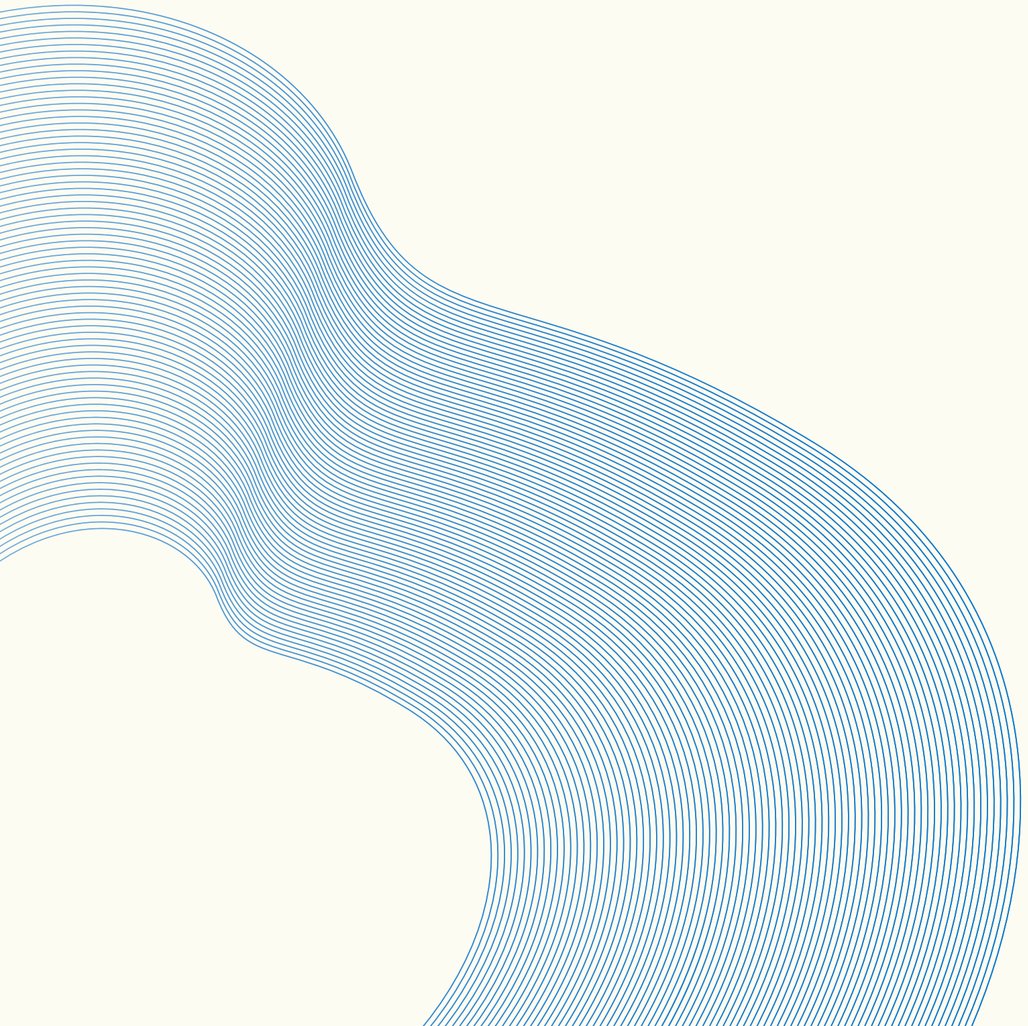
N.U.G. IT-Service GmbH

NIS2

Agenda



1. Allgemeines
2. Wer ist betroffen?
3. NIS2 gilt für (gelistete Sektoren)
4. Anforderungen
5. NIS2 Maßnahmen

Allgemeines

- Seit 2023 Richtlinie in Kraft (nicht direkt anwendbar) und muss bis 18.Oktober 2024 in nationales Recht umgesetzt werden

- Gibt Mindeststandart vor (Staaten dürfen strengere Vorschriften erlassen)

- Referentenentwurf für DE liegt vor

Wer ist betroffen?

NIS2 Nimmt wesentlich mehr Sektoren in die Verantwortung als die Vorgängerrichtlinie. Sicherheitsmaßnahmen und Meldepflichten müssen mindestens so wie von NIS2 vorgeschrieben umgesetzt werden

18 kritische Sektoren

Öffentliche und private Einrichtungen in 18 Sektoren mit mindestens 50 Beschäftigten oder mindestens 10 Mio. EUR Jahresumsatz und Jahresbilanzsumme

Sonderfälle

Unabhängig ihrer Größe (z.B. Gemeindeverwaltungen)

NIS2 gilt für:

Sektoren mit hoher Kritikalität (Anhang I der NIS2)

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten (B2B)
- Öffentliche Verwaltung
- Weltraum

Sonstige kritische Sektoren (Anhang II der NIS2)

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Produktion, Herstellung und Handel mit chemischen Stoffen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe/Herstellung von Waren
- Anbieter digitaler Dienste
- Forschung

Anforderungen

- Registrierung des Unternehmens bei einer nationalen Behörde

- Geschäftsführung haftet
- Maßnahmen überwachen
- Verpflichtende Schulungsteilnahme
- Mitarbeitern sollten ebenfalls Schulungen angeboten werden

- Frühwarnung (24 Std ab Kenntnis)
- Ausführlicher Bericht (72 Std ab Kenntnis)
- Abschluss- oder
- Fortschrittsbericht (1 Monat nach Meldung)

Maßnahmen zum Risikomanagement für Cybersicherheit

- **Policies:**
  Konzepte für Risikoanalyse und Sicherheit für Informationssysteme
- **Vorfallsbewältigung:**
  Erkennung, Analyse, Eindämmung und Reaktion auf Vorfälle
- **Business Continuity:**
  Backup-Management und Wiederherstellung, Krisenmanagement
- **Supply Chain:**
  Sicherheit in der Lieferkette
- **Einkauf:**
  Sicherheit bei Erwerb, Entwicklung und Wartung der IT-Systeme
- **Wirksamkeit:**
  Bewertung der Wirksamkeit der Risikomanagementmaßnahmen
- **Cyberhygiene, Schulung:**
  Cyberhygiene (z.B. Updates) und Schulungen in Cyber Security
- **Kryptografie:**
  Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
- **Personal, Zugriffe, Assets:**
  Personalsicherheit, Zugriffskontrolle und Asset Management
- **Authentifizierung:**
  Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung
- **Kommunikation:**
  Sichere Sprach-, Video- und Text-Kommunikation, ggf. auch im Notfall

Vielen Dank für Ihre Aufmerksamkeit

N.U.G. IT-Service GmbH

www.nug-it.de