

Ein neu überarbeiteter dreitägiger Workshop in deutscher Sprache

## Sicherheitsaspekte von Unified Communication-Umgebungen

Lernen von den Profis – Ihr Referent ist Christopher Werny

### Kursbeschreibung

Der Einsatz von Voice-over-IP (VoIP) ist in vielen Organisationen mittlerweile Standard. Während das Thema Sicherheit bei der klassischen Telefonie eine eher untergeordnete Rolle spielte, darf es bei der Telefonie (oder ihrer Migration) in die IP-Welt nicht vernachlässigt werden. Dabei ist es wichtig, nicht nur die klassischen VoIP-Komponenten (Telefone, Gate ways, Call Agent) zu betrachten, sondern auch Applikationsserver, die für eine VoIP-Umgebung Mehrwertdienste bereitstellen (z. B. Abrechnungsdaten, Mailboxen etc.). Durch die Migration entstehen neue Bedrohungen und Risiken, die angemessen adressiert werden müssen. Neben den reinen VoIP-basierten Fragestellungen behandelt der Kurs auch die in den letzten Jahren immer weiter verbreiteten Technologien zur Kollaboration. Darunter fallen Instant-Messaging, Presence, Video-Konferenzen und Telefonie, entweder als On-Premise Lösung oder Cloud-basierter Dienst. Durch die immer steigende Komplexität von neuen Technologien und Protokollen zur Abbildung der UC-Anforderungen ist ein grundlegendes Verständnis dieser Technologien, und der daraus resultierenden Implikationen für den sicheren Betrieb einer UC Umgebung, notwendig. Der Kurs behandelt zu Beginn die grundlegenden Komponenten, Protokolle und Standards in der VoIP-Welt. Im Anschluss werden relevante Bedrohungen und Schwachstellen vorgestellt und diskutiert, sowie adäquate Gegenmaßnahmen erläutert. Es werden aktuelle Angriffe auf Protokolle und Gateways diskutiert und Grundlagen für ein sicheres Design einer VoIP-Umgebung vorgestellt. Des Weiteren werden die zur Verfügung stehenden Sicherheitsfeatures (wie z.B. 802.1x und SRTP/SIP-TLS) von VoIP-Produkten unterschiedlicher Hersteller (Cisco, Avaya, Unify) erläutert, diskutiert und bewertet. Um den Teilnehmern ein besseres Verständnis zu vermitteln, wo die häufigsten Sicherheitsprobleme auftreten, werden Case-Studies aus aktuellen Sicherheitsprüfungen von VoIP-Umgebungen in großen Unternehmensnetzwerken vorgestellt und diskutiert. Anschließend werden die Technologien (Instant Messaging, Presence, Web/Video-Konferenzen) und Protokolle (z.B. XMPP/WebRTC) im Rahmen von „Unified Communication“ grundlegend behandelt. Anschließend werden, analog zu VoIP, relevante Bedrohungen und Schwachstellen diskutiert und geeignete Maßnahmen erläutert. Zusätzlich werden Cloud-basierte Produkte (Cisco WebEx, Skype for Business) erläutert und Methoden vorgestellt um die Sicherheit dieser Produkte bewerten zu können. Ein Design Kapitel in dem die wichtigsten Sicherheitsaspekte bei der Implementierung diskutiert werden runden diesen Themenblock ab. Nach dem dreitägigen Workshop sind Sie in der Lage, eine sichere VoIP (bzw. Unified Communication) Umgebung zu planen, und Sie besitzen die notwendigen Kenntnisse, um relevante Bedrohungen und Risiken zu bewerten und angemessen zu adressieren. Des Weiteren sind Sie in der Lage, für Ihre Umgebung eine Bewertung der Cloudbasierten Dienste vorzunehmen.

**27.-29. November 2018, Mainz**

**04.-06. Juni 2019, Düsseldorf**

Diese Veranstaltung wird als Weiterbildung bei Rezertifizierungsmaßnahmen von verschiedenen Instituten anerkannt.

# Sicherheitsaspekte von Unified Communication-Umgebungen

M 50

Ein neu überarbeiteter dreitägiger Workshop in deutscher Sprache

## SEMINARINHALT

### Grundlagen der VoIP-Technologie

- Grundlegende Technologien, Protokolle und Komponenten Bedrohungen und Schwachstellen
- Auf Protokoll-Ebene (Signalisierung, Transport)
- Auf Gateway-Ebene
- Auf Telefon/Endpunkt-Ebene
- Diskussion resultierender und gängiger Sicherheitsbedenken beim Einsatz von VoIP Angriffe auf VoIP-Technologien

### Angriffe auf VoIP-Technologien

- Sicherheitsdiskussion von SIP: Angriffe und wie diese verhindert werden können
- Sicherheitsdiskussion von H.323: Angriffe und wie diese verhindert werden können
- Angriffe gegen Gateway-Komponenten Planung eines sicheren VoIP-Netzwerks

### Planung eines sicheren VoIP-Netzwerks

- Einführung in die Building Blocks der Netzwerksicherheit (ERNW "Seven Sisters")
- Anwendung der Building Blocks auf die VoIP-Netzwerke Verschlüsselung in VoIP-Netzwerken

### Verschlüsselung in VoIP-Netzwerken

- Bewertung
- Strategien
- Stolpersteine

### Überblick und Bewertung der Sicherheitsfunktionen in Komponenten verschiedener Hersteller (Cisco, Avaya, Unify)

- SRTP & SIP-TLS
- 802.1x für Telefone

### Case Studies aus aktuellen Sicherheitsüberprüfungen von VoIP-Netzen in großen Unternehmensumgebungen

### Grundlagen der Unified Communication-Technologien

- Grundlegende Technologien, Protokolle und Komponenten

### Bedrohungen und Schwachstellen beim Einsatz von UC-Technologien

- Auf Protokoll-Ebene (XMPP/WebRTC)
- Auf Gateway-Ebene
- Auf Endpunkt-Ebene
- Diskussion resultierender und gängiger Sicherheitsbedenken beim Einsatz von UC-Technologien

### Bewertung von Cloud-basierten Anbietern

- Cisco WebEx
- Microsoft Skype for Business

### Planung eines sicheren UC-Netzwerks

- Anwendung der Building Blocks auf UCNetzwerke
- Anwendung von Security Best Practices auf UC-Komponenten

### HM TRAINING SOLUTIONS ON-SITE SERVICE

Alle HM Training Solutions Seminare stehen auch firmenintern zur Verfügung. Sie können auf den Bedarf Ihrer Organisation zuge schnitten werden. Weitere Details erhalten Sie unter der Telefonnummer +49 (0) 6022 508 200.

# Sicherheitsaspekte von Unified Communication-Umgebungen

M 50

Ein neu überarbeiteter dreitägiger Workshop in deutscher Sprache

## Warum Sie teilnehmen sollten

- Alle Grundlagen zur Beurteilung und Evaluierung von VoIP und UC-Umgebungen
- Welche Bedrohungen und Schwachstellen in VoIP und UC-Umgebungen existieren
- Verschiedene Ansätze, wie die resultierenden Risiken zu bewerten und zu adressieren sind
- Tiefgreifende technische Kenntnisse über die in VoIP und UC-Umgebungen ein gesetztes Netzwerk- und Sicherheitstechnologien

## Zielgruppen

- IT-Sicherheitsbeauftragte
- IT-Leiter
- Projektmanager (mit Sicherheitsfokus)
- Revisoren
- Administratoren mit Sicherheitsfokus

## Profil des Referenten



Ihr Trainer **Christopher Werny** ist langjähriger Auditor und Penetrationstester mit umfassender Erfahrung in großen und sehr großen Unternehmensnetzen. In dieser Funktion ist er auch beratend in der Strategieplanung IT-Security in verschiedenen sehr großen Unternehmen tätig. Sein Spezialgebiet liegt im Bereich der Sicherheit von VoIP, virtualisierten Umgebungen sowie IPv6. Als langjähriger Referent hat er auf unterschiedlichen Konferenzen Vorträge gehalten, wie zum Beispiel dem Heise IPv6 Kongress in den Jahren 2011 und 2012 sowie auf internationalen Konferenzen wie der ITU und der DayCon. Seit 2007 widmet er sich besonders dem Thema der Sicherheit von VoIP-Umgebungen und berät dort sehr große Unternehmen, um sie bei der Einführung von VoIP zu unterstützen. Bei ERNW leitet er das Team Network Security.

# DETAILS ZUM ANMELDEFORMULAR

## /// Drei Wege zur Anmeldung

- Per Post:** Bitte dieses Anmeldeformular ausfüllen und an HM Training Solutions senden.
- Per Fax:** Bitte dieses Formular an folgende Faxnummer senden: +49 (0) 6022 508 9999.
- Per E-Mail:** [Info@hm-ts.de](mailto:Info@hm-ts.de)

## /// Gebühren

€ 1.990 € +19% Mehrwertsteuer

## /// Bestätigungsbrief

Ihre Anmeldung bestätigen wir per Mail oder Brief. Er enthält Details über die Veranstaltung und den Ort. Mittagessen, Kaffeepausen und die Seminardokumentation sind im Preis enthalten.

## /// Änderungen

HM Training Solutions behält sich das Recht vor, bei Eintreten nicht vorhersehbarer Umstände das Seminar räumlich und/oder zeitlich zu verlegen, einen anderen Referenten ersatzweise einzusetzen oder die Veranstaltung zu stornieren. Weitergehende Ansprüche bestehen nicht.

## /// Stornierung seitens des Teilnehmers

Bitte reichen Sie Stornierungen schriftlich per Post oder Fax, Fax-Nr. +49 (0) 6022 508 9999, ein. Bestätigte Anmeldungen können bis zu sechs Wochen vor Seminarbeginn kostenfrei storniert werden, danach berechnen wir die gesamte Seminargebühr. Eine Übertragung an einen Ersatzteilnehmer ist jederzeit möglich.

## /// Hotel

Ihre Anmeldebestätigung enthält alle Details zum Hotel, in dem das Seminar stattfindet.

## /// Firmeninterne Seminare

Alle Trainings von HM Solutions können auch firmenintern und zugeschnitten auf den Bedarf der jeweiligen Organisation durchgeführt werden. Weitere Informationen erhalten Sie unter der Telefon-Nr. +49 (0) 6022 508 200.

**Die Teilnehmerzahl ist begrenzt.  
Wir berücksichtigen Ihre Anmeldung  
in der Reihenfolge des Eingangs.**

# ANMELDEFORMULAR

## Sicherheitsaspekte in WLAN-Umgebungen

- (M 50) 27.-29. November 2018, Mainz
- (M 50) 04.-06. Juni 2019, Düsseldorf

- Bitte reservieren Sie \_\_\_\_\_ Platz/Plätze  
zum Einzelpreis von 1.990 € +19% MwSt.

**Wir senden Ihnen die Kursdokumentation als pdfs vor Kursbeginn zu!**

- Bitte hier ankreuzen, falls Sie das Handout in Papierform erhalten möchten.

Herr/Frau \_\_\_\_\_ Vorname \_\_\_\_\_ Nachname \_\_\_\_\_

Funktion \_\_\_\_\_

Firma \_\_\_\_\_

Adresse \_\_\_\_\_

Postleitzahl \_\_\_\_\_

Land \_\_\_\_\_

Telefonnummer \_\_\_\_\_

Mobilfunknummer \_\_\_\_\_

E-Mail \_\_\_\_\_

Unterschrift \_\_\_\_\_

**BUCHUNGSREFERENZ**

**HM 50**

## /// Zahlung

- Bitte um Rechnungsstellung

Rechnungsadresse (falls nicht identisch mit obiger Anschrift).

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

PO-Nummer \_\_\_\_\_

## /// Zusätzliche Teilnehmer

1. Herr/Frau Vorname Nachname

\_\_\_\_\_

Funktion \_\_\_\_\_

2. Herr/Frau Vorname Nachname

\_\_\_\_\_

Funktion \_\_\_\_\_

3. Herr/Frau Vorname Nachname

\_\_\_\_\_

Funktion \_\_\_\_\_