

IoT Security – In Industrie, Unternehmen und Haushalt («IOTSEC»)

Erfahren Sie, warum Sprachassistenten wie Alexa ins Sicherheitskonzept Ihres Unternehmens gehören und wie Sie vernetzte Produktionsanlagen nachhaltig absichern – ohne selbst Maschinenbauer oder Chemieingenieur zu sein.

Dauer: 2 Tage

Preis: 2'200.– zzgl. 8.1% MWST

Kursdokumente: Digicomp Kursunterlagen

Inhalt

1. Einführung IoT-Security
 - IoT-Security vs. Cybersecurity
 - Verbraucher vs. industrielle IoT-Geräte
 - Warum IoT-Security wichtig ist
 - Wie gehen Organisationen an das Thema IoT-Security heran?
 - Prinzipien der IoT-Security
 - Aufkommende Technologien für IoT-Security
 - IoT-Security
2. Überblick IoT-Technologien
 - IoT: Historischer Hintergrund
 - Entwicklung von IoT-Technologien
 - Cyber-physikalische Systeme
 - Aufkommende IoT-Technologien
 - IoT-Technologien: Risiken vs. Chancen
3. Das IoT-Ökosystem verstehen
 - Der Lebenszyklus von IoT-Geräten
 - IoT-Architekturen
 - Elemente eines IoT-Ökosystems
4. Risiken und Probleme im IoT-Bereich
 - Herausforderungen
 - Bedrohungen
 - Schwachstellen
 - Angriffe
5. IoT-Security Konzepte entwerfen
 - IoT-Security und IoT-Systeme (Lebenszyklus)
 - Security für die IoT-Entwicklung
 - Security für die IoT-Implementierung
 - Sich entwickelnde Richtlinien und Standards
6. IoT-Security: technische Massnahmen
 - Hardware-Security
 - Software- und Firmware-Security
 - Sensoren
 - Schnittstellen
 - Netzwerk Security
 - Protokolle
 - Cloud- und webbasierte Elemente
7. Identitäts- und Zugriffsmanagement (IAM)
 - IAM Grundlagen
 - Entwerfen einer effektiven IAM-Infrastruktur
 - Entwurf von sicheren Authentifizierungsverfahren

- Entwerfen effektiver Autorisierungsmechanismen
- 8. Implementieren einer IoT-Security Strategie
 - Entwicklung und Durchsetzung von Strategien, Richtlinien, Prozessen und Verfahren
 - Bewertung und Management von Risiken
 - Verwaltung von Zulieferern und Drittanbietern
 - Kontinuierliche Überwachung und Analyse
 - Security Awareness
 - Incident Management
 - Security Audits
 - Penetration Testing

Key Learnings

- Verständnis über die Grundlagen von IoT-Security
- Überblick der IoT-Technologien
- Verständnis über das IoT-Ökosystem
- Kenntnisse über die Sicherheitsrisiken und Probleme im IoT-Bereich
- Entwerfen von IoT-Security Konzepten
- Kenntnisse über technische Massnahmen von IoT-Security
- Kenntnisse über das Identitäts- und Zugriffsmanagement (IAM)
- Implementieren einer IoT-Security-Strategie

Methodik & Didaktik

- 1. Tag: Vormittags Theorie / Nachmittags Gruppenarbeit
- 2. Tag: Vormittags Hacking Lab / Nachmittags Theorie & Abschluss

Zielpublikum

Dieser Kurs richtet sich an CIO, CISO, IT Manager, IT Sicherheitsbeauftragte, Projektverantwortliche und Administratoren.

Weiterführende Kurse

- [IoT Security Hacks – Hands-On \(«IOTSE2»\)](#)

Haben Sie Fragen oder möchten Sie einen Firmenkurs buchen?

Wir beraten Sie gerne unter 044 447 21 21 oder info@digicomp.ch. Detaillierte Infos zu den Terminen finden Sie unter www.digicomp.ch/weiterbildung-security/cyber-security-defense/kurs-iot-security-in-industrie-unternehmen-und-haushalt