Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **DEDEK JINDŘICH** **Oponent:** **Ing. Oldřich Luňáček, Ph.D.**

Studijní program: **Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Akademický rok: **2018/2019**

Téma diplomové práce: **Role prevence v bezpečnosti**

Hodnocení práce:

Cílem diplomové práce Bc. Jindřicha Dedka „Role prevence v bezpečnosti“ bylo analyzovat a obhájit důležitou činnost, kterou prevence v pravém slova smyslu opravdu je. Téma je to velmi aktuální, protože prevence prostupuje téměř celým spektrem lidské činnosti. Lze konstatovat, že se zpracovatel zhostil svého úkolu na dostatečné úrovni.

Autor si práci rozdělil do několika na sebe navazujících částí dle toho, aby splnil jednotlivé body zadání. V rámci teoretické části práce byla pozornost zaměřena na definici pojmu prevence, jak je vlastně realizována, a především jaká je její role v zajištění bezpečnosti. Autor řešil problematiku prevence ve stanovených oblastech. Byla provedena analýza platné legislativy, a dále bylo provedeno rozdělení prevence do několika typů. Autor dále definoval rozhodující činitele, kteří dohlížejí a řídí tuto oblast. Lze konstatovat, že zadání v tomto teoretickém bodu bylo splněno a autor vcelku objasnil danou problematiku. Tento postup práce je adekvátní řešené problematice a lze s ním souhlasit.

Praktická část začíná třetí kapitolou, která je zaměřena na identifikaci a specifikace přístupů, jak realizovat prevenci z hlediska procesů. Student provádí SWOT analýzu a používá hodnocení, aniž by zdůvodnil, co která hodnota znamená a proč zrovna používá to či ono kritériím, proč použil SWOT analýzu, a ne žádnou jinou metodu. Student se snaží poukázat na naprostou odlišnost řešení prevence u informační bezpečnosti. Správně konstatuje že se jedná o významově odlišnou oblast, která prochází velmi dynamickým vývojem v porovnání s ostatními, které jsou zde historicky a jsou vylepšovány postupně. Zrušení časovo prostorových bariér v oblasti informační bezpečnosti dává zcela jiný rozměr v případě toho, že budeme řešit analýzu a eliminaci hrozeb. Proto musí být řešení prevence v oblasti informační bezpečnosti odpovídající situaci, jak po stránce procesní, tak po stránce technologií. Bohužel, zde autor nepřipomene vhodné nástroje, které nám mohou být nápomocny a tím je znalostní management. Využití knowledge managementu může být efektivním nástrojem, s tím jsou spojeny otázky spojené s tvorbou a využíváním znalostních bází, znalostních portálů apod.

Při řešení typů preventivních opatření se zpracovatel zaměřil na analýzu 4 stanovených oblastí. V každé oblasti definuje hrozby, posléze definuje následek a navazuje definicí opatření. S mnoha situacemi nelze jednoznačně souhlasit např. v oblast silniční přepravy porucha – poškozené značení následek – výpadky dodávek, a opatřením mají být cyklostezky, pruhy pro kamiony a celkové rozdělení dopravy. Pokud by autor použil např. graf elementárních hrozeb pro každou oblast, mohl by lépe definovat hrozby, pak by se mu přesněji podařilo vytýčit protiopatření. Některé řešení jsou

nejasná, bez bližšího vysvětlení, protože třeba není uvedeno, z jakého zdroje autor čerpá, a co jednotlivá čísla vlastně znamenají. Podobná situace je i u ostatních analyzovaných oblastí. Pátá kapitola má být vlastním těžištěm samotné práce autora. Lze kladně hodnotit, že si autor správně volí problematiku informační bezpečnosti. Navrhuje mnohá opatření, ale návrhy nejsou zpracovány detailně a do hloubky. Je otázkou, zda realizace některých návrhů by nepřinesla více zmaru než užitku. Bezpečnost každé organizace se odvíjí od nastavené a realizované vlastní bezpečnostní politiky vycházející z legislativních požadavků. Někdy jsou je pouhá obecná konstatování, jež nelze akceptovat jako adekvátní návrh řešení v diplomové práci (viz subjektivní autor názor na místo a plnění úkolů Policie České republiky). Problematika informační bezpečnosti je řešena v České republice, byť ji řeší vícero institucí. Může to přinášet mnohé problémy a výzvy, kterým stát musí při jejich řízení řešit.

Celou práci naprosto a neuvěřitelně sráží množství nepřesnosti anebo opomenutí či vysvětlení určitých oblastí, které měly být řešeny. Autor sice zpracoval návrh řešení, přesto zde postrádám adekvátní odůvodnění navržených kroků. Krátká formulace bez odůvodnění postrádá smysl. K uvědomění si důležitosti zpracování jednotlivých kapitol by přispělo používání dílčích závěrů jednotlivých kapitol, které mohlo napomoci autorovi lépe formulovat své myšlenky.

Z hlediska formální úpravy je nutno zmínit, že práce má sice jednotný styl, ale autor se bohužel nevyhnul značnému množství gramatických chyb. Dalo by se říci že použitá forma českého jazyka je nedůstojná diplomové práci. Autor si zcela jistě neprovedl kontrolu své práce, protože mnohá slova nejsou celá a některé pasáže nedávají smysl. U některých obrázků není uveden zdroj. U tabulek není legenda nebo alespoň popis hodnot co znamenají. Autor se nesnažil zpracovat své dílo v odpovídající formě, jak má vypadat diplomová práce.

Předložená diplomová práce odpovídá zadání a lze konstatovat, že s mnoha výhradami splňuje požadavky kladené na diplomové práce. Student prokázal analytické schopnosti, jakožto i schopnosti tvůrčí inženýrské práce při řešení problematiky prevence v bezpečnosti. a proto jeho diplomovou práci doporučuji k obhajobě.

Při obhajobě diplomové práce žádám o zodpovězení následujících otázek:

1. Definujte významový rozdíl mezi pojmy data, informace a znalosti.

2. V textu práce používáte pojmy opatření a protiopatření. Jaký je mezi rozdíl?

3. Ve svém řešení navrhuje administrativně nařizující přístup, kde důležitou roli sehrává administrátor. Můžete popsat nevýhody a výhody, řešení, kdy firma řeší tuto roli vlastním zaměstnancem anebo formou „outsourcingu“?

4. V textu uvádíte „*pokud se firma stane terčem hackerského útoku a přijde o veškerá data nebo i finance, už se jen těžko obnoví, anebo bude schopná pokračovat*“. Jaká preventivní opatření byste navrhnul, aby tato situace nenastala?

5. Jaké preventivní programy realizuje Ministerstvo vnitra a Národní úřad pro kybernetickou a informační bezpečnost oblasti informační a kybernetické bezpečnosti?

6. V práci navrhujete, že by firmy měly realizovat školení většinou i s přezkoušením a zahrnout i něco ze základních prvků informační bezpečnosti. Jaké povinné minimum by tyto školení měly obsahovat?

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

E - dostatečně.

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

Datum 4. 6. 2019 Podpis oponenta diplomové práce