

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: Bc. Kristián Zednikovič

Oponent: Mgr. Martin Bačík

Studijní program: **Informační technologie**
Specializace: **Kybernetická bezpečnost**
Akademický rok: **2024/2025**

Téma diplomové práce: Útoky na cloudovou infrastrukturu a multi-tenant aplikace

Hodnocení práce:

Práce sa venuje vysoko aktuálnej a odborne náročnej problematike – bezpečnosti cloudových infraštruktúr so špecifickým dôrazom na viacnásobné zdieľanie prostredia (multi-tenancy), čo je kľúčová oblasť pri návrhu moderných SaaS riešení.

Práca obsahuje rozsiahlu teoretickú časť, praktickú implementáciu, simulácie reálnych útokov a návrhy mitigácií. Pokrýva široké spektrum útokov (IAM misconfig, BOLA, XSS, SQLi, public Blob leaks, session hijacking atď.).

Autor pracuje s najnovšími trendami (Zero Trust, AI threats, confidential computing, PQC) a aktuálnym technologickým stackom (Azure, Entra ID, Node.js, React).

Práca kombinuje teoretické znalosti, vývoj aplikácie, cloudové nasadenie a penetračné testovanie – úroveň obtiažnosti je vysoká, pričom autor zvládol preukázať orientáciu v komplexných témach ako IAM abuse, multi-tenantné API ochrany či supply chain riziká.

Autor pristúpil k téme veľmi systematicky – najskôr vybudoval teoretický rámec, identifikoval typické hrozby, následne pripravil aplikáciu v Azure a demonštroval reálne útoky na vlastný deployment. Prístup je metodologicky správny – zahŕňa definovanie výskumných otázok, delimitáciu rozsahu, popis technického prostredia aj simuláciu útokov. Pojatie zahŕňa praktické overenie zraniteľností a validáciu obranných opatrení, čo zvyšuje výpovednú hodnotu.

Diplomant preukázal hlboké porozumenie problematike. Praktický prínos spočíva vo vytvorení multi-tenant aplikácie, simulácii zneužitia IAM politík, API abuse, únikov dát z Blob storage, odchyťávaní session tokenov, aplikácii SSDLC princípov a mitigácii cez Key Vault, RBAC či CSP. Prínos vidím najmä vo výborne dokumentovaných simuláciách a návrhoch na mitigáciu, ktoré môžu slúžiť ako referencia pre bezpečnostných architektov.

Práca je rozsiahla (viac ako 130 strán), typograficky jednotná, dobre členená, s bohatým zoznamom zdrojov (vedecké publikácie, dokumentácia poskytovateľov bezpečnostných systémov a cloudových služieb, OWASP, NIST).

Menšie nedostatky:

- Občasná redundancia (napr. niektoré mitigácie sa opakujú v rôznych častiach).
- Niektoré ilustrácie by mohli byť vizuálne výraznejšie (vhodné farebné odlišenie komponentov v diagramoch a schémach).
- Citovanie zdrojov v texte je niekde formálne neúplné (číslo v hranatej zátvorke bez priamej väzby na bibliografiu).

Práca Bc. Kristiána Zednikoviča je kvalitná, odborne vyspelá a demonštruje schopnosť samostatne riešiť komplexné bezpečnostné problémy v oblasti cloudu a multi-tenant architektúr. Diplomant preukázal schopnosť kombinovať teóriu s praktickým testovaním a navrhol konkrétne mitigácie založené na overených postupech.

Otázky k obhajobe:

Ako by ste riešili tenant-based throttling a ochranu proti „noisy neighbor“ efektu na úrovni Azure SQL?

Overovali ste zraniteľnosť aplikácie voči OAuth token substitution alebo Refresh Token abuse?

Uvažovali ste o použití Azure Policy alebo Defender for Cloud ako ďalšej vrstvy obrany? Prečo/Prečo nie?

Viete porovnať výhody a riziká nasadenia vašej aplikácie v Azure App Service vs. Azure Kubernetes Service z pohľadu bezpečnosti?

Celkové hodnocení práce:

Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:

A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně, F – nedostatečně.

Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

A - výborně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 3.5.2025

Podpis oponenta diplomové práce