BÜSING MÜFFELMANN & THEYE RECHTSANWÄLTE UND NOTARE

FACT SHEET NIS-2

WORUM GEHT'S BEI NIS-2?

GEGENSTAND:
EU-Richtlinie zur Cybersicherheit. Unternehmen in der Pflicht zur Umsetzung von IT-Sicherheitsmaßnahmen.

RELEVANZ IN DEUTSCHLAND:
Ca. 30.000 Unternehmen unmittelbar betroffen; ca. 2,3 Mrd. EUR Umsetzungskosten.

TIMELINE:
Umsetzung der Richtlinie bis 17. Oktober 2024 in deutsches Recht.

WER IST BETROFFEN?

„WESENTLICHE EINRICHTUNGEN"
Große Unternehmen
(ab 250 MA; 50 Mio. EUR Jahresumsatz):

- Energie
- Verkehr
- Bankenwesen
- Finanzmarkt
- Gesundheit
- Trinkwasser
- Abwasser
- Verwaltung von IKT-Diensten
- Weltraum

„WICHTIGE EINRICHTUNGEN"
Mittlere Unternehmen
(ab 50 MA; 10 Mio. EUR Jahresumsatz):

- Energie
- Verkehr
- Bankenwesen
- Finanzmarkt
- Gesundheit
- Trinkwasser
- Abwasser
- Verwaltung von IKT-Diensten
- Weltraum

Große & mittlere Unternehmen:

- Post und Kurier
- Abfall
- Chemie
- Lebensmittel
- Produktion
- Digitale Dienste
- Forschung

ACHTUNG:
Betroffene Unternehmen werden IT-Sicherheitspflichten in der Lieferkette auch an **Klein- und Kleinstunternehmen** durchreichen. Für diese gelten die NIS-2-Pflichten dann mittelbar.

WELCHE MAßNAHMEN SIND UMZUSETZEN?

- Konzept Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Business Continuity und Krisenmanagement
- Sicherheit der Lieferkette
- Sicherheitsmaßnahmen bei Erwerb/Entwicklung/Wartung von IKT
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen
- Cyberhygiene und Schulungen zur Cybersicherheit
- Kryptografie und ggf. Verschlüsselung
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle
- Multi-Faktor-Authentifizierung

MELDEPFLICHTEN:
Meldung von Cyber Security Incidents innerhalb von 24 Stunden bei Aufsichtsbehörde.

BUßGELDER UND HAFTUNG

WESENTLICHE EINRICHTUNGEN:
10 Mio. EUR oder
2 % des weltweiten Jahresumsatzes

WICHTIGE EINRICHTUNGEN:
7 Mio. EUR oder
1,4 % des weltweiten Jahresumsatzes

„CYBERSECURITY WIRD CHEFSACHE":
Schadenersatzansprüche gegen Geschäftsführer bzw. Vorstandsmitglieder bei unzureichender Cybersicherheit im Unternehmen.

Stand: März 2024 Dr. Justus Gaden, gaden@bmt.eu