ExperTeach NETWORKING

Security-Konzepte und Technologien

Verschlüsselung, Authentisierung und Datenintegrität

Netzwerksicherheit ist von entscheidender Bedeutung, um die Privatsphäre, Sicherheit und das reibungslose Funktionieren von Netzwerken und damit verbundenen Diensten zu gewährleisten.

Unternehmen, Organisationen und Einzelpersonen müssen angemessene Sicherheitsmaßnahmen implementieren, um sich vor den vielfältigen Bedrohungen in der digitalen Welt zu schützen.

In diesem Security-Kurs werden unterschiedliche Methoden vorgestellt, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Ressourcen in einem Computernetzwerk sicherzustellen. Das in diesem Kurs vermittelte Know-how legt damit den Grundstein für die eigenverantwortliche Übernahme von Aufgaben in der Security-Planung und -Administration IP-basierter Netzwerke. Gleichzeitig ist es die Basis für eine Vielzahl von weiterführenden Kursen im Security-Bereich.

Kursinhalt

- Ziele von Netzwerksicherheit
- Schwachstellen IP-basierter Netzwerke
- Typische Angriffs-Methoden
- Planung und Management von Sicherheitsmaßnahmen
- Symmetrische und asymmetrische Verschlüsselung
- Datenintegrität und Authentiziät
- Authentisierungsmaßnahmen
- Zertifikate und PKI
- IPsec und TLS zur Sicherung von Kommunikationsprozessen
- Firewalls, IPS und Proxys
- Applikationssicherheit für E-Mail, WWW und DNS
- Network Access Control
- LAN Security – Von ARP Inspection bis IEEE 802.1X
- WLAN-Security
- VPNs – Die Sicherung privater Daten
- Security in Cloud-Umgebungen
- SD-WAN und SASE
- Endpoint Security – Antivirus, Antispyware Firewall & Co.
- Security Awareness – Die Mitarbeiter einbinden

Zielgruppe

Technische Hintergründe und Maßnahmen zur Netzwerk-Sicherheit, wie sie in diesem Security-Kurs vermittelt werden, sind im Grunde für alle interessant, die in irgendeiner Form mit Computernetzwerken und dem Internet in Berührung kommen.
Insbesondere eignet sich der Kurs für Administratoren, Planer und Consultants, die einen umfassenden Überblick über dieses Themen-Umfeld benötigen.

Voraussetzungen

Optimale Voraussetzungen sind fundiertes Basiswissen im Umfeld LAN, Router und Internet sowie tiefer gehende Kenntnisse des IP-Protokolls.

Kursziel

Der Kurs vermittelt Ihnen zunächst die Grundlagen der Kryptografie, um das Prinzip sicherer Kommunikation zu verstehen. Anschließend erhalten Sie einen Überblick über Sicherheitsmechanismen im Netzwerk sowie die sichere Nutzung von Protokollen, und lernen deren gezielten Einsatz zum Schutz der eigenen Architektur einzuschätzen.

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/**SECU**

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 € 225,- (zzgl. MwSt) erwerben.

Training	Preise zzgl. MwSt.
Termine in Deutschland	5 Tage CHF 2.855,-
Termine in Österreich	5 Tage CHF 2.855,-
Termine in der Schweiz	5 Tage CHF 3.290,-
Online Training	5 Tage CHF 2.855,-

Termin/Kursort — Kurssprache Deutsch

07.12.-11.12.26	HY Düsseldorf	14.06.-18.06.27	HY Online
07.12.-11.12.26	HY Online	12.07.-16.07.27	HY Berlin
18.01.-22.01.27	HY Berlin	12.07.-16.07.27	HY Hamburg
18.01.-22.01.27	HY Hamburg	12.07.-16.07.27	HY Online
18.01.-22.01.27	HY Online	12.07.-16.07.27	HY Online
18.01.-22.01.27	HY Online	16.08.-20.08.27	HY Frankfurt
22.02.-26.02.27	HY Frankfurt	16.08.-20.08.27	HY Online
22.02.-26.02.27	HY Online	16.08.-20.08.27	HY Online
22.02.-26.02.27	HY Online	16.08.-20.08.27	HY Zürich
22.02.-26.02.27	HY Zürich	13.09.-17.09.27	HY Online
05.04.-09.04.27	HY Online	13.09.-17.09.27	HY Wien
05.04.-09.04.27	HY Wien	18.10.-22.10.27	HY Düsseldorf
10.05.-14.05.27	HY Düsseldorf	18.10.-22.10.27	HY Online
10.05.-14.05.27	HY Online	22.11.-26.11.27	HY München
14.06.-18.06.27	HY München	22.11.-26.11.27	HY Online

Stand 27.10.2026

ExperTeach

Inhaltsverzeichnis

Security-Konzepte und Technologien – Verschlüsselung, Authentisierung und Datenintegrität

1 Cybersecurity – Angriffe und Gegenmaßnahmen
1.1 Attack Vector und Attack Surface
1.1.1 Angreifer und ihre Motive
1.1.2 Angriffsziele
1.2 Targets und Assets
1.2.1 Firmen auskundschaften
1.2.2 Netzwerke durchleuchten
1.2.3 Social Engineering - Mining
1.3 Angriffsvarianten
1.3.1 Exploitation
1.3.2 Social Engineering Attacks
1.3.3 DoS-Varianten
1.4 Protokoll- und Netzwerkangriffe
1.4.1 LAN Attacks
1.4.2 WLAN Sicherheit
1.4.3 Das Internet-Protokoll und seine Schwächen
1.4.4 Angriffe auf Router
1.4.5 Angriffe auf die Schicht 4
1.4.6 Applikationen angreifen

2 Sicherheit planen und umsetzen
2.1 Rechtliche Security-Vorgaben
2.1.1 Richtlinien und Zertifizierungen (ISO 27001)
2.1.2 BSI – IT-Grundschutz
2.1.3 KRITIS
2.1.4 NIS2 und RCE
2.2 Strukturanalyse – Plan
2.2.1 Sicherheitsrichtlinien
2.2.2 Security Policy – Zugriffsregeln erstellen
2.3 Schutzmaßnahmen im Überblick – Do
2.4 Schwachstellenanalyse und Penetrations-Tests – Check
2.5 Angriffe erkennen – Act

3 Grundlagen der Kryptographie
3.1 Verschlüsselung
3.1.1 Symmetrische Verschlüsselung
3.1.2 Asymmetrische Verschlüsselung
3.1.3 Key Management
3.2 Datenintegrität durch Hash-Werte
3.2.1 Typische Eigenschaften
3.2.2 Bekannte Verfahren
3.3 Authentisierung
3.3.1 Password-based
3.3.2 Single Sign On
3.3.3 Biometrie
3.3.4 Public-Key-Verfahren
3.4 Zertifikate
3.4.1 Zertifikate beantragen
3.4.2 Zertifikate ausstellen
3.4.3 Authentisierung
3.4.4 Certificate Revocation List
3.4.5 Infrastruktur

4 Kommunikationsprozesse sichern
4.1 IPsec – Sicherheit für IP
4.1.1 Die IPsec-Header
4.1.2 IKEv1
4.1.3 IKEv2
4.2 SSL/TLS – Applikations-Sicherheit
4.2.1 Der TLS Protokollstapel
4.2.2 TLS-Versionen und SSL
4.2.3 Der Verbindungsaufbau bis TLS 1.2
4.2.4 Der Verbindungsaufbau bei TLS 1.3

5 Das Design sicherer Netze
5.1 Sicherheitszonen trennen
5.1.1 VLANs -Trennung auf Ebene 2
5.1.2 IP Security Zones
5.2 Firewalls
5.2.1 Statische Paketfilter
5.2.2 Stateful Firewalls
5.2.3 Regelwerke
5.2.4 Next Generation Firewall
5.2.5 DMZ-Konzepte
5.3 Proxy – Stellvertreter für Client und Server
5.4 Intrusion Prevention System
5.4.1 Host-based IPS - HIPS
5.4.2 Network-based IPS - NIPS
5.4.3 Detection und Prevention Methoden
5.5 SIEM Systeme

6 Applikationen sichern
6.1 Absicherung der Dienste
6.2 DNS-Kommunikation
6.2.1 DNSsec
6.2.2 DANE
6.2.3 DNS over TLS/DTLS vs. DNS over HTTPS
6.3 E-Mail-Kommunikation sichern
6.3.1 Spam
6.3.2 Malware in E-Mails
6.3.3 Phishing
6.3.4 E-Mail: Security-Konzepte
6.3.5 Anti-Spoofing mit SPF, DKIM und DMARC
6.4 Web Security
6.4.1 Schutzmaßnahmen
6.4.2 Web Application Firewall – Reverse Proxy
6.5 TLS Inspection
6.5.1 Outbound Inspection
6.5.2 Inbound Inspection

7 Network Access Control
7.1 RADIUS – Ein AAA Dienst
7.1.1 Protokollabläufe
7.1.2 Das Paketformat
7.1.3 RADIUS-Authentisierung und Autorisierung
7.1.4 RADIUS Accounting
7.1.5 AD-Integration
7.1.6 LDAP-Anbindung
7.2 LAN Security
7.2.1 IEEE 802.1X
7.2.2 MAC Auth bzw. MAB
7.2.3 Web Auth und Guest Access
7.2.4 MacSec – IEEE 802.1AE
7.3 WLAN Security
7.3.1 WPA2 und IEEE 802.11i
7.3.2 WPA3 – Verbesserte Sicherheit
7.4 VPN Verbindungen
7.4.1 Site-2-Site VPNs
7.4.2 Remote Access VPNs
7.4.3 Clientless TLS VPN

8 Cloud Services schützen
8.1 Cloud Computing – IT im Wandel
8.1.1 Treiber für die Cloud
8.1.2 Cloud-Varianten – Private, Public &Co.
8.2 Sicherheit in der Cloud
8.2.1 Public Cloud vs. interne IT
8.2.2 Cloud-Modelle und Security-Verantwortung
8.2.3 Datenschutz in der Cloud
8.2.4 C5 Testat – Audits für die Cloud
8.3 Sichere Server-Virtualisierung
8.3.1 Schutzmaßnahmen in virtuellen Netzwerken
8.3.2 Container-Virtualisierung
8.4 Sicherer Zugriff auf die Cloud
8.4.1 Erreichbarkeit von Services in der Cloud
8.4.2 Client to Cloud-Services schützen
8.4.3 SD-WAN
8.5 Secure Access Service Edge (SASE)

9 Endpoint Security
9.1 Client Side Attacks
9.2 Schutzmaßnahmen
9.2.1 Viren- und Bedrohungs-Schutz
9.2.2 Patch Management
9.2.3 Festplattenverschlüsselung
9.2.4 Host-Based Firewalls
9.3 Peripherie-Geräte sichern

10 Security Awareness
10.1 Der Mensch – das schwächste Glied?
10.1.1 Grenzen der IT Security
10.1.2 Schulung und Training erforderlich
10.2 Themen und Lernziele von Security Awareness
10.2.1 Security Maßnahmen transparent machen
10.2.2 Verhaltensmaßnahmen vermitteln
10.2.3 Vertraulichkeit plausibel machen
10.2.4 Die Hintergründe erläutern
10.3 Methoden von Security Awareness Trainings
10.3.1 In den Alltag einbinden
10.3.2 Vertiefende Maßnahmen

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