Cybersecurity for Executives.

Cybersecurity ist Chefsache - und entscheidend für die Zukunft Ihres Unternehmens.

Seminar	7 Termine verfügbar	Teilnahmebescheinigung
Präsenz / Virtual Classroom	8 Unterrichtseinheiten	Online durchführbar

Seminarnummer: 31601

Stand: 08.05.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/31601

Eine praxisnahe 1-Tages-Schulung für Geschäftsführung, Vorstände und Führungskräfte mit Leitungsverantwortung (gilt als Nachweispflicht nach § 38 Abs. 3 BSIG).

Der Kurs vermittelt, welche Verantwortung die Geschäftsleitung unter NIS2 trägt, wie Cyberrisiken als Geschäftsrisiken zu bewerten sind und wie wirksame Cyber-Governance, Krisenführung und Resilienz auf Leitungsebene organisiert werden.

Im Fokus stehen nicht technische Details, sondern die Fragen, die für die Unternehmensleitung entscheidend sind: Welche Maßnahmen müssen genehmigt und überwacht werden? Wie trifft die Geschäftsleitung im Cybervorfall die richtigen Entscheidungen? Wie werden Meldepflichten, Kommunikation, Wiederanlauf und Drittparteienrisiken wirksam gesteuert? Anhand einer durchgängigen Fallstudie und Executive-Übungen entwickeln die Teilnehmenden ein klares Verständnis für ihre Rolle, ihre Pflichten und die konkrete Umsetzung in der Unternehmenspraxis.

Nutzen

- NIS2-Anforderungen für die Geschäftsleitung verständlich und praxisnah aufbereitet
- Klare Einordnung von Cybersecurity als Führungs- und Unternehmensrisiko
- Stärkung der Entscheidungsfähigkeit im Cybervorfall
- Konkrete Orientierung für Governance, Reporting und Board Oversight
- Besseres Verständnis von Meldepflichten, Kommunikations- und Eskalationswegen
- Klare Sicht auf Resilienz, Wiederanlauf und Business Continuity
- Bewusstsein für kritische Drittparteien- und Lieferkettenrisiken
- Executive-taugliche Übungen statt technischer Detaildiskussion
- Direkte Übertragbarkeit auf reale Management- und Aufsichtspraxis
- Beitrag zur Nachweisbarkeit von Schulung und Leitungsbefähigung nach § 38 Abs. 3 BSIG

Mit realisitscher Live-Simulation einer Cyber-Krise.

Zielgruppe

- Geschäftsführer mittelständischer Unternehmen
- Vorstände, Partner, Gesellschafter mit operativer Verantwortung
- Entscheider ohne IT-Hintergrund, die Sicherheit verstehen wollen

Voraussetzungen

Es werden **keine** IT-Kenntnisse vorausgesetzt.

Inhalte des Seminars

Modul 1: Verantwortung & Haftung der Geschäftsleitung

- Warum Cybersecurity unter NIS2 explizit Führungsaufgabe ist
- Billigung & Überwachung von Cyber-Risikomaßnahmen (Managementpflichten)
- Anforderungen an ein belastbares Lagebild (Fakten vs. Hypothesen)
- Persönliche Verantwortungsdimension: Entscheidungs- und Nachweislogik

Modul 2: Was die Geschäftsleitung genehmigen & überwachen muss

- Bausteine eines angemessenen Cyber-Risikomanagements
- Policies, Rollen/Verantwortung und Steuerungsmodell
- Anforderungen an ein belastbares Lagebild (Fakten vs. Hypothesen)
- Zugriffskontrolle, Awareness und Wirksamkeitsprüfung (KPIs/Reviews)

Modul 3: Executive Risk Management

- Technische Risiken in Business-Impact übersetzen
- Betriebsunterbrechung, Datenabfluss, Ausfall kritischer Dienste
- Anforderungen an ein belastbares Lagebild (Fakten vs. Hypothesen)
- Drittparteien-/Lieferkettenvorfälle und Reputations-/Regulatorikfolgen

Modul 4: **Incident Leadership**

- Rolle der Geschäftsleitung im Vorfall: Krise führen vs. operativ reagieren
- Anforderungen an ein belastbares Lagebild (Fakten vs. Hypothesen)
- Entscheidungen: Isolation, Weiterbetrieb, Priorisierung, Wiederanlauf
- Externe Unterstützung (IR/Forensik/Versicherung) und Kommunikationsführung

Modul 5: Meldepflichten & Stakeholder-Steuerung

- Überblick über Melde-/Kommunikationsanforderungen bei erheblichen Vorfällen
- Fokus „erste 24 Stunden“: Struktur, Taktung, Verantwortlichkeiten
- Anforderungen an ein belastbares Lagebild (Fakten vs. Hypothesen)
- Konsistente Botschaften: was ist sicher, was ist Annahme, was ist unklar

Modul 6: Business Continuity, Resilienz & Wiederanlauf

- Warum Cybersecurity bei Resilienz beginnt (nicht bei Prävention endet)
- Kritische Leistungen identifizieren und Wiederanlaufreihenfolge priorisieren
- Anforderungen an ein belastbares Lagebild (Fakten vs. Hypothesen)
- Backup/Restore/DR realistisch bewerten und testen

Modul 7: Supply Chain & Drittparteienrisiko

- Kritische Lieferanten, Cloud-Anbieter, Managed Services: Risiken strukturieren
- Bewertung nach Kritikalität, Konzentrationsrisiko und Ersetzbarkeit
- Anforderungen an ein belastbares Lagebild (Fakten vs. Hypothesen)
- Einbindung in Incident Leadership, Wiederanlauf und Governance

Modul 8: Cybersecurity Governance

- Executive Reporting: wie Cyber dauerhaft in die Leitungsebene kommt
- KPIs/Dashboards, Trendsteuerung und Maßnahmen-Tracking
- Anforderungen an ein belastbares Lagebild (Fakten vs. Hypothesen)
- Integration in Unternehmens-Governance

Modul 9: Live Simulation einer Cyber-Krise (Incident Tabletop)

- Realistische Live-Simulation eines Cybervorfalls
- Entscheidungstraining im Executive-Modus: Lagebild-Taktung, klare Prioritäten, maximale Handlungsfähigkeit
- Anforderungen an ein belastbares Lagebild (Fakten vs. Hypothesen)
- Stakeholder-Steuerung in Echtzeit: Kunden, Presse, Partner, Versicherung – konsistente Botschaften und Update-Rhythmus

Wichtige Hinweise

Diese Schulung gilt als Nachweispflicht für die Schulung der Geschäftsleitung gemäß § 38 Abs. 3 BSIG.

- mit dieser Schulung werden alle verpflichtenden und optionalen Inhalte auf Grundlage des BSI-Dokuments erfüllt.

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/31601 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.