötige Expertenwissen für die Koordinierung und Umsetzung der Vorfälle kann ein solcher Ansatz Ihrem Unternehmen helfen, sich vor bisher unbekanntem Bedrohungen zu schützen.

[Möchten Sie wissen, wie Sie oder Ihre Mitarbeiter Karrieren im Bereich Cybersicherheit fördern können?](#)

[Hier erfahren Sie mehr: Cisco Security-Zertifizierungen.](#)

20. Was können Sie jetzt unternehmen, um Ihren Sicherheitsstatus zu verbessern?

Sie haben es mit aktiven Angreifern zu tun, die gut finanziert und unendlich geduldig sind. Außerdem stehen Sie vor dauerhaften Herausforderungen, die scheinbar endlos Aufwand verursachen, beispielsweise die Pflege von genauen Bestandsinformationen über Benutzer, Anwendungen und Geräte. Sie jonglieren mit Geschäftsrisiken und Sicherheitsrisiken und müssen gleichzeitig Teams in die Lage versetzen, schnell zu reagieren. Dennoch werden geschäftliche Entscheidungen weiterhin ohne Berücksichtigung der Sicherheit getroffen. Wenn dann noch neue Auflagen, Unternehmensvorgaben, knappe Budgets, das Risikomanagement und die übliche Fluktuation im Sicherheitsteam dazukommen, nimmt der Druck gar nicht mehr ab.

Die Herausforderungen bei der Verteidigung Ihres Unternehmens nehmen zu und werden auch künftig nicht nachlassen. Es ist an der Zeit, intelligenter zu arbeiten, Verteidigungsmaßnahmen zu rationalisieren und sich auf Prävention sowie das Erkennen und Beheben von Bedrohungen zu konzentrieren. In diesem Bericht haben wir 20 Bereiche zusammengestellt, die Sie berücksichtigen können, um die Sicherheit in Ihrem Unternehmen zu erhöhen. Dazu sprechen wir Empfehlungen aus, die wie folgt zusammengefasst werden können:

- Setzen Sie auf mehrstufige Verteidigungsmaßnahmen, die MFA, Netzwerksegmentierung und Endpunktsicherheit umfassen sollten.
- Steigern Sie die Transparenz so weit wie möglich, um Kontrollmechanismen für Daten zu stärken, das Risiko zu senken und die Compliance zu erhöhen.
- Stärken Sie die Abwehr, aktualisieren und patchen Sie Ihre Geräte, und rücken Sie die Cyberhygiene mit Übungen und Schulungen in den Mittelpunkt.
- Verbessern Sie Ihre Sicherheitsreife, indem Sie ein Zero-Trust-Framework aufbauen (Abbildung 13).

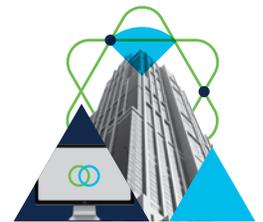
Abbildung 11: Eine Zero-Trust-Strategie kann die Sicherheit von Mitarbeitern, Workloads und Arbeitsumgebungen steigern.



Sicherheit für Ihre Mitarbeiter
Sicherer Zugriff für Benutzer und deren Geräte, die eine Verbindung zu Anwendungen herstellen



Sicherheit für Ihre Workload
Sicherheit für alle Verbindungen in Ihren Anwendungen in jeder Umgebung



Sicherheit für Ihre Arbeitsumgebung
Sichere Verbindungen im gesamten Netzwerk

Wir bei Cisco glauben, dass es für die Sicherheitsbranche an der Zeit ist, sich weiterzuentwickeln. Sicherheitslösungen sollten wie ein Team funktionieren. Teams kommunizieren in Echtzeit, lernen voneinander und reagieren als koordinierte Einheit. Die Endpunktsicherheit muss mit der Netzwerksicherheit und der Cloudsicherheit ineinandergreifen, und Sie benötigen eine MFA-Lösung, die Identität und Zugriff abdeckt. **Wir sind überzeugt, dass echte Sicherheit für Ihr Unternehmen am besten durch einen Plattformansatz erreicht werden kann. Dieser ermöglicht eine lückenlose Sicherheitsabdeckung.**

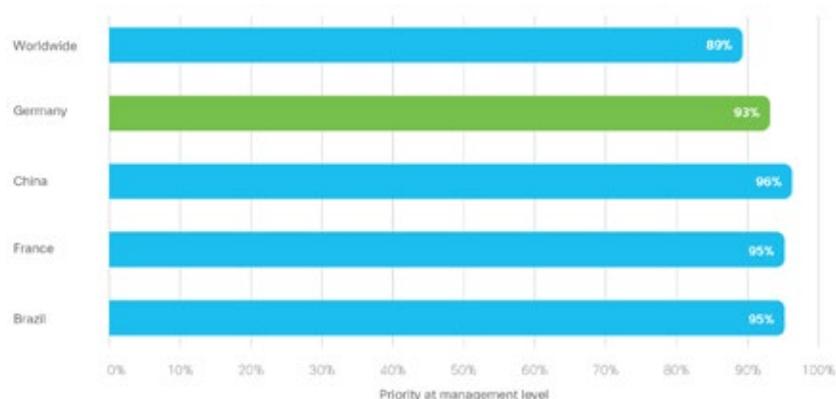
Was in Deutschland anders ist

Datenschutz und Sicherheit haben in Deutschland einen besonders hohen Stellenwert. Interessant ist daher, dass es durchaus größere Unterschiede zwischen den Entscheidern in Deutschland und dem Rest der Welt gibt.

1. Priorität auf Führungsebene

93% der Befragten aus Deutschland sagen, dass ihre Führungsspitze der IT-Sicherheit eine hohe Priorität einräumt – weltweit ist dieser Wert über die Jahre leicht auf 89% abgesunken. Eine noch höhere Priorität räumen CXO-Entscheider dem Thema der Unternehmensführung nur noch in China (96%), Frankreich und Brasilien (jeweils 95%) ein. Deutschland liegt damit in der Spitzengruppe.

93% der deutschen CISO's wertet IT-Sicherheit als höchste Priorität



2. Wichtigstes KPI bei einem Angriff

Schnelle Reaktionen auf Angriffe sind für Unternehmen besonders wichtig. Daher haben 90% aller Unternehmen klare Kennzahlen zur Bewertung der Effektivität von

Sicherheitsmaßnahmen etabliert. Dazu gehören

- die Zeitspanne, bis ein Angriff erkannt wird
- die Zeit zum Patchen der Sicherheitslücke
- die Zeit, den Angriff einzudämmen
- die Zeit, bis das Problem komplett behoben ist

In Deutschland liegt der Fokus dabei klar auf einer möglichst kurzen Zeit zur Behebung des Problems. Für 56% der Befragten war das der wichtigste Infikator. Müssen diese Zahlen auch dem Vorstand vorgelegt werden, steigt der Wert sogar auf 61%. Global priorisieren die Befragten dagegen die KPI „Zeit bis zur Angriffserkennung“ höher (65%). Die Ausnahme bildet Italien. Hier geben 67% der schnellen Behebung die höchste Priorität.

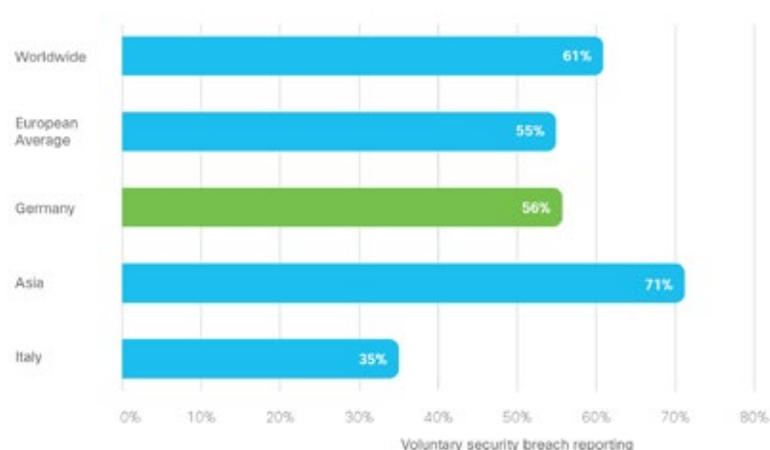
Für 56% der Befragten liegt die Zeit, bis ein Problem komplett behoben ist, im Fokus

3. Bekanntgabe von Sicherheitsverstößen

Eine schwierige Frage für Vorstände ist immer wieder, ob und wann man einen Sicherheitsverstoß öffentlich macht. Sie befürchten oft einen Reputationsverlust und Gewinneinbrüche. Allerdings kann ein offener Umgang auch Vertrauen zurückholen, das bei einer verschleppten Bekanntgabe verloren gehen könnte. Trotzdem die DSGVO hierfür den rechtlichen Rahmen verschärft hat, sind deutsche Unternehmen deutlich zurückhaltender als andere.

In Asien melden 71% aller Unternehmen freiwillig Sicherheitsverstöße, global sind es 61%. Deutsche Unternehmen sind mit einer Rate von 56% knapp über dem europäischen Mittel von 55% und damit noch zurückhaltender als Firmen in anderen Ländern. In Europa bildet Italien mit 35% freiwilliger Bekanntgaben das Schlusslicht.

Mit 56% liegen deutsche Unternehmen unterhalb dem globalen Mittel, wenn es um die Kommunikation von Sicherheitsverstößen geht



4. Patchen von Sicherheitslücken

Weltweit ist die Anzahl der Angriffe wegen fehlender Sicherheitspatches sehr gestiegen (von 30% auf 46% in nur einem Jahr). Auf den ersten Blick liegt Deutschland hier mit 39% erfreulicherweise deutlich unter dem weltweiten Durchschnitt. Andere europäische Länder wie Frankreich (36%), Spanien (33%) und Italien (30%) sind hier aber noch deutlich besser aufgestellt.

Da bei Angriffen über Sicherheitslücken in der Regel deutlich mehr Daten abfließen als bei anderen Angriffen, gilt es für deutsche Unternehmen, das Aktualisieren von Software im Fokus zu behalten. Unsere „Nachbarn“ im Süden und Westen machen vor, wie es geht.

Nur 39% (weltweit 46%) Angriffe durch Sicherheitslücken wegen fehlender Sicherheitspatches in Deutschland

5. Besondere Abwehr-Herausforderungen

87% In welchen technischen Bereichen ist das Absichern von Geräten und Personen besonders schwierig? Besonders schwierig empfinden Deutsche Unternehmen das Absichern von mobilen Geräten (40%), gefolgt von Public-Cloud-Anwendungen (36%). Es folgen Probleme mit dem unbedarften Verhalten von Anwendern (33%) und Privat-Cloud-Infrastrukturen. Weltweit liegen die Einschätzungen sehr weit auseinander. Insbesondere in englischsprachigen Ländern wie UK, USA und Kanada (mehr als 50%), Australien (mehr als 60%) und Indien (über 70%) stufen die Befragten die Absicherung von Private-Cloud-Infrastrukturen und Mobilien Geräten als besonders oder extrem schwierig ein.. Deutlich weniger Sorgen haben nur noch Unternehmen aus Italien und Japan (30% oder weniger).

Sicherheit jetzt und in der Zukunft

Unsere Vision ist es, unsere Kunden vor den Bedrohungen von heute und morgen zu schützen, damit sie sich auf ihre eigentliche Mission konzentrieren und die Sicherheit uns überlassen können.

Vor diesem Hintergrund führen wir die Cisco Sicherheitsplattform [SecureX](#) ein, die vom stärksten Sicherheitsteam der Welt entwickelt wurde und zur Arbeitsweise Ihres Unternehmens passenden Schutz bietet.

- Wir beginnen mit **erstklassigen Lösungen**, die Netzwerke, Endpunkte, Anwendungen und Clouds schützen.
- Wir nutzen eine **Überprüfung der Vertrauenswürdigkeit**, um sicherzustellen, dass nur die richtigen Personen Zugriff auf Ihr Netzwerk erhalten.
- Wir stützen jedes Produkt auf branchenführende [Talos Threat-Intelligence](#), um eine höhere Anzahl von Bedrohungen zu blockieren und die Sicherheit für Unternehmen zu stärken.
- Wir bieten **automatisierte Reaktionen auf fortschrittliche Bedrohungen** und **rationalisieren die Betriebsabläufe durch integriertes Bedrohungs- und Sicherheitsmanagement** in unserem gesamten Portfolio.
- **Wir entwickeln unsere Lösungen so, dass sie mit den anderen Technologien zusammenarbeiten, die Sie für integrierte Sicherheitsreaktionen verwenden** – selbst wenn diese von anderen Anbietern stammen.

SecureX ermöglicht Transparenz, automatisierte Aktionen und einen verbesserten Sicherheitsstatus. Auf der **SecureX-Plattform** wurden zusätzlich maßgeschneiderte, über die Cloud bereitgestellte Anwendungen entwickelt, um die Komplexität bei der Sicherheit zu verringern. Wir verbinden das integrierte Sicherheitsportfolio von Cisco mit Drittanbieterprodukten aus der Kundenumgebung zu einer konsistenten Schnittstelle. Innovationen von Cisco auf Plattformebene bieten die am stärksten integrierten Analysen weltweit. Alles greift ineinander:

- [SecureX](#) vereint Sicherheits-, Netzwerk- und IT-Betriebsteams mit kollaborativen Workflows zur Steigerung der Produktivität.
- [Cisco Threat Response](#) vereinfacht die Untersuchung und Beseitigung von Bedrohungen, um die SecOps-Effizienz zu steigern.
- [Analysefunktionen](#) vereinfachen die Erkennung unbekannter Bedrohungen, um Richtlinienentscheidungen, Reaktionszeiten und die Wirksamkeit von Bedrohungsreaktionen zu verbessern.

Mit unserer integrierten und branchenführenden Threat-Intelligence bietet Cisco Ihnen den Umfang, die Skalierbarkeit und die Funktionen, um mit der Komplexität und dem Umfang von Bedrohungen Schritt zu halten. Wenn Sicherheit an erster Stelle steht, unterstützen Sie Innovationen und schützen Ihre Ressourcen. Cisco priorisiert Sicherheit in allem, was wir tun. Nur mit Cisco erreichen Sie wirksame Netzwerksicherheit, um die neuen Bedrohungen von morgen zu bewältigen. Weitere Informationen über unseren Plattformansatz finden Sie unter cisco.com/go/security.

Über die Cisco Reihe zur Cybersicherheit

In den vergangenen zehn Jahren hat Cisco eine Fülle an maßgeblichen Informationen zu Sicherheit und Threat-Intelligence für Sicherheitsfachleute 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.

Cisco Security veröffentlicht nun eine Reihe von forschungsbasierten, datengesteuerten Publikationen unter der Überschrift „Cisco Reihe zur Cybersicherheit“. Wir haben die Anzahl der Titel erweitert, sodass sie jetzt auch verschiedene Berichte für Sicherheitsexperten mit anderen Interessen enthalten. Die Berichte für die einzelnen Jahre greifen auf die tiefgreifenden und umfangreichen Kenntnisse von Bedrohungsforschern und Innovatoren in der Sicherheitsbranche zurück und enthalten die Benchmark-Studie zum Datenschutz, den Bedrohungsbericht und die Cisco Benchmark-Studien. Weitere Berichte werden jeweils im Verlauf des Jahres veröffentlicht.

Weitere Informationen sowie alle Berichte und archivierten Kopien finden Sie unter www.cisco.com/go/securityreports.



Datenschutz 2019



Bedrohungsbericht 2019



CISO Benchmark 2019



E-Mail: Vorsicht beim Anklücken



Sicherheitsergebnis



Nachverfolgung von Bedrohungen



Verbraucherumfrage zum Thema Datenschutz



Die wichtigsten Bedrohungen im Jahr 2019



Datenschutz 2020



CISO Benchmark 2020

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. Eine Liste der Adressen, Telefon- und Faxnummern finden Sie auf der Cisco Website unter www.cisco.com/go/offices.

Veröffentlicht im Februar 2020

CISO_02_0220

© 2020 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 Marken von Cisco finden Sie unter folgender URL: 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. (1876404)

 Sicherheit