

Information

Ort und Hotel

Hilton Bonn, Tel.: 0228/7269-0
RAMADA PLAZA Berlin City Centre, Tel.: 030/236250-0
Mercure Hamburg Airport, Tel.: 040/53209-0
NH Düsseldorf-City, Tel.: 0211/7811-0

ComConsult hat in 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 15:00 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 herstellernerneutrale Netzwerk Seminare. Unter Federführung des anerkannten Kommunikationsspezialisten Dr. Jürgen Suppan sind Aktualität und praktische Umsetzbarkeit der Information stets gewährleistet.

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

Anmeldung

Netzzugangskontrolle: Technik, Planung und Betrieb

Ich melde mich verbindlich für das Seminar zum Preis von 1.890,- € zzgl. MwSt. für folgenden Termin an:

- 27.02. - 29.02.12 in Berlin**
- 07.05. - 09.05.12 in Bonn**
- 17.09. - 19.09.12 in Düsseldorf**
- 26.11. - 28.11.12 in Bonn**
- Ich benötige keine Hotelreservierung
- Bitte buchen Sie für mich ein Zimmer

vom _____ bis _____

Vorname, Nachname

Firma

Abteilung

Straße

PLZ, Ort

Telefon, Fax

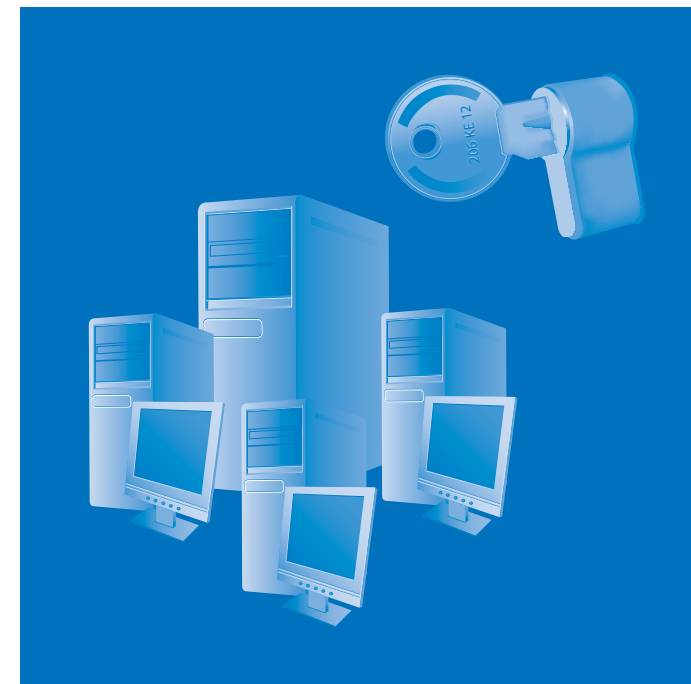
eMail

Ich habe die Seminarbedingungen zur Kenntnis genommen.

Unterschrift

Netzzugangskontrolle: Technik, Planung und Betrieb

Seminar



27.02. - 29.02.12 in Berlin

07.05. - 09.05.12 in Bonn

17.09. - 19.09.12 in Düsseldorf

26.11. - 28.11.12 in Bonn

Netzzugangskontrolle: Technik, Planung und Betrieb

Motivation

Dieses Seminar vermittelt den aktuellen Stand der Technik der Netzzugangskontrolle (Network Access Control, NAC) und zeigt die Möglichkeiten aber auch die Grenzen für den Aufbau einer professionellen NAC-Lösung auf. Schwerpunkt bildet die detaillierte Betrachtung der Standards IEEE 802.1X, EAP und RADIUS. Dabei wird mit IEEE 802.1X in der Fassung von 2010 und mit IEEE 802.1AE (MACsec) auch auf neueste Entwicklungen eingegangen.

In diesem Seminar lernen Sie

- welchen Bedrohungen Ihr LAN durch die Kopplung mit mobilen Endgeräten und Fremdgeräten ausgesetzt ist
- welche Alternativen es zur Zugangskontrolle, zur Trennung von Benutzergruppen und zum Aufbau mandantenfähiger LANs gibt
- die Konzepte kennen, die für eine port-basierte Zugangskontrolle zum LAN relevant sind
- wie der Standard IEEE 802.1X arbeitet
- welche Rolle EAP dabei spielt
- welche Authentisierungsmethoden über EAP für welches Sicherheitsniveau angemessen sind
- welche Rolle der RADIUS-Server dabei spielt
- wie unterschiedliche RADIUS-Server für NAC konfiguriert werden
- wie eine Infrastruktur für IEEE 802.1X in der Praxis umgesetzt werden kann und welche Probleme dabei gelöst werden müssen
- wie ein Gastzugang realisiert werden kann
- wie ein Monitoring und Trouble Shooting einer NAC-Lösung durchgeführt wird und welche typischen Fehlersituationen in der Praxis auftreten und wie mit ihnen umgegangen werden kann
- wo aktuell die Grenzen von IEEE 802.1X liegen
- welche Änderungen mit Version IEEE 802.1X-2010 des Standards einhergehen, welche Rolle IEEE 802.1AE (MACsec) dabei spielt und wie neben Cisco TrustSec die Produktsituation aktuell aussieht
- wie weitergehende Dienste zur Prüfung der Endgeräte-Compliance verbunden mit einer entsprechenden Autorisierung realisiert werden können
- was Network Endpoint Assessment (NEA) und Trusted Network Connect (TNC) im Detail bedeuten
- welche herstellerspezifische Lösungen für Endpoint Assessment existieren
- wie Microsofts Network Access Protection (NAP) in der Praxis umgesetzt werden kann

Der Inhalt

Bedrohungen im kabelbasierten LAN

- ARP-Spoofing / ARP-Poisoning
- DHCP-Spoofing • MAC-Spoofing • Angriffe auf VLAN

Authentisierung, eine Wissenschaft für sich

- Passwort-basierte Authentisierung und ihre Grenzen
- Challenge-Response-Verfahren
- Authentisierung über Zertifikate
- RADIUS als universelles Protokoll für die Authentisierung

Einführung in IEEE 802.1X

- Komponenten, Schnittstellen, Protokolle und Funktionsweisen • Das Extensible Authentication Protocol (EAP) als zentraler Baustein
- Unterschiede von IEEE 802.1X im kabelbasierten LAN und im WLAN • Umgang mit PXE Boot und Endgeräten, die kein IEEE 802.1X unterstützen
- MAC-Adress-Authentisierung und IEEE 802.1X
- Problembereich simultane Authentisierung mehrerer Endgeräte an einem Netzwerk-Port
- Umgang mit an IP-Telefonen angeschlossenen PCs, Desktop-Switches oder virtuellen Maschinen auf PCs
- Grenzen von IEEE 802.1X in der Version von 2004 oder warum IEEE 802.1X-2004 im LAN nicht so sicher wie im WLAN ist • IEEE 802.1X-2010: Was bringt die Neuauflage des Standards • Konzepte in IEEE 802.1AE MACsec und Cisco TrustSec

Die Möglichkeiten und Tücken von EAP

- Anwendungsszenarien und Eignung der verschiedenen EAP-Methoden
- EAP-Methoden im Detail: wie funktionieren einfache Methoden wie EAP-MD5, zertifikatsbasierte Authentisierung mit EAP-TLS, Authentisierung im Tunnel mit EAP-TTLS und PEAP, wie aufwendig ist der Betrieb und welches Sicherheitsniveau kann erreicht werden
- Maschinenaauthentisierung und Nutzerauthentisierung: Einsatzszenarien und Fallstricke
- Netzbetriebssystem, Directory Service und EAP im Zusammenspiel • Möglichkeiten für ein Single Sign-on

Architekturen und praktische Anwendungsbeispiele

- Aufbau Trusted und Untrusted LAN: IEEE 802.1X im Vergleich zu „traditionellen“ Techniken
- Homogene und heterogene Client-Landschaften: Umgang mit Thin Clients, Druckern, Multifunktionsgeräten,

- IP-Telefonen und anderen Spezialgeräten
- Architekturen für mandantenfähige LANs: IEEE 802.1X in Kombination mit logischer Netztrennung (VLAN, VRF und MPLS) und Firewall-Techniken am Netzübergang
- Aushandlung der Authentisierungsmethode
- Autorisierung von Mandanten durch dynamische VLAN-Zuweisung und/oder Access Control Lists (ACLs)
- Softwareverteilung und IEEE 802.1X
- Beispiele aus der Projektpraxis für Realisierungen von NAC-Lösungen • Live-Demonstration

RADIUS im Detail: Das Herz einer NAC-Lösung

- RADIUS-Server Konfiguration für NAC am Beispiel von FreeRADIUS, Microsoft NPS und Cisco ACS
- Directory Integration (LDAP und Active Directory): Wie unterscheiden sich die Produkte?
- Praxisbeispiele für die Konfiguration von EAP-TLS, PEAP und EAP-MD5
- Monitoring der NAC-Lösung: Was muss der RADIUS-Server leisten und wie unterscheiden sich die Produkte?

Trouble Shooting von NAC

- Fehlerquelle Endgerät, Switch, RADIUS-Server und Directory • Typische Fehlersituationen: Erkennung der Symptome und Möglichkeiten zur Behebung
- Notwendige Messtechnik • Analyse von Traces

Techniken für die Prüfung der Endgeräte-Compliance

- Technologien im Überblick: Agentenbasierte und agentenlose Systeme
- Funktion von NEA/TNC und NAP im Detail
- Wie funktionieren die Phasen Detection, Authentication, Assessment, Enforcement und Remediation?
- Assessment: Wie erfolgt die Ermittlung der relevanten Parameter des aktuellen Zustands des Endgeräts (z.B. Aktivität der Personal Firewall, Aktualität des Virenschutzes)?
- Remediation: Was ist für die Herstellung eines sicheren Zustands durch entsprechende Anpassung der Konfiguration des Endgeräts notwendig?
- Produktsituation NEA/TNC • Life Demo NAP
- Weitere herstellerspezifische Lösungen
- Agentenlose Systeme: Wie funktioniert die Prüfung des Endgeräts und welche Produkte gibt es?

Der Referent

Dr. Simon Hoff, Dipl.-Inform. Daniel Prinzen