Filip Zavoral
ZS 2023
1/1 Z

Kentico CGI

nový prakticky orientovaný předmět
ve spolupráci s odborníky z praxe
přednášky + workshop

NSWI202

Bezpečnost sw systémů v praxi

Secure Development Life Cycle
Přehled jednotlivých fází SDLC, jak včasně identifikovat zranitelnosti definované v OWASP TOP 10 a jakým způsobem k nim přistupovat. Také se zaměříme na penetrační testování, které je důležitou součástí životního cyklu vývoje aplikací. Dále se budeme věnovat poznatkům získaných z předcházejících penetračních testů a jak je co nejlépe aplikovat na budoucí projekty. Na konci semestru využijeme znalosti z této přednášky k absolvování praktického workshopu.

Security in the Cloud
Techniky a ověřené postupy pro zabezpečení cloudové infrastruktury. Dotkneme se témat jako "Infrastructure as Code (IaC)", "Infrastructure hardening" a vývoj SaaS produktu hostovaného v cloudu. Seznámíme se s průběhem "Disaster recovery" testů a jak tyto testy pomáhají zlepšovat dostupnost a spolehlivost cloudové infrastruktury.

Compliance
Ucelený přehled o bezpečnostních normách se zaměřením na certifikace SOC 2 a ISO 27001. Studenti se seznámí s klíčovými požadavky a doporučenými postupy pro dosažení a udržení požadavků stanovených v těchto normách. Seznámíme se spojenými aktivitami jako je pravidelné posuzování bezpečnosti, zavádění vhodných kontrolních mechanismů a prokazování souladu se stanovenými předpisy. Ukážeme si, jak využít znalosti získané na předchozích přednáškách k implementaci standardů informační bezpečnosti ve společnosti.

Workshop
Půldenní workshop je zaměřen na odhalování bezpečnostních zranitelností ve webových aplikacích na základě metodiky OWASP. Workshop zahrnuje teoretickou a praktickou část. Teoretická část stručně popisuje nejčastější webové zranitelnosti - jejich dopad na bezpečnost, integritu a dostupnost webové aplikace. V praktické části si studenti vyzkouší najít bezpečnostní zranitelnosti v reálném produktu.

Identifikace, autentizace, autorizace a auditing
Identifikace, identifikátor, autentizace (znalost, vlastnictví, biometrie), credentials, autorizace, federalizace. Budou rozebrány moderní metody používané pro bezpečnou autentizaci jako druhý faktor a jako passwordless mechanismy autentizace. Detailně budou rozebrány mechanismy xOTP (HOTP, TOTP), WebAuthn a navazující technologie pro passwordless autentizaci PassKey.

Single Sign On a federalizovaná autentizace
Detailně bude rozebrána problematika Single Sign On v interním prostředí organizace a protokoly LDAP, Kerberos a SAML2. Bude diskutována problematika federalizované autentizace v prostředí internetu pomocí protokolu OpenID Connect (i ve vazbě na OAuth2) a jeho aplikace v rámci federalizovaného přihlašování. Detailně budou rozebrány role jednotlivých zúčastněných entit, sekvence volání, formáty přenášených dat a formáty souvisejících metadatových souborů. Bude zmíněna také role odvozených protokolů v nově připravované Evropské peněžence digitální identity.

Praktická cvičení
Studenti naprogramují minimální webovou aplikaci, která pro autentizaci využívá některou z technologií WebAuthentication/FIDO2 nebo PassKey.
Studenti nakonfigurují poskytovatele identity podle protokolu OpenID Connect (server Keycloak) a implementují demo aplikaci, která použije federalizovaného protokolu OpenID Connect pro přihlášení uživatele. Alternativně bude provedena integrace Kentico pomocí OpenID Connect.