Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **BC. VLADIMÍRA MANDINCOVÁ** **Oponent:** **Ing. Petr HRŮZA, Ph.D.**

Studijní program: **Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Akademický rok: **2014/2015**

Téma diplomové práce: **Návrh implementace bezpečnostní politiky v informačním a komunikačním systému vybrané firmy**

Hodnocení práce:
Cílem diplomové práce Bc. Vladimíry MANDINCOVÉ na téma *„Návrh implementace bezpečnostní politiky v informačním a komunikačním systému vybrané firmy“* bylo popsat současný stav předmětné problematiky a úroveň řešení v informačních zdrojích. Vytvořit model informačního a komunikačního systému pro firemní prostředí a popsat zásady tvorby bezpečnostní politiky z hlediska komplexního způsobu zabezpečení. Hlavním cílem práce je analyzovat bezpečnostní rizika pro vnější a vnitřní prostředí a na základě této analýzy navrhnout implementaci bezpečnostní politiky. Nakonec má autorka provést zobecnění a návrh doporučení při zvládání rizik.

V teoretické části diplomové práce autorka popsala základní pojmy z oblasti informačních technologií. Ve druhé kapitole se věnoval obecně oblasti bezpečnostní politiky. **Autorka bezpečnostní politiku chápe pouze jako proces řešení bezpečnosti IT v organizaci. Ale bezpečnostní politika je také jeden ze základních dokumentů firmy v oblasti bezpečnosti IT. Bezpečnostní politika IT celé společnosti je jedním ze základních dokumentů, které stanovují požadavky týkající se bezpečnosti. Politika vychází z cílů, strategií, závěrů z analýzy rizik, výsledků kontroly, monitorování, auditů. O tom se autorka v práci vůbec nezmiňuje. Proto je práce zaměřena pouze na řešení bezpečnosti v oblasti IT. Toto vnímání pojmu se pak odráží na řešení v praktické části diplomové práce.** Ve třetí kapitole velice stručně pojednává o ISMS. ISMS objasnila stručně a nevěnovala mu tolik pozornosti. Přitom ISMS je v současnosti pro oblast implementace bezpečnostní politiky nevyhnutelný a důležitý. Ve čtvrté kapitole analyzuje právní rámec týkající se bezpečnostní politiky. **Některé uváděné bezpečnostní normy jsou již několik let zrušeny a nahrazeny novými (jak v ČR, tak i na Slovensku). Mrzí mě, že autorka se v celé práci vůbec nezmínila o normě ISO/IEC 27002, která popisuje nejlepší praktiky pro zajištění bezpečnosti informací v organizaci. V práci se drží normy STN ISO/IEC 17799, která byla právě nahrazena normou ISO/IEC 27002. Další významnou normou je ISO/IEC 27001, o jejíž existenci se pouze jednou autorka zmiňuje na straně 25 (ISMS se věnuje sice třetí kapitola, ale autorka čerpá z jiných zdrojů). Proto teoretickou část hodnotím jako neúplnou a neaktuální.**

Na základě chápání pojmu bezpečnostní politika IT autorkou v teoretické části práce, budu proto praktickou část i z tohoto pohledu posuzovat. V praktické části diplomové práce autorka stručně popsala společnost, ve které následně chce implementovat bezpečnostní politiku. Následně v kapitole šest provedla stručnou SWOT analýzu společnosti. Součástí SWOT analýzy měly být obsahy také kapitol sedm a osm. V sedmé kapitole analyzovala autorka areál a budovu společnosti. **Analýzu zaměřila pouze na požární bezpečnost. Při analýze areálu a budovy ale opomenula například analýzu zabezpečení vstupu a vjezdu do areálu či do budovy společnosti.** Teprve kapitola 9 řeší analýzu IT. Kapitola 9.2 nazvaná přístupy uživatelů by neměla obsahovat

podkapitoly 9.2.1 a 9.2.2, které řeší infrastrukturu a kabeláž, ale měla by se více zaměřit na vymezení lokálního a vzdáleného přístupu jak uživatelů ale také zaměstnanců společnosti. V kapitole 10 autorka uvádí možnosti a návrhy řešení havárie zaměřené na oblast IT u vybrané společnosti, kde z praktického hlediska zaměřila pouze na řešení bezpečnosti před požárem v místnosti se servery. V 11. kapitole autorka popsala obecné problémy při implementaci bezpečnostní politiky. **Podklady pro vypracování kapitoly 9 a 10 autorka neuvádí v seznamu literatury.**
Závěrem chci konstatovat, že řešení bezpečnostní politiky informačního a komunikačního systému firmy je velice složitý proces, který nelze jednoduše popsat v jedné diplomové práci.

Základní struktura diplomové práce je logická a jednotlivé kapitoly na sebe někdy nenavazují. Na konci teoretické i praktické části autorka provedla stručné shrnutí řešeného problému a v praktické části navrhla možnosti zlepšení. V práci je několik překlepů a chyb ve formátování, které mohly vzniknout při převodu dokumentu do formátu pdf. Příště bych doporučoval autorce si práci před odevzdáním překontrolovat. V závěru práce autorka sumarizuje zjištěné poznatky. **Seznam literatury nezahrnuje všechny zdroje, ze kterých autorka čerpala.** Práci je možné i přes nedostatky charakterizovat jako původní.

Při obhajobě prosím o zodpovězení následujících otázek:

1. **Jaká norma nahrazuje STN ISO/IEC 17799 Informačné technológie? Od kdy je platná, kdy byla přijata v ČR a kdy na Slovensku?**

2. **Podle zadání bodu 3. měla autorka analyzovat bezpečnostní rizika pro vnější a vnitřní prostředí. Která bezpečnostní rizika podle vás řadíte do vnějšího a vnitřního prostředí?**

3. **Myslíte si, že je potřeba v nějakých časových intervalech provádět školení správců a zaměstnanců firmy k používání informačního systému a k dodržování bezpečnosti v oblasti IT? Ve kterých případech je potřeba toto školení opakovaně provádět** (v práci uvádíte pouze při nástupu nového zaměstnance)**?**

4. **V ČR je platný Zákon o kybernetické bezpečnosti. Je tento zákon důležitý pro řešení bezpečnosti v KIS? Kterých informačních systémů se tento zákon dotýká? Uvažuje se o přijetí takového zákona i na Slovensku?**

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

D - uspokojivě.

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

Datum 30.5.2015 Podpis oponenta diplomové práce