Ihre Checkliste für NIS 2-Compliance:

Wie Sie sich in 7 Schritten vorbereiten

Die NIS 2-Richtlinie der Europäischen Union nimmt Unternehmen in die Pflicht, ihre Cybersicherheit zu verbessern, regelmäßig Audits durchzuführen und sicherheitsrelevante Vorfälle frühzeitig zu melden. Verpflichtend ist die Einhaltung der Vorgaben vor allem für Unternehmen, die kritische Dienste bereitstellen – aber auch für alle, die diese Anbieter als Lieferanten unterstützen oder unterstützen möchten. Die folgenden Schritte tragen dazu bei, dass Ihr Unternehmen die NIS 2-Vorgaben einhält.

1 Identifizieren Sie Ihre Cyberrisiken

Schwachstellen können sich in Ihrem Netzwerk, Ihren Systemen und Anlagen verbergen und Sie einem Risiko aussetzen. Ein gutes Beispiel sind nicht verwaltete Passwörter oder falsch konfigurierte oder inaktive Accounts, die dem Diebstahl von Zugangsdaten Vorschub leisten. Evaluieren Sie die Sicherheitsmaßnahmen Ihres Unternehmens sorgfältig, um Probleme zu identifizieren, ihre Auswirkungen abzuschätzen und Maßnahmen zur Behebung einzuleiten.

Was Sie tun müssen

Führen Sie eine unternehmensweite Risikobewertung durch und entwickeln Sie einen Plan zur Reduzierung der Schwachstellen.

2 Stärken Sie die Zugriffskontrollen

Wenn Sie Datenschutzverstöße verhindern wollen, müssen Sie unbefugte Zugriffe auf Systeme und Benutzerkonten verhindern. Stellen Sie die Weichen für eine strenge Zugriffskontrolle – mit einer starken Identity-Plattform, die die Benutzerverwaltung zentralisiert und mit granularen Autorisierungsrichtlinien sicherstellt, dass nur autorisierte Anwender auf bestimmte Ressourcen zugreifen und bestimmte Aktionen durchführen können.

Was Sie tun müssen

Integrieren Sie starke Identity-Governance, um strengere Zugriffskontrollen zu ermöglichen.

3 Schützen Sie privilegierte Zugriffe

Angreifer können privilegierte Accounts übernehmen, um Angriffe zu orchestrieren, kritische Infrastrukturen auszuschalten und wichtige Dienste herunterzufahren. Schützen Sie privilegierte Accounts, indem Sie den Zugang zu Admin-Konten beschränken und die Passwörter für diese Accounts regelmäßig ändern.

Was Sie tun müssen

Schützen Sie privilegierte Accounts mit Best Practices wie Zugriff nach dem Least-Privilege-Prinzip.

4 Implementieren Sie Phishing-resistente MFA

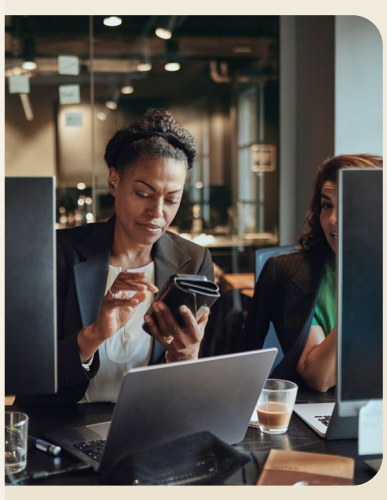
Social-Engineering-Angriffe sind auf dem Vormarsch. Daher fordert die NIS 2-Richtlinie von Unternehmen die Implementierung einer Phishing-resistenten Multi-Faktor-Authentifizierung (MFA). Diese bietet zusätzlichen Schutz bei der Authentifizierung von Mitarbeitern, Kunden und Lieferanten, ohne deren digitale User Experience zu beeinträchtigen.

Was Sie tun müssen

Nutzen Sie Phishing-resistente MFA, um die Authentifizierung ohne Mehraufwand für die Benutzer zu verbessern.

5 Schützen Sie sich vor Ransomware

Einer der Hauptgründe für die Einführung der NIS 2-Richtlinie sind die verheerenden und kostspieligen Ransomware-Angriffe der vergangenen Jahre. Implementieren Sie Sicherheitslösungen, die diese Angriffe proaktiv stoppen, zum Beispiel Endpoint-Privilege-Management-Lösungen zur Durchsetzung des Least-Privilege-Prinzips. Überwachen Sie darüber hinaus die Anwendungen in Ihrer Umgebung und integrieren Sie zeitgemäße Lösungen für Virenschutz und Endpoint Detection & Response.



Was Sie tun müssen

Integrieren Sie dedizierte Sicherheitslösungen zum Schutz vor Ransomware, etwa im Bereich Endpoint-Privilege-Management.

6 Stellen Sie Ihre Software-Lieferkette auf den Prüfstand

Die von Ihnen verwendete Software von Drittanbietern könnte mit schädlichem Code infiziert sein. Werfen Sie einen genauen Blick auf Ihre Software-Lieferkette – und denken Sie darüber nach, eine dedizierte Secrets-Management-Lösung zum Schutz sensibler Daten (etwa der Passwörter und Keys) zu implementieren.

Was Sie tun müssen

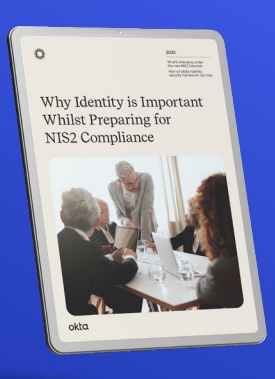
Prüfen Sie, ob eine Secrets-Management-Lösung das Risiko von Angriffen auf die Lieferkette verringern würde.

7 Implementieren Sie eine Zero-Trust-Strategie

Klassische perimeterbasierte Sicherheitsarchitekturen sind für die moderne, offene Welt der Cloud-Dienste und hybriden Arbeitsmodelle nicht geeignet. Denken Sie darüber nach, einen zeitgemäßen Zero-Trust-Ansatz zu implementieren und durch starkes Identity-Management zu unterstützen, das Zugriffe nach dem Least-Privilege-Prinzip, durchgängige Authentifizierung und Bedrohungsanalysen integriert.

Was Sie tun müssen

Setzen Sie auf eine Identity-basierte Zero-Trust-Strategie, um Benutzern die richtigen Zugriffsrechte auf die richtigen Ressourcen zur richtigen Zeit zu ermöglichen.



Erfahren Sie mehr über NIS 2-Compliance und starkes Identity-Management

Die digitale Identität ist das Fundament für den Schutz der Zugriffe auf kritische Informationen. Robustes Identity-Management ermöglicht es Unternehmen, den Zugriff auf Ressourcen zu kontrollieren, die Authentifizierung zu stärken und die Rechenschaftspflicht mit einem klar dokumentierten Audit-Pfad zu belegen.

Wenn Sie mehr darüber wissen möchten, wie starkes Identity-Management Ihr Unternehmen bei der Einhaltung der NIS 2-Vorgaben unterstützt, lesen Sie unser Whitepaper „Warum starkes Identity-Management für NIS 2-Compliance wichtig ist“.

Whitepaper herunterladen

© Okta 2025. Alle Rechte vorbehalten.