

Posudek konzultanta bakalářské práce

Název: DNS Firewall a jeho nasazení a integrace v rámci kybernetického operačního centra

Student: Martin Doležal

Vedoucí práce: doc. Ing. Jan Jeřábek, Ph.D.

Autor práce v úvodních kapitolách popisuje fungování bezpečnostního operačního centra (SOC) a zevrubně představuje Domain Name System (DNS) s důrazem na pojmy relevantní pro tuto práci. Obecně se zabývá možnostmi zabezpečení DNS a do tohoto kontextu zasazuje DNS Firewall.

V navazující kapitole se autor věnuje konkrétní implementaci DNS Firewallu v testovacím prostředí SOCu. Autor správně chápe nutnost napojení na základní služby centra. Zde oceňuje nastudování technologií a jejich integraci s DNS Firewalllem. Autor dobře chápe výhody a přidanou hodnotu spojení DNS Firewallu a ostatních technologií SOCu, zejména pak integraci s platformou pro správu Threat Intelligence.

Autor v dalších kapitolách mapuje možnosti napojení na DNS Firewall, jejich výhody a nevýhody a smysluplně definuje limity při využití různých způsobů napojení. Zároveň se zabývá možnostmi vynucení využití DNS Firewallu a definuje jejich omezení. Zejména oceňuje, že autor omezení různých způsobů napojení pouze nemapuje, ale navrhuje způsoby, jakými dopady těchto omezení zmírnit. V rámci práce autor provedl testy výkonnosti a dostupnosti a výsledky zasazuje do kontextu jiných veřejných DNS serverů.

Autor v bakalářské práci správně definuje výzvy a potřeby, které bylo nutné před nasazením technologie v rámci SOCu otestovat. Zvláště oceňuje neopomenutí možnosti poskytování různé úrovně služby a přizpůsobení potenciálním požadavkům připojených organizací, z čehož vyplývá, že autor korektně chápe potřeby pro poskytování technologie DNS Firewallu jako služby. Poznatky zjištěné v rámci práce budou využity při případném produkčním nasazení DNS Firewallu. Závěry vyplývající z bakalářské práce hodnotím jako velmi přínosné.

3. června 2022

Lukáš Novák