Factsheet NIS2-Richtlinie*

Die neue EU-Richtlinie zur Netz- und Informationssicherheit (NIS2) soll das Cybersicherheitsniveau in der Europäischen Union vereinheitlichen und erhöhen. Mit ihr werden Sicherheitsmaßnahmen für viele Unternehmen und Organisationen in 18 Sektoren verpflichtend. Auch für viele, die bisher nicht betroffen waren.

Wen betrifft die NIS2-Richtlinie?

Alle Unternehmen, die von Bedeutung für die Funktionsfähigkeit der Gesellschaft oder der Wirtschaft sind, zählen laut NIS2 zu den kritischen Diensten. Dabei wird zwischen „wesentlichen" und „wichtigen" Einrichtungen unterschieden.

Die NIS2-Richtlinie tritt im Oktober 2024 in Kraft.

Wesentliche Unternehmen und Organisationen

- ✓ **Großunternehmen** mit mehr als 249 Beschäftigten oder 50 Mio. Euro Umsatz und 43 Mio. Euro Bilanzsumme in den elf kritischen Sektoren:
  - Energie
  - Trinkwasser
  - Verkehr
  - Abwasser
  - Finanzmärkte
  - Weltraum
  - Gesundheitswesen
  - Digitale Infrastruktur
  - ICT-Dienste (B2B)
  - Öffentliche Verwaltung
- ✓ **Größenunabhängige Sonderfälle** wie DNS-Anbieter, Einrichtungen der Zentralregierung, alle bisherigen KRITIS-Unternehmen
- ✓ **Weitere Unternehmen oder Organisationen,** die von der Bundesregierung als „wesentlich" eingestuft werden – zum Beispiel aufgrund einer Monopolstellung.

Wichtige Unternehmen und Organisationen

- ✓ **Großunternehmen** mit mehr als 249 Beschäftigten oder 50 Mio. Euro Umsatz und 43 Mio. Euro Bilanzsumme in den sieben Sektoren:
  - Abfall
  - Chemie
  - Nahrungsmittel
  - Forschung
  - Fertigung
  - Digitale Dienste
  - Post- und Kurierdienste
- ✓ **Mittelständische Unternehmen** mit mindestens 50 Beschäftigten oder einem Umsatz von mehr als 10 Mio. Euro und einer Bilanzsumme von mehr als 10 Mio. Euro aus den elf kritischen Sektoren und den oben genannten sieben weiteren Sektoren.
- ✓ **Größenunabhängige Sonderfälle,** die von der Bundesregierung als "wichtig" eingestuft werden.

Quelle: https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html

Welche Cybersicherheitsmaßnahmen müssen betroffene Unternehmen umsetzen?

Um ihre IT-Infrastruktur und ihre Daten zu schützen, müssen wesentliche und wichtige Einrichtungen diverse (technische) Cybersicherheitsvorkehrungen und organisatorische Maßnahmen umsetzen:

- ✓ Interne Richtlinien zur Risikobewertung und zur Stärkung der Informationssicherheit
- ✓ Strategien zur Bewältigung von Sicherheitsvorfällen; Offenlegung von Schwachstellen
- ✓ Back-up-System, um Betriebsunterbrechungen und Versorgungsengpässe zu vermeiden
- ✓ Aufbau eines Krisenmanagements
- ✓ Lieferkettensicherheit herstellen
- ✓ Einkauf, Entwicklung und Wartung von sicheren IT- und Netzwerksystemen
- ✓ Überprüfung der Effektivität von Cybersicherheits- und Risikomaßnahmen
- ✓ Regelmäßige Mitarbeiterschulungen zur „Cyber Security Hygiene“
- ✓ Verschlüsselung der gesamten Kommunikation (Kryptographie)
- ✓ Personalsicherheit
- ✓ Zugangskontrollen etablieren
- ✓ Asset Management aufbauen
- ✓ Multi-Faktor-Authentifizierung einführen
- ✓ Sichere Sprach-, Video- und Textkommunikation
- ✓ Gesicherte Notfallkommunikationssysteme etablieren

Welche Meldepflichten haben die neuen KRITIS-Unternehmen?

Erhebliche Sicherheitsvorfälle müssen umgehend an die zuständigen Behörden gemeldet werden:

- ✓ **Innerhalb von 24 Stunden:** Frühwarnung an die Behörde
- ✓ **Nach 72 Stunden:** Detaillierter Bericht an die Behörde
- ✓ **Nach einem Monat:** Umfassender Fortschritts- und Abschlussbericht

Welche Sanktionen drohen bei Nichteinhaltung der NIS2-Richtlinie?

- ✓ **Wesentliche Einrichtungen:** bis zu 10 Millionen Euro oder 2 Prozent des Jahresumsatzes
- ✓ **Wichtige Einrichtungen:** bis zu 7 Millionen Euro oder 1,4 Prozent des Jahresumsatzes
- ✓ **Persönliche Haftung von Geschäftsführung und anderer Leitungsorgane**

Wie könnte ein Umsetzungsplan für die NIS2-Richtlinie aussehen?

1. Überprüfen, ob man unter die Richtlinie fällt
2. Risikobewertung und Ist-Analyse
3. Identifizieren von Schwachstellen und Handlungsfeldern
4. Priorisieren von Projekten und Erstellen eines Zeitplans
5. Einbeziehung aller Stakeholder
6. Mitarbeiterschulungen
7. Testen der Sicherheitsmaßnahmen
8. Regelmäßiges Überprüfen der Sicherheitsmaßnahmen

* Die Informationen in diesem Factsheet entsprechen dem Stand von November 2023. Es ist zu beachten, dass sich der rechtliche Rahmen in Bezug auf NIS2 ändern kann.