2023

Was sich mit der NIS2-Richtlinie ändert

Wie Sie ein holistisches, Identity-zentriertes Security-Framework bei der Umsetzung unterstützt

Warum starke Identitäten zur Vorbereitung der NIS2-Compliance wichtig sind

okta

Inhalt

3 Einführung

4 NIS2 im Überblick

5 Wie Sie sich auf NIS2 vorbereiten

7 Der Stellenwert der Identitäten für die NIS2-Compliance

9 Das holistische, identitätszentrierte Security-Framework von Okta

11 Konsequenzen bei Nicht-Einhaltung der NIS2-Vorgaben

NIS2 und der Schutz Ihrer Supply Chain

12 Formalisieren Sie Ihren Response-Plan

Machen Sie Ihr Team fit

13 Wie NIS2 und ISO 27001 zusammenhängen

15 Fazit

Einführung

Die Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) der Europäischen Union wurde 2016 verabschiedet und trat 2018 in Kraft. Sie zielte darauf ab, ein einheitlich hohes Sicherheitsniveau für Netz- und Informationssysteme in der gesamten EU zu gewährleisten, und definiert Sicherheitsmaßnahmen und Meldepflichten für Betreiber kritischer Dienste sowie Service Provider. Die Richtlinie wurde jüngst mit der NIS2-Richtlinie aktualisiert. Diese verschärft abermals die Sicherheitsmaßnahmen und Meldepflichten und weitet den Anwendungsbereich auf neue Sektoren aus.

Das vorliegende Whitepaper soll einen Überblick über NIS2 geben und aufzeigen, wie NIS2 mit gängigen Security-Frameworks wie ISO 27001 kombiniert werden kann, wie wichtig Identität in diesem Kontext ist und was Organisationen tun können, um sich auf die Einführung von NIS2 vorzubereiten.

NIS2 im Überblick

Da immer mehr große Unternehmen die NIS2-Vorgaben in die Risiko-Management-Programme für ihre Lieferanten einbinden, müssen heute die meisten Unternehmen den Bestimmungen genügen, um wettbewerbsfähig zu bleiben.

NIS2 ist eine aktualisierte Fassung der ursprünglichen NIS-Richtlinie, die darauf abzielt, die Cybersicherheit von Unternehmen und öffentlichen Einrichtungen in der Europäischen Union zu verbessern, die wichtige und kritische Infrastrukturen für die europäische Wirtschaft bereitstellen. Die ursprüngliche NIS-Richtlinie wurde 2016 verabschiedet und trat im Mai 2018 in Kraft. Die NIS2 wurde vom Europäischen Parlament und anschließend vom Rat im November 2022 förmlich angenommen. Sie trat am 16. Januar 2023 in Kraft. Jetzt bleibt den Mitgliedstaaten bis 17. Oktober 2024 Zeit, die Maßnahmen in nationales Recht umzusetzen.

Die NIS2 gilt für alle Einrichtungen mit mindestens 50 Beschäftigten und einem Jahresumsatz von 10 Mio. EUR, die wichtige oder kritische Dienste für die europäische Wirtschaft und Gesellschaft erbringen. Dazu gehören auch Unternehmen und Zulieferer mit Sitz außerhalb der EU, die Dienstleistungen innerhalb der EU ausführen. Auch wenn die Richtlinie Ausnahmen für kleine Unternehmen vorsieht, ist davon auszugehen, dass größere Unternehmen die NIS2-Vorgaben in ihre Lieferanten-Management-Systeme aufnehmen werden. Schlussendlich werden also die meisten Organisationen die NIS2 umsetzen müssen, um wettbewerbsfähig zu sein.

Die Richtlinie verpflichtet die von der NIS2 betroffenen Unternehmen und Einrichtungen, geeignete und angemessene technische und organisatorische Maßnahmen zu ergreifen, um die Risiken für die Sicherheit von Netz- und Informationssystemen sowie für die physische Umgebung (einschließlich der Rechenzentren) zu mindern. Außerdem nimmt sie die Unternehmen und Einrichtungen in die Pflicht, relevante Sicherheitsvorfälle proaktiv den zuständigen Behörden zu melden, und definiert besonders strenge Meldepflichten für Anbieter von digitalen Infrastrukturdiensten.

Wie Sie sich auf NIS2 vorbereiten

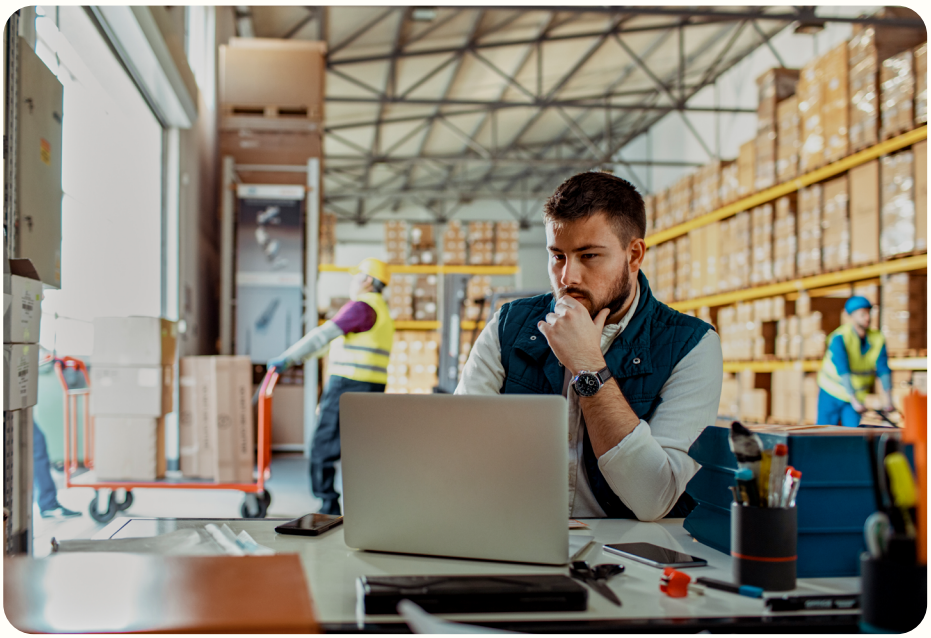
Die EU-Mitgliedstaaten haben bis Oktober 2024 Zeit, die NIS2-Richtlinie in ihr nationales Recht zu übernehmen. Unternehmen sollten diese Zeit nutzen, um sich auf die Richtlinie vorzubereiten und die folgenden Schritte einzuleiten:

- **Identifizieren, bewerten und adressieren Sie Ihre Risiken:** Die NIS2 verpflichtet die Management-Teams wichtiger und kritischer Unternehmen und Einrichtungen, geeignete und angemessene technische, betriebliche und organisatorische Maßnahmen zu ergreifen, um die Risiken für die Sicherheit von Netz- und Informationssystemen und der physischen Umgebung zu minimieren. Unternehmen und Einrichtungen sollten ihre Risiken ermitteln, deren Auswirkungen bewerten und Maßnahmen zur Minimierung einleiten.
- **Bewerten Sie Ihr Security-Standing:** Die Evaluierung der Risiken und des Security-Standings kann Ihnen helfen, Schwachstellen wie nicht gemanagte Passwörter oder falsch konfigurierte oder inaktive Konten zu identifizieren, die potenziell dem Diebstahl von Zugangsdaten Vorschub leisten könnten. Unternehmen sollten daher ein umfassendes Security-Assessment durchführen, um ihr Security-Standing zu bewerten und Verbesserungsmöglichkeiten zu ermitteln – etwa die Einführung Phishing-resistenter Authentifizierungsfaktoren.
- **Ergreifen Sie geeignete Maßnahmen zum Schutz privilegierter Accounts:** Angreifer können privilegierte Accounts übernehmen, um Angriffe zu orchestrieren, kritische Infrastrukturen auszuschalten und wichtige Dienste herunterzufahren. NIS2 verpflichtet die betroffenen Unternehmen, den Zugang zu Admin-Konten zu beschränken und Passwörter mit Admin-Rechten regelmäßig zu ändern. Unternehmen sollten geeignete Maßnahmen zum Schutz privilegierter Zugänge ergreifen, etwa indem sie Best Practices wie Least Privilege Access, durchgängige Authentifizierung und Threat-Analysen umsetzen.

Oktober 2024

Die Deadline, bis zu der die NIS2 in nationales Recht umzusetzen ist

- **Schützen Sie sich vor Ransomware:** Teure und verheerende Ransomware-Angriffe sind in der EU nach wie vor eine enorme Herausforderung, und ein wichtiger Grund, warum die EU-Regulierungsbehörden die NIS2-Richtlinie entwickelt haben. Unternehmen sollten geeignete Security-Lösungen und Best Practices einführen, um sich proaktiv gegen Ransomware zu schützen. Hierzu gehören beispielsweise der Einsatz von Endpoint Privilege Security zur Durchsetzung des Least-Privilege-Access-Prinzips, strenge Anwendungskontrollen sowie zeitgemäße Lösungen in den Bereichen Next Generation Antivirus (NGAV) und Endpoint Detection & Response (EDR).
- **Implementieren Sie eine Zero-Trust-Strategie:** Klassische perimeterbasierte Security-Architekturen, die entwickelt wurden, um eine klar definierte Netzwerkgrenze zu verteidigen, sind für die moderne Welt der Cloud-Services und hybriden Workforces nicht geeignet. Implementieren Sie stattdessen einen Zero-Trust-Ansatz mit mehreren Verteidigungsebenen – etwa Least Privilege Access, durchgängiger Authentisierung und Threat-Analysen – um sämtliche Zugriffe zu validieren.
- **Stellen Sie Ihre Software-Lieferkette auf den Prüfstand:** Angriffe auf die Lieferkette sind ein wichtiges Anliegen der EU-Regulierungsbehörden und ein Hauptgrund für die Entwicklung der NIS2-Richtlinie. Unternehmen sollten ihre Software-Lieferkette kritisch untersuchen und darüber nachdenken, diese mit einer Secrets-Management-Lösung besser zu schützen.



Der Stellenwert der Identitäten für die NIS2-Compliance

Security ist nicht leicht, weil sie stets ein komplexes Zusammenspiel von Menschen, Prozessen und Technologie umfasst. In diesem Umfeld kommt der Identität eine Schlüsselrolle zu: Sie dient als Eckpfeiler moderner Cybersecurity-Strategien und als zentrale Komponente zur Aufrechterhaltung einer robusten Cyberhygiene – auch mit Blick auf die Einhaltung von Compliance-Vorgaben wie NIS2.

Identität ist das tragende Fundament, in dem die Security-Policies, die Betriebsabläufe und die IT-Systeme verankert sind, die den Zugang zu kritischen Informationen schützen. Hierzu gehört auch die Verifizierung der Benutzeridentitäten, die Authentifizierung der Zugänge, die Autorisierung der Aktivitäten und Berechtigungen sowie die Verwaltung von der Zugriffskontrollen. Eine wirksame Identity Governance stellt sicher, dass nur autorisierte Anwender Zugang zu geschützten Ressourcen erhalten – und dass sie diese Ressourcen nur mit den geringsten Privilegien, die zur Erfüllung ihrer Aufgaben erforderlich sind, nutzen können. Zusätzliche Security-Ebenen wie die Multi-Faktor-Authentifizierung können den Schutz der Identitäten weiter verbessern.

Mit Blick auf die Einhaltung gesetzlicher Vorgaben wie NIS2 dient die Identität als leistungsfähiges Instrument zur Minimierung der mit unbefugten Zugriffen verbundenen Risiken. Darüber hinaus stellen starke Identitäten die Rechenschaftspflicht innerhalb des Unternehmens sicher: Sie ermöglichen die Identifizierung von Personen, die für Handlungen verantwortlich sind, und vereinfachen so die Rückverfolgbarkeit. Das Identitätsmanagement bildet zudem die Grundlage für ein effizientes Benutzermanagement, das die administrativen Abläufe rationalisiert und die Sicherheit über das gesamte Unternehmen hinweg verbessert. Mit einem robusten Identity Management profitieren Sie außerdem von einem transparenten Prüfpfad für Ihre kritischen Anwendungen, der es Ihnen leicht macht, Zugriffe zurückzuverfolgen und Berechtigungen lückenlos zu managen.

Identität ist das tragende Fundament, in dem die Security-Policies, die Betriebs-abläufe und die IT-Systeme verankert sind, die den Zugang zu kritischen Informationen schützen.

Hier sind einige Beispiele, wie Sie ein starkes Identity Management bei der Einhaltung der NIS2-Compliance unterstützt:

1. **Zugangskontrolle:** Ein robustes Management der Benutzeridentitäten ermöglicht es Unternehmen, eine strenge Zugangskontrolle durchzusetzen. Indem sie jedem Anwender und jedem Bereich eine eindeutige Identität zuweisen, können Unternehmen sicherstellen, dass nur autorisierte Personen auf sensible Ressourcen zugreifen und bestimmte Aktionen innerhalb ihres Netzes und ihrer IT durchführen können.
2. **Authentisierung und Autorisierung** Ein starkes Identity Management vereinfacht die Implementierung robuster Authentifizierungs-mechanismen, etwa von Multi-Faktor-Authentifizierung. So können Unternehmen die Identität jedes Nutzers überprüfen, bevor Zugang gewährt wird. Darüber hinaus können Unternehmen granulare Autorisierungsrichtlinien definieren, um sicherzustellen, dass Benutzer je nach Rolle und Verantwortlichkeit über die richtigen Privilegien und Berechtigungen verfügen.
3. **Incident Response:** Im Falle eines Angriffs kommt dem Identity Management eine Schlüsselrolle zu, wenn es gilt, die beteiligten Anwender und Bereiche zu identifizieren. Ein robustes Identitäts-management ermöglicht es den Unternehmen, die Aktivitäten in ihren Systemen zu verfolgen – und so die Weichen für eine zuverlässige Incident Response und eine effiziente Fehlerbehebung zu stellen.
4. **Monitoring der Compliance:** Die NIS2 verpflichtet Unternehmen und Einrichtungen, geeignete Maßnahmen zur Minimierung der Risiken für die Sicherheit ihrer Netzwerke und Informationssysteme zu implementieren. Ein starkes Identity Management ermöglicht es Unternehmen, Benutzeraktivitäten zu überwachen und zu dokumentieren, um so die Einhaltung der Vorgaben zu gewährleisten. Auf diese Weise können die Unternehmen auch jederzeit ihrer Rechenschaftspflicht nachkommen, da sie wissen, wer wann auf bestimmte Ressourcen zugegriffen hat.

Unternehmen, denen der hohe Stellenwert der digitalen Identitäten für die Security und Compliance bewusst ist, sind sehr gut positioniert, um ihre kritischen Informationen zuverlässig zu schützen, die Einhaltung von Compliance-Vorgaben sicherzustellen und eine resiliente und sichere Umgebung zu schaffen.

Das holistische, identitäts-zentrierte Security-Framework von Okta

Okta setzt beim Identitätsmanagement auf einen ganzheitlichen Ansatz, der die digitalen Identitäten des Unternehmens ebenso zuverlässig schützt wie seine Anwender, seine Anwendungen und seine Devices. Okta ist bewusst, dass jeder Nutzer – ob Mensch oder Maschine – privilegierte Rechte erlangen und zum Sicherheitsrisiko werden kann. Daher stehen für uns die Identitäten im Fokus, wenn es gilt, eine robuste Cyberhygiene zu implementieren – gerade im Kontext von Zero Trust.

Okta legt den Fokus auf wirksame und individualisierbare Lösungen, die den Zugang zu Daten regulieren und wertvolle Informationen schützen. Das Portfolio umfasst darüber hinaus durchgängige Lösungen für die Authentifizierung und Autorisierung von Zugriffen gemäß den Prinzipien von Zero Trust. Okta ermöglicht es Unternehmen, Zugriffe auf Cloud-Ressourcen streng zu kontrollieren und Benutzeraktivitäten kontinuierlich zu überwachen und zu dokumentieren – und schafft so die Voraussetzungen für eine lückenlose Einhaltung von Compliance-Vorgaben und für die nachhaltige Minimierung von Risiken. Die Umsetzung einer umfassenden Identity-Strategie ist ein entscheidender Schritt, um kritische Infrastrukturen zuverlässig vor Bedrohungen wie Cyberattacken, Ransomware und Software-Supply-Chain-Schwachstellen zu schützen.

Darüber hinaus hilft sie Unternehmen dabei, die Anforderungen von Artikel 21 der NIS2 zu erfüllen, der Maßnahmen zum Risikomanagement in der Cybersecurity sowie verbindliche Meldepflichten umfasst – und eine breite Palette von Empfehlungen enthält. Okta bietet eine Vielzahl von Security-Lösungen, die Cyberbedrohungen stoppen und die Identitäten und sensiblen Daten der Unternehmen schützen – darunter auch eine leistungsstarke, Phishing-resistente Multi-Faktor-Authentifizierung, wie sie von NIS2 ausdrücklich gefordert wird.

Die Implementierung einer ganzheitlichen Identity-Strategie ist ein zentraler Schritt, um Cyberangriffe, Ransomware und Software-Supply-Chain-Schwachstellen zu stoppen.

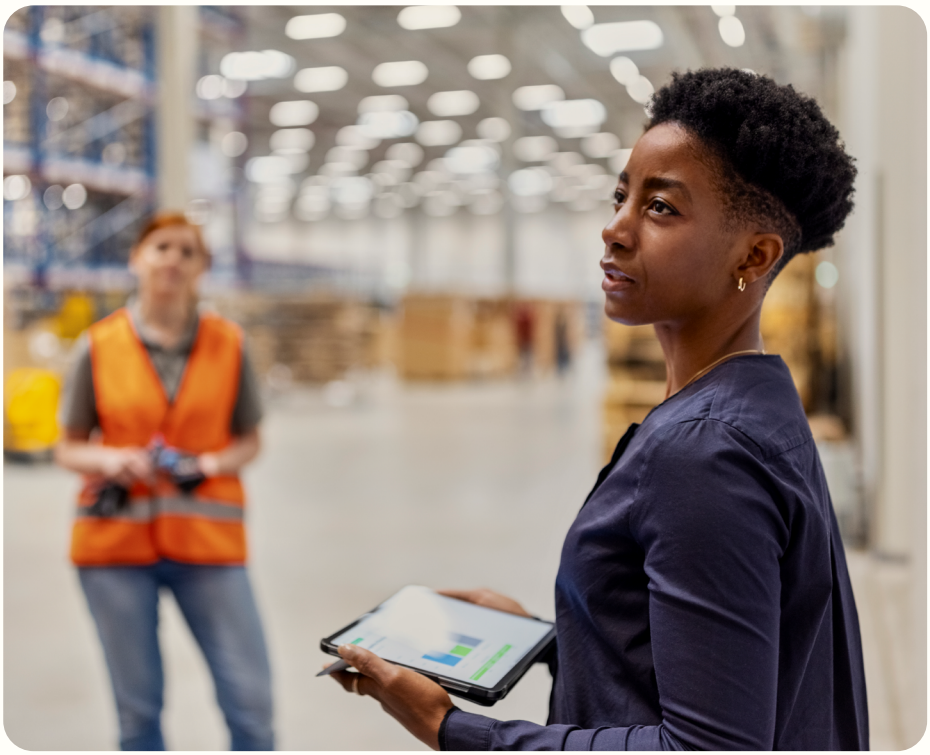
Die Plattform von Okta ist skalierbar und flexibel und ermöglicht es Unternehmen, über alle Systeme und Umgebungen hinweg eine Policy-basierte Authentifizierung zu implementieren. Dies ermöglicht es Kunden, innovative Services bereitzustellen, die Usability zu verbessern und die Einhaltung von Datenschutz- und Security-Vorgaben sicherzustellen.

Die Okta Workforce Identity Cloud (WIC) ist eine leistungsfähige Plattform, die den Zugang für jeden Benutzer – ob Mitarbeiter, Lieferant oder Geschäftspartner – schützt, ganz egal, wo sie sich befinden und welches Device sie verwenden. Auf diese Weise hilft sie den Verantwortlichen der Unternehmen dabei, die Produktivität und Effizienz zu steigern, ihre IT und ihre Infrastrukturen zu modernisieren und das Security-Standing zu stärken.

Mit ihren einfach konfigurierbaren Policies ermöglicht es die Okta Workforce Identity Cloud (WIC) den Kunden, granulare Security-Maßnahmen für jede Risikokategorie umzusetzen – und dabei stets das richtige Gleichgewicht zwischen Security und Usability zu finden. Funktionalitäten wie Single Sign-On (SSO), adaptive Multi-Faktor-Authentifizierung (MFA) und passwortlose Authentifizierung ermöglichen es Unternehmen, ihr Security-Standing zu verbessern und ihren Mitarbeitern jederzeit eine hochwertige Experience zu bieten.

API Access Management, Advanced Server Access und Access Gateway helfen Unternehmen, ihre Management-Prozesse zu zentralisieren, privilegierte Zugriffe zu schützen und die gesamte Konfiguration zu automatisieren. All das trägt maßgeblich zur Effizienz im täglichen Betrieb bei. Okta Identity Governance (OIG) führt Okta Workflows, Okta Lifecycle Management und Okta Access Governance in einer durchgängigen Lösung zusammen, um dynamische Bedrohungen zu stoppen und die Effizienz zu optimieren.

Kurz: Ein modernes Identity-Framework wie die Workforce Identity Cloud hilft den Unternehmen dabei, die Weichen für die durchgängige Einhaltung der NIS2-Vorgaben zu stellen: Sie verbessert das Security-Standing, implementiert ein robustes Access-Management und garantiert die zuverlässige und hochverfügbare Bereitstellung zeitgemäßer Identitätsdienste.



Konsequenzen bei Nicht-Einhaltung der NIS2-Vorgaben

10 Millionen Euro

oder 2 % des Jahresumsatzes bei Nichteinhaltung der NIS2 – je nachdem, was höher ist.

Die Nichteinhaltung der NIS2 kann dazu führen, dass Unternehmen mit Bußgeldern belegt werden. Die NIS2-Richtlinie unterscheidet zwischen kritischen Einrichtungen und wichtigen Einrichtungen. Zu den ersteren gehören öffentliche und private Unternehmen in Sektoren wie Verkehr, Energie und Versorgung, Gesundheitswesen, öffentliche Verwaltung und digitale Infrastruktur (einschließlich Cloud-Service-Anbieter), die mit einem Bußgeld von 10 Mio. EUR oder 2 % des weltweiten Jahresumsatzes (je nachdem, welcher Wert höher ist) belegt werden können. Wichtige Einrichtungen, zu denen öffentliche und private Unternehmen in Sektoren wie Lebensmittelversorgung, Chemie, Postdienste, Abfallwirtschaft, Fertigung usw. gehören, können mit Bußgeldern in Höhe von bis zu 7 Mio. EUR oder 1,4 % des weltweiten Jahresumsatzes (je nachdem, welcher Wert höher ist) belegt werden. Darüber hinaus sieht Artikel 32 Absatz 5 vor, dass bei kritischen Unternehmen, die die vorgesehenen Maßnahmen nicht durchsetzen, ihre Zertifizierungen eingefroren werden können und ihr Geschäftsführer von seinen Führungsaufgaben enthoben werden kann.

NIS2 und der Schutz Ihrer Supply Chain

Angesichts der potenziell verheerenden Folgen von Ereignissen wie der Pandemie ist auch die Gewährleistung intakter und sicherer Lieferketten ein grundlegender Aspekt der NIS2.

Um das Risiko von Cyberangriffen über Dritte zu minimieren, müssen Unternehmen das Risiko-Standing ihrer Supply Chain regelmäßig bewerten – und sogar noch mehr: Sie müssen darüber hinaus sicherstellen, dass ihre Lieferanten im täglichen Business ebenfalls die Vorgaben der NIS2 einhalten. Hierzu gehört nicht zuletzt die Umsetzung der Sicherheits-maßnahmen entlang der gesamten Lieferkette, beispielsweise die Durchführung von Risikobewertungen und Audits bei Lieferanten, die Ausarbeitung entsprechender vertraglicher Vereinbarungen, in denen die Security-Vorgaben spezifiziert sind, und die laufende Überwachung und Kommunikation mit den Lieferanten. Wenn Unternehmen sicherstellen, dass ihre Zulieferer die aktualisierten NIS2-Anforderungen einhalten, können sie ihr Gesamtrisiko nachhaltig reduzieren und die Sicherheit ihrer digitalen Infrastruktur stärken. Unternehmen sollten von ihren Lieferanten erwarten, dass sie nach Industriestandard (z. B. ISO 27001) erstellte Berichte sowie externe Penetrationstests vorweisen – und ihren Kunden auch die Möglichkeit geben, eigene Penetrationstests durchzuführen.

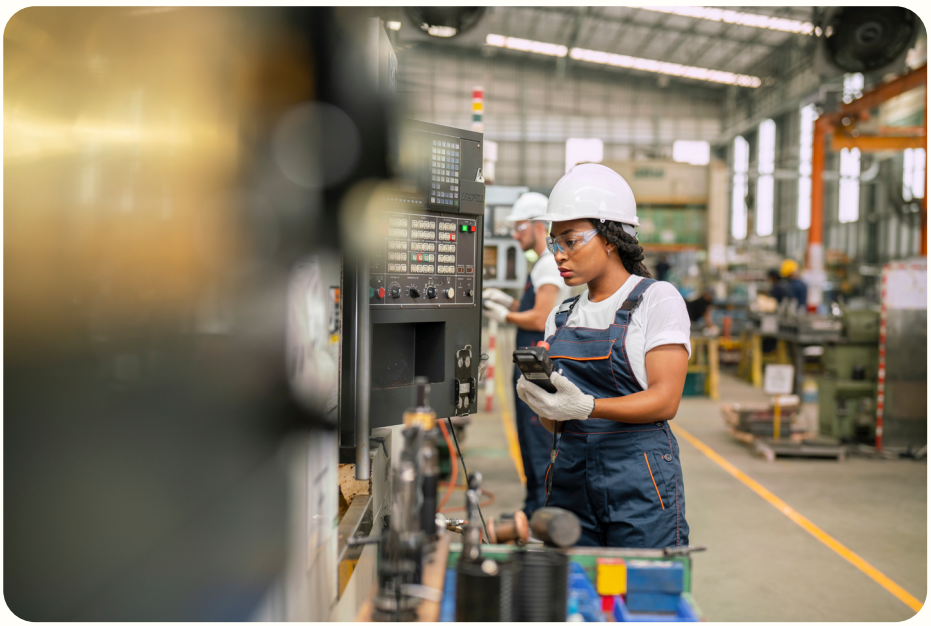
Die Workforce Identity Cloud (WIC) und die Customer Identity Cloud (CIC) von Okta umfassen leistungsfähige Lösungen zum Schutz der Identitäten in B2B- und B2C-Beziehungen und können damit die Einhaltung der NIS2-Vorgaben maßgeblich erleichtern.

Formalisieren Sie Ihren Response-Plan

Die NIS2-Verordnung verpflichtet Unternehmen zur zeitnahen Meldung aller sicherheitsrelevanten Zwischenfälle. Der erste Bericht muss innerhalb von 24 Stunden nach einem Event eingereicht werden, gefolgt von einem technischen Bericht innerhalb von 72 Stunden. Um diesen Anforderungen gerecht zu werden, brauchen Unternehmen einen klar strukturierten Incident-Response-Plan. Okta kommt dabei eine entscheidende Rolle zu, da unsere Lösungen den Kunden einen umfassenden Einblick in die Berechtigungen und Zugriffsversuche geben – und das über alle Infrastrukturen und Technologien hinweg. Diese Funktionalität hilft Unternehmen maßgeblich bei der Rekonstruktion der Vorgänge im Netzwerk und der Zugriffe auf die Ressourcen und leistet damit einen wichtigen Beitrag zur Dokumentation und Meldung der Vorfälle. Um die Einhaltung der NIS2-Anforderungen zu gewährleisten, empfehlen wir, die Prozesse zur Meldung von Vorfällen, zur Erfassung von Informationen und zur Berichterstellung kritisch auf den Prüfstand zu stellen. Um die Wirksamkeit des Incident-Response-Plans bewerten und verbessern zu können, haben sich darüber hinaus regelmäßige Übungen bewährt.

Machen Sie Ihr Team fit

Die NIS2 betont dabei insbesondere die Bedeutung von Schulungen zur Cybersicherheit und Cyberhygiene für Mitarbeiter, Lieferanten und Drittanbieter. Arbeiten Sie darüber hinaus kontinuierlich an der Schärfung der Cyber-Awareness der Mitarbeiter, und fördern Sie eine auf Sicherheit fokussierte Unternehmenskultur. Achten Sie darauf, dass Ihre Mitarbeiter ihre Rolle beim Schutz der Netzwerk- und Informationssysteme kennen und sich der potenziellen Risiken und Bedrohungen bewusst sind.

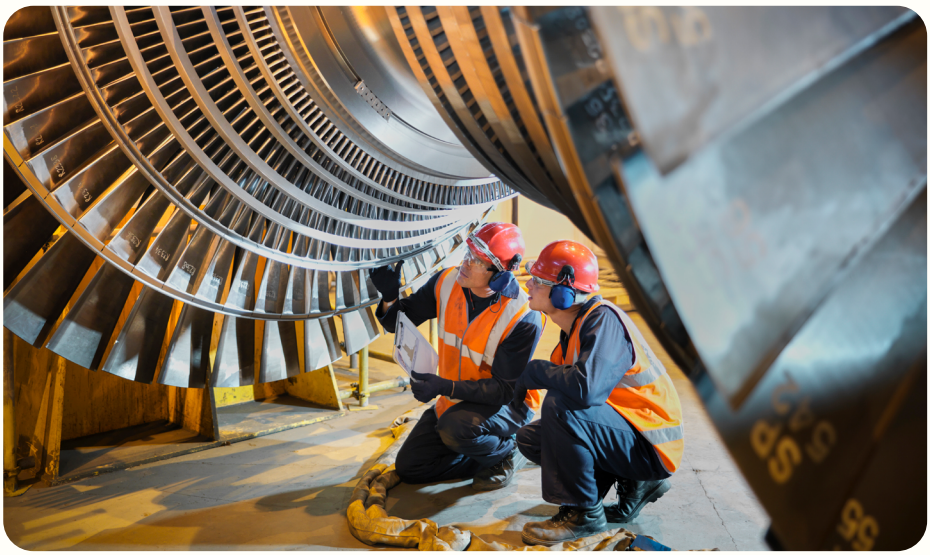


Wie NIS2 und ISO 27001 zusammenhängen

Die ISO 27001 ist eine internationale Norm für das Management der Informationssicherheit und liefert einen detaillierten Rahmen für die Einrichtung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems (ISMS). Als internationaler Standard soll sie Unternehmen und Einrichtungen dabei helfen, ihre IT-Security-Risiken zu managen und ihre wertvollen Informationen zu schützen.

NIS2 und ISO 27001 haben also das gleiche Ziel: die Sicherheit von Netzwerk- und Informationssystemen zu verbessern. Das bedeutet auch, dass sich die NIS2 in Teilbereichen mit der ISO 27001 überschneidet. Organisationen können ihre bestehende ISO 27001-Zertifizierung also nutzen, um die NIS2-Anforderungen zu erfüllen.

Die folgende Tabelle zeigt eine grobe, nicht vollständige Korrelation zwischen den Anforderungen der NIS2-Richtlinie der EU und den ISO 27001-Kontrollen aus Anhang A der Norm ISO/EIC 27001:2023. In Anbetracht der Komplexität und der spezifischen Ziele und Aufgabenbereiche dieses Gedankenspiels ist es wichtig, darauf hinzuweisen, dass dieser allgemeine Abgleich nicht vollständig ist. Spezialisierte Fachleute sollten eine gründliche, auf den konkreten Kontext Ihres Unternehmens zugeschnittene Analyse durchführen. Dennoch ist die folgende Tabelle ein guter Ausgangspunkt. Um die NIS2 vollumfänglich mit der ISO 27001 abzugleichen, sollte Ihr Unternehmen eine Gap-Analyse durchführen. So können Sie fundiert die Bereiche identifizieren, in denen ihre ISO 27001-Implementierung bislang hinter den Anforderungen von NIS2 zurückbleibt. Im nächsten Schritt gilt es dann, Ihr ISMS zu aktualisieren, um diese Lücken zu schließen und die Einhaltung beider Normen zu gewährleisten.



Bereich	NIS2-Anforderungen	Relevante ISO 27001-Kontrollen
Risikomanagement	Fordert, dass Unternehmen über Risikomanagement-Prozesse verfügen	A.6.1 (Interne Organisation) A.8 (Asset Management) A.12.1 (Betriebliche Verfahren und Zuständigkeiten)
Sicherheit von Systemen und Anlagen	Fordert von den Unternehmen, dass sie die Sicherheit ihrer Netzwerke und Informationssysteme gewährleisten	A.11 (Physische und Umgebungssicherheit) A.12.1 (Betriebliche Verfahren und Zuständigkeiten) A.13 (Kommunikationssicherheit) A.14 (Erwerb, Entwicklung und Wartung von Systemen)
Umgang mit sicherheitsrelevanten Vorfällen	Unternehmen und Einrichtungen sollten darauf vorbereitet sein, schnell und angemessen auf sicherheitsrelevante Vorfälle zu reagieren	A.16 (Management von Informationssicherheitsvorfällen) A.12.6 (Management technischer Schwachstellen)
Business Continuity Management	Unternehmen und Einrichtungen sollten über Pläne verfügen, die die Kontinuität ihrer Dienste gewährleisten	A.17 (Aspekte der Informationssicherheit im Rahmen des Managements der Betriebskontinuität)
Monitoring, Auditierung und Tests	Unternehmen und Einrichtungen sollten regelmäßig Audits und Tests durchführen, um ihre Sicherheits-maßnahmen zu validieren	A.18.2 (Interne Revision) A.12.7 (Überlegungen zur Prüfung von Informationssystemen)
Einhaltung gesetzlicher und vertraglicher Bestimmungen	Unternehmen und Einrichtungen sollten alle geltenden gesetzlichen und vertraglichen Sicherheits-anforderungen einhalten	A.18 (Compliance) A.15.2 (Informationssicherheit im Projektmanagement)
Meldung von Sicherheitsvorfällen	Unternehmen und Einrichtungen sollten Vorfälle mit weitreichenden Auswirkungen melden	A.16.1 (Management von Informationssicherheitsvorfällen und Verbesserungen)
Supply Chain Security	Unternehmen und Einrichtungen sollten die Sicherheit innerhalb ihrer Lieferkette gewährleisten	A.15 (Lieferantenbeziehungen)

Fazit

Die NIS2 ist eine umfangreiche Cybersecurity-Verordnung der EU, die die Sicherheit von Netzwerk- und Informationssystemen von Unternehmen verbessern soll, die wichtige und kritische Infrastrukturen betreiben. Unternehmen und Einrichtungen, die von der Richtlinie betroffen sind, sollten eine Reihe von Schritten einleiten, um sicherzustellen, dass sie den Anforderungen genügen. Dazu gehört die Identifizierung und Minimierung von Risiken, die Bewertung des Security-Standings, der Schutz privilegierter Zugriffe, die Stärkung der Ransomware-Abwehr, die Einführung einer Zero-Trust-Strategie, die Validierung der Software-Lieferkette, die Formalisierung der Incident Response und die Schulung der Mitarbeiter.

Eine Reihe von Frameworks für Cybersecurity und Informationssicherheit deckt diese Anforderungen bereits gut ab. Eine davon ist die ISO 27001. Wenn Unternehmen die NIS2 und die ISO 27001 miteinander abgleichen, werden sie feststellen, dass sie ihre bestehende ISO 27001-Zertifizierung nutzen können, um die Einhaltung der NIS2-Anforderungen zu dokumentieren – und so Zeit und Ressourcen sparen. Schlussendlich kann die Einhaltung der NIS2- und ISO 27001-Vorgaben den Unternehmen dabei helfen, Cybersecurity-Risiken zu minimieren, ihre wertvollen Informationen zu schützen und das Vertrauen ihrer Kunden und Stakeholder zu gewinnen.

Wenn Sie mehr darüber wissen möchten, wie die Okta Workforce Identity Cloud, die Okta Customer Identity Cloud und andere Lösungen Ihr Unternehmen bei der Einhaltung der NIS2-Vorgaben unterstützen können, **wenden Sie sich an unser Team**.

Über Okta

Mehr dazu erfahren Sie unter: www.okta.com/de. Okta ist der führende unabhängige Anbieter von Identity-Lösungen für Entwickler und Unternehmen. Die Okta Identity Cloud verbindet Unternehmen sicher mit ihren Kunden, Partnern und Mitarbeitenden. Mit tiefen Integrationen für über 7.000 Anwendungen ermöglicht die Okta Identity Cloud einfache und sichere Zugriffe – für jeden User und jedes Device.

Tausende von Kunden – darunter 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn und News Corp – setzen auf Okta, um schneller zu arbeiten, ihren Umsatz zu steigern und sicher zu bleiben. Okta ermöglicht es Kunden, die Technologien, auf die sie bei ihrer Arbeit angewiesen sind, einfach und sicher einzusetzen – und ihre Aufgaben auf diese Weise schneller zu erledigen.

© Okta 2023. Alle Rechte vorbehalten.

okta

Niederlassung München
Salvatorplatz 3
80333 München
info_germany@okta.com
+49 (89) 26203329