MEDIALINE

IT Security

NIS 2 - Die neue Richtlinie zur Cybersicherheit

Wirksame Cybersicherheit - Verantwortung für Management und Unternehmen

Die NIS-2-Richtlinie der EU stellt neue Anforderungen an die Cybersicherheit in Unternehmen. Dieses Datenblatt hebt die wichtigsten Änderungen, Verpflichtungen und Risiken hervor und bietet Lösungen, um die Einhaltung der Vorschriften zu gewährleisten.

Kritische Sektoren und betroffene Risiken

Die Richtlinie gilt für Organisationen aus hochkritischen und kritischen Sektoren:

Sektoren von hoher Kritikalität
(Essential Entities):

- Energie (Strom, Fernwärme und -kälte, Öl, Gas, Wasserstoff)
- Verkehr (Luft, Schiene, Wasser, Straße)
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheit (einschließlich Herstellung von pharmazeutischen Produkten, Impfstoffen)
- Trinkwasser
- Abwässer
- Digitale Infrastruktur (Internet-Austauschpunkte, DNS-Dienstleister, TLD-Namensregister, Cloud-Computing-Anbieter, Rechenzentren, Content Delivery Network, Trust Service Provider, öffentliche elektronische Kommunikationsdienste)
- IKT-Dienstleistungsmanagement (Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste)
- Öffentliche Verwaltung
- Weltraum

Andere kritische Sektoren
(wichtige Einrichtungen):

- Post- und Kurierdienste
- Abfallwirtschaft
- Chemikalien
- Lebensmittelproduktion
- Fertigung (medizinische Geräte, Computer, Elektronik, Maschinen, Kraftfahrzeuge, Anhänger)
- Digitale Anbieter (Online-Marktplätze, Suchmaschinen, Plattformen für soziale Netzwerke)
- Forschungsinstitute

Die Auswirkungen der NIS 2

- **Erweiterte Verantwortung der Führungskräfte**
  Führungskräfte sind für die Entwicklung, Umsetzung und Überwachung von Sicherheitsstrategien verantwortlich. Die Nichteinhaltung kann zu einer persönlichen Haftung führen (betrifft nur Geschäftsführer, nicht Team- oder Abteilungsleiter).
- **Erhöhte Rechenschaftspflicht**
  Unternehmen müssen ihre Sicherheitsmaßnahmen regelmäßig dokumentieren und gegenüber den Behörden nachweisen.

⚠ Damit verbundene Risiken

- Größere Anfälligkeit für Cyberangriffe
- Verschärfung der Meldepflichten für Sicherheitsvorfälle
- Schädigung des Rufs und der Marke im Falle von Sicherheitsverletzungen

Zentrale Verpflichtungen im Rahmen der NIS 2

Berichte über Vorfälle

- Verpflichtung zur Meldung von Sicherheitsvorfällen innerhalb von 24 Stunden.
- Innerhalb von 72 Stunden sind ausführliche Follow-up-Berichte erforderlich.

Umsetzung von Sicherheitsstandards

- Einführung von technischen und organisatorischen Maßnahmen zur Risikoanalyse und -minderung.
- Regelmäßige Sicherheitskontrollen und Audits.

Folgen der Nichteinhaltung

Sanktionen:

- Geldbußen von bis zu **10 Mio. EUR** oder **2 %** des weltweiten Jahresumsatzes für **Essential Entities.**
- Geldbußen von bis zu **7 Mio. EUR** oder **1,4 %** des weltweiten Jahresumsatzes für **wichtige Einrichtungen.**

Reputationsrisiken:
Verlust des Vertrauens bei Kunden und Partnern.

Betriebliche Auswirkungen:
Ausfallzeiten aufgrund von unzureichender IT-Sicherheit.

Unsere Lösung für Ihre Compliance

Wir unterstützen Sie bei der Umsetzung der NIS 2-Anforderungen:

Analysieren Sie Ihren Status quo:
Identifizierung von Schwachstellen und Risiken.

Entwicklung von Sicherheitskonzepten:
Maßgeschneiderte Strategien zur Einhaltung der Richtlinie.

Schulungskurse und Workshops:
Sensibilisierung von Management und Mitarbeitern.

Durchführung und Überwachung:
Einführung von robusten IT-Sicherheitsmaßnahmen und kontinuierliche Überwachung.

Werden Sie jetzt aktiv!

Schützen Sie Ihr Unternehmen rechtzeitig und vermeiden Sie Sanktionen und Risiken.
Kontaktieren Sie uns für weitere Informationen unter **sales@medialine.ag**

Stand: 12/2024