okta

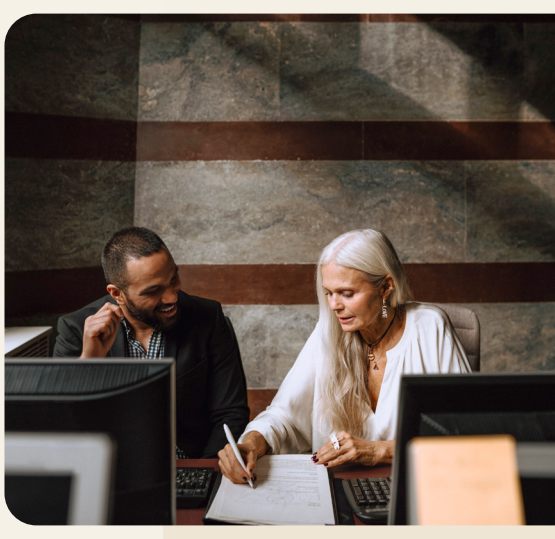
Ihre Checkliste für die NIS2-Compliance:

Wie Sie sich in 7 Schritten vorbereiten

Die bevorstehende NIS2-Richtlinie der Europäischen Union nimmt Unternehmen in die Pflicht, ihre Cybersecurity 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 bereiten Ihr Unternehmen auf die NIS2 vor.

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 ungemanagte Passwörter oder falsch konfigurierte oder inaktive Konten, die dem Diebstahl von Zugangsdaten Vorschub leisten. Evaluieren Sie die Sicherheitsmaßnahmen Ihres Unternehmens sorgfältig, um Probleme zu identifizieren, ihre Folgen abzuschätzen und Maßnahmen zur Behebung einzuleiten.



Was Sie tun müssen

Führen Sie ein unternehmensweites Risiko-Assessment durch und entwickeln Sie einen Plan zur Schließung der Schwachstellen.

2 Stärken Sie die Zugangskontrolle

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

Was Sie tun müssen

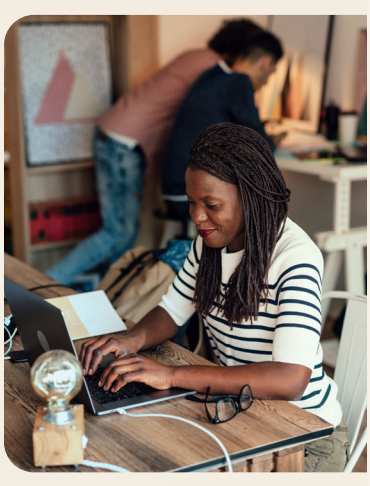
Integrieren Sie eine starke Identity-Governance, um strengere Zugriffskontrollen zu ermöglichen.

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 mit Admin-Rechten regelmäßig ändern.

Was Sie tun müssen

Schützen Sie privilegierte Konten mit Best Practices wie Least Privilege Access.



4 Implementieren Sie Phishing-resistente MFA

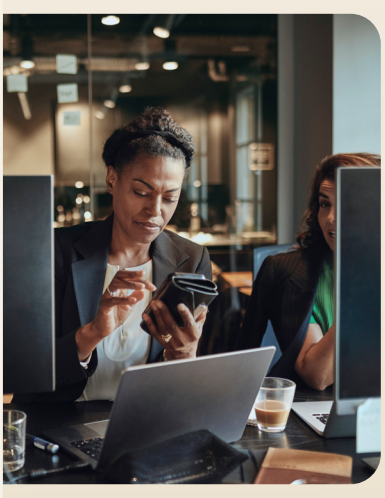
Social-Engineering-Angriffe sind auf dem Vormarsch. Daher fordert die NIS2 von Unternehmen die Implementierung einer Phishing-resistenten Multi-Faktor-Authentifizierung (MFA). Diese bietet zusätzlichen Schutz bei der Authentifizierung von Mitarbeitern, Kunden und Lieferanten, ohne deren digitale Experience zu beeinträchtigen.

Was Sie tun müssen

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

5 Schützen Sie sich vor Ransomware

Einer der Hauptgründe für die Einführung der NIS2 sind die verheerenden und kostspieligen Ransomware-Angriffe der vergangenen Jahre. Implementieren Sie Security-Lösungen, die diese Angriffe proaktiv stoppen, zum Beispiel Endpoint-Privilege-Management-Lösungen zur Durchsetzung von Least Privilege. Überwachen Sie darüber hinaus die Anwendungen in Ihrer Umgebung und integrieren Sie zeitgemäße Antivirus- und Endpoint-Detection-&-Response-Lösungen.



Was Sie tun müssen

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

6 Stellen Sie Ihre Software-Lieferkette auf den Prüfstand

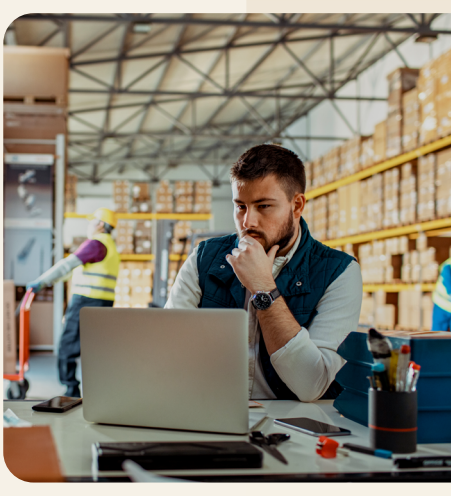
Die von Ihnen verwendete Software von Drittanbietern könnte mit bösartigem Code infiziert sein. Werfen Sie einen genauen Blick auf Ihre Software-Lieferkette – und denken Sie darüber nach, eine dedizierte Secrets-Management-Lösung zum Schutz sensibler Daten (etwa der Passwörter und Keys) zu implementieren.

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 Security-Architekturen sind für die moderne, offene Welt der Cloud-Dienste und der hybriden Workforces nicht geeignet. Denken Sie darüber nach, einen zeitgemäßen Zero-Trust-Ansatz zu implementieren und durch ein starkes Identitätsmanagement zu unterstützen, das Least Privilege Access, durchgängige Authentisierung und Threat-Analysen integriert.



Was Sie tun müssen

Setzen Sie auf eine Identity-basierte Zero-Trust-Strategie, um Anwendern den richtigen Zugang zu den richtigen Ressourcen zur richtigen Zeit zu ermöglichen.

Erfahren Sie mehr über NIS2 und starke Identitäten

Die Identität ist das Fundament für den Schutz der Zugriffe auf kritische Informationen. Ein robustes Identitätsmanagement 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 starke Identitäten Ihre Unternehmen bei der NIS2-Compliance unterstützen, lesen Sie unser Whitepaper **„Warum starke Identitäten zur Vorbereitung der NIS2-Compliance wichtig sind“**.

Zum Download

okta