2025

Was sich mit der NIS 2-Richtlinie ändert

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

Warum starkes Identity-Management für NIS 2-Compliance wichtig ist

okta

Inhalt

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 NIS 2-Richtlinie aktualisiert. Diese verschärft abermals die Sicherheitsmaßnahmen und Meldepflichten und weitet den Anwendungsbereich auf neue Sektoren aus.

Das vorliegende Whitepaper soll einen Überblick über die NIS 2-Richtlinie geben und aufzeigen, wie diese Richtlinie mit gängigen Sicherheits-Frameworks wie ISO 27001 kombiniert werden kann, wie wichtig digitale Identitäten (Identities) in diesem Kontext sind und was Unternehmen tun können, um sich auf die Einhaltung der NIS 2-Richtlinie vorzubereiten.

Die NIS 2-Richtlinie im Überblick

Da immer mehr große Unternehmen die NIS 2-Vorgaben in die Risiko-Management-Programme für ihre Lieferanten einbinden, müssen heute die meisten Unternehmen den Bestimmungen genügen, um wettbewerbsfähig zu bleiben.

Die NIS 2-Richtlinie 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 NIS 2-Richtlinie wurde vom Europäischen Parlament und anschließend vom Rat im November 2022 förmlich angenommen. Sie trat am 16. Januar 2023 in Kraft, und den Mitgliedstaaten blieb bis 17. Oktober 2024 Zeit, die Maßnahmen in nationales Recht umzusetzen.

Die NIS 2-Richtlinie gilt für alle Unternehmen und Einrichtungen, die wichtige oder kritische Dienste für die europäische Wirtschaft und Gesellschaft erbringen, mindestens 50 Beschäftigte haben und einen Jahresumsatz von 10 Millionen EUR oder mehr erzielen. 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 NIS 2-Vorgaben in ihre Lieferanten-Management-Systeme aufnehmen werden. Schlussendlich werden also die meisten Unternehmen und Einrichtungen die NIS 2-Richtlinie umsetzen müssen, um wettbewerbsfähig zu sein.

Die Richtlinie verpflichtet die 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 die NIS 2-Richtlinie vorbereiten

Da die NIS 2-Richtlinie jetzt in Kraft ist, müssen Unternehmen schnell handeln und die folgenden Schritte einleiten, um die Vorgaben einzuhalten:

- **Identifizieren, bewerten und adressieren Sie Ihre Risiken.** Die NIS 2-Richtlinie 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 identifizieren, deren Auswirkungen bewerten und Maßnahmen zur Minimierung einleiten.
- **Bewerten Sie Ihre Sicherheitslage.** Die Evaluierung der Risiken und der Sicherheitslage kann Ihnen helfen, Schwachstellen wie nicht verwaltete Passwörter oder falsch konfigurierte oder inaktive Konten zu identifizieren, die dem Diebstahl von Zugangsdaten Vorschub leisten könnten. Unternehmen sollten daher eine umfassende Sicherheitsanalyse durchführen, um ihre Sicherheitslage zu bewerten und Verbesserungsmöglichkeiten zu identifizieren, z. B. 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. Die NIS 2-Richtlinie verpflichtet die betroffenen Unternehmen, den Zugang zu Admin-Konten zu beschränken und Passwörter für diese Accounts regelmäßig zu ändern. Unternehmen sollten geeignete Maßnahmen zum Schutz privilegierter Zugriffe ergreifen, etwa indem sie Best Practices wie Zugriff nach dem Least-Privilege-Prinzip, durchgängige Authentifizierung und Bedrohungsanalysen umsetzen.

- **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 NIS 2-Richtlinie entwickelt haben. Unternehmen sollten geeignete Sicherheitslösungen und Best Practices einführen, um sich proaktiv gegen Ransomware zu schützen. Hierzu gehören beispielsweise der Einsatz von Endpoint-Privilege-Management-Lösungen zur Durchsetzung des Least-Privilege-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 Sicherheitsarchitekturen, die für den Schutz klar definierter Netzwerkgrenzen entwickelt wurden, sind für die moderne Welt der Cloud-Services und hybriden Arbeitsmodelle nicht geeignet. Implementieren Sie stattdessen einen Zero-Trust-Ansatz mit mehreren Verteidigungsebenen (z. B. Zugriff nach dem Least-Privilege-Prinzip, durchgängige Authentifizierung und Bedrohungsanalysen), 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 NIS 2-Richtlinie. Unternehmen sollten ihre Software-Lieferkette kritisch untersuchen und darüber nachdenken, diese mit einer Secrets-Management-Lösung besser zu schützen.

Die Bedeutung des Identity-Managements für die NIS 2-Compliance

Sicherheit ist nicht leicht, weil sie stets ein komplexes Zusammenspiel von Menschen, Prozessen und Technologie umfasst. In diesem Umfeld kommt der digitalen Identity-Management eine Schlüsselrolle zu: Es dient als Eckpfeiler moderner Cybersicherheitsstrategien und als zentrale Komponente zur Aufrechterhaltung einer robusten Cyberhygiene – auch mit Blick auf die Einhaltung von Compliance-Vorgaben der NIS 2-Richtlinie.

Identity-Management-Systeme sind das tragende Fundament für die Sicherheitsrichtlinien, die Betriebsabläufe und die IT-Systeme, die den Zugriff auf kritische Informationen schützen. Hierzu gehört auch die Verifizierung der Benutzeridentitäten, die Authentifizierung der Zugriffe, die Autorisierung der Aktivitäten und Berechtigungen sowie die Verwaltung der Zugriffskontrollen. Wirksame Identity Governance stellt sicher, dass nur autorisierte Benutzer Zugriff auf geschützte Ressourcen erhalten und dabei nur über die Berechtigungen verfügen, die zur Erledigung ihrer Aufgaben erforderlich sind. Mit Sicherheitsebenen wie Multi-Faktor-Authentifizierung können Sie den Identity-Schutz noch weiter verbessern.

Mit Blick auf die Einhaltung gesetzlicher Vorgaben wie NIS 2 dient die digitale Identität als leistungsfähiges Instrument zur Minimierung der mit unbefugten Zugriffen verbundenen Risiken. Darüber hinaus stellen starkes Identity-Management die Rechenschaftspflicht innerhalb des Unternehmens sicher: Sie ermöglichen die Identifizierung von Personen, die für Handlungen verantwortlich sind, und vereinfachen so die Rückverfolgbarkeit. Identity-Management bildet zudem die Grundlage für effizientes Benutzermanagement, das die administrativen Abläufe rationalisiert und die Sicherheit im gesamten Unternehmen verbessert. Mit robustem Identity-Management profitieren Sie außerdem von einem transparenten Prüfpfad für Ihre kritischen Anwendungen, der es Ihnen leicht macht, Zugriffe zurückzuverfolgen und Berechtigungen lückenlos zu verwalten.

Identity-Management-Systeme sind das tragende Fundament für die Sicherheitsrichtlinien, die Betriebsabläufe und die IT-Systeme, die den Zugriff auf kritische Informationen schützen.

Hier sind einige Beispiele, wie Sie starkes Identity-Management bei der Einhaltung der NIS 2-Vorgaben unterstützt:

1. **Zugriffskontrollen:** Durch die angemesse Verwaltung von Benutzeridentitäten können Unternehmen strenge Zugriffskontrollen durchsetzen. Indem sie jedem Benutzer bzw. jeder Entität eine eindeutige Identity zuweisen, können Unternehmen sicherstellen, dass nur autorisierte Personen auf sensible Ressourcen zugreifen und bestimmte Aktionen innerhalb ihres Netzwerks und ihrer IT-Systeme durchführen können.
2. **Authentifizierung und Autorisierung:** Starkes Identity-Management vereinfacht die Implementierung robuster Authentifizierungsmechanismen, etwa von Multi-Faktor-Authentifizierung. So können Unternehmen die Identität jedes Benutzers überprüfen, bevor Zugriff 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 robustem Identity Management eine Schlüsselrolle zu, da es Unternehmen die Identifizierung der beteiligten Benutzer und Entitäten sowie die Nachverfolgung der Aktivitäten in ihren Systemen ermöglicht – und damit die Weichen für effiziente Untersuchungen, Attributionen und Fehlerbehebungen stellt.
4. **Compliance-Überwachung:** Die NIS 2-Richtlinie verpflichtet Unternehmen und Einrichtungen, geeignete Maßnahmen zur Minimierung der Risiken für die Sicherheit ihrer Netzwerke und Informationssysteme zu implementieren. 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.
5. **Business Continuity:** Die NIS 2-Richtlinie legt großen Wert auf die Gewährleistung des unterbrechungsfreien Geschäftsbetriebs als kritische Komponente des Risikomanagements im Bereich Cybersicherheit. Ein zuverlässiges System für Identitäts- und Zugriffsmanagement (IAM) mit Funktionen für Hochverfügbarkeit und Disaster Recovery trägt erheblich dazu bei, da Ausfallzeiten minimiert und schnelle Wiederherstellungen nach einer Störung gewährleistet werden. Durch die Implementierung starker IAM-Prozesse können Unternehmen die operative Resilienz steigern und kritische Daten und Systeme schützen. Damit kommen Sie der NIS 2-Verpflichtung für Backup-Management und Disaster Recovery nach.

Unternehmen, denen der hohe Stellenwert der digitalen Identitäten für Sicherheit 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 ganzheitliche Identity-zentrierte Sicherheits-Framework von Okta

Okta setzt bei Identity-Management auf einen ganzheitlichen und einheitlichen Ansatz, der die digitalen Identitäten des Unternehmens ebenso zuverlässig schützt wie seine Anwender, Anwendungen und Geräte. Okta ist bewusst, dass jeder Benutzer – ob Mensch oder Maschine – privilegierte Berechtigungen erlangen und zum Sicherheitsrisiko werden kann. Daher steht für uns bei der Implementierung robuster Cyberhygiene – und ganz besonders bei der Implementierung eines Zero-Trust-Frameworks – zuverlässiges Identity-Management im Fokus.

Okta konzentriert sich auf wirksame und anpassbare Lösungen, die den Zugriff auf Daten regulieren und wertvolle Informationen schützen. Das Portfolio umfasst darüber hinaus durchgängige Lösungen für die Authentifizierung und Autorisierung von Zugriffen nach dem Zero-Trust-Prinzip. 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 die 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 dieser Ansatz Unternehmen dabei, die Anforderungen von Artikel 21 der NIS 2-Richtlinie zu erfüllen, der Maßnahmen für das Management von Cybersicherheitsrisiken sowie verbindliche Meldepflichten umfasst – und eine breite Palette von Empfehlungen enthält. Okta bietet eine Vielzahl von Sicherheitslösungen, die Cyberbedrohungen stoppen und die Identities und sensiblen Daten der Unternehmen schützen – darunter auch eine leistungsstarke, Phishing-resistente Multi-Faktor-Authentifizierung, wie sie von NIS 2 ausdrücklich gefordert wird.

Okta Platform ist skalierbar sowie flexibel und ermöglicht es Unternehmen, für alle Systeme und Umgebungen eine richtlinienbasierte Authentifizierung zu implementieren. Dies ermöglicht es Kunden, innovative Services bereitzustellen, die Benutzerfreundlichkeit zu verbessern und die Einhaltung von Datenschutz- und Sicherheitsvorschriften sicherzustellen.

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

Okta Workforce Identity ist eine leistungsfähige Lösung, die den Zugang für alle Benutzer – Mitarbeiter, Lieferanten und Geschäftspartner – unabhängig davon schützt, wo sie sich gerade befinden und welches Gerät 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 die Sicherheitslage zu stärken. Dank der einfach konfigurierbaren Richtlinien können Kunden mit Okta Workforce Identity für jede Risikokategorie granulare Sicherheitsmaßnahmen umsetzen – und dabei stets das richtige Gleichgewicht zwischen Sicherheit und reibungsloser User Experience finden. Funktionalitäten wie Single Sign-On (SSO), adaptive Multi-Faktor-Authentifizierung (MFA) und passwortlose Authentifizierung ermöglichen es Unternehmen, ihre Sicherheitslage zu verbessern und ihren Mitarbeitern jederzeit hochwertige User Experiences 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.

Identity Threat Protection (ITP) bietet einen Sicherheitsansatz, mit dem Unternehmen potenzielle Bedrohungen proaktiv erkennen, sich davor schützen und darauf reagieren können, bevor sie eskalieren. Dadurch wird die Gesamtsicherheit verbessert.

Kurz: Ein modernes Identity-Framework wie Okta Workforce Identity hilft Unternehmen, die Weichen für die durchgängige Einhaltung der NIS 2-Vorgaben zu stellen: Die Sicherheitslage wird verbessert, robustes Zugriffsmanagement wird implementiert und die zuverlässige Bereitstellung hochverfügbarer, zeitgemäßer Identity-Services wird garantiert.

Feature	Beschreibung	Vorteil für die Compliance
Single Sign-On (SSO)	Vereinfachter sicherer Zugriff auf Anwendungen im gesamten Unternehmen.	Reduziert das Risikopotenzial von Anmeldedaten-Diebstahl, da die Passwortnutzung auf einem Minimum gehalten wird, wodurch die operative Kontinuität gewährleistet und die operative Resilienz gestärkt wird.
Adaptive Multi-Factor Authentication (AMFA)	Kontextbezogene Authentifizierung basierend auf Benutzerverhalten und Risikofaktoren.	Stärkt die Sicherheit, indem sichergestellt wird, dass nur autorisierte Benutzer auf vertrauliche Systeme zugreifen können, sodass Risiken durch Cyberbedrohungen minimiert werden.
Lifecycle Management (LCM)	Automatisierte Provisionierung und Deprovisionierung, damit die richtigen Benutzer über die richtigen Zugriffsrechte verfügen.	Vereinfacht das Zugriffsmanagement und gewährleistet, dass Benutzer während des gesamten Beschäftigungszyklus über geeignete Zugriffsebenen verfügen, was für die Gewährleistung der operativen Resilienz erforderlich ist.
Privileged Access Management (PAM)	Durchsetzung von Zugriff nach dem Least-Privilege-Prinzip für kritische Accounts und Ressourcen.	Reduziert das Risiko von nicht autorisierten Zugriffen auf vertrauliche Informationen.
Workflows	No-Code-Automatisierung für Identity-bezogene Prozesse (z. B. Zugriffsprüfungen, Incident-Response-Prozesse und Reporting).	Automatisiert wichtige Identity-Management-Prozesse und ermöglicht effizientes Incident-Response- und Compliance-Reporting.
Okta Device Assurance (ODA)	Verifizierung des Sicherheitsstatus von Geräten, die auf das Unternehmen zugreifen.	Gewährleistet, dass nur sichere, konforme Geräte auf Unternehmensressourcen zugreifen können; entspricht NIS 2-Fokus auf Endpoint-Schutz.
Identity Threat Protection mit Okta AI	Kontinuierliche Überwachung des Benutzerrisikos und der Session-Integrität, inkl. automatischer Aktionen wie Beendigung von Sessions, Aufforderungen zu zusätzlicher Authentifizierung bei erkannten Risiken, außerdem Bereitstellung Identity-bezogener Ereignis- und Erkennungsprotokolle.	Hilft Unternehmen bei der Erfüllung von Compliance-Vorgaben mit Aktivitätenüberwachung, schneller Incident Response und detaillierten Protokollen für Audit, die Verantwortbarkeit, Transparenz und Compliance gewährleisten.
Okta Identity Governance (OIG)	Vereinfachtes Identity-Management durch automatische Provisionierung und Deprovisionierung, Verwaltung von Berechtigungen und Zugriffen, Unterstützung benutzerdefinierter Workflows und Bereitstellung detaillierter Aktivitätsprotokolle, zentrale Zugriffskontrolle und ein Self-Service-Portal für Benutzerzugriffsanforderungen.	Hilft bei der Beseitigung von Risiken durch nicht autorisierte Zugriffe, indem gewährleistet wird, dass nur Personen mit geeigneten Anmeldedaten auf wichtige Funktionen zugreifen können; dadurch wird die Wahrscheinlichkeit operativer Ausfälle verringert.

Konsequenzen bei Nicht-Einhaltung der NIS 2-Vorgaben

10 Mio. €

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

Die Nichteinhaltung der NIS 2-Vorgaben kann dazu führen, dass Unternehmen mit Bußgeldern belegt werden. Die NIS 2-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 Millionen 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 Millionen 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.

Die NIS 2-Richtlinie und der Schutz Ihrer Lieferkette

Angesichts der potenziell verheerenden Folgen von Ereignissen wie der Pandemie ist auch die Gewährleistung intakter und sicherer Lieferketten ein grundlegender Aspekt der NIS 2-Richtlinie.

Um das Risiko von Cyberangriffen über Dritte zu minimieren, müssen Unternehmen die Risikolage ihrer Lieferkette regelmäßig bewerten – und sogar noch mehr: Sie müssen darüber hinaus sicherstellen, dass ihre Lieferanten im täglichen Business ebenfalls die NIS 2-Vorgaben einhalten. Hierzu gehört nicht zuletzt die Umsetzung der Sicherheitsmaßnahmen entlang der gesamten Lieferkette, beispielsweise die Durchführung von Risikobewertungen und Audits bei Lieferanten, die Ausarbeitung entsprechender vertraglicher Vereinbarungen, in denen die Sicherheitsvorgaben spezifiziert sind, und die laufende Überwachung und Kommunikation mit den Lieferanten. Wenn Unternehmen sicherstellen, dass ihre Zulieferer die aktualisierten NIS 2-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 Okta-Lösungen schützen Identities in B2B- und B2C-Beziehungen und können damit die Einhaltung der NIS 2-Vorgaben maßgeblich erleichtern.

Formalisieren Sie Ihren Incident-Response-Plan

Die NIS 2-Richtlinie verpflichtet Unternehmen zur zeitnahen Meldung aller sicherheitsrelevanten Vorfälle. Der erste Bericht muss innerhalb von 24 Stunden nach einem Ereignis eingereicht werden, gefolgt von einem technischen Bericht innerhalb von 72 Stunden. Um diesen Anforderungen gerecht zu werden, benötigen 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 NIS 2-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 NIS 2-Richtlinie betont 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 die NIS 2-Richtlinie und ISO 27001 zusammenhängen

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 Informations-Sicherheits-Management-Systems (ISMS). Als internationaler Standard soll sie Unternehmen und Einrichtungen dabei helfen, ihre IT-Sicherheitsrisiken zu managen und ihre wertvollen Informationen zu schützen.

NIS 2 und ISO 27001 haben also das gleiche Ziel: die Verbesserung der Sicherheit von Netzwerk- und Informationssystemen. Das bedeutet auch, dass sich die NIS 2-Richtlinie in Teilbereichen mit der ISO 27001 überschneidet. Unternehmen können ihre bestehende ISO 27001-Zertifizierung also nutzen, um die NIS 2-Anforderungen zu erfüllen.

Die folgende Tabelle zeigt eine grobe, nicht vollständige Korrelation zwischen den Anforderungen der NIS 2-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 Vorgaben der NIS 2-Richtlinie vollumfänglich mit denen der ISO 27001 abzugleichen, sollte Ihr Unternehmen eine Gap-Analyse durchführen. Auf diese Weise können Sie fundiert die Bereiche identifizieren, in denen ihre ISO 27001-Implementierung bislang hinter den NIS 2-Anforderungen zurückbleibt. Im nächsten Schritt gilt es dann, Ihr ISMS zu aktualisieren, um diese Lücken zu schließen und die Einhaltung beider Normen zu gewährleisten.

Bereich	NIS 2-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 Informations-systeme 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)
Absicherung der Lieferkette	Unternehmen und Einrichtungen sollten die Sicherheit innerhalb ihrer Lieferkette gewährleisten	A.15 (Lieferantenbeziehungen)

Fazit

Die NIS 2 ist eine umfangreiche Cybersicherheitsverordnung der EU, die die Sicherheit von Netzwerk- und Informationssystemen von Unternehmen verbessern soll, die wichtige und kritische Infrastrukturen betreiben. Von der Richtlinie betroffene Unternehmen und Einrichtungen, sollten mit einer Reihe von Schritten sicherstellen, dass sie die Vorgaben einhalten. Dazu gehört die Identifizierung und Minimierung von Risiken, die Bewertung der Sicherheitslage, 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 Vorgaben von NIS 2 und ISO 27001 miteinander abgleichen, werden sie feststellen, dass sie ihre bestehende ISO 27001-Zertifizierung nutzen können, um die Einhaltung der NIS 2-Anforderungen zu dokumentieren – und so Zeit und Ressourcen sparen. Schlussendlich kann die Einhaltung der NIS 2- und ISO 27001-Vorgaben Unternehmen dabei helfen, Cybersicherheitsrisiken zu minimieren, ihre wertvollen Informationen zu schützen und das Vertrauen ihrer Kunden und Stakeholder zu gewinnen.

Wenn Sie mehr darüber erfahren möchten, wie Okta Ihr Unternehmen bei der Einhaltung der NIS 2-Vorgaben unterstützen kann, **wenden Sie sich an unser Team**.

Über Okta

Okta ist das weltweit führende Identity-Unternehmen™. Wir schützen die Identity, damit unsere Kunden und Partner jede Technologie sicher nutzen können. Unsere Lösungen unterstützen Unternehmen sowie Entwickler dabei, mit Identity-Management die Sicherheit und Effizienz zu steigern und die Ziele zu erreichen. Gleichzeitig werden Benutzer, Mitarbeiter und Partner zuverlässig geschützt. Weltweit führende Marken vertrauen bei Authentifizierung, Autorisierung und mehr auf Okta. Weitere Informationen finden Sie unter okta.com/de.

okta

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