Opis przedmiotu:

Celem zajeć jest zaprezentowanie różnych aspektów bezpieczeństwa aplikacji. Omówione zostaną często spotykane luki bezpieczeństwa wraz ze sposobami na ich unikanie, komponenty aplikacji krytyczne pod względem bezpieczeństwa oraz dodatkowe elementy związane z bezpieczeństwem, jak np. testowanie czy normy ISO. Wszystkie prezentowane zagadnienia będą podparte stroną praktyczną, czyli przeglądem produktów dostępnych na rynku wraz z przykładowym kodem w ulubionym języku programowania.

Program

1. Bezpieczeństwo aplikacji
    - wprowadzenie do zagadnienia
    - przegląd często spotykanych zagrożeń...
    - ... i sposoby na ich unikanie
    - rankingi OWASP i CWE
    - baza CVE, kalkulator CVSS
2. Certyfikaty, podpisy elektroniczne, znaczniki czasu
    - podstawy teoretyczne, PKI, zastosowania certyfikatów
    - certyfikaty dostępne na rynku, rola Narodowego Centrum Certyfikacji, usługi kwalifikowane
    - strona praktyczna, przegląd rozwiązań, tworzenie własnych centrów certyfikacji
3. Uwierzytelnianie i autoryzacja
    - komponenty składowe rozwiązania i ich rola
    - znaczenie w różnych warstwach sieciowych
    - przegląd protokołów i rozwiązań dostępnych na rynku, w tym NTLM i Kerberos
    - mechanizmy kontroli dostępu, w tym RBAC & ABAC
    - procesy związane zarządzaniem tożsamościami i dostępem
4. Federacja tożsamości i delegacja autoryzacji
    - protokoły OAuth2, OpenID Connect i XACML
    - bezpieczeństwo w różnych typach architektury
    - integracja z usługami firm trzecich: SMS, systemy płatności, Auth0, Google, Facebook
5. Bezpieczeństwo baz danych
    - przykład rozwiązań proponowanych przez Microsoft SQL Server
6. Bezpieczeństwo na poziomie infrastruktury
    - bezpieczeństwo serwerów aplikacji
    - przegląd komponentów jak firewalle, proxy, IDS/IPS, WAF
    - znaczenie monitoringu, rola SIEM
7. Architektura zabezpieczeń
    - znaczenie dobrych wymagań
    - rodzaje kontrolek i ich zastosowanie
    - przegląd i znaczenie podstawowych zasad bezpieczeństwa (ang. security principles)
    - przegląd warstw architektury i ich rola

- koncepcja tzw. security domains

8. Modelowanie zagrożeń
    - metodyka STRIDE
    - zastosowanie narzędzi wspierających
9. Bezpieczeństwo informacji
    - podstawowe koncepcje i pojęcia
    - przepływy informacji i ich zabezpieczenie
    - wykorzystanie modelowania zagrożeń
10. Testowanie bezpieczeństwa
    - testy penetracyjne i skany podatności, rodzaje, metodyki
    - przegląd narzędzi do przeprowadzania testów
    - wprowadzenie do hakowania
11. Bezpieczeństwo w procesie wytwarzania oprogramowania
    - omówienie procesu, przegląd głównych etapów
    - przegląd ważniejszych aktywności, m.in. zbieranie wymagań, analiza ryzyka, threat modelling.
12. Znaczenie wprowadzenia i utrzymywania polityki bezpieczeństwa