

Industrial Security

Sicherheitsmanagement, Firewalling und Safety in der OT

Waren Fabrikationsumgebungen bislang weitgehend autark und von anderen Netzen isoliert, so werden im Rahmen von Industrie 4.0 die Systeme und Steuerungen zunehmend mit dem IT-Netzwerk vernetzt. Ziel ist es, die Prozesse zu optimieren und zu automatisieren. Die ersten Schadprogramme wie Stuxnet, Wannacry & Co. aber zeigten, dass somit massive Gefahren für die Sicherheit ganzer Industrie-Systeme entstehen. Der Absicherung durch intelligente Firewalls, IDS-Systeme und weitere Schutzmaßnahmen kommt somit eine sehr hohe Bedeutung zu, wobei sich die Anforderungen zwischen der klassischen IT-Welt und einer Fabrikationsumgebung stark unterscheiden. Zudem werden hohe Standards an die Betriebssicherheit (Safety) der industriellen Netzwerke gestellt.

Kursinhalt

- Typische Angriffe auf Fabrikumgebungen und Sicherheitslücken
- Risikoanalyse
- Kommunikationswege im ICS und deren Schutz
- Sicherheitskonzepte für die Kopplung von IT und Fabrikation
- Identity and Access Management (IAM)
- Device Hardening und Virens Scanner – Design und Umsetzung im ICS
- Sicherheit durch Visibility und Transparenz
- Firewalls – Design und Umsetzung im ICS
- Intrusion Detection Systeme (IDS) – Design und Umsetzung im ICS
- Fernwartungszugänge sowie VPNs für Predictive Maintenance – Design und Umsetzung im ICS
- Wireless LAN und WirelessHART: Sicherheitslücken und deren Absicherung
- Smartphone und Tablets im ICS
- Security Information and Event Management (SIEM) im ICS
- Design und Architektur von industriellen Sicherheitslösungen: IEC-62443
- Schutz spezifischer Protokolle wie PROFINET, Modbus, Ethernet/IP usw.
- Weitere Standards und Best Practices
- Safety – Vorschriften und Umsetzung

E-Book Das ausführliche deutschsprachige digitale Unterlagenpaket, bestehend aus PDF und E-Book, ist im Kurspreis enthalten.

Zielgruppe

Dieser Kurs wendet sich an Netzwerkadministratoren und Netzplaner, die eine Security Policy in industriellen Umgebungen planen und umsetzen müssen. Praktische Beispiele und Traces vertiefen das erlernte Wissen.

Voraussetzungen

Für die erfolgreiche Teilnahme sind grundlegende Kenntnisse zu industriellen Netzwerken notwendig.

Dieser Kurs im Web



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

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.

Training	Preise zzgl. MwSt.	
Termine in Deutschland	3 Tage	€ 2.195,-
Online Training	3 Tage	€ 2.195,-
Termin/Kursort	Kursprache Deutsch 	
22.10.-24.10.25  Frankfurt	22.10.-24.10.25  Online	

Stand 07.05.2025



EXPERTeach



Inhaltsverzeichnis

Industrial Security – Sicherheitsmanagement, Firewalling und Safety in der OT

1 Grundlagen industrieller Sicherheit	Sicherheitslösungen	5.5 Anomalie und Threat Detection
1.1 Industrie 4.0: Neue Risiken und Herausforderungen	3.5.1 Visibility und Transparenz	5.6 Security Monitoring
1.2 Begriffe und ihre Bedeutung	3.5.2 Design von Fernwartungszugängen am Beispiel Siemens	5.7 Security Responding
1.3 Sicherheitsempfehlungen für industrielle Netzwerke	3.6 Zugriffsschutz auf Systeme und Netze	6 Best Practices und Trends
1.4 Maßnahmen und Tools zur Steigerung von Sicherheit und Verfügbarkeit in der Industrie	3.6.1 Komponenten	6.1 Best Practices
1.4.1 Lösungen zur Umsetzung der Sicherheitsmaßnahmen	3.6.2 MAC Address Bypass	6.2 Trends und Ausblick
1.4.2 Fernwartungszugang	3.6.3 Secure Group Tagging	
1.4.3 IDS/IPS-Systeme	3.7 Firewalls – Design und Umsetzung im ICS	
1.4.4 Security Information and Event Management – SIEM	4 Sicherheit von industriellen Netzwerkprotokollen	
1.5 Bekannte Bedrohungen und Trends	4.1 Entstehung Feldbus-Systeme und Industrielles Ethernet	
1.6 Risikoanalyse	4.2 Modbus	
1.7 Standards	4.3 Profibus	
1.8 Typische Anbieter	4.4 Profinet	
2 Safety – Vorschriften und Umsetzung	4.5 EtherNet/IP	
2.1 Definition	4.6 Wireless ICS-Technologien	
2.2 Entwicklung	4.6.1 WirelessHART	
2.3 Vorschriften	4.7 Wireless LAN (WLAN)	
2.4 Handlungsempfehlungen	4.7.1 Authentisierung im WLAN	
3 Sicherheitskonzepte für die Kopplung von IT und Fabrikation	4.7.2 Neue Mechanismen für mehr Sicherheit im WLAN	
3.1 Sicherheitsaspekte in Fabrikationsumgebungen	4.7.3 WPA: Wi-Fi Protected Access	
3.2 Kommunikationswege im ICS	4.7.4 Authentisierung nach IEEE 802.1X	
3.3 Typische Angriffe und Sicherheitslücken	4.7.5 IEEE 802.11i	
3.3.1 Angriff auf Netzwerke	4.7.6 Protected Management Frames	
3.3.2 Angriff auf Server	4.8 OPC – Open Platform Communications	
3.3.3 Client Site Attacks	4.9 Local Area Networks (LANs)	
3.3.4 Mobile Endgeräte angreifen	4.9.1 MAC Spoofing	
3.3.5 Social Engineering	4.9.2 ARP Cache Poisoning	
3.3.6 Angriffe im Internet of Things	4.9.3 Neighbor Solicitation	
3.3.7 Cloud Security	4.9.4 Flooding der Switching Table	
3.3.8 Advanced Persistent Threats	4.9.5 VLAN Hopping	
3.4 Typische Angriffe auf Fabrikumgebungen	4.9.6 Mirror Ports	
3.4.1 Physikalischer Zugriff	4.9.7 DHCP Spoofing	
3.4.2 Ungeschützte Netzzugänge	4.9.8 Router Advertisements	
3.4.3 Mobile Endgeräte und Wechseldataenträger	4.9.9 Schutz von LAN-Umgebungen	
3.4.4 Türschließsysteme und Thermostate	5 Cyber Risk: Erkennung, Auswertung und Reaktion	
3.4.5 Fernwartungszugänge	5.1 Cyber Risk in Fabrikumgebungen	
3.4.6 Watering Hole Attacks	5.2 Risiken	
3.5 Design und Architektur von industriellen	5.3 Sicherheitsmetriken	
	5.4 Situative Awareness	

