Thales-HSM der nShield-Serie

Ziel und Zielgruppe:

Ziel der Schulung ist die Vorbereitung auf den Betrieb von HSM der nShield-Serie von Thales. Vermittelt werden u. a. die grundsätzliche Funktionsweise, die System-Architektur sowie das Vorgehen zur Installation und Konfiguration der HSM und der daran angebundenen Server. In praktischen Übungen werden die Themen Installation, Konfiguration und Desaster-Recovery vertieft und von den Teilnehmern durchgeführt.

Die Teilnahme an der Schulung vermittelt u.a. folgende Fähigkeiten:

- Vollständige Konfiguration eines nShield-HSMs für den Einsatz in einer Security World
- Erstellung und Wartung einer Security World
- Erstellung und Verwaltung von Administrator- und Operator-Card-Sets (OCS und ACS)
- Schlüsselerzeugung im HSM mittels Kommandozeile
- Kenntnisse über die wichtigsten Kommandozeilen-Befehle
- Logging und Monitoring

Die Schulung richtet sich an Administratoren und Betriebspersonal. Für die Teilnahme an der Schulung existieren keine formalen Voraussetzungen, Grundlagenwissen im Bereich Kryptographie ist aber hilfreich.

Rahmen:

Schulungsumfang: 1 Tag
Teilnehmer: 4-6 Personen
Uhrzeit: 09:30 - 18:00 Uhr
Ort: Düsseldorf
Schulungsgebühr: 950 Euro / Person

Agenda:

- Grundlagen Kryptographie und PKI
    - Symmetrische Kryptographie (Blockchiffren, Hash-Funktionen)
    - Asymmetrische Kryptographie (Public-Key-Verschlüsselung, Digitale Signaturen, X.509-Zertifikate)
- General Purpose HSM
    - Was sind HSM?
    - Was sind die Vorteile des Einsatzes von HSM?
- nShield
    - Vorstellung der Produktserie nShield und Eckdaten der zugehörigen HSM

- Client-Software
    - Installation unter Windows
    - Installation unter Linux
- Security-World
    - World-Datei
    - Keyblobs und Keyfiles
    - ACS (Administrator Cardset)
- End Application Keys
    - Preload
    - OCS (Operator Cardset)
- Remote-Management
    - Remote Operator
    - Remote Administration
- Features und CodeSafe/SEE
    - Installation von Features
    - Überblick CodeSafe/SEE
- Firmware und Versionierung
    - Installation von Firmware und Net-Images
- Desaster-Recovery
    - HSM-Defekt und Backup
    - ACS-Quorum verloren
    - OCS-Quorum verloren
    - PIN einer ACS-Karte vergessen
    - PIN einer OCS-Karte vergessen
- Logging und Monitoring
    - HSM, RFS und Client als Logging-Quellen
    - SNMP, Log-Files, Syslog, Windows-Event-Manager
- Trouble-Shooting
  Im letzten Teil der Schulung werden Fehlersituation an Testsystemen erzeugt, die von den Teilnehmern erkannt und gelöst werden sollen. Dabei unterstützen die zuvor erlernten Logging- und Monitoring-Techniken.