Public-Key-Infrastrukturen («PKI»)

Sie lernen die theoretischen Grundlagen zur Public-Key-Infrastructure (PKI) kennen. Anschliessend lernen Sie, alle Komponenten einer vollständigen PKI-Umgebung einzurichten, richtig zu konfigurieren, zu verwalten, zu sichern und zu troubleshooten.

Dauer: 2 Tage
Preis: 1'700.– zzgl. 8.1% MWST
Kursdokumente: Digicomp Kursmaterial

Inhalt

Eine Public-Key-Infrastruktur (PKI) ist ein wirksames Werkzeug für den Schutz von Systemen und Diensten im Internet. PKI ist, obwohl seit über 20 Jahren in Entwicklung, erst in den letzten paar Jahren bei Sicherheitsverantwortlichen zum Thema geworden. Ein wesentlicher Markttreiber sind die neuen Möglichkeiten der Digitalen Signaturen, die eine PKI voraussetzen.

Public-Key-Kryptografie ist eine ausgereifte Technologie, die die Basis bildet für sichere Protokolle. Ein Standardmechanismus für die Verteilung von Public Keys war lange Zeit nicht verfügbar. Heute sind jedoch auf beiden Seiten Fortschritte erzielt worden. Sie müssen kein Experte in Public-Key-Kryptografie mehr sein, um deren Vorteile zu erkennen. Denn heute sind verschiedenste Produkte im Markt verfügbar. Dieser Kurs hilft Ihnen, von den vielen Möglichkeiten die für Sie richtigen auszuwählen und erfolgreich einzusetzen.

Inhalte Tag 1: Theorietag

1. Einleitung
    - Problemstellung
    - Geschichte
    - Rechtliche Aspekte
2. Kryptografische Grundlagen
    - Symmetrische und asymmetrische Verfahren
    - Digitale Unterschriften
    - Key Management
3. Authentisierung
    - Passwortbasiert
    - Einmalpasswörter
    - Kerberos
    - Public-Key-Zertifikate
4. PKI-Basis
    - Zertifikate
    - Certificate Revocation List
    - Policies
    - Zertifizierungspfade
5. PKI-Komponenten
    - Certification Authority (CA)
    - Registration Authority (RA)
    - Repository
    - Archiv
    - Zertifikatsinhaber
    - Relying Party
6. PKI-Architekturen
    - Einzel-CA
    - Hierarchische Infrastruktur

    - Netzstruktur
    - Cross-Zertifizierung
    - Brücken CA
7. Verifikation
    - Konstruktion und Überprüfen von Zertifizierungspfaden
8. Certificate Revocation List (CRL)
    - Inhalt
    - Erzeugen und Verteilen von CRLs
9. Directories
    - X.500, LDAP
10. X.509-Zertifikate
    - ASN.1-Typen
    - Grundinhalt
    - Extensions
    - Verwendung
11. Vertrauen, Abläufe, Policies
    - Certificate Policies (CP)
    - Certificate Practice Statement
12. Anwendungen
    - Web: SSL/TLS
    - E-Mail: S/MIME
    - IPsec

Inhalte Tag 2: Praxistag

Aufbau einer zweistufigen Certification-Authority-Umgebung mit einer Stand-alone Offline Root Certification Authority

- Aufbau einer darunterliegenden Enterprise (AD-basierten) Online Sub Certification Authority
- Was wird anders konfiguriert, wenn nur eine einstufige CA-Umgebung (Enterprise Root CA) zum Einsatz kommt?
- Einsatz des CaPolicy.inf Files
- Vollständige und richtige Sperrlistenkonfiguration (CRL), einschliesslich Konfiguration eines Online-Responders
- Konfiguration von Zertifikatsvorlagen
- Konfiguration der automatischen Zertifikatsanforderung und Verteilung sowie Erneuerung mittels GPOs
- Richtige Konfiguration und Einrichtung von SSL-Zertifikaten
- Zertifikatssperrungen
- Besondere Konfigurationen: private Schlüssel archivieren, Zertifikatsagenten einrichten usw.
- Überwachung von Certification Authoritys
- Sicherung und Wiederherstellung von Certification Authoritys
- Verwendung der Befehlszeilen-Tools (z.B. certutil.exe) und der PowerShell bei der Konfiguration und Verwaltung von Certification Authoritys

Key Learnings

Am Ende des Theorieteils sind Sie in der Lage,

- die Architektur und Komponenten einer Public-Key-Infrastruktur zu formulieren
- Problemlösungen beim Aufbau einer Public-Key-Infrastruktur zu kennen
- zu wissen, worauf Sie achten müssen, wenn Sie Zertifikatsinhalte definieren
- über die wichtigsten Standardanwendungen Bescheid zu wissen

Nach dem Public-Key-Infrastructure-Praxistag werden Sie in der Lage sein, alle notwendigen Komponenten einer vollständigen PKI-Umgebung einzurichten, richtig zu konfigurieren, zu verwalten, zu sichern und ein Troubleshooting durchzuführen.

Methodik & Didaktik

Dieses Seminar ist auf zwei Seminartage ausgelegt. Am ersten Tag lernen Sie die theoretischen Grundlagen zur PKI kennen. Der zweite Tag ist ein reiner Praxistag, an dem die am ersten Tag erlernten Grundlagen in die Praxis umgesetzt werden.

Zielpublikum

Entwickler und technische Architekten, die eine PKI aufbauen oder geschützte Applikationen herstellen wollen.

Weiterführende Kurse

- Administering Microsoft Endpoint Configuration Manager («55348A»)

Haben Sie Fragen oder möchten Sie einen Firmenkurs buchen?

Wir beraten Sie gerne unter 044 447 21 21 oder info@digicomp.ch. Detaillierte Infos zu den Terminen finden Sie unter www.digicomp.ch/weiterbildung-security/cyber-security-defense/kurs-public-key-infrastrukturen