Cyber-Resilienz im Fokus

Wir diskutieren Thesen – mit dem Ziel, voneinander zu lernen und gemeinsam Lösungen zu skizzieren.

Working Roundtable anlässlich des NIS-2-Congress

Warum Cyber-Resilienz?

- Cyber-Resilienz ist mehr als nur IT-Sicherheit – sie ist die Fähigkeit, den Betrieb auch unter widrigen Umständen aufrechtzuerhalten.
- NIS-2 fordert von Organisationen mehr als bloße Abwehrmaßnahmen – es geht um vorausschauende, resiliente Strukturen.
- Cyber-Resilienz ist das neue Fundament der digitalen Sicherheit – gefordert nicht nur durch Angreifer, sondern durch NIS-2 ganz konkret.

These 1: Resilienz beginnt beim Management – nicht in der IT

- These: Resilienz beginnt beim Management – nicht in der IT
- Diskussionsimpuls: Ohne strategische Einbindung der Geschäftsleitung bleiben Investitionen reaktiv.
- - Rollen & Verantwortlichkeiten
- - Verankerung in der Unternehmenskultur
- - Unterstützung durch den Vorstand

These 2: Von Compliance zu echter Resilienz

- These: Von Compliance zu echter Resilienz: NIS-2 als Chance nutzen
- Diskussionsimpuls: Die Umsetzung von NIS-2 bietet die Chance, strukturell resilienter zu werden – wenn man sie strategisch denkt.
- - Maturity-Modelle und KPIs
- - Von Reaktion zu Antizipation
- - Budget, Reporting und politische Unterstützung

These 3: Lieferketten sind der blinde Fleck der Cyber-Resilienz

- These: Lieferketten sind der blinde Fleck der Cyber-Resilienz
- Diskussionsimpuls: Wie gelingt es, Resilienz entlang komplexer Lieferketten realistisch zu bewerten und durchzusetzen?
- - Risiken durch Zulieferer & Dienstleister
- - Vertragsgestaltung vs. echte Kontrolle
- - Kollaborative Sicherheitsstandards

These 4: Übung schlägt Technik

- These: Übung schlägt Technik: Resilienz muss trainiert werden
- Diskussionsimpuls: Cybersecurity-Tools garantieren keine Handlungsfähigkeit im Ernstfall.
- - Business Continuity & Incident Response
- - Planspiele & Krisenübungen
- - Interdisziplinäre Beteiligung