TÜVIT

Inspired by Knowledge

NIS-2

Das Wichtigste auf einen Blick

Die Zeichen stehen auf NIS-2: Da ein Ausfall zu erheblichen Störungen und Einschränkungen führen würde, geraten Kritische Infrastrukturen (KRITIS) zunehmend ins Visier von Cyberkriminellen. Die Widerstandsfähigkeit dieser gegenüber Cyberbedrohungen zu stärken und das Cybersicherheitsniveau innerhalb der EU zu erhöhen, ist daher das erklärte Ziel der EU-Richtlinie NIS-2 („The Network and Information Security Directive“).

Mit NIS-2 kommen auf viele Unternehmen und Organisationen neue Verpflichtungen sowie umfangreiche Sicherheitsmaßnahmen zu. Wir prüfen initial, ob Sie zu den betroffenen Einrichtungen gehören, erarbeiten gemeinsam mit Ihnen erforderliche Maßnahmen und unterstützen Sie bei der erfolgreichen Umsetzung.

Wer ist von NIS-2 betroffen?

Die NIS-2-Richtlinie betrifft Betreiber von kritischen Infrastrukturen und digitalen Diensten in der EU und verpflichtet diese dazu, eine Reihe an Mindestanforderungen zu erfüllen, um die eigenen Systeme und Netzwerke gegen Cyberangriffe abzusichern.

Stichtag 17. Oktober 2024

Die neue EU-Richtlinie trat am 16. Januar 2023 in Kraft. Spätestens bis zum 17. Oktober 2024 ist sie ohne Übergangsfristen von den Mitgliedsstaaten in nationales Recht zu überführen. Hierfür liegt mit dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) ein Referentenentwurf des Bundesinnenministeriums vor.

NIS-2 – Das Wichtigste auf einen Blick

Unterscheidung zwischen „wesentlichen“ & „wichtigen“ Sektoren

Die NIS-2-Richtlinie differenziert neben dem Kriterium der Größe des Unternehmens (ab 50 Mitarbeitenden; Jahresumsatz von über 10 Mio. Euro) unter anderem zwischen wesentlichen und wichtigen Sektoren. Mit der Klassifizierung gehen unterschiedliche Aufsichtsregelungen einher.

WESENTLICHE SEKTOREN		WICHTIGE SEKTOREN	
▪ Energie	▪ Abwasser	▪ Post- & Kurierdienste	▪ Verarbeitendes Gewerbe/Herstellung von Waren
▪ Verkehr	▪ Digitale Infrastruktur	▪ Abfallbewirtschaftung	▪ Anbieter digitaler Dienste
▪ Bankwesen	▪ Verwaltung von ITK-Diensten (B2B)	▪ Chemikalien (Produktion, Herstellung und Handel)	▪ Forschung
▪ Finanzmarkt-infrastrukturen	▪ Öffentliche Verwaltung	▪ Lebensmittel (Produktion, Verarbeitung und Vertrieb)	
▪ Gesundheitswesen	▪ Weltraum		
▪ Trinkwasser			

Hinzu kommen – unabhängig von ihrer Größe – unter anderem weitere Kritische Infrastrukturen und zusätzliche Einrichtungen , die vom Staat als „wesentlich“ eingestuft werden.

Maßnahmen, die betroffene Unternehmen umsetzen müssen

1. **Risikomanagement:** Überwachung von Maßnahmen zur Minimierung von Cyberrisiken
2. **Verantwortlichkeit des Managements**
3. **Policies:** Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
4. **Vorfallbewältigung:** Prävention, Detektion und Bewältigung von Sicherheitsvorfällen
5. **Business Continuity:** Aufrechterhaltung des Betriebs (wie Backup-Management und Wiederherstellung nach einem Notfall) und Krisenmanagement
6. **Supply Chain:** Ausfallsicherheit der Lieferkette
7. **Einkauf:** Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen
8. **Wirksamkeit:** Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen
9. **Schulungen:** Cyberhygiene und Schulungen im Bereich der Cybersicherheit
10. **Kryptografie:** Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
11. **Personal, Zugriff & Asset-Management:** Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Assets
12. **Authentifizierung & Kommunikation:** Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme

Unsere Leistungen auf einen Blick

Betroffenheitsanalyse und Workshops

Gap-Analysen und Ziel-Maßnahmenplan

Beratung und Implementierung

Audits und Re-Audits

Über uns: DIGITALISIERUNG. SICHER. GESTALTEN. Wir beraten Kunden in ihrem Bestreben, das Vertrauen in robuste, hoch verfügbare IT-Infrastrukturen und -Organisationen zu stärken und begleiten Auftraggeber auf ihrem Weg der sicheren digitalen Transformation.

Kontakt: Carsten Keil | Tel.: +49 160 888 54 06 | c.keil@tuvit.de
TÜV NORD IT Secure Communications GmbH & Co. KG | Hohenzollerndamm 184 | 10713 Berlin
tuvit-consulting.de