Kompaktseminar BSI-KritisV - IT&Telekom.

KRITIS & NIS-2 Kompakt: Das branchenübergreifende Praxis-Update

Seminar	8 Termine verfügbar	Teilnahmebescheinigung
Präsenz	8 Unterrichtseinheiten	Online durchführbar

Seminarnummer: 31418

Stand: 24.11.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/31418

Mit der Umsetzung der NIS-2-Richtlinie und dem BSIG wächst der Handlungsdruck auf Organisationen massiv. Um Haftungsrisiken zu vermeiden, müssen Betroffene handeln. Das Kompaktseminar vermittelt branchenübergreifend einen Überblick über Betroffenheitsprüfung, Sicherheitsmaßnahmen nach dem Stand der Technik sowie Melde- und Nachweispflichten.

Nutzen

- **Regulatorische Anforderungen einordnen:** Die Teilnehmenden lernen die gesetzlichen Anforderungen kennen und können die Betroffenheit ihrer Organisation systematisch prüfen.
- **Umsetzungsklarheit:** Das Seminar übersetzt den rechtlichen „Stand der Technik“ in die Praxis. Im Fokus steht die Anwendung einer praxiserprobten Risikomanagement-Methode, mit der Organisationen die komplexen Anforderungen strukturiert bewältigen können. Branchenspezifische Sicherheitsstandards (B3S) werden dabei beispielhaft als zusätzliche Orientierungshilfe herangezogen.
- **Audit-Readiness:** Die Teilnehmenden erhalten Orientierung zur Vorbereitung erforderlicher Nachweise gegenüber dem BSI sowie zu Zuständigkeiten und nachvollziehbarer Dokumentation.
- **Regelwerke effizient zusammenführen:** B3S, ISO 27001, BSI IT-Grundschutz, NIST-Rahmenwerke und IEC 62443 weisen inhaltliche Überschneidungen auf, unterscheiden sich jedoch in Anwendungsbereich und Anforderungen. Das Seminar zeigt Ansätze zur gemeinsamen Umsetzung vergleichbarer Anforderungen und zur Vermeidung von Doppelarbeit. Regelwerksspezifische und gesetzliche Anforderungen bleiben dabei gesondert zu berücksichtigen.
- Realitätsnahes Notfalltraining (Intensiv-Übung): Ein besonderer Schwerpunkt liegt auf einer Simulation „Ransomware“. Das Szenario basiert auf echten, anonymisierten Sicherheitsvorfällen aus der aktuellen Beratungspraxis. Die Teilnehmenden profitieren von direkten Einblicken in reale

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

Angriffsverläufe, üben die Reaktionsketten und leiten praxisbezogene Handlungsmöglichkeiten für das eigene Notfallmanagement ab.

Zielgruppe

- Das Seminar richtet sich an Fach- und Führungskräfte sowie Mitarbeitende aus allen KRITIS-Sektoren und -Branchen, die regulatorische Anforderungen mit der betrieblichen Umsetzung verbinden möchten. Angesprochen sind insbesondere Verantwortliche und Beauftragte für Informations- und IT-Sicherheit, Datenschutz, Risikomanagement, Compliance und Notfallmanagement.

  Das Angebot richtet sich auch an Verantwortliche, die prüfen möchten, ob ihre Organisation unter die KRITIS- oder NIS-2-Regulierung fällt. Schließen Sie sich zahlreichen Verantwortlichen an, die derzeit branchenübergreifend bewährte Strategien zur Bewältigung der neuen Regularien etablieren.

Inhalte des Seminars

- **Regulatorisches Praxis-Update:** Ziele des KRITIS-Schutzes, aktuelles BSIG, BSI-KritisV und NIS-2-Umsetzung; Einordnung des IT-Sicherheitsgesetzes 2.0 und Abgrenzung zum KRITIS-Dachgesetz.
- **Alle KRITIS-Sektoren und NIS-2-Branchen** im Überblick (Energie, Gesundheit, Transport, IT, Verwaltung u.v.m.) sowie Abgrenzung der Sektorenmodelle.
- **Betroffenheit systematisch prüfen:** kritische Dienstleistungen, Anlagenkategorien und Schwellenwerte; Betreiber kritischer Anlagen sowie besonders wichtige und wichtige Einrichtungen unterscheiden.
- **Praxis-Check:** Ist die Organisation betroffen? An fiktiven Unternehmen prüfen die Teilnehmenden die mögliche Betroffenheit und identifizieren fehlende Angaben. Als Vorbereitung dient die Frage: Welche Informationen zu Einrichtungsart, Anlagen und Schwellenwerten liegen in der eigenen Organisation bereits vor?
- **Sicherheitsanforderungen praktisch umsetzen:** Risikomanagement, technische und organisatorische Maßnahmen, Vorfallmanagement und Betriebsfortführung; B3S als branchenspezifische Umsetzungshilfe.
- **Pflichten gegenüber dem BSI:** Registrierung, Meldung erheblicher Sicherheitsvorfälle und Nachweiserbringung – mit klaren Zuständigkeiten, nachvollziehbarer Dokumentation und gezielter Prüfungsvorbereitung.
- Branchenübergreifende Umsetzungsbeispiele und **Best-Practice-Austausch**: von der Risikoanalyse über die Maßnahmenplanung bis zur Nachweisvorbereitung.

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

- **Tabletop-Übung:** „Ransomware“ In Kleingruppen entwickeln die Teilnehmenden erste Handlungsschritte und klären Zuständigkeiten, Informationsbedarf, Eskalationswege und mögliche Meldepflichten.

- **Moderierte Gruppendiskussion** zu DORA, Cyber Resilience Act (CRA), KI-Verordnung (AI Act) und NIS-2-Durchführungsverordnung (EU) 2024/2690: Anwendungsbereiche, Schnittstellen und praktische Umsetzungsfragen gemeinsam einordnen.

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/31418 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.