MPKI

Infrastruktura veřejných klíčů

Popis:

Třídenní kurz poskytne studentům znalosti a dovednosti pro praktické nasazení a správu PKI v prostředí Microsoft Windows Server 2019/2022 a Windows 10/11. Posluchači si na kurzu prakticky vyzkouší instalaci a konfiguraci Active Directory certifikačních služeb a použití PKI v aplikacích a službách. Je určen pro pokročilé uživatele, správce informačních systémů a všechny zájemce o použití elektronických podpisů a aplikované kryptografie.

Absolvent kurzu bude umět:

- Nasadit a spravovat služby PKI v organizaci
- Vytvářet a nastavovat šablony certifikátů
- Vydávat a odvolávat certifikáty
- Používat certifikáty v různých aplikacích a systémech
- Vytvářet a ověřovat elektronický podpis
- Zálohovat a obnovovat PKI

Požadavky pro absolvování kurzu:

- Obecná znalost Windows serverového operačního systému a jeho komponent
- Obecná znalost principů elektronické pošty
- Zkušenosti se správou Active Directory a IIS
- Teoretické znalosti principů a algoritmů PKI

Kurz určen pro:

Administrátory a další zájemce o praktické nasazení technologií infrastruktury veřejných klíčů (PKI) ve vlastní organizaci.

Literatura:

Všichni účastníci školení obdrží materiály společnosti OKsystem.

Technické vybavení:

Všechny učebny jsou vybaveny nadstandardními počítači připojenými k Internetu, učebny jsou

prostorné, klimatizované, bezbariérové a s připojením na Wi-Fi. V případě zájmu lze školení absolvovat online live.

Osnova:

Kapitola 1: Úvod do PKI a elektronického podpisu

- Úvod do kryprografie - přehled
- Druhy elektronického podpisu
- Digitální certifikát veřejného klíče

Kapitola 2: Microsoft certifikační služby

- Certifikační autorita
- Lab: Nasazení Enterprise Root CA
- Konfigurace certifikační autority
- Odvolání certifikátu, seznam odvolaných certifikátů (CRL)
- Definice a publikování CRL a AIA informací
- Lab: Konfigurace Enterprise Root CA
- OCSP a Online Responder
- Lab: Konfigurace Online Responderu

Kapitola 3: Vytváření a konfigurace certifikačních šablon

- Úvod do certifikačních šablon (certificate templates)
- Vytváření vlastních šablon pomocí funkce duplikace a jejich nastavení
- Publikování certifikačních šablon
- Lab: Implementace certifikačních šablon

Kapitola 4: Vydávání certifikátů

- Proces vytvoření žádosti o certifikát, generování klíčů
- Možnosti vydávání certifikátů
- Šifrovaná komunikace s Web serverem s použitím protokolu SSL
- Vydávání certifikátů se SAN (Subject Alternative Name)
- Lab: Manuální vydání a instalace certifikátu
- Zabezpečená elektronická pošta s použitím S/MIME
- Lab: Vytvoření a ověření elektronického podpisu, šifrování zprávy a příloh v Microsoft Outlook
- Vydávání časových razítek a digitální podepisování dokumentů
- Lab: Vytvoření a ověření elektronického podpisu pomocí Microsoft Word a Adobe Acrobat Reader
- Automatické vydávání certifikátů (Autoenrollment)
- Vydávání certifikátů za jiného uživatele (pomocí Enrollment Agent)
- Export a import certifikátů
- Lab: Vydávání certifikátů - různé metody

Kapitola 5: Zálohování a obnova PKI

- Implementace archivace klíčů a jejich obnovy
- Zálohování, migrace a obnova databáze certifikační autority
- Lab: Bezpečná odinstalace certifikační autority

Kapitola 6: Vytváření hierarchie certifikačních autorit v Enterprise prostředí

- Konfigurace CAPolicy.inf pro instalaci CA
- Instalace Offline Root CA
- Instalace podřízené (Subordinate) Enterprise CA
- Lab: Implementace hierarchické CA
- Definice CA administrátorů a certifikačních manažerů