

# Cisco UC Security

## Absichern der CUCM-Umgebung



Die komplexe Welt von Unified Communications schafft neue Herausforderungen an die Netzwerksicherheit. In diesem Kurs lernen die Teilnehmer, welche Securitymaßnahmen 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

Jeder Teilnehmer erhält ausführliche deutschsprachige Kursunterlagen von ExperTeach, die von Cisco als Derivative Work anerkannt sind.

### 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.



### Vormerkung und Buchung

Gerne merken wir für Sie für die Dauer von zwei Wochen kostenfrei und unverbindlich einen Kursplatz vor. Auf [www.experteach.de](http://www.experteach.de) können Sie unter *Anmeldung* bequem Vormerkung, Buchung und Hotelreservierung vornehmen. Oder rufen Sie uns einfach an unter 06074-4868-0.

Für geschlossene Teilnehmergruppen modifizieren wir diesen Kursinhalt gerne entsprechend Ihren Anforderungen. Bitte sprechen Sie uns an!



Auf Wunsch senden wir Ihnen gerne unseren kompletten Katalog zu, der Sie über alle Trainings und andere Dienstleistungen informiert.

Cisco UC Security

5 Tage €2.595,00 • CHF 4.195,00 • zzgl. MwSt.

### Termin/Kursort

23.07.-27.07.12	Frankfurt	28.01.-01.02.13	Frankfurt
22.10.-26.10.12	Frankfurt		

Aktuelle Informationen finden Sie auf [www.experteach.de](http://www.experteach.de) USEC



EXPERTeach



Deutschsprachige  
Kurse

IT & TK Training

<p><b>1 Security im Umfeld des Communication Managers</b></p> <p><b>1.1</b> Warum Sicherheit bei der Kommunikation wichtig ist</p> <p><b>1.1.1</b> Vertraulichkeit</p> <p><b>1.1.2</b> Unveränderlichkeit</p> <p><b>1.1.3</b> Nachweisbarkeit</p> <p><b>1.1.4</b> Verfügbarkeit</p> <p><b>1.2</b> Die grundsätzlichen Bedrohungen</p> <p><b>1.2.1</b> Spoofing</p> <p><b>1.2.2</b> Lauschen</p> <p><b>1.2.3</b> Denial of Service</p> <p><b>1.3</b> Native Security-Funktionen</p> <p><b>1.3.1</b> Authentication</p> <p><b>1.3.2</b> Digest Authentication</p> <p><b>1.3.3</b> Secure Signaling</p> <p><b>1.3.4</b> Secure RTP</p> <p><b>1.3.5</b> Encrypted Configuration</p> <p><b>1.3.6</b> IPSec</p> <p><b>1.3.7</b> Phone Hardening</p> <p><b>1.3.8</b> Security by Default</p> <p><b>2 Grundlagen der Kryptographie</b></p> <p><b>2.1</b> Datenschutz durch Verschlüsselung</p> <p><b>2.1.1</b> Symmetrische Verschlüsselung</p> <p><b>2.1.2</b> Asymmetrische Verschlüsselung</p> <p><b>2.2</b> Datenintegrität und Authentisierung</p> <p><b>2.2.1</b> Data Origin Authentication</p> <p><b>2.2.2</b> Authentisierung des Gesprächspartners</p> <p><b>2.2.3</b> Zertifikate</p> <p><b>2.2.4</b> PKI und CA</p> <p><b>2.2.5</b> SCEP</p> <p><b>3 Zertifikate im Communications Manager Umfeld</b></p> <p><b>3.1</b> Self Signed Certificates</p> <p><b>3.2</b> CAPF – Certificate Authority Proxy Function</p> <p><b>3.2.1</b> Communications Manager als CA</p> <p><b>3.2.2</b> Communications Manager als Subordinated CA</p> <p><b>3.2.3</b> Ersetzen der Self Signed Certificates</p> <p><b>3.3</b> CTL Provider und CTL Client</p> <p><b>3.3.1</b> Sammeln der Cluster-Zertifikate</p> <p><b>3.3.2</b> Erstellen des CTL-Files</p> <p><b>3.4</b> Praktische Übungen (1)</p> <p><b>3.5</b> Erstellen von LSCs</p> <p><b>3.6</b> Phone Security Profiles</p> <p><b>3.7</b> Praktische Übungen (2)</p> <p><b>4 Switch-basierte Sicherheitsfunktionen</b></p> <p><b>4.1</b> Schutz des Datenverkehrs</p> <p><b>4.1.1</b> DHCP Snooping</p> <p><b>4.1.2</b> Dynamic ARP Inspection</p>	<p><b>4.1.3</b> IP Source Guard</p> <p><b>4.1.4</b> DoS Protection</p> <p><b>4.2</b> Sicherheit durch Access-Listen</p> <p><b>4.3</b> IEEE 802.1X – Das Grundkonzept</p> <p><b>4.3.1</b> Komponenten</p> <p><b>4.3.2</b> Protokolle</p> <p><b>4.3.3</b> Das Extensible Authentication Protocol (EAP)</p> <p><b>4.3.4</b> EAP und Netzwerkbetriebssysteme</p> <p><b>4.3.5</b> Radius und VLAN Assignment</p> <p><b>4.3.6</b> Guest und Failure VLAN</p> <p><b>4.3.7</b> 802.1X und Cisco Phones</p> <p><b>4.4</b> Praktische Übungen</p> <p><b>4.4.1</b> ACS-Vorbereitung</p> <p><b>5 Firewalls</b></p> <p><b>5.1</b> Statische Paketfilter</p> <p><b>5.1.1</b> Funktionsweise statischer Paketfilter</p> <p><b>5.1.2</b> Statische Paketfilter – Schwächen und Grenzen</p> <p><b>5.2</b> Dynamische Paketfilter – Stateful Firewalls</p> <p><b>5.2.1</b> Funktionsweise dynamischer Paketfilter</p> <p><b>5.2.2</b> Dynamische Paketfilter – Stärken und Schwächen</p> <p><b>5.3</b> Proxy Firewalls</p> <p><b>5.3.1</b> Application Layer Gateways</p> <p><b>5.3.2</b> Circuit Relays – Generische Proxies</p> <p><b>5.4</b> Voice over IP und Firewalls</p> <p><b>5.4.1</b> Ports für VoIP</p> <p><b>5.4.2</b> Session Border Controller</p> <p><b>5.5</b> Praktische Übungen</p> <p><b>5.6</b> ASA – Zugriff mit ASDM</p> <p><b>5.7</b> Das Security-Konzept der ASA</p> <p><b>5.7.1</b> Logging und Debugging</p> <p><b>5.7.2</b> Access-Listen</p> <p><b>5.7.3</b> Inspection</p> <p><b>5.8</b> Packet Tracer</p> <p><b>6 IPSec</b></p> <p><b>6.1</b> Die Ziele von IPSec</p> <p><b>6.2</b> IPsec im Einsatz</p> <p><b>6.2.1</b> Host to Host</p> <p><b>6.2.2</b> IPSec – Gateway-to-Gateway</p> <p><b>6.2.3</b> IPSec und dynamische Einwahl</p> <p><b>6.3</b> IPSec – Die Betriebsarten</p> <p><b>6.3.1</b> Der Tunnel Mode</p> <p><b>6.3.2</b> Der Transport Mode</p> <p><b>6.3.3</b> Wogegen IPSec nicht schützen kann</p> <p><b>6.4</b> Der grundlegende Aufbau von IPSec</p> <p><b>6.4.1</b> Der Authentication Header (AH)</p> <p><b>6.4.2</b> Encapsulating Security Payload (ESP)</p> <p><b>6.5</b> ISAKMP ein Rahmenwerk</p> <p><b>6.6</b> Security Associations</p> <p><b>6.7</b> Internet Key Exchange</p>	<p><b>6.7.1</b> Die Phasen von IKE</p> <p><b>6.7.2</b> Main Mode</p> <p><b>6.8</b> IPSec Support des Communications Managers</p> <p><b>6.8.1</b> Einbinden von Zertifikaten</p> <p><b>6.8.2</b> Gateway Security</p> <p><b>6.9</b> Praktische Übungen</p> <p><b>7 Zusätzliche Sicherheitsfunktionen</b></p> <p><b>7.1</b> Secure SRST</p> <p><b>7.2</b> Secure Conferencing</p> <p><b>7.3</b> ASA mit UC-Funktionalität</p> <p><b>7.3.1</b> TLS Proxy</p> <p><b>7.3.2</b> Phone Proxy</p> <p><b>7.4</b> Praktische Übungen</p>
--	---	--



**ExperTeach Gesellschaft für Netzwerkkompetenz mbH**

Waldstr. 94 • D-63128 Dietzenbach  
 Telefon +49 6074 4868-0 • Telefax +49 6074 4868-109  
 info@experteach.de • www.experteach.de

© ExperTeach GmbH, alle Angaben ohne Gewähr

Stand 08.05.2012