Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **PERNICOVÁ ANETA** **Oponent:** **Ing. Oldřich LUŇÁČEK, Ph.D.**

Studijní program: **Inženýrská informatika**
Studijní obor: **Informační technologie**
Akademický rok: **2019/2020**

Téma diplomové práce: **Zneužití identity osob jako nový typ bezpečnostní hrozby**

Hodnocení práce:
Cílem diplomové práce Bc. Aneta Pernicové „Zneužití identity osob jako nový typ bezpečnostní hrozby“ bylo zpracovat velmi aktuální téma týkajícího se řešení problematiky zneužití identity osob. Lze konstatovat, že se zpracovatelka zhostila svého úkolu na velmi dobré úrovni.

Autorka si práci rozdělila do několika na sebe navazujících částí tak, aby co nejvěrněji naplnila zadání práce. Lze říct, že se jedná o zdařilé dílo. V rámci teoretické části práce byla pozornost zaměřena na definici pojmu identita, včetně podrobného popisu jednotlivých druhů identity. Se šíří detailního popisu lze nanejvýše souhlasit, včetně legislativního ukotvení řešené problematiky. Ve druhé části autorka rozebrala aktuální problém dneška, kterým je kybernetická bezpečnost. Zde se zpracovatelka pokusila identifikovat možné bezpečnostní hrozby, které jsou založeny na zneužití identity v „digitálním světě“. Bohužel otázkou zůstává, proč neuvedla možné metody, jež by mohly být použity k řešení bezpečnostních hrozeb a rovnou tyto hrozby jmenuje a analyzuje. V kapitole třetí je pozornost zaměřena na zranitelnost. Zde postrádám osvětlení základního pojmu, co je to zranitelnost a jak se dá eliminovat.

V praktické části autorka zpracovala případové studie na vybraných příkladech, kdy se jedná by o zneužití identity. Zároveň jsou jasně navržená protiopatření, se kterými lze souhlasit. Některé by však mohly být detailněji popsány a vysvětleny. Zpravidla se autorka věnuje případům, kdy je hrozba na straně útočníka a působí zvenčí. Asi by bylo vhodné upozornit, že hrozba může být také vnitřní, kdy zaměstnanec organizace zneužije identitu zákazníka ke svému prospěchu a způsobí klientovi škodu. Závěrečná pátá část je věnována návrhu možných protiopatření. Protiopatření jsou navržena na základě předchozí analýzy zjištěných hrozeb. Cílem je maximálně ochránit aktivum každé osoby, a to je identita jednotlivého osoby. S jednotlivými návrhy lze souhlasit. Většího významu by jistě nabyly, pokud by se autorka věnovala v jednotlivých návrzích například tomu, pro jakou skupinu osob je to více důležité, a které osoby jsou zranitelnější a podobně.

Lze konstatovat, že autorka práci logicky rozdělila. Nejprve podrobuje téma analýze a následně v praktické části zužitkovává nabyté poznatky. Navržená opatření jsou vlastním přínosem autorky řešeného problému. Jako malý nedostatek práce vidím věnování menší pozornosti řešení identity ve skutečném světě tzn. „ fyzické“ identity osoby. Kvalitní analýzu tématu doplňují odpovídající návrhy opatření vždy s cílem chránit požadované aktivum, tzn. identitu osoby v komplexním pojetí.

Práce je hodnotná tím, že analyticky poukazuje, jaká nebezpečí jsou možná vidět dnes a jaká lze očekávat v budoucnu. Bc. Pernicová se snaží poukázat na naprostou odlišnost řešení v oblasti

informační bezpečnosti. Jedná o významnou oblast, která prochází velmi dynamickým vývojem v porovnání s ostatními, které jsou zde historicky a jsou vylepšovány postupně. Zajištění identity v oblasti informační bezpečnosti dává zcela jiný rozměr v případě toho, že budeme řešit identitu osob. Proto musí být přijatá řešení velmi progresivní, protože jakékoliv narušení identity v kybernetickém prostoru může mít nedozírné následky. Autorka by mohla ve svých návrzích připomenout efektivní nástroje pro zvýšení ochrany aktiv a tím může být například znalostní management. Využití znalostního managementu může být efektivním nástrojem, sdílená zkušenost napomůže jako prevence. Podobným použitelným nástrojem by mohla být i SWOT analýza.

Velmi kladně hodnotím zvolené řešení tématu, autorka volí správná rozhodnutí, byť by mohla být více detailnější. Jsou navržena mnohá opatření, ale návrhy nejsou zpracovány detailně do hloubky. Bezpečnost každé osoby a tím i ochrana vlastní identity v jakékoliv formě se vždy odvíjí od nastavené a realizované vlastní bezpečnostní politiky každého jedince.

Z hlediska formální úpravy je nutno zmínit, že práce má jednotný styl. Autorka předkládá své dílo v odpovídající formě, jak má vypadat diplomová práce. Práci by prospělo, kdyby autorka části textu v rozumné míře dala do podoby grafů či obrázků. Předložená diplomová práce odpovídá zadání a lze konstatovat, že splňuje požadavky kladené na diplomové práce. Studentka prokázala analytické schopnosti, jakožto i schopnosti tvůrčí inženýrské práce při řešení problematiky prevence v bezpečnosti. a proto její diplomovou práci doporučuji k obhajobě.

Při obhajobě diplomové práce žádám o zodpovězení následujících otázek:

1. Ve druhé kapitole připomínáte evropské normy, postrádám zde české normy řešící ochranu osobních údajů. Můžete objasnit, které české národní normy (zákony) řeší ochranu osobních údajů a problematiku důvěry pro elektronické transakce?

2. V textu práce zmiňujete algoritmus MD 5. Můžete objasnit problematiku haše, hašovacích funkcí, k čemu jsou a proč je používáme?

3. Můžete definovat pojem zranitelnost?

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

A - výborně.

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

Datum 17. 8. 2020 Podpis oponenta diplomové práce