>> Windows Server

PKI Design, Implementation & Maintanance

EGOS! the education company

Unternehmensnetzwerke benötigen in vielfältigen Anwendungen (EFS, SmartCard-Logon, VPN, Lync, SSL, IPSec) Zertifikate und eine Infrastruktur um diese sicher im Unternehmen zu verwalten.

Ihr Nutzen

Sie können eine Public Key Infrastructure planen und erstellen. Ebenso wissen Sie um die Vorteile einer "Certification Authority" Bescheid und können etwaig auftretende Probleme beseitigen. Die Verteilung, Planung, Revokation von Schlüsseln in Unternehmensumgebungung ist ein Schwerpunkt des Seminars. Praktische Tipps aus Projekten runden das Thema ab.

Preis pro Teilnehmer

EUR 2550,- exklusive der gesetzlichen MwSt.

Seminardauer

4 Tag(e)/Day(s)

Voraussetzungen

Gute Administrationskenntnisse inkl. Netzwerk und Active Directory in Windows Server

Hinweise

Version: 2025

Seminarinhalte

1. Tag
* Einführung in Kryptographie
- Methoden und Techologien
- Algorythmen und Keys
- Encryption und Signing
- Public Key Infrastructures
- Begiffe CRL, CRT, AIA
- Zertifikate und "Certification Authorities"

* Entwerfen einer "Certification Authority" Hierarchie
- Identifizieren notwendiger CA Entwurfselemente
- Analysieren von Entwurfsbedingungen

2. Tag
* Erstellen einer "Certification Authority" Hierarchie
- Erstellen einer Offline-CA
- Überprüfen von Zertifikaten
- Planen einer untergeordneten/subordinate CA
- Multi-Tier CAs

* Verwalten der Windows PKI Komponenten
- Verwalten von Zertifikaten (Revoke, Renew, etc.)

* Verwalten von CA's
- Certification Practice Statement (CSP)
- CRL und AIA Distribution via LDAP/AD/HTTP
- Role Separation
- CAPolicy.inf und erweiterte CA Einstellungen

* Erstellen und Verwalten von Zertifikatsvorlagen

3. Tag
* Online Certificate Status Protocol (OCSP)

* Zertifikats-Verteilung
- Manuelle Verteilung
- Automatische Zuweisung (AutoEnrollment)
- Web-Enrollment
- Online Responder Service
- Webservices für Enrollment und Policy Enrollment
- Network Device Enrollment Service (NDES)
- Verteilung von Smart Card Zertifikaten
- Inside X509 Certificates

4. Tag
* Key Archiv
- Erstellen und Verwalten des Archivs
- Wiederherstellung

* Command-Line Werkzeuge
- certutil und certreq
- PowerShell Cmd-Lets für CA-Management
- PowerShell cert: Drive

* Erstellen von Trusts zwischen Organisationen
- Erweiterte PKI Hierarchien
- Trusts mit Einschränkungen: Qualified Subordination

* Unterstützung von Smart Cards
- Authentication against AD, VPN, 802.1x

* Sicherer Webzugang mit SSL
- Aktivieren von SSL auf einem Web Server
- Zertifikat basierte Authentifizierung

* Konfiguration der Sicherheit für E-Mails
- Wiederherstellen von privaten Schlüsseln für E-Mail

* Entwerfen einer Wiederherstellungsstrategie

* Disaster Recovery