ComConsult GmbH
Akademie

INTERNET-DMZ UND INTERNE SICHERHEITSZONEN: AUFBAU UND MANAGEMENT

Ein durchdachtes Zonenkonzept ist elementar für die Sicherheit in Netzwerken. Ziele der Veranstaltung sind das Aufzeigen von Anforderungen an Netzsegmentierung, Diskussion möglicher Umsetzungstechniken sowie Vermittlung praktischer Erfahrungswerte.

Das Seminar vermittelt die Grundlagen der Netzsegmentierung für interne Netzbereiche und gibt darüber hinaus Informationen über den Aufbau von DMZs für die Internetanbindung. Somit legt es den Grundstein für einen Wissensaufbau beim Thema Netzwerksicherheit. Weiterhin wird Expertenwissen an die Teilnehmer vermittelt, das in langjähriger Projekterfahrung der Referenten erarbeitet wurde. So können neben aktuellen logischen Konzepten und Umsetzungstechniken auch Herausforderungen unad Hürden bei der Netzsegmentierung aufgezeigt werden. Unabhängig von der Erfahrungsstufe der Teilnehmer können dadurch wertvolle Erfahrungswerte und Best Practices an die Teilnehmer weitergereicht werden, um die Planung und den Betrieb einer solchen Netzwerkinfrastruktur effizient umzusetzen.

Präsenz: 1.890,-- €
Online: 1.800,-- €

Firewalls

- Funktionsweise und Einsatzbereiche der verschiedenen Firewall-Typen vom einfachen Paketfilter über Stateful Inspection Firewalls bis zum Application Layer Gateway
- Integration von IPS, VPN
- Next Generation Firewalls: Begriffsdefinition, eingesetzte Techniken (speziell zur Anwendung- und Identitätserkennung), Marktsituation
- Darstellung von komplexen Firewall-Architekturen anhand von Projektbeispielen
- Management und Betrieb von Firewall-Systemen

Sicherer Fernzugriff: VPN, Portallösungen und Server-based Computing

- Authentifizierungsmethoden, PKI und starke Authentifizierung
- VPN-Techniken: IPsec, IKEv2, SSL-VPN und Portallösungen
- Client-to-Site-VPN und Site-to-Site-VPN
- Fernzugriff über Terminal Server und VDI
- Protokollierung von Fernzugriffen

Internet-DMZ

- Aufbau einer DMZ
- Servervirtualisierung in einer Internet-DMZ
- SAN-/NAS-Anbindung für eine Internet-DMZ
- Einsatz von Proxy-Techniken
- Notwendigkeit von Verschlüsselungsendpunkten in einer DMZ
- Content Security
- Absicherung von Web-Applikationen und Einsatz von Web Application Firewalls
- Sicherer Webzugriff
- E-Mail-Sicherheit: Verschlüsselungstechniken, SPAM-Abwehr und Gateway-Lösungen

Cloud-Computing und Zonenkonzepte

- Public Cloud, Private Cloud und Hybrid Cloud
- Kerndisziplin: Data Loss Prevention (DLP)
- Sicherheitsarchitekturen und Zonenkonzepte für Private Clouds und Hybrid Clouds

Aufbau von internen Sicherheitszonen

- Zwiebelschalenmodelle zur Absicherung kritischer Ressourcen im Rechenzentrum
- Data Center Firewalls: Höchste Anforderungen an Verfügbarkeit, Durchsatz und Delay
- Redundanzverfahren und Netzintegration für Data Center Firewalls: Active-Active Firewall-Cluster und Umgang mit dynamischen Routing-Protokollen
- Integration von Anwendungen in Zonenarchitekturen: Umgang mit Mehr-Tier-Applikationen, Unified Communications, Verteilten Systemen, Active Directory und Datenbanken
- Logische Trennung im Netz: Einsatz von VLAN und VRF sowie Einschätzung der Rolle von IEEE 802.1AE MACsec und Cisco TrustSec
- Konzepte für RZ-interne und Campus-weite Sicherheitszonen
- Kurzschlussvermeidung: Multi-homed Server und Load Balancer
- Virtualisierung im internen Netz: entscheidende Unterschiede in der Zonierung im Vergleich zur Internet-DMZ
- Virtualisierte Switches in Zonenarchitekturen
- Zonenkonzepte und integrierte DC-Architekturen (vBlock, Flexpod und Co.)
- Virtualisierung von Firewalls und anderen Sicherheitskomponenten
- Projektbeispiele

Sicherer Betrieb von Internet-DMZs und internen Sicherheitszonen

- Terminal Server als Jump Host: Möglichkeiten und Grenzen
- Virtualisierungstechniken und VDI zur sicheren Entkopplung administrativer Zugriffe
- Zonen für die Administration und Überwachung: Firewall-Inflation droht
- Berücksichtigung von SAN und NAS in Zonenkonzepten
- Projektbeispiele

REFERENTEN

Dr. Hoff ist technischer Direktor der ComConsult GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung, Planung und Betrieb in den Bereichen IT-Sicherheit, lokale Netze und mobile Kommunikationssysteme zurück.

Simon Oberem ist als Berater bei der ComConsult GmbH in dem Bereich IT-Sicherheit tätig. Im Projektgeschäft befasst er sich maßgeblich mit den Aspekten von ISMS nach ISO 27001, auch auf Basis BSI-Grundschutz sowie deren praxistauglicher Umsetzung.

Online-Anmeldung unter
https://www.comconsult.com/internet-dmz-interne-sicherheitszonen/

ComConsult GmbH
Pascalstraße 27, 52076 Aachen
Telefon: 02408/951-0
E-Mail: kundenservice@comconsult.com