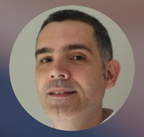
NIS2: Was ist Ihre Deadline?



Matthew Wilkins
Research Director,
European Services

Milan Kalal
Senior Research Manager,
European Services

Richard Thurston
Research Manager,
European Security Services

Dominique Bindels
Consulting Manager,
Custom Solutions Europa

In diesem InfoBrief

Die NIS2-Richtlinie weitet den Anwendungsbereich ihrer Vorgängerin erheblich aus, indem sie strengere Anforderungen für mehr Sektoren vorschreibt und das Risikomanagement ganz oben auf die Tagesordnung der CEOs setzt. Trotz des hohen allgemeinen Bewusstseins sind die Detailkenntnisse über NIS2 immer noch begrenzt, was zu langsamen Fortschritten und mangelndem Engagement des Vorstandes führt. Europäische Unternehmen sehen sich mit Bereitschaftslücken und sektorübergreifenden Herausforderungen konfrontiert, die durch politische Unterschiede und menschliche Faktoren noch verschärft werden. Die Richtlinie fordert einen kulturellen Wandel und betont die oft vernachlässigten Auswirkungen auf die Kompetenzen. Infolgedessen steigt die Nachfrage nach externen Partnern, wobei Dienstleister die bevorzugte Wahl sind, um die Einhaltung der Vorschriften zu gewährleisten. Die Umsetzung wirksamer Sicherheitsstrategien und die Zustimmung der Interessengruppen sind für ein erfolgreiches Engagement unerlässlich.

Dieser von Insight gesponserte InfoBrief untersucht das Bewusstsein, den Status und die Herausforderungen europäischer Unternehmen in Bezug auf die Cybersicherheitsrichtlinie NIS2 der Europäischen Union. Gemeinsam mit Insight bewertet IDC das Compliance-Bewusstsein und die Compliance-Bereitschaft von Unternehmen, den Einfluss menschlicher Faktoren und die Rolle, die externe Partner bei der Unterstützung von Unternehmen auf dem Weg zur NIS2-Konformität spielen können.

IDC
InfoBrief, gesponsert von Insight
Oktober 2024 | IDC #EUR252648424

Inhaltsverzeichnis

KLICKEN SIE UNTEN, UM DIE EINZELNEN ABSCHNITTE DIESES DOKUMENTS AUFZURUFEN.

NIS2: Was, wann und wo?

EU-Richtlinie zur Netz- und Informationssicherheit II (NIS2)

Was?

- Ziele: Stärkung des Risikomanagements und der Widerstandsfähigkeit im Bereich der Cybersicherheit kritischer Infrastrukturen in der Europäischen Union (EU)
- Ersetzt und modernisiert die bestehende NIS1-Richtlinie
- Gilt jetzt für Unternehmen mit mehr als 50 Mitarbeitern oder einem Jahresumsatz von mehr als 10 Mio. €.
- Erweiterung des Anwendungsbereichs von 7 auf 18 Sektoren
- Gilt für Einrichtungen, die bestimmte kritische Dienste oder grundlegende Infrastrukturen bereitstellen
- Definiert zwei Kategorien von Entitäten: Unverzichtbar und wichtig

Wann?

Update Oktober 2024: Die Umsetzung auf nationaler Ebene verzögert sich in den meisten EU-Mitgliedstaaten und könnte erst 2025 in Kraft treten.

Juni 2016

Die NIS1-Richtlinie wird angenommen.

Januar 2023

Die NIS2-Richtlinie tritt auf EU-Ebene in Kraft.

17. Oktober 2024

Die Mitgliedsstaaten müssen die NIS2-Richtlinie in nationales Recht umsetzen.

Wo?

- Die Richtlinie wird für Unternehmen mit Sitz in der EU gelten, die innerhalb der EU tätig sind.
- Sie wird auch für Unternehmen gelten, die ihren Sitz nicht in der EU haben, aber in der EU tätig sind.
- Nicht-EU-Unternehmen, die keine Dienstleistungen in der EU anbieten, sind von NIS2 nicht direkt betroffen.

Nichteinhaltung der Vorschriften

Die Nichteinhaltung der NIS2-Richtlinie kann für alle unverzichtbaren Entitäten zu hohen Bußgeldern und Strafen führen. Darüber hinaus sind die Leitungsorgane für die Umsetzung von Cybersicherheitsmaßnahmen verantwortlich und können bei Verstößen persönlich haftbar gemacht werden.

NIS2 hat einen breiteren Anwendungsbereich als die erste NIS-Richtlinie

- Erweiterung des Anwendungsbereichs von 7 auf 18 Sektoren
- Gilt für Einrichtungen, die bestimmte kritische Dienste oder grundlegende Infrastrukturen bereitstellen
- Definiert zwei Kategorien von Entitäten: **Unverzichtbar** und **wichtig**

Unverzichtbare Entitäten

Wichtige Entitäten

Zusätzliche Sektoren in NIS2

Größenschwelle: 250 oder mehr Beschäftigte oder mehr als 50 Millionen Euro Jahresumsatz

Größenschwelle: 50 oder mehr Beschäftigte oder mehr als 10 Millionen Euro Jahresumsatz

Quelle: IDC, 2024

Risikomanagement steht ganz oben auf der Tagesordnung der CEOs

Da die Hälfte der europäischen CEOs die Verbesserung des Risikomanagements ihres Unternehmens als oberste Priorität angibt, ist das Thema Risiko eindeutig in den Fokus der Unternehmensführung gerückt. Durch die proaktive Identifizierung und Minderung von Risiken zielen CEOs darauf ab, die Kontinuität des Geschäftsbetriebs und die Widerstandsfähigkeit gegenüber Unsicherheiten zu gewährleisten. Cybersicherheit ist eine Manifestation des Geschäftsrisikos, eine Aufgabe, die darin besteht, die Vermögenswerte, den Ruf und die langfristige Überlebensfähigkeit eines Unternehmens zu schützen, da sich die Bedrohungen ständig weiterentwickeln. Ein wirksames Risikomanagement im Bereich der Cybersicherheit umfasst nicht nur den Schutz sensibler Daten und Systeme vor Sicherheitsverletzungen, sondern auch die Vorbereitung auf mögliche Vorfälle, um deren Auswirkungen zu minimieren. Die Integration des Risikomanagements in Cybersicherheitsstrategien ermöglicht es CEOs, fundierte Entscheidungen zu treffen, Ressourcen effizient zuzuweisen und das Vertrauen der Stakeholder zu erhalten.

46 %

der europäischen CEOs sehen die Verbesserung des **Risikomanagements** als höchste Priorität

Identifizierung von Risiken	Risikobewertung	Risikominderung	Risikoüberwachung	Risikokommunikation
Systematische Identifizierung potenzieller Cyber-Sicherheitsbedrohungen und Schwachstellen, die sich auf den Geschäftsbetrieb auswirken könnten.	Analyse identifizierter Risiken, Bewertung potenzieller Auswirkungen und Wahrscheinlichkeiten und entsprechende Einordnung.	Umsetzung geeigneter technischer und betrieblicher Maßnahmen zur Reduzierung der Auswirkungen identifizierter Risiken.	Kontinuierliche Überwachung des Cyber-Sicherheitsumfelds und der Risikolandschaft, um Veränderungen oder neu auftretende Bedrohungen zu erkennen.	Einrichtung klarer und effektiver Kommunikationskanäle, um sicherzustellen, dass relevante Informationen an interne und externe Stakeholder weitergegeben werden.

Proaktiver Ansatz

Das allgemeine Bewusstsein für NIS2 ist hoch, das Detailwissen jedoch nicht

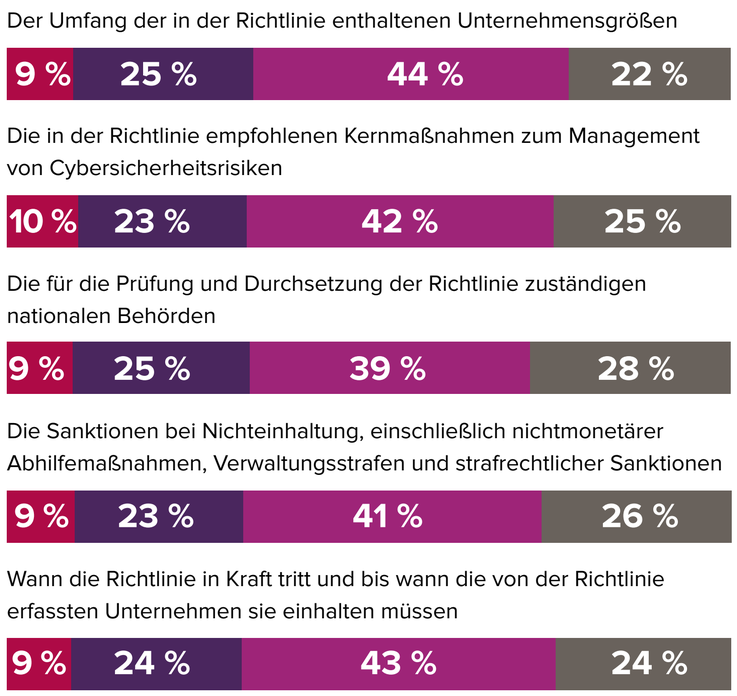
Das allgemeine Bewusstsein für die wichtigsten Aspekte der NIS-Richtlinie2 ist hoch, aber der Wissensstand ist unterschiedlich.

Dies zeigt, dass die Mehrheit der europäischen Unternehmen die NIS2-Richtlinie verfolgt und sich der Hauptaspekte bewusst ist, die ihr Unternehmen betreffen werden.

Umgekehrt hat jedes dritte europäische Unternehmen keine oder nur sehr geringe Kenntnisse über eine Richtlinie, die in sehr naher Zukunft in Kraft treten wird.

Die Zahl der europäischen Unternehmen, die über detaillierte Kenntnisse der wichtigsten Aspekte von NIS2 verfügen, ist deutlich geringer. Nur jedes vierte Unternehmen gibt an, die Richtlinie zu kennen und viel darüber zu wissen.

F. Wie gut kennen Sie die folgenden Aspekte der neuen NIS2-Richtlinie?



Ich bin mir dessen bewusst und weiß viel darüber:

22 %

25 %
(17 % der britischen Unternehmen)

28 %
(18 % der belgischen und niederländischen Unternehmen)

26 %
(18 % der belgischen Unternehmen und 14 % der niederländischen Unternehmen)

24 %

Nur jedes vierte Unternehmen ist sich der verschiedenen Aspekte der NIS2-Richtlinie *bewusst* und verfügt über *detaillierte Kenntnisse*.

Quelle: IDC, 2024

Unternehmen kämpfen mit langsamen Fortschritten und mangelndem Engagement des Vorstands

Die meisten Unternehmen machen nur langsame Fortschritte und haben Schwierigkeiten in verschiedenen Bereichen der NIS2-Konformität. Verschärft werden diese Herausforderungen durch das mangelnde Engagement der Unternehmensleitung (C-Level), dass sich in erster Linie auf das Geschäft und das Wachstum konzentriert und der Einhaltung von Vorschriften nur geringe Priorität einräumt – trotz der drohenden Bußgelder für Führungskräfte von Unternehmen, die sich nicht an die Vorschriften halten.

58 %

74 % | 56 % | 55 % | 52 % | 43 %

der Unternehmen berichten, dass sie nur langsam Fortschritte bei der Einhaltung der NIS2 machen.

F. Wie zufrieden sind Sie mit den Fortschritten Ihres Unternehmens bei der Einhaltung der NIS2?

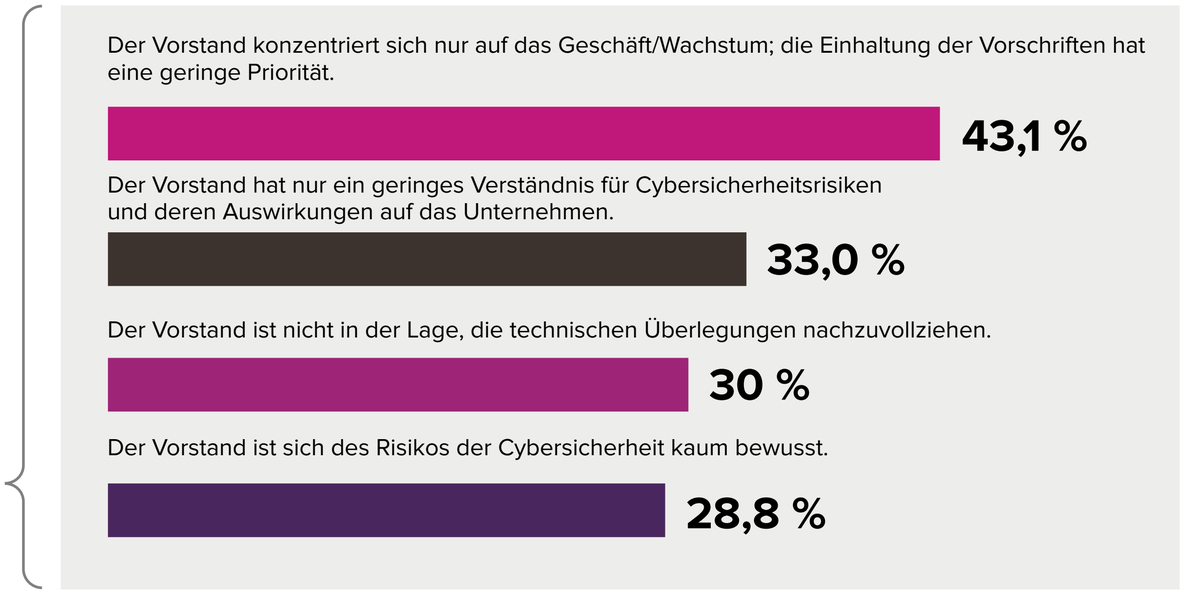
42 %

40 % | 38 % | 38 % | 38 % | 34 %

der Unternehmen geben an, dass ihre Vorstände nicht mit der Einhaltung der NIS2 befasst sind.

F. Ist der Vorstand Ihres Unternehmens über die Einhaltung von NIS2 informiert und engagiert?

Gründe für mangelndes Engagement des Vorstands



F. Warum glauben Sie, dass sich der Vorstand Ihres Unternehmens nicht für die Einhaltung von NIS2 einsetzt?

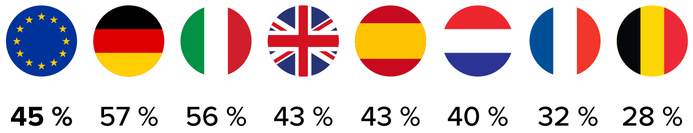
Europäische Unternehmen sind nur mangelhaft vorbereitet

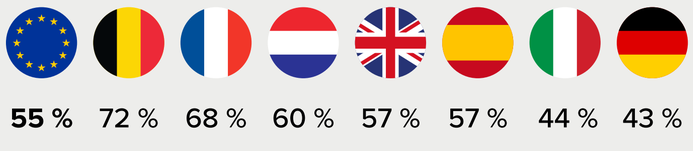
Da nur die Hälfte der europäischen Unternehmen der Ansicht ist, dass sie NIS2 erfüllen, bleibt noch viel zu tun. Die Einhaltung der Vorschriften ist jedoch in den einzelnen Ländern der Europäischen Union sehr unterschiedlich. Beispielsweise halten sich doppelt so viele **deutsche** Unternehmen für konform wie **belgische** Firmen, und nur 32 % der **französischen** Unternehmen halten sich für konform.

Unabhängig vom Konformitätsstatus gibt es in europäischen Unternehmen keine herausragenden Maßnahmen zum Risikomanagement oder zur Informationssicherheit (wie für die NIS2-Konformität erforderlich). Diese Situation verdeutlicht das Fehlen einer unilateral vereinbarten Strategie für Maßnahmen zur Einhaltung der NIS2-Vorschriften durch europäische Unternehmen.

Sicherheits- und **IT-Dienstleister** sind die wichtigsten Kanäle, über die europäische Unternehmen über die Umsetzung von NIS2 auf lokaler oder nationaler Ebene informiert werden, wie 4 von 10 Unternehmen angaben. Interessanterweise werden **nationale Cyber-Sicherheitsbehörden** in diesem Zusammenhang nur von einem Drittel der europäischen Unternehmen genannt.

Status der Einhaltung
(Selbstauskunft)





F. Glauben Sie, dass Ihr Unternehmen die neue NIS2-Richtlinie bereits erfüllt?

Maßnahmen vor Ort
Top 3

1. Sicherheit bei der Beschaffung, Entwicklung und Wartung von Netz- und Informationssystemen
2. Mehrstufige und starke Authentifizierung sowie sichere Kommunikation
3. Leitlinien und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit

F. Welche der folgenden Maßnahmen zum Risiko- und Informationssicherheitsmanagement (wie für die Einhaltung von NIS2 erforderlich) hat Ihr Unternehmen eingeführt?

Nationale Sensibilisierung
Top 2

1. **44** % wir sind uns der Risiken bewusst, da unser Sicherheits- und IT-Dienstleister aktiv das Bewusstsein dafür schärft
2. **32** % wir sind uns der Risiken bewusst, da unsere nationale Cyber-Sicherheitsbehörde aktiv dafür sensibilisiert

34 % wir sind uns der Risiken bewusst, da unser Sicherheits- und IT-Dienstleister aktiv dafür sensibilisiert

32 % wir sind uns bewusst und haben an der Beratungsphase teilgenommen

F. Bitte geben Sie an, inwieweit Ihr Unternehmen über die Umsetzung von NIS2 auf lokaler/nationaler Ebene informiert ist und in welchem Kontext diese Informationen stehen.

Quelle: IDC, 2024

Die größten Herausforderungen sind in allen Branchen gleich

Je weiter jedoch die europäischen Unternehmen auf dem Weg zur Einhaltung von NIS2 voranschreiten, desto häufiger werden die Maßnahmen, mit denen sie konfrontiert sind, sektorübergreifend genannt.

Besonders problematisch sind Richtlinien und Verfahren wie die Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit, die Sicherheit von Informationssystemen und die Zugangskontrolle.

Die anspruchsvollsten Konformitätsmaßnahmen

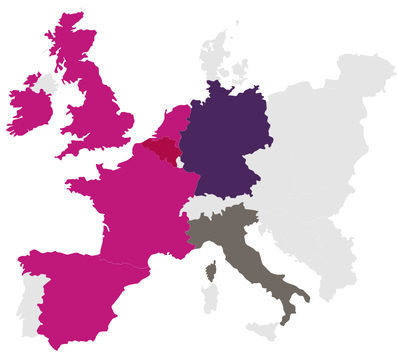
	Alle Branchen	Öffentliche Verwaltung	Gesundheitswesen	Bankwesen	Fertigung	Digitale Infrastruktur
Nr. 1	Sicherheit bei der Beschaffung, Entwicklung und Wartung von Netz- und Informationssystemen		Leitlinien und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit	Risikomanagement und Sicherheitsrichtlinien für Informationssysteme	Sicherheit bei der Beschaffung, Entwicklung und Wartung von Netz- und Informationssystemen	Leitlinien und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
Nr. 2	Leitlinien und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit	Risikomanagement und Sicherheitsrichtlinien für Informationssysteme	Sicherheit bei der Beschaffung, Entwicklung und Wartung von Netz- und Informationssystemen		HR-Sicherheit, Zugangskontrollrichtlinien und Asset Management	Sicherheit bei der Beschaffung, Entwicklung und Wartung von Netz- und Informationssystemen
Nr. 3	Risikomanagement und Sicherheitsrichtlinien für Informationssysteme	Leitlinien und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit	Risikomanagement und Sicherheitsrichtlinien für Informationssysteme	Grundsätze und Verfahren für den Einsatz von Kryptographie und Verschlüsselung	Geschäftskontinuität und Krisenmanagement	Multi-Faktor-Authentifizierung (MFA), kontinuierliche Authentifizierung und sichere Kommunikation

F. Welche NIS2-Maßnahmen sind für Ihr Unternehmen am schwierigsten zu erfüllen?

Die Sicherheit bei der Beschaffung, Entwicklung und Wartung von Netz- und Informationssystemen wird von kleinen Unternehmen (50 bis 99 Beschäftigte), mittleren Unternehmen (100 bis 499 Beschäftigte) und sehr großen Unternehmen (über 1000 Beschäftigte) als größte Herausforderung genannt.

Geschäftskontinuität und Krisenmanagement (Backups und Disaster Recovery) sind die wichtigsten Herausforderungen für große Unternehmen (500–999 Beschäftigte).

Die dringendsten Herausforderungen unterscheiden sich jedoch von Land zu Land. Unternehmen in **Deutschland**, **Italien** und **Belgien** nennen andere Herausforderungen als Unternehmen in **Frankreich**, dem **Vereinigten Königreich**, den **Niederlanden** und **Spanien**.



- Sicherheit bei der Beschaffung, Entwicklung und Wartung von Netz- und Informationssystemen
- Geschäftskontinuität und Krisenmanagement (Back-up und Disaster Recovery)
- Multi-Faktor-Authentifizierung (MFA), kontinuierliche Authentifizierung und sichere Kommunikation
- HR-Sicherheit, Zugangskontroll-richtlinien und Asset Management

Die Vorbereitung wird durch unterschiedliche Strategien und menschliche Faktoren behindert

Unternehmen in der gesamten EU stoßen bei ihren Bemühungen, die kommende NIS2-Verordnung einzuhalten, auf erhebliche Hindernisse. Die Vorbereitungsphase wird insbesondere durch widersprüchliche Richtlinien und menschliche Faktoren wie unzureichende Schulung des Personals und mangelndes Problembewusstsein behindert. Darüber hinaus werden diese Herausforderungen durch das Fehlen zeitnaher und klarer Leitlinien seitens der nationalen Behörden noch verschärft, da dies zu Unsicherheit hinsichtlich der Einhaltung der Vorschriften führt. Diese Situation wird durch unzureichende Mittelzuweisungen für grundlegende Technologieinvestitionen noch verschärft, was den Fortschritt erheblich behindert und das Risiko von Verstößen und Cybersicherheitslücken erhöht.

Wichtigste Fragen zur Vorbereitung

	Alle Länder	EU	Deutschland	Frankreich	Italien	Niederlande	Vereinigtes Königreich
Nr. 1	Unterschiedliche Richtlinien und Kontrollen in den verschiedenen EU-Ländern, in denen wir tätig sind			Menschliche Faktoren, einschließlich Schulung und Sensibilisierung der Mitarbeiter			Mangel an rechtzeitigen und klaren Vorabanweisungen seitens unserer nationalen Sicherheitsbehörden
Nr. 2	Menschliche Faktoren, einschließlich Schulung und Sensibilisierung der Mitarbeiter		Fehlende Haushaltsmittel für Technologieinvestitio-nen	Unterschiedliche Richtlinien und Kontrollen in den verschiedenen EU-Ländern, in denen wir tätig sind			Das Management von Cyber-Risiken als Pflichtaufgabe und nicht als optionale oder empfohlene Maßnahme zu betrachten
Nr. 3	Mangel an rechtzeitigen und klaren Vorabanweisungen seitens unserer nationalen Sicherheitsbehörden	Mangelndes Budget für Technologieinvestitionen	Menschliche Faktoren, einschließlich Schulung und Sensibilisierung der Mitarbeiter	Mangel an rechtzeitigen und klaren Vorabanweisungen seitens unserer nationalen Sicherheitsbehörden		Erfassung unseres Status und unserer Fähigkeiten in Bezug auf die Anforderungen	Fehlende Ressourcen für die Umsetzung von Änderungen an Strategien, Praktiken oder Prozessen

Quelle: IDC, 2024

NIS2 wird sich auf die menschlichen Faktoren auswirken und einen kulturellen Wandel erforderlich machen

Die kommende NIS2-Richtlinie konzentriert sich zwar auf die Verbesserung der technischen Sicherheitsstandards, hat aber auch erhebliche Auswirkungen auf die **menschlichen Faktoren und Fähigkeiten** innerhalb von Unternehmen, da sie einen Kulturwandel hin zu einem stärkeren **Bewusstsein für Cybersicherheit**, die **Schulung von Mitarbeitern** und eine tiefere Integration des **Cyber-Risikomanagements** in den täglichen Betrieb erfordert.

Wege zur Bewältigung der Herausforderungen im Zusammenhang mit menschlichen Faktoren:

Umfassende Schulungsprogramme: Regelmäßige, auf die jeweilige Rolle zugeschnittene Cyber-Sicherheitsschulungen für alle Mitarbeiter. So wird sichergestellt, dass jeder sich seiner Verantwortung bewusst ist.

Starke Führung und Governance: Sicherstellen, dass die oberste Führungsebene aktiv an der Schaffung einer Kultur der Cybersicherheit beteiligt ist.

Kollaboratives Risikomanagement: Richten Sie abteilungsübergreifende Risikomanagement-Teams ein, die sich aus IT- und Nicht-IT-Mitarbeitern zusammensetzen, um die Cybersicherheit mit den Geschäftszielen in Einklang zu bringen.

Investitionen in die Fortbildung: Bieten Sie Ihren Mitarbeitern Weiterbildungsmöglichkeiten an, insbesondere in den Bereichen Cybersicherheit, Compliance und Risikomanagement, um sicherzustellen, dass das Unternehmen über die richtigen Fachkenntnisse verfügt.

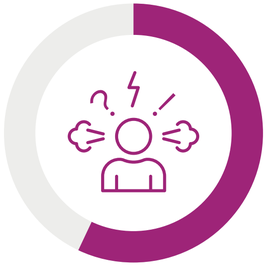
Aufbau einer Kultur der Sicherheit: Fördern Sie das Bewusstsein für Cybersicherheit im gesamten Unternehmen und betonen Sie, dass es sich hierbei nicht nur um ein IT-Problem handelt, sondern um etwas, das jeden betrifft.

Indem sie diese Herausforderungen direkt angehen, können Unternehmen eine widerstandsfähigere Belegschaft aufbauen, die besser in der Lage ist, mit einer komplexen Sicherheitslandschaft umzugehen und die Einhaltung neuer Vorschriften zu gewährleisten.

Quelle: IDC, 2024

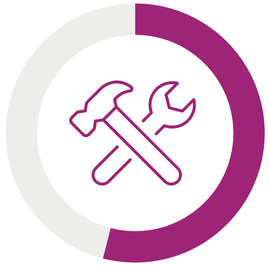
Die Auswirkungen auf die Qualifikationen sind beträchtlich, werden aber oft vernachlässigt

Obwohl das Personal eine entscheidende Rolle bei der Einhaltung der NIS2-Richtlinie spielt, hat **jedes zweite** Unternehmen Probleme mit der Qualifikation.



57 %

der Unternehmen berichten, dass ihre internen Teams mit der Einhaltung der Vorschriften überfordert sind.



54 %

der Unternehmen berichten, dass sie häufig Abkürzungen oder Umgehungslösungen verwenden, um ihre Compliance-Fristen einzuhalten.

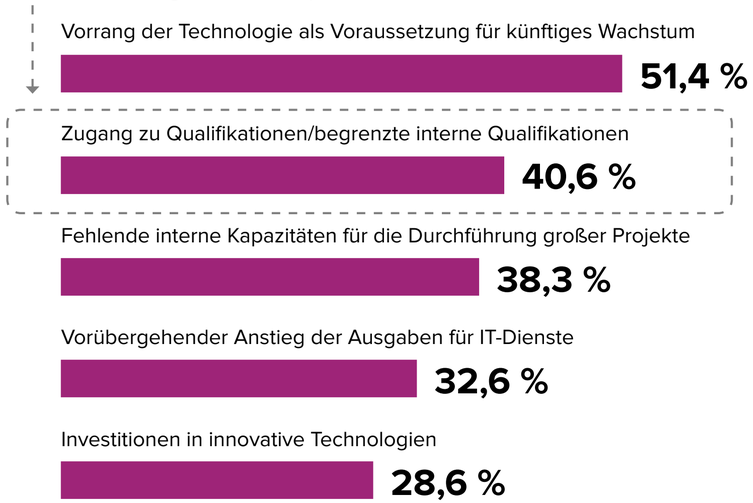
52 %

der Unternehmen geben an, dass sie nicht über die internen Fähigkeiten verfügen, um die Vorschriften vollständig zu erfüllen.

F. Inwieweit stimmen Sie den folgenden Aussagen zu?

Während Qualifikationsdefizite den Weg eines Unternehmen zur NIS2-Konformität negativ beeinflussen können, kann die Zusammenarbeit mit externen Partnern Qualifizierungsprobleme abmildern und sich positiv auswirken, indem auf Erfahrungen aus ähnlichen Engagements aufgebaut wird.

Die Zusammenarbeit mit externen Anbietern, um die begrenzten internen Ressourcen durch ein breiteres Spektrum an Kompetenzen zu ergänzen, ist einer der Hauptgründe für den Anstieg der Ausgaben für Dienstleistungen in europäischen Unternehmen:



F. Was sind die Hauptgründe für den Anstieg der Ausgaben für externe IT-Dienstleistungen in Ihrem Unternehmen?

Quelle: IDC, 2023

Unternehmen, die ihre Kompetenzprobleme in den Griff bekommen, haben einen Vorteil gegenüber ihren Mitbewerbern und können die NIS2-Konformität möglicherweise früher erreichen.

Quelle: IDC, 2024

Unternehmen tendieren dazu, die Umsetzung von NIS2 auszulagern, behalten aber strategische Kompetenzen intern

Unternehmen, die mit Managed Security Providers (MSPs) zusammenarbeiten, lagern in der Regel arbeitsintensive Aufgaben aus, die spezielle Fähigkeiten erfordern, wie z. B. Sicherheitsmaßnahmen. Sie behalten strategische Funktionen wie Compliance, Corporate Governance, Risikomanagement und Datensicherheit im eigenen Haus. Die Einhaltung von NIS2 ist ein wichtiger Motivationsfaktor für Unternehmen, die derzeit keine MSPs einsetzen, deren Einsatz zu erwägen und von der Expertise und den Ressourcen der MSPs zu profitieren.

MSP-Engagement	Ausgelagert			Intern		
42 % arbeiten bereits mit einem Anbieter von **Managed Security Services zusammen**.	**40 %** Cloud-Sicherheit	**39 %** Sicherheitsmaßnahmen	**39 %** Bereitstellung von Technologie oder Strategien zur Erfüllung der NIS2-Anforderungen	**43 %** Strategische Ausrichtung auf Compliance, Governance oder Risiko	**41 %** Prävention von Ransomware	**43 %** Datensicherheit
54 % planen, innerhalb der nächsten zwei Jahre mit einem **Anbieter von Managed Security Services** zusammenzuarbeiten.	**39 %** Bereitstellung von Technologie oder Strategien zur Erfüllung der NIS2-Anforderungen	**38 %** Cloud-Sicherheit	**37 %** Anpassung der Sicherheitsstrategie an die NIS2-Konformität	**43 %** Sicherheitsmaßnahmen	**40 %** Datensicherheit	**38 %** Resilienz aufbauen, um neuen Bedrohungen einen Schritt voraus zu sein

F.: Würde Ihr Unternehmen die Zusammenarbeit mit einem Anbieter von Managed Cyber Security Services in Betracht ziehen?

F.: Bitte geben Sie an, was Ihr Unternehmen in den nächsten zwei Jahren in den folgenden Bereichen plant.

Quelle: IDC, 2024

Sicherheitsstrategie und Einbindung von Stakeholdern fördern das Engagement externer Partner

Das Engagement der Partner bei der Einhaltung der NIS2-Vorschriften ist hoch.

53 % arbeiten derzeit mit einem Partner/Berater zusammen.

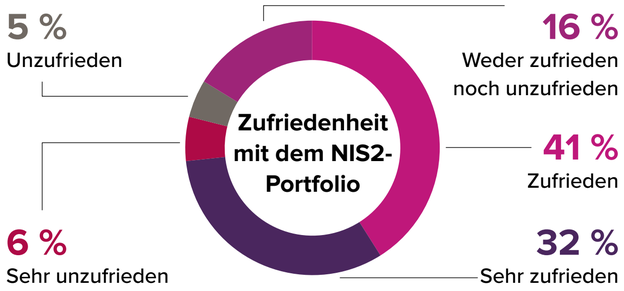
38 % beabsichtigen, in Zukunft mit einem Partner zusammenzuarbeiten.

Die Hälfte der europäischen Unternehmen arbeitet bereits mit externen Partnern zusammen, um die NIS2-Konformität zu gewährleisten. Weniger als 10 % der europäischen Unternehmen planen nicht, einen solchen Partner hinzuzuziehen, was den wahrgenommenen Wert externer Unterstützung unterstreicht. In Belgien beabsichtigen jedoch 18 % der Unternehmen nicht, mit einem externen Partner zusammenzuarbeiten, um die NIS2-Konformität zu gewährleisten.

Das Angebot der Partner entspricht den Bedürfnissen der europäischen Unternehmen.

73 % der europäischen Unternehmen sind *zufrieden* oder *sehr zufrieden* mit den NIS2-Angeboten ihrer Partner, was auf eine sehr hohe Zufriedenheit mit dem Engagement der Partner hinweist.

Diese Zahl sinkt auf **51 % in der Kategorie der kleinen Unternehmen**, was zeigt, dass die Partner noch viel tun müssen, um den **Bedürfnissen der kleinen Unternehmen** gerecht zu werden.

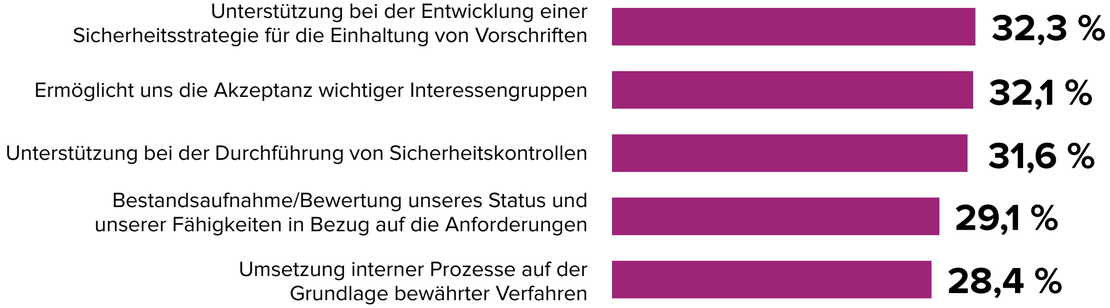


F.: Wie zufrieden sind Sie mit den aktuellen Angeboten der Sicherheitsdienstleistungspartner Ihres Unternehmens, um die Anforderungen Ihres Unternehmens in Bezug auf NIS2 zu erfüllen?

Quelle: IDC, 2024

Inwieweit benötigen europäische Unternehmen externe Partner, die sie bei der Einhaltung der NIS2-Vorschriften unterstützen?

F.: In welchen Bereichen sehen Sie die wichtigste Rolle Ihres Cybersicherheits-Dienstleisters in Bezug auf die NIS2-Compliance Ihres Unternehmens? Die wichtigsten 5



Hinweis: Die Prozentsätze geben den Anteil der Befragten an, die die jeweiligen Bereiche ausgewählt haben.

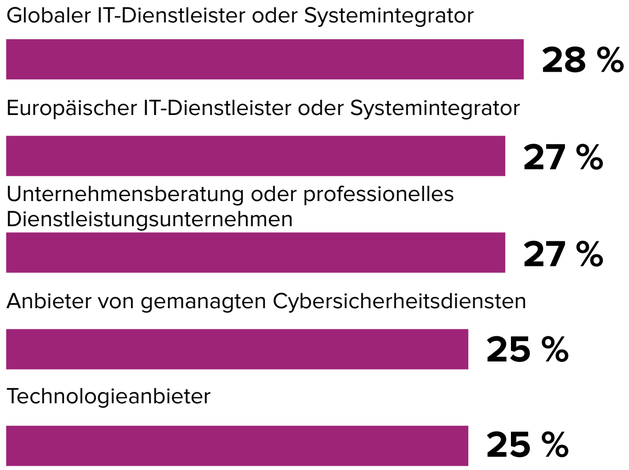
Strategische Ausrichtung und Aufsicht: Eine Sicherheitsstrategie ist entscheidend für die Einhaltung von Vorschriften, da eine starke Cybersicherheit und die Einhaltung von Vorschriften Hand in Hand gehen.

Aktivitäten: Während europäische Unternehmen auf dem Weg zur NIS2-Konformität voranschreiten, unterstützen externe Partner bei Aktivitäten wie Managementgenehmigung, Strategie, Benchmarking, Implementierung, Bereitstellung von Ausrüstung und Sicherheitsoperationen.

Wert: Bei der Auswahl externer Partner für die Einhaltung der NIS2-Richtlinien müssen europäische Unternehmen potenzielle Partner anhand einer Vielzahl von Kompetenzen bewerten. Umgekehrt müssen Dienstleister ihre Fähigkeiten und Erfolge in diesen Schlüsselbereichen des Engagements nachweisen.

Dienstleistungsanbieter werden für NIS2 am meisten bevorzugt

Partnerpräferenz für NIS2



F.: Welche externen Partner würde Ihr Unternehmen für die Einhaltung der NIS2-Richtlinien bevorzugen?

Die Präferenzen für externe Partner zur Unterstützung europäischer Unternehmen bei der Einhaltung der NIS2-Richtlinie sind **vielfältig** und zeigen, wie **umkämpft** der Markt für externe Partner ist.

Betrachtet man Europa als Ganzes, so sind IT-Dienstleister die **bevorzugten Partner** für NIS2 – sie rangieren sogar noch vor den Anbietern von Managed Cyber Security Services.

Die Präferenzen sind jedoch von Land zu Land unterschiedlich:


Globaler IT-Dienstleister oder Systemintegrator


Europäischer IT-Dienstleister und Systemintegrator


Anbieter von gemanagten Cybersicherheitsdiensten


Globaler IT-Dienstleister oder Systemintegrator


Unternehmensberatung oder professionelles Dienstleistungsunternehmen

Die wichtigste Voraussetzung für belgische Unternehmen ist, dass sie „*die Compliance-Anforderungen unseres Landes wirklich gut kennen*“. Dies zeigt, dass die Kenntnis der Compliance-Regeln **Priorität** hat.

Quellen für Informationen über NIS2?

30 % der europäischen Unternehmen nennen IT-Dienstleister als wichtigste Informationsquelle zum Thema NIS2.

Kleine Unternehmen nutzen ihre **Branchenkollegen** und **Ökosystempartner**, während große Unternehmen die **Branchenregulierungsbehörden** als Hauptquelle für NIS2-Informationen angeben.

Die Partnerpräferenz nach Unternehmensgröße zeigt zwar eine generelle Präferenz für **IT-Dienstleister**, macht aber auch deutlich, dass kleine Unternehmen in Europa gleichermaßen bereit sind, mit einem Anbieter von **Managed Security Services** zusammenzuarbeiten, und dass große Unternehmen Compliance-Know-how über die Art des Partners stellen.

Kleines Unternehmen *(50–99 Mitarbeiter)*	Globaler IT-Dienstleister, Systemintegrator oder Anbieter von verwalteten Cybersicherheitsdiensten
Mittelgroßes Unternehmen *(100–499 Mitarbeiter)*	Europäischer IT-Dienstleister oder Systemintegrator
Großunternehmen *(500–999 Mitarbeiter)*	Ein Unternehmen, das die Compliance-Anforderungen unseres Landes sehr gut kennt
Sehr großes Unternehmen *(Mehr als 999 Mitarbeiter)*	Globaler IT-Dienstleister oder Systemintegrator

Letztlich zeigen die eng beieinander liegenden Präferenzen, dass es keinen Partnertyp gibt, der die NIS2-Anforderungen europäischer Unternehmen **optimal** erfüllt. Dies **erschwert** die Auswahl für Unternehmen, die Unterstützung suchen, zeigt aber auch, dass alle Arten von Partnern die Notwendigkeit und die Möglichkeit haben, ihre Botschaften und Angebote zu **verbessern**.

Quelle: IDC, 2024

Empfehlungen

In dem Maße, in dem sich Unternehmen im Zuge der digitalen Transformation zu digitalen Unternehmen entwickeln, werden Daten zu kritischem geistigem Eigentum und gewinnen für das Unternehmen, seine Kunden und Partner zunehmend an Bedeutung.

In diesem Sinne hat die Europäische Union 2016 die Richtlinie zur Netz- und Informationssicherheit erlassen, die 2023 als NIS2 aktualisiert wurde. Alle in der EU tätigen Unternehmen sind davon betroffen und müssen daher eine Reihe von NIS2-Anforderungen erfüllen.

Die Einhaltung von NIS2 kommt in ganz Europa nur langsam voran, und die Unternehmen in der Region sind mit zahlreichen Problemen konfrontiert. Externe Partner sind eine Quelle der Unterstützung und werden bereits von europäischen Unternehmen auf ihrem Weg zur Einhaltung der NIS2-Richtlinien genutzt.

Jetzt handeln: Trotz der Verzögerungen bei der Umsetzung von NIS2 in nationales Recht sollten Unternehmen ihre Bemühungen zur Einhaltung nicht aufschieben. Setzen Sie die Vorbereitungen fort, indem Sie die aktuellen Cybersicherheitsmaßnahmen gründlich bewerten, Lücken identifizieren und notwendige Verbesserungen umsetzen.

Bewusstsein schaffen: Führen Sie Schulungen und Workshops durch, um Lücken in Bezug auf Bewusstsein und Wissen zu schließen und sicherzustellen, dass alle betroffenen Mitarbeiter die Anforderungen und Auswirkungen der Richtlinie verstehen. Ziehen Sie bei Bedarf externe Experten hinzu, um diesen Prozess zu beschleunigen und ein umfassendes Verständnis im gesamten Unternehmen sicherzustellen.

Beziehen Sie die Unternehmensleitung ein: Da 58 % der europäischen Unternehmen von langsamen Fortschritten bei der Einhaltung von NIS2 berichten und 42 % angeben, dass sich ihre Vorstände nicht mit NIS2 befassen, ist die Einhaltung der Vorschriften ein zentrales Thema für europäische Unternehmen.

Engagieren Sie sich proaktiv: Berücksichtigen Sie menschliche Faktoren, indem Sie Richtlinien und Verfahren zur Cybersicherheit entwickeln und klar kommunizieren. Sorgen Sie dafür, dass die oberste Führungsebene aktiv einbezogen wird und eine starke Cybersicherheitskultur innerhalb des Unternehmens gefördert wird. Dies verbessert Ihre allgemeine Cybersicherheitslage und erleichtert die Einhaltung der NIS2-Anforderungen.

Beziehen Sie Partner ein: Um interne Qualifikationsdefizite auszugleichen, sollten Unternehmen auf die Expertise strategischer Partner, wie z.B. IT-Dienstleister zurückgreifen. Dieser Ansatz kann dazu beitragen, Qualifikationslücken zu verringern, die Einhaltung der Vorschriften zu verbessern und mögliche Sanktionen zu vermeiden.

Bewerten Sie sorgfältig: Die europäischen Unternehmen sind mit den NIS2-Angeboten der Sicherheitsdienstleister sehr zufrieden. Bei der Auswahl potenzieller NIS2-Partner müssen Unternehmen potenzielle Anbieter anhand aller Parameter bewerten, einschließlich Strategie, Benchmarking, Implementierung und SecOps.

Mitteilung von Insight

Als führender Lösungsintegrator mit umfassenden Kenntnissen von Sicherheitslösungen und der EU-Regulierungslandschaft ist Insight gut gerüstet, um Unternehmen bei der Implementierung robuster Sicherheitskontrollen im Hinblick auf die kommenden NIS2-Anforderungen zu unterstützen. Da wir die dringende Notwendigkeit einer einheitlichen Kommunikation auf allen Ebenen erkannt haben, können wir Ihnen dabei helfen, ein gemeinsames Verständnis von NIS2 in Ihrem gesamten Unternehmen zu schaffen. Wir konzentrieren uns auf sinnvolle Veränderungen, legen Wert auf Risikominimierung statt auf oberflächliche Berichterstattung und optimieren die Rendite Ihrer IT-Investitionen.

Verlassen Sie sich auf Insight als strategischen Partner bei der Bewältigung der Komplexität von NIS2 und der Umsetzung eines proaktiven Cybersicherheitsansatzes zur Einhaltung der Richtlinie.

Demografische Daten

Größe des Unternehmens:

10 %

59–99 Mitarbeiter

33 %

100–499 Mitarbeiter

21 %

Mehr als 1000 Mitarbeiter

36 %

500–999 Mitarbeiter

Vertikale Branchen:

1 %	Weltraum
6 %	Digitale Anbieter
10 %	Digitale Infrastruktur
8 %	Energie
10 %	Bankwesen
4 %	Finanzmarktinfrastrukturen
10 %	Öffentliche Verwaltung
8 %	Gesundheitswesen
11 %	IKT-Dienstleistungsmanagement
20 %	Fertigung
11 %	Verkehr und Logistik
0,3 %	Wasser, Abwasser, Abfallwirtschaft

Länder:

8 %	Belgien
17 %	Frankreich
17 %	Deutschland
17 %	Italien
8 %	Niederlande
17 %	Spanien
17 %	Vereinigtes Königreich

Einfluss auf die Entscheidung:

67 %	IT-Entscheidungsträger
33 %	Digitale Anbieter

Rollen:

34 %	IT-Sicherheitsmanager oder -direktor
47 %	IT-Manager oder Direktor
8 %	VP oder Betriebsleitung
2 %	VP oder Leiter der Abteilung Risiko oder Compliance
6 %	Chief Information Officer oder Chief Technology Officer
2 %	CISO (Beauftragter für Informationssicherheit)
7 %	Verantwortlicher für den Betrieb
8 %	Chief Risk Officer oder Chief Compliance Officer

Quelle: IDC 2024, n = 600, CAWI-Erhebungsmethode

Über IDC

International Data Corporation (IDC) ist der weltweit führende Anbieter von Marktinformationen, Beratungsdienstleistungen und Veranstaltungen auf dem Gebiet der Informationstechnologie und der Telekommunikation sowie der Verbrauchertechnologiemärkte.

Mit mehr als 1300 Analysten weltweit bietet IDC globale, regionale und lokale Expertise zu Chancen und Trends in Technologie und Wirtschaft in mehr als 110 Ländern. Analysen und Erkenntnisse von IDC unterstützen IT-Profis, Geschäftsleute und Investoren bei fundierten Entscheidungen über Technologien und die Erzielung ihrer wichtigsten Geschäftsziele.

IDC wurde 1964 gegründet und ist eine hundertprozentige Tochtergesellschaft der International Data Group (IDG, Inc.), dem weltweit führenden Unternehmen für Medien-, Daten- und Marketingdienstleistungen im Technologiebereich.

IDC Custom Solutions

Diese Veröffentlichung wurde von IDC Custom Solutions erstellt. Als weltweit führender Anbieter von Marktinformationen, Beratungsdienstleistungen und Veranstaltungen auf dem Gebiet der Informationstechnologie und der Telekommunikation sowie der Verbrauchertechnologiemärkte hilft IDC Custom Solutions Kunden bei Planung, Marketing, Vertrieb und Erfolg auf dem Weltmarkt. Wir erstellen umsetzbare Marktinformationen und einflussreiche Content-Marketing-Programme, die messbare Ergebnisse liefern.

IDC UK
5th Floor, Ealing Cross, 85 Uxbridge Road, London, W5 5TH, Vereinigtes Königreich
T +44.208.987.7100

@idc | @idc | idc.com

© 2024 IDC Research, Inc IDC-Materialien sind für die externe Verwendung lizenziert, und die Verwendung oder Veröffentlichung von IDC-Forschungsergebnissen bedeutet in keiner Weise, dass IDC Produkte oder Strategien des Sponsors oder des Lizenznehmers unterstützt.