

IT Governance

Security ins Geschäftsmodell einbinden

IT Governance ist heute unverzichtbar, um digitale Infrastrukturen widerstandsfähig und regelkonform zu gestalten. Dieser IT Governance Kurs vermittelt ein ganzheitliches Verständnis für strategische, organisatorische und technische Aspekte moderner Informationssicherheit in Zeiten von NIS2, DORA und dem AI Act.

Im Zentrum stehen die Analyse aktueller Bedrohungslagen, die Entwicklung wirksamer Sicherheitsmaßnahmen sowie der Aufbau eines strukturierten Sicherheitsmanagements. Dabei werden auch menschliche Faktoren, Security Awareness und der gezielte Umgang mit Schwachstellen behandelt. Der Kurs schafft Klarheit in einem komplexen Umfeld und unterstützt dabei, Sicherheit als kontinuierlichen Prozess zu etablieren.

Kursinhalt

- Regulatorik (NIS2, DORA, AI Act, CRA)
- Managementsysteme (ISO 27001, IT-Grundschutz, ISMS, BCM)
- Risikomanagement
- Sicherheitsarchitekturen und Lösungen
- SIEM, IDS/IPS, Firewall
- Security Operations Center (SOC)
- Authentifizierung und Zugriffskontrollen (MFA, RBAC, PAM)
- Business Continuity Management
- Supply Chain Security
- Security Awareness
- Social Engineering
- Kryptographie, Protokollsicherheit
- KI in der Sicherheit
- Cyber Resilience
- Asset Management und Schwachstellenanalyse
- Europäische Zusammenarbeit
- Behörden und Aufsicht (BSI, CERT.at)

Zielgruppe

Dieser Kurs richtet sich an IT-Sicherheitsverantwortliche, Entscheidungsträger und technische Fachkräfte, die ein vertieftes Verständnis für IT-Governance und aktuelle regulatorische Anforderungen entwickeln möchten. Sie werden in die Lage versetzt, Sicherheitsstrategien und Compliance-Maßnahmen effektiv umzusetzen und die relevanten Vorschriften und Standards zu verstehen.

Voraussetzungen

Sie sollten ein grundlegendes Verständnis für Netzwerke und die Arbeitsweise verschiedener Technologien und Protokolle mitbringen.

Kursziel

Ziel des Kurses ist es, Ihnen zu vermitteln, wie regulatorische Maßnahmen Sicherheits- und Compliance-Anforderungen unterstützen. Sie lernen, deren Bedeutung für den Schutz von Daten und Systemen zu verstehen, den Nutzen für Ihr Unternehmen einzuschätzen und Maßnahmen praxisnah umzusetzen.

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.de/go/ITGO

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Premium Print Paket



Zu diesem Kurs können sie optional das hochwertige Premium Print Paket zum Preis von € 150,- (zzgl. MwSt) erwerben.

Stand 26.03.2026

Training		Preise zzgl. MwSt.	
Termine in Deutschland	3 Tage	€ 1.795,-	
Online Training	3 Tage	€ 1.795,-	
Termin/Kursort	Kurssprache Deutsch		
20.07.-22.07.26	Frankfurt	02.09.-04.09.26	Online
20.07.-22.07.26	Online	16.11.-18.11.26	Frankfurt
02.09.-04.09.26	Frankfurt	16.11.-18.11.26	Online



Inhaltsverzeichnis

IT Governance – Security ins Geschäftsmodell einbinden

- 1 Grundlagen der IT-Sicherheit**
 - 1.1 Bedrohungslage und Herausforderungen**
 - 1.1.1 Angreifer und ihre Motive
 - 1.1.2 Angriffsvarianten im Überblick
 - 1.2 Wirtschaftliche Bedeutung der Cybersicherheit**
 - 1.2.1 Wirtschaftlicher Schaden
 - 1.2.2 Reputationsverlust
 - 1.2.3 Cybersicherheit als wirtschaftlicher Erfolgsfaktor
 - 1.2.4 Schadensminimierung durch Präventionsmaßnahmen
 - 1.3 Resilienz und Schutz des Binnenmarkts**
 - 1.3.1 Cybersicherheit als Bestandteil der EU-Strategie
 - 1.3.2 Interdependenzen innerhalb der EU
 - 1.3.3 Internationale Herausforderungen
 - 1.3.4 IT-Sicherheit - Rolle der Unternehmen und Staaten
- 2 Regulatorische Grundlagen – NIS2, DORA & Co.**
 - 2.1 Definition und Bedeutung von IT Governance**
 - 2.1.1 Zusammenhang zwischen IT Governance und Netzwerksicherheit
 - 2.1.2 Rollen und Verantwortlichkeiten in der IT Governance
 - 2.1.3 Organisatorische Prozesse
 - 2.2 NIS2-Richtlinie**
 - 2.2.1 KRITIS – Ein kurzer Blick zurück
 - 2.2.2 Ziele und Hintergründe der NIS2-Richtlinie
 - 2.2.3 Pflichten für Unternehmen und Behörden
 - 2.2.4 Handlungsanweisungen für betroffene Sektoren
 - 2.2.5 Checkliste zur NIS2-Richtlinie
 - 2.3 DORA – Digital Operational Resilience Act**
 - 2.3.1 Fokus auf kritische Finanzinfrastrukturen
 - 2.3.2 Vergleich mit bisherigen Sicherheitsstandards
 - 2.3.3 Handlungsempfehlungen
 - 2.4 Cyber Resilience Act (CRA)**
 - 2.4.1 Hintergrund und Zielsetzung
 - 2.4.2 Sicherheitsanforderungen für vernetzte Produkte
 - 2.5 European AI Act**
 - 2.5.1 Die Regulierung von KI
 - 2.5.2 Klassifizierung von KI Systemen nach Risikostufen
 - 2.5.3 Sektoren und ihre Pflichten
 - 2.5.4 Zeitliche Einordnung
 - 2.6 Praktische Implikationen der Regulierungen**
 - 2.6.1 Sicherheitsmaßnahmen im Unternehmen
 - 2.6.2 Dokumentation und Nachweisführung für Audits
 - 2.7 Vergleich und Zusammenspiel der EU-Richtlinien**
 - 2.7.1 Synergien für umfassende IT-Security
- 3 Die Rolle staatlicher Behörden**
 - 3.1 Bundesamt für Sicherheit in der Informationstechnik (BSI)**
 - 3.1.1 Aufgaben, Funktionen und Bedeutung für Unternehmen
 - 3.1.2 Das IT-Sicherheitsgesetz
 - 3.2 IT-Grundschutz-Kompendien**
 - 3.2.1 Einführung in die IT-Grundschutz-Kompendien
 - 3.2.2 Risikoanalyse nach BSI-Vorgaben
 - 3.3 BSI-Sicherheitsstandards und -empfehlungen**
 - 3.3.1 BSI-Empfehlungen für Netzwerksicherheitsmaßnahmen
 - 3.3.2 Praktische Anwendung – Checklisten und Tools
 - 3.4 Österreichische Behörden
 - 3.4.1 BMI, MILCERT und CERT.at – Operative Sicherheit
 - 3.4.2 Österreichischer Informationssicherheitshandbuch
 - 3.4.3 NIS2 und DORA Österreich – NISG und FMA
 - 3.5 European Union Agency for Cybersecurity (ENISA)
 - 3.5.1 Leitlinien zur Cybersicherheit
 - 3.5.2 NIS2 Umsetzungsverordnung
 - 3.5.3 Methodische Orientierung
- 4 Organisatorische Sicherheitsmaßnahmen**
 - 4.1 Sicherheitsanforderungen aus Governance-Perspektive**
 - 4.1.1 IT-Richtlinien und Zertifizierungen (ISO/IEC 27001)
 - 4.1.2 OT-Security (ISA/IEC 62443)
 - 4.1.3 Sicherheitsrichtlinien planen
 - 4.1.4 Sicherheitsrichtlinien umsetzen
 - 4.2 Asset Management**
 - 4.2.1 Inventarisierung – Assets erfassen
 - 4.2.2 Schwachstellen und Abhängigkeiten
 - 4.2.3 Supply Chain Risiken
 - 4.3 Risikomanagement**
 - 4.3.1 Bedrohungslage erkennen - Threat Modeling
 - 4.3.2 Identifikation und Bewertung von Risiken
 - 4.3.3 Entwicklung von Maßnahmen zur Risikobehandlung
 - 4.4 Durchführung von IT-Sicherheitsaudits**
 - 4.4.1 Notfallmanagement
 - 4.5 Sicherheitsarchitekturen**
 - 4.5.1 Perimeter Security – Der historische Ansatz
 - 4.5.2 Defense in Depth – Sicherheit erweitert
 - 4.5.3 Zero Trust – Misstrauen als Prinzip
 - 4.6 Cloud-Governance und Netzwerksicherheit**
 - 4.6.1 Datenschutz in der Cloud
 - 4.6.2 CS Testat – Audits für die Cloud
 - 4.6.3 Edge Computing – Next Generation Cloud
- 5 Technische Aspekte der Netzwerksicherheit**
 - 5.1 Schwachstellen in Netzwerkkonstrukturen**
 - 5.1.1 Exploitation
 - 5.1.2 Social Engineering
 - 5.1.3 Lateral Movement
 - 5.1.4 DoS und DDos
 - 5.2 Präventive Schutzmaßnahmen**
 - 5.2.1 Physischer Schutz
 - 5.2.2 Protokollsicherheit
 - 5.2.3 Kryptographie und Verschlüsselung
 - 5.2.4 Disaster Recovery
 - 5.3 Netzwerksicherung**
 - 5.3.1 Firewalls
 - 5.3.2 IDS/IPS
 - 5.3.3 Security Services Edge (SSE)
 - 5.4 Zugangsmanagement und Identitätskontrolle**
 - 5.4.1 Multi-Faktor-Authentisierung (MFA)
 - 5.4.2 Rollenbasierte Zugriffssteuerung (RBAC)
- 5.4.3 Sichere Verwaltung privilegierter Accounts (PAM)**
 - 5.5 Überwachung und Protokollierung
 - 5.5.1 Logging-Strategien für Netzwerke
 - 5.5.2 Echtzeit-Monitoring mit Dashboards
 - 5.5.3 SIEM-Systeme
 - 5.5.4 Anomalieerkennung durch KI-gestützte Tools
 - 5.6 OT-Security – Zone und Conduit Model
- 6 Security Awareness – Der Faktor Mensch**
 - 6.1 Mitarbeiter einbeziehen**
 - 6.1.1 Cyberhygiene
 - 6.1.2 NIS2 fordert Schulung
 - 6.2 Awareness Programme**
 - 6.2.1 Transparenz und Verhalten
 - 6.2.2 Wirksamkeit hinterfragen
 - 6.2.3 Vertraulichkeit
 - 6.3 Methoden von Security Awareness Trainings**
 - 6.3.1 Zentrale Rolle
 - 6.3.2 Vertiefende Maßnahmen
 - 6.3.3 KI & ML – Dynamische Trainings
 - 6.4 Herausforderung – AI Based Social Engineering**
 - 6.4.1 Mining mit LLMs
 - 6.4.2 KI Phishing
 - 6.4.3 KI-Angriffe erkennen
- 7 Krisenmanagement und Incident Response**
 - 7.1 Notfallmanagement**
 - 7.1.1 Vorfalunterstützung – Mit CERT-Bund und MIRT
 - 7.1.2 Erstellung eines Notfallhandbuchs
 - 7.1.3 Testen und Verfeinern von Wiederanlaufprozessen
 - 7.2 Entwicklung eines Incident-Response-Plans**
 - 7.2.1 Monitoring und automatisierte Alarme bei Systemausfällen
 - 7.2.2 Definition von Eskalationsstufen
 - 7.2.3 Einsatz eines Incident Response Teams
 - 7.3 Durchführung von Notfallübungen und Simulationen**
 - 7.3.1 Planspiele für Sicherheitsvorfälle – Blue Teaming
 - 7.3.2 Testlauf für Business Continuity Management
 - 7.4 Aufbau und Betrieb eines Security Operation Centers (SOC)**
 - 7.4.1 Technische Anforderungen an ein SOC
 - 7.4.2 Aufgaben und täglicher Betrieb eines SOC
 - 7.4.3 SOC – Modelle und Typen
 - 7.5 SOC als Managed Service – MSSP
 - 7.5.1 Service-Level-Agreements (SLAs) und Reaktionszeiten
 - 7.5.2 Datenhoheit und Compliance
 - 7.5.3 Transparenz und Reporting
 - 7.5.4 Integration in die bestehende IT-Sicherheitsarchitektur
 - 7.6 Kontinuierliche Verbesserung und Feedback-Schleifen
 - 7.6.1 Forensische Analyse von Sicherheitsvorfällen
 - 7.6.2 Lessons Learned aus Sicherheitsvorfällen
 - 7.6.3 Anpassung von Richtlinien und Prozessen

