SC170 NIS2, ITSiG, CRA - Worauf müssen wir uns bei Cybersicherheit und Regulierung einstellen?

Kurzbeschreibung:

Cyber-Risiken und -Resilienz sind inzwischen das zentrale Thema auf Vorstands- und Geschäftsführerebene. Mit NIS2 und dem Cyber Resilience Act (CRA) stehen zwei Gesetze für 2024/2025 ins Haus, die zu einschneidenden Veränderungen in der breiten Unternehmenslandschaft führen. Unser **Noon2Noon-Format** bringt Sie auf den neuesten Stand, spielt Anwendungsszenarien durch und fördert im geschützten Rahmen den Erfahrungsaustausch auf der **Entscheider-Ebene**.

Die europäische **NIS2**-Richtlinie erweitert die KRITIS-Sektoren und den Pflichtenkatalog der KRITIS-Betreiber für effektives Risikomanagement. Das **IT-Sicherheitsgesetz** wird bis Oktober 2024 angepasst. Die neuen Pflichten gelten unmittelbar für die KRITIS-Betreiber, die ihre Lieferanten entsprechend einbinden werden. Auch die Anbieter digitaler Dienste sind verstärkt im Fokus der Regulierung. Der **CRA** trägt die Cyber-Regulierung auf die Produktebene. Schon ab 2027 könnte es soweit sein, dass Produkte mit digitalen Elementen Security by Design und Schwachstellenabsicherung über den gesamten Lebenszyklus bieten müssen.

- Was ist neu und worauf müssen sich die Unternehmen in kurzer Zeit einrichten?
- Welche weiteren Cyber-Anforderungen ergeben sich aus neuen Regeln zur **Produkthaftung**, **Produktsicherheit** und der **Maschinen-Verordnung**?

In unserem **PREMIUM** Workshop **SC170 NIS2, ITSiG, CRA - Worauf müssen wir uns bei Cybersicherheit und Regulierung einstellen?** diskutieren wir mit Ihnen im interaktiven Format die neuen Entwicklungen, bestimmen Handlungsbedarfe in konkreten Case Studies und ermöglichen den Erfahrungsaustausch mit Experten und Entscheidern.

Zielgruppe:

- Vorstände und Geschäftsführer
- Entscheider für Cyber-Security
- Compliance-Verantwortliche

Voraussetzungen:

- Grundkenntnisse im IT-Sicherheitsrecht sind hilfreich, aber nicht zwingend erforderlich

Sonstiges:

Dauer: 2 Tage

Preis: 850 Euro plus Mwst.

Ziele:

- Verständnis der regulatorischen Veränderungen
- Bestimmung unternehmerischer Handlungsbedarfe
- Auswirkungen auf Produktmanagement, Compliance- und Governance-Strukturen

Inhalte/Agenda:

- **Tag 1: Cyber-Regulierung in Europa – wo stehen wir?**
- **12:30 Eintreffen und gemeinsames Mittagessen**
- **KRITIS**
  - Von NIS1 zu NIS2
    - · Wer ist betroffen?
    - · Was ist zu tun?
    - · Was gilt für Digital Dienste?
  - Von ITSiG 2.0 zu ITSiG 3.0 – was plant der Gesetzgeber?
  - KRITIS-Dachgesetz
- **Produkte**
  - Cyber Resilience Act
  - Cyber Security Act
  - Cyber-Sicherheit in der Produktregulierung
    - · Produkthaft-Richtlinie – was ändert sich?
    - · Produktsicherheits-Richtlinie – alles beim Alten?
    - · Maschinen-Richtlinie – auch das noch!
- **Strafbarkeit des Hack-back und Lehren des Tages**
- **18:30 Gemeinsames Abendessen**

TAG 2: Anwendungsszenarien und Fallstudien

- **09:00 Tooling für das Risikomanagement: DriveLock in der Praxis**
- **Wie entwickele ich meine Cyber-Governance?**
  - Fallstudien
    - · Fallstudie 1: Cyber-Vorfall und Krisenmanagement
    - · Fallstudie 2: Management-Haftung
  - Praktische Schlussfolgerungen / Handlungsempfehlungen
- **Plenum – erste Ergebnisse**
- **Was ändere ich im Vendoren-Management?**
  - Fallstudien
    - · Fallstudie 3: IT Procurement und Auditierung
    - · Fallstudie 4: Vertragliche Haftungsabsicherung und Versicherung
  - Praktische Schlussfolgerungen / Handlungsempfehlungen
- **Plenum – weitere Ergebnisse**
- **Zusammenfassung**
- **Gemeinsames Mittagessen / Abreise**