CHECKLISTE

NIS2-Richtlinie: Das müssen Sie wissen

In 8 Schritten zu mehr Cybersicherheit -
mit unserer Checkliste bereiten Sie sich optimal vor

Ihre Ansprechpartner:

Friedhelm Otto
Bereichsleiter Cloud Security & Infrastructure

Sebastian Nipp
Bereichsleiter Cloud Security & Infrastructure

Gerardo Immordino
Bereichsleiter Managed Modern Endpoint

novaCapta

NIS2 Anforderungen im Überblick

Die EU-Cybersicherheitsrichtlinie NIS2 muss bis 17. Oktober 2024 in nationales Gesetz umgewandelt und anschließend rechtsverbindlich von betroffenen Unternehmen bis Ende Q4/2024 umgesetzt werden.

NIS2 baut auf früheren Rechtsvorschriften wie NIS1 und DSGVO auf, ergänzt diese jedoch um neue, höhere Anforderungen.

Im Vergleich zu bestehenden Gesetzen und Kontrollrahmen legt NIS2 einen stärkeren Schwerpunkt auf Sicherheit und Geschäftskontinuität, einschließlich der Sicherheit der Lieferkette.

Die konkreten Anforderungen umfassen folgende vier Ziele und entsprechende Prinzipien:

1. **Sicherheitsrisiko verwalten:**
   Governance, Risikomanagement, Assetmanagement, Lieferkettenmanagement

2. **Schutz vor Cyberangriffen:**
   Richtlinie und Verfahren zum Schutz von Diensten, Identitäts- und Zugangskontrolle, Datensicherheit, Sicherheit des Systems, widerstandsfähige Netze und Systeme, Sensibilisierung und Schulung des Personals

3. **Cybersicherheitsvorfälle erkennen:**
   Sicherheitsüberwachung, proaktive Erkennung von Sicherheitsereignissen

4. **Minimierung der Auswirkungen von Sicherheitsvorfällen:**
   Reaktions- und Wiederherstellungsplan, gelernte Lektionen

Durch NIS2 werden deutlich mehr Unternehmen als zuvor (über 160.000) in die Pflicht genommen, zusätzlich steigen Berichtspflicht und Durchsetzungsdruck durch z.B. höhere Sanktionen und die Haftung der Managementebene.

Die EU-Cybersicherheitsrichtlinie NIS2 muss bis zum 17. Oktober 2024 in nationales Gesetz umgewandelt und anschließend rechtsverbindlich von betroffenen Unternehmen bis Ende Q4/2024 umgesetzt werden.

Nutzen Sie unsere Checkliste, um sich optimal auf die Umsetzung der NIS2-Richtlinie vorzubereiten!

1 Prüfen Sie, ob NIS2 Ihr Unternehmen betrifft.

Die NIS2-Richtlinie identifiziert **18 kritische Sektoren**, die in solche mit hoher Kritikalität und sonstige kritische Sektoren unterteilt werden:

Sektoren mit hoher Kritikalität:

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten
- Öffentliche Verwaltung
- Weltraum

Sonstige kritische Sektoren:

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Chemie
- Verarbeitendes Gewerbe / Herstellung von Waren
- Anbieter digitaler Dienste
- Forschung
- Lebensmittel

Als weiteres Kriterium legt NIS2 die **Unternehmensgröße** fest. Unterschieden wird wie folgt:

Wichtige Einrichtungen:

- **Unternehmesgröße:** Mittel
- **Mitarbeitende**: ab 50
- **Jahresumsatz:** 10-50 Mio. € **ODER**
- **Jahresbilanzsumme:** bis 43 Mio. €

Wesentliche Einrichtungen:

- **Unternehmensgröße:** Groß
- **Mitarbeitende:** ab 250
- **Jahresumsatz:** ab 50 Mio. EUR **ODER**
- **Jahresbilanzsumme:** ab 43 Mio. €

2 Planen Sie Ressourcen und Budget ein und klären Sie Verantwortlichkeiten.

3 Führen Sie einen Readiness Check durch.

Beantworten Sie dabei u.a. folgenden Fragen:

- Setzen Sie **Kryptografie** und Verschlüsselung ein?
- Verwenden Sie **Multi-Faktor-Authentifizierung?**
- Verfügen Sie über eine grundlegende **Cybersicherheitshygiene** und -schulungen?
- Besteht eine umfassende **Sicherheitspolitik?**
- Haben Sie einen festgelegten Umgang sowohl mit **Vorfällen** als auch Schwachstellen und deren Offenlegung?
- Sorgen Sie für **Sicherheit in der Lieferkette** durch die Berücksichtigung von Schwachstellen bei Lieferanten?
- Erfolgen regelmäßige Bewertungen der Wirksamkeit von Maßnahmen zum **Management von Cybersicherheitsrisiken?**
- Können Sie die **Geschäftskontinuität** sicherstellen inkl. Krisenmanagement?

4 Risikomanagement: Identifizieren, bewerten und mindern Sie Sicherheitsrisiken.

5 Security Analyse: Ermitteln Sie Ihren aktuellen Status Quo zur IT-Sicherheit.

6 Setzen Sie ermittelte Maßnahmen um

indem Sie z.B.

- Sicherheitslücken schließen
- Fortschrittliche Lösungen für Endpoint Security einsetzen
- Zugriffsmanagement etablieren

7 Etablieren Sie klare und transparente Meldeverfahren.

8 Überprüfen Sie Ihre Sicherheitsverfahren kontinuierlich.

novaCapta

Sie benötigen Unterstützung?

Wir wissen, dass NIS2 eine komplexe Herausforderung darstellen kann und helfen Ihnen gerne dabei, die Konformität zu erreichen und anschließend auch kontinuierlich zu erhalten.

Wir verfügen über fundierte Erfahrung bei der Umsetzung grundlegender Sicherheitsmaßnahmen in Unternehmen, u.a. bestätigt durch unsere ISO 27001 Zertifizierung.

Als ausgezeichneter Microsoft Partner nutzen wir dabei die Vorteile umfassender Microsoft-Sicherheitslösungen wie z.B. Microsoft Defender for Cloud oder Microsoft Intune.

Im Rahmen unseres kostenfreien Compliance Navigators machen wir Sie mit den konkreten Grundlagen und Anforderungen von NIS2 vertraut und zeigen auf, wie Sie NIS2 mit Microsoft Technologien zu Ihrem Vorteil nutzen können.

Der abschließende Blick auf Best Practices und potenzielle Vorgehensweisen runden den 1,5-stündigen Erfahrungsaustausch ab.

Über novaCapta

Die novaCapta ist führender Microsoft Partner für den Mittelstand sowie große Unternehmen im DACH-Raum. Mit jahrelanger Erfahrung und als Microsoft Solutions Partner Cloud berät die novaCapta Kunden zu den für sie besten Microsoft Technologien und passt diese individuell auf spezifische Anforderungen an.

Unternehmen aller Branchen profitieren von der ganzheitlichen Digitalisierungsberatung und Lösungen für den Digital Workplace: Von der strategischen IT-Beratung, über Infrastruktur, Security, Kollaboration, Anwendungsentwicklung, Business Applications und KI-Lösungen bis hin zu Managed Services sowie Change & Adoption.

Ihre Ansprechpartner:

Friedhelm Otto
Bereichsleiter Cloud Security & Infrastructure

Sebastian Nipp
Bereichsleiter Cloud Security & Infrastructure

Gerardo Immordino
Bereichsleiter Managed Modern Endpoint