ExperTeach Networking

Security in Fabrikationsumgebungen

Firewalling und Safety

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 Virenscanner – 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 Sie erhalten das ausführliche deutschsprachige Unterlagenpaket aus der Reihe ExperTeach Networking – Print, E-Book und personalisiertes PDF!

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, wie sie in den Kursen Industrielles Ethernet I – Design und Implementierung und Industrielles Ethernet II – Spezielle Anforderungen und Protokolle vermittelt werden.

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/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.
Classroom Training	**3 Tage**	**CHF 2.795,-**

Termin/Kursort

09.12.-11.12.19	Frankfurt	02.11.-04.11.20	Frankfurt
20.04.-22.04.20	Frankfurt		

Stand 03.10.2019

Security in Fabrikationsumgebungen

Digitalisierung, Industrie 4.0 & IoT

Inhaltsverzeichnis

Security in Fabrikationsumgebungen – Firewalling und Safety

1 Grundlagen industrieller Sicherheit
1.1 Industrie 4.0: Neue Risiken und Herausforderungen
1.2 Begriffe und ihre Bedeutung
1.3 Sicherheitsempfehlungen für industrielle Netzwerke
1.4 Maßnahmen und Tools zur Steigerung von Sicherheit und Verfügbarkeit in der Industrie
1.4.1 Lösungen zur Umsetzung der Sicherheitsmaßnahmen
1.4.2 Fernwartungszugang
1.4.3 IDS/IPS-Systeme
1.4.4 Security Information and Event Management – SIEM
1.5 Bekannte Bedrohungen und Trends
1.6 Risikoanalyse
1.7 Standards
1.8 Typische Anbieter

2 Safety – Vorschriften und Umsetzung
2.1 Definition
2.2 Entwicklung
2.3 Vorschriften
2.4 Handlungsempfehlungen

3 Sicherheitskonzepte für die Kopplung von IT und Fabrikation
3.1 Sicherheitsaspekte in Fabrikationsumgebungen
3.2 Kommunikationswege im ICS
3.3 Typische Angriffe und Sicherheitslücken
3.3.1 Angriff auf Netzwerke
3.3.2 Angriff auf Server
3.3.3 Client Site Attacks
3.3.4 Mobile Endgeräte angreifen
3.3.5 Social Engineering
3.3.6 Angriffe im Internet of Things
3.3.7 Cloud Security
3.3.8 Advanced Persistent Threats
3.4 Typische Angriffe auf Fabrikumgebungen
3.4.1 Physikalischer Zugriff
3.4.2 Ungeschützte Netzzugänge
3.4.3 Mobile Endgeräte und Wechseldatenträger
3.4.4 Türschließsysteme und Thermostate
3.4.5 Fernwartungszugänge
3.4.6 Watering Hole Attacks
3.5 Design und Architektur von industriellen Sicherheitslösungen
3.5.1 Visibility und Transparenz
3.5.2 Design von Fernwartungszugängen am Beispiel Siemens
3.6 Zugriffsschutz auf Systeme und Netze
3.6.1 Komponenten
3.6.2 MAC Address Bypass
3.6.3 Secure Group Tagging
3.7 Firewalls – Design und Umsetzung im ICS

4 Sicherheit von industriellen Netzwerkprotokollen
4.1 Entstehung Feldbus-Systeme und Industrielles Ethernet
4.2 Modbus
4.3 Profibus
4.4 Profinet
4.5 EtherNet/IP
4.6 Wireless ICS-Technologien
4.6.1 WirelessHART
4.7 Wireless LAN (WLAN)
4.7.1 Authentisierung im WLAN
4.7.2 Neue Mechanismen für mehr Sicherheit im WLAN
4.7.3 WPA: Wi-Fi Protected Access
4.7.4 Authentisierung nach IEEE 802.1X
4.7.5 IEEE 802.11i
4.7.6 Protected Management Frames
4.8 OPC – Open Platform Communications
4.9 Local Area Networks (LANs)
4.9.1 MAC Spoofing
4.9.2 ARP Cache Poisoning
4.9.3 Neighbor Solicitation
4.9.4 Flooding der Switching Table
4.9.5 VLAN Hopping
4.9.6 Mirror Ports
4.9.7 DHCP Spoofing
4.9.8 Router Advertisements
4.9.9 Schutz von LAN-Umgebungen

5 Cyber Risk: Erkennung, Auswertung und Reaktion
5.1 Cyber Risk in Fabrikumgebungen
5.2 Risiken
5.3 Sicherheitsmetriken
5.4 Situative Awareness
5.5 Anomalie und Threat Detection
5.6 Security Monitoring
5.7 Security Responding

6 Best Practices und Trends
6.1 Best Practices
6.2 Trends und Ausblick

ExperTeach AG
Kronenstrasse 11 • 8735 St. Gallenkappel • Telefon: +41 55 420 2591 • Fax: +41 55 420 2592
info@experteach.ch • www.experteach.ch