

CIO

CSO

COMPUTERWOCHE

STUDIE

CYBERSICHERHEIT & DIGITALE RESILIENZ 2026



plusserver

T Systems

baramundi



Ein aktuelles Studienprojekt von
CIO, CSO und COMPUTERWOCHE

Gold-Partner

plusserver T Systems

Partner



Alle Angaben in diesem Ergebnisband wurden mit größter Sorgfalt zusammengestellt. Trotzdem sind Fehler nicht ausgeschlossen. Verlag, Redaktion und Herausgeber weisen darauf hin, dass sie weder eine Garantie noch eine juristische Verantwortung oder jegliche Haftung für Folgen übernehmen, die auf fehlerhafte Informationen zurückzuführen sind.

Der vorliegende Ergebnisberichtsband, einschließlich all seiner Teile, ist urheberrechtlich geschützt. Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen, auch auszugsweise, bedürfen der schriftlichen Genehmigung durch den Herausgeber.

Digitale Resilienz als Managementaufgabe



Matthias Teichmann
Director Research

Cyberangriffe gehören heute zu den zentralen Geschäftsrisiken für Unternehmen in der DACH-Region. Sie bedrohen nicht nur IT-Systeme, sondern auch Wertschöpfung, Reputation und regulatorische Handlungsfähigkeit. In hochvernetzten digitalisierten Organisationen geht es beim Thema Resilienz nicht allein darum, ob ein Angriff verhindert wird, sondern auch darum, wie schnell und kontrolliert ein Unternehmen unter Druck reagieren kann. Digitale Resilienz wird somit zur Führungsaufgabe.

Gerade in der DACH-Region mit ihrer starken Industrie- und Mittelstandsstruktur ist die Angriffsfläche groß: Vernetzte Produktionsumgebungen, hybride IT-Landschaften, Cloud-Services und komplexe Lieferketten schaffen Abhängigkeiten, die im Krisenfall schnell kaskadieren können. Gleichzeitig stoßen viele Organisationen an ihre Grenzen – durch Fachkräftemangel, historisch gewachsene Strukturen und eine Sicherheitsverantwortung, die zu häufig fragmentiert zwischen IT, Compliance und Risikomanagement verteilt ist.

Künstliche Intelligenz verschärft diesen Handlungsdruck. Aufseiten des Angreifers ermöglicht sie hochgradig skalierbare und dynamisch angepasste Attacken – vom personalisierten Phishing bis hin zum Identitätsbetrug. Auf der Verteidigungsseite kann KI dabei helfen, Komplexität zu beherrschen, indem sie eine bessere Erkennung relevanter

Bedrohungen, schnellere Entscheidungsunterstützung und effizientere Incident-Response-Prozesse ermöglicht. Voraussetzung hierfür ist eine klare strategische Einbettung. KI ist kein Selbstzweck, sondern ein Instrument, dessen Nutzen sich nur entfaltet, wenn Governance, Datenqualität und Verantwortlichkeiten stimmen.

Mit NIS2 und DORA wird Resilienz regulatorisch eingefordert. Beide Regelwerke verschieben den Fokus von rein technischen Maßnahmen hin zu überprüfbarer Managementverantwortung: Es braucht klare Zuständigkeiten auf Führungsebene, belastbare Melde- und Krisenprozesse sowie einen systematischen Umgang mit Risiken aus Drittparteien und Lieferketten. Für viele Unternehmen bedeutet das einen Kulturwandel – weg von reaktiver IT-Sicherheit, hin zu vorausschauender Steuerung. Und, wie unser Autor feststellt: „NIS2- und DORA-Compliance ist in den Köpfen, muss aber noch in die Systeme.“

Diese Studie soll aufzeigen, wie weit Unternehmen in der DACH-Region auf diesem Weg sind. Es soll verdeutlicht werden, wo Strukturen greifen und wo Lücken bestehen – und, dass Cybersicherheit vor allem dann wirksam wird, wenn sie als strategische Managementdisziplin verstanden wird.

Wir wünschen Ihnen eine erkenntnisreiche Lektüre!

Inhalt

6

21

Die wichtigsten Ergebnisse

Management Summary..... 6

Das zentrale Ergebnis

Die Umsetzung von NIS2 leidet unter Komplexität und hohem Aufwand 8

Die weiteren Key Findings 11

1. NIS2 und DORA entfalten Wirkung weit über Geltungsbereich hinaus 12
2. Die Umsetzung von DORA ist verspätet, aber in vollem Gange 13
3. Industriespionage erscheint bedrohlicher als Angriffe auf die Lieferkette 14
4. NIS2 hat einen deutlichen Einfluss auf die Lieferkette 16
5. Veraltete und proprietäre OT-Systeme erschweren die NIS2-Umsetzung..... 18
6. Die Maßnahmen für DORA sind ähnlich gehemmt wie die NIS2-Implementierung 19
7. Security-Verantwortliche denken über NIS2 oft anders als die IT-Leitung 20

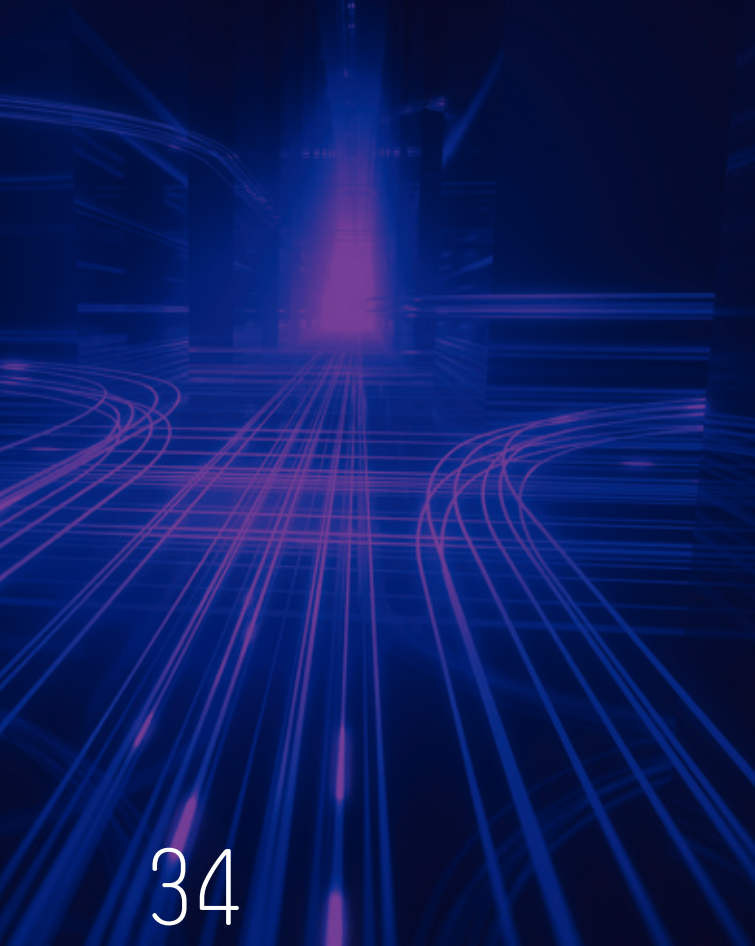
Editorial 3

Weitere Studienergebnisse

1. Die Verantwortung für Security liegt meistens nicht bei den sogenannten Security-„Verantwortlichen“ 22
2. Bei NIS2-Schulungen für das Management gibt es Nachholbedarf..... 23
3. IT-Risiken müssen noch stärker ins Risikomanagement einbezogen werden 24
4. Risikomanagement-Systeme und (Integrations-)plattformen sind weit verbreitet 25
5. Regeln für den Einsatz von künstlicher Intelligenz (KI) gehören fast zum Standard 26
6. Die große Mehrheit setzt bereits KI in der IT-Sicherheit ein..... 27
7. Compliance ist wichtig, aber nicht das Wichtigste 28
8. Das Ziel der KI-Nutzung ist (voll)automatisierte Cybersicherheit 29
9. Datensouveränität ist nicht der Hauptfokus digitaler Souveränität 30
10. Identitätssicherheit steht im Fokus, nicht Ransomware-Schutz..... 32

Studiendesign

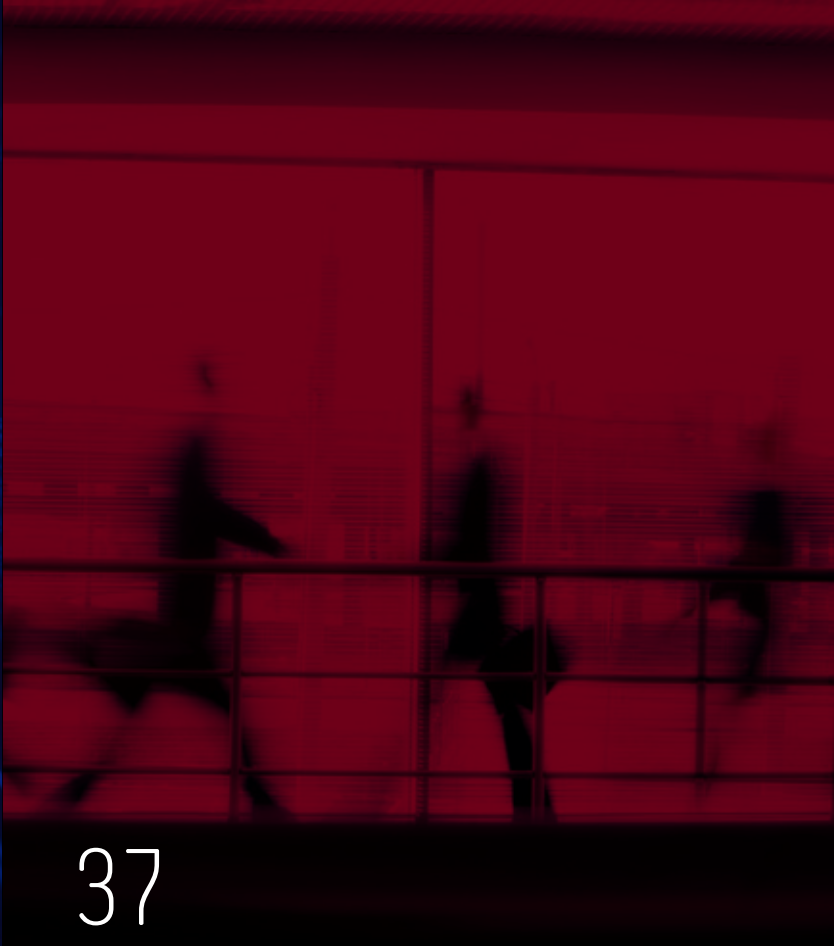
- Impressum 47
- Studiensteckbrief..... 48
- Stichprobenstatistik..... 49
- Studienkonzept, Round-Table-Moderation, Autor dieser Ausgabe 50
- Studienreihe..... 51



34

Blick in die Zukunft

NIS2- und DORA-Compliance ist in den Köpfen,
muss aber noch in die Systeme..... 35



37

CIO-Agenda 2026

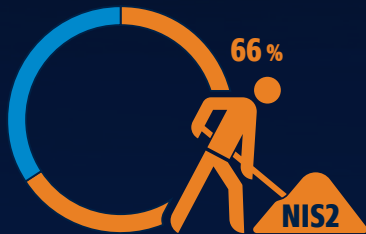
Daten zur allgemeinen Einschätzung der Marktlage 37



41

Die Studienpartner stellen sich vor

plusserver..... 42
T-Systems 44



Ein großer Teil der Unternehmen hat NIS2 immer noch nicht vollständig umgesetzt

Zehn Prozent der Befragten wissen immer noch nicht, ob sie betroffen sind. Jeweils **39 Prozent** der Unternehmen beklagen hohe Aufwände bei der Umsetzung oder die Komplexität der Vorgaben aus der NIS2-Richtlinie.



Über die Hälfte der Befragten sieht Industriespionage als große oder sehr große Bedrohung

40 Prozent nennen große Risiken durch Identitätsdiebstahl, aber nur etwa jedes dritte Unternehmen sieht große Cyberrisiken in der Lieferkette. Dabei beginnen inzwischen Industriespionage und Diebstahl von Identitäten oft mit Attacken auf die Lieferkette.



Die NIS2-Richtlinie verändert bereits spürbar die Lieferkette

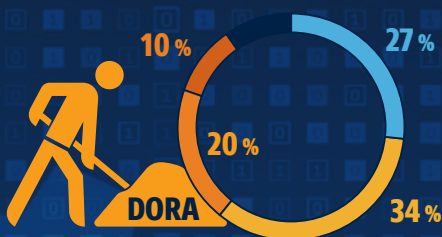
Mehr als die Hälfte der befragten Unternehmen hat wegen NIS2 einige oder sogar sehr viele Veränderungen an der Lieferkette vorgenommen. Nur **vier Prozent** meinen, die eigene Lieferkette sei von den NIS2-Vorgaben nicht betroffen.



Operational Technology (OT) ist eine besondere Herausforderung bei NIS2

Bei **70 Prozent** der befragten Unternehmen ist auch der OT-Bereich von NIS2 betroffen.

Dabei sehen **48 Prozent** in den veralteten und proprietären OT-Systemen eine große Herausforderung, wenn es um die NIS2-Umsetzung geht.



Die DORA-Compliance steht mehrheitlich noch aus

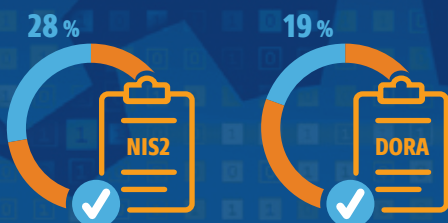
Trotz Anwendungspflicht der DORA-Verordnung gaben nur **27 Prozent** der Unternehmen an, DORA bereits vollständig umgesetzt zu haben.

34 Prozent gehen zum Teil bei den Schutzmaßnahmen über das geforderte Maß hinaus.

Weitere knapp **20 Prozent** planen eine vollständige Umsetzung bis Ende 2025, **zehn Prozent** planen dies bis Ende 2026.

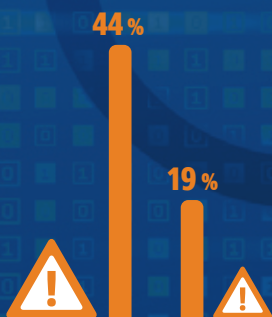
Management Summary

Die Key Findings im Überblick



NIS2 und DORA entfalten Wirkung weit über Geltungsbereich hinaus

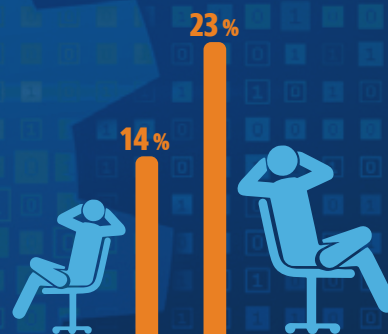
28 Prozent der Unternehmen, die weder direkt noch indirekt unter NIS2 fallen, haben die Vorgaben der Cybersicherheitsrichtlinie bereits umgesetzt. Im Fall von DORA sind es immerhin **19 Prozent**, die auch ohne Verpflichtung die Vorgaben implementiert haben.



Die Anforderungen durch DORA stellt viele Unternehmen vor Probleme

44 Prozent der befragten Unternehmen bereitet die Umsetzung von DORA große Schwierigkeiten.

Nur **19 Prozent** sagen, der Schwierigkeitsgrad von DORA sei gering. Die größten Herausforderungen sehen die Befragten – interessanterweise übrigens analog zu NIS2 – in der Komplexität von DORA und den hohen Aufwänden bei der Umsetzung.



IT-Leitung und Security-Verantwortliche sind bei NIS2-Fragen oft uneins

Nur **14 Prozent** der Security- und Risk-Verantwortlichen meinen, in den NIS2-Richtlinien stünde eigentlich nichts, was man nicht sowieso IT-Security-seitig machen müsste. Auf der IT-Leitungsebene denken jedoch **23 Prozent**, dass dem so ist.

Das zentrale Ergebnis

Die Umsetzung von NIS2 leidet unter Komplexität und hohem Aufwand

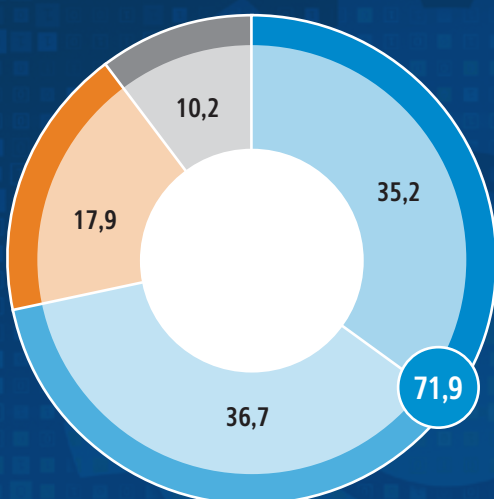
47 Prozent der befragten Unternehmen halten die Umsetzung von NIS2 für schwierig oder sehr schwierig, nur 15 Prozent sehen geringe Erschwernisse bei der NIS2-Umsetzung. Drei Viertel der Befragten haben für die NIS2-Umsetzung zwar ein dediziertes Budget. Zum Zeitpunkt der Umfrage erfüllten nach eigenen Angaben aber erst 34 Prozent vollständig die NIS2-Vorgaben.

NIS2 ist gegenwärtig eines der bedeutendsten Themen in der Cybersicherheit in Deutschland. Nur 18 Prozent der befragten Unternehmen sehen sich nicht betroffen von der NIS2-Richtlinie oder dem deutschen

NIS2-Umsetzungsgesetz. Und weitere zehn Prozent der Befragten können Ende 2025 immer noch nicht einschätzen, ob das eigene Unternehmen betroffen ist oder nicht.

Ist Ihr Unternehmen von der NIS2-Richtlinie betroffen?

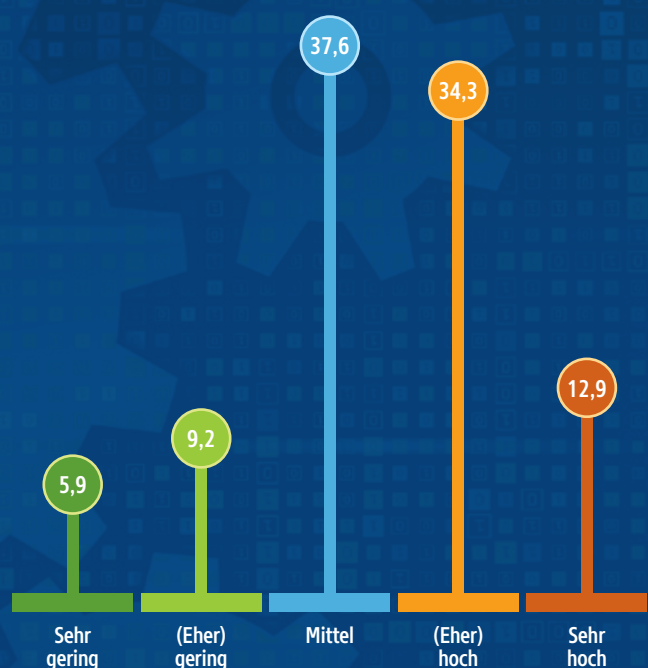
Angaben in Prozent. Basis: n = 324



- Ja, direkt von NIS2 betroffen
- Ja, indirekt von NIS2 betroffen
- Nein, nicht von NIS2 betroffen
- Weiß nicht

Wie bewerten Sie den Schwierigkeitsgrad der Umsetzung von NIS2 für Ihr Unternehmen?

Angaben in Prozent. Filter: Unternehmen, die direkt bzw. indirekt von der NIS2-Richtlinie betroffen sind ODER bereits in irgendeiner Form an der Umsetzung von NIS2-Vorgaben arbeiten. Basis: n = 272



Dabei besteht deutlicher Handlungsbedarf. Das gilt zum einen für die Klärung des notwendigen Budgets: 22 Prozent der Befragten haben kein spezielles Budget für die NIS2-Umsetzung bereitgestellt.

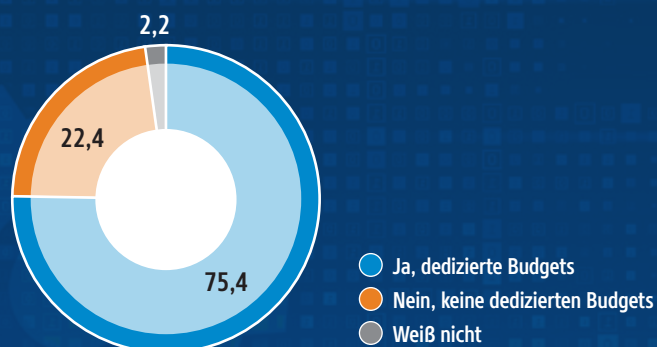
Zum anderen gibt nur gut ein Drittel der Unternehmen in der Umfrage an, dass die NIS2-Vorgaben vollständig umgesetzt sind. Das gilt für kleine wie auch große Firmen: Bei den kleinen Unternehmen mit weniger als 500 Beschäftigten und den mittelgroßen Unternehmen mit 500 bis 999 Mitarbeitenden liegt der Anteil bei 67 Prozent. Nur bei den großen Firmen ab 1000 Beschäftigten sind es mit 63 Prozent etwas weniger als zwei Drittel.

Zur ganzen Wahrheit gehört aber auch, und das ist in diesem Kontext die gute Nachricht, dass ein weiteres Drittel der Unternehmen zwar noch nicht jede einzelne NIS2-Anforderung vollständig erfüllt, dafür aber an (vielen) anderen Stellen die grundlegenden Anforderungen von NIS2 sogar übererfüllen.

Nicht untypisch für NIS2 ist ja auch, dass sich viele Anforderungen bekannt anfühlen, weil sie an bestehende Best Practices anknüpfen. Ob sie formal und nachweisbar vollständig erfüllt sind (inkl. Governance, Haftung, Meldeprozesse), wird sich in der Praxis oft erst noch zeigen.

Sind in Ihrem Unternehmen dedizierte Budgets für die Umsetzung von NIS2-Anforderungen zur Verfügung gestellt worden?

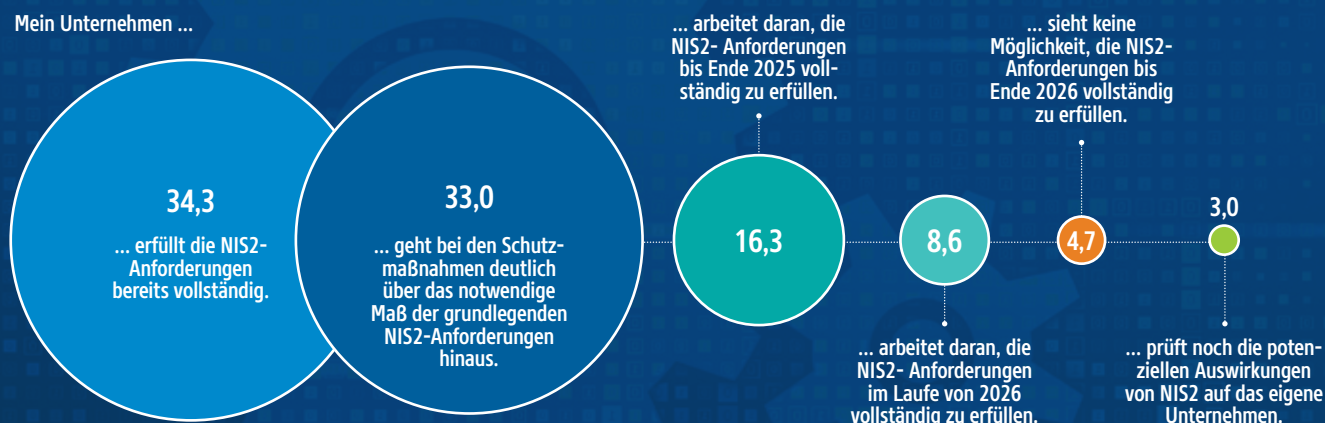
Angaben in Prozent. Filter: Unternehmen, die direkt bzw. indirekt von der NIS2-Richtlinie betroffen sind ODER bereits in irgendeiner Form an der Umsetzung von NIS2-Vorgaben arbeiten. Basis: n = 272



Wie gut erfüllt Ihr Unternehmen die NIS2-Anforderungen?

Angaben in Prozent. Filter: Unternehmen, die DIREKT bzw. INDIREKT von der NIS2-Richtlinie betroffen sind. Basis: n = 233

Mein Unternehmen ...



Die noch offene Umsetzung liegt begründet in einer Vielzahl von Herausforderungen, von denen die Unternehmen in der Umfrage berichten. Mit jeweils 39 Prozent der Antworten werden die hohen Aufwände bei der Anpassung auf NIS2 und die komplexen Vorgaben aus NIS2 als Erschwernisse genannt. Rund jedes dritte Unternehmen sieht Probleme in den unklaren regulatorischen Anforderungen und bei der Integration von NIS2-Vorgaben in bestehende IT-Systeme und -Prozesse (34 Prozent).

Offensichtlich besteht weiterhin ein hoher Aufklärungs- und Informationsbedarf für eine umfassendere Umsetzung von NIS2, und das bei Unternehmen jeder Größenordnung. Es herrscht dringender Handlungsbedarf, zumal auch in Deutschland nun die rechtlichen Vorgaben bestehen.

NIS2-Richtlinie

Die NIS2-Richtlinie (Network and Information Systems Directive 2) ist eine europäische Rechtsvorschrift, die auf die Verbesserung der Cybersecurity und des Schutzes kritischer Infrastrukturen abzielt. Ob ein Unternehmen unter die Vorgaben der NIS2-Richtlinie fällt, hängt von dessen Branche, Unternehmensgröße und jährlicher Bilanzsumme ab.

Unternehmen können auch indirekt von der NIS2-Richtlinie betroffen sein. Dies ist vor allem dann der Fall, wenn sie als Lieferanten oder Dienstleister für Unternehmen arbeiten, die direkt von NIS2 betroffen sind.

DORA-Verordnung

Die DORA-Verordnung (Digital Operational Resilience Act) betrifft primär Unternehmen im europäischen Finanzsektor und deren IT-Dienstleister.

DORA soll die digitale operationale Resilienz im Finanzsektor erhöhen und die Widerstandsfähigkeit gegenüber Cyberangriffen und anderen IT-Risiken verbessern. Die Verordnung legt verbindliche Maßnahmen für das Management von IKT-Risiken, Notfallpläne, die Meldung von Vorfällen und das Risikomanagement in Bezug auf Drittanbieter fest.

Was sind für Ihr Unternehmen die größten Herausforderungen bei der Umsetzung von NIS2?

Angaben in Prozent. Maximal drei Antworten möglich. Filter: Unternehmen, die direkt bzw. indirekt von der NIS2-Richtlinie betroffen sind ODER bereits in irgendeiner Form an der Umsetzung von NIS2-Vorgaben arbeiten. Basis: n = 272

Hoher Aufwand für Anpassung von Prozessen und Richtlinien	39,0
Komplexität der Anforderungen der NIS2-Verordnung	38,6
Unklare regulatorische Anforderungen bzw. Interpretationsspielräume	34,2
Integration in bestehende IT-Systeme und -Prozesse	33,8
Ressourcen- und Personalmangel (z. B. Fachkräfte, Budget)	19,9
Fehlendes internes Know-how oder Schulungsbedarf	12,9
Komplexität in der Zusammenarbeit mit Lieferanten/Dienstleistern	12,5
Technologische Herausforderungen (z. B. Legacy-Systeme, Schnittstellen)	9,6
Zeitdruck bei der Umsetzung	9,2
Abstimmung mit anderen Compliance-Anforderungen (z. B. DORA, ISO 27001)	7,4
Weiß nicht	1,1

Die weiteren Key Findings

Die wichtigsten Daten, Analysen
und Insights der Studie

NIS2 und DORA entfalten Wirkung weit über Geltungsbereich hinaus

Unter den befragten Unternehmen, die weder direkt noch indirekt von NIS2 betroffen sind, sagen nur zehn Prozent, dass sie keinen Grund sehen, die Cybersicherheitsrichtlinie ganz oder teilweise umzusetzen. Immerhin 28 Prozent erklären, dass sie die NIS2-Vorgaben umfassend implementiert haben, obwohl sie dazu gar nicht verpflichtet sind. Die DORA-Compliance erreichen immerhin 19 Prozent der Befragten freiwillig.

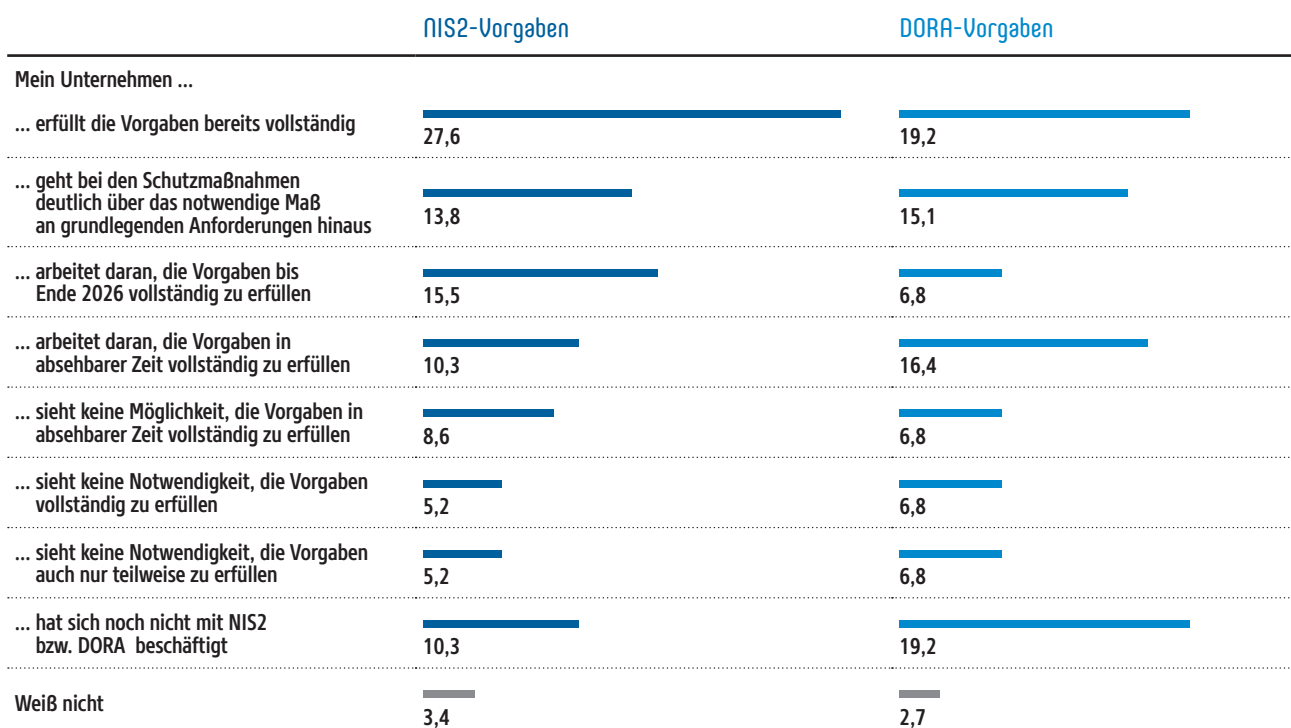
Unter den meisten Unternehmen aus der Umfrage, die weder direkt noch indirekt durch NIS2 reguliert werden, ist die Cybersicherheitsrichtlinie trotzdem ein wichtiges Thema. Mehr als 40 Prozent dieser Unternehmen haben NIS2 nach eigenen Angaben vollständig oder im überdurchschnittlichen Umfang umgesetzt. Weitere 16 Prozent wollen die NIS2-Compliance bis Ende 2026 erreichen, wohlgermerkt, obwohl sie dazu nicht rechtlich verpflichtet sind.

Bei DORA ist der Anteil der freiwilligen Umsetzung etwas weniger stark ausgeprägt, doch auch hier sagen 34 Prozent der Befragten, dass sie die entsprechenden Vorgaben vollständig oder deutlich über das notwendige Maß an grundlegenden DORA-Anforderungen hinaus implementiert haben.

Demnach haben sowohl NIS2 als auch DORA die Cybersicherheit auch in solchen Unternehmen beeinflusst, die nicht zum Anwendungsbereich der Richtlinien gehören. Bei DORA sind es nur 14 Prozent der Befragten, die mangels Betroffenheit auch keinen Anlass sehen, die Richtlinie ganz oder teilweise umzusetzen. Im Fall von NIS2 liegt dieser Anteil sogar nur bei zehn Prozent.

Wie gut erfüllt Ihr Unternehmen die NIS2- bzw. DORA-Vorgaben, obwohl es weder direkt noch indirekt von diesen betroffen ist?

Angaben in Prozent. Filter: Unternehmen, die NICHT von der NIS2- bzw. DORA-Richtlinie betroffen sind. Basis: n = 58 (NIS2) / n = 73 (DORA).



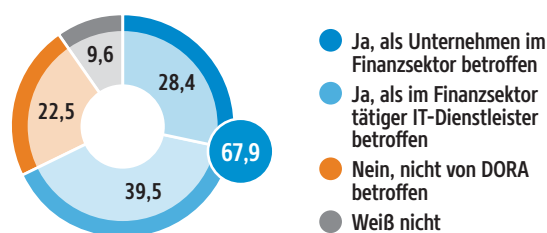
Die Umsetzung von DORA ist verspätet, aber in vollem Gange

Auch wenn die DORA-Verordnung bereits seit dem 17. Januar 2025 angewendet werden muss, sagen nur 27 Prozent der Unternehmen zum Zeitpunkt der Befragung, dass sie die Vorgaben bereits komplett erfüllt haben. Es sind 34 Prozent der Unternehmen, die vielleicht nicht jedes Kriterium vollständig erfüllen, aber in anderen Bereichen über die geforderten Schutzmaßnahmen hinausgehen.

Mehr als die Hälfte der Unternehmen (54 Prozent) plante die vollständige Umsetzung erst bis Ende 2025, weitere zehn Prozent wollten es bis Ende 2026 geschafft haben. Vier Prozent jedoch sehen keine Chance, DORA zumindest bis Ende 2026 umgesetzt zu haben. Obwohl mehr als zwei Drittel der Unternehmen (67 Prozent) sogar ein spezielles Budget zur Umsetzung von DORA vorgesehen haben, ist die Umsetzung der EU-Verordnung selbst viele Monate nach Anwendungspflicht in vielen Fällen nicht abgeschlossen. Dabei ist den meisten der befragten Unternehmen bewusst, dass sie von DORA betroffen sind. Nur jedes zehnte Unternehmen aus der Umfrage wusste dies noch nicht.

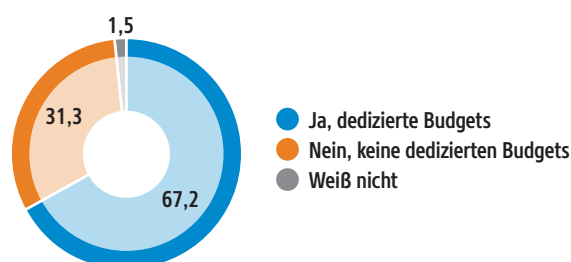
Ist Ihr Unternehmen von der DORA-Verordnung betroffen?

Angaben in Prozent. Basis: n = 324



Sind in Ihrem Unternehmen für die Umsetzung von DORA-Auflagen dedizierte Budgets zur Verfügung gestellt worden?

Angaben in Prozent. Filter Unternehmen, die von DORA betroffen sind ODER – obwohl nicht betroffen – trotzdem bereits daran arbeiten, die Anforderungen zu erfüllen. Basis: n = 262

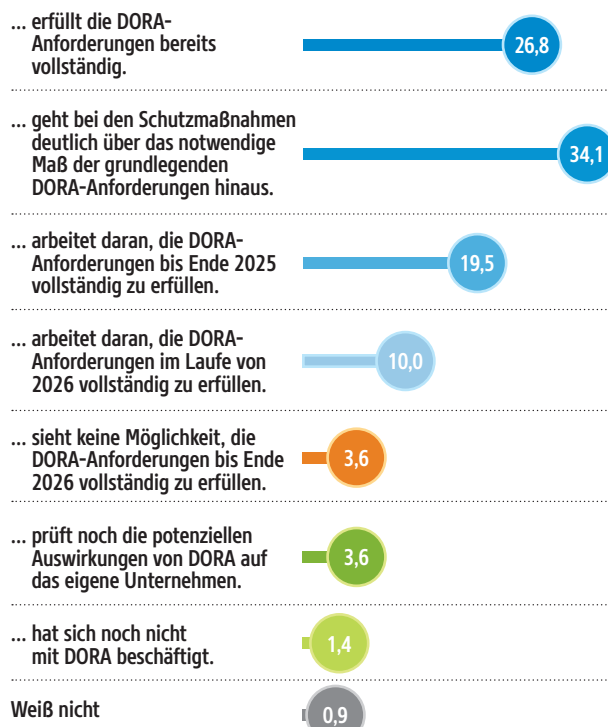


Kritisch zu sehen ist, dass ebenfalls zehn Prozent der Befragten erwarten, die Vorgaben erst bis Ende 2026 umsetzen zu können. Unter den Befragten sind sowohl Finanzdienstleister (28 Prozent der Befragten) als auch ITK-Dienstleister der Finanzbranche (40 Prozent der Umfrageteilnehmer). Beide Gruppen aber müssten bereits die Umsetzung abgeschlossen haben. Zwar ist offensichtlich die DORA-Umsetzung häufig in Verzug, aber entsprechende Aktivitäten liefen auf Hochtouren, um in Jahresfrist das Ziel der DORA-Compliance erreicht zu haben.

Inwieweit ist Ihr Unternehmen bereits auf DORA vorbereitet?

Angaben in Prozent. Filter: Unternehmen, die von DORA betroffen sind. Basis: n = 220

Mein Unternehmen ...



Industriespionage erscheint bedrohlicher als Angriffe auf die Lieferkette

Etwas mehr als die Hälfte der befragten Unternehmen schätzt die Gefahr, Opfer von Industriespionage zu werden, als groß oder sehr groß ein. Angriffe aus der oder auf die Lieferkette hält dagegen nur etwa jedes dritte Unternehmen für eine große oder sehr große Gefahr. Stärker verbreitet ist diese Sorge allerdings im C-Level (59 Prozent).

Was wird sonst noch als großes oder sehr großes Risiko angesehen? Gefürchtet werden in den Unternehmen besonders die Nachlässigkeit eigener Mitarbeitender (45 Prozent der Befragten), finanziell getriebene Cyberattacken (43 Prozent) und Cyberbedrohung durch fremdstaatliche Nachrichtendienste.

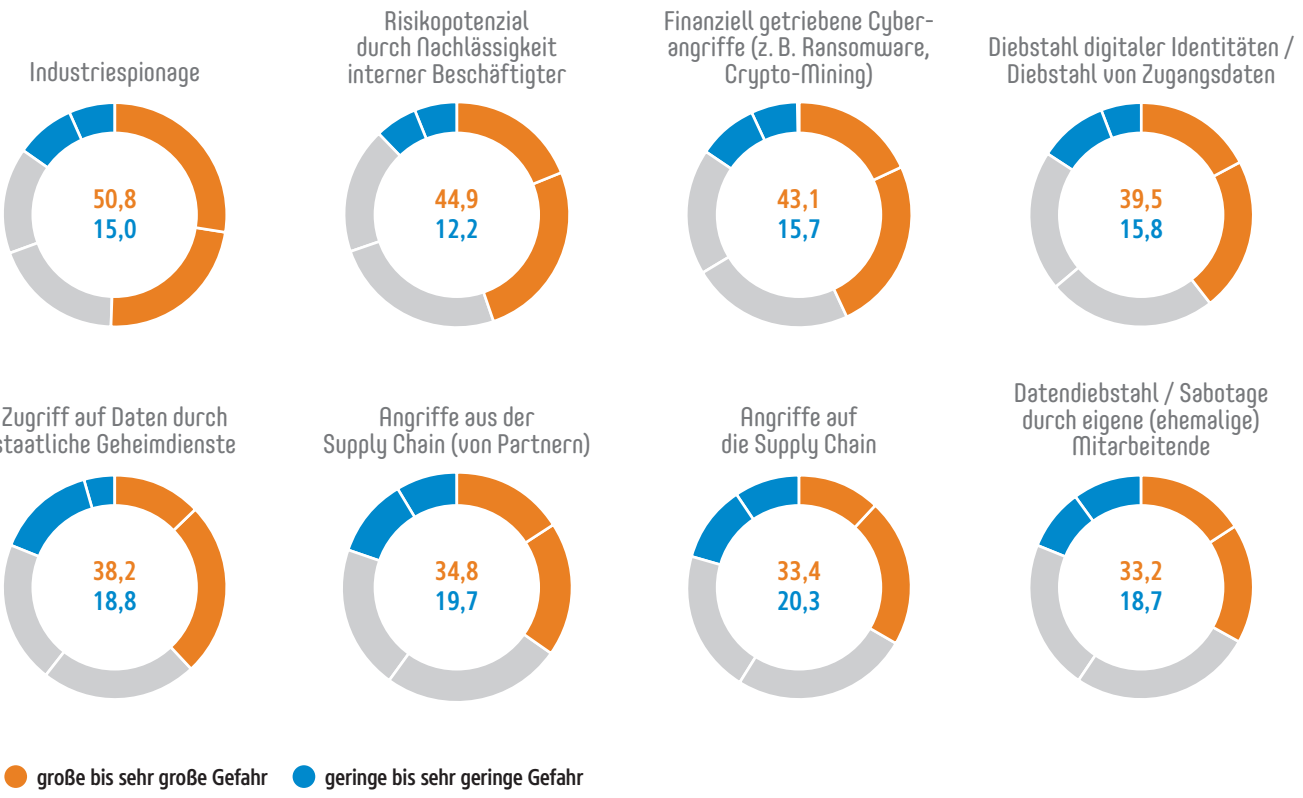
Die Lieferkette, deren Schutz explizit zu den Risikomanagement-Maßnahmen nach der Cybersicherheitsrichtlinie NIS2 gehört, wird im Vergleich seltener als Risikobereich betrachtet: 35 Prozent nennen Attacken aus

der Lieferkette, die von Geschäftspartnern ausgehen bzw. von diesen zu verantworten sind, als großes oder sehr großes Risiko. Nur jedes dritte Unternehmen (33 Prozent) sieht die Lieferkette selbst im Fokus von Angriffen.

Auch in den nächsten ein bis zwei Jahren rechnen nur 19 Prozent der Befragten mit deutlich zunehmenden Lieferkettenrisiken, dagegen erwarten 46 Prozent eine relevante Zunahme von finanziell getriebenen Cyberangriffen.

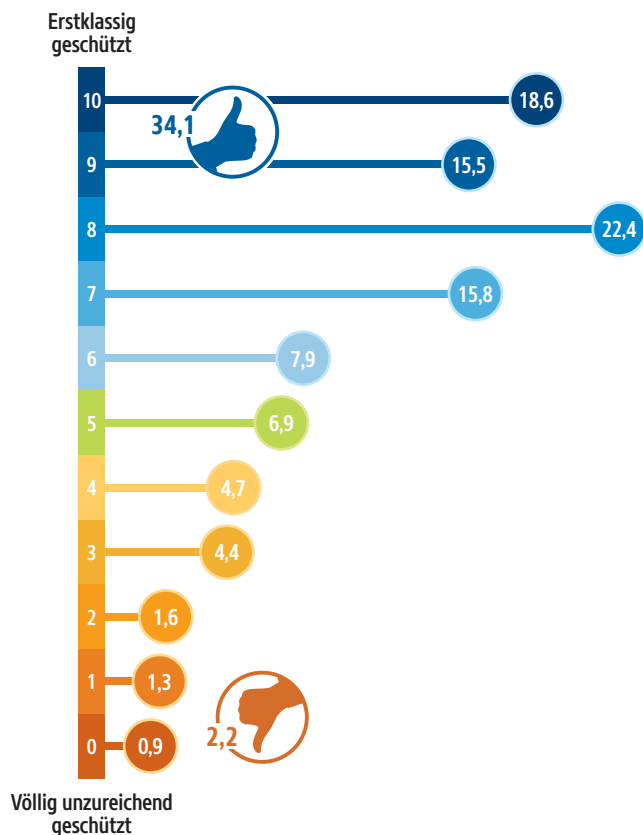
Wie groß schätzen Sie die Gefahr für Ihr Unternehmen ein, Opfer eines der folgenden Cybervorfälle zu werden?

Angaben in Prozent. Basis: n = 324



Und wie gut fühlen Sie sich als Unternehmen insgesamt vor den Gefahren der Cyberkriminalität geschützt?

Angaben in Prozent. Basis: n = 317



Gleichzeitig stuft sich mehr als jedes dritte befragte Unternehmen (34 Prozent) als sehr gut oder erstklassig geschützt ein. Einen unzureichenden oder völlig unzureichenden Schutz beklagen dagegen nur zwei Prozent der Befragten. Fachbereiche sind weniger optimistisch, was den eigenen Cyberschutz angeht. Hier sagen nur 13 Prozent, dass sie ihr Unternehmen für sehr gut oder erstklassig geschützt halten. Im C-Level dagegen sind es ganze 43 Prozent der Befragten, die so denken.

Bemerkenswert ist, dass der eigene Schutz des Unternehmens gar nicht ausreichend ist, denn viele Attacken erfolgen bereits über und aus der Lieferkette, auch dann, wenn das Ziel Industriespionage ist. Das Cyberrisiko „Lieferkette“ wird aber noch nicht so stark wahrgenommen, obwohl es explizit in NIS2 adressiert wird.

Welche dieser Gefahren werden für Ihr Unternehmen in den kommenden ein bis zwei Jahren an Relevanz deutlich zunehmen?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 324

Finanziell getriebene Cyberangriffe (z. B. Ransomware, Crypto-Mining)	46,0
Risiken durch KI und Automatisierung (z. B. Fehlentscheidungen, Manipulation)	33,0
Risikopotenzial durch Nachlässigkeit interner Beschäftigter	32,4
Diebstahl digitaler Identitäten / Diebstahl von Zugangsdaten	32,4
Zugriff auf Daten durch staatliche Geheimdienste	31,2
Industriespionage	29,9
Lieferkettenrisiken	19,1
Physische Sicherheitsrisiken (z. B. Naturkatastrophen, Sabotage)	19,1
Reputationsrisiken (z. B. durch Sicherheitsvorfälle oder Compliance-Verstöße)	18,5
Andere Gefahren	0,3
Weiß nicht	3,4

NIS2 hat einen deutlichen Einfluss auf die Lieferkette

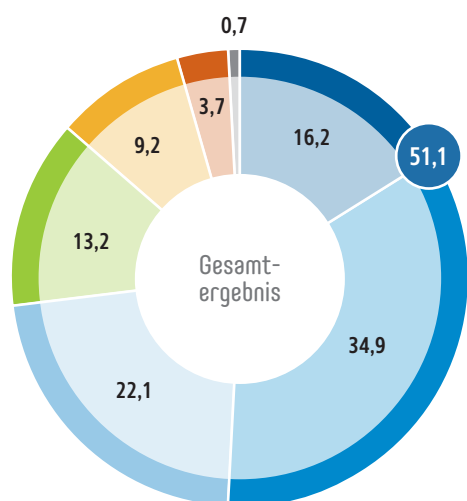
Nur 13 Prozent der Befragten erklären, NIS2 habe keinen nennenswerten Einfluss auf die Ausgestaltung der Lieferkette. Für neun Prozent sind die Auswirkungen von NIS2 auf die Lieferbeziehungen noch nicht absehbar. Vier Prozent glauben, NIS2 habe keinen Einfluss auf die eigene Lieferkette. Dem stehen 51 Prozent der Unternehmen gegenüber, die Veränderungen bei ihrer Lieferkette durch NIS2 feststellen.

Obwohl die Lieferkette in der Umfrage nicht als besonders bedeutendes Cyberrisiko gesehen wird und Angriffe auf die oder aus der Lieferkette im Vergleich zu anderen Cyberbedrohungen als weniger bedrohlich betrachtet werden, haben die NIS2-Vorgaben deutliche Auswirkungen auf die Lieferkette und damit zu Veränderungen bei Geschäftspartnern, Lieferanten und Dienstleistern geführt.

Bei größeren Unternehmen ab 1000 Beschäftigten bestätigen sogar 58 Prozent der Befragten, dass NIS2 die Lieferkette verändert hat. Bei mittelgroßen Unternehmen mit 500 bis 999 Beschäftigten sind es immer noch 53 Prozent, während dieser Anteil bei kleineren Unternehmen mit weniger als 500 Beschäftigten auf 43 Prozent sinkt.

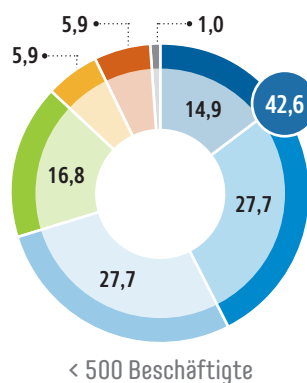
Wirkt sich NIS2 auf die Lieferketten Ihres Unternehmens aus? Gibt (oder gab) es aufgrund von NIS2 Veränderungen bei Geschäftspartnern, Lieferanten und Dienstleistern?

Angaben in Prozent. Filter: Unternehmen, die direkt bzw. indirekt von der NIS2-Richtlinie betroffen sind ODER bereits in irgendeiner Form an der Umsetzung von NIS2-Vorgaben arbeiten. Basis: n = 272

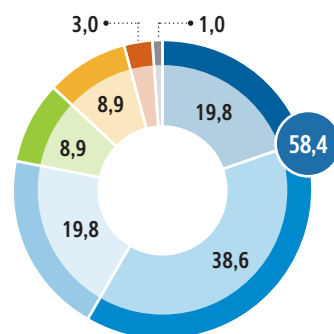


- Sehr viele Veränderungen
- Einige Veränderungen
- Wenige Veränderungen
- Keine nennenswerte Veränderung
- Noch unklar – Auswirkungen von NIS2 sind derzeit noch nicht absehbar
- Nicht relevant – NIS2 betrifft unsere Lieferkette nicht
- Weiß nicht

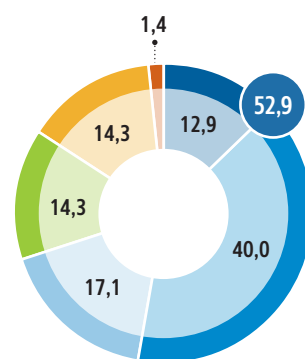
Ergebnis-Split nach Unternehmensgröße



< 500 Beschäftigte



1000 Beschäftigte und mehr

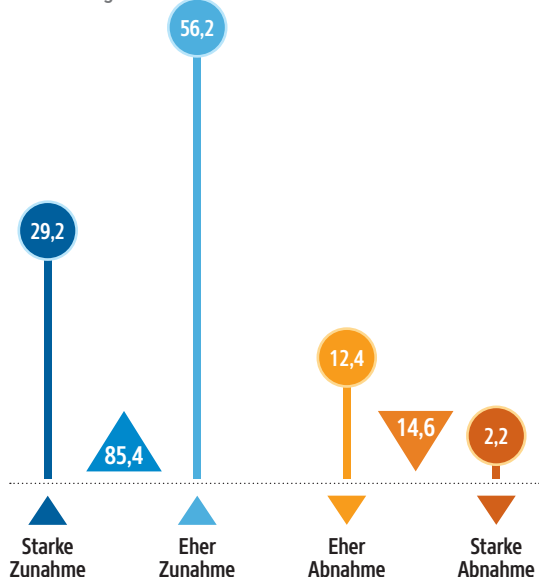


500 bis 999 Beschäftigte

Wie verändert sich die Anzahl der Geschäftspartner, Lieferanten und Dienstleister?

Angaben in Prozent. Filter: Unternehmen, bei denen sich NIS2 auf Lieferketten auswirkt.
Basis: n = 137

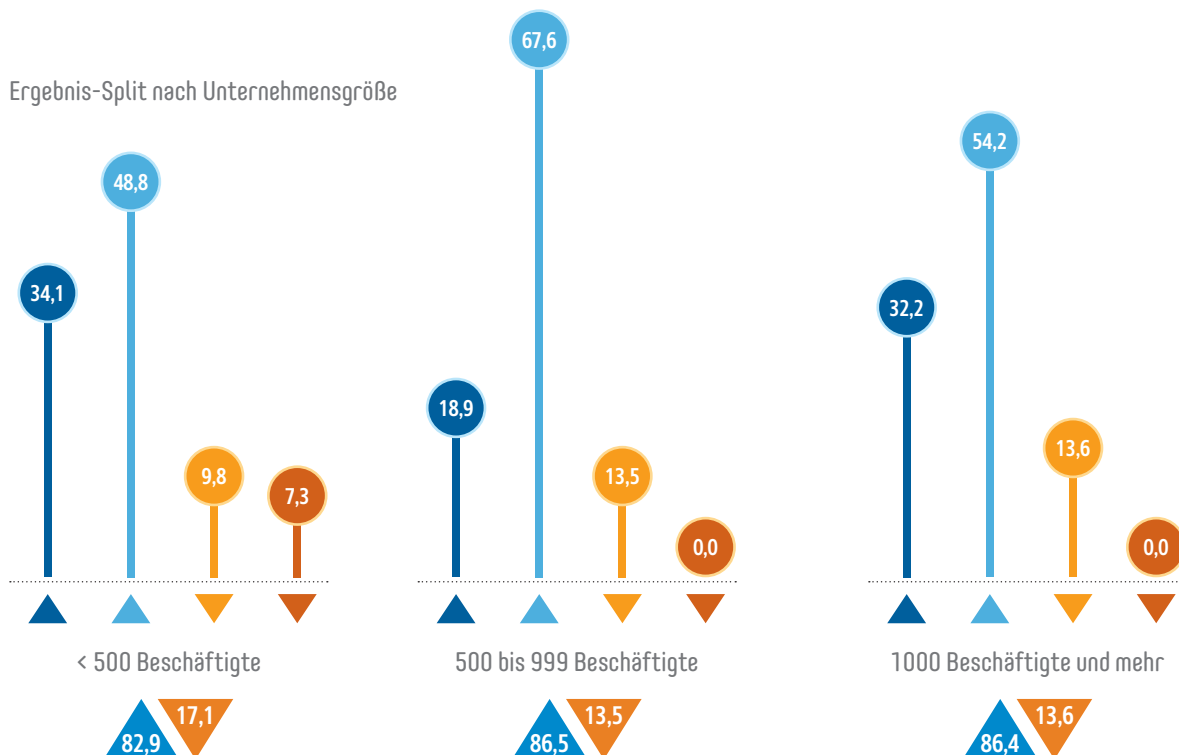
Gesamtergebnis



Interessanterweise hat die Anzahl der Lieferanten durch die Einflüsse von NIS2 nicht etwa durch Auslistung (zum Beispiel mangels Einhaltung von IT-Sicherheitsvorgaben) abgenommen, sondern sie ist tendenziell eher gestiegen. So berichten 85 Prozent der Befragten von einer Zunahme und entsprechend nur 15 Prozent von einer Abnahme bei der Zahl ihrer Lieferanten.

Daraus könnte man schließen, dass die befragten Unternehmen ihre Abhängigkeit von bestimmten Lieferanten verringern wollen, indem sie mehr Lieferantenbeziehungen aufbauen.

Ergebnis-Split nach Unternehmensgröße



Veraltete und proprietäre OT-Systeme erschweren die NIS2-Umsetzung

29 Prozent der befragten Unternehmen sehen ihren OT-Bereich stark betroffen von den Vorgaben der NIS2-Richtlinie, weitere 42 Prozent halten einen Teil ihrer OT-Systeme für NIS2-relevant. Jedoch glauben 19 Prozent der Unternehmen, nur ihr IT-Bereich sei von NIS2 betroffen, bei sieben Prozent findet die Betroffenheitsprüfung außerdem im OT-Bereich statt.

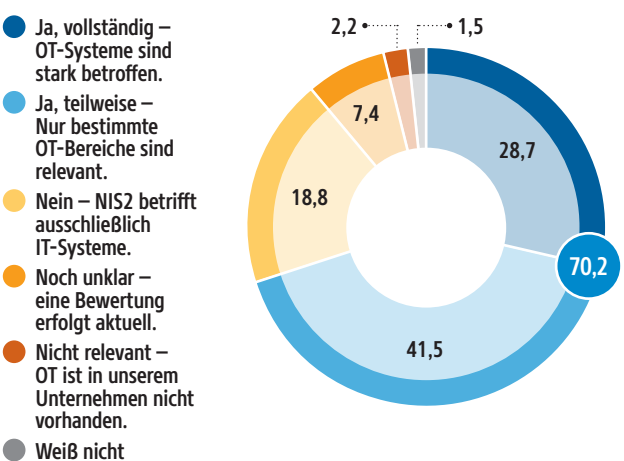
Da nur zwei Prozent der Unternehmen angeben, keine OT-Systeme einzusetzen, ist die Klärung der Frage, inwieweit NIS2 auch den OT-Bereich betrifft, sehr relevant. 70 Prozent der Befragten erklären, dass auch ihre OT-Systeme den NIS2-Vorgaben entsprechen müssen und liegen damit richtig, im Gegensatz zu den fast 20 Prozent der Unternehmen, die NIS2 nur auf die IT beziehen.

Die Klärung und Feststellung, wie der OT-Bereich von NIS2 betroffen ist, ist jedoch nicht die einzige Herausforderung. 48 Prozent der befragten Unternehmen beklagen veraltete oder proprietäre OT-Technologien ohne aktuelle Sicherheitsfunktionen, 47 Prozent berichten von Schwierigkeiten, Sicherheitsanforderungen in bestehende OT-Systeme zu integrieren. Weitere Herausforderungen bei der Umsetzung von NIS2 im OT-Bereich sind für 32 Prozent der Befragten der Mangel an Fachpersonal mit kombiniertem IT- und OT-Know-how, bei 30 Prozent der Unternehmen die Abhängigkeit von Drittanbietern oder Herstellern für Sicherheitsupdates. Zudem nennen 23 Prozent der Befragten einen hohen Aufwand für Monitoring und Incident Response in OT-Umgebungen. Zudem nennen 19 Prozent der Befragten die Kosten für Nachrüstungen und Sicherheitsmaßnahmen. 18,3 Prozent der Befragten nennen die Gefahr von Produktionsunterbrechungen durch Sicherheitsmaßnahmen. 14,7 Prozent der Befragten nennen die Komplexität bei der Netz-trennung und Segmentierung (IT vs. OT). 12,0 Prozent der Befragten nennen fehlende Standards und klare Vorgaben speziell für OT. 0,5 Prozent der Befragten wissen nicht.

Damit zeigt sich, dass der OT-Bereich bei der NIS2-Umsetzung nicht etwa ausgespart werden darf, sondern besondere Beachtung erfordert.

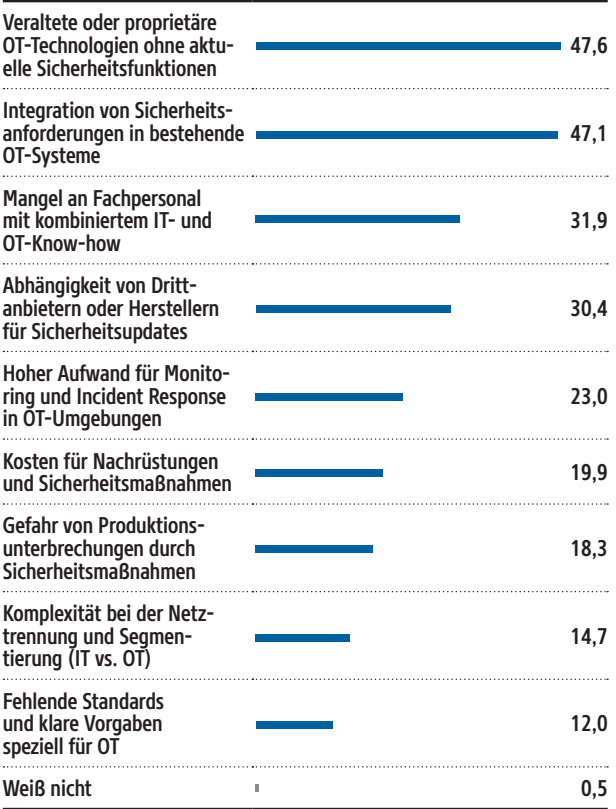
Muss die NIS2-Richtlinie in Ihrem Unternehmen auch im Bereich der Operational Technology (OT) umgesetzt werden?

Angaben in Prozent. Filter: Unternehmen, die direkt bzw. indirekt von der NIS2-Richtlinie betroffen sind ODER bereits in irgendeiner Form an der Umsetzung von NIS2-Vorgaben arbeiten. Basis: n = 272



Welche besonderen Herausforderungen sehen Sie bei der Umsetzung von NIS2 im OT-Bereich?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen, bei denen die NIS2-Richtlinie auch im Bereich Operational Technology (OT) umgesetzt werden muss. Basis: n = 191



Die Maßnahmen für DORA sind ähnlich gehemmt wie die NIS2-Implementierung

18 Prozent der befragten Unternehmen, die sich mit DORA befassen, sehen sehr große Schwierigkeiten bei der Umsetzung, weitere 26 Prozent immer noch hohe oder eher hohe Schwierigkeitsgrade. Dabei sind es die größeren Unternehmen mit mindestens 1000 Beschäftigten, die zu einem Anteil von 20 Prozent besonders häufig sehr große Erschwernisse beklagen.

In den Fachbereichen der befragten Unternehmen werden die Schwierigkeiten bei der DORA-Umsetzung weniger häufig als sehr groß bezeichnet, hier sind es nur zwölf Prozent, die dies sagen.

Als Gründe für die Schwierigkeiten bei der Implementierung von DORA nennen 39 Prozent der Befragten die Komplexität der Anforderungen, und 34 Prozent erwähnen die hohen Aufwände, die bei der Anpassung der Prozesse und Richtlinien entstehen. Damit ähnelt die Art der Herausforderungen, die bei DORA am häufigsten genannt werden, stark

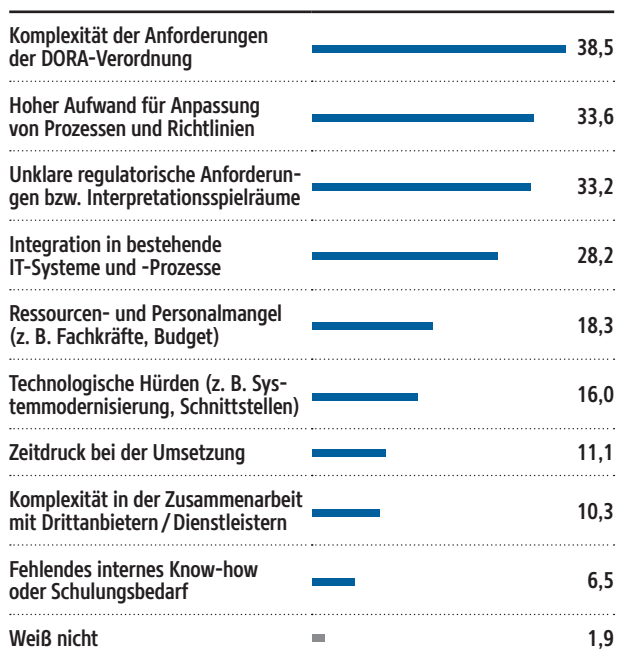
jenen, von denen in der Umfrage in Bezug auf NIS2 berichtet wurde.

Fehlendes Know-how und Schulungsbedarf sehen nur sieben Prozent der Befragten als Herausforderung bei der DORA-Umsetzung, obwohl die Anforderungen ja bei vielen Unternehmen als komplex angesehen werden. Die größeren Unternehmen mit mindestens 1000 Beschäftigten nennen jedoch häufiger einen Schulungsbedarf aufgrund von DORA, hier sind es immerhin 14 Prozent der Befragten.

Interessanterweise werden fehlendes Know-how und Schulungsbedarf bei NIS2 mit 13 Prozent der Nennungen insgesamt häufiger genannt als im Fall von DORA. Bei NIS2 scheinen die größeren Unternehmen mit mindestens 1000 Mitarbeitenden aber seltener Schulungsbedarf zu sehen, hier sagen dies nur zehn Prozent der Befragten.

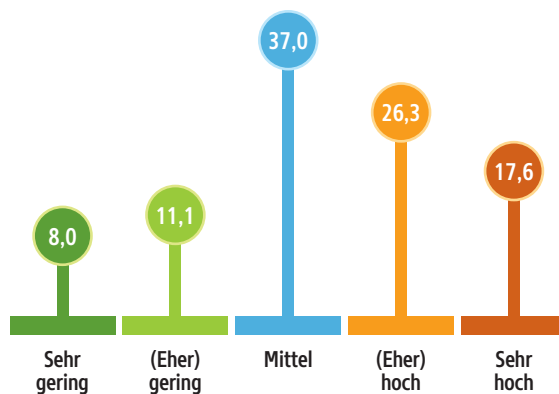
Was sind für Ihr Unternehmen die größten Herausforderungen bei der Umsetzung von DORA?

Angaben in Prozent. Filter: Unternehmen, die von DORA betroffen sind ODER – obwohl nicht betroffen – trotzdem bereits daran arbeiten, die Anforderungen zu erfüllen. Basis: n = 262



Wie bewerten Sie den Schwierigkeitsgrad der Umsetzung von DORA für Ihr Unternehmen?

Angaben in Prozent. Filter: Unternehmen, die von DORA betroffen sind ODER – obwohl nicht betroffen – trotzdem bereits daran arbeiten, die Anforderungen zu erfüllen. Basis: n = 262



7 Security-Verantwortliche denken über NIS2 oft anders als die IT-Leitung

Bittet man Verantwortliche für Security und Risk sowie IT-C-Level und IT-Leitungen um die Bewertung von Statements zu NIS2 und Cybersicherheit, weichen Zustimmung und Ablehnung der beiden Gruppen meist deutlich voneinander ab. Dies ist wichtig zu wissen, da die Federführung von Security-Entscheidungen oftmals bei den Verantwortlichen mit IT-Leitungsfunktionen angesiedelt ist.

„In den NIS2-Richtlinien steht eigentlich nichts, was man nicht sowieso IT-Security-seitig machen müsste“, dem stimmen nur 14 Prozent der befragten Security- oder Risk-Verantwortlichen zu. Auf IT-Leitungsebene jedoch denken 23 Prozent der Befragten, dass dem so ist.

Ähnlich ist dies bei der Aussage „NIS2 bewirkt schon mal eines: Sie schafft mehr Aufmerksamkeit für das IT-Security-Thema bei Nicht-Experten und Expertinnen“: Das bestätigen nur 16 Prozent der Verantwortlichen für Security oder Risk. Im IT-C-Level, bei IT-Leitungen, IT-Fachbereichsleitungen und in IT-Bereichen (Security, Ops) sind es aber 24 Prozent der Befragten, die diese Meinung vertreten.

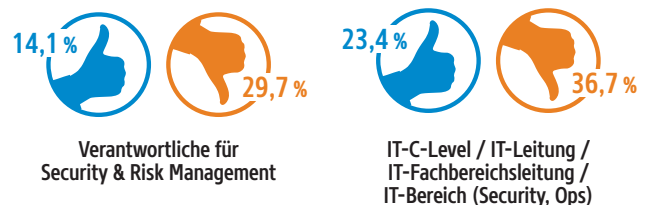
Relativ einig sind sich diese Gruppen jedoch, wenn es um die NIS2-Implementierung im OT-Bereich geht, also bei der Betriebstechnologie. Die Zustimmung zu „Eine Umsetzung von NIS2 im OT-Bereich ist kaum realisierbar“ beträgt bei den Security- / Risk-Verantwortlichen zehn Prozent, in den IT-Leitungsebenen elf Prozent der Befragten.

Insgesamt standen im Rahmen dieser Studie ein gutes Dutzend Statements zur Bewertung. Nur bei vier Statements waren sich die beiden fokussierten Gruppen halbwegs einig, und zwar in der Einschätzung, dass sich „der Schutz vor Ransomware-Attacken (...) in den vergangenen zwölf Monaten deutlich verbessert“ hat, es „ein viel zu großes Risiko ist, die IT-Security der KI zu überlassen“, „mehr Regulierung (...) zu mehr IT-Sicherheit“ führt und dass „KI ein Zusatz, kein Ersatz für IT-Security-Dienstleister“ ist.

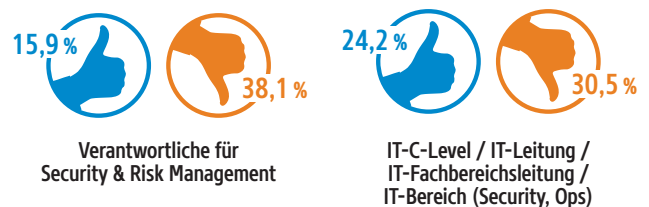
Nachfolgend sind nun einige Statements aufgeführt. Sagen Sie uns bitte jeweils, inwieweit Sie diesen Aussagen zustimmen können?

Angaben in Prozent. Basis: n = 324

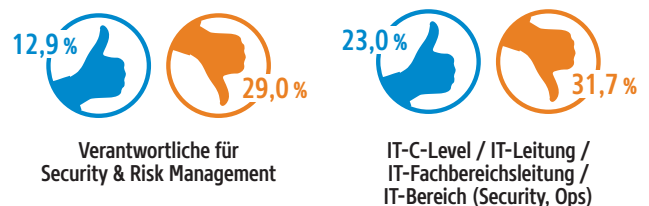
„In den NIS2-Richtlinien steht eigentlich nichts, was man nicht sowieso IT-Security-seitig machen müsste.“



„NIS2 bewirkt schon mal eines: Sie schafft mehr Aufmerksamkeit für das IT-Security-Thema bei Nicht-Experten und Expertinnen.“



„Eine Umsetzung von NIS2 im OT-Bereich ist kaum realisierbar.“



- „Stimme zu“ bis „Stimme voll und ganz zu“
- „Stimme nicht zu“ bis „Stimme überhaupt nicht zu“

Weitere Studienergebnisse

Komplementäre Analysen
und Insights der Studie

Die Verantwortung für Security liegt meistens nicht bei den sogenannten Security-„Verantwortlichen“

CISOs, CSOs und (IT-)Security-Vorstände haben nur in 13 Prozent der befragten Unternehmen die federführende Verantwortung für die Security. Selbst wenn mindestens zehn Prozent des IT-Budgets für Security aufgewendet werden, sind es nur 15 Prozent dieser Gruppe, die wirklich Security-Verantwortliche sind.

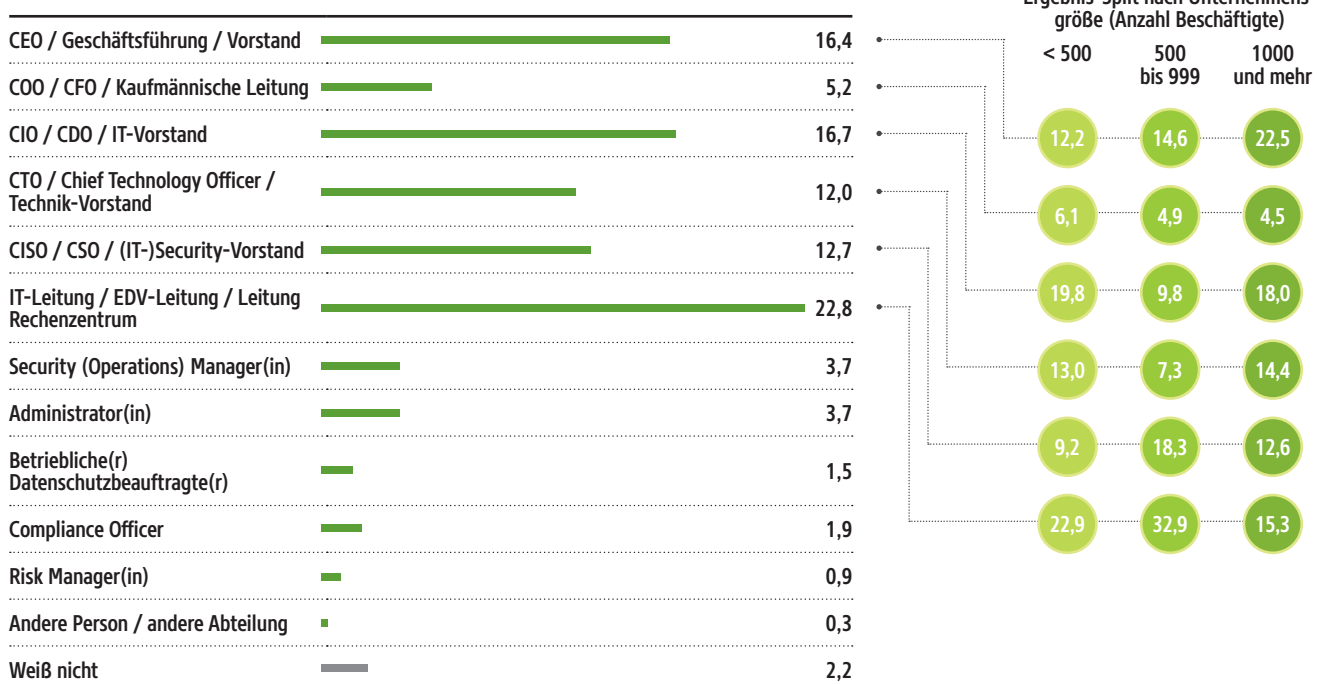
Am häufigsten obliegt der IT-Leitungsebene (IT-Leitung / EDV-Leitung / Leitung Rechenzentrum) die Hauptverantwortung für die Security mit 23 Prozent der Nennungen. Auf Platz 2 liegen CIO / CDO / IT-Vorstand, die bei 17 Prozent der Befragten die Security-Verantwortung federführend innehaben.

Besonders häufig ist die IT-Leitungsebene bei den mittelgroßen Unternehmen mit 500 bis 999 Beschäftigten mit der Security-Verantwortung betraut, hier ist es jedes dritte Unternehmen (33 Prozent der Befragten), das dies sagt.

Da NIS2 explizit Maßnahmen im Risikomanagement fordert, ist es interessant zu sehen, wie die bisherige Zuständigkeit unter den Risikomanagerinnen und Risikomanagern für IT-Sicherheit ist. Laut Umfrage sind es bisher nur ein Prozent dieser Gruppe, die für Security verantwortlich zeichnen. Das gilt für alle Unternehmensgrößen, nicht nur bei kleinen Unternehmen, die womöglich noch kein ausgeprägtes Risikomanagement eingeführt haben.

Wer ist in Ihrem Unternehmen federführend verantwortlich für das Thema IT-Security?

Angaben in Prozent. Basis: n = 324



Bei NIS2-Schulungen für das Management gibt es Nachholbedarf

Obwohl von NIS2 Security-Schulungen für die Geschäftsführung gefordert werden, bieten erst 44 Prozent der Unternehmen solche NIS2-Trainings als verpflichtende Maßnahme an, weitere 37 Prozent sehen dies noch als freiwillige Fortbildung an. Bei elf Prozent der Unternehmen gibt es eine solche Schulung noch gar nicht. Hier besteht also dringender Handlungsbedarf.

Management-Schulungen zu NIS2 und DORA kommen im Vergleich zu anderen Security-Trainings seltener als verpflichtende Maßnahme vor. Selbst bei großen Unternehmen mit mindestens 1000 Mitarbeitenden sind verpflichtende NIS2-Fortbildungen für das Management nur bei jedem zweiten dieser Unternehmen vorgesehen. Bei acht Prozent der großen Unternehmen gibt es gar keine NIS2-Schulungen für die Geschäftsführung.

Blickt man mit dem Datenschutz auf einen anderen Compliance-Bereich, sind hier Schulungen erst bei 47 Prozent der Unternehmen über alle Unternehmensgrößen hinweg ver-

pflchtend. Scheinbar hat sich hier die ebenfalls obligatorische Schulung zum Datenschutz immer noch nicht durchsetzen können. 37 Prozent der Unternehmen stufen die Datenschutz-Schulung als freiwillig ein.

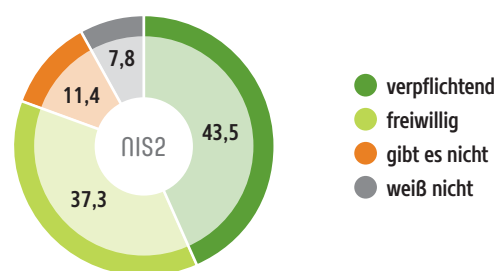
Besonders häufig gibt es verpflichtende Security-Schulungen zu aktuellen Bedrohungen, hier sagen 56 Prozent der Befragten, dass eine entsprechende Fortbildung verpflichtend ist. Weitere 34 Prozent der Unternehmen sehen eine freiwillige Unterweisung zu diesem Thema vor. Gar keine entsprechende Schulung gibt es bei neun Prozent der befragten Unternehmen.

Welche Schulungen, Weiterbildungen oder Trainings bietet Ihr Unternehmen seinen Beschäftigten als verpflichtende Maßnahme im Bereich IT-Security an?

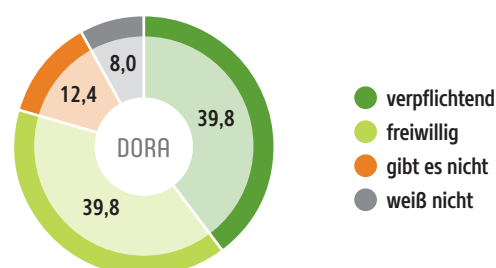
Angaben in Prozent. Basis: n = 324

Regelmäßige Schulungen zu aktuellen Bedrohungen	55,8
Schulungen/Trainings rund um Compliance / Datenschutz	46,5
Schulungen / Trainings rund um IT-Security Awareness	45,9
Interne Zertifizierungsprogramme für IT-Security-Verantwortliche	44,8
NIS2-Schulung für Management und Geschäftsführung	43,5
Schulungen/Trainings zur sicheren Nutzung von Cloud-Diensten	42,1
DORA-Schulung für Management und Geschäftsführung	39,8
Andere Schulungen / Trainings	17,7

NIS2-Schulung für Management und Geschäftsführung
Angaben in Prozent. Basis n= 306



DORA-Schulung für Management und Geschäftsführung
Angaben in Prozent. Basis n= 299



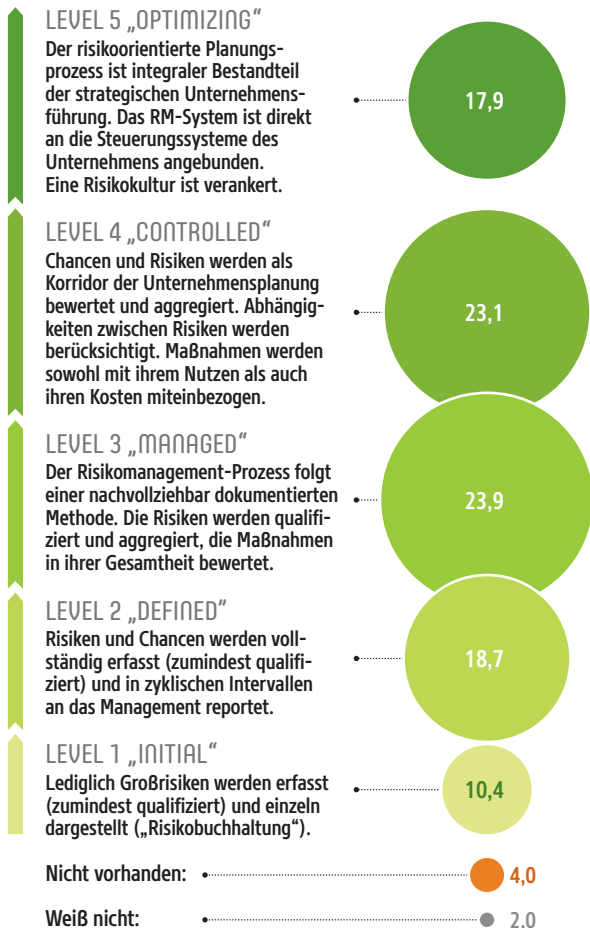
3 IT-Risiken müssen noch stärker ins Risikomanagement einbezogen werden

84 Prozent der befragten Unternehmen sehen sich im „Risk Maturity Model“ mindestens auf Stufe 2 und haben ihrer Ansicht nach alle Risiken erfasst. Doch nur 44 Prozent der Befragten haben sich auch dediziert mit IT-Risiken und IT-Sicherheitsrisiken befasst. 45 Prozent wollen dies erst in näherer Zukunft nachholen, weitere elf Prozent sehen dies auch in Zukunft nicht vor.

Mit Blick auf NIS2 muss sich das Risikomanagement in vielen der befragten Unternehmen ändern, denn IT-Risiken und IT-Sicherheitsrisiken müssen Teil des betrieblichen Risikomanagements sein. Ist dies nicht der Fall, sollten sich Unternehmen im „Risk Maturity Model“ nicht schon auf Stufe 2 oder höher einstufen.

Wie schätzen Sie den Reifegrad des Risikomanagements in Ihrem Unternehmen ein (nach dem „Risk Maturity Model“)?

Angaben in Prozent. Filter: Teilnehmer, die im C-Level, in der IT-(Security-)Leitung oder im Risk Management tätig sind. Basis: n = 251



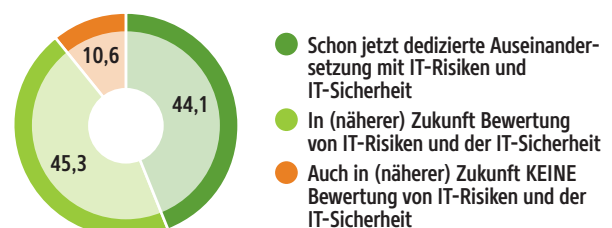
Gut die Hälfte der großen Unternehmen sehen im Risikomanagement schon heute eine dedizierte Auseinandersetzung mit IT-Risiken und IT-Sicherheit vor.

Bei kleinen Unternehmen sinkt dieser Anteil auf 34 Prozent, bei mittelgroßen Unternehmen sind es 44 Prozent, die bereits die IT-Risiken und die IT-Sicherheit als Teil des Risikomanagements sehen.

Wenn IT-Risiken und IT-Sicherheit im Risikomanagement Berücksichtigung finden, ist die IT-Abteilung aber nur in sechs von zehn Fällen stark involviert, dabei ist IT-Sicherheit ein Gebiet, bei dem Expertise gefragt ist, um die Risiken angemessen bewerten zu können.

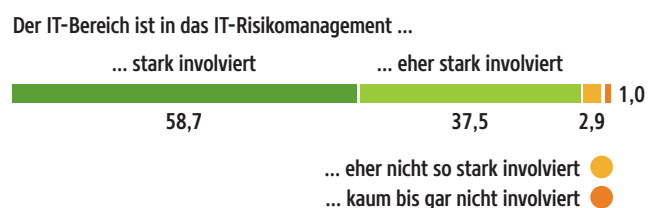
Ist die IT eigener Bestandteil des Risikomanagements Ihres Unternehmens?

Angaben in Prozent. Filter: Unternehmen, die ein Risikomanagement Reifegrad 1 bis 5 etabliert haben. Basis: n = 236



Wie stark ist der IT-Bereich in das IT-Risikomanagement Ihres Unternehmens involviert?

Angaben in Prozent. Filter: Unternehmen, bei denen sich die IT schon jetzt dediziert mit IT-Risiken und IT-Sicherheit auseinandersetzt. Basis: n = 104



Risikomanagement-Systeme und (Integrations-)plattformen sind weit verbreitet

Basisaufgaben des Risikomanagements sind bei 61 Prozent der Befragten durch Managementsysteme oder (Integrations-)Plattformen abgedeckt. Bei weiteren 36 Prozent der Unternehmen ist dies geplant. Nur zwei Prozent der Befragten haben keine solche Lösung im Risikomanagement und planen dies auch nicht.

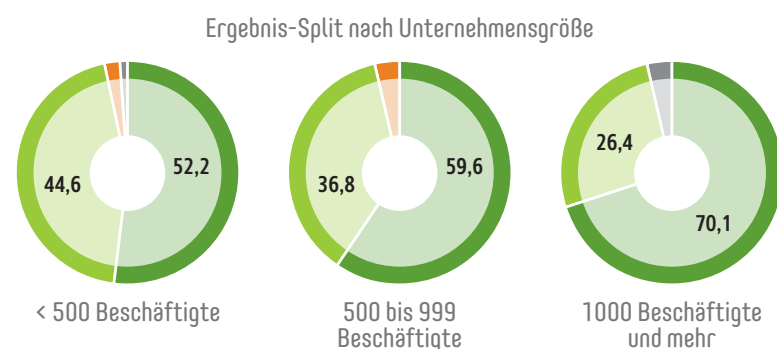
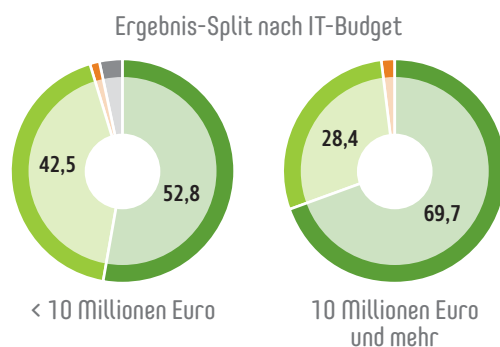
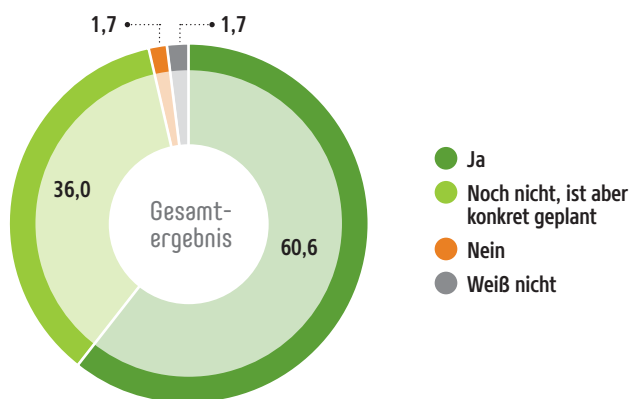
Bei großen Unternehmen ab 1000 Beschäftigten sind es sogar 70 Prozent der Befragten, bei denen Basisaufgaben des Risikomanagements durch Managementsysteme oder (Integrations-)Plattformen abgedeckt sind. Bei kleinen Unternehmen mit weniger als 500 Mitarbeitenden sinkt dieser Wert auf 52 Prozent. Bei den mittelgroßen Unternehmen mit 500 bis 999 Beschäftigten sind es 60 Prozent der Befragten mit Managementsystemen oder (Integrations-)Plattformen, die Basisaufgaben im Risikomanagement abdecken.

Einen Einfluss hat auch die Höhe des zur Verfügung stehenden IT-Budgets: Sind es zehn Millionen Euro pro Jahr oder mehr, steigt der Anteil der Befragten mit entsprechenden Managementsystemen oder (Integrations-)Plattformen auf 70 Prozent. Ist das IT-Budget kleiner, sinkt dieser Anteil auf 53 Prozent.

Wichtig erscheint es dabei, dass die Managementsysteme oder (Integrations-)Plattformen auch die IT-Risiken und IT-Sicherheitsrisiken abdecken, damit die Unternehmen leichter den Vorgaben von NIS2 oder DORA gerecht werden können.

Werden in Ihrem Unternehmen Basisaufgaben des Risikomanagements durch Managementsysteme oder (Integrations-)Plattformen abgedeckt?

Angaben in Prozent. Filter: Unternehmen, die ein Risikomanagement Reifegrad 1 bis 5 etabliert haben. Basis: n = 236



5 Regeln für den Einsatz von künstlicher Intelligenz (KI) gehören fast zum Standard

72 Prozent der befragten Unternehmen haben Richtlinien für den Einsatz von KI, mindestens für Teilbereiche. Davon sind es 34 Prozent der Befragten, die für das ganze Unternehmen dokumentierte und verbindliche KI-Regeln eingeführt haben. Bei fünf Prozent werden KI-Regeln gerade entwickelt, vier Prozent der Befragten haben keine solchen Richtlinien.

Nur zwei Prozent der Unternehmen sagen, sie setzen gar keine KI ein, entsprechend haben sie natürlich auch keinen Bedarf an Richtlinien, um den KI-Einsatz zu regeln. Mit einem Anteil von vier Prozent geben überraschend wenig Unternehmen an, dass sie über keine KI-Policy verfügen. Bei allen anderen, also der großen Mehrheit der Unternehmen, sind KI-Richtlinien ein Thema.

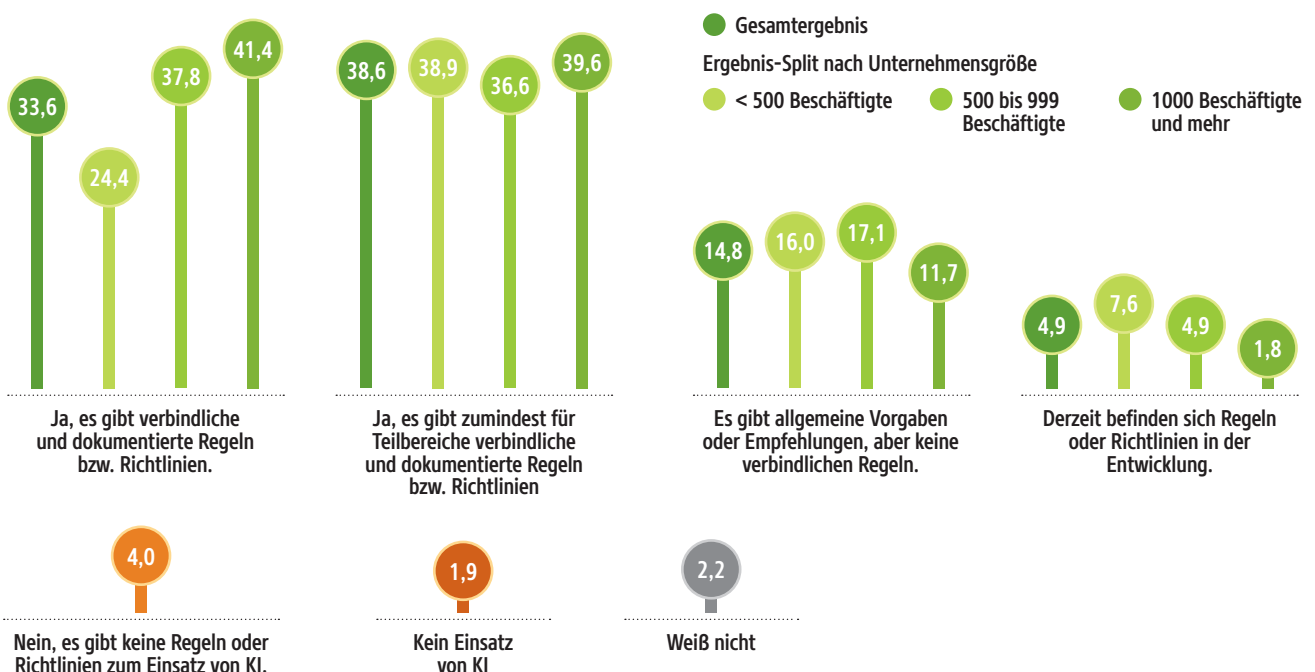
Der Grad an Implementierung von KI-Richtlinien nimmt mit der Größe des Unternehmens zu. Bei kleineren Unternehmen mit weniger als 500 Beschäftigten liegt der Anteil derer, die KI-Regeln zumindest in

Teilbereichen oder aber im ganzen Unternehmen haben, bei 63 Prozent. Mittelgroße Unternehmen mit 500 bis 999 Beschäftigten haben spezielle KI-Regeln in 74 Prozent der Fälle. Bei großen Unternehmen ab 1000 Beschäftigten sind es sogar 81 Prozent, die in Teilbereichen oder sogar im ganzen Unternehmen verbindliche und dokumentierte KI-Richtlinien bestätigen.

Die Höhe des IT-Budgets wirkt sich ebenfalls aus: Bei zehn Millionen Euro oder mehr als jährliches IT-Budget liegt der Anteil der Firmen mit KI-Regeln bei 76 Prozent. Ist das IT-Budget geringer, sinkt dieser Wert auf 70 Prozent der befragten Unternehmen.

Gibt es in Ihrem Unternehmen verbindliche Regeln oder Richtlinien für den Einsatz von künstlicher Intelligenz (KI)?

Angaben in Prozent. Basis: n = 324



Die große Mehrheit setzt bereits KI in der IT-Sicherheit ein

Fast die Hälfte der Unternehmen setzt KI als Empfehlungssystem in der IT-Sicherheit ein. Die KI schlägt also Maßnahmen vor, ohne eigenständig Änderungen vorzunehmen. Doch bereits 41 Prozent der Befragten geben der KI in der IT-Sicherheit administrative Rechte, zum Beispiel für die automatische Durchführung von Sicherheitsmaßnahmen.

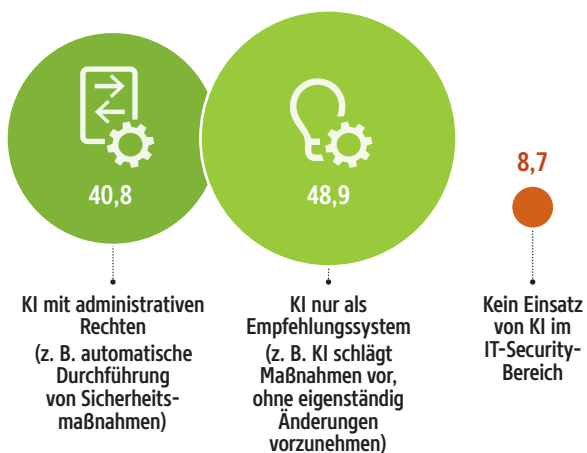
Nur neun Prozent der Befragten setzen bisher keine KI in der IT-Sicherheit ein, zwei Prozent können es nicht genau sagen. Damit ist KI in der IT-Security bereits sehr weit verbreitet und hat oftmals schon administrative Rechte zur Ausübung von IT-Sicherheitsmaßnahmen.

Interessant ist, dass der Anteil der Unternehmen, die KI als Empfehlungssystem in der IT-Sicherheit einsetzen, über alle Unternehmensgrößen hinweg nahezu gleich ist. Unterschiede nach Größenordnung gibt es jedoch bei KI-Lösungen, die administrative Rechte erhalten. Dies ist bei kleinen Firmen nur bei 36 Prozent der Fall, bei mittelgroßen und großen Unternehmen ab 1000 Mitarbeitenden sind es dagegen 44 Prozent der Befragten, die dies bejahen.

Die Umfrage zeigt auch, für welche IT-Sicherheitsbereiche KI-basierte Methoden eingesetzt werden, um Abläufe und Prozesse

Wie setzt Ihr Unternehmen künstliche Intelligenz (KI) im Bereich IT-Sicherheit ein?

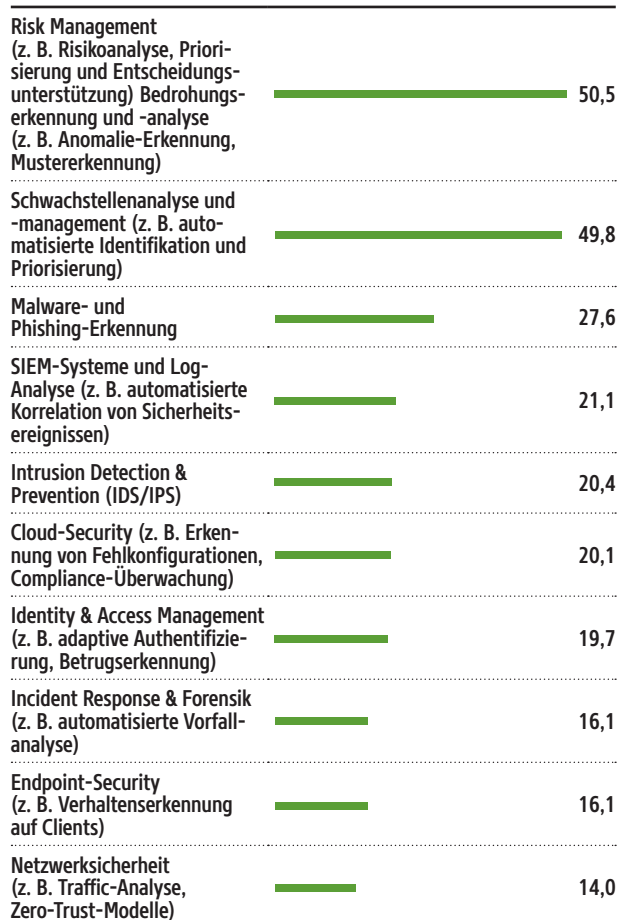
Angaben in Prozent. Filter: Unternehmen, die KI einsetzen. Basis: n = 311



zu optimieren. Besonders häufig ist dies mit 51 Prozent der Nennungen im Risk Management der Fall, also für Risikoanalysen, Priorisierung und Entscheidungsunterstützung, Bedrohungserkennung und -analyse wie Anomalie-Erkennung und Mustererkennung.

In welchen IT-Security-Bereichen setzt Ihr Unternehmen KI-Methoden bzw. KI-gestützte Software-Lösungen ein, um Abläufe und Prozesse zu optimieren oder automatisieren?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen, die KI im IT-Security-Bereich einsetzen. Basis: n = 279



7 Compliance ist wichtig, aber nicht das Wichtigste

Die zunehmenden gesetzlichen und regulatorischen Anforderungen sind für 60 Prozent der Befragten ein Thema, das für die IT-Sicherheit im Unternehmen wichtig ist. Doch es gibt noch wichtigere Themen: 65 Prozent der Unternehmen nennen Hardware-Sicherheit, 64 Prozent die fehlenden Schnittstellen zwischen Security-Systemen und Non-Security-Systemen.

Nur für die kleinen Unternehmen mit weniger als 500 Beschäftigten sind die regulatorischen und gesetzlichen Anforderungen das wichtigste Thema in der IT-Sicherheit, dies sagen hier 67 Prozent der Befragten. Die Bedeutung des Compliance-Themas sinkt dagegen mit der Unternehmensgröße. Mittlere Unternehmen mit 500 bis 999 Beschäftigten nennen die rechtlichen Anforderungen zu 59 Prozent, bei den großen Unternehmen ab 1000 Beschäftigten sind es dagegen nur noch 53 Prozent.

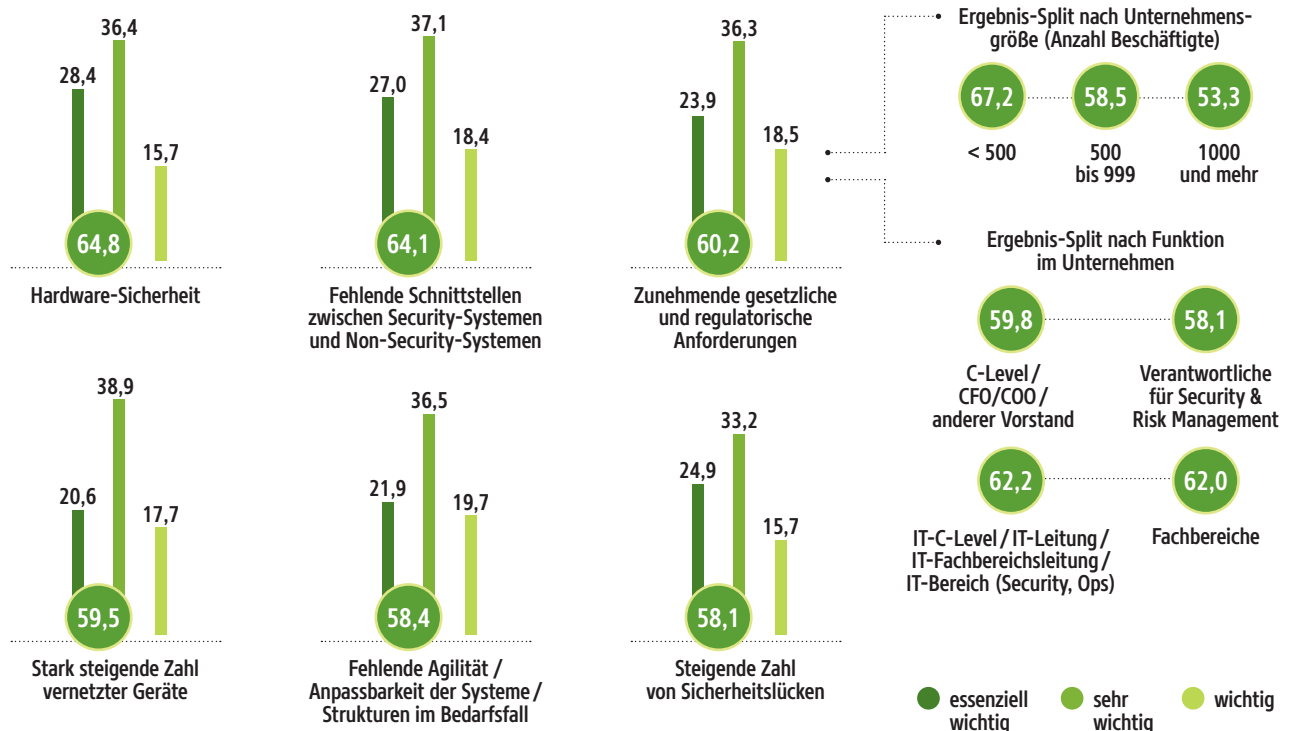
Auch die Rollen der Befragten machen einen gewissen Unterschied in der Bewertung, ob Compliance wirklich so wichtig ist, wie

die allgemeine Berichterstattung suggeriert. Besonders wichtig ist Compliance als Security-Thema der IT-Leitungsebene und den Fachbereichen mit 62 Prozent der Nennungen. Im C-Level sinkt dieser Anteil auf 60 Prozent der Nennungen. Bei den Verantwortlichen für Security und Risk ist der Anteil vergleichsweise am geringsten, hier sagen dies 58 Prozent der Befragten.

Auch wenn die Unterschiede bei den Rollen nicht sehr groß sind, zeigt die Tendenz dennoch, dass IT und Fachbereiche eher die Compliance als Thema sehen als die oftmals für die Umsetzung zuständigen Personen aus Security und Risk.

Für wie wichtig halten Sie die folgenden Themen in Bezug auf die IT-Security in Ihrem Unternehmen?

Angaben in Prozent. Basis: n = 324



Das Ziel der KI-Nutzung ist (voll)automatisierte Cybersicherheit

Unter den Unternehmen, die KI in der IT-Sicherheit nutzen, wollen sich nur zwölf Prozent darauf beschränken, eine Unterstützung durch die KI zu bekommen und Entscheidungen allein dem Menschen zu überlassen. Dagegen wollen 23 Prozent eine vollautomatische Security, bei der der Mensch eine Eingriffsmöglichkeit hat.

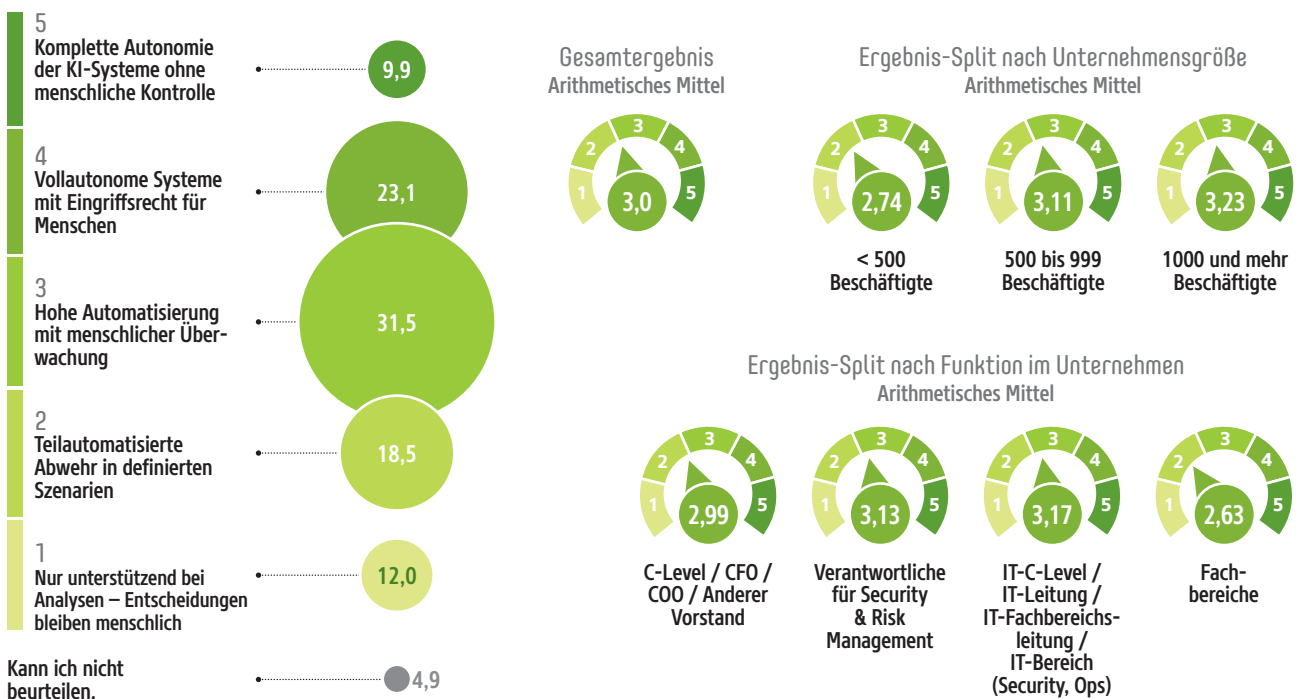
Eine komplette Autonomie für die KI ist das Ziel bei immerhin zehn Prozent der Befragten, wenn es um IT-Sicherheit geht. Hier wäre keine Eingriffsmöglichkeit mehr für den Menschen vorgesehen. Große Unternehmen mit mindestens 1000 Beschäftigten sind noch eher bereit, auf dieses Eingriffsrecht für den Menschen zu verzichten. Hier sind es 17 Prozent der Befragten, die eine vollkommen autonome Security wünschen. Bei kleinen Unternehmen, die oftmals weniger Security-Personal haben, ist diese vollkommene Autonomie in der IT-Sicherheit für KI nur bei fünf Prozent der Befragten das Ziel.

Offensichtlich ist es also eher nicht der Personalmangel, der zu dem Wunsch nach Autonomie für die KI in der Cybersicherheit führt. Betrachtet man die Rolle der Verantwortenden, sind es die Verantwortlichen für Security und Risk, die deutlich weniger zur kompletten Autonomie der KI in der Security tendieren, hier sind es nur sechs Prozent. Dafür ist der Anteil derer, die vollautonome Systeme mit Eingriffsrecht für Menschen wünschen, unter den Verantwortlichen für Risk und Security besonders hoch, es sind hier 28 Prozent der Befragten.

Offensichtlich wünschen sich Security-Verantwortliche eine möglichst weitgehende Entlastung durch autonome Systeme, ohne aber selbst die Kontrolle abgeben zu müssen.

Wie weit sollte der Einsatz von künstlicher Intelligenz in der Cyberabwehr Ihres Unternehmens gehen?

Angaben in Prozent. Basis: n = 324



9

Datensouveränität ist nicht der Hauptfokus digitaler Souveränität

58 Prozent der Befragten sagen, dass Datenlokalität allein keine Rechtssicherheit bringt, denn es kommen die Gesetze jenes Landes zur Anwendung, in dem der Cloud-Service-Provider seinen Unternehmenssitz hat. Nur 20 Prozent meinen, dies sei nichtzutreffend. Gleichzeitig sind die Unternehmen im Bereich Datensouveränität nach eigener Einschätzung weniger reif als bei Technologie und Prozessen.

So stufen nur 44 Prozent der Unternehmen den eigenen Grad an Datensouveränität als hoch oder sehr hoch ein. Bei Operativer Souveränität und Technologischer Souveränität sind es dagegen jeweils 51 Prozent der Befragten, die einen hohen oder sehr hohen Reifegrad in ihrem Unternehmen sehen. Dadurch liegt dann die digitale Souveränität insgesamt bei nur knapp der Hälfte der Unternehmen (49 Prozent der Befragten) auf einem hohen oder sehr hohen Niveau.

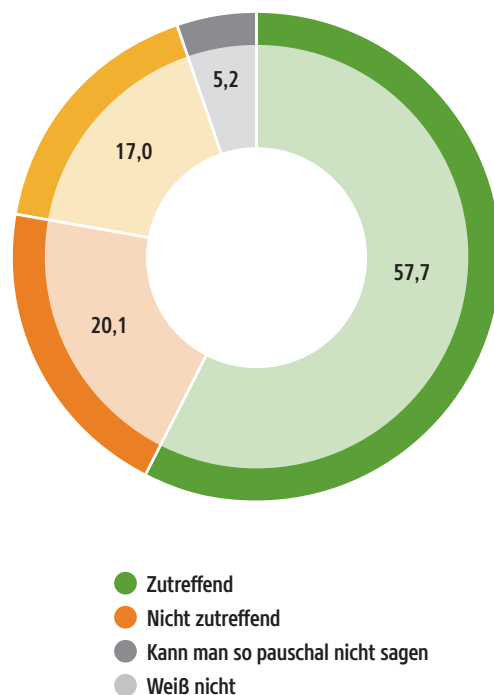
Interessant ist jedoch, dass der Datensouveränität gar nicht der gleich hohe Stellenwert beigemessen wird wie der Operativen Souveränität und der Technologischen Souveränität. Als für ihr Unternehmen essenziell wichtig bis geschäftskritisch stufen 50 Prozent der Befragten die Technologische Souveränität ein, 41 Prozent der Unternehmen sehen die Operative Souveränität als derart wichtig an. Doch nur 39 Prozent erklären, die Datensouveränität sei essenziell wichtig bis geschäftskritisch für ihr Unternehmen.

Datensouveränität wird also im Gegensatz zum Datenschutz, der in vielen Umfragen als führendes Thema identifiziert wird, als weniger zentral gesehen. Ein wichtiger Aspekt, der bedacht werden sollte, wenn über digitale Souveränität diskutiert wird.

Ist die folgende Aussage bezüglich Daten in der Cloud zutreffend oder nicht zutreffend?

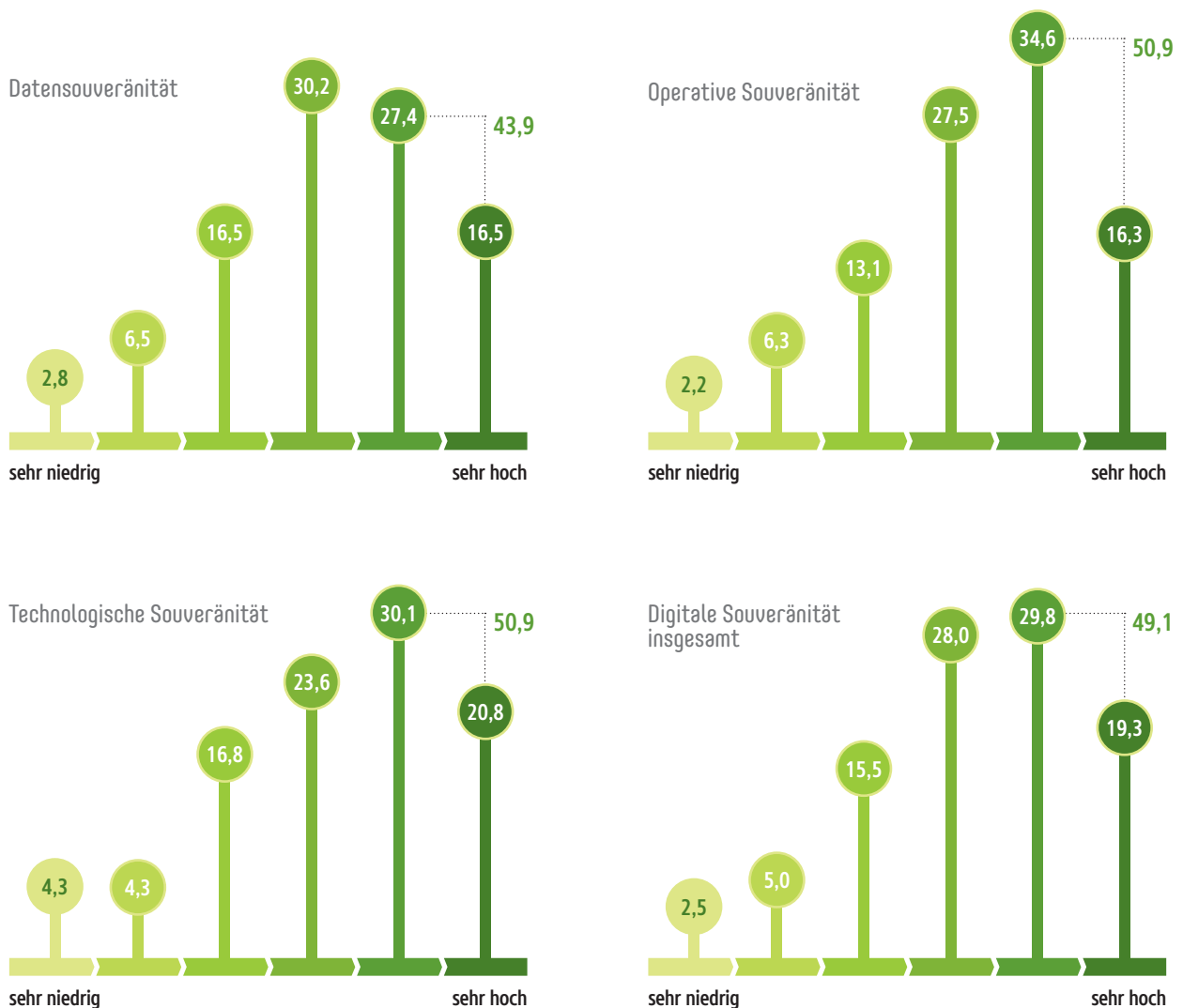
„Datenlokalität allein bringt keine Rechtssicherheit, denn es kommen die Gesetze jenes Landes zur Anwendung, in dem der Cloud-Service-Provider seinen Unternehmenssitz hat.“

Angaben in Prozent. Basis: n = 324



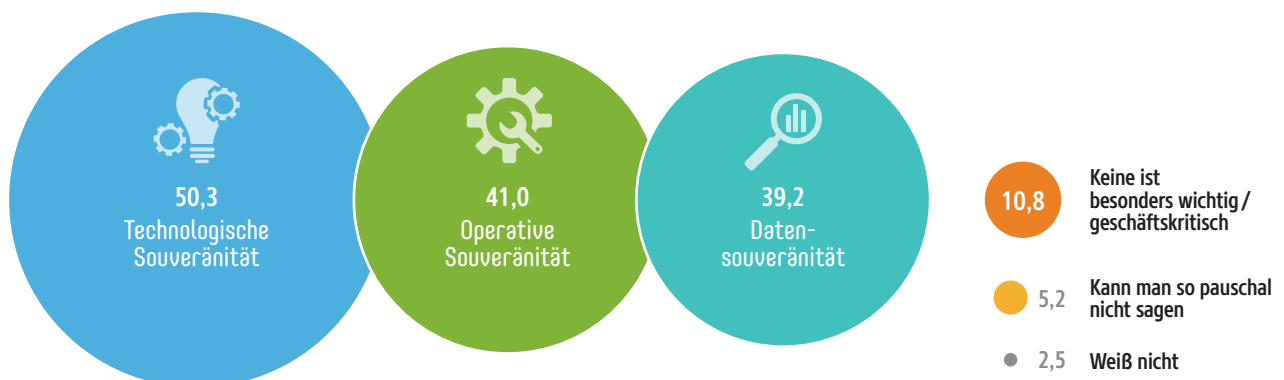
Wie stufen Sie den Grad der digitalen Souveränität Ihres Unternehmens ein?

Angaben in Prozent. Basis: n = 324



Welche Dimensionen der digitalen Souveränität sind für Ihr Unternehmen essenziell wichtig bis geschäftskritisch?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 324



10 Identitätssicherheit steht im Fokus, nicht Ransomware-Schutz

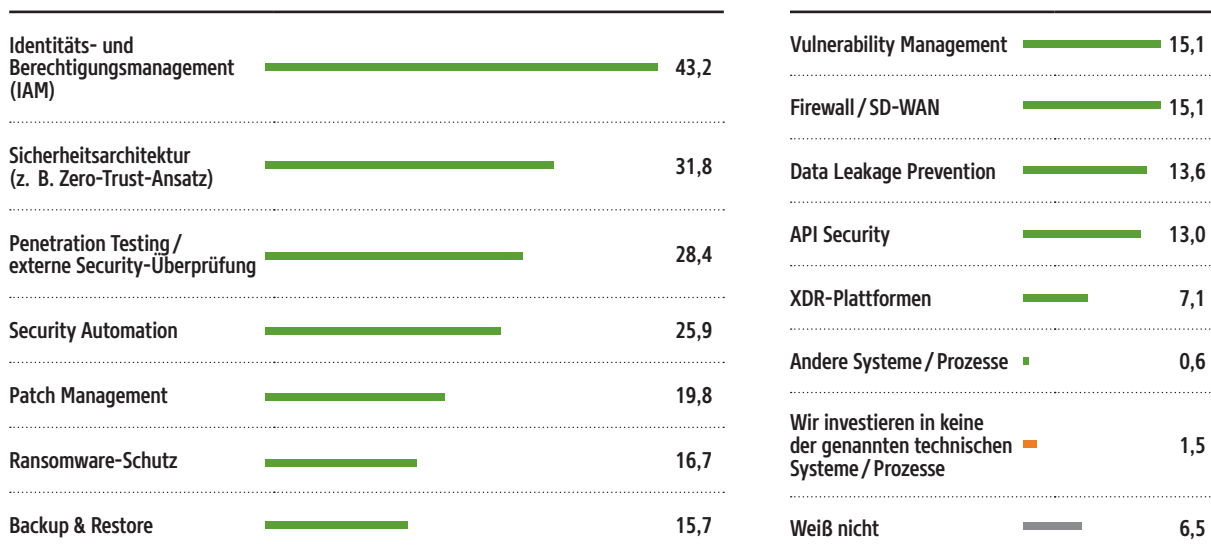
Auch wenn Ransomware die Schlagzeilen füllt, wollen 43 Prozent der Unternehmen in den nächsten Monaten in Identitäts- und Berechtigungsmanagement (IAM) investieren. Spezieller Ransomware-Schutz steht dagegen nur bei 17 Prozent der Befragten in der Investitionsplanung. API-Sicherheit ist sogar nur für 13 Prozent der Unternehmen ein Thema für Investitionen, obwohl dies zum Beispiel zur Absicherung der Lieferkette wichtig ist.

Die Dominanz von Identity and Access Management bei den geplanten Security-Investitionen hängt nicht von der Höhe des Security-Budgets ab. Ob der Anteil des Budgets für Security mehr oder weniger als zehn Prozent des gesamten IT-Budgets beträgt, macht keinen Unterschied.

Besonders häufig nennen die mittelgroßen Unternehmen mit 500 bis 999 Beschäftigten das Identitäts- und Berechtigungsmanagement als geplante Investition, hier sind es 51 Prozent der Befragten. Bei großen Unternehmen mit 1000 Beschäftigten oder mehr liegt dieser Anteil nur bei 39 Prozent. Möglicherweise haben die großen Unternehmen auf diesem Gebiet früher als andere ihre Hausaufgaben auch schon in den zurückliegenden Jahren erledigt.

In welche der folgenden technischen Systeme / Prozesse plant Ihr Unternehmen in den kommenden Monaten zu investieren?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 324

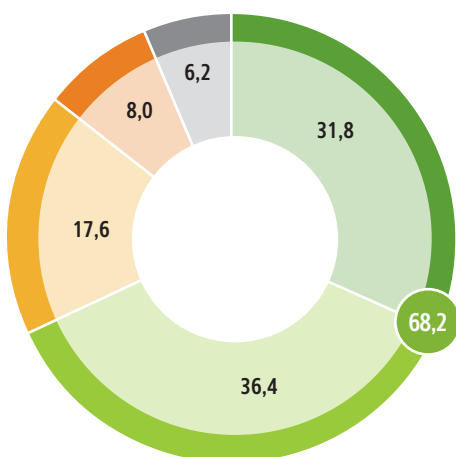


Auf den Plätzen 2 und 3 der geplanten Security-Investitionen liegen Sicherheitsarchitekturen (wie der Zero-Trust-Ansatz) mit 32 Prozent der Nennungen und Penetration Testing / externe Security-Überprüfung mit einem Anteil von 28 Prozent der Befragten.

Nicht so häufig werden Investitionen in XDR-Lösungen (Extended Detection and Response) genannt. Dabei sagen erst 40 Prozent der Befragten, dass sie bereits XDR nutzen. Bei den weitaus häufiger als geplante Investition genannten Sicherheitsarchitekturen wie Zero Trust liegt die Nutzung bereits bei 68 Prozent der Unternehmen, trotzdem wollen dort viele Befragte noch weiter investieren.

Setzt Ihr Unternehmen ein Zero-Trust-Konzept ein?

Angaben in Prozent. Basis: n = 324

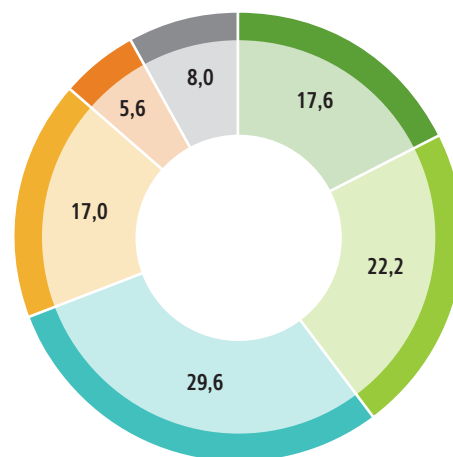


- Ja, schon seit mindestens einem Jahr
- Ja, seit einigen Monaten
- Nein, es ist aber geplant.
- Nein, wir haben keinen Bedarf/Interesse an Zero Trust.
- Weiß nicht

Zero Trust ist ein Sicherheitskonzept, bei dem keinem Gerät, keinem Nutzer und keinem Dienst – weder innerhalb noch außerhalb des Unternehmensnetzes – per se vertraut wird. Sämtliche Anwender und Dienste müssen einzeln authentifiziert werden.

Hat Ihr Unternehmen XDR-Tools oder -Plattformen im Einsatz?

Angaben in Prozent. Basis: n = 324



- XDR-Nutzung seit mehr als einem Jahr
- XDR-Nutzung seit einigen Monaten
- Derzeit Evaluierung von XDR-Lösungen
- Kein Einsatz von XDR binnen Jahresfrist geplant
- Kein Bedarf/Interesse an XDR
- Weiß nicht

XDR (Extended Detection and Response) steht für die erweiterte Erkennung und Reaktion auf Cyberbedrohungen im gesamten Netzwerk. XDR erhöht im Vergleich zu bisherigen Endpoint-Protection-Lösungen (u. a. EDR) die Sichtbarkeit im Netzwerk durch die breitere Analyse von Daten aus der IT-Umgebung und fördert dadurch auch die schnellere Erkennung von Bedrohungen bei abweichendem Verhalten.

Blick in die Zukunft

© stock.adobe.com / envrfx (auch S. 5)

Die inhaltliche Einordnung
der Studienergebnisse –
eine Marktperspektive

NIS2- und DORA-Compliance ist in den Köpfen, muss aber noch in die Systeme

Die meisten Unternehmen haben sich schon mit NIS2 oder DORA befasst, doch die Tragweite der Anforderungen für die Security-Konzeption ist bislang nicht genug im Bewusstsein der Firmen. Cyberrisiken wie unsichere Lieferketten müssen noch Einzug in viele Risikomanagement-Systeme halten. Sonst wird es keine NIS2- oder DORA-Compliance geben.

Von Oliver Schonschek

Ohne Zweifel ist Industriespionage eine ernstzunehmende Cyberbedrohung für die Wirtschaft in Deutschland. Das ist den Unternehmen auch durchaus bewusst. Weniger im Bewusstsein verankert ist aber, wie Industriespionage inzwischen funktioniert.

Cyberangriffe durch Industriespione und andere Kriminelle müssen nicht direkt erfolgen. Sondern sie können indirekt über Geschäftspartner, Lieferanten und Dienstleister stattfinden, wenn dort Schwachstellen bestehen, die sich leicht ausnutzen lassen. Sicherheitslücken in der Lieferkette bedrohen alle Glieder der Supply Chain, denn wird zum Beispiel die digitale Identität eines Lieferanten gestohlen und missbraucht, können die Angreifenden die Vertrauensstellung des Zulieferers ausnutzen und so einfacher Zugang zu den Systemen des Auftraggebers bekommen.

Dieser Angriffsweg wird immer häufiger beschritten, doch nur jedes dritte Unternehmen aus der Umfrage sieht die Lieferkettenrisiken entsprechend kritisch. Dabei nennen die umzusetzende NIS2-Richtlinie der EU und das entsprechende Umsetzungsgesetz in Deutschland explizit den notwendigen Schutz der Lieferkette.

Noch ist aber die Umsetzung von NIS2 bei weitem nicht abgeschlossen. Zehn Prozent der Befragten wissen noch nicht einmal, ob und inwieweit sie betroffen sind. Die Unternehmen, die NIS2 umsetzen, sehen oftmals eine hohe Komplexität und große Aufwände dabei. Gleichzeitig sind es immerhin 28 Prozent der Unternehmen, die weder direkt noch indirekt unter NIS2 fallen, aber trotzdem bereits die Vorgaben der Cybersicherheitsrichtlinie umgesetzt haben.

Offensichtlich ist NIS2 und in den Finanzbereichen entsprechend DORA ein wichtiges Thema, das die IT-Sicherheit weitläufig beschäftigt. Sogar der Einkaufsbereich regulierter Unternehmen hat auf NIS2 reagiert und zum Beispiel die Zahl der Lieferanten erhöht, wohl um Abhängigkeiten zu reduzieren. So meinen nur vier Prozent der Befragten, die eigene Lieferkette sei von den NIS2-Vorgaben nicht betroffen.

Die notwendigen Schlüsse für die IT-Sicherheit werden aber nicht immer gezogen, wie zum Beispiel die eher geringe Einstufung der Cyberrisiken aus der Lieferkette zeigt. Auch in der OT-Sicherheit, also dem Schutz für Betriebstechnologie, besteht noch

deutlicher Handlungsbedarf. Gerade veraltete und proprietäre OT-Systeme werden als eine große Herausforderung gesehen, wenn es um die NIS2-Umsetzung geht.

Bei der DORA-Verordnung ist die Anwendung bereits seit Januar 2025 verpflichtend, aber nur 27 Prozent der befragten Unternehmen aus dem Finanzbereich sagen, dass sie DORA bereits vollständig umgesetzt haben. Die Implementierung von DORA fällt vielen der betroffenen Unternehmen nicht leicht, ähnlich wie bei NIS2. Komplexe Anforderungen und hohe Aufwände führen aber nicht nur zu Verzögerungen.

Eine große Zahl an Unternehmen scheint sich in den Anforderungen von NIS2 und DORA zu verlieren, wobei der Blick auf so kritische Bereiche wie Sicherheitslücken in der Lieferkette verstellt wird. Aufklärung und Schulungen würden Not tun, doch wie die Umfrage zeigt, ist NIS2 trotz der notwendigen Umsetzung nicht das Schulungsthema Nummer eins in der Security. Selbst die verpflichtende NIS2-Schulung für die Geschäftsführung bieten erst 44 Prozent entsprechend an, weitere 37 Prozent der Befragten sehen dies noch als freiwillige Schulungen an.

Auch wenn NIS2 und DORA viele Schlagzeilen füllen und in den Unternehmen durchaus präsent sind, ist die tatsächliche Umsetzung oftmals noch lückenhaft. Eine Ursache dafür kann darin gesehen werden, dass IT-Risiken und Risiken aus NIS2 und DORA häufig noch nicht Teil des betrieblichen Risikomanagements geworden sind. Projekte zu NIS2 und DORA bestehen oft separat, mit einem eigenen Budget. Ziel müsste es aber sein, dass die Cyberrisiken aus NIS2 und DORA als Teil der Geschäftsrisiken erkannt und behandelt werden. In diesem Kontext sind auch die IT-Sicherheitsrisiken, die im Zusammenhang mit der Lieferkette entstehen, ein relevantes Thema.

Nur dann kann eine Implementierung von NIS2 und DORA wirklich nachhaltig und umfassend gelingen, und nur dann können diese Compliance-Vorgaben wirklich zur erforderlichen Steigerung der Cyberresilienz beitragen. Man könnte auch sagen: Wer Industriespionage fürchtet, muss seine Resilienz steigern, denn diese Angriffe finden fortlaufend statt. Wer aber die Cyberresilienz erhöhen will, tut gut daran, NIS2 und DORA umfassend zu implementieren. Sonst gibt es keine NIS2- oder DORA-Compliance, dafür aber womöglich die nächste, erfolgreiche Cyberattacke über die Lieferkette.

CIO-Agenda 2026

**Daten zur allgemeinen Einschätzung
der Marktlage**

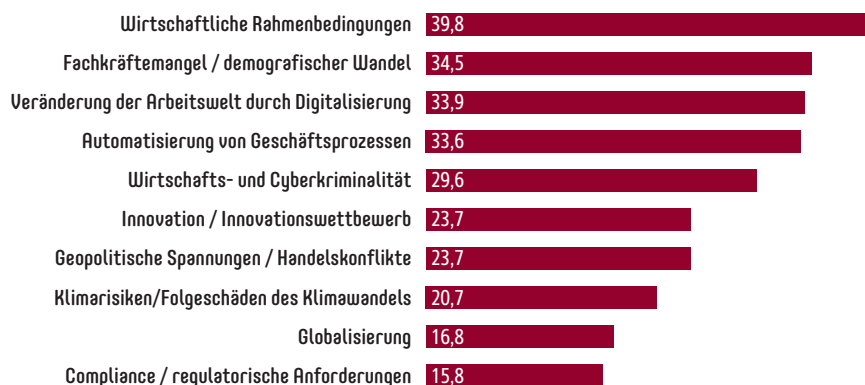
Exklusive Einblicke:
Wie IT-Verantwortliche das Business
in Gegenwart und Zukunft gestalten

2026 – Ein weiteres Jahr der Herausforderungen

Die Herausforderungen

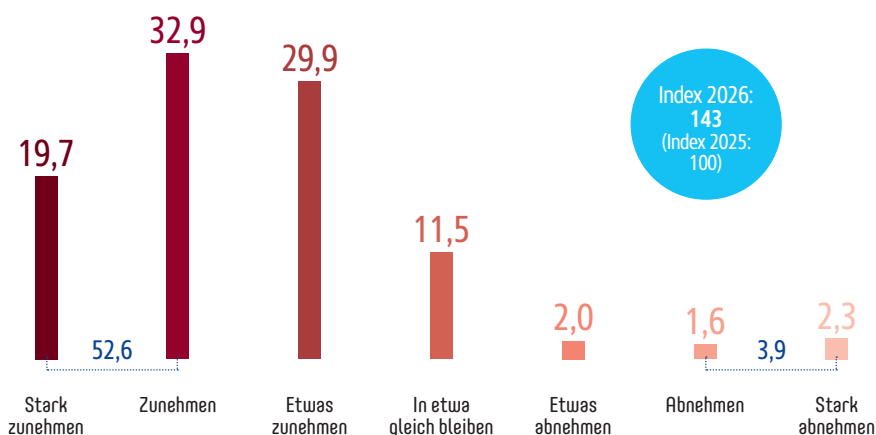
Welcher Art sind die Herausforderungen, vor denen Ihr Unternehmen 2026 vorrangig stehen wird?

(Mehrfachnennungen möglich)



Das Gesamtmaß der Herausforderungen

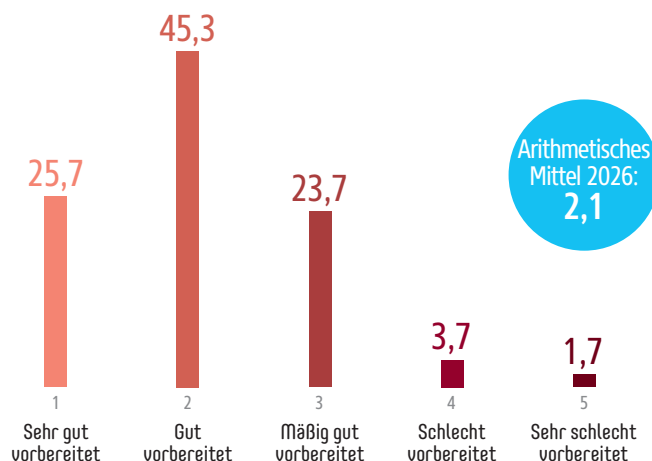
Wie wird sich das Gesamtmaß der Herausforderungen für Ihr Unternehmen im Jahr 2026 im Vergleich zu 2025 voraussichtlich entwickeln?



Grad der Vorbereitung

Wie gut ist Ihr Unternehmen auf diese Herausforderungen vorbereitet?

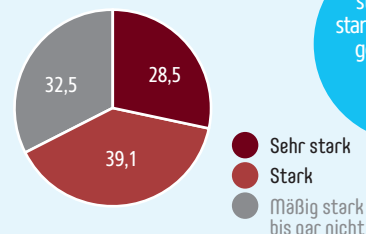
(Angaben auf einer Skala von 1 bis 5)



Generative KI

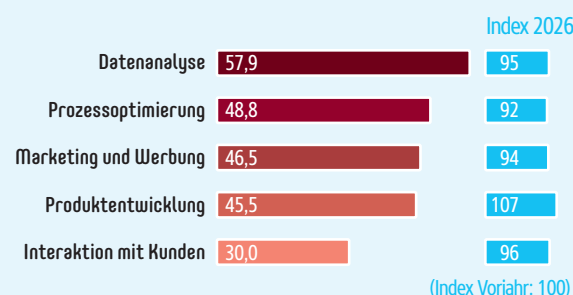
Nutzungsgrad

Wie stark wird generative KI in Ihrem Unternehmen genutzt?



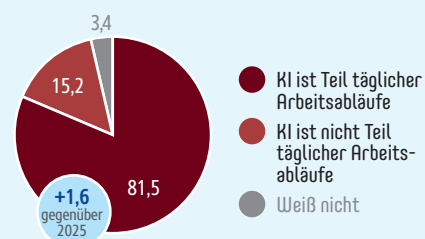
Anwendungsbereiche

In welchen Bereichen wird generative KI in Ihrem Unternehmen genutzt?



KI-Alltag

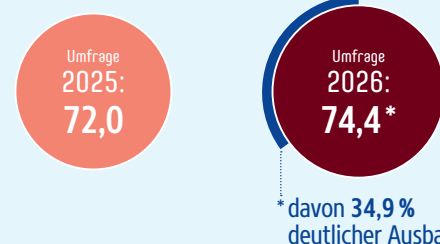
Ist generative KI Teil Ihrer täglichen Arbeitsabläufe, indem Sie entsprechende Tools aufrufen, Chatbots einsetzen oder auch KI integrativer Teil der IT-Systeme ist, mit denen Sie regelmäßig arbeiten?



Nutzungspläne

Welche Pläne hat Ihr Unternehmen bezüglich der Nutzung generativer KI in den kommenden 2 bis 3 Jahren?

Ausbau der Nutzung



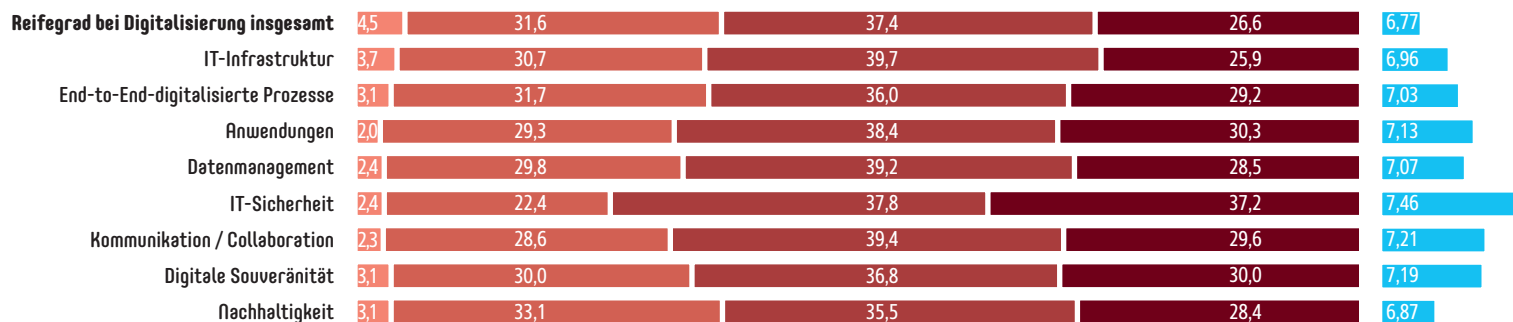
Digitale Transformation

Digitaler Reifegrad

Stellen Sie sich bitte die digitale Transformation als eine Wegstrecke von 0 bis 10 vor.
An welchem Punkt der Wegstrecke verorten Sie derzeit Ihr Unternehmen?

Bewertung auf einer Skala von 0 (In Sachen Digitalisierung stehen wir noch völlig am Anfang) bis 10 (Wir sind allerbestens für die digitale Zukunft aufgestellt)

Arithmetisches
Mittel



Darstellung auf einer Wegstrecke von 1 bis 10:

0 bis 1

2 bis 6

7 bis 8

9 bis 10

Technology Adoption

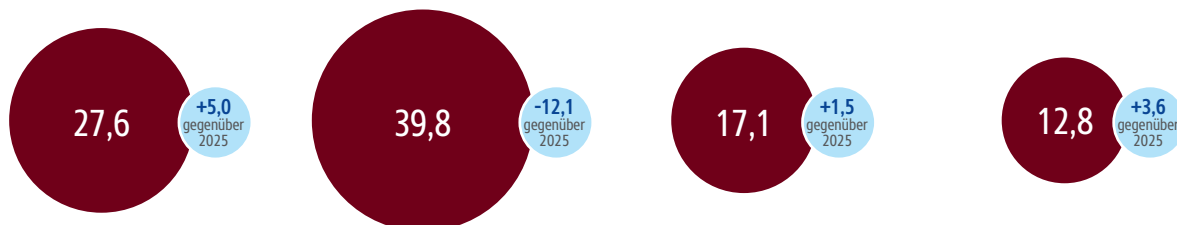
Welche der folgenden Beschreibungen charakterisiert Ihr Unternehmen am besten?

Innovators & Early Adopters
Unser Unternehmen ist ein Vorreiter der digitalen Transformation.

Early Majority
Unserem Unternehmen fällt es eher leicht, vom Wettbewerb gestartete Digitalisierungsinitiativen zu übernehmen bzw. sich diesen anzupassen.

Late Majority
Unserem Unternehmen fällt es eher schwer, vom Wettbewerb gestartete Digitalisierungsinitiativen zu übernehmen bzw. sich diesen anzupassen.

Laggards
Unser Unternehmen hat den Digitalisierungsinitiativen des Wettbewerbs nichts entgegensetzen.



Strategische Partnerschaften im digitalen Wandel

Mit welchen externen Partnern arbeiten Sie heute schon zusammen, um die Zukunftsfähigkeit Ihres Unternehmens zu sichern, Digitalisierungsprojekte umzusetzen oder neue Fachkräfte zu gewinnen? Mit wem planen Sie künftige Allianzen und strategische Partnerschaften?



CIO-Agenda 2026

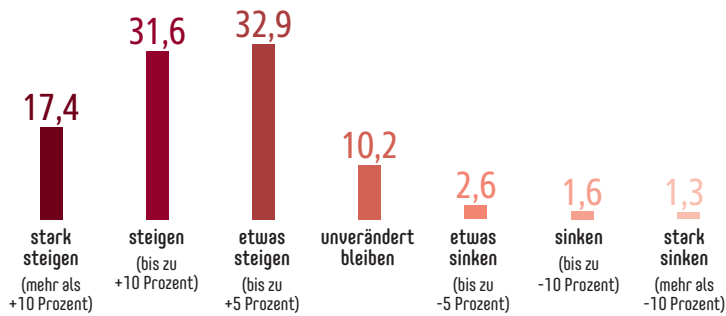
Alle Angaben in Prozent

Investitionen

IT-Budgets 2026

Wie wird sich das IT-Gesamtbudget Ihres Unternehmens im Jahr 2026 im Vergleich zu 2025 entwickeln?

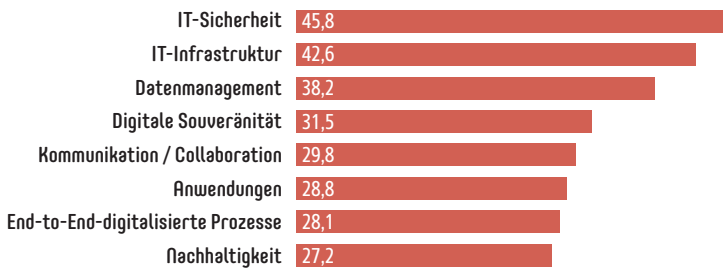
Das IT-Budget 2026 wird ...



Investitionsschwerpunkte in den nächsten drei Jahren

In welche der folgenden (IT-/Technologie-)Bereiche plant Ihr Unternehmen in den kommenden drei Jahren substantiell zu investieren?

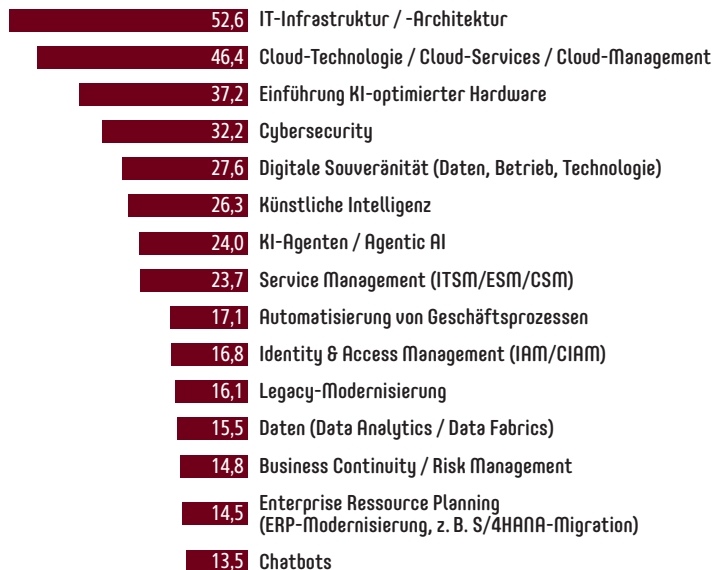
(Mehrfachnennungen möglich)



IT-Investitionsfelder in den nächsten drei Jahren

In welche der folgenden IT-Themen / Technologien plant Ihr Unternehmen in den kommenden drei Jahren zu investieren?

(Mehrfachnennungen möglich, Top-15-Antworten)



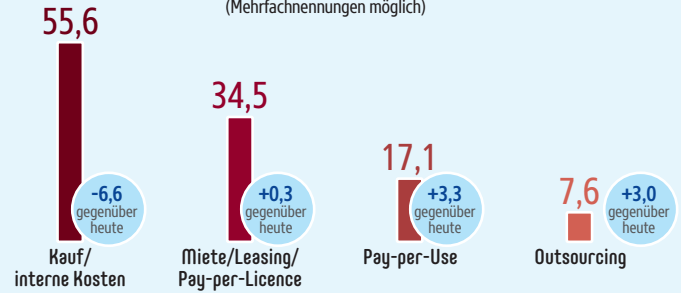
Beschaffungsprozesse

Wie sieht der IT-Beschaffungsprozess Ihres Unternehmens bei Hardware, Software und Services heute und zukünftig aus? Welche Facetten von Kauf über Miete bis hin zu Outsourcing umfasst der IT-Beschaffungsprozess jeweils?

Zukünftige Beschaffung von ...

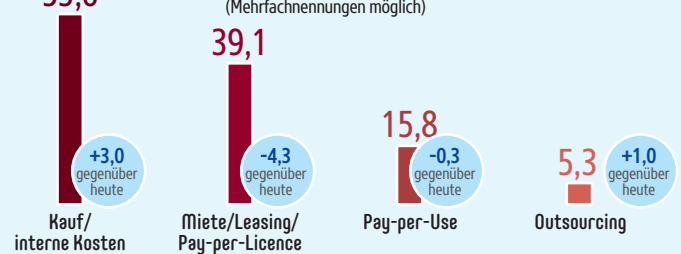
Hardware

(Mehrfachnennungen möglich)



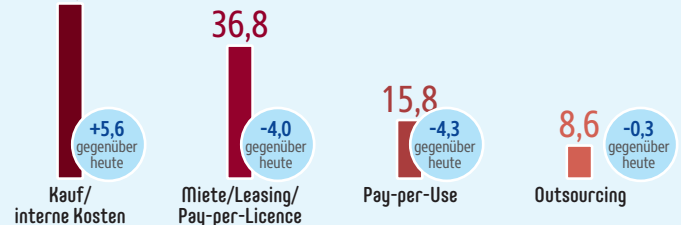
Software

(Mehrfachnennungen möglich)



Services

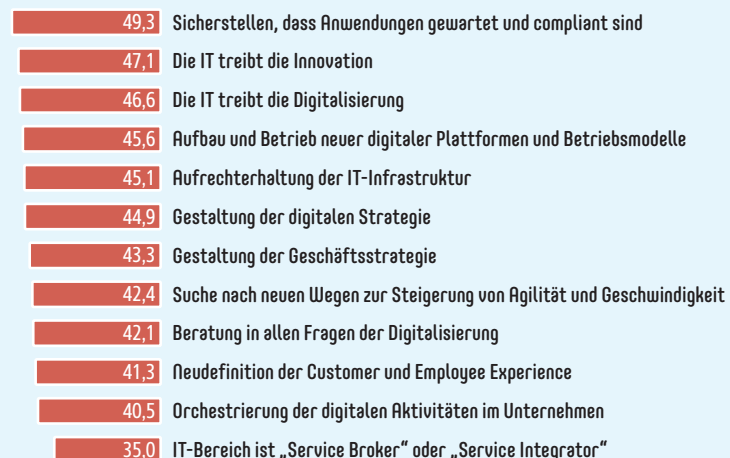
(Mehrfachnennungen möglich)



Die Rolle des CIO in fünf Jahren

Wie wird sich Ihrer Meinung nach der Fokus des CIOs / IT-Leiters bzw. IT-Bereichs in fünf Jahren verändert haben?

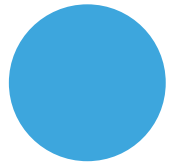
Verstärkter Fokus auf:



Die Studienpartner stellen sich vor

plussserver,
T-Systems

*Die Vorstellung unserer Studienpartner wird von den beteiligten Unternehmen selbst erstellt.
Für die Porträts ist stets der jeweilige Studienpartner verantwortlich.*



Nicht nur die Mindeststandards erfüllen:

Resilienz entsteht, wenn Cloud und Security zusammen- gedacht werden

Chief Commercial Officer Peter Höhn über den Aufbau resilienter IT-Infrastrukturen, die Rolle europäischer Cloud-Anbieter und die Bedeutung der Partnerschaft mit dem Security-Spezialisten Cosanta.

Herr Höhn, viele Unternehmen stehen derzeit unter Druck, ihre IT-Strukturen widerstandsfähiger zu gestalten. Was verstehen Sie unter digitaler Resilienz?

Resiliente Unternehmen sind in der Lage, ihre Systeme und Daten jederzeit anzupassen, zu schützen und wiederherzustellen. Unabhängig davon, welche externen Faktoren eintreten. Dazu gehört technische Stabilität ebenso wie organisatorische und rechtliche Handlungsfähigkeit.

Welche Rolle spielt dabei die Herkunft und Architektur der IT-Infrastruktur?

Wenn sensible Daten in globalen Cloud-Ökosystemen liegen, müssen Unternehmen genau verstehen, wer Zugriff hat und welche Rechtsräume gelten. Europäische Anbieter wie plusserver bieten hier eine Alternative mit Datenhaltung und Betrieb nach europäischen Standards, Transparenz über alle Ebenen der Wertschöpfung und Compliance-by-Design.

plusserver hat sich früh strategisch breiter aufgestellt und investiert in Security-Kompetenz. Welche Bedeutung hat dabei die Partnerschaft mit Cosanta?

Resilienz entsteht, wenn Cloud und Security zusammengedacht werden. Gemeinsam mit Cosanta bündeln wir unsere Stärken in souveräner Infrastruktur und Cybersecurity. Für unsere Kunden entsteht dadurch ein ganzheitlicher Schutzansatz, der sich flexibel an neue regulatorische und technologische Anforderungen anpassen lässt.

Wie sollten sich Unternehmen 2026 aufstellen, um NIS2 und DORA nachhaltig zu erfüllen?

Wichtig ist, das Thema nicht als reine Compliance-Übung zu sehen. Wer heute in Transparenz, europäische Infrastruktur und Security-Kompetenz investiert, stärkt seine Zukunftsfähigkeit. Ziel sollte es sein, nicht nur die gesetzlichen Mindeststandards zu erfüllen, sondern ein belastbares Fundament für sichere digitale Geschäftsmodelle zu schaffen.

Ein Ökosystem für digitale Souveränität und Sicherheit

Die plusserver GmbH ist ein führender deutscher Cloud-Anbieter. Mit eigenen BSI-C5-testierten und DSGVO-konformen Rechenzentren in Deutschland erfüllt das Unternehmen höchste Sicherheits- und Zertifizierungsstandards. Gemeinsam mit der Cosanta GmbH, einem eigenständigen Security-Spezialisten innerhalb der plusserver-Gruppe, entsteht ein starkes Ökosystem für digitale Resilienz – von der souveränen Cloud-Infrastruktur bis zu zentralen Security-Prozessen, die regulatorischen Anforderungen wie NIS2 und DORA gerecht werden.



Resilienz ist keine isolierte Lösung, sondern ein Zusammenspiel aus souveräner Infrastruktur, Security-Kompetenz und klarer Verantwortung über Daten und Prozesse.

– **Peter Höhn,**
Chief Commercial Officer, plusserver



plusserver GmbH
Welserstraße 14, 51149 Köln
Telefon: +49 (0)221 8282 8550
E-Mail: beratung@plusserver.com
www.plusserver.com

WE SECURE YOUR SUCCESS

Als zuverlässiger Security-Partner schützen wir, was Unternehmen erfolgreich macht: ihre Daten, ihre Systeme und ihre digitale Zukunft – seit 25 Jahren.

Mit Standorten in 26 Ländern und mehr als 26.000 Mitarbeitenden weltweit sowie einem Jahresumsatz von über 4 Milliarden Euro ist T-Systems einer der führenden europäischen Dienstleister für Informationstechnologie und Digitalisierungslösungen. *

Der Schutz der digitalen Handlungsfähigkeit von Unternehmen, Behörden und kritischen Infrastrukturen steht für uns an oberster Stelle. Um dies umsetzen zu können, verbinden wir modernste Cybersecurity-Architekturen mit der operativen Stärke unserer 15 globalen Security Operations Centers.

Unsere Lösungen decken den gesamten Sicherheitslebenszyklus ab: von der Analyse über die Beratung und Implementierung bis hin zum 24/7-Betrieb komplexer Security-Infrastrukturen. Mit einem Zero-Trust-Ansatz, cloudsouveränen Architekturen und KI-ge-

stützter Bedrohungserkennung stellen wir sicher, dass digitale Prozesse zuverlässig geschützt bleiben und ihre Sicherheit jederzeit kontrollierbar und nachvollziehbar ist.

Unternehmen profitieren von unserer langjährigen Erfahrung: Wir erkennen Bedrohungen frühzeitig, wehren Angriffe automatisiert ab und schützen kritische Assets konsequent. Durch Managed Cyber Defense, starke Identitäts- und Zugriffsmechanismen, moderne Netzwerksicherheitslösungen sowie OT- und Cloud Security schaffen wir einen robusten Schutzschild für jede Branche und jede Unternehmensgröße.

* Stand Mai 2025



Dabei setzen wir auf Transparenz und Partnerschaft. Wir entlasten Organisationen, schaffen Klarheit in komplexen Sicherheitslandschaften und unterstützen dabei, Compliance-Vorgaben, Datenschutzanforderungen und regulatorische Auflagen zuverlässig zu erfüllen. Unser Anspruch ist es, Risiken zu minimieren, ohne Innovationen zu bremsen – denn echte Sicherheit ermöglicht unternehmerische Freiheit.

Mit unserer langjährigen Erfahrung, führenden Sicherheitsstandards und einem starken europäischen Footprint sorgen wir für Zukunftssicherheit in einer zunehmend vernetzten und zugleich unsicheren, geopolitisch volatilen Welt. Wir machen Cybersecurity planbar, skalierbar sowie messbar und stärken damit die digitale Resilienz unserer Kunden nachhaltig.

Sicherheit stärkt Resilienz.
Unser Auftrag ist es, digitale Risiken beherrschbar zu machen, um den Raum für erfolgreiche Innovationen und Digitalisierung zu schaffen.

Thomas Masicek

SVP Cyber Security T-Systems International

T-Systems International GmbH
Hahnstraße 43d, 60528 Frankfurt am Main
Telefon: 0800 33 09030
E-Mail: cyber.security@t-systems.com
www.t-systems.com/de/de/security

Studiendesign

Alle wissenswerten Informationen
zu Aufbau, Methodik
und Stichprobe der Studie

Studienpartner

Gold-Partner:

plusserver GmbH

Welserstraße 14
51149 Köln
Telefon: +49 221 8282 8550
E-Mail: beratung@plusserver.com
www.plusserver.com

T-Systems International GmbH

Hahnstraße 43d
60528 Frankfurt am Main
Telefon: 0800 33 09030
E-Mail: cyber.security@t-systems.com
www.t-systems.com/de/de/security

Partner:

baramundi software GmbH

Forschungsallee 3
86159 Augsburg
Telefon: +49 821 56708 380
E-Mail: request@baramundi.com
www.baramundi.com

Gesamtstudienleitung

Matthias Teichmann

Director Research
Custom Research Team
Telefon: +49 172 8637540
matthias.teichmann@foundryco.com

Projektmanagement

Armin Rozsa

Research Manager
Custom Research Team
Telefon: +49 89 36086 184
armin.rozsa@foundryco.com

Sales-Team

Daniela Häring

Account Managerin, Sales
Telefon: +49 152 90023492
daniela.haering@foundryco.com

Christine Nestler

Director, Sales
Telefon: +49 172 8111821
christine.nestler@foundryco.com

Ami Pepic

Senior Sales Managerin
Telefon: +49 173 5703524
ami.pepic@foundryco.com

Impressum

Studienkonzept/
Fragebogenentwicklung:
Matthias Teichmann

Endredaktion/
CvD Studienberichtsband:
Matthias Teichmann

Analysen / Kommentierungen:
Oliver Schonschek, München

Kommentierungen
CIO-Agenda 2026:
Matthias Teichmann

Hosting / Koordination
Feldarbeit:
Armin Rozsa

Artdirector &
Grafik CIO-Agenda 2026:
Daniela Petrini, Reutte

Grafik:
Patrick Birnbreier, München

Umschlaggestaltung unter
Verwendung einer Illustration
von © shutterstock.com/
Riefki Roediyanto

Lektorat:
Elke Reinhold, München

Ansprechpartner:
Matthias Teichmann
matthias.teichmann@foundryco.com

Herausgeber:

FoundryCo, Inc.

Anschrift:
IDG Tech Media GmbH
Georg-Brauchle-Ring 23
80992 München
Telefon: +49 89 36086-0
Fax: +49 89 36086 118

Vertretungsberechtigter:
Maria Savvidou, Geschäftsführerin

Registergericht:
Amtsgericht München, HRB 99110

Umsatzsteueridentifikationsnummer:
DE 811 257 834

Weitere Informationen unter:
www.foundryco.com

Studiensteckbrief

Herausgeber	CIO, CSO und COMPUTERWOCHE
Studienpartner	Gold-Partner: plusserver GmbH T-Systems International GmbH Partner: baramundi software GmbH
Grundgesamtheiten	Oberste (IT-)Verantwortliche in Unternehmen der DACH-Region: Beteiligte an strategischen (IT-)Entscheidungsprozessen im C-Level-Bereich und in den Fachbereichen (LoBs); Entscheidungsbefugte sowie Experten und Expertinnen aus dem IT-(Security-)Bereich
Teilnehmergenerierung	Persönliche E-Mail-Einladung über die exklusive Unternehmens- datenbank von CIO, CSO und COMPUTERWOCHE sowie – zur Erfüllung von Quotenvorgaben – über externe Online-Access-Panels
Gesamtstichprobe	324 abgeschlossene und qualifizierte Interviews
Untersuchungszeitraum	17. November bis 06. Dezember 2025
Methode	Online-Umfrage (CAWI)
Fragebogenentwicklung und Durchführung	Custom Research Team von CIO, CSO und COMPUTERWOCHE in Abstimmung mit den Studienpartnern

Stichprobenstatistik

Branchenverteilung*

Land- und Forstwirtschaft, Fischerei, Bergbau.....	7,4 %
Energie- und Wasserversorgung.....	6,5 %
Chemisch-pharmazeutische Industrie, Life Science	7,4 %
Medizin- und Labortechnik.....	4,9 %
Metallerzeugende und -verarbeitende Industrie	8,3 %
Maschinen- und Anlagenbau	9,9 %
Automobilindustrie und Zulieferer	7,7 %
Herstellung von elektrotechnischen Gütern, IT-Industrie	26,2 %
Konsumgüter-, Nahrungs- und Genussmittelindustrie.....	7,7 %
Medien, Papier- und Druckgewerbe.....	4,6 %
Baugewerbe, Handwerk	6,2 %
Groß- und Einzelhandel (inkl. Onlinehandel).....	14,2 %
Banken und Versicherungen.....	11,7 %
Transport, Logistik und Verkehr.....	9,3 %
Dienstleistungen für Unternehmen.....	17,0 %
Hotel- und Gastgewerbe, Tourismus.....	8,0 %
Öffentliche Verwaltung, Gebietskörperschaften, Sozialversicherung	7,7 %
Schule, Universität, Hochschule	3,7 %
Gesundheits- und Sozialwesen	3,7 %
Andere Branchengruppe	4,0 %

Unternehmensgröße deutschlandweit

Weniger als 100 Beschäftigte.....	9,3 %
100 bis 249 Beschäftigte	16,4 %
250 bis 499 Beschäftigte	14,8 %
500 bis 999 Beschäftigte	25,3 %
1000 bis 9999 Beschäftigte	24,7 %
10.000 Beschäftigte und mehr	9,6 %

Umsatzklasse deutschlandweit

Weniger als 100 Millionen Euro	21,0 %
100 Millionen bis unter 1 Milliarde Euro	38,0 %
1 bis unter 2 Milliarden Euro	19,1 %
2 bis unter 5 Milliarden Euro	12,7 %
5 Milliarden Euro und mehr	9,3 %

Jährliche Aufwendungen in IT-Systeme

Weniger als 1 Million Euro.....	18,2 %
1 bis unter 10 Millionen Euro	40,7 %
10 bis unter 100 Millionen Euro.....	30,6 %
100 Millionen Euro und mehr	10,5 %

* Mehrfachnennungen möglich

Das Studienkonzept

Die Multi-Client-Studien von CIO, CSO und COMPUTERWOCHE sind mehr als nur Befragungen von C-Level-Verantwortlichen und IT-Fachleuten. Hinter den Marktforschungsprojekten steht ein nachhaltiges Studienkonzept, das auf eine Laufzeit von mindestens sechs Monaten ausgelegt ist.

Die Veranstaltung der initialen redaktionellen Round Tables, moderiert von leitenden Redakteuren und Redakteurinnen von CIO, CSO und COMPUTERWOCHE, steht zu Beginn eines jeden Studienprojekts.

Über den Verlauf der Round-Table-Veranstaltungen wird ausführlich berichtet, und die Themen, die den Branchenfachleuten besonders „auf den Nägeln brennen“, werden auch bei der Entwicklung des Studienfragebogens mitberücksichtigt. Die Unternehmen, die das Projekt als Partner begleiten, können eigene Ideen und Fragestellungen einbringen.

Etwa drei Monate nach der methodischen und inhaltlichen Ausgestaltung der Studie liegen die zentralen Ergebnisse in Form eines hochwertigen Survey Reports vor. Die Studienergebnisse werden auf Messen und Events, wie der Hannover Messe, dmexco oder it-sa, präsentiert, zum Teil in Form von Podiumsdiskussionen, bei denen sich die Studienpartner einem interessierten Fachpublikum stellen können.

Begleitet wird das gesamte Studienprojekt durch kontinuierliche Berichterstattung von CIO, CSO und COMPUTERWOCHE, zum Thema im Allgemeinen und zur Studie im Speziellen. Fachwissen und Kompetenz unserer Autoren und Autorinnen sowie unseres redaktionellen Teams tragen maßgeblich dazu bei, dass die Ergebnisse der Multi-Client-Studien richtig eingeordnet werden können. Berichtet und kommentiert wird auf allen modernen Medienkanälen; Infografiken, Bildergalerien und Video-Interviews tragen dazu bei, dass die Studien auf großes Interesse stoßen.

Der Autor dieser Studie



Oliver Schonschek
freier Analyst und Fachjournalist

Round-Table-Moderation



Jens Dose
Jens Dose ist Redakteur des CIO Magazins. Neben den Kernthemen rund um CIOs und ihre Projekte beschäftigt er sich auch mit der Rolle des CISO und dessen Aufgabengebiet.



Julia Mutzbauer
Julia Mutzbauer ist als Redakteurin für die Medienmarke CSO zuständig, dort vor allem für die inhaltliche Ausrichtung des Onlinemagazins. Für die tägliche Berichterstattung beschäftigt sie sich mit allen Themen rund um Cybersicherheit. Zudem pflegt sie das CSO-LinkedIn-Netzwerk.



Oliver Schonschek
Oliver Schonschek ist freier Analyst und Fachjournalist und schreibt für führende Fachmedien über IT, Sicherheit und Datenschutz, darunter COMPUTERWOCHE und CIO. Er ist Herausgeber und Autor mehrerer Fachbücher und wurde in den USA mehrfach als Influencer und Media Leader für Technologien wie Blockchain, KI, VR/AR und Mobile Computing ausgezeichnet.

Protokolle

Lena Bertler, München
Richard Ruf, München
Florian Stocker, München

Unsere Studienreihe



Folgen Sie uns auf LinkedIn:
<https://www.linkedin.com/showcase/research-services-germany>



plusseryer

T Systems

 baramundi