NIS2-Richtlinie im Überblick

Was ist die NIS2-Richtlinie?

- NIS steht für **N**etz- und **I**nformations**s**icherheit.
- Ziel ist hohes gemeinsames Cyber-Sicherheitsniveau in Europa.
- Sie definiert neue Mindeststandards für die IT-Sicherheit in bestimmten Unternehmen oder Institutionen. So können die Länder neue strengere Vorschriften erlassen und durchsetzen.

Wann und wo gilt die NIS2-Richtlinie?

- NIS2 ist seit 2023 auf EU-Ebene in Kraft.
- NIS2 muss bis Oktober 2024 durch die EU-Mitgliedsstaaten in deren nationales Recht überführt werden.

Wen betrifft die NIS2-Richtlinie?

NIS2 betrifft öffentliche und private Einrichtungen in 18 Wirtschaftssektoren mit mindestens 50 Beschäftigten oder mindestens 10 Millionen Euro Jahresumsatz. Unter Umständen fallen auch Einrichtungen unabhängig von ihrer Größe unter NIS2. Das gilt beispielsweise für Teile der digitalen Infrastruktur oder der öffentlichen Verwaltung, KRITIS oder Unternehmen, die Teil einer Lieferkette bei betroffenen Einrichtungen sind.

Wichtig: NIS2 ist Chefsache! Zukünftig haften Führungskräfte der erfassten Einrichtungen für Verstöße gegen bestehende Vorschriften.

Welche 18 Sektoren sind von der NIS2-Richtlinie betroffen?

Sektoren mit hoher Kritikalität (Anhang 1 der NIS2)

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

Sonstige kritische Sektoren (Anhang 2 der NIS2)

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

Welche Pflichten resultieren aus der NIS2-Richtlinie?

Maßnahmen zur Umsetzung eines geeigneten Risikomanagements

- Konzepte zur Risikoanalyse und der Sicherheit in der Informationstechnik
- Krisenmanagement – Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs, z.B. durch Backup-Management und Wiederherstellung nach einem Notfall
- Sicherheit in der Lieferkette
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen
- grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik
- Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung
- Sicherheit hinsichtlich des Personals – Konzepte für die Zugriffskontrolle und das Management von Anlagen,
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

Governance & Awareness

- Leitungsorgane sind verpflichtet, ergriffene Maßnahmen im Bereich Cybersicherheit zuzulassen und diese zu überwachen.
- Geschäftsführer müssen sich entsprechend schulen lassen.
- Bei Verstößen müssen diese andernfalls haften.

Meldepflichten bei Sicherheitsvorfällen

- Meldung an die zuständigen Aufsichtsbehörden innerhalb von 24 Stunden nach dem Vorfall
- Aktualisierung inkl. ausführlichem Berichts binnen 72 Stunden
- Abschlussmeldung muss innerhalb eines Monats geleistet werden

NIS2 – welche Strafen drohen bei Missachtung oder Verstößen?

Je nach Gruppe und Verstoß können die Bußgelder zwischen 100.000 – 10 Mio. Euro liegen. Neben empfindlichen Bußgeldern drohen bei Verstößen auch Weisungen durch die entsprechenden Aufsichtsbehörden, die bis zur Untersagung der Betriebstätigkeit oder gar der Untersagung der Leitungsaufgaben der Geschäftsführung des jeweiligen Unternehmens reichen.

WICHTIG: Jedes Unternehmen und jede Einrichtung müssen proaktiv und eigenverantwortlich eruieren, ob sie von NIS2 betroffen sind.

Sie sind betroffen und benötigen Hilfe bei der Umsetzung von NIS2?

Wir sind gerne für Sie da.

info@pegasus-gmbh.de +49 9402 503 – 300

pegasus IT
Member of ITventive Group