PowerPackage Zertifikate & PKI

Verschlüsselung, Authentisierung, Integrität & Praxis

Dieses PowerPackage kombiniert die Inhalte der Kurse Zertifikate & PKI und Active Directory Certificate Services in einer Veranstaltung.

Egal ob TLS-Verschlüsselung, Token-Authentisierung, Signatur von Firmware oder Excel Macros, oder Verschlüsselung von Sprache und E-Mails – überall kommen Zertifikate zum Einsatz. Dieser Kurs führt in die Grundlagen der Kryptographie ein, klärt über die Notwendigkeit von Zertifikaten auf und erläutert deren Inhalte und Einsatzzwecke. Jene, die ihr Wissen rund um das Thema Verschlüsselung, Authentisierung & Daten Integrität erweitern wollen, werden mit diesem Kurs auf ihre Kosten kommen.

Mit Hilfe der Active Directory Certificate Services (ADCS) des Windows Server wird in Teil 2 eine zweistufige PKI aufgebaut. Ziel ist es, eine PKI bereitzustellen, welche allen Anforderungen eines Unternehmens gerecht wird. Die Teilnehmer können in dem Labor sämtliche Kursinhalte konfigurieren und ausprobieren.

Kursinhalt

Teil 1

- Asymmetrische und symmetrische Verschlüsselung
- Hash-Werte und Digitale Signaturen
- Zertifikats-Inhalte und deren Bedeutung sowie Zertifikats-Formate
- Einsatzzecke wie TLS-Verbindungen, Mutual-Authentication und Code Signing
- Anforderungen an Zertifikatsinhalte
- Bestandteile einer PKI
- Nutzung von privaten und öffentlichen Zertifizierungsstellen sowie Let's Encrypt
- Erstellen eines Certificate Signing Requests und Ausstellen von Zertifikaten
- Klassische Sperrlisten und OCSP
- Verwalten der Lebenszyklen von Zertifikaten und Zertifizierungsstellen
- Einsatzmöglichkeiten am Beispiel von Active Directory Certificate Services, OpenSSL und XCA

Teil 2

- Installation einer PKI mit einer offline Root & Enterprise Issuing CA
- Konfiguration der CAPolicy.inf
- Anpassungen der Konfiguration mit dem Certutil
- Veröffentlichen von CRL und AIA Distribution Points
- Nutzung des Online Responder Service
- Editieren von Certificate Templates
- Konfiguration von Autoenrollment
- Ausstellen von SAN-Zertifikaten
- Private Key Archival
- Backup und Key Recovery
- Best Practices

E-Book Sie erhalten ausführliche Kursunterlagen aus der Reihe ExperTeach Networking in deutscher Sprache. Diese sind auch als ExperTeach E-Book verfügbar.

Zielgruppe

Der Workshop eignet sich für Netzwerktechniker und -administratoren, die sich tiefgründig mit dem Thema Zertifikate, Certification Authorities und mit der Verwaltung einer Microsoft CA beschäftigen möchten.

Voraussetzungen

Kenntnisse zu Netzwerksicherheit hilfreich; eine gute Vorbereitung ist ein Besuch des Kurses Security-Konzepte und Technologien. Gute Kenntnisse mit Microsoft Server-Betriebssystemen sowie dem MS Active Directory sind ebenso eine Voraussetzung für diesen Workshop.

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/**PPPK**

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training	Preise zzgl. MwSt.
Termine in Deutschland	5 TageCHF 3.075,-
Termine in Österreich	5 TageCHF 3.075,-
Online Training	5 TageCHF 3.075,-

Termin/Kursort — Kurssprache Deutsch

13.05.-17.05.24	HY Frankfurt	26.08.-30.08.24	HY Online
13.05.-17.05.24	HY Online	23.09.-27.09.24	HY Düsseldorf
17.06.-21.06.24	HY Online	23.09.-27.09.24	HY Online
17.06.-21.06.24	HY Wien	04.11.-08.11.24	HY Hamburg
22.07.-26.07.24	HY Frankfurt	04.11.-08.11.24	HY Online
22.07.-26.07.24	HY Online	09.12.-13.12.24	HY Online
26.08.-30.08.24	HY München	09.12.-13.12.24	HY Wien

Stand 17.04.2024

PowerPackage Zertifikate & PKI

Inhaltsverzeichnis

PowerPackage Zertifikate & PKI – Verschlüsselung, Authentisierung, Integrität & Praxis

1 Grundlagen
1.1 Anfänge der Kryptographie
1.2 Symmetrische Verschlüsselung
1.2.1 Lebensdauer und Verteilung der Schlüssel
1.2.2 Erzeugung von Schlüsseln
1.2.3 Diffie-Hellman
1.3 Asymmetrische Verschlüsselung
1.3.1 RSA
1.3.2 Hybride Verfahren
1.4 Datenintegrität: Hash-Werte
1.4.1 Typische Eigenschaften
1.4.2 Angriffe auf Hash-Werte

2 Public Key Infrastructure
2.1 Zertifikate ausstellen
2.1.1 Gültigkeits Zeitraum
2.1.2 Antragsteller
2.1.3 Key Usage & Enhanced Key Usage
2.1.4 Key Store
2.2 Authentifizierung
2.3 Verschlüsselung
2.4 Certificate Revocation List
2.4.1 CRL Security
2.4.2 Laufzeit
2.4.3 Delta CRLs
2.4.4 Autorisierung
2.4.5 Verfügbarkeit
2.4.6 Verfügbarkeit, ff.
2.4.7 Critical
2.4.8 Sperrgrund
2.4.9 Speicherorte
2.5 Infrastruktur
2.5.1 Hardware Security Module
2.5.2 Path Validation
2.5.3 Path Discovery
2.5.4 Veröffentlichungspunkte
2.5.5 Online Certificate Status Protocol
2.5.6 Lebenszyklus
2.6 Microsoft CA Typen
2.7 Simple Certificate Enrollment Protocol
2.8 Public PKI
2.9 Organisationsvertrauen

ExperTeach AG
Kronenstrasse 11 · 8735 St. Gallenkappel · Telefon: +41 55 420 2591 · Fax: +41 55 420 2592 · info@experteach.ch · www.experteach.ch