# Seminaragenda

## NIS-2-Richtlinie und deutsches Umsetzungsgesetz

***Fokus: Energie und Krankenhäuser – Systematik, Spezialregime und Managementverantwortung***

## 1. Europarechtliche Systematik der NIS-2 (15 Minuten)

- Regelungsziel und Harmonisierungsansatz der Richtlinie (EU) 2022/2555.
- Unterscheidung zwischen wesentlichen und wichtigen Einrichtungen.
- Sektorlogik und Schwellenwerte als Ausgangspunkt jeder Anwendungsprüfung.

## 2. Deutsches NIS2-Umsetzungsgesetz als Artikelgesetz (15 Minuten)

- Umsetzung durch Artikelgesetz mit Änderungen mehrerer Fachgesetze.
- Reform und Erweiterung des BSI-Gesetzes (BSIG-E).
- Erweiterte Eingriffs- und Aufsichtsbefugnisse sowie Bußgeldrahmen.

## 3. Allgemeines Cybersicherheitsregime nach BSIG-E (20 Minuten)

- Risikomanagementmaßnahmen (§ 28 BSIG-E) als zentraler Pflichtenkern.
- Meldepflichten bei erheblichen Sicherheitsvorfällen.
- Lieferketten- und Drittparteienmanagement.
- Verpflichtung der Geschäftsleitung zur Billigung, Überwachung und Umsetzung der Sicherheitsmaßnahmen.

## 4. Spezialitätsprüfung: Sektorale Sicherheitsregime (25 Minuten)

- A. Energie: § 11 EnWG als eigenständige IT-Sicherheitsnorm; IT-Sicherheitskatalog der Bundesnetzagentur; ergänzende Anwendung des BSIG.
- B. Krankenhäuser: Einordnung als wesentliche Einrichtungen; Anwendung des BSIG als Kernregime mangels eigenständiger IT-Sicherheitskodifikation.

- C. Finanzsektor (Überblick): DORA als eigenständiges Cyber-Spezialregime mit teilweise verdrängender Wirkung.
- D. Weitere Sektoren (Verkehr, Wasser, Digitale Infrastruktur): Besonderheiten ohne vollständige Spezialkodifikation.

## 5. Aufsichtssystem und Behördenzuständigkeiten (15 Minuten)

- Allgemeine Cybersicherheitsaufsicht durch das BSI.
- Sektorale Energieregulierung durch die Bundesnetzagentur.
- Finanzaufsicht im Rahmen von DORA.
- Koordinierung, Doppelaufsicht und Meldepflichtenkollisionen.

## 6. ISMS als zentrales Umsetzungsinstrument (15 Minuten)

- Struktur und Funktion eines Informationssicherheitsmanagementsystems (ISMS).
- ISMS als Konkretisierung des 'Standes der Technik' im BSIG und im § 11 EnWG.
- Verankerung des ISMS auch in spezialgesetzlichen Regelungen (z.B. IT-Sicherheitskatalog Energie, DORA).
- ISMS als haftungsrelevantes Organisationsinstrument der Geschäftsleitung.

## 7. Besondere Verpflichtung und Haftung der Geschäftsleitung (10 Minuten)

- Eigenständige Billigungs- und Überwachungspflicht nach NIS-2 / BSIG-E.
- Pflicht zur aktiven Implementierung geeigneter Sicherheitsstrukturen.
- Schulungs- und Informationspflichten der Leitungsorgane.
- Persönliche Bußgeldrisiken und Organisationsverschulden.
- Einordnung in das allgemeine Gesellschaftsrecht (Legalitätspflicht, Compliance-Organisation).

## 8. Zertifizierung und Standards (10 Minuten)

- ISO/IEC 27001: Auditlogik und Zertifizierungszyklen.
- BSI IT-Grundschutz: Bausteinprinzip und Schutzbedarfsfeststellung.
- Sektorabhängige strategische Auswahl und Kombinationsmöglichkeiten.

## 9. Praktischer Umsetzungsfahrplan (5 Minuten)

- Anwendungsbereichsprüfung (Sektor und Schwellenwert).
- Bestimmung des maßgeblichen Sicherheitsregimes (BSIG allein oder kumulativ mit Spezialrecht).
- Implementierung und Dokumentation eines wirksamen ISMS.
- Kontinuierliche Überwachung durch die Geschäftsleitung.