Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **BC. PAPŠÍK LUKÁŠ** **Oponent:** **Ing. Václav Kopáček**

Studijní program: **Bezpečnostní technologie, systémy a management**
Studijní obor/Specializace: **Bezpečnostní management**
Akademický rok: **2021/2022**

Téma diplomové práce: **Specifikace řešení kybernetických bezpečnostních incidentů**

Hodnocení práce:
Cílem diplomové práce Bc. Lukáše Papšíka „Specifikace řešení kybernetických bezpečnostních incidentů“ bylo analyzovat bezpečnostní modely a přístupy pro řešení kybernetické bezpečnosti, analyzovat kybernetické útoky a následně vytvořit konkrétní model pro řešení kybernetického bezpečnostního incidentu. Analýza a návrhy opatření v oblasti kybernetické bezpečnosti považuji za aktuální a velmi dobře zvolené téma. Práce je zpracována přehledně, bez gramatických chyb a jednotlivé kapitoly na sebe logicky navazují. Po formální stránce se autor dopustil drobných chyb, zejména při využívání zkratek v textu. Na celkový dojem z práce to však nemá vliv. Autor splnil všechny body diplomové práce.

Diplomová práce je rozdělena na teoretickou a praktickou část.

V úvodu teoretické části autor definuje právní hledisko problematiky kybernetické bezpečnosti. Dále se zabývá jednotlivými typy kybernetických útoků. Dále se zabývá způsobem, jak kybernetickým útokům zamezit a analyzuje způsoby přístupu různých typů organizací k procesnímu zajištění kybernetické bezpečnosti. Teoretická část je zpracovana velmi dobře s vlastními dílčími závěry autora.

V úvodu praktické části autor popisuje organizaci, pro kterou bude vytvářet bezpečnostní model přístupu ke kybernetickým útokům, zpracovává analýzu rizik organizace a navrhuje technická opatření v oblasti kybernetické bezpečnosti. Následně navrhuje bezpečnostní modely pro řešení kybernetických bezpečnostních incidentů. V závěru práce autor uvádí aplikaci bezpečnostního modelu, jehož cílem je zachytit kybernetický útok typu Spear-phishing co nejrychleji. Analyzuje průběh řízení celého incidentu včetně nápravných opatření. Návrh bezpečnostních modelů a demonstraci na konkrétním kybernetickém útoku považuji za největší přínos diplomové práce. Praktické části mohl autor věnovat více pozornosti a analyzovat několik kybernetických útoků v rámci vybraného modelu, komparovat jejich rozdílnost z pohledu technických opatření, dopadu pro organizaci a následného Disaster Recovery.

Diplomovou práci doporučuji k obhajobě.

V rámci obhajoby diplomové práce žádám o zodpovězení následujících otázek:

1. Pokud se zamyslíte nad systémy technické ochrany fyzické bezpečnosti (např. PZTS, EPS, VSS) obecně a v rámci modelové organizace, jsou podle Vás také terčem kybernetických útoků? Pokud ano, diskutujte dopady a uveďte jaká opatření byste zavedl, aby se snížila pravděpodobnost kybernetického útoku.

2. Můžete uvést příklad kybernetického útoku, který lze detekovat pouze za pomocí technologie? Můžete uvést, jaké předpoklady k tomu musí organizace splňovat?
3. V modelové organizaci uvádíte, že má vybudované vlastní pracoviště SOC. Myslíte, že každá organizace by měla být napojena na SOC? Zhodnoťte, v jakém případě je vhodné vybudovat SOC přímo v organizaci a kdy využívat SOC jako službu.

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

B - velmi dobře.

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

Datum 29. 5. 2022 Podpis oponenta diplomové práce