Oponentský posudek disertační práce

KYBERNETICKÁ BEZPEČNOST V KRITICKÝCH INFORMAČNÍCH INFRASTRUKTURÁCH

Autor:

Ing. Josef Bernátek

Oponent:

doc. Mgr. Oldřich Krulík, Ph.D.

Aktuálnost tématu práce

Aktuálnost práce je mimo veškerou diskusi, autor ostatně poukazuje i na zavádějící nebo ne úplně šťastně zvolené postupy v bezpečnostní komunitě, při jejichž řešení není důvod otálet.

Splnění cílů práce

Cíle práce, nakolik k mého pohledu relativně netypicky pojaté, byly bezesporu naplněny.

Metody a postupy řešení

Hypotézy práce mohly být dozajista naformulovány více typicky, aby bylo možné je jednoznačněji verifikovat nebo falsifikovat. V tomto stavu se jedná spíše o výzkumné otázky nebo o konstatování, která si autor klade za cíl sledovat.

Výsledky práce a konkrétní přínosy autora, význam práce pro praxi

Doporučení v kapitole 6.1 jsou podle mého názoru potřebná, významná, potenciálně přínosná a zasluhovala by reakci praxe. Je možné ve stručnosti shrnout, jak k nim autor dospěl a zda existuje potenciál jejich praktického využití? Doporučení v kapitole 6.2.4 je velmi přínosné, jako ostatně celá kapitola 6. Název této kapitoly (Diskuze) je ovšem zavádějící, daleko vhodnější by byl například pojem „Doporučení pro praxi", s tím, že verifikace respektive falsifikace hypotéz v úvodu kapitoly 6. by se přesunula do Závěru práce.

Vůči doporučením v kapitolách 6.3, 6.4 nebo 6.5 nevznáším připomínek. Jedná se o aspekty velmi potřebné. Mohlo by však v některých případech jednoznačněji zaznít, jak k těmto doporučením autor dospěl – zda na základě vlastních odborných

zkušeností a praxe, nebo na základě komunikace s experty, jedná se o výsledek šetření atd.

Význam práce pro rozvoj studijního programu

Celá kapitola 2 a 3 by mohla, jen s malým dopracováním, sloužit jako svého druhu učebnice nebo jiný odborný vzdělávací text.

Konkrétně pasáž věnovaná definicím (3.1) a organizačně-kompetenčním aspektům problematiky (3.3) je z mé strany zcela bez připomínek. Do značné míry se může ve vztahu k tématu jednat o rukověť pro další zainteresované badatele. Vedoucí práce, doc. Požár byl v tomto ohledu zárukou, že se autor neodchýlí od zavedených definic, respektive že je ještě rozšíří.

Kapitoly 3.5 a 3.6 by mohly sloužit jako mikromanuál, výuková podklad (základ wikiskript), kde by se nicméně opět uplatnila určitá infografika, organigram.

Formální úprava a práce a její jazyková úroveň

Vůči formální úpravě práce vznáším pouze drobné připomínky:

Některé pasáže jsou psány natolik hutně, že je třeba jejich čtení věnovat maximální soustředění. Obecně by se v textu uplatnilo více infografiky.

V textu je možné občas naleznout neshodu podmětu s přísudkem nebo nadbytečné slovo.

Počet odkazů na zdroje v práci kolísá, existují zde celé stránky bez jakéhokoli poznámkového aparátu nebo jen s omezeným poznámkových aparátem (i když zde zaznívají poměrně objevná zjištění). To může být způsobeno tím, že všechny uvedené informace pochází, například, z osobní zkušenosti autora – což by však v textu mohlo být výslovně zmíněno.

Právní předpisy jsou v celém textu psány ne vždy ideálním způsobem (Zákon č. ... Sb., ... v platném znění, nebo ve znění pozdějších předpisů).

V kapitole 3.2 jsou jak právní předpisy, tak dominantně strategické a další dokumenty neprávní povahy, Toto by bylo vhodnější oddělit.

V kapitole 3.3 by mohla být jako příloha uvedena tabulka domácích pracovišť typu CERT/CSIRT.

Kapitola 3.4 je značně úsporná. Téma by na jednu stranu mohlo získat daleko větší pozornost, ale ve prospěch autora vyznívá, že je to do určité míry rozptýleno v dalších kapitolách.

Kapitoly 3.9 až 3.13 by mohly tvořit společnou kapitolu vyššího řádu, více pojatou i jako manuál nebo přehled modu operandi incidentů tohoto charakteru.

Kapitoly 4 a 5 jsou jako celek velmi zajímavé a přesvědčivé. Autor přitom postupuje velmi sevřeně, mohl by občas použít tabulku či jiný názorný element, shrnující jeho respondenty (třeba v části 5.4).

Závěr (s. 104) je koncipován podle mého názoru značně stručně. V jeho rámci by přitom nebylo například od věci zopakovat hypotézy z Úvodu práce, a ve stručnosti uvést základní informace o tom, na základě jakých zjištění se nepotvrdily.

V seznamu zdrojů je uvedeno 127 podkladů, které nicméně mohly být v práci tohoto charakteru roztříděny podle typů (právní předpisy, monografie, periodika, atd.).

Připomínky a závěrečné zhodnocení práce

Co se týče konkrétních připomínek, viz jiné pasáže tohoto posudku. Práce je jako celek poměrně zdařilá, byť zde existuje potenciál pro určité zlepšení (větší názornost, „uživatelská vstřícnost", širší srozumitelnost pochodů, které vedly k výsledkům atd.). To však nic nemění na tom, že práci hodnotím ve výsledku pozitivně a **doporučuji ji k obhajobě**.

Možné otázky v rámci obhajoby:

Disponuje autor možnostmi svá doporučení v kapitole 6 nějak přenést do praxe? Komunikoval tato doporučení se stáními orgány, respektive v jejich rámci sám působí?

Jak je pojata šedá zóna, co může být příčinou nehlášení určitých incidentů ve vztahu ke kyberprostoru? Souvisí trendy v počtu hlášení s rostoucí rolí jiných pracovišť typu CSIRT/CERT než národního (v České republice)?

Co se rozumí „ekonomickým dopadem" v kapitole 6.1.2?

V Praze, 7. VIII. 2020

doc. Mgr. Oldřich Krulík, Ph.D.