

GET READY FOR NIS2

NEUE VERBINDLICHE EU-VORGABEN FÜR MEHR CYBERSICHERHEIT

Für viele Unternehmen und Organisationen gelten durch die NIS2-Richtlinie (EU) 2022/2555 ab Oktober 2024 verpflichtende Sicherheitsmaßnahmen und Meldepflichten – auch für viele, die bisher nicht betroffen waren.

WAS BEDEUTET NIS2?

Zweite EU-Richtlinie zur Netzwerk- & Informationssicherheit

WAS SIND DIE ZIELE VON NIS2?

- Hohes gemeinsames Cyber-Sicherheitsniveau in allen 27 EU-Ländern
- EU-weit einheitliche Sicherheitsstandards
- Schaffung eines Rahmens für sichere Innovation & Digitalisierung durch klare Richtlinien

WEN BETRIFFT NIS2?

- Öffentliche & private Einrichtungen in 18 Sektoren, mit min. 50 Beschäftigten oder min. 10 Mio. € Jahresumsatz & -bilanz

VERANTWORTUNG DER GERSCHÄFTSFÜHRUNG

Die Geschäftsführung muss die Umsetzung der Maßnahmen überwachen, an Schulungen teilnehmen und haftet für Verstöße. Sind die Maßnahmen nicht nachweisbar, muss mit Bußgeldern (bis 2% des Jahresumsatzes) gerechnet werden.

DIE NIS2-CHECKLISTE

- Aufbau eines ISMS inkl. Konzepten zur Risikoanalyse & Sicherheit von Informationssystemen
- Prävention, Erkennung & Bewältigung von Sicherheitsvorfällen
- Business Continuity (z. B. Backup-Management, Disaster Recovery) & Krisenmanagement
- Sicherheit in der Lieferkette
- Sicherheitsmaßnahmen bei der Beschaffung, Entwicklung & Wartung der IT-Systeme
- Bewertung der Wirksamkeit der Maßnahmen
- Gesicherte Sprach-, Video- & Textkommunikation
- Cyberhygiene (z. B. Updates) & Schulungen in Cybersicherheit
- Personalsicherheit, Zugriffskontrolle & Ressourcenmanagement
- Kryptografie & ggf. Verschlüsselung & Asset Management
- Multi-Faktor-Authentifizierungslösungen oder kontinuierliche Authentifizierung sowie ggf. gesicherte Notfallkommunikationssysteme
- Für Unternehmen der Stufe „Wesentliche Einrichtung“ weitere Mindestanforderungen: Beispielsweise der Betrieb eines Security Operations Center