Warsztaty: Zarządzanie infrastrukturą klucza publicznego na platformie Windows Server 2019

Opis: Uczestnicy podczas ćwiczeń praktycznych wdrażają rozwiązania oparte o certyfikaty dla aplikacji i usług sieciowych.

Czas: 24 godziny

Wymagania wstępne: Praktyczna znajomość systemu Windows (serwer i klient) na poziomie administratora systemu, podstawy wirtualizacji.

Dla kogo: Warsztaty skierowane są do administratorów oraz specjalistów IT pracujących w systemach Windows Server 2012 R2 lub Windows Server 2016, którzy chcą zdobyć wiedzę i umiejętności niezbędne do planowania, instalacji i infrastruktury usług certyfikacyjnych w środowisku Windows 2019.

Zakres tematyczny:

1) Przegląd infrastruktury klucza publicznego

a. Wprowadzenie do PKI
b. Podstawy kryptografii
c. Certyfikaty i urzędy certyfikacji

2) Projektowanie hierarchii urzędów certyfikacyjnych

a. Identyfikacja wymagań i planowanie struktury CA dla domeny AD

3) Tworzenie hierarchii urzędów certyfikacji

a. Konfiguracja pliku CAPolicy.inf
b. Tworzenie autonomicznego głównego urzędu certyfikacji (Offline Root CA)
c. Tworzenie podrzędnego urzędu certyfikacji przedsiębiorstwa (Sub Enterprise CA)
d. Definiowanie ustawień publikacji list CRL i AIA
e. Publikacja list CRL i AIA

4) Zarządzanie strukturą CA

a. Zatwierdzanie, odrzucanie żądań certyfikatów
b. Zarządzanie archiwizacją i odtwarzaniem bazy certyfikatów
c. Zarządzanie konfiguracją CA

5) Konfiguracja szablonów certyfikatów

a. Przegląd szablonów
b. Planowanie, wdrażanie i publikowanie szablonów

6) Konfiguracja dystrybucji certyfikatów

a. Zarządzanie zmianami w istniejących certyfikatach
b. Konfiguracja automatycznego i ręcznego zatwierdzania żądań

7) Archiwizacja i odtwarzanie kluczy certyfikatów

8) Wdrażanie środowiska autoryzacji za pomocą kart czipowych (Smart Cards)

a. Wstęp do usług autoryzacji przy pomocy SmartCard
b. Tworzenie certyfikatów potrzebnych dla kart czipowych
c. Zgłaszanie żądania dla karty czipowej
d. Zatwierdzanie żądań certyfikatów dla SmartCard

9) Zabezpieczanie ruchu WEB przy pomocy SSL

a. Podstawowe pojęcia
b. Włączanie szyfrowania dla katalogów wirtualnych IIS
c. Kojarzenie certyfikatów z kontami użytkowników w Active Directory
d. Kojarzenie certyfikatów w IIS

10) Zabezpieczanie poczty elektronicznej

a. Przegląd zagadnień związanych z szyfrowaniem poczty
b. Szyfrowanie i podpisywanie cyfrowe poczty elektronicznej (Microsoft Office Outlook 2019 i Exchange 2019)

11) Podpisywanie cyfrowe skryptów i aplikacji

12) Migracja usług certyfikatów z poprzednich wersji Windows Server