Kod szkolenia: **SSL/TLS/CNF**

Tytuł szkolenia: **Konfiguracja protokołu SSL/TLS**

Dni: 2

Opis:

Adresaci szkolenia

Szkolenie adresowane jest do osób pragnących poznać zagadnienia związane z uruchomieniem i konfiguracją protokołu SSL/TLS do prawidłowego zabezpieczenia komunikacji pomiędzy systemami.

Cel szkolenia

Uczestnicy dowiedzą się w jaki sposób zaplanować i przygotować konfigurację systemów wykorzystujących protokół SSL/TLS w zależności od ich zastosowań (np. aplikacje webowe, poczta elektroniczna, sieć urządzeń typu IoT).

Mocne strony szkolenia

Szkolenie prowadzone jest w formie warsztatu podczas którego uczestnicy przygotowują różne konfiguracje protokołu SSL/TLS. Pozwoli im to w praktyce zapoznać się z różnymi technikami uwierzytelniania, wymiany klucza oraz zapewniania integralności i poufności danych.

Wymagania

Od uczestników szkolenia wymagana jest umiejętność obsługi komputera w systemie Windows lub Linux.

Specjalne wymagania techniczne

Uczestnicy w trakcie zajęć korzystają z komputera z systemem Windows lub Linux. Niezbędne jest posiadanie co najmniej jednego czytnika kart elektronicznych zgodnego z PC/SC.

Parametry szkolenia

2 * 8 godzin (2 * 7 godzin netto) wykładów i warsztatów.

Program szkolenia:

1. Wprowadzenie do bezpieczeństwa informacji

    - dlaczego należy chronić dane
    - techniki zabezpieczania informacji
    - pojęcie integralności, poufności i uwierzytelnienia
    - kryptografia i jej zastosowania
    - najważniejsze współczesne algorytmy kryptograficzne: rodzina SHA, AES, DES, 3DES, DH, RSA, algorytmy oparte o krzywe eliptyczne (ECDH, ECDSA)
    - tryby szyfrowania z uwierzytelnieniem (ang. *authenticated encryption*, AE): CCM, GCM
    - problem bezpiecznego przechowywania kluczy kryptograficznych
    - repozytoria kluczy: JKS, JCEKS, PKCS#12, BC i BCFKS

2. Infrastruktura klucza publicznego

    - rola infrastruktury klucza publicznego (ang. *public key infrastructure*, PKI)
    - klucz prywatny i publiczny
    - zgłoszenia certyfikacyjne (ang. *certificate signing request*, CSR)
    - certyfikat klucza publicznego: rodzaje certyfikatów dla usług sieciowych
    - lista unieważnionych certyfikatów (ang. *certificate revocation list*, CRL)
    - protokół OCSP (ang. *online certificate status protocol*)

3. Działanie protokołu SSL/TLS

    - cechy protokołu SSL/TLS oraz jego zastosowania
    - wersje protokołu
    - przebieg działania i elementy protokołu: SSL Handshake, SSL Change Cipher, SSL Alert Protocol, SSL Record Protocol
    - protokół DTLS
    - rozszerzenia protokołu SSL/TLS

4. Konfiguracja protokołu SSL/TLS

    - pakiety algorytmów (ang. *cipher suites*)
    - wybór metody uwierzytelnienia serwera i klienta
    - jednostronne i obustronne uwierzytelnienie w protokole SSL/TLS
    - pozyskanie certyfikatów
    - wybór metody wymiany/uzgodnienia klucza, pojęcie PFS (ang. *perfect forward secrecy*)
    - wybór algorytmów i parametrów protokołu
    - konfiguracja wybranych serwerów (np. dla usługi HTTPS)

- wpływ certyfikatu oraz parametrów protokołu na zachowanie przeglądarki internetowej
- działanie i wykorzystanie PSK (ang. *pre-shared key*)
- działanie i wykorzystanie SRP (ang. *secure remote password*)
- wykorzystanie programowych i sprzętowych końcówek SSL/TLS
- wykorzystanie sprzętowych modułów bezpieczeństwa (ang. *hardware security module*, HSM), terminatorów SSL/TLS oraz kart elektronicznych, biblioteki PKCS#11
- testowanie działania protokołu
- weryfikacja poprawności konfiguracji

5. Protokół SSL/TLS w usłudze HTTPS

   - mechanizm HSTS (ang. *HTTP Strict Transport Security*)
   - mechanizm HPKP (ang. *HTTP Public Key Pinning*)
   - wykorzystanie CSP (ang. *Content Security Policy*)

6. Podsumowanie

   - aktualne zalecenia dotyczące algorytmów i parametrów protokołu
   - protokół TLS 1.3