Cisco UC Security

Absichern der CUCM-Umgebung

Platinum Learning Business Enablement

Die komplexe Welt von Unified Communications schafft neue Herausforderungen an die Netzwerksicherheit. In diesem Kurs lernen die Teilnehmer, welche Security-Maßnahmen in einer UC-Umgebung auf Basis des Cisco UCM erforderlich sind. Sie lernen wichtige Angriffsszenarien sowie Best Practices für das richtige Netzdesign zur Abwehr dieser Gefahren kennen. Die Inhalte des Kurses werden an einem Testnetz vertieft.

Kursinhalt

- Symmetrische und asymmetrische Verschlüsselung
- Hash-Werte und Message Authentication Codes
- Zertifikate und PKI
- CallManager als Certificate Authority – Verschlüsselung für Telefone
- Weitere Security-Funktionen des Unified Communications Managers
- Der Unified Communications Manager in einer Enterprise CA
- Switch-based Security – Voice-VLANs bis IEEE.802.1X
- Verschlüsselung zu Gateways und Trunks
- Einsatz der ASA als Phone Proxy
- Einsatz der ASA als TLS Proxy

E-Book Sie erhalten das ausführliche deutschsprachige Unterlagenpaket von ExperTeach – Print, E-Book und personalisiertes PDF!

Zielgruppe

Der Kurs eignet sich für Planer und Administratoren sowie für Sicherheitsbeauftragte, die für die Absicherung einer UC-Infrastruktur auf Basis von Cisco zuständig sind.

Voraussetzungen

Die Teilnehmer sollten gute Security-Kenntnisse mitbringen. Außerdem werden IOS-Kenntnisse mindestens auf dem Niveau eines CCNA Voice sowie Kenntnisse zu Cisco UC vorausgesetzt. Der vorherige Besuch des Kurses Security für VoIP – Verschlüsselung, Authentisierung und Firewalls wird empfohlen.

Dieser Kurs im Web

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

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		**5 Tage**	**CHF 4.795,-**
Termin/Kursort			
25.11.-29.11.19	Frankfurt	11.05.-15.05.20	Frankfurt
09.12.-13.12.19	Wien	23.11.-27.11.20	Frankfurt

Cisco UC Security

Stand 19.09.2019

Deutschsprachige Kurse

Inhaltsverzeichnis

Cisco UC Security – Absichern der CUCM-Umgebung

1 Security im Umfeld des Communication Managers
1.1 Warum Sicherheit bei der Kommunikation wichtig ist
1.1.1 Vertraulichkeit
1.1.2 Unveränderlichkeit
1.1.3 Nachweisbarkeit
1.1.4 Verfügbarkeit
1.2 Native Security-Funktionen
1.2.1 Authentication
1.2.2 Digest Authentication
1.2.3 Secure Signaling
1.2.4 Secure RTP
1.2.5 Encrypted Configuration
1.2.6 IPSec
1.2.7 Phone Hardening
1.2.8 Security by Default

2 Grundlagen der Kryptographie
2.1 Datenschutz durch Verschlüsselung
2.1.1 Symmetrische Verschlüsselung
2.1.2 Asymmetrische Verschlüsselung
2.2 Datenintegrität und Authentisierung
2.2.1 Data Origin Authentication
2.2.2 Authentisierung des Gesprächspartners
2.3 Zertifikate
2.4 PKI und CA
2.4.1 Certificate Revocation List
2.4.2 Online Certificate Status Protocol
2.4.3 SCEP

3 Zertifikate im Communications Manager Umfeld
3.1 Self Signed Certificates
3.2 CAPF – Certificate Authority Proxy Function
3.2.1 Communications Manager als CA
3.2.2 Communications Manager als Subordinated CA
3.2.3 Ersetzen der Self Signed Certificates
3.3 CTL Provider und CTL Client
3.3.1 Set Cluster to Mixed Mode – Klassich
3.3.2 Set Cluster to Mixed Mode – Clientless
3.3.3 Mixed Mode
3.4 Phone Security Profiles
3.5 Erstellen von LSCs

4 Cisco Collaboration Edge
4.1 Das Konzept
4.1.1 Firewall Traversal
4.1.2 Portusage
4.1.3 Mobile and Remote Access
4.1.4 Business-to-Business Video
4.2 Voraussetzungen und Einrichtung
4.2.1 Kommunikationsbeziehungen und Zertifikate
4.2.2 Truststores der Expressways
4.2.3 Server-Zertifikate der Expressways
4.2.4 CSR für Expressway-C
4.2.5 CSR für Expressway-E

5 Switch-basierte Sicherheitsfunktionen
5.1 Schutz des Datenverkehrs
5.1.1 DHCP Snooping
5.1.2 Dynamic ARP Inspection
5.1.3 IP Source Guard
5.1.4 DoS Protection
5.2 Sicherheit durch Access-Listen
5.3 IEEE 802.1X – Das Grundkonzept
5.3.1 Komponenten
5.3.2 Protokolle
5.3.3 Das Extensible Authentication Protocol (EAP)
5.3.4 Radius und VLAN Assignment
5.3.5 Guest und Failure VLAN
5.4 802.1X und Cisco Phones
5.5 Einrichtung von 802.1X
5.5.1 Telefone mit 802.1X Support
5.5.2 Zertifikate im Radius Server

6 IPSec
6.1 Die Ziele von IPSec
6.2 IPsec im Einsatz
6.2.1 Host to Host
6.2.2 IPSec – Gateway-to-Gateway
6.2.3 IPSec und dynamische Einwahl
6.3 IPSec – Die Betriebsarten
6.3.1 Der Tunnel Mode
6.3.2 Der Transport Mode
6.4 Der grundlegende Aufbau von IPSec
6.4.1 Der Authentication Header (AH)
6.4.2 Encapsulating Security Payload (ESP)
6.5 ISAKMP ein Rahmenwerk
6.6 Security Associations
6.7 Internet Key Exchange
6.7.1 Die Phasen von IKE
6.7.2 Main Mode
6.8 IPSec Support des Communications Managers
6.8.1 Einbinden von Zertifikaten
6.8.2 Gateway Security

7 Secure SIP Trunk
7.1 Verschlüsselung: SIPS und SRTP
7.2 Absichern von SIP-Trunks
7.2.1 SIP Trunk und Security Profile
7.2.2 SIPS und SRTP auf dem Gateway

8 Firewalls
8.1 Statische Paketfilter
8.1.1 Funktionsweise statischer Paketfilter
8.1.2 Statische Paketfilter – Schwächen und Grenzen
8.2 Dynamische Paketfilter – Stateful Firewalls
8.2.1 Funktionsweise dynamischer Paketfilter
8.2.2 Dynamische Paketfilter – Stärken und Schwächen
8.3 Proxy Firewalls
8.3.1 Application Layer Gateways
8.3.2 Circuit Relays – Generische Proxies
8.4 Voice over IP und Firewalls
8.4.1 Ports für VoIP
8.4.2 Session Border Controller
8.5 Cisco ASA
8.6 Das Security-Konzept der ASA
8.6.1 Logging und Debugging
8.6.2 Access-Listen
8.6.3 Inspection

9 Zusätzliche Sicherheitsfunktionen
9.1 Secure SRST
9.2 Secure Conferencing
9.3 ASA mit UC-Funktionalität
9.3.1 TLS Proxy
9.3.2 Phone Proxy
9.4 Praktische Übungen

A Lab
A.1 Vorbereitung
A.1.1 Topologie
A.1.2 Adressierung
A.1.3 Server und Co.
A.1.4 Los geht's
A.1.5 ISDN
A.2 Zertifikate im CallManager Cluster
A.2.1 Laden der Trust-Zertifikate
A.2.2 Erstellen der Certificate Signing Requests
A.2.3 Beantragen der Zertifikate
A.2.4 Laden der Zertifikate
A.3 CTL – Certificate Trust List
A.3.1 CTL-Client
A.3.2 Clientless
A.4 Telefon-Zertifikate
A.4.1 Zertifikate für Jabber
A.4.2 Verschlüsselung aktivieren
A.5 Firewall Traversal über Expressway
A.5.1 Zertifikate – Bestandsaufnahme
A.5.2 Trust-Zertifikate für C und E
A.5.3 Zwischenspiel: Einrichten MRA
A.5.4 Verbindung zwischen Expressway-C und CallManager herstellen
A.5.5 Verbindung zwischen Expressway-C IM&P
A.5.6 Erstellen des CSR für Expressway-C
A.5.7 Erstellen des CSR für Expressway-E
A.5.8 Beantragen der Zertifikate
A.5.9 Einspielen der Zertifikate
A.5.10 Traversal Zone zwischen Expressway-C und -E
A.5.11 Test Funktionalität
A.6 802.1X mit Cisco ISE
A.6.1 Konfiguration der Switch Ports
A.6.2 Konfiguration der ISE
A.7 IP-Sec für Gateways
A.7.1 Zertifikate auf dem Gateway
A.7.2 IP-Sec Policy anlegen
A.7.3 IP-Sec auf dem Gateway
A.7.4 SRTP aktivieren
A.8 Secure SIP-Trunk
A.8.1 Vorbereitung im CallManager
A.8.2 Zertifikate für das Gateway
A.8.3 Aktivieren von SIPS und SRTP
A.9 Firewall
A.9.1 Interne FW
A.9.2 Externe FW
A.10 Secure SRST

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