

NIS-2-Richtlinie

Unternehmerische Konsequenzen des europäischen Weges zur Cybersicherheit

Die Umsetzung der EU-Richtlinie führt zu einer erheblichen Verschärfung der Unternehmerhaftung, weil Kritische Leitungsorgane **persönlich für Verstöße haftbar** gemacht werden.

Der Gesetzesentwurf sieht eine Managerhaftung vor!

Viele Unternehmer sind von dem Haftungsrisiko betroffen. Denn der Geltungsbereich erstreckt sich bereits auf mittlere Unternehmen mit mind. 50 Beschäftigten und einem Jahresumsatz/Jahresbilanz ab 10 Mio. EUR und erweitert die unternehmerischen Pflichten um ein definiertes Risikomanagement und Berichtspflichten im Bereich der Cybersicherheit.

Die Regelungen gelten auch für Subunternehmer, Dienstleister & Lieferanten!

Eine kurze Übersicht der Verpflichtungen:

- ✓ Explizite Verpflichtung der Leitungsorgane zur Überwachung und Weiterbildung
→ Keine Delegation, kein Outsourcing der Haftung!
- ✓ Zwang zur Cybersecurity-Prävention durch Umsetzung des Stands der Technik
- ✓ Digitale und physische Absicherung der IT-Infrastruktur
- ✓ Krisenmanagement, Cyberhygiene, Kryptografie, Personalsicherheit, Authentifizierungstechnologien, Notfallkommunikation
- ✓ Meldepflichten: Erstmeldung innerhalb von 24 Stunden, erste Bewertung innerhalb von 72 Stunden und ein detaillierter Abschlussberichts innerhalb eines Monats

Es drohen vielen Unternehmen und „Leitenden“ empfindliche Sanktionen bis zu 10 Millionen Euro oder 2% des Jahresumsatzes!

Unsere Empfehlung

Bereiten Sie sich jetzt auf die folgenden Mindestanforderungen vor:

- ✓ Durchführung von Risikoanalysen
- ✓ Erstellung von Informationssicherheitskonzepten
- ✓ Einrichtung eines Notfall- und Krisenmanagements
- ✓ Entwicklung von Maßnahmen zur Sicherheit der Lieferkette, einschließlich der Einbeziehung von Subunternehmern und der Einführung von Cybersicherheitspraktiken