smart Public Key Infrastructure (PKI) unter Windows Server - Aufbau und Praxis

Wissensgarantie: 12 Monate

Examen-ID: nv

Trainings-ID: sSEC-PKI

Prüfung: nv

Zum Seminar →

Das nehmen Sie mit

Kaum ein Microsoft Backoffice Produkt oder -Technologie kommt heute ohne Zertifikate aus: Exchange bzw. Skype for Business verwenden Zertifikate zur Server Authentifizierung, WLAN Implementierungen nutzen Zertifikate zur Überprüfung des Zutritts sowie Direct Access benutzt Zertifikate zur Benutzerauthentifizierung.

Umso wichtiger ist eine fundierte Ausbildung im Umgang mit Zertifikaten und im Aufbau einer Public Key Infrastrukture. In diesem zweitägigen Seminar erlernen Sie die notwendigen theoretischen Grundlagen zum Aufbau und Betrieb einer zweistufigen Public Key Infrastructure (PKI).

Im zweiten Teil implementieren Sie praxisnahe Anwendungen welche durch den Einsatz von Zertifikaten innerhalb Ihrer PKI ermöglicht werden, beispielsweise 802.1X bzw. SmartCard Authentifizierung, Digitale Signaturen oder VPN Verbindungen (SSL und Direct Access).

Nach Abschluss dieses Seminars haben die Teilnehmer*innen Wissen zu folgenden Themen:

- Kryptographische Grundlagen
- Symmetrische vs. Asymmetrische Verschlüsselung
- Hash Funktionen
- Digitale Signatur

- Zertifikate, Normen und Standards
- Public Key Infrastructure
- Aufbau und Betrieb einer PKI
- Aus der Praxis

Dieses Seminar wird auf der Server Version: Windows Server 2019 abgehalten, wobei Teilnehmer*innen, die Windows Server 2016 und 2012 im Einsatz haben dieses Seminar ebenso besuchen können, da der Trainer*in während des Seminars auf diese Versionen eingeht.

Das nehmen Sie mit

Kaum ein Microsoft Backoffice Produkt oder -Technologie kommt heute ohne Zertifikate aus: Exchange bzw. Skype for Business verwenden Zertifikate zur Server Authentifizierung, WLAN Implementierungen nutzen Zertifikate zur Überprüfung des Zutritts sowie Direct Access benutzt Zertifikate zur Benutzerauthentifizierung. Umso wichtiger ist eine fundierte Ausbildung im Umgang mit Zertifikaten und im Aufbau einer Public Key Infrastrukture. In diesem zweitägigen Seminar erlernen Sie die notwendigen theoretischen Grundlagen zum Aufbau und Betrieb einer zweistufigen Public Key Infrastructure (PKI). Im zweiten Teil implementieren Sie praxisnahe Anwendungen welche durch den Einsatz von Zertifikaten innerhalb Ihrer PKI ermöglicht werden, beispielsweise 802.1X bzw. SmartCard Authentifizierung, Digitale Signaturen oder VPN Verbindungen (SSL und Direct Access).

Nach Abschluss dieses Seminars haben die Teilnehmer*innen Wissen zu folgenden Themen:

- Kryptographische Grundlagen
- Symmetrische vs. Asymmetrische Verschlüsselung
- Hash Funktionen
- Digitale Signatur
- Zertifikate, Normen und Standards
- Public Key Infrastructure
- Aufbau und Betrieb einer PKI
- Aus der Praxis

Dieses Seminar wird auf der Server Version: Windows Server 2019 abgehalten, wobei Teilnehmer*innen, die Windows Server 2016 und 2012 im Einsatz haben dieses Seminar ebenso besuchen können, da der Trainer*in während des Seminars auf diese Versionen eingeht.

Zielgruppen

- Netzwerkadministrator*innen und Entscheidungsträger*innen für die unternehmensinterne IT-Sicherheit.
- Administratoren

Wichtige Informationen
Dieses Training wurde durch den Smart Hybrid Public Key Infrastructure (PKI) mit Windows Server und Intune (Cloud PKI)
ersetzt.

Termine & Optionen