

Verschlüsselung und Public Key Infrastructure PKI - Intensiv

Zertifikate & PKI - Dieser Kurs vermittelt die Funktionsweise von Verschlüsselung und PKI in weit verbreiteten Anwendungen und Protokollen.
Intensiv-Seminar aus vielfältigen Theorie Inhalten und intensivem Praxisanteil mit vielen Labs.

Listenpreis

3.250,00 € exkl. MwSt

3.867,50 € inkl. MwSt

Dauer

5 Tage

Leistungen Präsenz

- Schulung im Trainingscenter
- Verpflegung
- Teilnahmebestätigung / Zertifikat

Leistungen bei VCL Training

- Technischer Support
- Online Zugang
- Teilnahmebestätigung / Zertifikat

Ihre Ansprechpartnerin



Manuela Krämer
Leitung
Informationssicherheit

Kontakt/Fragen:
m.kraemer@cbt-training.de
Telefon: +49 (0)89-4576918-12

Inhalte

Tag 1 - 2

- **Grundlagen Verschlüsselungs-Technologien**
  - Mathematische Grundlagen
  - Organisatorische Grundlagen
  - Technische Grundlagen
  - Verschlüsselung und Integritätssicherung
  - Algorithmen (AES, RSA, Diffie-Hellman, IDEA, SHA-1/2 und andere)
  - Zertifikate (PGP-Zertifikate und X.509 Zertifikate)
  - Protokolle (IPSec, TLS, OCSP, SCEP und andere)
  - Verzeichnisdienste und Zusammenhänge
- **Publik Key Infrastructure**
  - Certificate Authority
  - Registration Authority
  - Validation Authority
  - Trusted Third Party
- **Praktische Anwendungsfälle**
  - E-Mail-Verschlüsselung
    - Arten der E-Mail-Verschlüsselung
    - Prozesse und Richtlinien zur Umsetzung von E-Mailverschlüsselung
  - File / Container / Volume Verschlüsselung
    - File- & Container Verschlüsselung
    - Volume / Plattenverschlüsselung
  - Management & Verschlüsselung mobiler Datenträger & Systeme
    - Hardware-Lösungen für Verschlüsselung mobiler Datenträger
    - Software-Lösungen für Verschlüsselung mobiler Datenträger
    - Herausforderung Usability vs. Security Digital Rights Management
    - Definition
    - Architektur
    - Funktionsweise
    - Chancen und Herausforderungen
  - Digital Rights Management



- Definition
- Architektur
- Funktionsweise
- Chancen und Herausforderungen

Tag 3 - 5 Praxis: zahlreiche Labs und Demos

- **OpenSSL - Das Schweizer Taschenmesser**
  - Generieren von Schlüsseln
  - Erzeugen und Prüfen von Hashes
  - Erstellen von Zertifikatsanträgen
  - Signieren von Dokumenten
  - Konvertieren von kryptografischen Objekten
- **Einfache Linux CA**
  - Schlüsselgenerierung
  - Erstellen von Zertifikatsanträgen
  - Signieren der Anträge
  - Sperren von Zertifikaten
  - Konvertieren von Schlüsseln und Zertifikaten
- **Windows Zertifizierungsdienste**
  - Konfigurationsmöglichkeiten
  - Beantragen und Sperren von Zertifikaten
  - Zertifikats-Templates
  - Bestandteile der Microsoft Zertifizierungsdienste
  - Automatisierungsmöglichkeiten und Integration in das AD

Ziele

Vermittlung der Funktionsweise von Verschlüsselung und PKI in weit verbreiteten Anwendungen und Protokollen.

- Grundlagen Verschlüsselungs-Technologien
- Publik Key Infrastructure
- E-Mail-Verschlüsselung
- File / Container / Volume Verschlüsselung
- Management & Verschlüsselung mobiler Datenträger & Systeme
- Digital Rights Management
- OpenSSL - Das Schweizer Taschenmesser
- Einfach Linux CA
- Windows ZertifizierungsdiensteZahlreiche Labs und Demos runden den Praxis-Kurs ab.

Zielgruppe

IT-Sicherheitsverantwortliche, IT-Mitarbeiter,
IT-Leiter, Sicherheitsbeauftragte, Geschäftsführer, IT-Manager...



Voraussetzungen

Die Teilnehmer sollten technisch und mathematisch interessiert sein. Spezielle Kenntnisse aus diesen Bereichen werden nicht vorausgesetzt.

Anwenderkenntnisse von Windows- oder Unix-Systemen, Linux Grundkenntnisse sollten vorhanden sein. Erfahrungen aus dem Bereich der System- und Netzwerkverwaltung sind hilfreich.