HAVER MAILÄNDER

Bin ich betroffen?

Schwellenwert – wer fällt darunter?

• Große Unternehmen in kritischen Sektoren (Energie, Verkehr, digitale Infrastruktur, Gesundheit, Wasser / Abwasser, Abfall, Finanzmarkt-Infrastrukturen, Post / Kurier u.a., Managed Service Provider & Managed Security Service Provider) > 250 Mitarbeitende ODER > 50 Mio. € Umsatz

• Mittlere Unternehmen in denselben Sektoren ≥ 50 Mitarbeitende ODER ≥ 10 Mio. € Umsatz

WICHTIG: Die Einstufung erfolgt auf Gruppenebene, d.h. verbundene Unternehmen werden zusammengerechnet.

HAVER MAILÄNDER

Was ist konkret zu tun?

1. Risikomanagement

Implementierung und Dokumentation von:

- Konzepten in Bezug auf Risikoanalyse und Sicherheit für Informationssysteme
- Sicherheitsmaßnahmen & Schwachstellenmanagement
- Notfall- & Recovery- Verfahren inkl. Kommunikationsmanagement
- Schulungen und Sensibilisierungsmaßnahmen
- Lieferkettensicherheit (u.a.)

2. Registrierungs- und Meldepflichten

• Registrierung innerhalb von 3 Monaten
Bei einem erheblichen Sicherheitsvorfall:
• Frühmeldung an Behörde innerhalb von 24h
• Detailmeldung innerhalb von 72h
• Abschlussmeldung nach 1 Monat

3. Governance & Awareness

Die Geschäftsleitung ist für die Umsetzung von Cybersecurity-Maßnahmen persönlich verantwortlich. Sie muss sich schulen lassen, Maßnahmen beschließen, überwachen und dokumentieren.

HAVER MAILÄNDER

Warum lohnt sich die Umsetzung?

Bußgelder vermeiden

- bis zu 10 Mio. € bzw. 2 % des weltweiten Jahresumsatzes (je nachdem, was höher ist)

- bei wichtigen Einrichtungen: bis zu 7 Mio. € bzw. 1,4 %

Organhaftung vermeiden

- Die Geschäftsleitung haftet persönlich für die Umsetzung der erforderlichen technisch-organisatorischen Maßnahmen (TOMs)

- Delegation ≠ Entlastung

Wirtschaftlicher Aspekt

Jährlicher volkswirtschaftlicher Schaden von 289 Mrd. € in Deutschland durch Cyberangriffe (2025).

Quelle: Bitkom Wirtschaftsschutzstudie 2025