

Information

Ort und Hotel

Hilton Bonn, Tel.: 0228/7269-0
Günnewig Hotel Stadtpalais Köln, Tel.: 0221/88042-0
NH Düsseldorf-City, Tel.: 0211/7811-0

ComConsult hat in den Veranstaltungshotels ein Zimmerkontingent für Sie vorgebucht, nutzen Sie unser Vorzugspreise. Das Seminar beginnt am ersten Tag um 10:00 Uhr und endet am letzten Tag um 16:00 Uhr.

Kosten und Leistungen

Der Preis beinhaltet neben der Teilnahmegebühr die Veranstaltungsunterlagen, ein Teilnehmerzertifikat, Getränke und Mittagsmenues an allen Tagen sowie die „Happy Hour“ am ersten Veranstaltungstag, zu der alle Teilnehmer herzlich eingeladen sind.

Die Unterlagen enthalten das gesamte Arbeitsmaterial der Veranstaltung und bieten dem Teilnehmer zahlreiche wichtige Informationen für die zukünftige berufliche Praxis.

Seminarbedingungen

Bis zu 14 Tagen vor Seminarbeginn behält sich der Veranstalter das Recht vor, das Seminar zu stornieren. Schriftliche Absagen von Teilnehmern sind bis 15 Tage vor Veranstaltungsbeginn kostenlos möglich, ab dem 14. Tag vor Veranstaltungsbeginn sind 50 % des Teilnahmebetrages zu zahlen. Bei Nichterscheinen oder Stornierung am Veranstaltungstag wird der gesamte Teilnahmebetrag fällig; der Teilnehmer erhält nach Ablauf der Veranstaltung die kompletten Schulungsunterlagen per Post. Die Übertragbarkeit auf andere Mitarbeiter ist möglich. Bitte informieren Sie uns. Die Seminargebühr ist im Voraus zu entrichten. Der Veranstalter behält sich Änderungen im Programm vor.

Der Veranstalter

Die ComConsult Akademie ist einer der führenden deutschen Anbieter für herstellerneutrale Netzwerk Seminare. Unter Federführung des anerkannten Kommunikationsspezialisten Dr. Jürgen Suppan sind Aktualität und praktische Umsetzbarkeit der Information stets gewährleistet.

Die Referenten

Dr. Simon Hoff, Dominik Zöller

**Fax-Antwort: 02408/955-399
02408/955-398**

Anmeldung

Umfassende Absicherung von Voice over IP und Unified Communications

Ich melde mich verbindlich für das Seminar zum Preis von 1.590,- € zzgl. MwSt. für folgenden Termin an:

- 12.03. - 13.03.12 in Bonn**
- 11.06. - 12.06.12 in Köln**
- 01.10. - 02.10.12 in Düsseldorf**

- inkl. Report „Sicherheitsmechanismen für VoIP“ (338,- €)
- Ich benötige keine Hotelreservierung
- Bitte buchen Sie für mich ein Zimmer

Vorname, Nachname

Firma

Abteilung

Straße

PLZ, Ort

Telefon, Fax

eMail

Ich habe die Seminarbedingungen zur Kenntnis genommen.

Unterschrift

Umfassende Absicherung von Voice over IP und Unified Communications

Seminar



12.03. - 13.03.12 in Bonn

11.06. - 12.06.12 in Köln

01.10. - 02.10.12 in Düsseldorf

**ComConsult
Akademie**

**ComConsult
Akademie**

Umfassende Absicherung von Voice over IP und Unified Communications

Motivation

Unified Communications (UC) ist die konsequente Integration von Telekommunikation und TK-Anwendungen in die Office-IT. IT-Anwendungen können flexibel auf TK-Dienste zugreifen und umgekehrt können TK-Komponenten z.B. Datenbanken, Verzeichnisdienste, Authentisierungsdienste und Datenaustauschplattformen nutzen. Letztendlich wird man Office-IT- und TK-Komponenten kaum noch voneinander unterscheiden können. Da UC-Anwendungen meist schützenswerte Daten verarbeiten und transportieren, die ggf. sogar einen hohen Schutzbedarf hinsichtlich Vertraulichkeit oder Integrität haben (z.B. personenbezogene Daten, Positionsdaten und vertrauliche Gesprächsinhalte) und beim Betrieb dieser Anwendungen ebenfalls kritische Daten anfallen (z.B. Verbindungsdaten) ist die Absicherung von UC von besonderer Bedeutung. Da UC-Infrastrukturen zunächst die Gefährdungen der zugrundeliegenden Standard-IT-Komponenten und der IP-basierten Netzinfrastrukturen erben, sind spezifische Sicherheitsmaßnahmen erforderlich. Standard-Technologien – z.B. Voice over IP (VoIP) - ermöglichen zwar grundsätzlich eine Medien- und Datenverschlüsselung, die sichere Umsetzung dieser Mechanismen ist jedoch keine einfache Aufgabe. Für die große Zahl von Integrationspunkten und Schnittstellen in UC-Infrastrukturen ein hohes Niveau an Vertraulichkeit, Verfügbarkeit und Integrität zu erzielen, stellt Planer wie Projektverantwortliche vor große Herausforderungen. Außerdem muss die sichere Integration von mobilen Endgeräten wie Smartphones und Tablets berücksichtigt werden. Gleichzeitig wird UC von anderen Trends der IT unmittelbar betroffen (z.B. Virtualisierung und Cloud Computing), die sicherheitstechnisch bewertet werden müssen. Dieses Seminar zeigt Wege auf, wie die Vorteile von Unified Communications für das Unternehmen nutzbar gemacht werden können ohne gleichzeitig die Sicherheit geschäftsentscheidender Kommunikation aufs Spiel zu setzen.

In diesem Seminar lernen Sie

- Was sich in der IT-Landschaft durch Unified Communications ändert
- Welche Gefahrenpotentiale Unified Communications birgt
- Welche Standards zum Schutz der Kommunikation relevant sind
- Wie Inhalte und Daten geschützt werden können
- Welche Architekturen die Sicherheit erhöhen
- Wie man Unified Communications über Unternehmensgrenzen hinweg sicher betreibt
- Welche rechtlichen Aspekte es zu bedenken gilt

Der Inhalt

Unified Communications: Technologien, Anwendungen und Produkte im Überblick

- Von VoIP, Video, Instant Messaging, Präsenz über CTI bis Collaboration: Der Zoo an UC-Anwendungskomponenten im Überblick
- Integration in Unternehmensanwendungen
- Veränderungen in Kommunikationsanforderungen und -verhalten
- Architekturen für UC-Infrastrukturen
- Produktlandschaft: Was bieten die Hersteller?
- UC in LAN, WAN, Internet und Mobilfunk
- Folgen für die Informationssicherheit

Bekannte und denkbare Angriffsszenarien

- Angriffsszenarien und Angreiferprofile
- Spoofing und Man in the Middle
- Abhören von Sprach- und Datenströmen
- Denial of Service
- Unsichere Prozesse und Social Engineering
- Identitätsdiebstahl und Datenmanipulation

Techniken zur sicheren Kommunikation

- Relevante Verschlüsselungsstandards
- Schutz von Medienströmen und Signalisierung (SIP, H.323) für VoIP und Video mit SRTP, TLS, IPsec und anderen Techniken
- Identity Management, Authentisierung und Schlüsselmanagement für UC
- Umgang mit Zertifikaten
- Sicherheitsaspekte der Applikationsintegration
- Absicherung von Softphones
- Sicherer Umgang mit Präsenzdiensten und Instant Messaging
- Sicherheitsfunktionen der verschiedenen UC-Ausrüster im Enterprise-Bereich

Unified Communications als Dienst

- Sicherheitsaspekte gehosteter Kommunikationslösungen
- Unified Communications aus der Cloud

Gesetzliche Regelungen zur Kommunikations- und Datensicherheit

- Unterschiede zwischen öffentlichen und privaten Netzbetreibern
- Lawful Interception – Auswirkungen auf Daten- und Informationssicherheit
- Aufbewahrung von Gesprächs- und Verbindungsdaten
- Gesetzliche Bestimmungen zu Daten-, Verbraucher- und Persönlichkeitsschutz

Sicherheitskonzepte für UC

- BSI IT-Grundschutz-Kataloge, Richtlinien und Studien des

BSI zu UC

- Systematischer Aufbau eines Sicherheitskonzepts und strukturierter Maßnahmenkatalogs für UC
- Auswirkung von UC auf andere Sicherheitskonzepte

Absicherung von Unified Communications im Netzwerk

- Absicherung der zentralen UC-Komponenten
- Umfassende Härtingsmaßnahmen für Anwendungen, Dienste, zentrale Komponenten, Netzelemente und Endgeräte
- Sichere Überwachung und Administration
- Redundanz und Hochverfügbarkeit für UC-Umgebungen
- Virtualisierung von UC-Komponenten
- Load Balancing und Immunisierung gegen Denial of Service
- Sicherheitsaspekte bei Filialstrukturen
- Firewalls, Intrusion Detection / Intrusion Prevention zur Absicherung von UC
- Einbindung der IP-Telefonie in Lösungen zur Network Access Control, insbesondere Port-basierende Authentisierung gemäß IEEE 802.1X
- Macht Netztrennung als Sicherheitsmechanismus bei Unified Communications Sinn?
- Mandantenfähige UC-Umgebungen
- Desktop-Virtualisierung und UC
- Absicherung der Endgeräte

Unified Communications über Vertrauensgrenzen

- Schutz an der Unternehmensgrenze durch Proxies und Firewalls
- UC im Unternehmensverbund und mit Geschäftspartnern
- Kommunikation mit Partnern
- Föderationen und öffentliche Netze
- Probleme bei Firewalling
- Proxy-Architekturen
- Session Border Controller als Schlüsseltechnologie

Sichere Integration von Smartphones und Tablets

- Absicherung von Smartphones und Tablets: Gefährdungen und Maßnahmen
- Sichere Anbindung von Tablets und Smartphones an die IT-Infrastruktur
- Konsequenzen einer App-basierten Architektur auf die Informationssicherheit
- iOS und Android in der Unternehmens-IT: Risiken und Maßnahmen
- Zentrales Management von Tablets und Smartphones
- Virtualisierung von Smartphones
- Fixed Mobile Convergence
- Sicherheit von GSM, UMTS, LTE
- Absicherung von WLAN für die UC-Nutzung