NIS-2-Richtlinie: Leitfaden für Unternehmen

Dieser Bericht beantwortet die wichtigsten Fragen zur NIS-2-Richtlinie (EU 2022/2555) und gibt konkrete Handlungsempfehlungen für Unternehmen.

1. Bin ich betroffen?

Die NIS-2-Richtlinie gilt für Unternehmen in 18 kritischen Sektoren, darunter Energie, Verkehr, Gesundheit, digitale Infrastruktur, Finanzwesen, Lebensmittelproduktion und Abfallwirtschaft.

Größenschwellen:

- Wichtige Einrichtungen: ab 50 Mitarbeitenden oder >10 Mio. € Umsatz/Bilanzsumme
- Besonders wichtige Einrichtungen: ab 250 Mitarbeitenden oder >50 Mio. € Umsatz/Bilanzsumme
- Sonderfälle: bestimmte Anbieter (z. B. DNS, TK-Dienste) sind unabhängig von der Größe betroffen.

2. Was muss ich tun, wenn ich betroffen bin?

- Registrierung beim BSI innerhalb von 3 Monaten über das BSI-Portal.
- Risikomanagement etablieren: Risikoanalysen, technische und organisatorische Maßnahmen.
- Meldepflicht bei Sicherheitsvorfällen: Frühwarnung innerhalb von 24 Stunden, Vollmeldung innerhalb von 72 Stunden.
- Geschäftsleitung haftet persönlich für die Umsetzung und muss sich schulen lassen.

3. Wer prüft die Einhaltung der Richtlinie?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) überwacht die Registrierung, prüft Meldungen und kann Audits anordnen. Bei Verstößen drohen Bußgelder bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes.

4. Wie kann ich mich absichern?

- Einführung eines Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001 oder TISAX.
- Lieferkettensicherheit: Verträge mit Dienstleistern um Cybersecurity-Anforderungen ergänzen.
- Notfall- und Incident-Response-Pläne regelmäßig testen.
- Schulungen für Führungskräfte und Mitarbeitende.
- Gap-Analyse und Compliance-Dokumentation aufbauen.

Handlungsempfehlungen für Unternehmen

Maßnahme	**Beschreibung**
Betroffenheitsprüfung	Prüfen, ob Ihr Unternehmen unter die NIS-2-Richtlinie fällt.
Registrierung beim BSI	Innerhalb von 3 Monaten nach Inkrafttreten.
ISMS einführen	Implementierung eines Informationssicherheitsmanagementsystems.
Incident-Response-Pläne	Erstellung und regelmäßige Tests von Notfallplänen.
Schulung der Geschäftsleitung	Verpflichtende Cybersecurity-Schulungen für Führungskräfte.

Checkliste für Unternehmen

- Betroffenheitsprüfung durchgeführt
- Registrierung beim BSI abgeschlossen
- ISMS implementiert
- Incident-Response-Pläne getestet
- Schulungen durchgeführt