ZTNA, XDR & Endpoint Security

Zukunftsfähige Cybersicherheit!

Die IT-Landschaft hat sich in den letzten Jahren dramatisch gewandelt! Home-Office und mobiles Arbeiten sind in vielen Branchen zur Normalität geworden. Damit haben sich auch die Anforderungen an die IT-Infrastruktur verändert. Bekannte Sicherheitstechnologien wie Endpoint Security haben an Bedeutung gewonnen und neue Sicherheitsmethoden wie ZTNA und XDR sind entstanden.

Dieser Kurs beschäftigt sich mit der Absicherung von Endgeräten. Klassische und neue Sicherheitsmethoden und Sicherheitskonzepte wie Remote Access VPN, SASE, ZTNA und XDR werden erläutert. Zudem werden deren Einsatzmöglichkeiten aufgezeigt.

Kursinhalt

- Aktuelle Bedrohungslage
- Schwächen klassischer Sicherheitsarchitekturen
- Remote Access VPN
- Secure Access Service Edge
- ZTNA
- Endpoint Detection and Response
- Network Detection and Response
- eXtended Detection and Response
- Endpoint Security

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

Zielgruppe

Der Kurs richtet sich an Netzwerkadministratoren und -planer, die sich mit der Implementierung, Konzeption und Realisierung von klassischer und moderner Endpoint Security in IT-Infrastrukturen beschäftigen.

Voraussetzungen

Netzwerk-Grundlagen im Bereich TCP/IP und Routing sind von Vorteil. Im Bereich IT-Sicherheit sollten grundlegende Methoden zur Authentifizierung und Absicherung der Kommunikation bekannt sein.

Kursziel

Sie erlangen Verständnis über die Entstehung und die Komponenten aktueller Sicherheitsarchitekturen. Dabei lernen Sie wichtige Rahmenwerke kennen, die Vorgaben zur Umsetzung der Sicherheitsarchitekturen beinhalten. Außerdem werden Technologien und Methoden wie Remote Access VPN, ZTNA und XDR vermittelt.

Dieser Kurs im Web

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

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	2 Tage CHF 1.975,-
Online Training	2 Tage CHF 1.975,-

Termin/Kursort		Kurssprache Deutsch	
22.02.-23.02.27	HY Frankfurt	13.09.-14.09.27	HY Frankfurt
22.02.-23.02.27	HY Online	13.09.-14.09.27	HY Online
18.05.-19.05.27	HY Frankfurt	22.11.-23.11.27	HY Frankfurt
18.05.-19.05.27	HY Online	22.11.-23.11.27	HY Online

Stand 27.10.2026

ZTNA, XDR & Endpoint Security

Inhaltsverzeichnis

ZTNA, XDR & Endpoint Security – Zukunftsfähige Cybersicherheit!

1 Einleitung und Grundlagen
1.1 Wandel in der IT Landschaft
1.1.1 Von stationären Büros zu mobilen Arbeitsplätzen
1.1.2 Herausforderungen und Chancen für Unternehmen
1.2 Sicherheitsrelevante Aspekte des mobilen Arbeitens
1.2.1 Aktuelle Bedrohungslage
1.2.2 Schwächen klassischer Sicherheitsarchitekturen
1.3 Künstliche Intelligenz und maschinelles Lernen als neue Herausforderung
1.3.1 KI-gestützte Cyberangriffe und Bedrohungsszenarien
1.3.2 KI/ML – Herausforderungen für Home-Office-Sicherheitslösungen

2 Sicherheitsaspekte und Protokolle
2.1 Verschlüsselung von Daten
2.1.1 Symmetrische Verschlüsselung
2.1.2 Asymmetrische Verschlüsselung
2.1.3 Schlüsselaustausch-Varianten
2.2 Datenintegrität und Authentizität
2.2.1 Datenintegrität durch Hash-Werte
2.2.2 Authentizität am Bespiel HMAC
2.3 Klassische Authentisierungsverfahren
2.3.1 Vor- und Nachteile von Kennwörtern
2.3.2 Public-Key-Verfahren
2.3.3 Zertifikate
2.4 Moderne Authentisierungsverfahren
2.4.1 Single Sign On
2.4.2 FIDO2
2.4.3 SAML-Authentication
2.4.4 Biometrie
2.4.5 Multi Faktor Authentisierung
2.4.6 IAM – PIM und PAM

3 Security Frameworks für Home Office-Lösungen
3.1 IPSec – Sicherheit für IP
3.1.1 Sicherung der privaten IP-Pakete
3.1.2 Die IPsec-Header
3.1.3 IKE – Tunnel-Aufbau mit IPsec
3.1.4 Authentisierungsmöglichkeiten bei IPsec
3.1.5 NAT Traversal – NAT-T
3.2 SSL/TLS – Applikations-Sicherheit
3.2.1 TLS-Versionen und SSL
3.2.2 Der TLS-Verbindungsaufbau
3.2.3 Sichere Datenübertragung bei TLS

4 Architekturen für Home-Office und mobiles Arbeiten
4.1 Klassische IT-Architekturen vs. moderne Lösungen
4.2 Dezentrale Arbeitsumgebungen und Cloud Technologien
4.2.1 Moderne Cloud-Lösungen für Unternehmen
4.2.2 Office 365 und vergleichbare Lösungen
4.2.3 Integration von Kollaborationsplattformen
4.2.4 Sicherheitsrisiken und Best Practices für Cloud-Dienste
4.2.5 Vergleich: On-Premises, Hybrid- und Cloud-Ansätze
4.3 Architekturen und Network Access Control
4.3.1 Remote Access (RA)-VPN
4.3.2 Zero Trust Network Access (ZTNA)
4.4 Secure Access Service Edge (SASE)

5 Remote Access VPN (RA VPN)
5.1 Grundlagen von Remote Access VPN
5.2 IPsec RA-VPNs
5.2.1 Erweitere Authentisierung
5.2.2 IPsec und dynamische IP-Adresszuweisung
5.3 TLS VPNs im Einsatz
5.3.1 TLS für RA VPNs
5.3.2 Die Möglichkeiten bei TLS VPNs
5.4 Wireguard RA VPNs
5.5 Sicherheitsaspekte von Remote Access VPNs
5.5.1 Authentifizierung und Zugriffskontrolle
5.5.2 Angriffsszenarien und Schutzmaßnahmen
5.6 Performance und Skalierbarkeit
5.6.1 Bandbreitenanforderungen und Latenz
5.6.2 Lastverteilung und Hochverfügbarkeit
5.6.3 Optimierungsmöglichkeiten für große Nutzerzahlen
5.7 Zukunft von Remote Access VPN

6 Zero Trust Network Access (ZTNA)
6.1 ZTNA Grundlagen
6.1.1 Prinzipien und Funktionsweise
6.1.2 Unterschiede zu traditionellen VPNs
6.1.3 Anwedungsfälle und Einsatzgebiete
6.2 Sicherheitsaspekte von ZTNA
6.2.1 Authentisierung und Identitätsmanagement
6.2.2 Mikrosegmentierung und Zugriffskontrolle
6.2.3 Schutz vor Bedrohungen
6.3 Performance und Skalierbarkeit
6.3.1 Einfluss auf Latenz und Usability
6.3.2 Skaliebarkeit in Cloud-Umgebungen
6.3.3 Integration mit bestehenden IT-Umgebungen
6.4 Die Zukunft von ZTNA
6.4.1 Weiterentwicklung und neue Standards
6.4.2 Kombination mit SASE-Architekturen
6.4.3 Herausforderungen der Implementierung

7 Endpoint Security und moderne Sicherheitsansätze
7.1 Angriffe auf Endgeräte und Herausforderungen im Homeoffice
7.1.1 Typische Angriffsszenarien auf Endgeräte
7.1.2 Sicherheitsrisiken durch gemeinsam genutzte Geräte
7.1.3 Unsichere Netzwerke und Schatten IT
7.2 Endpoint Security Suites vs. klassische AV/AS-Lösungen
7.2.1 Unterschiede und Leistungsmerkmale
7.2.2 Integration mit modernen Sicherheitsplattformen
7.2.3 Vorteile und Herausforderungen bei der Implementierung
7.3 Überwachung und Schutz von Endgeräten
7.3.1 Prozessüberwachung und Verhaltensanalyse
7.3.2 Schutzmechanismen gegen Zero-Day-Exploits
7.3.3 Automatisierte Reaktionen auf Bedrohungen
7.4 Moderne Sicherheitslösungen für Endgeräte
7.4.1 Next-Generation Antivirus (NGAV)
7.4.2 Endpoint Detection & Response (EDR)
7.4.3 EDR & NDR und MDR
7.5 Extended Detection & Response (XDR)
7.5.1 Vorteile und Herausforderungen
7.5.2 Künstliche Intelligenz und maschinelles Lernen

8 Diskussionsrunde
8.1 Sicherheitsanforderungen im Home-Office
8.1.1 Herausforderungen bei der Anbindung an das Firmennetz
8.1.2 Sicherheitsrisiken und empfohlene Maßnahmen
8.2 Remote Access VPN vs. ZTNA
8.2.1 Vorteile und Nachteile beider Technologien
8.2.2 Einsatzszenarien und Empfehlungen
8.2.3 Integration in bestehende IT-Infrastrukturen
8.3 Endpoint Security im Kontext von Home-Office
8.3.1 Bedeutung moderner Endpoint-Sicherheitslösungen
8.3.2 Kombination von NGAV, EDR, NDR und XDR
8.4 Fazit und Ausblick auf die IT-Sicherheit der Zukunft

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