Delinea

Die Auswirkung von Business Alignment auf die Effektivität der Cybersicherheit

Globale Umfrage unter IT-Sicherheitsverantwortlichen

WHITEPAPER

Zusammenfassung

Die Auswirkungen der Cybersicherheit auf die Wirtschaft sind offensichtlich. Wenn beispielsweise ein massiver Cyberangriff stattfindet, kann das Business plötzlich zum Erliegen kommen, wie eine Notbremse, die einen mit voller Geschwindigkeit fahrenden Zug entgleisen lässt.

Über dieses Szenario hinaus wirkt sich die Arbeit des Cybersicherheitsteams auch auf die Effizienz des Tagesgeschäfts, die Geschwindigkeit der Servicebereitstellung, die Kosten, die Produktivität der Mitarbeiter, die Benutzererfahrung und den Umsatz aus. Diese Auswirkungen sind zwar nicht so dramatisch wie das Beispiel des Zugunglücks, aber sie können das Business verlangsamen und so stark vom Kurs abbringen, dass eine Wiederherstellung schwierig ist.

Die Bedeutung der Angleichung von Cybersicherheit und Business Enablement

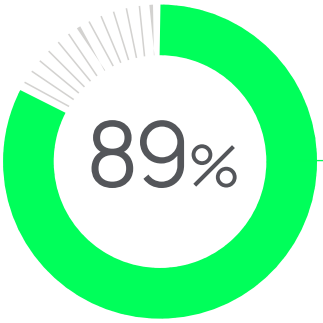
Angesichts der komplexen IT-Landschaft und des unsicheren Wirtschaftsklimas, dem Unternehmen ausgesetzt sind, ist die Abstimmung zwischen Cybersicherheit und Business für den Erfolg unerlässlich. Cybersicherheitsteams werden zunehmend darauf hingewiesen, dass sie nicht in einem Silo arbeiten und sich nur auf den Schutz der Technologie konzentrieren sollten. Sie hören, dass sie nicht die „Abteilung des Neinsagens" sein können und stattdessen „Business Enabler" werden müssen.

Viele sind sich jedoch nicht sicher, wie sie diese Schlagworte in die Tat umsetzen können. Die meisten Führungskräfte im Bereich der Cybersicherheit haben eine technische Ausbildung und sind in den technischen Abteilungen aufgestiegen. Womöglich haben sie die meiste Zeit ihrer Karriere in einem Silo gearbeitet. Ein Umdenken zum Umsetzen einer neuen Arbeitsweise lässt sich nicht über Nacht erreichen. Der erste Schritt besteht darin, sich ein genaues, gemeinsames Bild davon zu machen, wo unsere Branche heute steht.

In diesem Zusammenhang haben wir über 2.000 Entscheidungsträger im Bereich der Cybersicherheit in 22 Ländern befragt, die in Unternehmen mit mehr als 500 Mitarbeitern arbeiten, um den aktuellen Stand von Business Enablement zu verstehen. Genauer gesagt wollten wir mithilfe von Daten die Arten von Attributen ermitteln, die einen bedeutenden Einfluss auf das Business Enablement haben, einschließlich Ausrichtung, Fähigkeiten und Organisationsstrukturen.

Was wir herausgefunden haben, ist faszinierend und zugleich beunruhigend

Die Ergebnisse deuten darauf hin, dass die Cybersicherheitsbranche noch einen weiten Weg vor sich hat, um zu einem effektiven Business Enabler zu werden. Die Daten zeigen eine mangelnde Abstimmung zwischen den Teams und innerhalb der Teams, was sich negativ auf die Sicherheitslage und die Erreichung der Geschäftsziele auswirken kann.



Tatsächlich geben 89 % der Befragten an, dass ihr Unternehmen im vergangenen Jahr mindestens eine negative Auswirkung aufgrund mangelnder Cybersicherheit und mangelnder Geschäftsausrichtung erlitten hat.

Ein Großteil des Problems liegt darin, dass ein Unternehmen nicht in der Lage ist, Ziele und Messgrößen effektiv aufeinander abzustimmen. Und ein sehr großer Teil dieser Herausforderung besteht darin, dass die Unternehmen versuchen, sich über eine Vielzahl von Erwartungen zu einigen.

In diesem Bericht erhalten Sie einen Überblick über die aktuelle Situation und lernen einige der Faktoren kennen, die nicht nur die Cybersicherheitslage, sondern auch den Unternehmenserfolg bestimmen.

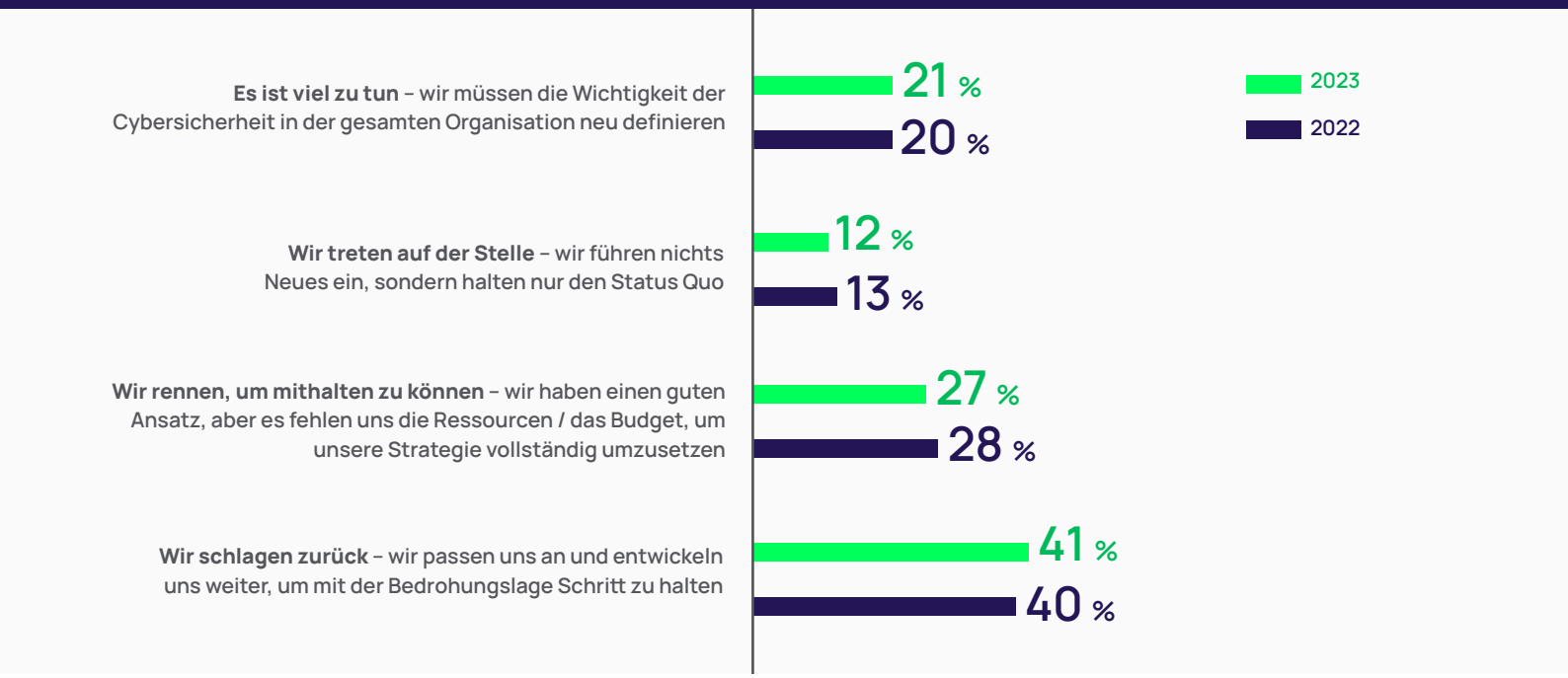
Wichtigste Erkenntnis 1

Wenn sich Führungskräfte im Bereich Cybersicherheit unsicher fühlen, ist es schwer, sich auf etwas anderes zu konzentrieren

Wir beginnen hier, um den Kontext zu verstehen, in dem Führungskräfte im Bereich der Cybersicherheit tätig sind.

Nur 40 % der befragten Entscheidungsträger geben an, dass sie bereit sind, den Kampf im Bereich der Cybersicherheit aufzunehmen. Tatsächlich sagen die meisten Sicherheitsverantwortlichen, dass sie einfach nur rennen, um mithalten zu können, auf der Stelle treten oder einfach noch extrem viel zu tun ist. Diese Prozentsätze sind im Vergleich zum letzten Jahr praktisch unverändert.

Abbildung 1 | Welche der folgenden Aussagen beschreibt Ihre derzeitige Sicherheitsstrategie am besten?



Interessanterweise sind sich die Mitarbeiter in den Teams nicht einig über den aktuellen Stand der Sicherheitslage ihres Unternehmens. Diejenigen, die eine höhere Position innehaben, beurteilen die derzeitige Sicherheitslage positiver als diejenigen, die tagtäglich für die IT und das Sicherheitsmanagement zuständig sind.

Abbildung 2 | Welche der folgenden Aussagen beschreibt Ihre derzeitige Sicherheitsstrategie am besten?

	CEO	CISO/CIO/CSO	IT- oder Sicherheitsdirektor	IT- oder Sicherheitsmanager
Es ist viel zu tun – wir müssen die Wichtigkeit der Cybersicherheit in der gesamten Organisation neu definieren	**39 %**	16 %	16 %	22 %
Wir treten auf der Stelle – wir führen nichts Neues ein, sondern halten nur den Status Quo	6 %	7 %	12 %	15 %
Wir rennen, um mithalten zu können – wir haben einen guten Ansatz, aber es fehlen uns die Ressourcen / das Budget, um unsere Strategie vollständig umzusetzen	17 %	21 %	28 %	31 %
Wir schlagen zurück – wir passen uns an und entwickeln uns weiter, um mit der Bedrohungslage Schritt zu halten	38 %	**56 %**	**44 %**	**32 %**

Ändern der Denkweise

Wenn man die Frage des „Business Enablement" in diesem Zusammenhang betrachtet, versteht man, warum es für eine Führungskraft im Bereich der Cybersicherheit schwierig sein könnte, ihren Aufgabenbereich über die Sicherheitsgrundlagen hinaus zu erweitern. Viele sind mit der täglichen Herausforderungen um den Schutz der Organisation und der reaktiven Bekämpfung von Bränden beschäftigt, sobald diese auftreten. Leider bedeutet dieser Mangel an Vertrauen in die Sicherheit, dass viele Führungskräfte im Bereich der Cybersicherheit nicht in der Lage sind, sich auch auf die Geschäftsziele zu konzentrieren.

Das wirklich Schlimme an dieser Situation sind die Opportunitätskosten. Der Druck, ein grundlegendes Sicherheitsniveau zu erreichen, „verdrängt" die Energie und die Ressourcen, die für die Verfolgung von Geschäftszielen benötigt werden, die traditionell nicht in den Verantwortungsbereich des Sicherheitsteams fallen.

Für einen CISO, für den noch sehr viel zu tun ist oder der sich abmühen muss, um mithalten zu können, kann der Ratschlag, sich auf die Geschäftsziele zu konzentrieren, seiner Weltanschauung zuwiderlaufen. Aber wie Sie in diesem Bericht erkennen werden, kann eine Verlagerung des Schwerpunkts auf die Einbeziehung von Geschäftszielen auch positive Auswirkungen auf die Sicherheitsziele haben.

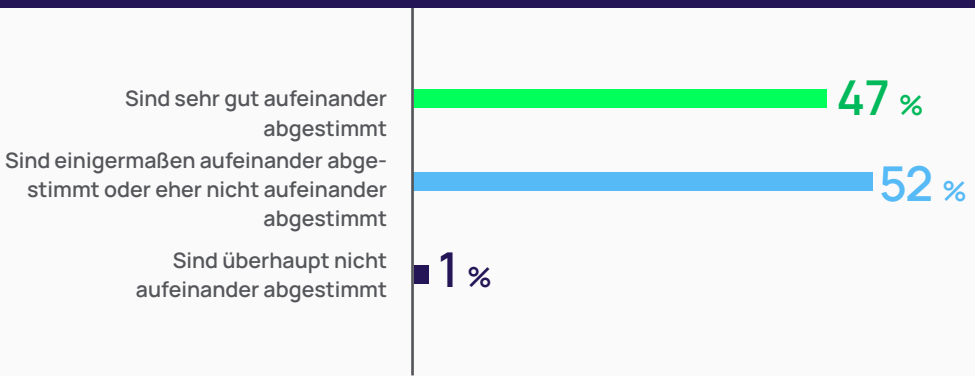
Wichtigste Erkenntnis 2

Entscheidungsträger im Bereich der Cybersicherheiten sagen, dass Geschäftsziele wichtig sind, geben aber zu, dass sie diese nicht erreichen

Führungskräfte im Bereich Cybersicherheit räumen ein, dass Sicherheit und Geschäftsziele nur unzureichend aufeinander abgestimmt sind

Insgesamt sind weniger als die Hälfte (47 %) der Entscheidungsträger der Meinung, dass ihre Cybersicherheitsziele in

Abbildung 3 | Wie gut sind Ihre Ziele im Bereich der Cybersicherheit auf die allgemeinen Geschäftsziele abgestimmt?



hohem Maße auf die Geschäftsziele abgestimmt sind.

Interessant ist, dass praktisch alle Unternehmen, die von ihrer Sicherheitslage überzeugt sind – also diejenigen, die sagen: „Wir schlagen zurück!" – ***auch*** sagen, dass sie entweder sehr oder zumindest einigermaßen auf die Geschäftsziele abgestimmt sind. Die Wahrscheinlichkeit, dass sie aufeinander abgestimmt sind, ist viel größer als bei ihren Kollegen, die nur auf der Stelle treten oder sich abmühen müssen, um mit dem Sicherheitsbedarf mithalten zu können.

Am anderen Ende des Spektrums glauben diejenigen, die am wenigsten Vertrauen in ihre Sicherheitslage haben, auch, dass sie auf die Geschäftsziele abgestimmt sind. Dies könnte darauf zurückzuführen sein, dass die Unternehmen ihre Abstimmung zwischen Sicherheit und Geschäftszielen überschätzen oder ihre Cybersicherheitslage unterschätzen.

Abbildung 4 | Wie gut sind Ihre Ziele im Bereich der Cybersicherheit auf die allgemeinen Geschäftsziele abgestimmt?

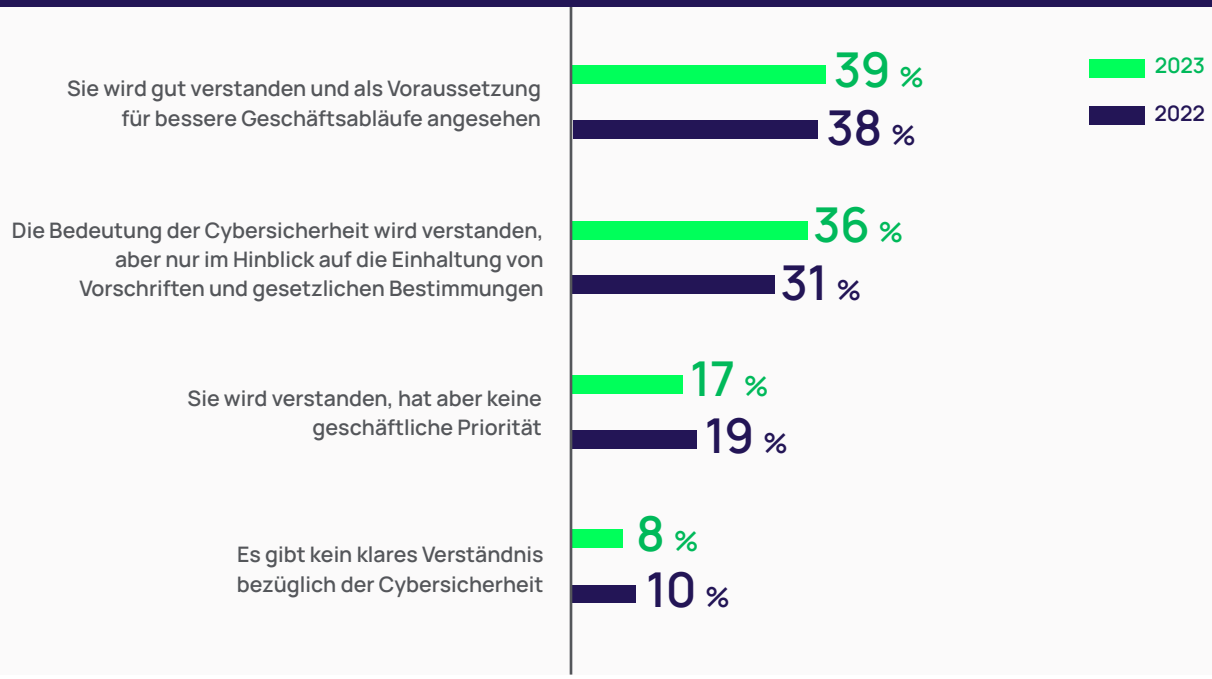
	Sind sehr gut aufeinander abgestimmt	Sie sind einigermaßen aufeinander abgestimmt	Sind eher nicht aufeinander abgestimmt	Sind überhaupt nicht aufeinander abgestimmt	Unsicher
Es ist viel zu tun – wir müssen die Wichtigkeit der Cybersicherheit in der gesamten Organisation neu definieren	59 %	36 %	4 %	1 %	1 %
Wir treten auf der Stelle – wir führen nichts Neues ein, sondern halten nur den Status Quo	29 %	56 %	13 %	2 %	0 %
Wir rennen, um mithalten zu können – wir haben einen guten Ansatz, aber es fehlen uns die Ressourcen / das Budget, um unsere Strategie vollständig umzusetzen	31 %	60 %	7 %	2 %	0 %
Wir schlagen zurück – wir passen uns an und entwickeln uns weiter, um mit der Bedrohungslage Schritt zu halten	56 %	43 %	1 %	0 %	0 %

Die höchsten Ebenen einer Organisation verstehen den Zusammenhang zwischen Unternehmen und Sicherheit nicht

Die Cybersicherheitsfunktion wird von den höchsten Ebenen des Unternehmens noch nicht als geschäftsfördernd anerkannt. Die Hälfte der Befragten (53 %) gibt zwar an, dass die Cybersicherheit im Vorstand und in der Geschäftsleitung verstanden wird, aber sie glauben, dass diese Führungskräfte die Sicherheitsfunktion nicht als geschäftsfördernd ansehen. Diese Zahl hat sich im vergangenen Jahr nicht wesentlich verändert.

Das ist eine schmerzhafte Erkenntnis, die jedoch zeigt, wie sehr Cybersicherheit und Geschäftsziele im Unternehmen auseinanderklaffen.

Abbildung 5 | Welche der folgenden Aussagen beschreibt am besten das Verständnis des Vorstands / der Geschäftsleitung für Cybersicherheit in Ihrem Unternehmen?

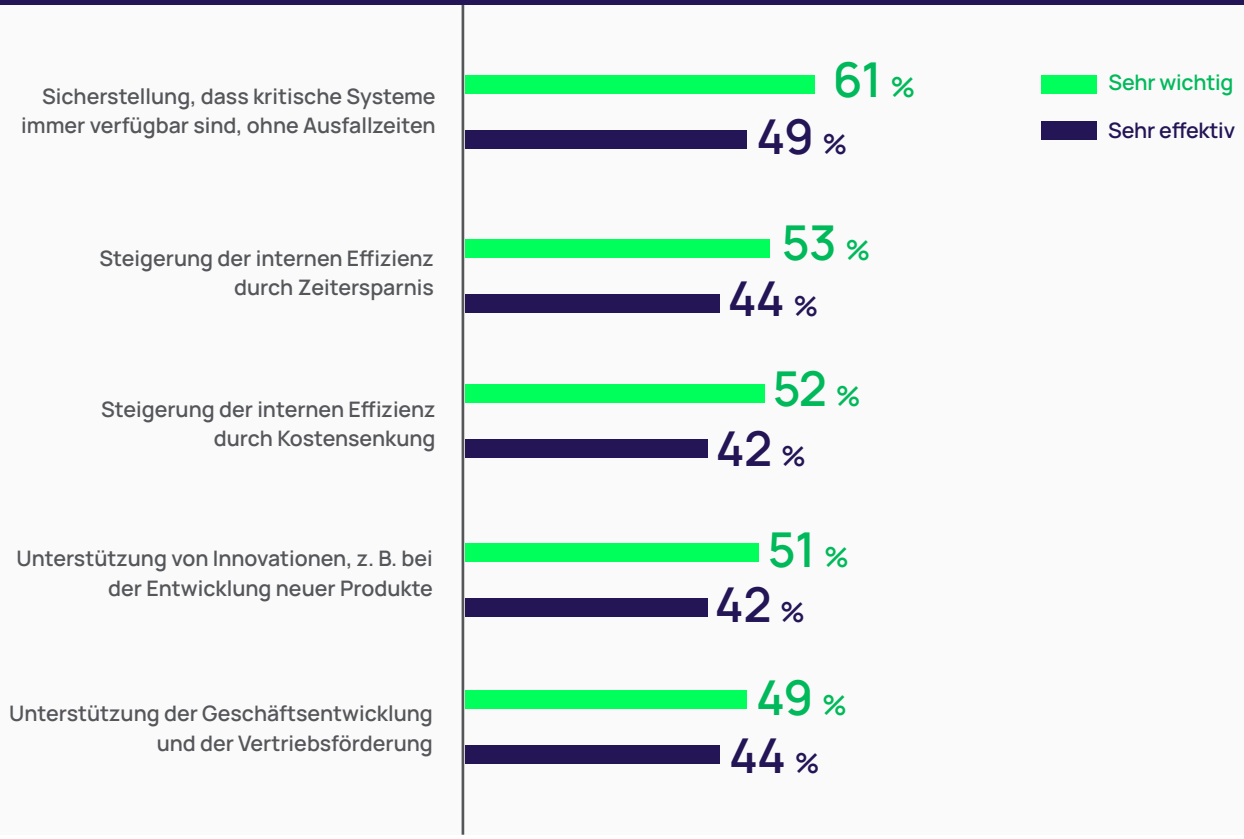


Führungskräfte im Bereich Cybersicherheit glauben nicht, dass sie ihre höchsten Prioritäten effektiv umsetzen können

Es zeigt sich, dass das primäre Ziel für die meisten Entscheider im Bereich Sicherheit zwar ein ***technisches*** ist – nämlich die Gewährleistung des Schutzes und der Verfügbarkeit kritischer Systeme –, dass aber etwa die Hälfte der Meinung ist, dass auch ***Geschäftsziele*** wie die Steigerung der Effizienz, die Senkung der Kosten, die Förderung von Innovationen und die Unterstützung des Vertriebs für ihre Teams wichtig sind.

Weniger als die Hälfte ist jedoch der Meinung, dass sie ihre vorrangigen Ziele – sowohl die technischen als auch die geschäftlichen – sehr gut erreichen.

Abbildung 6 | Wie wichtig sind die folgenden Ziele für Ihr Cybersicherheitsteam? Wie effektiv ist Ihr Cybersicherheitsteam Ihrer Meinung nach bei der Erreichung dieser Ziele?



Unternehmen, die in ihre Sicherheitslage am meisten Vertrauen haben, sind auch am ehesten in der Lage, sehr ***effektiv*** auf die Geschäftsziele einzugehen. Auch hier sind die Sicherheitsteams am wenigsten zuversichtlich hinsichtlich der Effektivität, wie die folgende Tabelle zeigt.

Abbildung 7 | Wie effektiv ist Ihr Cybersicherheitsteam Ihrer Meinung nach bei der Erreichung dieser Ziele?

	Sicherstellung, dass kritische Systeme immer verfügbar sind, ohne Ausfallzeiten	Unterstützung der Geschäfts-entwicklung und der Vertriebsför-derung	Steigerung der internen Effizienz durch Zeiter-sparnis	Unterstützung von Innovationen, z. B. bei der Entwicklung neuer Produkte	Steigerung der internen Effizienz durch Kostensenkung
Es ist viel zu tun – wir müssen die Wichtigkeit der Cybersicherheit in der gesamten Organisation neu definieren	62 %	60 %	65 %	58 %	61 %
Wir treten auf der Stelle – wir führen nichts Neues ein, sondern halten nur den Status Quo	51 %	49 %	44 %	40 %	43 %
Wir rennen, um mithalten zu können – wir haben einen guten Ansatz, aber es fehlen uns die Ressourcen / das Budget, um unsere Strategie vollständig umzusetzen	53 %	48 %	42 %	40 %	48 %
Wir schlagen zurück – wir passen uns an und entwickeln uns weiter, um mit der Bedrohungslage Schritt zu halten	62 %	53 %	55 %	55 %	48 %

Ändern der Denkweise

Für diese mangelnde Abstimmung kann es mehrere Gründe geben. Einige der möglichen Gründe sind:

1. **Fehlende Abstimmung der Sicherheitsziele auf die Geschäftsziele:** Sicherheitsverantwortliche konzentrieren sich möglicherweise zu sehr auf die Risikominderung und den Schutz von Assets, ohne die umfassenderen Unternehmensziele zu verstehen.

2. **Mangel an Kommunikation und Zusammenarbeit:** Es kann vorkommen, dass Sicherheitsverantwortliche ihre Ziele nicht effektiv an andere Geschäftsabteilungen oder Stakeholder weitergeben oder nicht mit ihnen zusammenarbeiten, um Sicherheitsstrategien zu entwickeln, die die Geschäftsziele unterstützen. Dies kann dazu führen, dass Sicherheitsmaßnahmen als Hindernis für die Erreichung von Geschäftszielen angesehen werden, anstatt sie zu fördern.

3. **Unzureichende Ressourcen:** Sicherheitsverantwortliche verfügen möglicherweise nicht über ausreichende Ressourcen, wie z. B. Budget, Personal oder Technologie, um Sicherheitsmaßnahmen zu implementieren, die den Geschäftszielen entsprechen. Dies kann zu Sicherheitsmaßnahmen führen, die unzureichend oder unwirksam sind oder andere Geschäftsbereiche unangemessen belasten.

4. **Unzureichende Metriken:** Sicherheitsverantwortliche verfügen möglicherweise nicht über die geeigneten Metriken, um die Wirksamkeit ihrer Sicherheitsmaßnahmen im Hinblick auf die Erreichung der Geschäftsziele zu messen. Dies kann dazu führen, dass der Eindruck entsteht, die Sicherheitsmaßnahmen seien nicht wirksam, obwohl sie es in Wirklichkeit sind.

5. **Mangelndes Verständnis der Geschäftsziele:** Sicherheitsverantwortliche haben möglicherweise kein klares Verständnis für die Geschäftsziele, Prioritäten und Herausforderungen des Unternehmens. Dies kann zu Sicherheitsmaßnahmen führen, die den spezifischen Anforderungen des Unternehmens nicht gerecht werden.

Wir werden im weiteren Verlauf des Berichts auf jeden dieser möglichen Gründe eingehen.

Wichtigste Erkenntnis 3

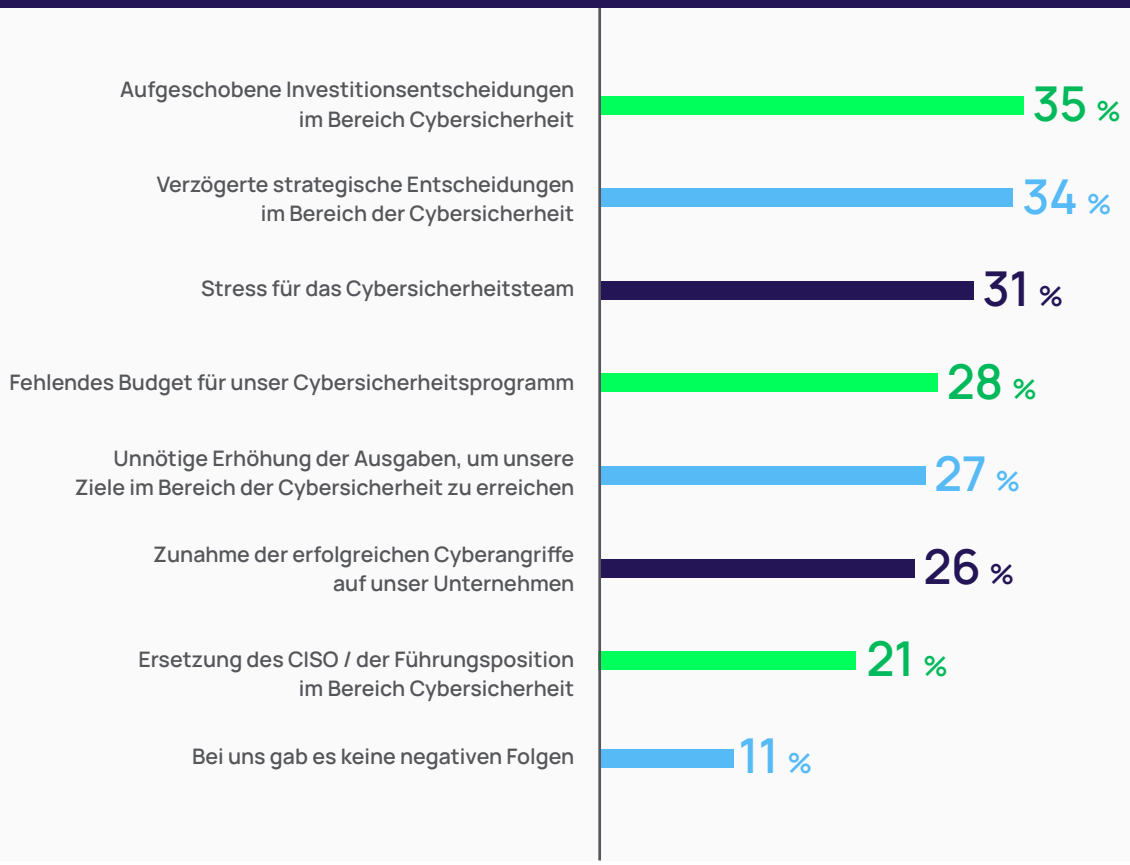
Mangelnde Abstimmung hat **sowohl** negative Auswirkungen auf Geschäfts- **als auch** Sicherheitsziele

Ein erfolgreicher Cyberangriff kann zu Datenschutzverletzungen, Systemausfällen, finanziellen Verlusten und einer Schädigung des Rufs eines Unternehmens führen, die alle die Geschäftsziele eines Unternehmens untergraben können. Die Forschungsergebnisse stützen diese Behauptung.

Die negativen Auswirkungen sind vielfältig

Tatsächlich geben 10 % der Befragten an, dass ihr Unternehmen im vergangenen Jahr mindestens eine negative Auswirkung aufgrund mangelnder Abstimmung von Cybersicherheit und Business erlitten hat.

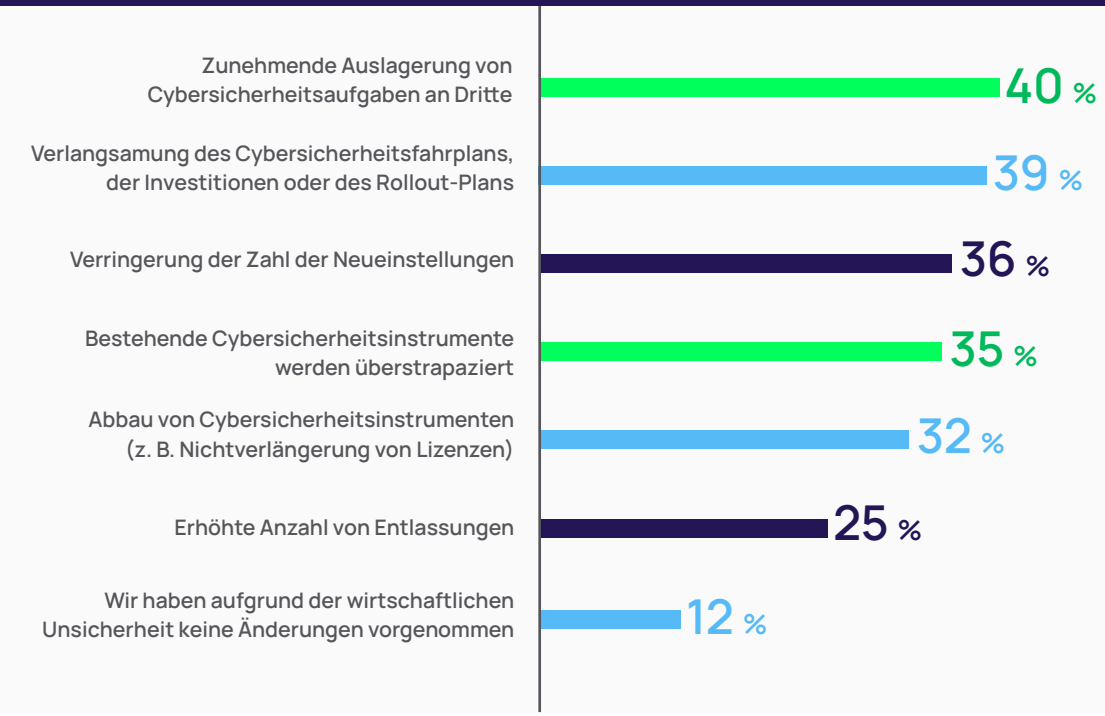
Abbildung 8 | Welche negativen Folgen, sofern vorhanden, haben Sie aufgrund einer mangelnden Abstimmung von Cybersicherheit und Geschäftszielen erlebt? (Bitte bis zu drei auswählen.)



Warum gerade jetzt? Das derzeitige Wirtschaftsklima ist dafür mitverantwortlich

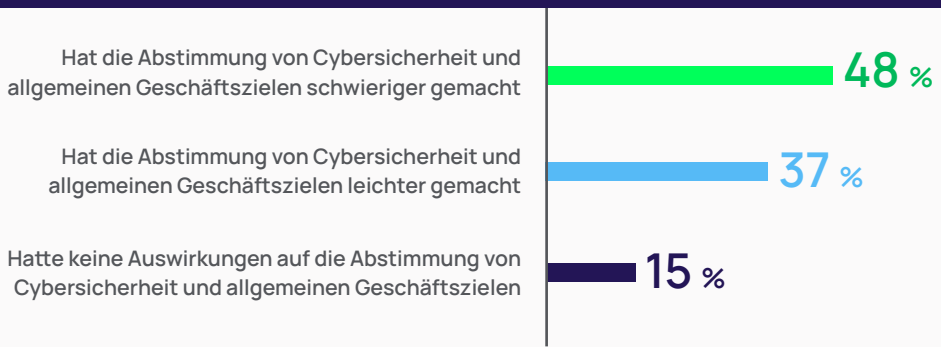
Achtundachtzig Prozent haben Veränderungen aufgrund wirtschaftlicher Unsicherheit erlebt. Viele dieser Änderungen haben negative Auswirkungen auf die Sicherheit, wie z. B. eine Verlangsamung des Fahrplans und der Investitionen in Technologie sowie fehlende Ressourcen, wie die nachstehende Grafik zeigt.

Abbildung 9 | Wie hat sich die jüngste wirtschaftliche Unsicherheit in den letzten 6 Monaten auf Ihr Cybersicherheitsteam ausgewirkt?



In einem Umfeld des Wandels kann die Anpassung eine Herausforderung sein. Etwa die Hälfte der Befragten ist der Meinung, dass die wirtschaftliche Unsicherheit die Abstimmung von Cybersicherheit und Business erschwert hat.

Abbildung 10 | Wie hat sich die jüngste wirtschaftliche Unsicherheit auf die Abstimmung von Cybersicherheitszielen und allgemeineren Geschäftszielen ausgewirkt?



Ändern der Denkweise

Bei solch hohen Einsätzen lautet die eigentliche Frage nach der Ausrichtung von Sicherheit und Business nicht „Wie können wir uns das leisten?“, sondern „Wie können wir es uns leisten, das nicht zu tun?“

Durch die Einbeziehung der Cybersicherheit in die allgemeine Geschäftsstrategie eines Unternehmens können Sie einen proaktiven Sicherheitsansatz entwickeln, der das Risiko von Cyberangriffen verringert und zum Schutz kritischer Geschäftsabläufe beiträgt.

Wichtigste Ressource:

Lesen Sie die Globale Umfrage unter IT-Sicherheitsverantwortlichen Benchmarking von Sicherheitslücken und privilegiertem Zugriff

Wichtigste Erkenntnis 4

Nicht aufeinander abgestimmte Metriken spiegeln die mangelnde Abstimmung von Cybersicherheit und Business wider

Wie man so schön sagt: Wenn man etwas verwalten will, muss man es messen. Um die Ziele des Business Enablement zu erreichen, müssen Teamziele und individuelle MBOs (Management by Objectives) oder OKRs (Objective and Key Results) miteinander verknüpft und kontinuierlich verfolgt werden.

Leider scheint das, von einigen Ausnahmen abgesehen, nicht der Fall zu sein. Was Führungskräfte gerne tun würden und was sie tatsächlich messen und melden, ist nicht dasselbe.

Der Unterschied zwischen technischen und geschäftlichen Metriken

Die Daten zeigen, dass die Leistung von Cybersicherheitsprogrammen immer noch in erster Linie anhand von technischen oder tätigkeitsbasierten Metriken, wie der Anzahl der verhinderten oder abgewehrten Angriffe beurteilt wird und nicht anhand von geschäftsorientierten Metriken wie dem wirtschaftlichen Wert, der Benutzererfahrung, den Versicherungskosten oder den Auswirkungen auf andere Teams.

Abbildung 11 | Welche der folgenden Punkte sind für die Messung des Erfolgs Ihrer Cybersicherheitsprogramme am wichtigsten? (Bitte bis zu drei auswählen.)

Allerdings ist der Gesamt-ROI / der wirtschaftliche Wert für kleinere Unternehmen mit weniger Mitarbeitern wichtiger.

Abbildung 12 | Welche der folgenden Punkte sind für die Messung des Erfolgs Ihrer Cybersicherheitsprogramme am wichtigsten? (Bitte bis zu drei auswählen.)

	1.	2.	3.
500–999 Mitarbeiter	Der wirtschaftliche Wert (Gesamt-ROI, **29 %**)	Anzahl der verhinderten Angriffe / Geringere Kosten / Zeitersparnis (jeweils **28 %**)	
1.000–4.999 Mitarbeiter	Anzahl der verhinderten oder eingedämmten Angriffe (**32 %**)	Erfolgreiche Implementierung / Zeitersparnis für das IT-Team (jeweils **31 %**)	
Mehr als 5.000 Mitarbeiter	Anzahl der verhinderten, eingedämmten Angriffe / Erfüllung der Compliance- und Audit-Ziele (jeweils **31 %**)		Geringere Kosten für einen erfolgreichen Cyberangriff (**30 %**)

Es überrascht nicht, dass Führungskräfte mit umfassender organisatorischer Verantwortung, wie z. B. CEOs/Eigentümer, mehr Wert auf die Messung der Benutzerfreundlichkeit und die Reduzierung von Problemen legen, als CISOs. Interessant ist jedoch, dass die Direktorenebene/Abteilungsleiter auch auf Geschäftskennzahlen, wie den wirtschaftlichen Wert/ROI Wert legen.

Abbildung 13 | Welche der folgenden Punkte sind für die Messung des Erfolgs Ihrer Cybersicherheitsprogramme am wichtigsten? (Bitte bis zu drei auswählen.)

	1.	2.	3.
CEO/ Eigentümer	Verbesserte Erfahrung für Geschäftsanwender (**31 %**)	Erfolgreiche Implementierung (pünktlich, budgetgerecht **30 %**)	Erfüllung von Compliance- und Auditzielen (**29 %**)
CIO/CSO /CISO	Anzahl der verhinderten oder eingedämmten Angriffe (**32 %**)	Erfolgreiche Implementierung (pünktlich, budgetgerecht **31 %**)	Der wirtschaftliche Wert / geringere Kosten / Einhaltung der Ziele (jeweils **28 %**)
Leiter der IT-Abteilung	Der wirtschaftliche Wert (Gesamt-ROI, **34 %**)	Anzahl der verhinderten oder eingedämmten Angriffe (**32 %**)	Geringere Kosten / Erfüllung der Compliance-Ziele (jeweils **30 %**)
IT-Direktor	Der wirtschaftliche Wert (Gesamt-ROI, **32 %**)	Anzahl der verhinderten / abgewehrten Angriffe / Zeitersparnis für IT-Teams (jeweils **30 %**)	
IT-Manager	Anzahl der verhinderten oder eingedämmten Angriffe (**33 %**)	Geringere Kosten / Erfüllung der Compliance-Ziele / Erfolgreiche Implementierung (jeweils **30 %**)	
Sicherheits-manager	Geringere Kosten für einen erfolgreichen Cyberangriff (**36 %**)	Erfolgreiche Implementierung (pünktlich, budgetgerecht **29 %**)	Erfüllung von Compliance- und Auditzielen (**27 %**)

Ändern der Denkweise

Cybersicherheitsteams konzentrieren sich häufig auf technische Metriken, da sie Daten liefern, die zur Bewertung der Sicherheitslage eines Unternehmens verwendet werden können. Technische Metriken wie die Anzahl der entdeckten und behobenen Schwachstellen, die Zeit, die für die Entdeckung von und die Reaktion auf Sicherheitsvorfälle benötigt wird und der Prozentsatz der Systeme mit aktualisierter Sicherheitssoftware geben Aufschluss über die Wirksamkeit der Sicherheitskontrollen und ermöglichen es den Teams, Bereiche mit Verbesserungsbedarf zu ermitteln.

Technische Metriken sind zwar wichtig, aber sie sind nicht die einzigen Faktoren, die den Erfolg eines Cybersicherheitsprogramms bestimmen. Bei der Cybersicherheit geht es letztlich um die Erreichung von Geschäftszielen – strategische Ergebnisse, die durch effektive Sicherheit ermöglicht werden.

Führungskräfte im Bereich Cybersicherheit können die Abstimmung verbessern, indem sie klare und messbare Geschäftsziele festlegen, die mit den strategischen Zielen ihres Unternehmens verbunden sind. Dies könnte die Identifizierung der kritischsten Assets für das Unternehmen, die potenziellen Auswirkungen eines Angriffs auf das Unternehmen und die Frage beinhalten, wie wirksame Sicherheitskontrollen die Verfügbarkeit, Vertraulichkeit und Integrität dieser Assets verbessern. Wenn zum Beispiel ein Dienst ausfällt, sind die finanziellen und betrieblichen Kosten klar. Die Ergebnisse der Cybersicherheit lassen sich an den Kosten des Nichtstuns im Vergleich zu den Kosten des Handelns messen.

Cybersicherheitsteams könnten auch daran arbeiten, ihre Kommunikation und Zusammenarbeit mit anderen Teilen des Unternehmens zu verbessern, z. B. mit dem Risikomanagement, der Compliance und dem Geschäftsbetrieb. Durch die enge Zusammenarbeit mit diesen Stakeholdern können Cybersicherheitsteams ein besseres Verständnis für den geschäftlichen Kontext und die Prioritäten gewinnen und ihre Aktivitäten entsprechend ausrichten.

Schließlich könnten Cybersicherheitsteams einen stärker risikobasierten Ansatz für die Sicherheit in Erwägung ziehen, bei dem technische Metriken in Verbindung mit den Geschäftsergebnissen zur Entscheidungsfindung herangezogen werden. Dies würde bedeuten, die größten Risiken für das Unternehmen zu ermitteln und die Ressourcen auf die Verringerung dieser Risiken zu konzentrieren, anstatt nur technische Metriken um ihrer selbst willen zu verfolgen.

Um die Cybersicherheit an den Unternehmenszielen zu messen, sollten Sie Folgendes beachten:

1. **Metriken zum Risikomanagement:** Messung der Effektivität eines Unternehmens bei der Erkennung und Eindämmung von Cybersicherheitsrisiken, einschließlich der Häufigkeit von Vorfällen sowie Reaktionszeiten.

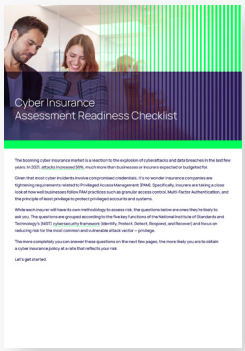
2. **Compliance-Metriken:**Zur Überprüfung, wie gut ein Unternehmen die behördlichen und branchenüblichen Standards für Cybersicherheit einhält.

3. **Metriken zur Geschäftskontinuität:** Messung der Fähigkeit eines Unternehmens, den Geschäftsbetrieb während eines Cybersicherheitsvorfalls aufrechtzuerhalten, einschließlich der Dauer der Ausfallzeit und der Wiederherstellungszeit.

4. **Kostenmetriken:** Verfolgung der Kosten für die Umsetzung und Aufrechterhaltung von Cybersicherheitsmaßnahmen im Verhältnis zum Gesamtbudget.

5. **Produktivitätsmetriken:** Messung der Geschwindigkeit, mit der ein neuer Mitarbeiter oder Lieferant eingearbeitet werden kann und die notwendigen Ressourcen und den Zugang zur Erledigung seiner Aufgaben erhält.

Mithilfe dieser Art von Metriken können Sie die Effektivität Ihrer Cybersicherheitsstrategie im Hinblick auf das Erreichen der Geschäftsziele des Unternehmens bewerten und fundierte Entscheidungen über Investitionen in Cybersicherheitsressourcen treffen.



Wichtigste Ressourcen:

- Checkliste für Cyberversicherungen: Beantworten Sie die Fragen, die Anbieter von Cyberversicherungen mit Sicherheit stellen werden
- Anpassung an rechtliche Rahmenbedingungen und Compliance-Anforderungen

Wichtigste Erkenntnis 5

Ohne strukturelle Veränderungen stehen die Zeichen für die Abstimmung von Cybersicherheit und Business schlecht

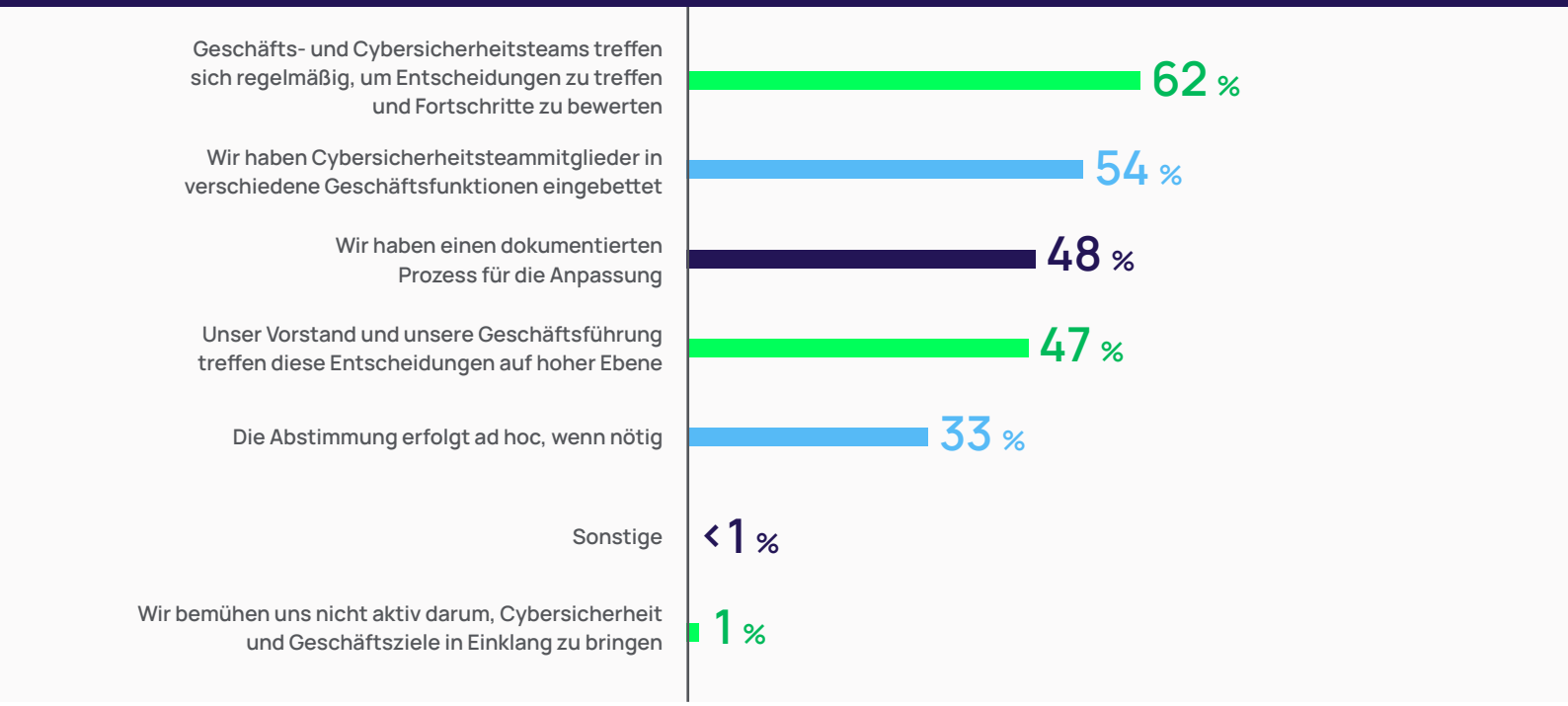
Damit Business und Cybersicherheit aufeinander abgestimmt werden können, ist es wichtig, die Organisationsstruktur zu berücksichtigen. Damit befassen wir uns also als nächstes.

Reden und seinen Worten Taten folgen lassen

Die gute Nachricht ist, dass funktionsübergreifende Gespräche in Unternehmen stattfinden. Die meisten Cybersicherheitsteams treffen sich regelmäßig mit ihren Kollegen auf hoher Ebene oder haben sogar Sicherheitsteammitglieder in die Geschäftsfunktionen integriert.

Allerdings dokumentiert weniger als die Hälfte der Unternehmen ihre Richtlinien und Verfahren, um die Abstimmung zu erleichtern.

Abbildung 14 | Wie stellt Ihr Unternehmen sicher, dass die Ziele der Cybersicherheit auf die allgemeinen Unternehmensziele abgestimmt werden? (Alle zutreffenden Antworten auswählen.)



Befragte, die von einer **„hohen Abstimmung“** sprechen, sagen Folgendes am ehesten:

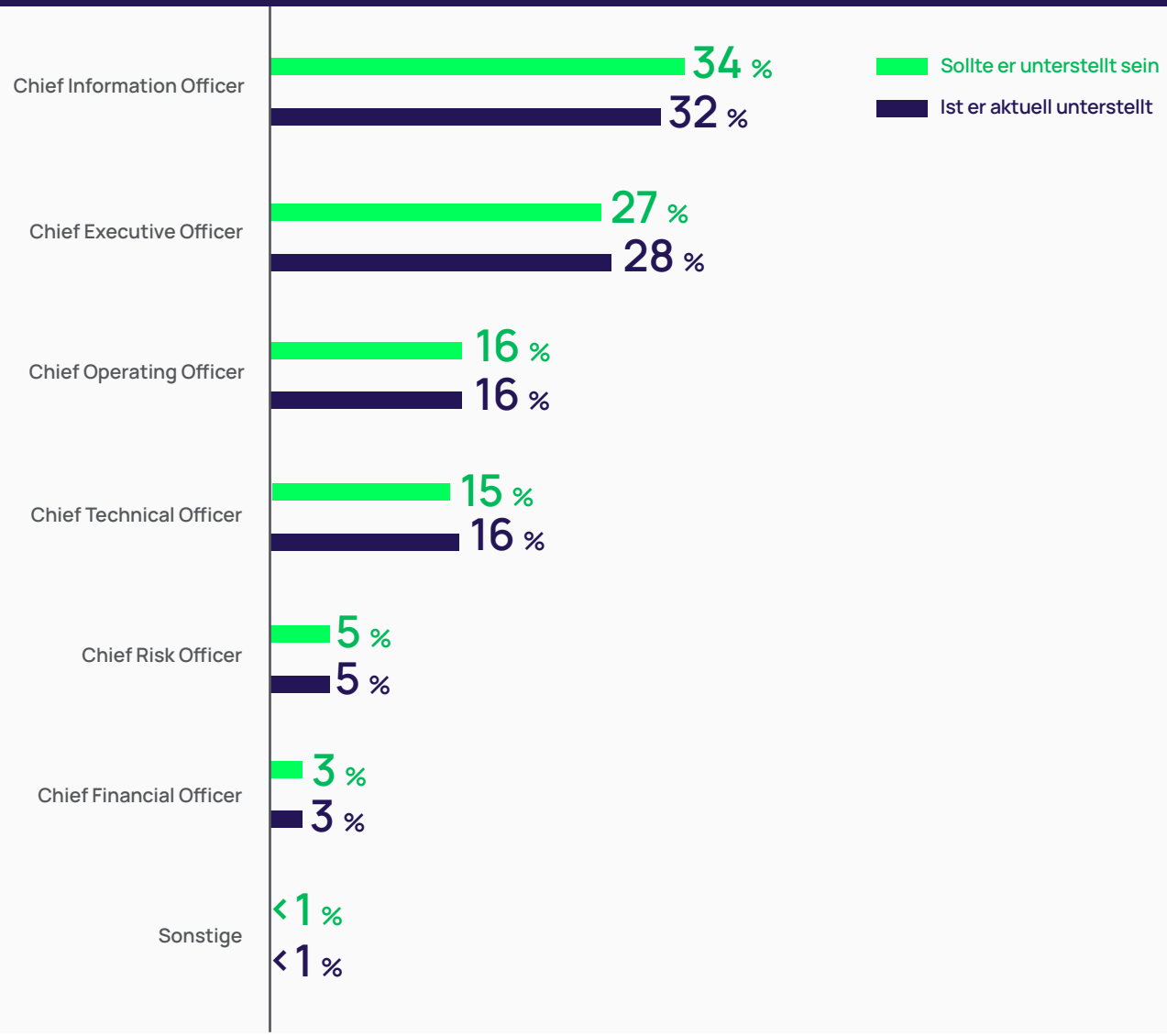
- Geschäfts- und Cybersicherheitsteams treffen sich regelmäßig, um Entscheidungen zu treffen und Fortschritte zu bewerten (68 %)
- Wir haben Cybersicherheitsteammitglieder in verschiedene Geschäftsfunktionen eingebettet (61 %)
- Unser Vorstand und unsere Geschäftsführung treffen diese Entscheidungen auf hoher Ebene (56 %)

Die Berichtsstruktur kann dem Business Enablement eher schaden als nützen

Mehr als ein Drittel (34 %) der Befragten ist der Meinung, dass die Person, der ein CISO unterstellt sein sollte, der CIO ist. Und in den meisten Unternehmen ist dies auch der Fall.

Es ist interessant zu beobachten, dass die Präferenzen hinsichtlich der Frage, wer wem unterstellt ist, je nach Berufsbezeichnung variieren. So bevorzugen CEOs eher, dass CISOs ihnen unterstellt sind, während IT-Direktoren eher der Meinung sind, dass CISOs ihrem direkten Vorgesetzten – dem CIO – unterstellt sein sollten.

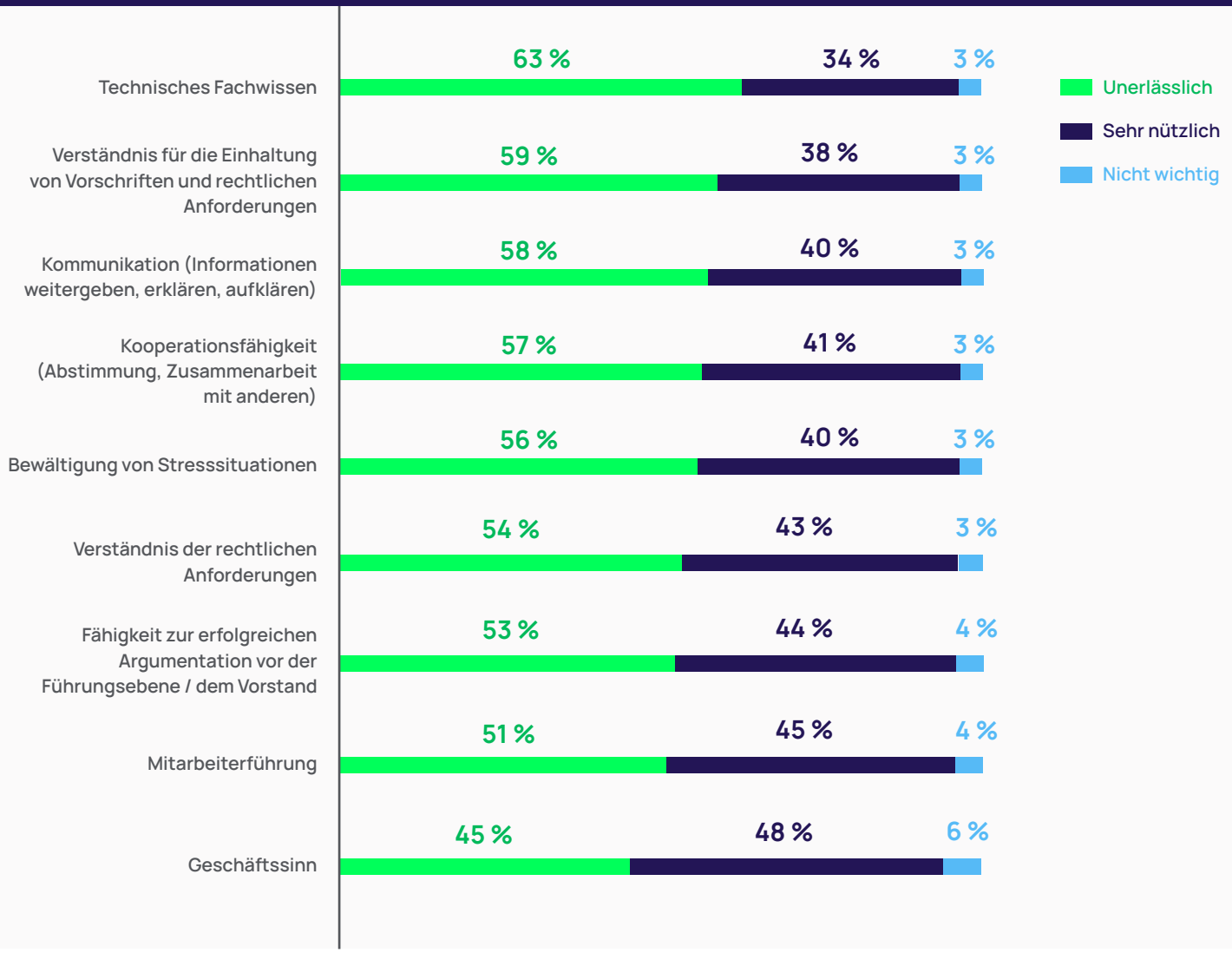
Abbildung 15 | Wem sollte Ihrer Meinung nach der CISO oder die ranghöchste Führungskraft im Bereich der Cybersicherheit unterstellt sein, um die Cybersicherheit am besten auf die Gesamtziele des Unternehmens abzustimmen? Wem untersteht derzeit der CISO oder die ranghöchste Führungskraft im Bereich Cybersicherheit in Ihrem Unternehmen?



Die aktuellen Qualifikationen spiegeln den Bedarf an einer stärkeren Fokussierung auf das Business unter den Führungskräften im Bereich Cybersicherheit wider

Insgesamt sind die Befragten der Meinung, dass technisches Fachwissen die wichtigste Fähigkeit für eine Führungskraft im Bereich der Cybersicherheit wie einem CISO ist. Sie stufen diese Fähigkeit viel höher ein, als geschäftsbezogene Fähigkeiten wie Kommunikation, Zusammenarbeit, Argumentation und Geschäftssinn.

Abbildung 16 | Wie wichtig sind diese Fähigkeiten für einen CISO / eine Führungskraft im Bereich Cybersicherheit? Pro Zeile eine Antwort wählen



Wie aus dem nachstehenden Diagramm hervorgeht, glauben die Befragten, dass es ihnen am meisten an der Fähigkeit mangelt, Stresssituationen zu bewältigen oder zu deeskalieren, gefolgt von Argumentations- und Kommunikationsfähigkeiten. Ohne diese Fähigkeiten werden es Führungskräfte im Bereich der Cybersicherheit sehr schwer haben, sich mit ihren Kollegen im Unternehmen abzustimmen.

Abbildung 17 | Wo liegen Ihrer Meinung nach Ihre eigenen Fähigkeitslücken? Alle zutreffenden Antworten auswählen

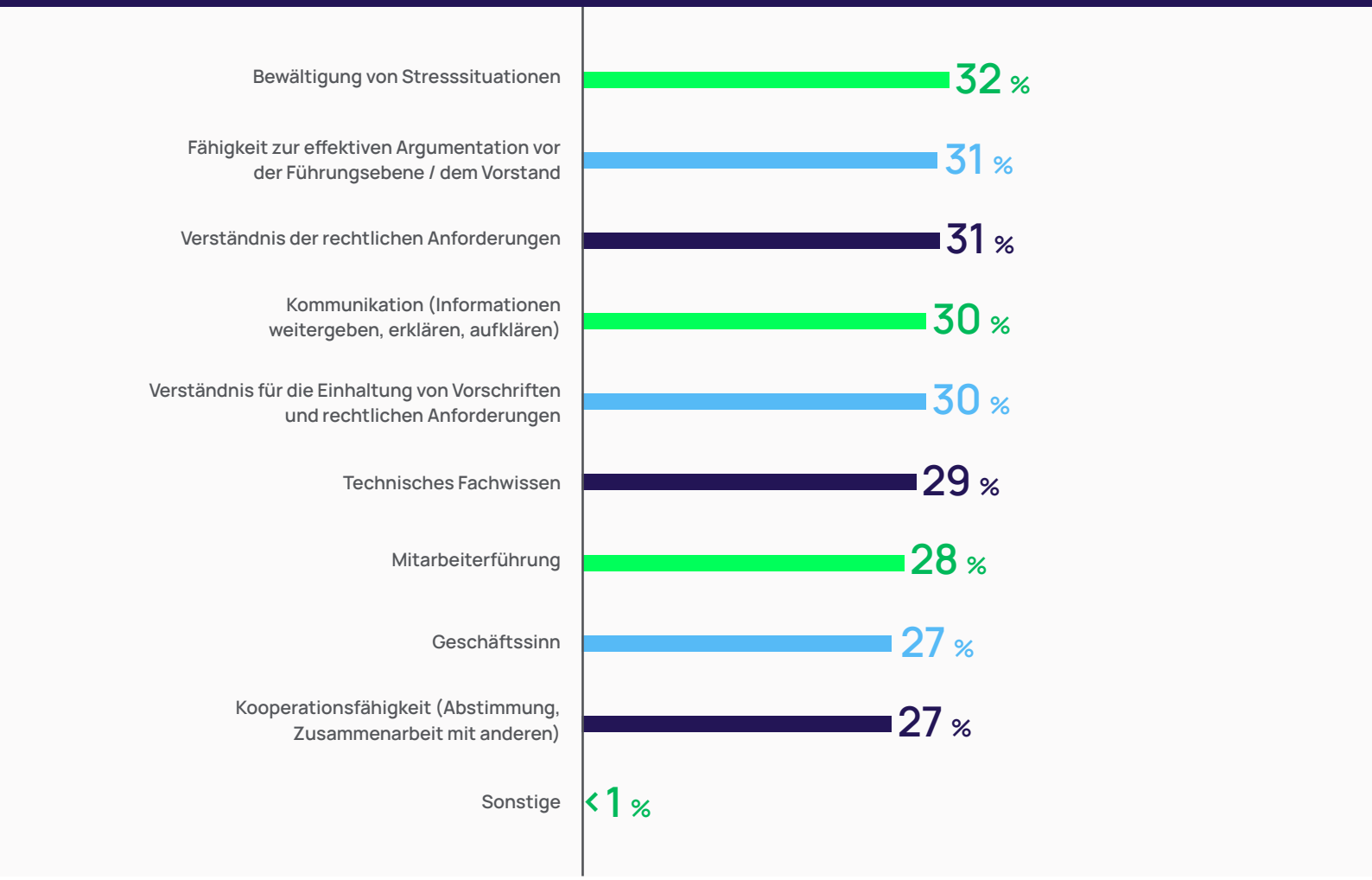


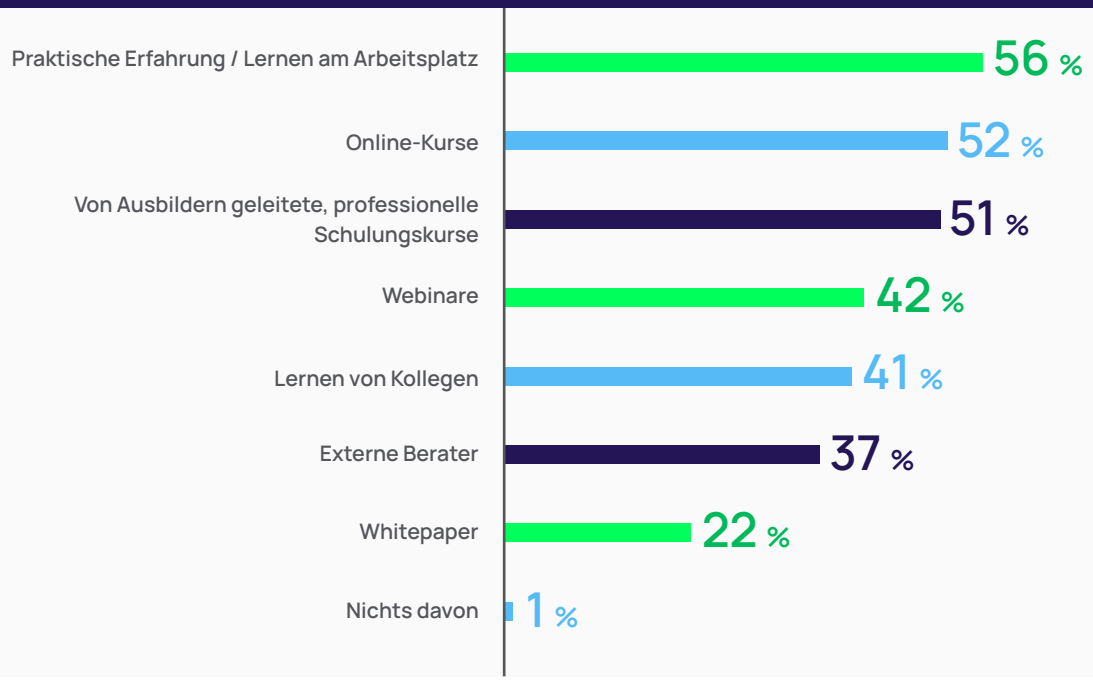
Abbildung 18 | Wo liegen Ihrer Meinung nach Ihre eigenen Fähigkeitslücken?

	1.	2.	3.
CEO/ Eigentümer	Bewältigung von Stresssituationen / Kommunikation (Informationen weitergeben, erklären, aufklären **38 %**)		Fähigkeit zur effektiven Argumentation vor der Führungsebene / dem Vorstand (**36 %**)
CIO/CSO/CISO	Verständnis der rechtlichen Anforderungen (**32 %**)	Bewältigung von Stresssituationen / Fähigkeit zur effektiven Argumentation vor der Führungsebene / dem Vorstand / Kommunikation / Verständnis für die Einhaltung von Vorschriften und rechtlichen Anforderungen (jeweils **31 %**)	
Leiter der IT-Abteilung	Bewältigung von Stresssituationen (**31 %**)	Verständnis der rechtlichen Anforderungen / Kommunikation / Mitarbeiterführung (jeweils **29 %**)	
IT-Direktor	Bewältigung von Stresssituationen (**32 %**)	Verständnis der rechtlichen Anforderungen (**31 %**)	Verständnis für die Einhaltung von Vorschriften und rechtlichen Anforderungen (**30 %**)
IT-Manager	Fähigkeit zur effektiven Argumentation vor der Führungsebene / dem Vorstand (**34 %**)	Geringere Kosten / Erfüllung der Compliance-Ziele / Erfolgreiche Implementierung (jeweils **30 %**)	
Sicherheits-manager	Mitarbeiterführung (**37 %**)	Geschäftssinn (**29 %**)	Fähigkeit zur erfolgreichen Argumentation vor der Führungsebene / dem Vorstand (jeweils **28 %**)

Reaktive Schulungen schließen die Qualifikationslücke nicht

Praktische Erfahrungen und Lernen am Arbeitsplatz sind die beliebtesten Methoden, mit denen die Befragten ihre Fähigkeiten verbessern. Es hat den Anschein, als würden die Mitarbeiter sagen: „Wir werden uns erst mit diesem Problem befassen, wenn wir es wirklich müssen“. Das verheißt nichts Gutes für den Aufbau von Fähigkeiten, die für ein proaktives, gezieltes Business Enablement erforderlich sind.

Abbildung 19 | Wie können Sie Ihre eigenen Fähigkeiten verbessern und sich weiterbilden, um sich an die Geschäftsziele anzupassen und die Gesamtleistung des Unternehmens zu verbessern?



Wie inzwischen klar geworden sein sollte, ist Business Enablement jedoch nicht nur eine Herausforderung bezüglich der Fähigkeiten. Auch hier kann es eine Herausforderung hinsichtlich des Willens geben.

Ändern der Denkweise

Um das Ziel des „Business Enablement“ besser zu erreichen, sollten Führungskräfte im Bereich der Cybersicherheit Folgendes berücksichtigen:

Durchführung von effektiven Sitzungen

Man könnte natürlich denken, dass der beste Weg die Abstimmung voranzutreiben, darin besteht, alle zusammenzubringen. Aber ein Treffen ist oft keine Garantie für eine erfolgreiche Abstimmung. In der Tat ist diese Art des Treffens vielleicht gar nicht erforderlich. Bei der Abstimmung geht es darum, Teams dazu zu bringen, auf ganz bestimmte Weise miteinander zu interagieren, unabhängig davon, ob sie sich tatsächlich treffen.

Letztendlich kann die Abstimmung synchron oder asynchron erfolgen. An einem oder an unterschiedlichen Standorten. Persönlich oder über ein Zoom-Meeting. Solange es den Teams hilft, sich gegenseitig zu verstehen, gemeinsame Ziele zu verfolgen und den Erfolg gemeinsam zu messen.

Entwicklung von Fähigkeiten

Es besteht eine hohe Wahrscheinlichkeit, dass Unternehmen nicht die perfekte Mischung aus Sicherheits- und Geschäftsfähigkeiten in einer Person finden werden. Um die richtige Mischung zu finden, müssen Führungskräfte im Bereich der Cybersicherheit nicht nur auf technische Experten zurückgreifen, sondern auch Personen mit nicht-traditionellem Hintergrund für die Arbeit in ihren Teams gewinnen.

Überdenken der Unterstellungsstruktur

Die Tatsache, dass der CISO dem CIO unterstellt ist, kann zwar Vorteile haben, birgt aber auch potenzielle Risiken.

Sollte der CISO dem CIO unterstellt sein?

POSITIV

- **Abstimmung mit der IT-Strategie:** Der CISO und der CIO arbeiten eng zusammen, um die IT-Sicherheitsstrategie des Unternehmens auf die allgemeine Geschäftsstrategie abzustimmen. Dieser Ansatz gewährleistet, dass die Sicherheit in alle Aspekte der IT integriert wird, einschließlich der Entwicklung und Implementierung neuer Technologien, Anwendungen und Infrastrukturen.
- **Klare Verantwortlichkeit:** Da der CISO dem CIO unterstellt ist, hat er die klare Verantwortung für die Sicherheit der IT-Systeme des Unternehmens. Diese Verantwortung trägt dazu bei, dass Sicherheitsrisiken erkannt, bewertet und umgehend und wirksam behandelt werden.
- **Ressourcenzuteilung:** Der CIO ist für die Zuteilung von Ressourcen für IT-Projekte verantwortlich. Da der CISO dem CIO unterstellt ist, wird sichergestellt, dass die Sicherheit bei der Zuteilung von Ressourcen berücksichtigt wird. Der CISO kann dem CIO dabei helfen, Bereiche zu identifizieren, in denen zusätzliche Ressourcen benötigt werden, um die Sicherheitslage des Unternehmens zu verbessern.
- **Bessere Kommunikation:** Der CISO und der CIO haben ein besseres Verständnis für die gegenseitigen Herausforderungen und können diese gemeinsam bewältigen. Da der CISO dem CIO unterstellt ist, hat er besseren Zugang zu den IT-Entscheidungsträgern und kann effektiver mit ihnen kommunizieren.

NEGATIV

- **Interessenkonflikt:** Der CIO ist dafür verantwortlich, dass IT-Dienste und -Projekte pünktlich und innerhalb des Budgets implementiert werden. Diese Konzentration auf die Implementierung kann manchmal mit der Verantwortung des CISO für die Gewährleistung der Sicherheit der IT-Systeme in Konflikt geraten. Dieser Konflikt kann dazu führen, dass der CISO unter Druck gesetzt wird, der Implementierung von IT-Diensten Vorrang vor der Sicherheit einzuräumen.
- **Mangel an Autonomie:** Kann die Autonomie des CISO und seine Fähigkeit, unabhängig zu arbeiten, einschränken. Wenn der CIO die Sicherheitsfunktion nicht unterstützt oder nicht ausreichend Ressourcen zur Verfügung stellt, kann der CISO Schwierigkeiten haben, die Sicherheitskontrollen wirksam umzusetzen.
- **Kommunikationsbarrieren:** Können die Fähigkeit einschränken, mit dem CEO und dem Vorstand zu kommunizieren, um die Sicherheitslage des Unternehmens zu verstehen.
- **Beschränkte Konzentration auf die Sicherheit:** Kann den Eindruck verstärken, dass die Sicherheit ein zweitrangiges Anliegen ist und nicht die Aufmerksamkeit und die Ressourcen erhält, die sie verdient.
- **Compliance vs. Risikomanagement:** Die Konzentration des CIO auf die Implementierung von IT-Diensten kann manchmal zu einem auf die Einhaltung von Vorschriften ausgerichteten Sicherheitsansatz führen, bei dem der Schwerpunkt eher auf der Erfüllung gesetzlicher Anforderungen als auf dem Management von Sicherheitsrisiken liegt.

Insgesamt kann es zwar vorteilhaft sein, wenn der CISO dem CIO unterstellt ist, doch ist es wichtig, diese potenziellen Probleme anzugehen, um sicherzustellen, dass der Sicherheit die gebührende Aufmerksamkeit geschenkt wird und dass der CISO unabhängig arbeiten und eine objektive Bewertung der Sicherheitslage des Unternehmens abgeben kann.

So sehen die nächsten Schritte aus

Es ist von entscheidender Bedeutung, dass die Cybersicherheit auf die Geschäftsziele abgestimmt wird, da sich Risiken direkt auf die Fähigkeit eines Unternehmens auswirken können, seine strategischen Ziele zu erreichen. Je besser die Cybersicherheit auf das Unternehmen abgestimmt ist, desto widerstandsfähiger wird das Unternehmen UND desto mehr kann es florieren.

Der Wechsel vom „Ich“ zum „Wir“

Der Aufbau einer effektiven Abstimmung von Sicherheit und Business erfordert eine Mischung von Fähigkeiten. Zudem sind gemeinsame Metriken erforderlich. Vor allem aber bedarf es einer breiten und konsequenten Umsetzung im gesamten Unternehmen. Führungskräfte im Bereich Cybersicherheit müssen eng mit anderen Funktionen zusammenarbeiten, um angemessene Ressourcen zuteilen und Entscheidungen treffen zu können.

Darüber hinaus müssen Unternehmen, die die Herausforderung vom „Ich“ zum „Wir“ meistern wollen, ganz anders über den Zweck der Cybersicherheit nachdenken. Anstatt die Verantwortung des Cybersicherheitsteams ausschließlich im Hinblick auf den Schutz von Ressourcen zu sehen, müssen sie ihre Perspektive auf strategische Geschäftsziele erweitern. Diese Perspektive muss in jeder Bewertung, jedem Vorstandsbericht und jeder Kommunikation des Sicherheitsteams im gesamten Unternehmen zum Ausdruck kommen.

Nur so können Unternehmen ihre Cyberresilienz gewährleisten und ein nachhaltiges Geschäftswachstum erzielen.

Untersuchungsmethode

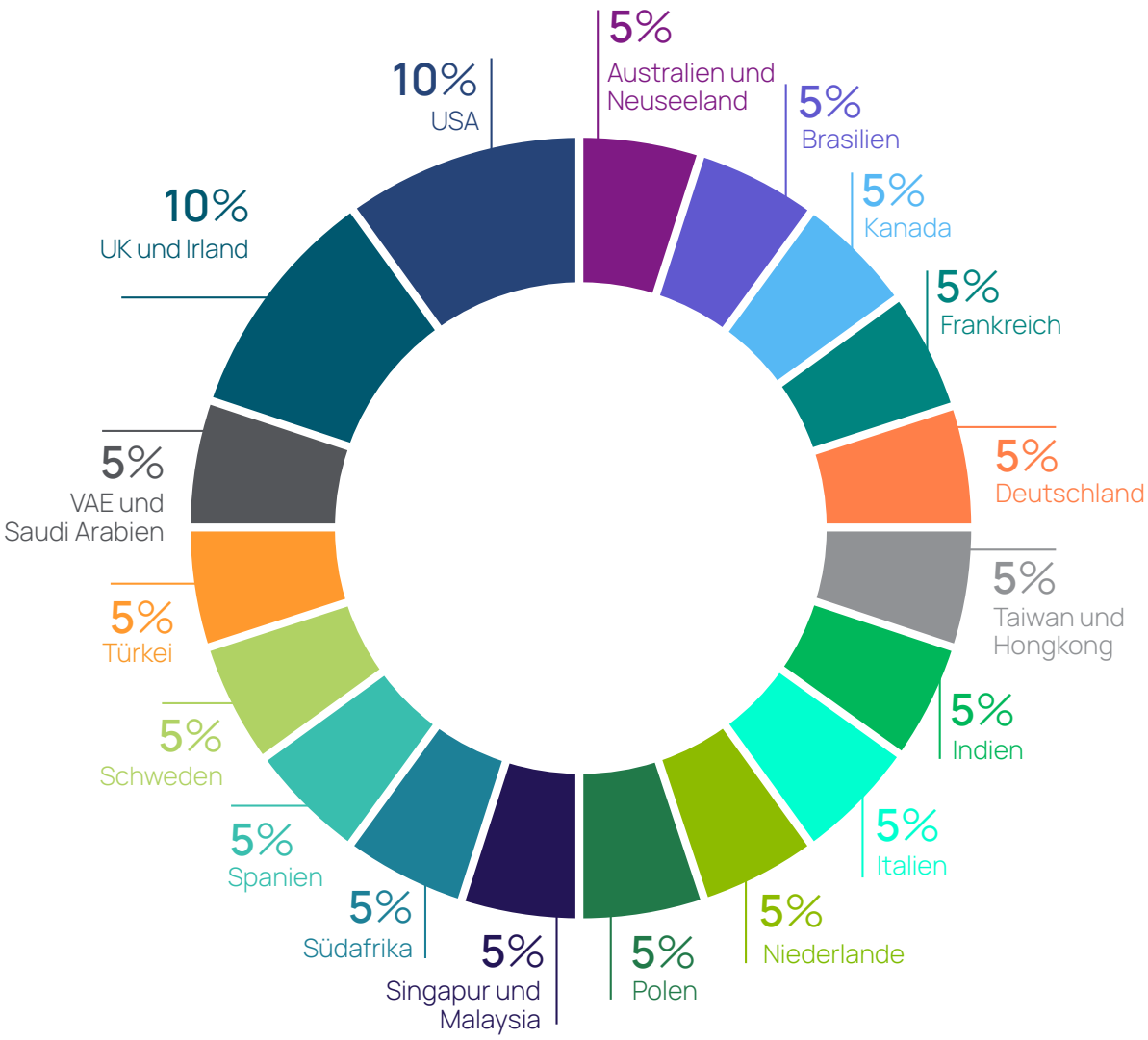
Bei der Umfrage wurden im März 2023 Antworten von 2.007 Personen gesammelt.

Sie enthält Antworten aus der Vorstandsebene, der Abteilungsleitungsebene und der Managementebene von Unternehmen. Die Befragten kamen aus 23 Ländern, 22 Branchen und arbeiteten in Unternehmen mit 500 oder mehr Beschäftigten.

Alle Teilnehmer gaben an, dass sie an Sicherheitsentscheidungen beteiligt waren, sei es als letzter Entscheidungsträger, als Teil eines Teams oder als Einflussnehmer.

Die Ergebnisse werden nicht gewichtet.

Land: In welchem Land leben Sie?

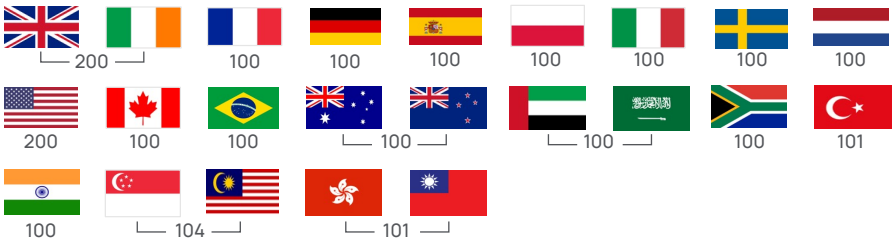


Zusammenfassung der demografischen Daten der Befragten

Demografische Daten

Befragte gesamt: **2.007**

Land des Wohnsitzes



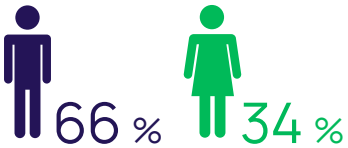
Rolle

Größe des Unternehmens

Anz. Mitarbeiter	500-999	1.000-4.999	Über 5.000
% der Befragten	35 %	40 %	26 %

Geschäftsbereich

Geschlecht und Alter



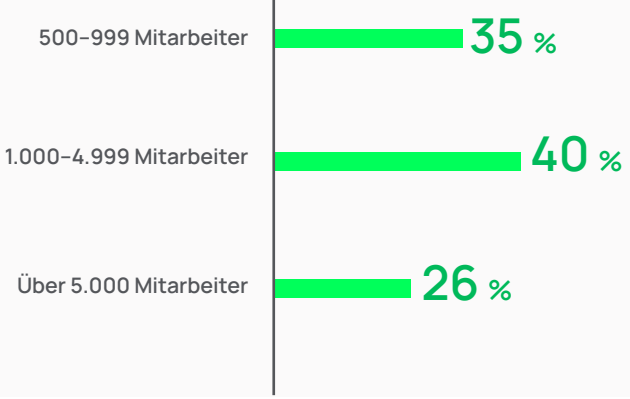
66 % der Befragten waren männlich und 34 % weiblich

der Befragten waren zwischen

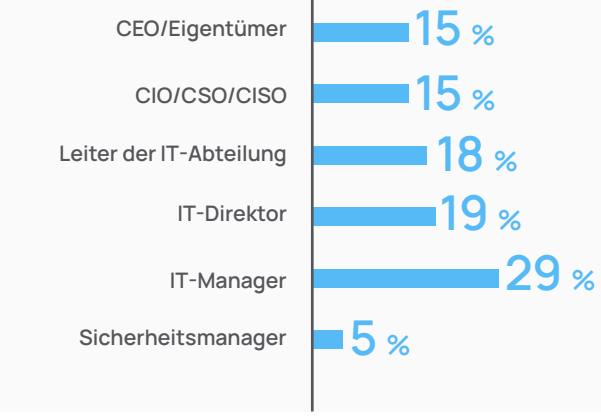
25–44

Größe der Organisation und Rolle: Wie viele Mitarbeiter beschäftigt die Organisation, für die Sie arbeiten? Welche der folgenden Angaben beschreibt Ihre Rolle im Unternehmen am besten?

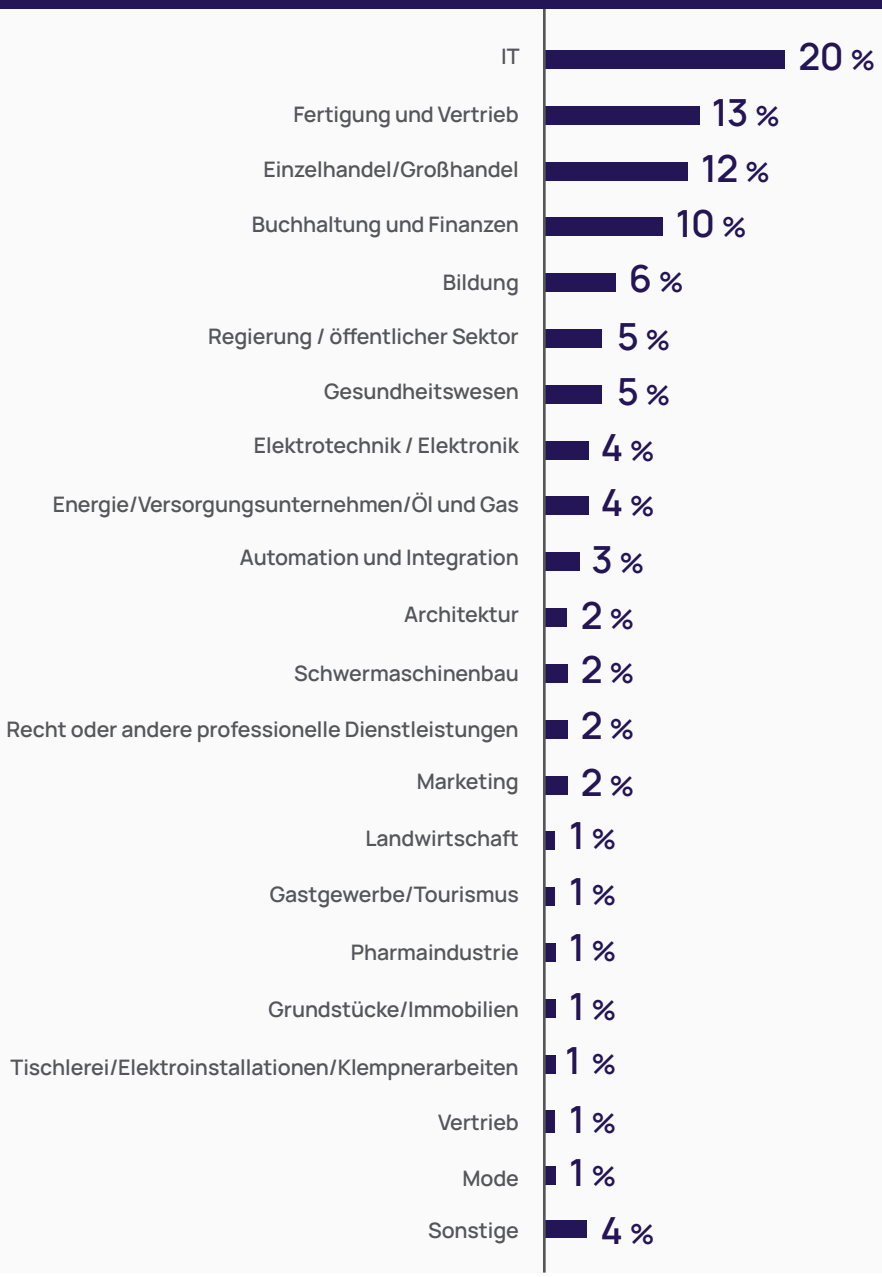
Größe der Organisation



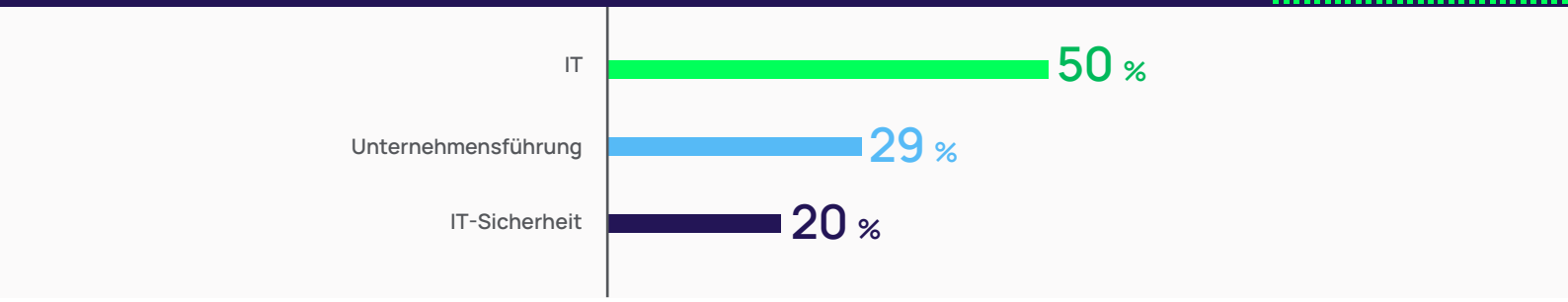
Rolle



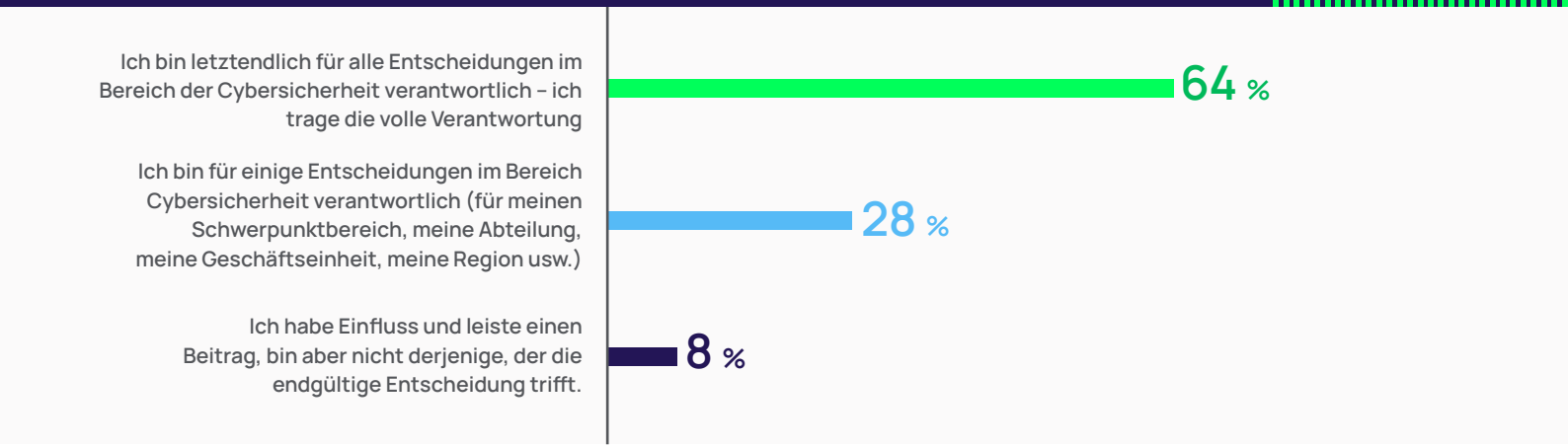
Branche: Welche dieser Angaben beschreibt Ihre Branche am besten?



Abteilungen: In welcher der folgenden Abteilungen sind Sie tätig?



Verantwortung: Inwieweit sind Sie für Entscheidungen im Bereich Cybersicherheit in Ihrem Unternehmen verantwortlich?



Delinea

Securing identities at every interaction

Delinea ist ein Vorreiter in der Sicherung von Identitäten durch zentralisierte Autorisierung. Dabei werden dank der nahtlosen Verwaltung der Interaktionen innerhalb des gesamten modernen Unternehmens die Organisationen sicherer. Mit Delinea können Organisationen über den gesamten Lebenszyklus der Identität hinweg diese für Cloud- und traditionelle Infrastruktur, Daten und SaaS-Anwendungen mit Kontext und Intelligenz ausstatten, um auf diese Weise Bedrohungen in Zusammenhang mit Identitäten auszuräumen. Dank der intelligenten Autorisierung bietet Ihnen Delinea als einzige Plattform die Möglichkeit, alle Identitäten aufzudecken, angemessene Zugriffsebenen zuzuweisen, Unregelmäßigkeiten zu erkennen und unverzüglich in Echtzeit auf Bedrohungen in Bezug auf Identitäten zu reagieren. Delinea verkürzt die Einarbeitungszeit Ihrer Teams von Monaten auf Wochen und fördert die Produktivität mit - Vergleich zu direkten Mitbewerbern - 90 % weniger Verwaltungsressourcen. Mit einer Verfügbarkeit von 99,99 % ist die Delinea Plattform eine der zuverlässigsten Lösungen für Identitätssicherheit auf dem Markt. Erfahren Sie mehr über Delinea auf **delinea.com**, **LinkedIn**, **X**, and **YouTube**.