proofpoint.

BERICHT

Voice of the CISO Report 2022

Weltweite Erkenntnisse zu den Herausforderungen, Erwartungen und Prioritäten von CISOs

proofpoint.com/de

Inhaltsverzeichnis

Das Jahr, in dem Cybersicherheit an erste Stelle rückte

Das Jahr 2021 erwies sich für CISOs auf der ganzen Welt als äußerst herausfordernd, da medienwirksame Angriffe ganze Lieferketten unterbrachen, die Schlagzeilen bestimmten und zu neuen Cybersicherheitsgesetzen führten.

Der Ransomware-Angriff von DarkSide auf Colonial Pipeline legte die Treibstoffversorgung weiter Teile der US-amerikanischen Ostküste lahm. Die Conti-Gruppe zwang das irische Gesundheitssystem in die Knie und führte zur Schließung von Krankenhäusern. Die Ransomware REvil führte zum Produktionsstopp bei JBS, dem größten Fleischverarbeiter der Welt. Außerdem konnte die REvil-Gruppe die Cloud-basierte Managed Service Provider-Plattform Kaseya erfolgreich angreifen.[1] Das führte zur Kompromittierung weiterer Managed Service Provider, die die Kaseya-Software zur Remote-Verwaltung einsetzten.

Dies sind nur einige von unzähligen Zwischenfällen, die bei Sicherheitsexperten für graue Haare sorgten.

Diese medienwirksamen Kompromittierungen hatten schwerwiegende wirtschaftliche sowie sicherheitsrelevante Folgen und zeigten ein weiteres Mal schonungslos, wie anfällig kritische Infrastrukturen und Lieferketten sein können, wenn sie von Cyberkriminellen angegriffen werden. Die exorbitanten Lösegeldforderungen bei manchen Zwischenfällen ließen einige Regierungen darüber nachdenken, Lösegeldzahlungen an Cybercrime-Gruppen per Gesetz zu verbieten.

Nachdem die Auswirkungen der Pandemie im Jahr 2021 allmählich abebbten, trat ein neues Problem auf: die große Kündigungswelle. Arbeitnehmer kündigten massenhaft oder entschieden sich, komplett aus dem Arbeitsmarkt auszusteigen – mit schwerwiegenden Folgen für den Informationsschutz sowie Insider-Bedrohungen.[2] Und zum Ende des Jahres gab die Log4j-Lücke[3] Angreifern die Möglichkeit, Code auszuführen und die Kontrolle über anfällige Geräte zu übernehmen. Dies führte zu Ausfällen unter anderem bei Amazon Web Services (AWS), Cisco, IBM und VMware.

2022 sind wir nun mit der unsichersten geopolitischen Lage konfrontiert, die Europa seit Jahrzehnten erlebt hat. Daher müssen CISOs jetzt zusätzlich die Auswirkungen von hybrider Kriegsführung auf ihre Sicherheitslage berücksichtigen.[4]

Um in dieser schwierigen Zeit die Stimmung unter Cybersicherheitsexperten einschätzen zu können, befragte Proofpoint 1.400 CISOs auf der ganzen Welt und bat sie darum, ihre persönlichen Erfahrungen aus den letzten 12 Monaten zu teilen und eine Prognose für die Zukunft abzugeben.

Dieser zweite Jahresbericht zeigt auf, wie CISOs sich nach dem Ende der Pandemie neu ausrichten, Strategien zur Unterstützung langfristiger Hybrid-Arbeitsmodelle umsetzen und immer raffiniertere Bedrohungen abwehren. Außerdem untersuchen wir, wie Unternehmen durch Mitarbeiter gefährdet werden und mit welchen Maßnahmen die CISOs dem entgegensteuern. Abschließend gehen wir auf die veränderte Rolle von CISOs und die wachsenden sowie neuen Anforderungen ein, die sie erfüllen müssen.

Dieser Bericht wäre ohne die Mitwirkung von Cybersicherheits- und Informationssicherheitsexperten in aller Welt nicht zustande gekommen. Vielen Dank für Ihre Beiträge und Rückmeldungen.

Lucia Milică, Global Resident CISO bei Proofpoint

1 Pierluigi Paganini (Cybernews): „An in-depth analysis of the Kaseya ransomware attack: here's what you need to know“ (Eine umfassende Analyse des Kaseya-Ransomware-Angriffs mit allen wissenswerten Details), Juli 2021.
2 Proofpoint: „Global Cybersecurity Study: Insider Threats Cost Organizations $15.4 Million Annually, up 34 Percent from 2020“ (Weltweite Untersuchung zur Cybersicherheit: Unternehmen entstehen durch Insider-Bedrohungen jährliche Kosten in Höhe von 15,4 Mio. USD – ein Anstieg um 34 % ggü. 2020), Januar 2022.
3 CISOMAG: „Log4j Explained: How It Is Exploited and How to Fix It“ (Beschreibung der Log4j-Sicherheitslücke und Behebungsmöglichkeiten), Dezember 2021.
4 Andrew Rose (Proofpoint): „How Conflict in Ukraine Could Revolutionize the Ransomware Threat“ (Wie der Ukraine-Konflikt die Ransomware-Bedrohung revolutionieren könnte), März 2022.

Kapitel 1: Die Ruhe nach der Krise

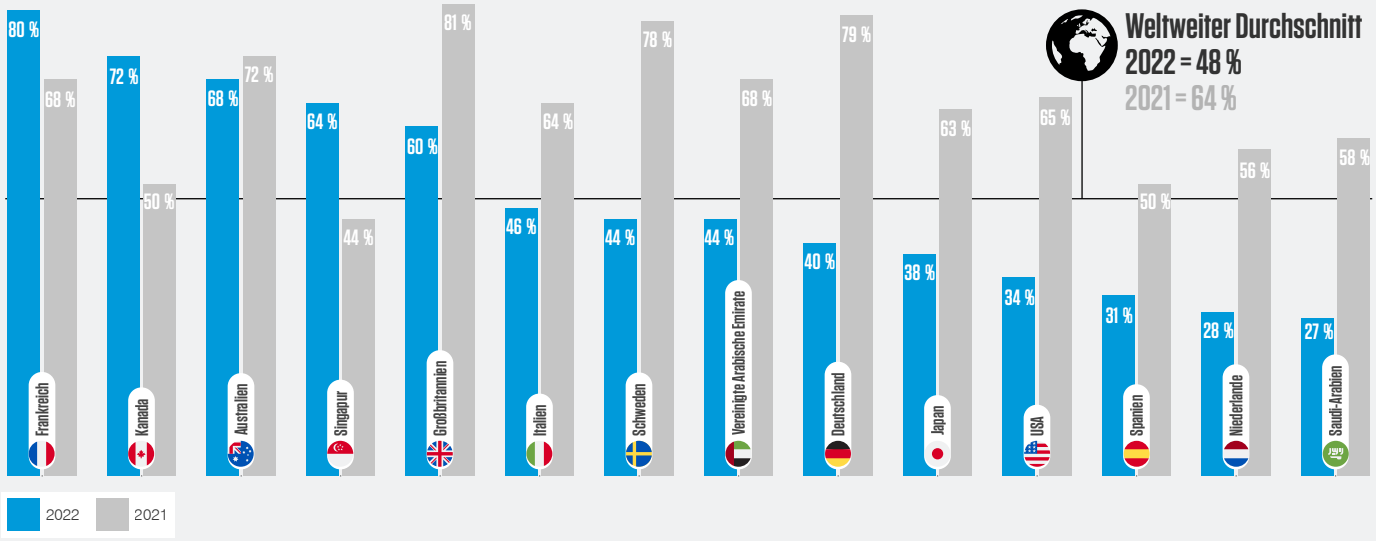
Nach einem durch beispiellose Veränderungen geprägten Jahr stellen sich CISOs auf der ganzen Welt auf neue Arbeitsmodelle ein. Doch nachdem sich die erste Hektik bei der Implementierung von Cloud- und Hybrid-Umgebungen sowie der Gewährleistung des planmäßigen Geschäftsbetriebs gelegt hat, haben viele CISOs nun eine bessere Kontrolle über ihren Arbeitsbereich.

Die Bekämpfung spontaner Brände ist einer koordinierteren Strategie gewichen. Es wurden neue Richtlinien, Schulungsmodule und technische Kontrollen eingeführt, die auf die heute stärker verteilten und Cloud-abhängigen Teams zugeschnitten sind.

48 % der befragten CISOs rechnen in den nächsten 12 Monaten mit einem schweren Cyberangriff, wobei ein Drittel das Risiko sogar als sehr hoch einschätzt.

Aus diesem Grund ist weniger als die Hälfte der befragten CISOs (**48 %**) der Meinung, dass ihr Unternehmen innerhalb der nächsten 12 Monate von einem schwerwiegenden Cyberangriff getroffen werden könnte. Im vergangenen Jahr waren das noch **64 %**.

Anteil der CISOs, die zustimmen, dass ihr Unternehmen in den nächsten 12 Monaten einem schweren Cyberangriff ausgesetzt sein könnte



CISOs aus Frankreich (**80 %**), Kanada (**72 %**) und Australien (**68 %**) sind am meisten wegen eines schweren Cyberangriffs besorgt.

Nur **28 %** der CISOs in den Niederlanden sowie **27 %** in Saudi-Arabien rechnen mit einem schwerwiegenden Angriff. Damit sind sie die optimistischsten unter allen befragten Regionen.

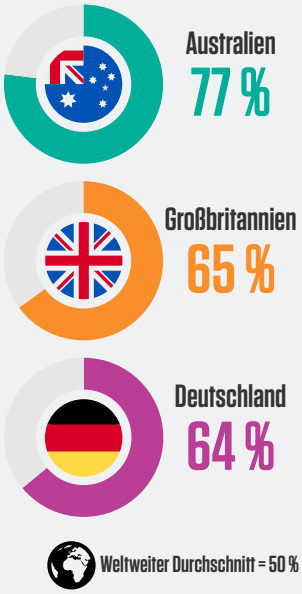
Große Unternehmen sind sich der Risiken stärker bewusst: **51 %** der Umfrageteilnehmer aus Unternehmen mit mehr als 5.000 Mitarbeitern halten einen schweren Cyberangriff für wahrscheinlich oder sehr wahrscheinlich.

56 % der CISOs aus den Bereichen IT, Technologie und Telekommunikation sehen Cyberangriffe auf ihr Unternehmen als wahrscheinlich – der höchste Wert unter allen Branchen, gefolgt von Fertigungsunternehmen (**54 %**).

Der Einzelhandel ist von allen Branchen die optimistischste: **33 %** der Befragten glauben, dass schwere Schäden durch Angriffe unwahrscheinlich sind. Im vergangenen Jahr waren das nur **5 %**.

Anteil der CISOs, die zustimmen, dass ihr Unternehmen im Jahr 2022 nicht auf gezielte Angriffe vorbereitet ist

Top 3 der Länder



CISOs sind inzwischen mit dem post-pandemischen Arbeitsumfeld vertrauter und glauben deshalb, mit Cyberbedrohungen besser fertigwerden zu können. Während sich 2021 noch **66 %** nicht für einen gezielten Angriff vorbereitet fühlten, sank dieser Wert in diesem Jahr auf **50 %**.

Aber sich vorbereitet oder gefährdet zu fühlen ist etwas anderes als wirklich vorbereitet zu sein. In den meisten Fällen ist diese wachsende Zuversicht bei CISOs wohl eher das Resultat der Freude über die überwundene Katastrophe als die Folge spürbar verringerter Risiken oder besserer Vorbereitungen.

Zudem sollte nicht vergessen werden, dass die Hälfte der CISOs weltweit nicht glaubt, ihr Unternehmen könnte einen Cyberangriff erkennen, abwehren und überstehen. In Großbritannien und Deutschland sind mittlerweile sogar zwei Drittel der CISOs dieser Meinung – und in Australien erklärten 75 %, dass ihr Unternehmen unvorbereitet ist.

Auch die Diskrepanz zwischen wahrgenommenem Risiko und Vorbereitung gibt uns zu denken. Viele CISOs scheinen sich des Problems bewusst zu sein, können oder wollen aber keine effektive Lösung implementieren, da sie nicht wissen, welche der vielen Bedrohungen am ehesten zuschlagen wird.

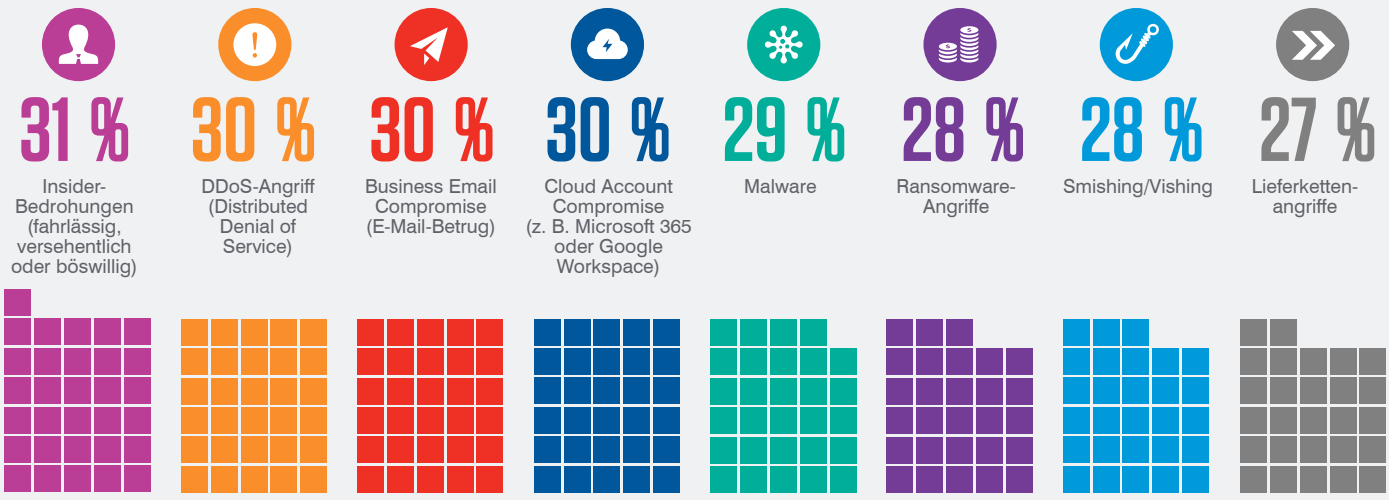
Angriffe aus allen Richtungen

Da die Bedrohungen immer zahlreicher und raffinierter werden, haben wir die CISOs erneut über die ihrer Meinung nach gefährlichsten Angriffsmethoden befragt. Ebenso wie im letzten Jahr zeigen die Ergebnisse einen fehlenden Einblick in die Bedrohungen, mit denen sie rechnen müssen.

Bedrohungen durch Insider, die fahrlässig, versehentlich oder kriminell handeln (**31 %**), Business Email Compromise (BEC) (**30 %**), Cloud-Kontenkompromittierung (**30 %**) sowie Distributed Denial-of-Service-Attacken (DDoS) (**30%**) stehen hier an erster Stelle. Währenddessen liegt die Sorge über Ransomware nur einen Prozentpunkt höher als im letzten Jahr, obwohl es in den vergangenen 12 Monaten zu mehreren medienwirksamen Angriffen gekommen ist.

Natürlich ist es keinesfalls falsch, bei verschiedenen Bedrohungen vorsichtig zu sein. Doch wenn Sicherheitsteams nicht sicher sind, aus welcher Richtung der nächste Angriff kommt, ist es fast unmöglich, Schutz- und Schulungsmaßnahmen gezielt einzusetzen.

Was betrachten Sie als größte Cyberbedrohung für Ihr Unternehmen bzw. Ihre Branche in den nächsten 12 Monaten? Wählen Sie bis zu drei Optionen aus.



10 von 14 untersuchten Ländern betrachten Insider-Bedrohungen als eine der drei größten Gefahren, die in Japan (**39 %**), Australien (**36 %**) und Italien (**34 %**) als besonders hoch eingeschätzt wird.

Ransomware wird in Deutschland, den Niederlanden und Spanien als größtes Risiko betrachtet.

8 von 14 untersuchten Ländern betrachten BEC als eine der drei größten Bedrohungen, wobei CISOs aus Frankreich (**43 %**) und den Vereinigten Arabischen Emiraten (**35 %**) sie am höchsten einschätzen.

Lieferkettenangriffe bereiten CISOs in Kanada, Spanien und Saudi-Arabien die größten Sorgen.

Die Gefahr durch Kompromittierung von Cloud-Konten wird in acht Regionen als besonders groß eingeschätzt, wobei sie in Schweden am höchsten (**38 %**) und in den Niederlanden am geringsten (**19 %**) bewertet wird.

Distributed Denial-of-Service-Attacken (DDoS) bereiten CISOs in den USA, Großbritannien und Singapur große Sorgen.

Es ist nachvollziehbar, dass CISOs nach den letzten Unsicherheiten keinen klaren Einblick in ihre Bedrohungslage haben. Aufgrund der schnellen Anpassung an neue Arbeitsweisen, den zunehmenden Cloud-Einsatz sowie veränderte Verhaltensmuster ist es äußerst schwierig, Bedrohungen einzustufen und angemessene Schutzmaßnahmen zu implementieren.

Dieser fehlende Überblick ist jedoch kein unüberwindbares Problem, da sich ein Faktor nicht ändert: Mehr als **90 %** aller Cyberangriffe beginnen mit einer E-Mail. Ganz gleich, ob es sich bei der Bedrohung um Ransomware, BEC oder die Kompromittierung von Cloud-Konten handelt, sollte der Schutz des Posteingangs stets der erste Schritt sein.

„Als Sicherheitsverantwortlicher hat man das Gefühl, auf einer abwärts führenden Rolltreppe nach oben zu laufen. Wenn Sie stehen bleiben, landen Sie schon bald ganz unten. Selbst wenn Sie einen Schritt nach dem anderen gehen, kommen Sie nicht voran. Für wirklichen Fortschritt müssen Sie rennen – und zwar ständig. Als CISO ist Fitness ein Muss.“

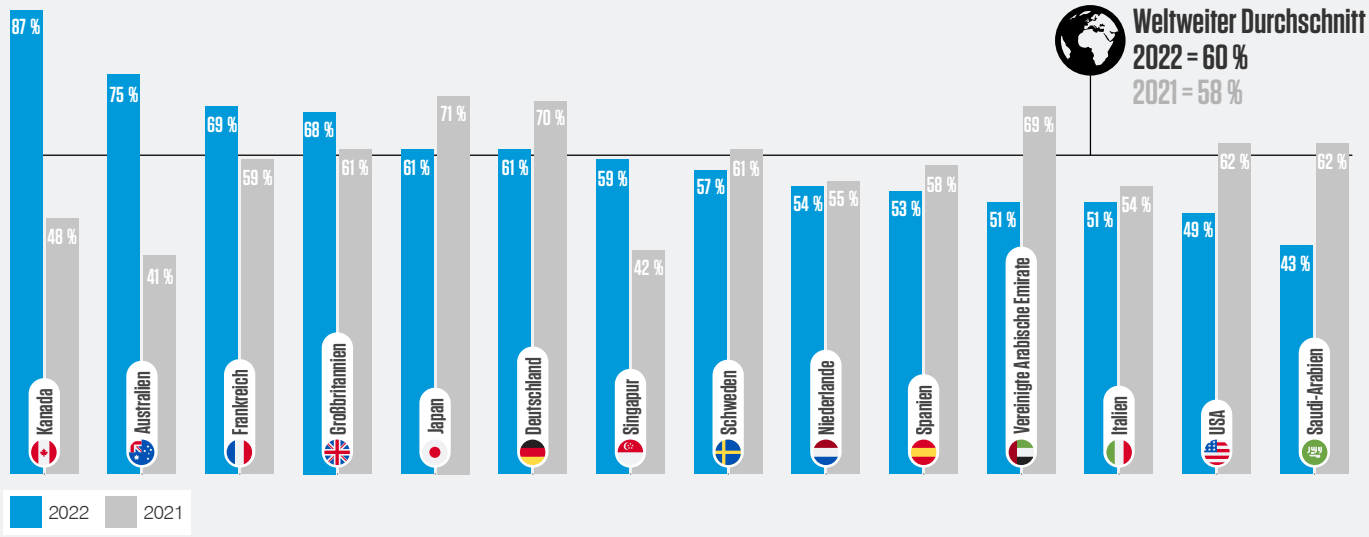
Malcolm Norman, CISO, Wood Plc

Kapitel 2: Mitarbeiter als neuer Perimeter

Nach zwei Jahren Homeoffice-Arbeit glauben die meisten CISOs, dass Mitarbeiter ihre Rolle beim Schutz ihres Unternehmens vor Cyberbedrohungen verstehen. Insgesamt stimmen **60 %** der Umfrageteilnehmer dieser Aussage zu, während es im vergangenen Jahr noch **58 %** waren. Etwa ein Viertel (**24 %**) stimmen ausdrücklich zu.

Der Trend zeigt sich in erster Linie in Kanada und Australien, wo das Vertrauen in die Mitarbeiter um 39 Prozentpunkte auf **87 %** bzw. um 34 Prozentpunkte auf **75 %** gestiegen ist.

Anteil der CISOs, die glauben, dass die Mitarbeiter ihre Rolle bei der Abwehr von Cyberbedrohungen verstehen



Diese Zunahme beim Vertrauen führen wir weitgehend auf Maßnahmen zur Unterstützung langfristiger Homeoffice- und Hybrid-Arbeitsmodelle zurück. Viele Unternehmen haben die letzten zwei Jahre stark in Cybersicherheitsschulungen und personenzentrierten Schutz investiert.

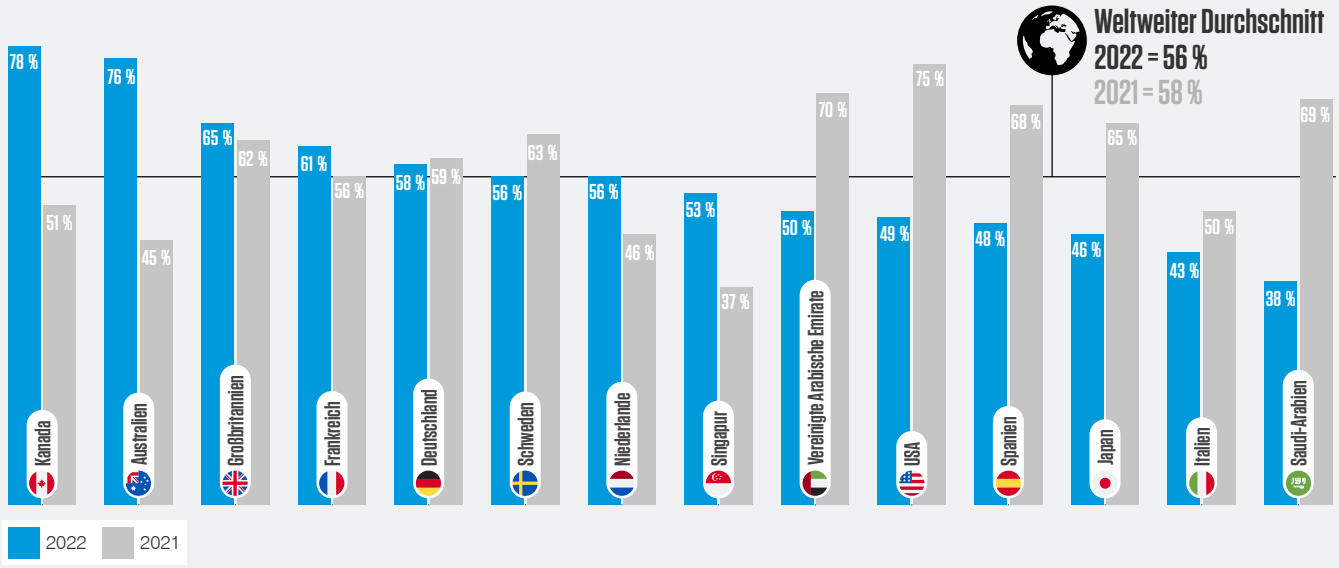
Da die Mitarbeiter ortsunabhängig arbeiten, liegt der Schwerpunkt weniger auf dem Schutz des Rechenzentrums oder Büronetzwerks. Immer mehr CISOs verstehen, dass die Mitarbeiter der neue Perimeter sind, und implementieren Maßnahmen zu ihrer Absicherung.

56 % der CISOs betrachten menschliche Fehler als größte Cyberschwachstelle ihres Unternehmens.

Im Gegensatz dazu hatten Länder mit strengeren oder formelleren Unternehmensumgebungen mitunter Schwierigkeiten mit der Anpassung an die neuen Gegebenheiten. Beispielsweise fiel das Vertrauen in die Mitarbeiter in Saudi-Arabien und den Vereinigten Arabischen Emiraten am stärksten um 19 Prozentpunkte auf **51 %** bzw. um 18 Prozentpunkte auf **43 %**.

Das größere Vertrauen in die Versiertheit der Mitarbeiter in Sicherheitsfragen zeigt sich auch in anderen Bereichen: In diesem Jahr glauben mit **56 %** Zustimmung weniger CISOs, dass menschliche Fehler die größte Cyberschwachstelle ihres Unternehmens ist.

Anteil der CISOs, die bestätigen, dass menschliche Fehler die größte Cyberschwachstelle in ihrem Unternehmen sind



Wenn **60 %** der CISOs glauben, dass ihre Mitarbeiter ihre Sicherheitsverantwortung verstehen, gleichzeitig aber **56 %** der Meinung sind, die Mitarbeiter wären die größte Cyberbedrohung, wirft das mehrere Fragen auf. Scheinbar ist vielen CISOs bewusst, dass die meisten ihrer Mitarbeiter nicht ausreichend auf ihre Rolle bei der Cyberabwehr vorbereitet sind.

Das Weltwirtschaftsforum meldet, dass **95 %** der Cybersicherheitsprobleme auf menschliche Fehler zurückzuführen sind.[5] Dies zeigt, dass viele CISOs die Risiken durch ihre Anwender immer noch deutlich unterschätzen. Nur **38 %** der CISOs in Saudi-Arabien sehen ihre Mitarbeiter als die größte Cyberschwachstelle, gefolgt von Italien (**43 %**) und Japan (**46 %**).

Das gilt auch für den Bildungssektor, wo nur **47 %** glauben, ihre Anwender würden das größte Risiko darstellen. Das andere Ende des Spektrums führten CISOs von Geschäfts- und Professional Services sowie Fertigungsunternehmen mit **61 %** bzw. **60 %** Zustimmung an.

Auch in anderen Bereichen gab es in den letzten 12 Monaten Veränderungen. So glaubt bei den CISOs im Gesundheitswesen in diesem Jahr nur etwas mehr als die Hälfte (**52 %**), dass die eigenen Mitarbeiter das Unternehmen gefährden, während es 2021 noch **48 %** waren. Das Gegenteil ist im Finanzsektor der Fall, wo **52 %** jetzt der Meinung sind, ihre Mitarbeiter würden das größte Cyberrisiko darstellen, während es im Jahr zuvor noch **61 %** waren.

„Bedrohungsakteure gehen immer raffinierter vor, während gleichzeitig Systeme sowie Daten zunehmend flexibler und grenzenloser genutzt werden. Daher müssen sich Sicherheitsverantwortliche und Geschäftsführer auf Prioritäten und Partner konzentrieren, die sie dabei unterstützen, die Angriffsfläche zu vereinfachen, zu verkleinern, sie zu verwalten und die damit verbundenen Ausgaben zu kontrollieren, damit auch neue und veränderte Bedrohungen keine Chance haben.“

Patrick Joyce, Vice President und Chief Security Officer (CISO und CSO), Medtronic

5 Weltwirtschaftsforum: „The Global Risks Report 2022 17th Edition Insight Report“ (Bericht zu weltweiten Risiken 2022), Januar 2022.

Kapitel 3: Risiken, Remote-Arbeit und die große Kündigungswelle

Die erzwungene Migration zu Homeoffice- und Hybrid-Arbeitsmodellen in den letzten Jahren diente als riesiger Testballon. Nach etwa 24 Monaten haben Unternehmen erkannt, welche Vorteile diese Arbeitsweise für Flexibilität, Kosteneinsparungen und Produktivität bedeutet.

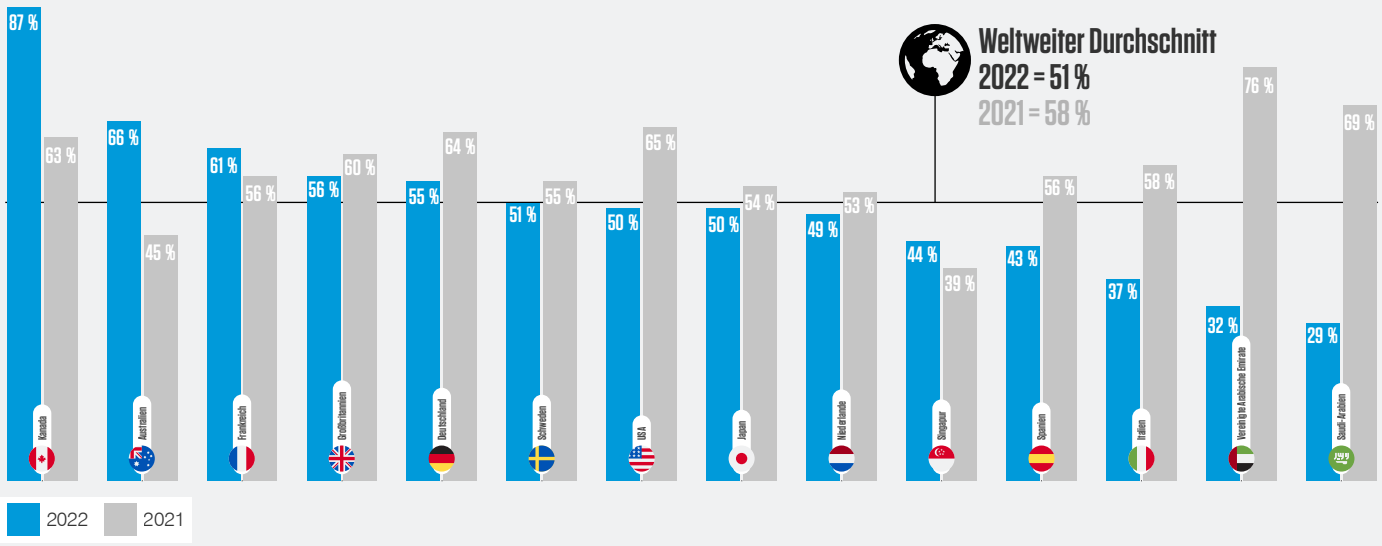
Da das Arbeitsmodell auch bei den Angestellten beliebt ist, wird es wahrscheinlich von Dauer sein. Und weil der Sicherheitsperimeter nun von den Mitarbeitern und ihrem jeweiligen Arbeitsplatz gebildet wird, benötigen Unternehmen eine neue Strategie.

Wie sich immer wieder zeigt, werden Anwender durch Hybrid- und Remote-Arbeitsmodelle auch verwundbarer für Angriffe. Und gleichzeitig stellen sie in jedem Fall ein sehr viel attraktiveres Ziel für Cyberkriminelle dar.

51 % der CISOs beobachten seit der massenhaften Einführung von Telearbeit mehr zielgerichtete Angriffe.

Mehr als die Hälfte der CISOs in allen Regionen bestätigt, dass gezielte Angriffe auf ihr Unternehmen seit der massenhaften Einführung von Hybrid-Arbeitsmodellen zugenommen haben. Im vergangenen Jahr gaben noch **58 %** der Umfrageteilnehmer diese Antwort. Den Rückgang führen wir darauf zurück, dass sie Erfahrungen mit dieser Umgebung sammeln konnten. Dennoch ist die Veränderung nicht erheblich und zeigt, dass die meisten CISOs eine erhöhte Bedrohungslage wahrnehmen. Dabei ist dieser Risikofaktor nicht das einzige Problem, das durch die breite Einführung von Hybrid-Arbeit entstanden ist.

Anteil der CISOs, deren Unternehmen seit der massenhaften Einführung von Telearbeit mehr zielgerichtete Angriffe erlebt hat



Kleine Unternehmen scheinen stärker betroffen zu sein: **59 %** der Unternehmen mit weniger als 500 Mitarbeitern werden seit der Einführung von Hybrid-Arbeitsmodellen häufiger angegriffen. Umgekehrt trifft das nur für **48 %** der großen Unternehmen (mehr als 5.000 Mitarbeiter) zu.

Die am stärksten betroffene Branche ist der Fertigungssektor (**65 %**), während Einzelhandel und Transportbranche mit **43 %** am wenigsten betroffen waren.

87 % der CISOs in Kanada und **66 %** in Australien melden eine Zunahme gezielter Angriffe nach dem breiten Wechsel ins Homeoffice. Das ist der größte Anteil in unserer Untersuchung.

In Saudi-Arabien berichteten dagegen nur **29 %** der CISOs von einer höheren Zahl zielgerichteter Angriffe. Die USA liegen mit dem weltweiten Durchschnitt von **50 %** gleichauf.

Die große Kündigungswelle: Eine neue Herausforderung für Sicherheitsteams

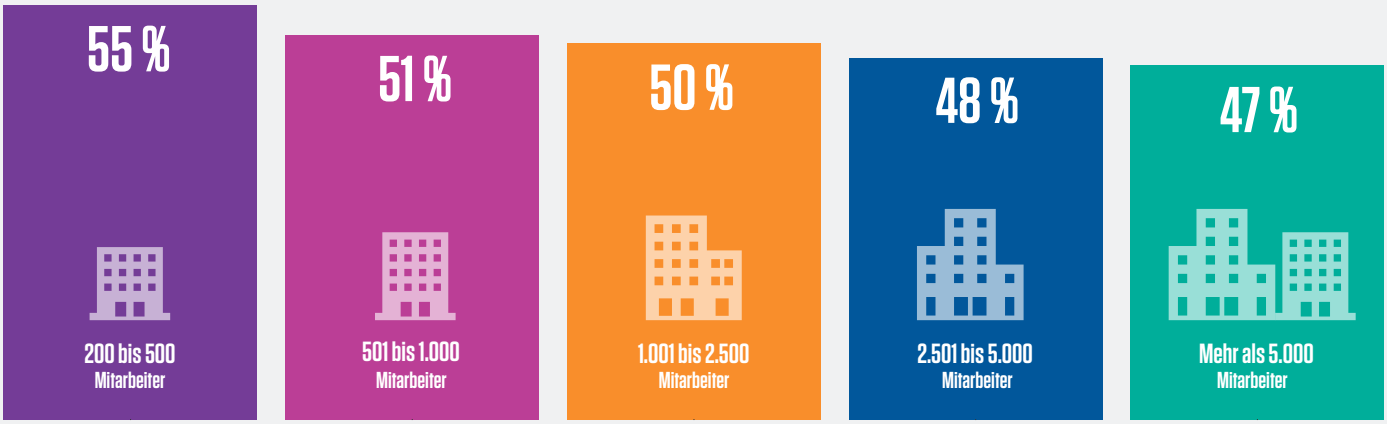
Angestellte verlassen ihre Unternehmen in großen Zahlen, sei es aufgrund von Burnout nach der Pandemie, Problemen bei der Kinderbetreuung oder veränderter Vorstellungen von der Work-Life-Balance. Ganz gleich, was der Grund ist: Die Cybersicherheit steht in jedem Fall auf dem Spiel.

Die große Kündigungswelle: 50 % der CISOs weltweit sind der Meinung, dass die Absicherung von Daten schwieriger geworden ist.

Wenn Angestellte kündigen, nehmen sie oft ihre Daten mit. Das kann ein Versehen sein, z. B. wenn gespeicherte Anmeldedaten auf einem privaten Gerät gespeichert sind. In vielen Fällen steckt jedoch Absicht dahinter. Ehemalige Angestellte haben vielleicht das Gefühl, die von ihnen erarbeiteten Daten würden ihnen gehören, oder sie möchten damit ihre neue Karriere anschieben.

Unabhängig von den Beweggründen erschwert diese Entwicklung vielen CISOs die Absicherung ihrer Daten. Ganz besonders trifft dies kleinere Unternehmen, die weniger Kontrollen implementiert haben: Für **55 %** der Umfrageteilnehmer aus Unternehmen mit weniger als 500 Mitarbeitern ist die Absicherung von Daten schwieriger geworden. Bei größeren Unternehmen (mehr als 5.000 Mitarbeiter) ist das nur bei **47 %** der Fall.

Anteil der CISOs, für die das Absichern von Daten schwieriger geworden ist (nach Unternehmensgröße)



„Die fundamentale Veränderung der Arbeitsweise in den letzten zwei Jahren hat nicht nur zu zahlreichen Schwierigkeiten geführt, sondern auch Chancen eröffnet. In erster Linie ist das die Einführung umfassender Strategien für Informationsschutz, die sich nicht auf die Absicherung von Netzwerken und anderen IT-Ressourcen beschränkt.“

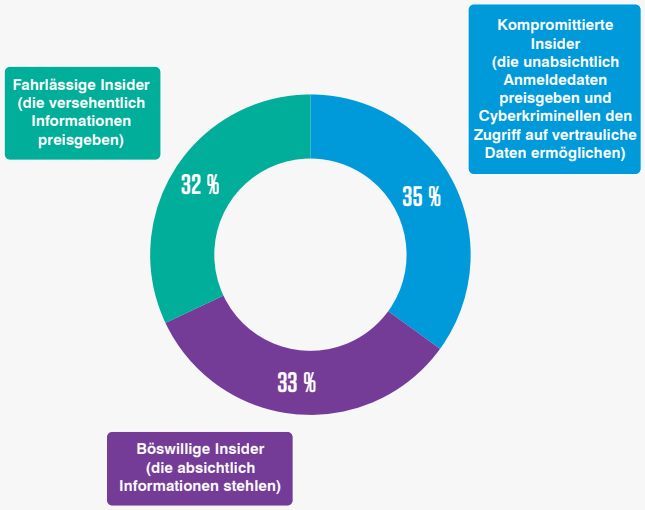
Paige Adams, Global Chief Information Security Office, Zurich Insurance Group

Daten bewegen sich nicht von selbst...

Sie werden von Angestellten bewegt – und nicht immer absichtlich. Ein weiteres Datenschutzproblem sind Kündigungen von Mitarbeitern. Wenn diese sich nach einem anderen Arbeitgeber umsehen, legen sie manchmal Verhaltensweisen an den Tag, die von Cyberkriminellen ausgenutzt werden. Dazu gehören unsachgemäßer Umgang mit Kennwörtern, die Umgehung von Sicherheitsmaßnahmen und die Nutzung von Unternehmensgeräten für private Zwecke.

Solche Verhaltensweisen sind die häufigste Ursache von Insider-Bedrohungen, da aktuelle Untersuchungen zeigen, dass **56 %** der Zwischenfälle auf Fahrlässigkeit zurückzuführen sind.[6] Und da mehr Angestellte außerhalb der Büroumgebung arbeiten und somit größere Freiheiten in Bezug auf ihre Sicherheitshygiene besitzen, sind kompromittierte, fahrlässige und böswillige Insider für CISOs weltweit ein Problem.

Datenverlust: Mit welcher Art von Datenschutzverletzung oder Unternehmens-kompromittierung durch Ihre Mitarbeiter rechnen Sie in den nächsten 12 Monaten am ehesten?



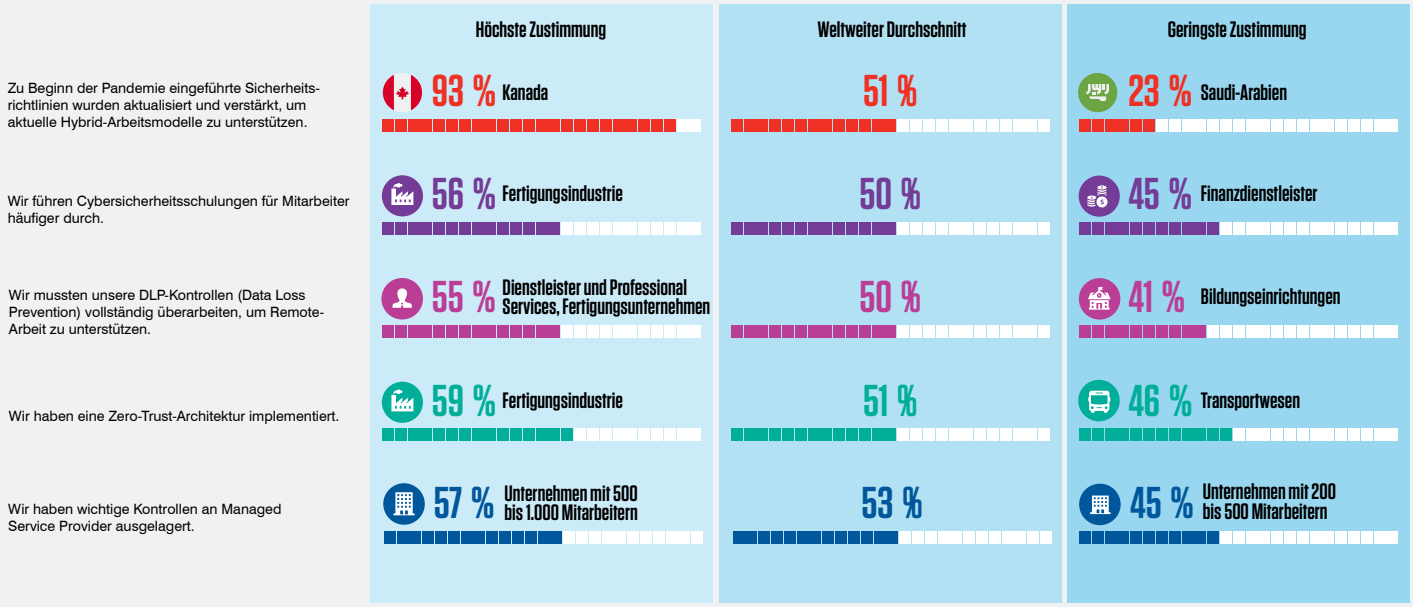
So reagieren Unternehmen auf die Herausforderungen von Hybrid-Arbeitsmodellen

Die Reaktionen auf diese wachsende Bedrohung fielen gemischt aus. Während CISOs in Ländern wie Kanada die Richtlinien aus der COVID-Zeit anpassten, um dem Trend zur Hybrid-Arbeit Rechnung zu tragen, hat das global betrachtet nur die Hälfte der CISOs (**51 %**) getan.

Die Hälfte aller weltweit befragten CISOs führt häufiger Cybersicherheitsschulungen für Mitarbeiter durch. Dies ist zwar ein gutes Zeichen, doch die Kehrseite der Medaille ist, dass **50 %** ein erhöhtes Risiko gezielter Angriffe zulassen. Abwehrstrategien, die auf die Bereitstellung einer Zero-Trust-Architektur und die Neugestaltung von DLP-Lösungen (Data Loss Protection) setzen, hatten für die Hälfte der Teilnehmer Priorität.

Die Auslagerung wichtiger Kontrollen zu Managed Service Providern wurde bei Unternehmen mit 500–1.000 Mitarbeitern am häufigsten genannt.

Wie sehr stimmen Sie den folgenden Aussagen in Bezug auf den Homeoffice-Trend zu?



6 Proofpoint: „Global Cybersecurity Study: Insider Threats Cost Organizations $15.4 Million Annually, up 34 Percent from 2020“ (Weltweite Untersuchung zur Cybersicherheit: Unternehmen entstehen durch Insider-Bedrohungen jährliche Kosten in Höhe von 15,4 Mio. USD – ein Anstieg um 34 % ggü. 2020), Januar 2022.

Kapitel 4: Eindämmung von Ransomware

Ransomware gehört schon sehr lange zum Arsenal von Bedrohungsakteuren, doch das Jahr 2021 zeigte, wie häufig diese Art von Schadsoftware tatsächlich eingesetzt wird. Ransomware findet wie keine andere Bedrohung leichte Ziele und garantiert große und schnelle Beute.

56 % der CISOs weltweit sind der Meinung, dass die medienwirksamen Ransomware-Angriffe aus den letzten zwei Jahren bei Unternehmensführungen das Bewusstsein für Cyberrisiken erhöht haben.

Die Häufigkeit und Komplexität dieser Angriffe hat im letzten Jahr um mehr als **150 %** zugenommen[7], was diesen alten Trick zu einer der größten Gefahren für moderne Unternehmen macht. Nach mehreren medienwirksamen Zwischenfällen in den letzten Jahren ist vielen CISOs klargeworden, dass sie Ransomware mehr Aufmerksamkeit widmen müssen.

Im Mai 2021 legte ein Angriff eine der größten Pipelines in den USA still[8] und nur kurze Zeit später musste der größte Fleischverarbeiter der Welt 11 Millionen US-Dollar Lösegeld zahlen, um seine Produktion wieder aufnehmen zu können.

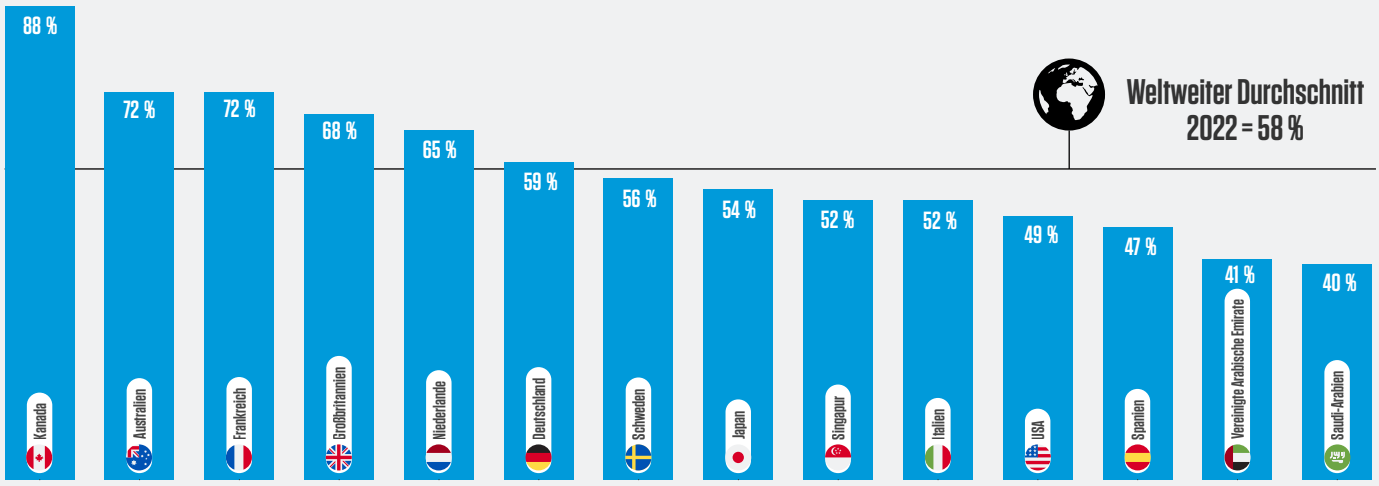
Die Höhe dieses Lösegeldes scheint außergewöhnlich hoch, doch Experten fürchten, dass dies schon bald zum Normalfall werden könnte. Die Gruppe hinter dem Pipeline-Hack soll im letzten Jahr eine Beute von mindestens 90 Millionen US-Dollar gemacht haben.[9] Gleichzeitig haben sich 2021 sowohl die durchschnittliche Lösegeldhöhe als auch die höchste Lösegeldforderung im Vorjahresvergleich verdoppelt.[10] Schlimmer ist jedoch, dass Lösegeldzahlungen nicht immer bedeuten, dass das Problem damit gelöst ist: Die Hälfte der zahlenden Opfer wird später erneut angegriffen.[11]

Doch obwohl so viel auf dem Spiel steht, scheinen viele Unternehmen nicht auf solche Erpressungen vorbereitet – unabhängig von deren Höhe und Ausmaß. Sorgen bereitet uns, dass **42 %** der CISOs weltweit noch nicht einmal über eine Richtlinie verfügen, die den Umgang mit Lösegeldforderungen regelt.

58 % der CISOs weltweit erklärten, dass ihr Unternehmen mit einer Richtlinie festgelegt hat, ob Lösegeld für die Wiederherstellung der Daten gezahlt werden sollte.

Aufgrund dieser exorbitanten Summen gibt es zwischen Regierungen und Branchenorganisationen intensive Debatten um die Legalität von Lösegeldzahlungen. Es ist jedoch nicht damit zu rechnen, dass die „Zahlen oder nicht zahlen?"-Diskussion schon bald zu einer gesetzlichen Regelung führt – wenn es denn jemals dazu kommt.

Anteil der CISOs, deren Unternehmen eine Cyberversicherung abgeschlossen haben und darauf vertrauen, dass sie im Notfall einspringt



7 ENISA: „ENISA Threat Landscape 2021" (ENISA-Bericht zur Bedrohungslage 2021), Oktober 2021.
8 Proofpoint: „Kurzinformation zu einer Bedrohung: Ransomware", Juli 2021.
9 Joe Tidy (BBC News): „Ransomware: Should paying hacker ransoms be illegal?" (Ransomware: Sollte die Lösegeldzahlung an Hacker illegal werden?), Mai 2021.
10 ENISA: „ENISA Threat Landscape 2021" (ENISA-Bericht zur Bedrohungslage 2021), Oktober 2021.
11 Proofpoint: „Was ist Ransomware?".

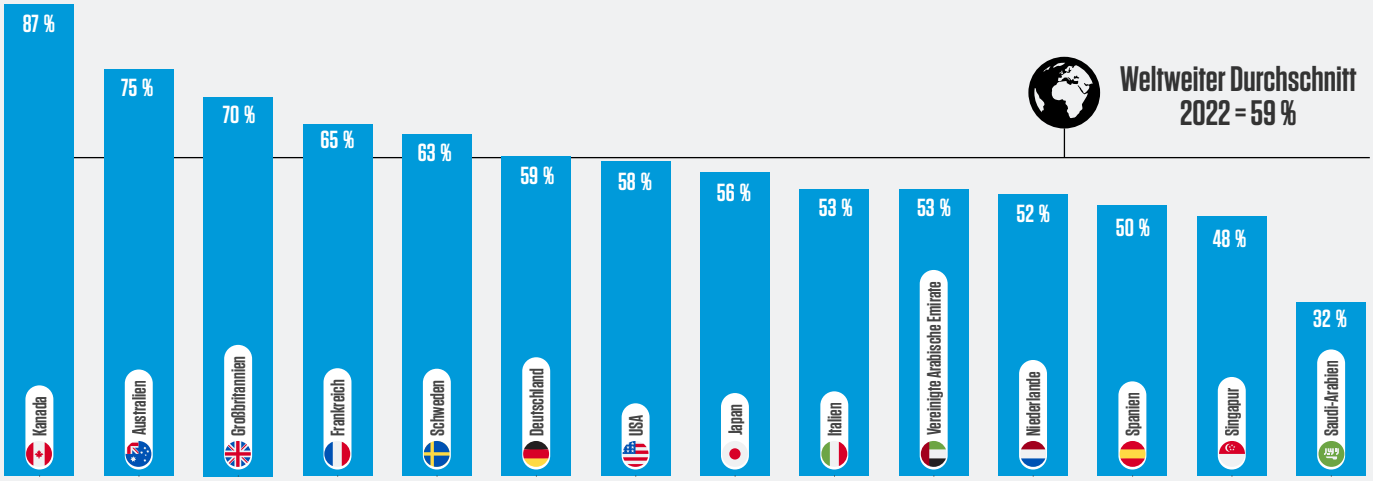
Gleichzeitig haben viele Unternehmen Cyberversicherungen abgeschlossen, um sich zusätzliche Sicherheit zu verschaffen. Mehr als die Hälfte (**58 %**) der CISOs weltweit vertraut darauf, dass ihr Versicherungsanbieter bei einem Zwischenfall zahlen wird, wobei CISOs in Kanada mit **88 %** das größte Vertrauen haben. Im Gegensatz dazu sind nur **40 %** der saudi-arabischen CISOs von ihrem Versicherer überzeugt.

59 % der CISOs weltweit konzentrieren sich stärker auf Ransomware-Prävention als auf Erkennung und Reaktion.

Die CISOs tun gut daran, skeptisch zu sein. Viele Versicherungsanbieter deckeln ihre Schadenssumme bei Ransomware-Attacken erheblich – und einige bieten überhaupt keine solchen Versicherungen mehr an.[12] Dies ist ein weiterer Grund dafür, dass Unternehmen sich weniger auf Reaktion und Wiederherstellung und mehr auf die Prävention konzentrieren sollten.

Ransomware ist nicht mehr der primitive Brute-Force-Angriff von einst. Anstatt einzubrechen, Dateien zu verschlüsseln und Lösegeld zu verlangen, legen sich heutige Cyberkriminelle heimlich auf die Lauer und warten ab, um maximale Wirkung zu erzielen. Mittlerweile schleicht sich Ransomware förmlich durch die Netzwerke und infiziert dabei Systeme, löscht Backups und exfiltriert Daten, sodass klassische Reaktionsstrategien wirkungslos werden.

Anteil der CISOs, die sagen, dass sich ihr Unternehmen auf die Prävention von Ransomware-Angriffen statt auf Erkennung und Reaktion konzentriert



Aus diesem Grund ändern einige CISOs ihre Vorgehensweisen. Fast **60 %** setzen verstärkt auf Prävention statt auf Reaktion. Andere sind hingegen erschreckend schlecht vorbereitet: **40 %** aller CISOs verfügen nicht über einen Plan für den Fall einer Ransomware-Infektion.

„Obwohl Ransomware in den letzten 18 Monaten ein so großes Thema war, sind Ransomware und damit zusammenhängende Erpressungsversuche auch weiterhin unser größtes Cybersicherheitsproblem. Die enorme Menge der Angriffe sowie die Entwicklungen bei Ransomware-Modellen zeigen, dass sich das Problem weiter verschärft. Die Abwehr dieser Bedrohung wird zudem dadurch erschwert, dass unsere Produktionssysteme und Lieferketten gezielt ins Visier genommen werden.“

Simon Strickland, Chief Information Security Officer, Johnson Matthey

12 Carolyn Cohn (Reuters): „Insurers run from ransomware cover as losses mount“ (Versicherer geben angesichts steigender Verluste auf), November 2021.

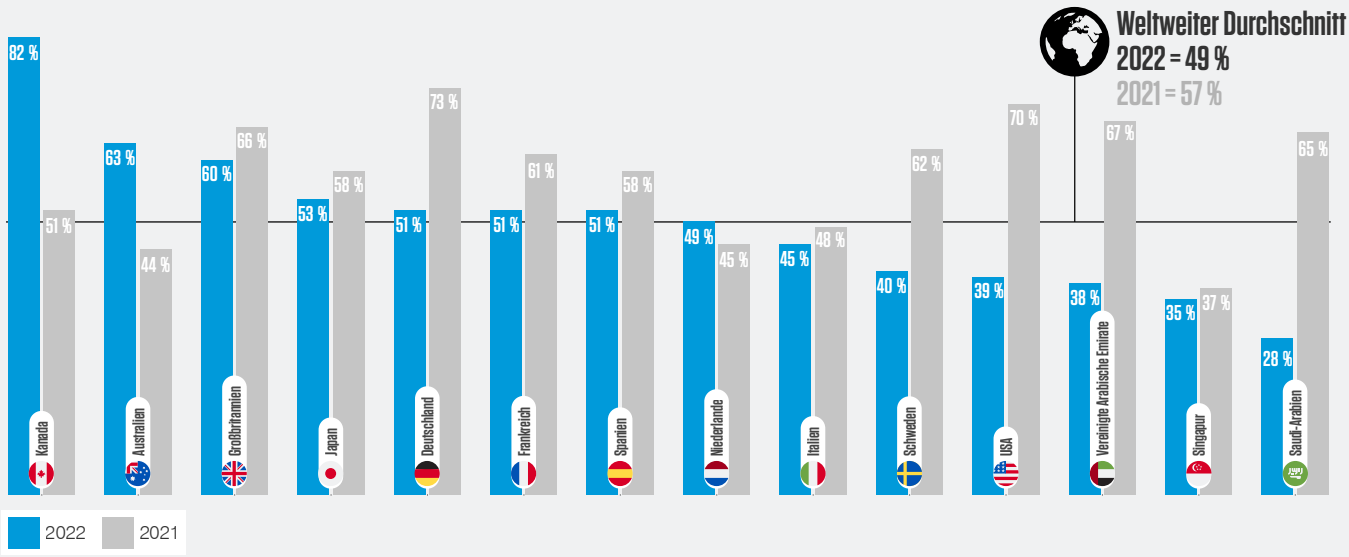
Kapitel 5: Vorstände, Überzeugungsarbeit und Rendite – die Sicht der CISOs

Durch die tragende Rolle der Cybersicherheit während der weltweiten Pandemie ist die Rolle des CISO so anspruchsvoll – und so wichtig – wie nie zuvor. Die enormen Anforderungen der letzten zwei Jahre haben dieser Position größere Prominenz verschafft und die CISOs ermutigt, ihre Meinungen laut und deutlich zu äußern.

Die CISOs sind sich in allen Regionen einig, dass die Erwartungen ihrer Vorgesetzten und Kollegen überzogen sind. Dabei unterscheiden sich die Ansichten von CISOs jedoch je nach Land sehr und haben sich zudem im letzten Jahr stark gewandelt. Dennoch hat die Hälfte der CISOs das Gefühl, vor einer unmöglichen Aufgabe zu stehen.

Die Hälfte der befragten CISOs findet, dass übertriebene Erwartungen an sie gestellt werden. Im letzten Jahr waren das noch 57 %.

Anteil der CISOs, die finden, dass die Erwartungen an ihre Rolle überzogen sind



Während deutsche CISOs am häufigsten der Meinung waren, dass die Erwartungen an ihre Rolle im vergangenen Jahr übertrieben waren, empfanden CISOs in Kanada den Druck im Jahr 2021 am höchsten.

Berichten am seltensten über überzogene Erwartungen: CISOs in Saudi-Arabien (**28 %**), Singapur (**35 %**) und in den Vereinigten Arabischen Emiraten (**38 %**).

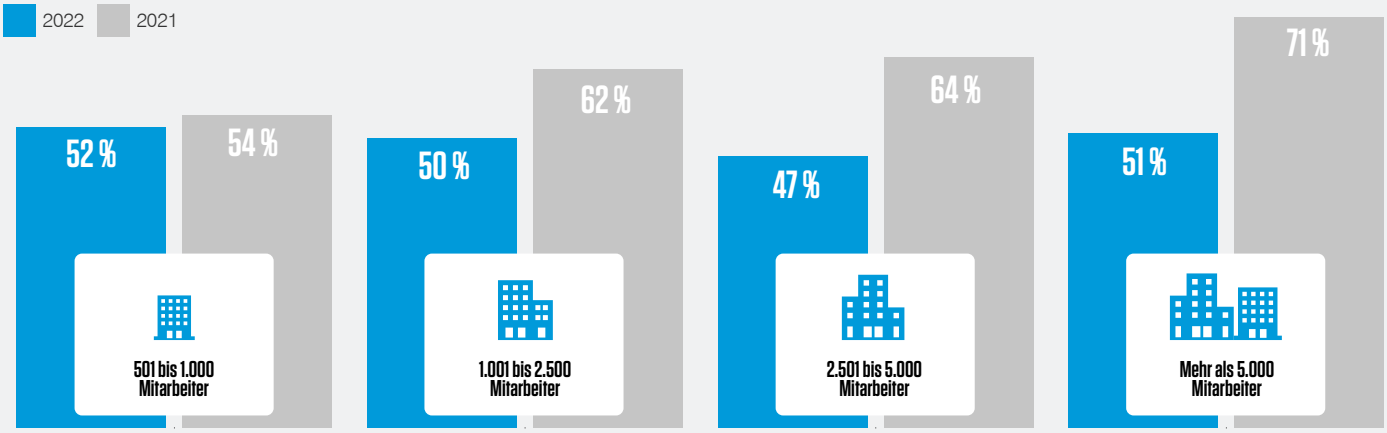
31 % mehr kanadische CISOs als noch 2021 sind der Meinung, dass in diesem Jahr überhöhte Erwartungen an sie gestellt werden. In den USA ist das Gegenteil der Fall.

Branchenübergreifend äußerten CISOs von Dienstleistern und Professional Services-Anbietern mit **57%** häufiger als ihre Kollegen aus anderen Branchen, dass überzogene Erwartungen an sie gestellt werden. Am wenigsten unter Druck sind CISOs im Bildungssektor (**39 %**) sowie im Einzelhandel (**42 %**).

CISOs kämpfen nicht nur mit einer hohen und zudem häufig undankbaren Arbeitslast, sondern auch mit unzureichender Unterstützung durch die Geschäftsführung, was sich seit 2021 verschärft hat. Nur etwas mehr als die Hälfte (**51 %**) der CISOs auf der ganzen Welt hatte im Jahr 2021 das Gefühl, sich beim Thema Cybersicherheit mit der Unternehmensleitung auf Augenhöhe zu befinden – ein starker Rückgang im Vergleich zum Vorjahr, als es noch **59 %** waren.

Diese Veränderung hängt auch von der Größe der Belegschaft ab und zeigt, dass CISOs in kleineren Unternehmen vor größeren Schwierigkeiten stehen. Dennoch wird der Rückgang bei der Unterstützung der Geschäftsführung auch von den meisten CISOs in großen Unternehmen (mehr als 5.000 Mitarbeiter) wahrgenommen: Während sich im letzten Jahr noch **71 %** unterstützt fühlten, sind es aktuell nur noch **51 %**.

Anteil der CISOs, die sich beim Thema Cybersicherheit mit der Geschäftsführung auf Augenhöhe fühlen (nach Unternehmensgröße)



Durchschnittliche Zustimmung = 51 %

Die fehlende Unterstützung und Abstimmung hat nicht nur Auswirkungen auf die verfügbaren Ressourcen und das Budget. Viele CISOs berichten auch, dass ihre Vorgesetzten direkt ihre Arbeitsleistung beeinträchtigen.

Mehr als die Hälfte (**51 %**) aller CISOs weltweit sagen, dass die festgelegte Berichtslinie die Effektivität ihrer Tätigkeit beeinträchtigen kann. Diese Ansicht ist bei geschäftlichen Dienstleistungen (**58 %**) und im Technologiesektor (**54 %**) besonders häufig zu finden. Bei Finanzdienstleistern sowie im Medien- und Bildungssektor ist dieses Problem jedoch deutlich seltener anzutreffen. Hier stimmten nur **46 %** dieser Aussage zu.

Nur die Hälfte der CISOs (50 %) auf der ganzen Welt glaubt, dass sie in ihrem Unternehmen erfolgreich arbeiten können.

Auch in anderen Bereichen ist die Beziehung zwischen CISO und Unternehmensführung angespannt: Nur die Hälfte der weltweit befragten CISOs ist heute der Meinung, dass sie in ihrem Unternehmen erfolgreich arbeiten können, während es vor einem Jahr noch **60 %** waren.

Im Gesundheitswesen sowie im Bildungsbereich fühlten sich CISOs am wenigsten von ihrem Arbeitgeber unterstützt, während sie bei Fertigungsunternehmen und in der Technologiebranche am besten arbeiten konnten.

„Überzogene Erwartungen sind das Ergebnis schlechter Unternehmensführung. Jeder CISO sollte sicherstellen, dass zuverlässige Methoden zur Risikokontrolle implementiert sind, damit sich das Unternehmen auf seine Kernaufgaben konzentrieren kann. Es kann nicht von CISOs erwartet werden, dass sie das Unternehmen zu jeder Zeit vor allen Bedrohungen schützen. Wenn das Unternehmen seine Risiken nicht ausreichend minimiert, muss die Unternehmensführung die Konsequenzen dafür tragen.“

Christian Toon, CISO, Pinsent Masons LLP

Details zu CISO-Prioritäten und Sorgen von Unternehmensführungen

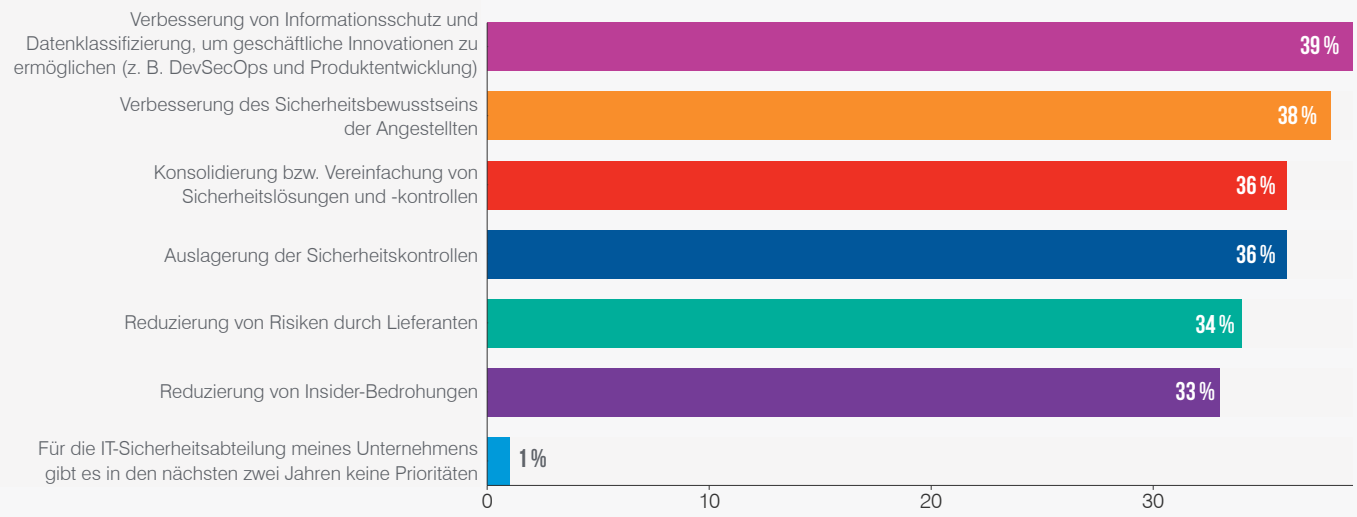
Folgende drei IT-Sicherheitsaspekte haben bei CISOs weltweit für die nächsten zwei Jahre die höchste Priorität:

- Verbesserter Informationsschutz (**39 %**)
- Verbesserung des Bewusstseins für Cybersicherheit (**38 %**)
- Konsolidierung und Auslagerung von Sicherheitslösungen und Kontrollen (**36 %**)

Während die ersten beiden Kategorien bei CISOs schon immer sehr hoch im Kurs standen, ist der letzte Punkt sicherlich auf die Ereignisse seit 2020 zurückzuführen. Da Angestellte im Homeoffice, im Büro sowie unterwegs arbeiten, werden IT-Umgebungen immer komplexer. Das bedeutet, dass zur Gewährleistung der Sicherheit neue Kompetenzen und zusätzliche Ressourcen benötigt werden.

Auch die große Kündigungswelle spielt hier eine Rolle. Da sich Angestellte in großer Zahl beruflich neu orientieren, müssen Unternehmen sicherstellen, dass sie stets über die Expertise und Kompetenz verfügen, um ihre Cyberstrategie umsetzen zu können. Dabei kann sich Auslagerung als kostengünstige und effiziente Möglichkeit erweisen.

Welche Maßnahmen haben für die IT-Sicherheitsabteilung Ihres Unternehmens in den nächsten zwei Jahren oberste Priorität? Wählen Sie bis zu drei Optionen aus.



Selbstverständlich sind Prioritäten je nach Branche und Unternehmen unterschiedlich. Bei großen Unternehmen mit mehr als 5.000 Mitarbeitern, deren IT-Umgebungen fast immer sehr komplex sind, hat Auslagerung für **41 %** die größte Priorität. Das liegt deutlich oberhalb des Durchschnitts bei allen anderen Unternehmensgrößen.

Innerhalb der Branchen ist die Verbesserung der Informationssicherheit die größte Priorität von Unternehmen in den Bereichen IT, Technologie, Telekommunikation, Finanzdienstleistungen, Fertigung sowie dem öffentlichen Sektor.

Auch von Land zu Land unterscheiden sich die Prioritäten. In Großbritannien stehen Anwenderschulungen ganz oben auf der Agenda: **46 %** erklärten, dass Sicherheitsbewusstsein unverzichtbar ist – eine leichte Zunahme gegenüber dem Vorjahr. Aber auch in anderen Ländern haben Schulungen hohe Priorität: Ganz oben in der Liste stehen die USA, Kanada, die Niederlande, Spanien und Australien. In Italien bleibt das Lieferantenrisiko eine der größten Sorgen und wird von **38 %** der CISOs zu den drei größten Prioritäten der nächsten zwei Jahre gezählt.

Die Effizienz hat für CISOs in Deutschland, Schweden und Japan die höchste Priorität. In diesen Ländern stehen die Konsolidierung und Optimierung von Sicherheitslösungen und -kontrollen an höchster Stelle.

Sorgen von Unternehmensführungen

Die Schlagzeilen bei Cybersicherheitsvorfällen aus den letzten zwei Jahren haben Führungskräfte auf der ganzen Welt an die aktuellen Cyberrisiken erinnert.

Wir wollten von CISOs auf der ganzen Welt wissen, was ihrer Geschäftsführung bei einem Cyberangriff auf das Unternehmen die größten Sorgen bereitet. Genannt wurden erhebliche Ausfallzeiten (**37 %**), Unterbrechung von Geschäftsabläufen (**36 %**) sowie Auswirkungen auf die Unternehmensbewertung (**36 %**).

Im Gegensatz dazu wurden Umsatzverluste am seltensten genannt, vielleicht, weil dieser Aspekt als Konsequenz der Top-3-Sorgen statt als direkte Auswirkung betrachtet wird. In jedem Fall machten sich Führungskräfte großer Unternehmen (mehr als 5.000 Mitarbeiter) die meisten Sorgen.

Cybersicherheitssorgen von Führungskräften: Wie schätzen Sie schlussfolgernd aus Ihren Interaktionen mit der Unternehmensführung deren größte Sorgen in Bezug auf einen schwerwiegenden Cyberangriff ein? Wählen Sie bis zu drei Optionen aus.

	Erhebliche Ausfallzeiten	Unterbrechung von Geschäfts-abläufen	Auswirkungen auf die Unternehmens-bewertung	Rufschädigung	Verlust aktueller Kunden	Umsatzverluste	Keine großen Sorgen
WELTWEIT	37 %	36 %	36 %	35 %	35 %	33 %	1 %
USA	34 %	40 %	47 %	36 %	37 %	39 %	1 %
Kanada	39 %	33 %	40 %	39 %	41 %	34 %	3 %
Großbritannien	42 %	33 %	48 %	37 %	35 %	29 %	0 %
Frankreich	44 %	45 %	48 %	45 %	47 %	46 %	0 %
Deutschland	42 %	26 %	40 %	30 %	38 %	29 %	5 %
Niederlande	29 %	31 %	21 %	39 %	31 %	23 %	0 %
Schweden	36 %	41 %	38 %	31 %	31 %	29 %	2 %
Italien	35 %	33 %	26 %	36 %	36 %	28 %	0 %
Spanien	28 %	34 %	26 %	37 %	28 %	33 %	0 %
Saudi-Arabien	29 %	39 %	35 %	27 %	37 %	38 %	4 %
Vereinigte Arabische Emirate	45 %	33 %	39 %	31 %	30 %	39 %	2 %
Australien	49 %	42 %	34 %	29 %	32 %	33 %	0 %
Singapur	36 %	33 %	29 %	31 %	33 %	32 %	1 %
Japan	34 %	44 %	34 %	42 %	36 %	31 %	2 %

Hauptsorge Zweit-/drittrangige Sorge

Weltweit betrachtet, sehen Unternehmensführungen in den USA, Großbritannien und Frankreich die Auswirkungen auf die Unternehmensbewertung als größtes Problem. Dagegen bereiten Reputationsschäden den Führungskräften in den Niederlanden, Italien und Spanien die größten Sorgen. In Deutschland, den Vereinigten Arabischen Emiraten, Australien sowie Singapur wiederum stehen erhebliche Ausfallzeiten an erster Stelle.

Für CISOs im Einzelhandel ist Rufschädigung das größte Risiko. Die Auswirkungen auf die Marke standen bei Unternehmensführungen in den Bereichen IT, Technologie und Telekommunikation weit oben auf der Agenda.

Erhebliche Ausfallzeiten stehen bei Führungskräften im Bildungssektor, bei Fertigungsunternehmen sowie bei Dienstleistern an erster Stelle, während die Unterbrechung von Geschäftsabläufen den Geschäftsführern im Gesundheitswesen die größten Sorgen bereitet.

Die Auswirkungen auf die Unternehmensbewertung werden vor allem von Unternehmen im Energie-, Öl- und Gassektor sowie von Versorgungsunternehmen als problematisch angesehen, aber auch in der IT-, Technologie- und Telekommunikationsbranche sowie in der Medien- und Unterhaltungsbranche.

Fazit

Da die CISOs sich in den letzten zwei Jahren an die neue Situation angepasst haben, haben viele ein deutlich besseres Gefühl in Bezug auf die aktuellen Bedrohungen. Zusammengefrickelte Systeme und hastig erstellte Richtlinien wurden durch strategischere Cyberabwehrmaßnahmen ersetzt. Gleichzeitig sind die Angestellten mittlerweile sehr gut mit der Arbeit außerhalb der Büroumgebung vertraut. Aus diesem Grund glauben CISOs auf der ganzen Welt, dass ihre Mitarbeiter besser mit ihrer Sicherheitsverantwortung vertraut sind – und ihre Unternehmen besser in der Lage sind, mit einem Cyberangriff umzugehen.

Häufig ist dieses Gefühl der Sicherheit jedoch unbegründet, da gezielte Angriffe, Ransomware und Insider-Bedrohungen zunehmen. Und weil die meisten Cyberangriffe auf menschliche Interaktionen angewiesen sind, bleiben Menschen auch weiterhin der größte Risikofaktor. Ein großer Grund zur Sorge ist, dass trotz der Hybrid-Arbeitsmodelle nur relativ wenige CISOs die Schutzmaßnahmen für den Mitarbeiter-Perimeter verstärkt haben.

Doch wieder einmal ist es möglich, dass ihnen schlicht die Möglichkeiten fehlen, ihre Mitarbeiter zu unterstützen. Ebenso wie im vergangenen Jahr gibt es in Bezug auf die Cybersicherheit oft Uneinigkeit zwischen CISOs und ihrer Unternehmensführung. Und viele sind der Meinung, dass die festgelegte Berichtslinie die Effektivität ihrer Tätigkeit beeinträchtigt.

Die gute Nachricht dabei ist: CISOs auf der ganzen Welt wissen, an welchen Stellen Verbesserungen nötig sind. Viele arbeiten bereits daran, Lösungen für Informationsschutz und Schulungen zur Sicherheitssensibilisierung auszubauen, was bei dauerhaft genutzten Hybrid-Umgebungen unverzichtbar ist. Auch dem Mangel an Kompetenzen und Fachkräften wird Rechnung getragen: Viele CISOs haben vor, in den kommenden Jahren Sicherheitslösungen auszulagern.

Insgesamt betrachten CISOs das Jahr 2022 als Ruhe nach dem Sturm. Doch angesichts wachsender geopolitischer Spannungen und zunehmender personenzentrierter Angriffe müssen die Lücken bei Sicherheitsbewusstsein, Vorbereitung und Prävention geschlossen werden, bevor in der Cybersicherheit der nächste Sturm losbricht.

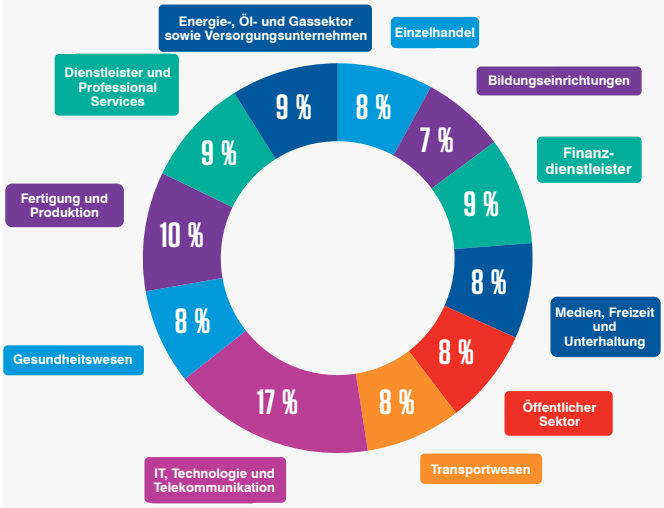
„Die heutigen Probleme von CISOs sind mindestens ebenso auf das Unternehmen wie auf die Technologie zurückführen. Cyberzwischenfälle treffen Unternehmen auf vielerlei Weise – von Rufschäden, die Vertrauen und Umsätze beeinträchtigen, bis hin zu potenziellen Strafen, die von Behörden verhängt werden. Deshalb muss der CISO von der Unternehmensführung gehört werden, um nicht nur Kennzahlen zur Cybersicherheitslage des Unternehmens zu präsentieren, sondern auch, um den Führungskräften die geschäftlichen Risiken verständlich darzulegen.“

Patrick Gaul, Executive Director, National Technology Security Coalition

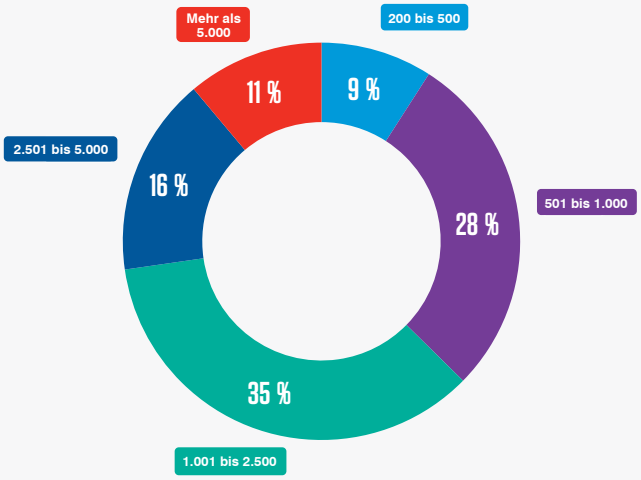
Methodik

Die Proofpoint Voice of the CISO-Umfrage 2022 wurde vom 22. Februar bis zum 8. März vom Forschungsunternehmen Censuswide durchgeführt. Dabei wurden 1.400 Chief Information Security Officer aus Unternehmen mit mindestens 200 Mitarbeitern befragt, wobei die Unternehmen in verschiedenen Branchen und 14 Ländern tätig sind. Für jeden Markt (USA, Kanada, Großbritannien, Frankreich, Deutschland, Italien, Spanien, Schweden, Niederlande, Vereinigte Arabische Emirate, Saudi-Arabien, Australien, Japan und Singapur) wurden je 100 CISOs interviewt.

Aufteilung der Umfrageteilnehmer nach Branche:



Aufteilung der Umfrageteilnehmer nach Unternehmensgröße:



Censuswide hält die Grundsätze des MRS Code of Conduct und ESOMAR ein.

proofpoint®

Kontaktieren Sie uns unter info@proofpoint.com, um zu erfahren, wie Sie Ihr Unternehmen besser schützen können.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter www.proofpoint.de.

0400-008-0101 05/22