

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 Authentizität
- 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

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

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.

Dieser Kurs im Web



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

Training	Preise zzgl. MwSt.	
Termine in Deutschland	5 Tage	€ 2.595,-
Termine in der Schweiz	5 Tage	€ 3.390,-
Online Training	5 Tage	€ 2.595,-
Termin/Kursort	Kurs Sprache Deutsch	
02.06.-06.06.25	München	15.09.-19.09.25 Frankfurt
02.06.-06.06.25	Online	15.09.-19.09.25 Online
07.07.-11.07.25	Berlin	03.11.-07.11.25 Düsseldorf
07.07.-11.07.25	Online	03.11.-07.11.25 Online
11.08.-15.08.25	Düsseldorf	08.12.-12.12.25 München
11.08.-15.08.25	Online	08.12.-12.12.25 Online
18.08.-22.08.25	Frankfurt	08.12.-12.12.25 Zürich

Stand 13.05.2025



EXPERTeach



Inhaltsverzeichnis

Security-Konzepte und Technologien – Verschlüsselung, Authentisierung und Datenintegrität

1	Cybersecurity – Angriffe und Gegenmaßnahmen	4.1	IPsec – Sicherheit für IP	7.2	LAN Security
1.1	Attack Vector und Attack Surface	4.1.1	Die IPsec-Header	7.2.1	IEEE 802.1X
1.1.1	Angreifer und ihre Motive	4.1.2	IKEv1	7.2.2	MAC Auth bzw. MAB
1.1.2	Angriffsziele	4.1.3	IKEv2	7.2.3	Web Auth und Guest Access
1.2	Targets und Assets	4.2	SSL/TLS – Applikations-Sicherheit	7.2.4	MacSec – IEEE 802.1AE
1.2.1	Firmen auskundschaften	4.2.1	Der TLS Protokollstapel	7.3	WLAN Security
1.2.2	Netzwerke durchleuchten	4.2.2	TLS-Versionen und SSL	7.3.1	WPA2 und IEEE 802.11i
1.2.3	Social Engineering - Mining	4.2.3	Der Verbindungsaufbau bis TLS 1.2	7.3.2	WPA3 – Verbesserte Sicherheit
1.3	Angriffsvarianten	4.2.4	Der Verbindungsaufbau bei TLS 1.3	7.4	VPN Verbindungen
1.3.1	Exploitation	5	Das Design sicherer Netze	7.4.1	Site-2-Site VPNs
1.3.2	Social Engineering Attacks	5.1	Sicherheitszonen trennen	7.4.2	Remote Access VPNs
1.3.3	DoS-Varianten	5.1.1	VLANs -Trennung auf Ebene 2	7.4.3	Clientless TLS VPN
1.4	Protokoll- und Netzwerkangriffe	5.1.2	IP Security Zones	8	Cloud Services schützen
1.4.1	LAN Attacks	5.2	Firewalls	8.1	Cloud Computing – IT im Wandel
1.4.2	WLAN Sicherheit	5.2.1	Statische Paketfilter	8.1.1	Treiber für die Cloud
1.4.3	Das Internet-Protokoll und seine Schwächen	5.2.2	Stateful Firewalls	8.1.2	Cloud-Varianten – Private, Public & Co.
1.4.4	Angriffe auf Router	5.2.3	Regelwerke	8.2	Sicherheit in der Cloud
1.4.5	Angriffe auf die Schicht 4	5.2.4	Next Generation Firewall	8.2.1	Public Cloud vs. interne IT
1.4.6	Applikationen angreifen	5.2.5	DMZ-Konzepte	8.2.2	Cloud-Modelle und Security-Verantwortung
2	Sicherheit planen und umsetzen	5.3	Proxy – Stellvertreter für Client und Server	8.2.3	Datenschutz in der Cloud
2.1	Rechtliche Security-Vorgaben	5.4	Intrusion Prevention System	8.2.4	C5 Testat – Audits für die Cloud
2.1.1	Richtlinien und Zertifizierungen (ISO 27001)	5.4.1	Host-based IPS - HIPS	8.3	Sichere Server-Virtualisierung
2.1.2	BSI – IT-Grundschutz	5.4.2	Network-based IPS - NIPS	8.3.1	Schutzmaßnahmen in virtuellen Netzwerken
2.1.3	KRITIS	5.4.3	Detection und Prevention Methoden	8.3.2	Container-Virtualisierung
2.1.4	NIS2 und RCE	5.5	SIEM Systeme	8.4	Sicherer Zugriff auf die Cloud
2.2	Strukturanalyse – Plan	6	Applikationen sichern	8.4.1	Erreichbarkeit von Services in der Cloud
2.2.1	Sicherheitsrichtlinien	6.1	Absicherung der Dienste	8.4.2	Client to Cloud-Services schützen
2.2.2	Security Policy – Zugriffsregeln erstellen	6.2	DNS-Kommunikation	8.4.3	SD-WAN
2.3	Schutzmaßnahmen im Überblick – Do	6.2.1	DNSsec	8.5	Secure Access Service Edge (SASE)
2.4	Schwachstellenanalyse und Penetrations-Tests – Check	6.2.2	DANE	9	Endpoint Security
2.5	Angriffe erkennen – Act	6.2.3	DNS over TLS/DTLS vs. DNS over HTTPS	9.1	Client Side Attacks
3	Grundlagen der Kryptographie	6.3	E-Mail-Kommunikation sichern	9.2	Schutzmaßnahmen
3.1	Verschlüsselung	6.3.1	Spam	9.2.1	Viren- und Bedrohungs-Schutz
3.1.1	Symmetrische Verschlüsselung	6.3.2	Malware in E-Mails	9.2.2	Patch Management
3.1.2	Asymmetrische Verschlüsselung	6.3.3	Phishing	9.2.3	Festplattenverschlüsselung
3.1.3	Key Management	6.3.4	E-Mail: Security-Konzepte	9.2.4	Host-Based Firewalls
3.2	Datenintegrität durch Hash-Werte	6.3.5	Anti-Spoofing mit SPF, DKIM und DMARC	9.3	Peripherie-Geräte sichern
3.2.1	Typische Eigenschaften	6.4	Web Security	10	Security Awareness
3.2.2	Bekanntes Verfahren	6.4.1	Schutzmaßnahmen	10.1	Der Mensch – das schwächste Glied?
3.3	Authentisierung	6.4.2	Web Application Firewall – Reverse Proxy	10.1.1	Grenzen der IT Security
3.3.1	Password-based	6.5	TLS Inspection	10.1.2	Schulung und Training erforderlich
3.3.2	Single Sign On	6.5.1	Outbound Inspection	10.2	Themen und Lernziele von Security Awareness
3.3.3	Biometrie	6.5.2	Inbound Inspection	10.2.1	Security Maßnahmen transparent machen
3.3.4	Public-Key-Verfahren	7	Network Access Control	10.2.2	Verhaltensmaßnahmen vermitteln
3.4	Zertifikate	7.1	RADIUS – Ein AAA Dienst	10.2.3	Vertraulichkeit plausibel machen
3.4.1	Zertifikate beantragen	7.1.1	Protokollabläufe	10.2.4	Die Hintergründe erläutern
3.4.2	Zertifikate ausstellen	7.1.2	Das Paketformat	10.3	Methoden von Security Awareness Trainings
3.4.3	Authentisierung	7.1.3	RADIUS-Authentisierung und Autorisierung	10.3.1	In den Alltag einbinden
3.4.4	Certificate Revocation List	7.1.4	RADIUS Accounting	10.3.2	Vertiefende Maßnahmen
3.4.5	Infrastruktur	7.1.5	AD-Integration		
4	Kommunikationsprozesse sichern	7.1.6	LDAP-Anbindung		

