netskope

Bericht +

Der moderne CISO:

Ein Gleichgewicht schaffen

Auf alles vorbereitet

Inhaltsverzeichnis

Zusammenfassung

Unternehmen müssen jeden Tag einen Balanceakt vollziehen, sei es zwischen Innovation und Zuverlässigkeit, Investition und Gewinn oder Geschwindigkeit und Sicherheit. Jede Führungskraft hat einen Einfluss darauf, wie Entscheidungen abgewogen und getroffen werden. Als „Schutzpatron" des Unternehmens befand sich der Chief Information Security Officer (CISO) bislang auf der der sicheren Seite dieser Skala.

Eine neue Studie von Netskope, bei der 1.031 CISOs weltweit befragt wurden, zeigt jedoch, dass dieses Rollenbild nicht länger der Realität entspricht. 65% der Befragten waren der Meinung, dass sich die Rolle des CISO rapide verändert. CISOs spielen im Unternehmen eine immer proaktivere Rolle: 59% bezeichnen sich selbst als „Business Enabler", 57% geben an, dass ihre Risikobereitschaft in den letzten Jahren zugenommen hat, und 67% wollen in Zukunft eine noch aktivere Rolle als „Business Enabler" spielen.

CISOs haben sich in den letzten zehn Jahren grundlegend verändert; heute sind sie von ihrer Fähigkeit überzeugt, ihr Unternehmen umgestalten zu können.

Die meisten haben jedoch das Gefühl, dass ihr Potenzial von anderen Führungskräften nicht ausreichend anerkannt wird. Zwei von drei CISOs (65%) glauben, dass ihre Rolle als Türöffner für Innovation von anderen Mitgliedern der Führungsebene nicht wahrgenommen wird, und 92% halten Unterschiede in der Risikobereitschaft für ein Problem der Führungsebene.

Die Forscher von Netskope hatten sich zum Ziel gesetzt, die Meinungen von CISOs zu strategischen und taktischen Fragen zu erfassen. Was taktische Aspekte betrifft, glauben CISOs, dass der zunehmende Trend hin zu Zero-Trust-Prinzipien ihnen dabei helfen wird, ein Gleichgewicht in ihren Unternehmen zu schaffen – sofern sie dabei richtig vorgehen. Die Mehrheit der CISOs (55%) ist der Meinung, widersprüchliche Prioritäten mit einem Zero-Trust-Ansatz besser ausbalancieren zu können und dass ein solcher Ansatz ihrem Unternehmen dabei helfen kann, wichtige Ziele zu erreichen, z. B. eine schnellere Entwicklung (59%) und mehr Innovation (58%).

Diese Einschätzungen klingen sehr optimistisch. Tatsache ist jedoch, dass derzeit nur 44% der Unternehmen Zero-Trust-Prinzipien anwenden, während 48% nicht wissen, wie sie den Einstieg in Zero-Trust vollziehen sollen.

Das dem Zero-Trust-Modell zugrundeliegende Paradox könnte ein Grund dafür sein, warum das Verständnis und die Akzeptanz dieses Ansatzes noch relativ gering sind. Da das Zero-Trust-Prinzip zusätzliche Kontrollen erfordert, wird die Behauptung, es könne die Flexibilität und Geschwindigkeit eines Unternehmens erhöhen, oft als kontraintuitiv empfunden.

58% der CISOs berichten, dass sich ihre Führungsteams und Vorstände nach Zero Trust erkundigen. Das Interesse an dem Konzept scheint jedoch größer zu sein als das Verständnis desselben. CISOs, die sich die Vorteile von Zero Trust zunutze machen und sich die Wertschätzung ihrer Kollegen in der Führungsetage sichern wollen, sollten Gespräche über Business Enablement und Geschäftsrisiken anregen und sich nicht auf die üblichen Überlegungen zu Investitionen in Tools beschränken, bevor die notwendigen geschäftlichen Diskussionen stattgefunden haben.

57 % **der CISOs geben an, dass sich ihre Risikobereitschaft in den vergangenen Jahren erhöht hat**

59 % **sehen sich als Business Enabler**

92 % **haben Schwierigkeiten mit der unterschiedlichen Risikobereitschaft in der Führungsetage**

Der fortschrittliche CISO von heute

Chief Information Security Officers (CISOs), deren Aufgabe seit jeher darin bestand, für die Sicherheit ihrer Unternehmen zu sorgen, werden gewöhnlich als übervorsichtig und defensiv wahrgenommen. Aufgrund ihrer großen Risikoscheu wurden sie von Kollegen sogar manchmal als „Abteilung der Neinsager" bezeichnet. Neue Forschungen von Netskope haben jedoch ergeben, dass dieses Bild überholt ist. Eine Umfrage, bei der 1.031 CISOs aus fünf Ländern (Vereinigte Staaten, Großbritannien, Frankreich, Deutschland, Japan) und aus den unterschiedlichsten Branchen befragt wurden, von Industrie bis Einzelhandel, ergab ein völlig anderes Bild – ein Ergebnis, das die Kollegen und Kolleginnen in den Vorstandsetagen der CISOs zu einer Neubewertung veranlassen sollte.

Einfach ausgedrückt: Die Rolle des CISO verändert sich rapide. Zu diesem Urteil kamen fast zwei Drittel der CISOs (65%), die von Netskope zu ihrer Risikobereitschaft, ihren Beziehungen zur Kollegenschaft und weiteren Themen befragt wurden.

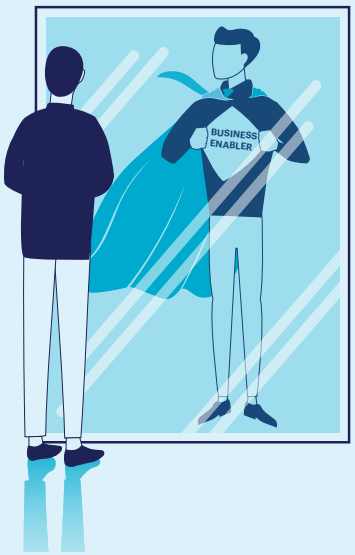
Eines ist sicher: CISOs haben die ihnen früher anhaftenden altmodischen Klischees längst hinter sich gelassen. Sie sehen ihre Hauptaufgabe nicht mehr in der Risikominderung, die sie oft durch die Unterbindung von Innovationen und die Schaffung undurchdringlicher Verteidigungsanlagen zu realisieren suchten. 62% der CISOs wollen nicht mehr als „Überbringer schlechter Nachrichten" wahrgenommen werden,

sondern begrüßen die zentrale Rolle, die ihnen digitale Technologien in modernen Unternehmen einräumen. Sie nehmen die damit verbundenen neuen Möglichkeiten bereitwillig an, um Innovationen voranzutreiben und geschäftliche Veränderungen zu bewirken. Kein Zweifel: Es gibt heute eine neue Generation fortschrittlicher CISOs, die bereit sind, neue Wege zu beschreiten und sich für ein Gleichgewicht in ihren Unternehmen einzusetzen.

> 62 % der CISOs wollen in ihren Unternehmen nicht mehr als „Überbringer schlechter Nachrichten" wahrgenommen werden

Länder im Blickpunkt

In Deutschland spüren CISOs diesen Wandel am wenigsten: 52 % sind der Meinung, dass sich ihre Rolle schnell verändert. In Japan hingegen ist wird er am stärksten wahrgenommen: 89 % der CISOs geben an, dass sich ihre Rolle schnell verändert.



Ein neues Selbstverständnis

Diese Veränderungen zeigen sich auch in der Art, wie CISOs ihre berufliche Identität wahrnehmen. Zwar sehen sich derzeit 36% in der Rolle des „Beschützers“„ der das Unternehmen verteidigt, doch dieser Prozentsatz dürfte immer weiter zurückgehen. Die Zahl der CISOs, die als „Designer“ wirken und die Arbeitskultur mitgestalten wollen, wird in den nächsten zwei Jahren voraussichtlich zunehmen, ebenso der Anteil jener, die sich als „Navigatoren“ sehen und die zukünftige Richtung des Unternehmens mitbestimmen möchten.

Es scheint sich also eine kontinuierliche Verlagerung von einer eher defensiven zu einer proaktiven Enabler-Rolle zu vollziehen.

Diese veränderte Selbstwahrnehmung des Sektors sollte eigentlich nicht überraschen. Schon seit einiger Zeit ist zu beobachten, dass sich Branchenverbände und Beratungsunternehmen einer neuen Sprache bedienen, die eine veränderte Wahrnehmung der Rolle des Sicherheitsexperten widerspiegelt. Bei den meisten Branchenveranstaltungen und -konferenzen gibt es heutzutage eher eine Sitzung zum Thema „Resilienz“ als zum Thema „Cybersicherheit“ schlechthin. Entsprechend werden Risiken von diesen Branchengruppen immer häufiger als unternehmensweite und nicht als rein technische Probleme angesehen. Bei unserer Umfrage gaben 65% der CISOs an, sich zunehmend für die Verbesserung der Resilienz des Unternehmens und nicht nur für die Verwaltung von Cyberrisiken verantwortlich zu fühlen.

Wodurch zeichnet sich ein fortschrittlich denkender CISO in der Praxis aus? Vor allem durch den Wunsch, eine proaktivere Rolle in seinem Unternehmen zu spielen. 66% der CISOs wünschen sich, bei geschäftlichen Entscheidungen öfter „Ja“ sagen zu können.

Genau das meinen CISOs, wenn sie sagen, dass sie gern als „Business Enabler“ fungieren würden. Die Mehrheit der CISOs (59%) sieht sich bereits in dieser Funktion, und 67% wollen in Zukunft eine noch aktivere Rolle als Business Enabler spielen. Nur jeder Vierte (26%) sieht sich derzeit nicht als „Business Enabler“, würde dies jedoch gerne sein.

> 65 % der CISOs sehen ihre Aufgabe zunehmend darin, die Resilienz des Unternehmens zu verbessern und nicht nur für das Management von Cyberrisiken verantwortlich zu sein.

Länder im Blickpunkt

43 % der CISOs in Großbritannien sehen sich noch nicht als „Business Enabler“, würden es aber gerne werden (gegenüber einem weltweiten Durchschnitt von 26 %). Dieses Ergebnis dies spiegelt die Tatsache wider, dass die Zahl der CISOs, die sich bereits als Enabler in ihrem Unternehmen sehen, in Großbritannien am geringsten ist.

> 67% der CISOs weltweit wollen in Zukunft eine noch aktivere Rolle als Business Enabler spielen

Wachsendes Selbstvertrauen

CISOs erwarten auch, mit zunehmendem Selbstbewusstsein in den kommenden Jahren eine größere Reife bei ihrer Entscheidungsfindung zu erlangen. Dies geht aus ihren Antworten auf einige Fragen zu typischen beruflichen Problemsituationen hervor.

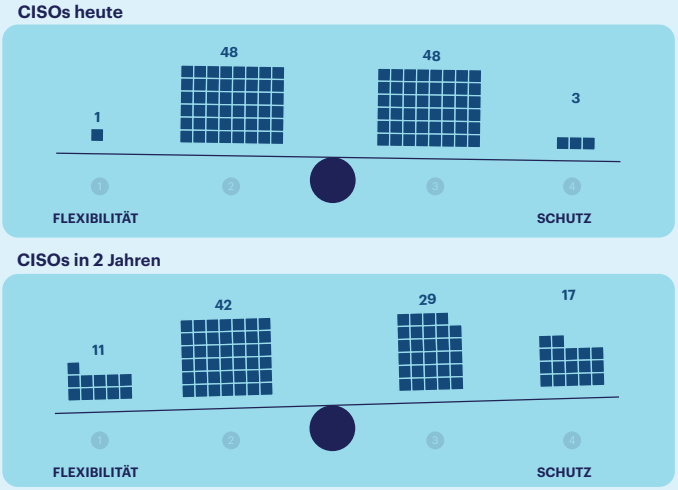
Mit Hinblick auf vier Kernbereiche, in denen häufig wichtige Geschäftsentscheidungen getroffen werden – Produktivität, Innovation, Prozesse und Agilität – wurden die CISOs gefragt, ob sie eher eine offene und flexible oder eine geschlossene und sichere Organisation anstreben. Diese Skala wurde bewusst gewählt, um eine offensichtliche Bevorzugung eines der beiden Extreme zu vermeiden.

Die Daten zeigen, dass CISOs derzeit eher in der Mitte der Skala angesiedelt sind. Mit Blick auf die nächsten zwei Jahre nehmen sie jedoch einen entschiedeneren Standpunkt ein. Dieses Muster zeichnet sich in allen vier Bereichen der Entscheidungsfindung ab, und das Ergebnis wirft einige interessante Möglichkeiten auf. Warten CISOs derzeit noch darauf, dass das Unternehmen bestimmte Entscheidungen trifft, oder beobachten sie die aktuellen Marktbedingungen, bevor sie sich auf eine Seite der Skala festlegen? Vielleicht sind sie gerade dabei, ihre technische Infrastruktur auszubauen und ihre Sicherheitslage zu verbessern, damit bald weniger Druck auf sie ausgeübt wird, dieses Gleichgewicht zu schaffen.

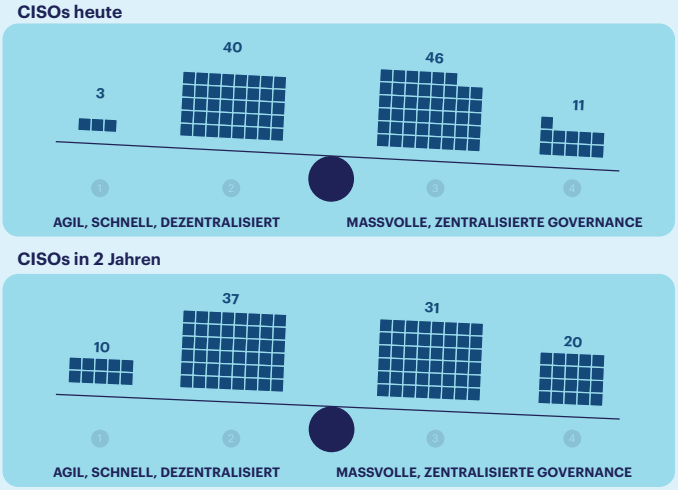
Q Wo sehen Sie sich auf einer Skala von 1 bis 4, wenn Sie als CISO Entscheidungen für das Unternehmen treffen?

■ Anzahl der Befragten

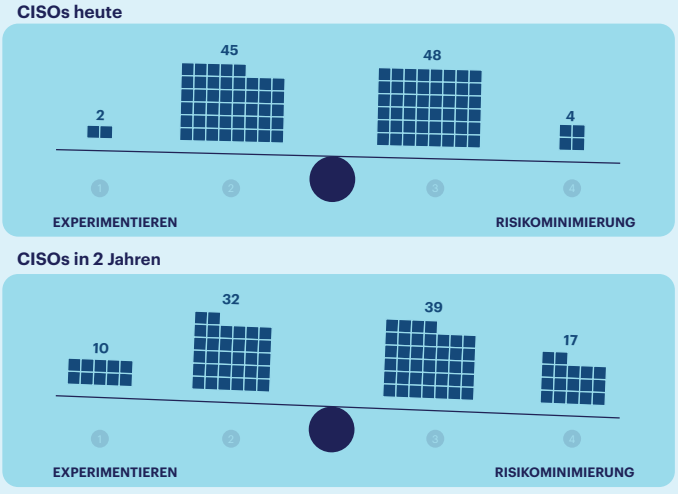
Produktivität der Belegschaft:
Die Notwendigkeit, dafür zu sorgen, dass Ihre Mitarbeiter überall sicher und effektiv arbeiten können



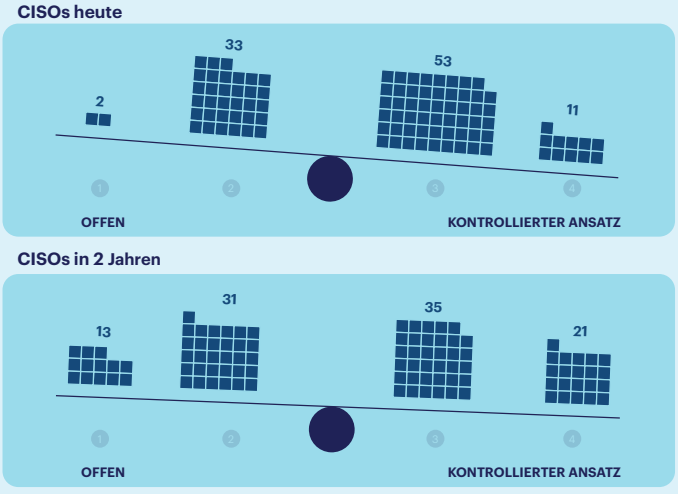
Geschäftliche Agilität:
Die Reaktionsfähigkeit des Unternehmens. Seine Fähigkeit, wichtige Entscheidungen zu treffen und wettbewerbsfähig zu bleiben



Unternehmerische Innovation:
Die Notwendigkeit der kontinuierlichen Weiterentwicklung und des Wachstums eines Unternehmens



Geschäftsprozesse und Effizienz:
Den richtigen Personen Zugang zu den benötigten Informationen, Daten und Instrumenten geben



Was auch immer der Grund dafür sein mag: CISOs rechnen damit, in den nächsten Jahren entscheidungsfreudiger zu werden – ein weiteres Anzeichen für die Veränderung ihrer Rolle.

Bemerkenswerterweise hat sich die Risikobereitschaft von CISOs in den letzten fünf Jahren trotz der Zunahme von Cyberbedrohungen erhöht. Dies ist die Meinung der Mehrheit (57 %). Jeder Siebte (13%) sagt sogar, dass die Risikobereitschaft erheblich zugenommen hat.

Als wichtiger Grund für die wachsende Risikobereitschaft wird ein besserer Zugang zu Daten und Analysen (76%) angegeben. Der zweithäufigste Grund sind Erfahrungen aus erster Hand, die CISOs mit einem bestimmten Cybersicherheitsproblem hatten (74%).

> Was auch immer der Grund dafür sein mag: CISOs rechnen damit, in den nächsten Jahren entscheidungsfreudiger zu werden – ein weiteres Anzeichen für die Veränderung ihrer Rolle

Sich widersprechende Perspektiven

Aus den erfassten Daten geht eindeutig hervor, dass CISOs bereit und willens sind, eine aktivere Rolle in ihren Unternehmen zu übernehmen, die auf einer selbstbewussteren Risikohaltung beruht. Dabei gibt es jedoch ein Problem. Auch wenn diese veränderten Denkweisen und Ambitionen positiv klingen und auf eine selbstbewusstere Berufsgruppe hindeuten, haben viele CISOs nach wie vor das Gefühl, von ihren Kollegen nicht uneingeschränkt akzeptiert zu werden.

Zwar halten 72% der von einer höheren Risikobereitschaft berichtenden CISOs ein neues Mandat der Geschäftsleitung für einen wichtigen Veränderungsfaktor, doch einige CISOs beklagen auch, dass ihre Kollegen in den Führungsetagen immer noch veraltete Ansichten in Bezug auf ihre Arbeit und ihren potenziellen Beitrag vertreten. Während zwei Drittel der CISOs das Gefühl haben, von anderen Führungskräften als „Business Enabler" wahrgenommen zu werden, ist fast jeder Dritte (30%) der Meinung, dass dies noch nicht der Fall ist.

Der Aussage, dass andere Mitglieder der Führungsebene die Rolle des CISO als Innovationsmotor nicht erkennen, stimmen immerhin 23% der Befragten voll und ganz zu. Als konkretes Beispiel aus der Praxis verweisen CISOs darauf, dass es bei ihrer Interaktion mit dem Unternehmen heute immer noch häufiger um Risikomanagement (58%) als um Chancen (42%) geht, obwohl sie gern verstärkt als Business Enabler fungieren würden.

Trotzdem sind sich die CISOs der Rolle bewusst, die sie in ihrem Unternehmen spielen können. Fast zwei Drittel (65%) glauben, dass sie mehr geschäftliche Innovationen in Gang setzen können als andere Mitglieder der Führungsetage. Dies spiegelt die zentrale Rolle digitaler Technologien in modernen Unternehmen wider, die die Entwicklung von KI-Anwendungen vorantreiben, Effizienzsteigerungen freisetzen und die sichere Umsetzung neuer Partnerschafts- und Lieferkettenmodelle unterstützen.

Q **Haben Sie das Gefühl, dass die Rolle des CISO von anderen Führungskräften als Business Enabler wahrgenommen wird?**

	Alle	UK	NA	FR	DE	JP
Ja	66 %	50 %	58 %	79 %	56 %	91 %
Nein	30 %	48 %	35 %	19 %	39 %	8 %
Ich weiß nicht	4 %	2 %	7 %	2 %	6 %	1 %

der CISOs glauben, dass sie mehr geschäftliche Innovationen bewirken können als andere Mitglieder der Führungsetage

glauben, dass sie von ihren Kollegen nicht als Enabler wahrgenommen werden

glauben, dass ihre Kollegen sie nicht für innovationsfördernd halten

Es gibt jedoch noch weitere Konflikte und Widersprüche. Lediglich 16% der befragten CISOs stufen ihre eigene Risikobereitschaft als gering ein. Doppelt so viele (32%) behaupten jedoch dasselbe von ihrem CEO. Diese beiden Zahlen zeigen, dass CISOs ihre eigene Risikobereitschaft für höher halten als die ihres CEOs – eine Umkehrung der gängigen Annahme. Die Teilnehmer der Studie berichten, dass diese unterschiedlichen Auffassungen zu ernstzunehmenden Problemen in der Vorstandsetage führen können.

Eine überwältigende Mehrheit (92%) der CISOs bestätigte, dass unterschiedliche Risikowahrnehmungen ein Problem in ihrer Führungsetage darstellen, wobei 32% von ihnen angaben, dass diese unterschiedlichen Wahrnehmungen häufig zu Konflikten führten.

Vor dem Hintergrund dieser sich widersprechenden Perspektiven und Ansätze bemühen sich CISOs intensiv darum, das richtige Gleichgewicht in ihrem Unternehmen zu schaffen. Sie müssen einen goldenen Mittelweg zwischen der Befähigung des Unternehmens und seinem Schutz finden und gleichzeitig die neuen Möglichkeiten ihrer Rolle nutzen, d.h. zum Erreichen der Unternehmensziele, beitragen, während sie ihre Kernaufgaben erfüllen und dafür sorgen, dass Sicherheitsprioritäten eingehalten werden.

Es überrascht daher nicht, dass eine große Mehrheit der CISOs (70%) ihre Rolle als „Balanceakt" betrachtet. Zwei Drittel (66%) haben das Gefühl, sich auf einer „Gratwanderung" zwischen den geschäftlichen und den sicherheitsbezogenen Anforderungen des Unternehmens zu befinden. Kein Wunder, dass 66% der CISOs die Beeinflussung und Schulung anderer Mitglieder der Führungsebene als einen zunehmend wichtigen Aspekt ihrer Rolle ansehen.

Länder im Blickpunkt

+ Dieser Meinung war man besonders in Frankreich und Japan, wo 74 % bzw. 88 % der Befragten das Gefühl hatten, dass andere Mitglieder der Führungsetage die innovationsfördernde Rolle des CISO derzeit nicht erkennen.

der CISOs stufen ihre Risikobereitschaft als gering ein

der CISOs würden die Risikobereitschaft ihres CEO als gering bezeichnen

+ Zero-Trust-Ansatz

Der Zero-Trust-Ansatz, der in der Theorie eher unflexibel klingt, ist vor allem deshalb attraktiv, weil er Unternehmen in der Praxis dabei hilft, flexibler zu werden, was in der schnelllebigen Welt von heute eine der obersten Prioritäten von Führungskräften ist. Voraussetzung für dem Erfolg dieses Ansatzes ist jedoch, dass er richtig umgesetzt wird (und zwar auf der Grundlage umfangreicher kontextbezogener Signale).

Wo suchen die CISOs also nach Lösungen und Strategien, die ihnen bei diesem Balanceakt helfen? Das „Zero-Trust"-Sicherheitsmodell scheint bei CISOs hoch im Kurs zu stehen: Sie führen eine Vielzahl von Vorteilen an, die sie sich von diesem Ansatz versprechen.

Das Prinzip „Zero Trust" ist nicht neu, sondern wurde bereits in den 90er Jahren entwickelt. Der Sicherheitsansatz fand aber erst in den späten 2010er Jahren Verbreitung. Inzwischen hat sich das Prinzip in der Branche durchgesetzt, da die herkömmlichen Methoden zur Zugriffskontrolle durch die Zunahme von cloudbasierten Services und Remote-Arbeit nicht mehr angemessen waren. Der Zero-Trust-Ansatz, der in der Theorie eher unflexibel klingt, ist vor allem deshalb attraktiv, weil er Unternehmen in der Praxis dabei hilft, flexibler zu werden, was in der schnelllebigen Welt von heute eine der obersten Prioritäten von Führungskräften ist. Voraussetzung für dem Erfolg dieses Ansatzes ist jedoch, dass er richtig umgesetzt wird (und zwar auf der Grundlage umfangreicher kontextbezogener Signale). Mit diesem Ansatz erhalten die richtigen Nutzern ohne die üblichen Reibungspunkte Zugang zu den von ihnen benötigten Ressourcen.

Dies ist einer der Gründe, warum so viele CISOs bereits eine sehr positive Einstellung gegenüber Zero-Trust-Prinzipien haben. Die Mehrheit (59%) ist der Meinung, dass Zero Trust Unternehmen in die Lage versetzt, sich schneller zu entwickeln (59%), Innovationen zu fördern (58%), flexibler zu werden (58%) und bessere Entscheidungen zu treffen (55%). 55% der CISOs glauben, mit einem Zero-Trust-Ansatz widersprüchliche Prioritäten besser ausgleichen zu können.

Was die Zukunft anbelangt, halten CISOs die Einführung eines Zero-Trust-Ansatzes sogar für den wichtigsten Faktor, der Unternehmen in den nächsten zwei Jahren zu mehr Offenheit und Flexibilität verhelfen kann.

Es gibt kein Sicherheitsmodell, das für sich allein genommen einen Königsweg darstellt. Die Studie macht jedoch deutlich, dass CISOs durchweg positive Erwartungen an Zero Trust haben und große Hoffnungen in den weiteren Einfluss des Modells setzen.

Es gibt einige Anzeichen dafür, dass Zero Trust bereits dazu beigetragen hat, das Vertrauen von Unternehmen und Informationssicherheitsabteilungen zu stärken. 73% der CISOs geben an, dass die Einführung eines Zero-Trust-Ansatzes im Unternehmen dazu beigetragen hat, ihre Risikobereitschaft in den letzten Jahren zu erhöhen (30% gehen noch weiter und sagen, dass der Ansatz eine sehr wichtige Rolle bei diesen Veränderungen der Risikobereitschaft gespielt hat).

Q **Wenn Ihr Unternehmen in den nächsten zwei Jahren von einer eher geschlossenen/geschützten Umgebung zu einer offeneren/flexibleren Umgebung übergehen würde, welche der folgenden Faktoren wären Ihrer Meinung nach für diese Entwicklung am wichtigsten?**

Letztendlich geht es bei Zero Trust darum, sicherzustellen, dass die richtigen Personen die richtigen Zugriffsmöglichkeit auf die richtigen Ressourcen im Netzwerk eines Unternehmens erhalten. Dabei geht es sowohl um Befähigung als auch um Kontrolle.

Ein scheinbares Paradox

Die befragten CISOs wiesen zwar vor allem auf die mit Zero Trust verbundenen Erwartungen und Möglichkeiten hin, doch einige Warnsignale sind trotzdem nicht zu überhören. So scheint sich die Begeisterung für das Zero-Trust-Modell bei den meisten Sicherheitsexperten und Unternehmen nicht immer unbedingt in praktischen Maßnahmen niederzuschlagen. Weniger als die Hälfte aller weltweiten Unternehmen (44%) arbeiten heute nach den Zero-Trust-Prinzipien und weitere 38% geben an, sie bald einführen zu wollen.

Bemerkenswert ist auch die Tatsache, dass das „Zero Trust"-Konzept anscheinend von der Unternehmensführung im Allgemeinen nicht gut verstanden wird, obwohl sie mit dem Begriff vertraut ist. 58% der CISOs berichten zwar, von ihrem Führungsteam zur Anwendung eines Zero-Trust-Ansatzes angehalten zu werden, doch nur 51% glauben, dass das Führungsteam bzw. der Vorstand diesen Ansatz wirklich versteht.

Es ist interessant zu sehen, inwieweit Sicherheitsverantwortliche von ihren Kollegen in der Führungsetage zum Thema Zero Trust befragt werden. Wenn CISOs ihr Ziel erreichen und als Business Enabler sowie strategische Partner anerkannt werden wollen, sollten sie sich im Gespräch mit anderen Führungskräften nicht zu sehr auf Tools und Technologien konzentrieren. Zero-Trust-Konzepte (und Zero-Friction-Konzepte) sind nur im Hinblick auf das wichtig, was sie ermöglichen - nämlich Risikominderung und Business Enablement.

> Das Paradox von Zero Trust besteht darin, dass eine möglichst geschlossene Umgebung das offenste, agilste und innovativste Unternehmen hervorbringt.

Das dem Zero-Trust-Modell zugrundeliegende Paradox könnte ein Grund dafür sein, warum das Verständnis und die Akzeptanz dieses Ansatzes noch relativ gering sind.

Zero-Trust-Prinzipien führen zu mehr Kontrollen und schränken den Zugriff auf das Unternehmensnetzwerk und seine Anwendungen ein. Das klingt zunächst nach zusätzlichen Reibungspunkten und einer Verlangsamung des Unternehmens. In Wirklichkeit ist jedoch das Gegenteil der Fall: Die Flexibilität und Schnelligkeit des Unternehmens erhöhen sich, da die detaillierten Kontrollen das Vertrauen in die Entscheidungsfindung stärken.

Mit anderen Worten: Das Paradox von Zero Trust besteht darin, dass eine möglichst geschlossene Umgebung das offenste, agilste und innovativste Unternehmen hervorbringt.

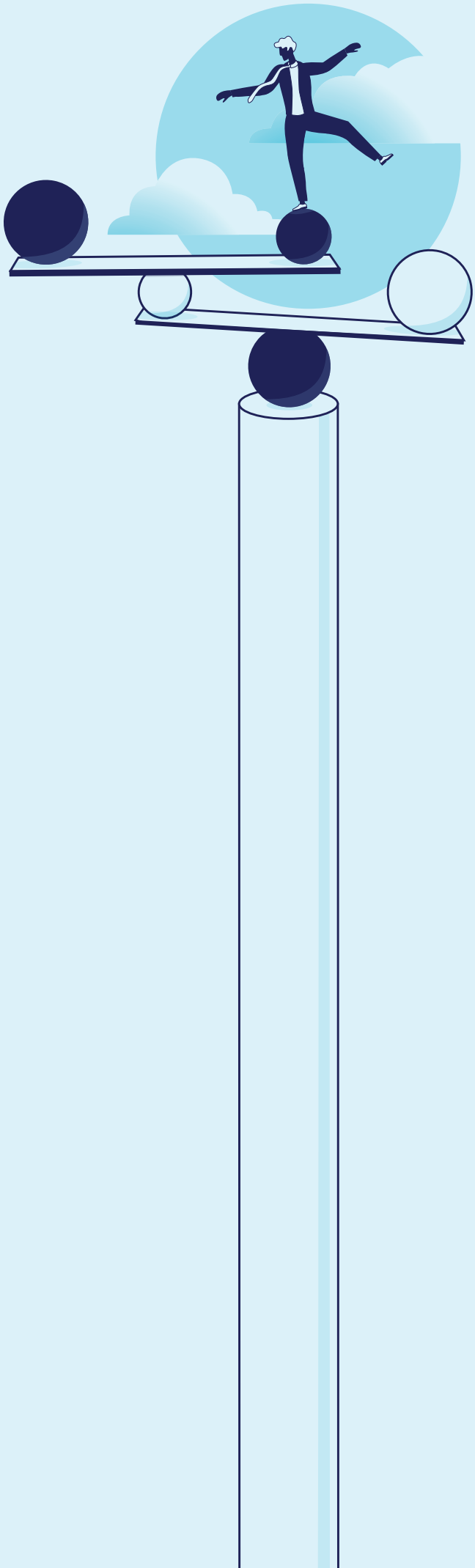
Q **Inwieweit stimmen Sie den folgenden Aussagen zu?**

58 %

Mein Führungsteam bzw. mein Vorstand fragt mich nach Zero Trust

51 %

Mein Führungsteam bzw. mein Vorstand versteht nicht wirklich, was Zero Trust ist



Fazit

Die Rolle des CISOs begann sich vor einem Jahrzehnt zu verändern. Die vorliegenden Daten zeigen, dass sich der moderne CISO aus dem Schatten anderer Mitglieder des Führungsteams herausgewagt hat und bereit ist, seiner Stimme in allgemeinen Unternehmensdiskussionen und Entscheidungsprozessen Gehör zu verschaffen.

Dieser globale Trend hat dazu geführt, dass sich selbstbewusste CISOs nicht mehr mit Back-Office-Supportfunktionen zufriedengeben. Sie wollen einen entscheidenden Beitrag zur Erreichung der Geschäftsziele leisten und das Unternehmen zu Wachstum und Innovation befähigen.

Doch auch wenn sich CISOs ihrer Fähigkeiten bewusst geworden sind, bleibt noch einiges zu tun, um das ihnen anhaftende Image abzubauen, denn nur allzu oft werden sie noch immer als Rückendeckung, technischer Sicherheitsdienst oder Schwarzmaler angesehen.

Die Entwicklung der Technologie hat CISOs dabei geholfen, ihre Ansichten in Bezug auf Risiken und ihre Rolle zu ändern, doch mit Technologie allein lässt sich die Wahrnehmung unter Fachkollegen nicht beeinflussen. Zero Trust ist das neueste Schlagwort, das auch bei nicht-technischen Stakeholdern immer beliebter wird. CISOs tun jedoch gut daran, diesen Begriff mit Vorsicht zu verwenden. Es ist zweifellos der richtige Ansatz, um eine Sicherheitsgrundlage für Business Enablement ohne Reibungspunkte zu schaffen, doch Gespräche mit Mitgliedern der Führungsebene sollten sich weniger auf Tools und Technologie konzentrieren, sondern vielmehr auf die Beantwortung der Frage: „Wie können wir diesen Business Case realisieren?“

CISOs, die genau aufzeigen können, wie sie ihre Kollegen in der Führungsetage bei der Erschließung neuer Umsatzquellen, der Effizienzsteigerung und der Einhaltung gesetzlicher Vorschriften unterstützen, werden auf höchster Ebene als wertvolle Akteure wahrgenommen.

Über Netskope

Netskope, ein weltweit führender Anbieter von SASE-Lösungen, hilft Organisationen bei der Einführung von Zero-Trust-Grundsätzen und KI/ML-Innovationen, um ihre Daten zu schützen und gegen Cyberbedrohungen zu verteidigen. Die schnell und einfach zu nutzende Plattform Netskope One und ihre patentierte Zero-Trust-Engine bieten optimierten Zugriff und Echtzeit-Sicherheit für Personen, Geräte und Daten, wo immer sie sich befinden. Tausende von Kunden vertrauen Netskope und seinem leistungsstarken NewEdge-Netzwerk, wenn es um die Verringerung von Risiken geht. Sie profitieren von unübertroffenen Einblicken in die Aktivitäten aller Cloud-, Web- und privaten Anwendungen und können ihre Sicherheitslage und Leistung ohne Kompromisse verbessern.
Weitere Informationen finden Sie unter netskope.com.