Kompakter Leitfaden zur NIS-2-Richtlinie

ETES
IT. OPEN SOLUTIONS

1

Ziel der NIS-2-Richtlinie

Die NIS-2-Richtlinie soll ein hohes gemeinsames Sicherheitsniveau für Netz- und Informationssysteme in der EU gewährleisten, um die Resilienz gegen Cyberbedrohungen zu erhöhen.

2

Wer ist betroffen?

Betreiber kritischer Anlagen
Energieversorgung, Wasserwirtschaft, Gesundheitswesen, Finanzsektor, Transport und Verkehr

Wesentliche & wichtige Einrichtungen
Definition nach NIS-2-Richtlinie auf Basis des Wirtschaftssektors und der Unternehmensgröße

Digitale Dienste
Cloud-Dienstleister, Online-Marktplätze, Suchmaschinen

Öffentliche Verwaltung
Nationale und regionale Behörden

Telekommunikation
Anbieter öffentlicher elektronischer Kommunikationsdienste

Lieferketten
Unternehmen, die Teil der Lieferketten der NIS-2 genannten Sektoren sind

Vertrauensdiensteanbieter
Erstellung elektronischer Signaturen, Siegel und Zeitstempel; elektronische Einschreiben und zugehörige Zertifikate

Ob eine Betroffenheit besteht, kann im ersten Schritt über die ETES **NIS-2 Betroffenheitsanalyse** abgefragt werden. Für eine eindeutige Einschätzung empfehlen wir eine individuelle Betrachtung und Beratung durch unsere Experten.

3

Hauptanforderungen

- **Sicherheitsmaßnahmen:** Implementierung technischer und organisatorischer Maßnahmen, regelmäßige Risikoanalysen, Sicherheitsrichtlinien und -patches
- **Meldung von Sicherheitsvorfällen:** Meldung signifikanter Sicherheitsvorfälle an die zuständigen Behörden innerhalb einer bestimmten Frist
- **Management und Governance:** Klare Verantwortlichkeiten, Schulung und Sensibilisierung der Mitarbeiter, regelmäßige Berichterstattung
- **Zertifizierung und Audits:** Durchführung regelmäßiger Sicherheitsaudits und gegebenenfalls Erlangung von Zertifizierungen
- **Supply Chain Security:** Sicherstellung der Sicherheitsmaßnahmen bei Lieferanten und Partnern, Vertragsmanagement und regelmäßige Überprüfung
- **Zusammenarbeit und Informationsaustausch:** Meldung von Vorfällen, Zusammenarbeit mit nationalen und europäischen Cybersicherheitsbehörden

4

Strafen und Sanktionen

Bei Nichteinhaltung der Richtlinie drohen hohe Geldstrafen und andere Sanktionen, um die Einhaltung der Vorschriften zu gewährleisten.

5

Schritte zur Umsetzung

1 **Analyse der aktuellen Situation**
Bewertung bestehender Sicherheitsmaßnahmen und Identifizierung von Lücken

2 **Entwicklung eines Aktionsplans**
Festlegung der erforderlichen Maßnahmen zur Erfüllung der NIS-2-Anforderungen

3 **Implementierung der Maßnahmen**
Einführung technischer und organisatorischer Sicherheitsmaßnahmen

4 **Schulung und Sensibilisierung**
Schulung der Mitarbeiter und Sensibilisierung für Cybersicherheitsrisiken

5 **Regelmäßige Überprüfung und Anpassung**
Durchführung regelmäßiger Audits und Anpassung der Maßnahmen an neue Bedrohungen

6

Wichtige Ressourcen

- **Nationale Cybersicherheitsbehörden:** Kontaktaufnahme für Unterstützung und Meldepflichten
- **EU-Institutionen:** Informationen und Leitfäden zur NIS-2-Richtlinie
- **Zertifizierungsstellen:** Unterstützung bei Audits und Zertifizierungen

Wir stehen Ihnen zur Seite! NIS-2 Umsetzung ganz einfach mit dem erfahrenen Team von ETES.