PKI (Public Key nfrastructure)Training using the role of Microsoft Windows Server Active Directory Certificate Services (ADCS)

This is a detailed and technical-oriented public key infrastructure training. Participants will spend most of their time on practical examples related to planning, implementation and management of the presented role by also using third-party tools. Additionally, knowledge about scenarios of high service availability, migration or disaster recovery will be presented. Equipment simulators will appear at the training and the use of smart cards will be explained.

Program

Certificate structure

- Analysis of the certificate structure for compliance with the requirements of Microsoft, Google and Mozilla browsers

Planning and implementation of a two-stage certification authority

- Configuration of Public Key Infrastructure in the Root / Issuing / PolicyCA structure based on the Hardware Security Module (HSM) simulator and configuration scripts.

Certificate templates

- Configuration and management of certificate templates

Limited registration agents on the example of certificates issued for smart cards

- Configuration of templates in terms of using certificates for registration on smart cards
- Best practices for registration agents
- Smart card management and use in various applications

Certification Authority (CA) migrations

- Legacy CSP Keys to Key Storage Provider migration
  CA to Windows Server 2019 migration
- SHA1 to SHA2 migration

Configuration and implementation of the OCSP role

- OCSP configuration for individual CAs
- Forcing notification of certificate revocation within a maximum of one hour by using a correctly configured OCSP role

Disaster Recovery

- Backup methods and strategies for certification authorities
- Manually restoring lost certificates using configured SMTP Exit Module notification
- Manually signing expiring CRLs with a malfunctioning ADCS service

Restoring archived keys

- Template configuration according to security requirements
- Key Recovery Agent (KRA) role
- Identification and key recovery on the example of a lost user certificate

Certificate signing

- Configuration of templates and certificate registration
- Time stamps
- Signing scripts on the example of a PowerShell script
- Workarounds related to policies that force signing of executed scripts

Policy CA

- Configuring restrictions of issued Network Device Enrollment Service certificates

Network Device Enrollment Service

- Service installation and security
- Sample certificate registration for a device

Integration of the implemented public key infrastructure with a UTM class device

- SSL/TLS communication with a device
- VPN over SSL connections
- HTTPS Content Inspection

Monitoring and management of a certification authority using C-View software

TRAINING CONSISTS OF:

- training 5 days x 8 hours a day
- teaching materials
- certificate of training completion
- post-training support