Hodnocení vedoucího diplomové práce

Autor práce: **Bc. Martin Šebela**

Název práce: **Systém pro správu bezpečnostních incidentů v síti WEBnet**

Aktivita studenta
Student byl během vypracovávání diplomové práce velmi aktivní. Zúčastnil se semináře na téma Postup při řešení bezpečnostních incidentů certifikovaným bezpečnostním týmem Masarykovy univerzity a také diskutoval záležitost se zakládajícím členem bezpečnostního týmu WIRT Západočeské univerzity v Plzni (dále jen ZČU), Ing. Alešem Padrtou, Ph.D.

Spolupráce s vedoucím
Spolupráce s vedoucím byla příkladná, při pravidelných konzultacích byla vždy diskutována dosavadní práce studenta a docházelo k vyjasňování a upřesňování některých bodů. Všechny připomínky ze strany vedoucího DP byly vždy vypořádány.

Původnost práce a práce související
Výstupem diplomové práce je unikátní software pro správu bezpečnostních incidentů, které bezpečnostní tým WIRT řeší. Software byl vytvořen a implementován do prostředí ZČU a podařilo se jej napojit na všechny potřebné informační systémy a další obslužné systémy, které jsou potřeba pro úspěšné vyřízení bezpečnostního incidentu.

Kvalita řešení
Text diplomové práce je dobře strukturovaný, jazyková i stylistická stránka je na odpovídající úrovni. Práce s referencemi je také dobrá.
Vytvořená aplikace byla navržena a implementována s využitím architektury MVC (model-view-controller). Bylo také připraveno kvalitní uživatelské rozhraní, které je intuitivní, s integrovanou nápovědou, a vizuálně i způsobem ovládání se podobá dříve vytvořenému systému pro rozesílání cvičných phishingových e-mailů (Bakalářská práce, Phishingator), který bezpečnostní tým WIRT také využívá.

Využitelnost dosažených výsledků
Vytvořená aplikace byla již nasazena v pilotním provozu na ZČU. Při řešení bezpečnostních incidentů urychlí vyřízení incidentu v průměru 3x v porovnání s dosud využívaným systémem a 5x v porovnání s „ručním" řešením. Incident je v kterékoli části sítě možné kompletně vyřešit v řádu jednotek minut. Systém navíc eliminuje případné chyby nebo opomenutí některého z nutných kroků a nevyžaduje nutnou kvalifikaci pracovníka WIRT.

Splnění zadání
Cílem práce bylo seznámit se s postupy reakce CSIRT na bezpečnostní incidenty, provést analýzu bezpečnostních incidentů a identifikovat nejzávažnější a nejčastější bezpečnostní incidenty. Na základě analýzy navrhnout, implementovat a otestovat systém v praxi. Dále bylo úkolem analyzovat výsledky a navrhnout případná rozšíření systému.
Všechny cíle práce byly splněny.

Navrhuji hodnocení známkou **výborně** a práci **doporučuji k obhajobě**.

V Plzni 21. května 2021

Ing. Jiří Čepák