MUNI
ECON

Oponentní posudek disertační práce

Název práce: Metodika hodnocení úrovně kybernetické bezpečnosti

Autor práce: Ing. Lukáš Podešva

Školitel: doc. Ing. Miloš Koch, CSc.

Aktuálnost tématu

Téma práce se soustředí na problematiku návrhu metodiky hodnocení kybernetické bezpečnosti na úrovni podniku. Toto téma je mimořádně aktuální, a to zejména v rovině aplikační. Přestože je tato oblast v praktické rovině implementována skrze řadu norem, standardů a nařízení majících mnohdy charakter zákonů či předpisů, jedná se často o nástroje zaměřené na velké korporace a státní instituce. Doktorand výsledky své práce směřuje zejména pro využitelnost na úrovni malých a středních podniků, což lze hodnotit pozitivně a nabízí to potenciál minimálně aplikačního přínosu.

Cíl práce a jeho naplnění

Hlavním cílem předložené práce je (v souladu se zadáním) „navrhnout komplexní metodiku pro hodnocení úrovně kybernetické bezpečnosti organizací, která integruje vědecké poznatky a nejlepší praxe v oblasti kybernetické bezpečnosti, která bude efektivně identifikovat a řešit slabá místa v procesech kybernetické bezpečnosti". Takto stanovený je velmi hodně ambiciózní a svým způsobem široce pojatý, už jen s ohledem na použití termínů „komplexní", „efektivně identifikovat" a „řešit slabá místa", kdy je potřeba uchopení právě těchto obecnějších termínů v práci vyjasnit a upřesnit. Domnívám se, že se toto celkem daří v rámci definování vedlejších cílů a výzkumných otázek a víceméně i pak samotná struktura a postup zpracování dizertační práce vyjasňují logiku naplnění tohoto cíle a poskytují čtenáři dostatečnou představu o celkovém přínosu práce a použitých metodách.

Celkově se autorovi určitě hlavní cíl i dílčí cíle podařilo naplnit, i když v některých dílčích aspektech lze najít určitě rezervy. Podrobně zpracovaná literární rešerše pomohla autorovi identifikovat klíčové bezpečnostní procesy podniků, motivace útočníků a modelové přístupy k ekonomickému hodnocení výnosů a nákladů kybernetické bezpečnosti, které následně zakomponoval do svého návrhu metodiky hodnocení kybernetické bezpečnosti. Vytvořenou metodiku se pokusil validovat na omezeném vzorku firem, přičemž v rámci diskuse svých dosažených výsledků a závěrů si je vědom limitů svého přístupu i možností dalšího rozvoje v akademické i aplikační rovině.

Použitá data, metody a literární rešerše

V práci využívané metody a data jsou v práci představeny celkově srozumitelným způsobem. Literární rešerše je rozsáhlá a ukazuje, že se doktorand s řešenou problematikou velmi podrobně seznámil. Její základní struktura má velmi dobrou logiku. Podívat se na existující normy a standardy v oblasti kybernetické bezpečnost a vystihnout jejich základní a pro práci podstatné charakteristiky je naprosto logické východisko celé práce. Shrnující tabulka (tabulka 3.7, která je předpokládám autorova vlastní invence, neboť zde chybí ozdrojování), kromě jasné identifikace klíčových oblastí, které by nová navrhovaná metodika měla obsahovat, ukázala možnosti a potenciální aplikační přínos předložené práce, kdy jedním z klíčových přínosů je zaměření rozvoje metodiky do oblasti malých a středních firem, kde jsou různá zákonná řízení aplikována velmi omezeně. Pozitivně hodnotím, že přesně tímto směrem v rámci své práce doktorand zamířil.

Literární rešerše odborných prací je ve své hlavní struktuře rovněž logicky vystavěna a bezpochyby pomohla definovat další aspekty navrhované metodiky, jakou je např. použitý ekonomický model

hodnocení přínosů a nákladů zavádění opatření v oblasti kybernetické bezpečnosti, faktory definující zranitelnost a kybernetická rizika podniku a jeho atraktivitu z hlediska útočníka a celkově i klíčové aspekty procesní stránky kybernetické bezpečnosti. Literární rešerše rozhodně ukazuje, že si doktorand nastudoval velké množství relevantní literatury a dokázal ji věcným a účelným způsobem zpracovat. Drobnou výtku bych měl snad jen k samotnému přístupu k prezentaci jednotlivých studií, kdy bych místo po odstavcích popisovaných jednotlivých článků zvolil systematičtější přístup, který by se snažil tyto články vhodněji uspořádat, systematizovat a kategorizovat, např. dle shody na závěrech, použitých metodách, datech apod.

Z hlediska použitých dat doktorand vychází jednak z „mikrodat" dat portálu ZEFIS, dále pak z dalších veřejně dostupných sekundárních dat pro potřebu kalibrace některých parametrů dále využívaného modelu. Pokud jde o použitá data z dotazníku, je otázkou, jestli pro upřesnění rizika kybernetického incidentu nešlo získat i další charakteristiky firem a provést tak podrobnější kvantitativní analýzu než vyjádření pravděpodobností skrze relativní četnosti dle dvou, byť asi klíčových, faktorů. Soudím tak na základě uvedeného dotazníku, kde jsou vybrány otázky 102, 133, 134 a 280.

Pokud jde o použité ukazatele, tak mají svůj základ v literatuře, nicméně bych i v rámci kapitoly 4 uvítal jejich explicitnější návaznost na literaturu. Např. logika ukazatele RSMA je vcelku intuitivní, na druhé straně převod na skóre a jeho barevné rozlišení v obrázku 4.1 vypadá na první pohled arbitrárně. Spíše bych řekl, že by postup měl být (a možná i byl) ten, že z (empirických) výsledků z tabulky 4.2., lze navázat získané pravděpodobnosti na RSMA skóre.

Tato data byla dále kombinovaná s agregovanými sektorovými daty a logicky posloužila jako základ pro model očekávaných výnosů z investic do kybernetické bezpečnosti. Pozitivně bych hodnotil autorovu otevřenost z hlediska toho, že využívá dat jen pro omezenou množinu sektorů, což samozřejmě představuje i limity použitelnosti vytvořené metodiky (nicméně ne postupu jejího vytvoření). V části 4.3 nicméně postrádám aspoň drobnější diskuzi nad výslednými mapami kybernetického rizika a rozdíly oproti mapám z obrázků 4.1 a 4.2. Platí, že dále zmiňované dva sektory jsou podmnožinou dostupných dat využitých pro obrázky 4.1 a 4.2?

V rámci finální metodiky hraje významnou roli stanovení vah procesů (tabulka 4.6). Rozumím, že váhy byla stanoveny v návaznosti na expertní odhady, nicméně, pozornost by si zasloužilo bližší vysvětlení, jestli se jedná o nějaké vážené průměry, jestli jsou některé váhy (pravděpodobnosti) takřka stejné bez ohledu na firmu/experta a u některých je vyšší volatilita a případně, jestli lze případnou heterogenitu ve vahách ztotožnit s nějakou typickou charakteristikou firmy (což by mohlo být v metodice zohledněno).

Výsledky na základě vytvořené metodiky jsou prezentovány na příkladu simulované firmy (zde by se hodilo zdůvodnit, proč bylo nastavení zvoleno právě takto, jestli se jedná o typickou firmu apod.). Na základě kvalitativního šetření pak byla validita ověřována v rámci tří firem. Přestože se nemusí jednat o reprezentativní a dostatečně robustní ověření validity, má tento postup ověřování validity smysl a výsledky přinejmenším napovídají, že by pro koncového uživatele z řad středních a malých firem mohl být přínosný.

Postup řešení a dosažené výsledky

Postup řešení spolu s celou strukturou dizertační práce určitě vede k naplnění cíle. Logika postupu je celkově solidně vysvětlena a uchopena. Použitý postup i zvolená data mají svou oporu v literatuře, i když bych uvítal jejich přímější napojení v rámci celé čtvrté kapitoly. Návrh metodiky je navázán na provedenou literární rešerši a přestože by se u řady nastavení modelu a parametrů navrhované metodiky dalo diskutovat o větší či menší relevanci těchto nastavení (viz některé poznámky z předchozí části), zdá se, že v aplikační rovině, byť na základě omezené validace, může navržená metodika představovat pro malé a střední firmy přínos a má i svůj potenciál na další rozpracování.

Z hlediska naplnění stanovených cílů a získání odpovědí na výzkumné otázky bylo ve větší či menší míře všeho dosaženo.

Rešerše existujících metodik byla provedena relativně důkladně, byly identifikovány klíčové bezpečnostní procesy a na tomto základě navržena metodika nová, z hlediska své logiky i flexibilní. Větší pozornost by si nicméně zasloužilo lépe definovat (v návaznosti na provedenou rešerši) v čem je hlavní přínos oproti např. postupům dle existujících norem a standardů. Samotná validace metodiky byla rovněž provedena, i když spíše v omezeném rozsahu.

V rámci devíti výzkumných otázek lze odpovědi na ně v rámci předložené práce určitě nalézt. Snad jen u otázek 5 (váhové modely), 6 (prezentace úrovně kvality kybernetické bezpečnosti) a 7 (specifické ukazatele) si nejsem jistý, jestli skutečně je na ně v rámci 4. kapitoly dostatečně zodpovězeno. Formálně asi ano, ale např. v rámci otázky 5 si nejsem jistý, co si vlastně nakonec představit pod váhovým modelem. U otázky 6 sice skutečně vrací daná metodika procentní „výkon kybernetické bezpečnosti", ale pro uživatelskou aplikaci bych očekával informaci typu „co mohu zlepšit", „proč jsem v té či oné kategorii" horší" nebo ideálně, „jaké reálné riziko mi kvůli nedostatku v té či oné oblasti hrozí". U otázky 7 je dle mého názoru problém s přílišnou agregací některých ukazatelů. Na jedné straně např. počet počítačů v síti může být významný faktor rizikovosti, ale klíčová bude spíš architektura samotné sítě a nastavení jejího zabezpečení (toto bych očekával, že bude v práci alespoň diskutováno).

Význam pro rozvoj vědního oboru a praxi

K diskuzi nad omezeními, možnostmi dalšího rozšíření a zejména pak přínosy dizertační práce z hlediska vědecko-výzkumného, aplikačního i pedagogického nemám zcela zásadní připomínky. Shrnuto je to v části 6.2, kdy bych nicméně opět více pracoval s argumentací podpořenou referencemi na literaturu (jestli např. některé z přístupů, metod apod. nějakým originálním způsobem nerozvíjí). Význam aplikační a určitě i společenský spatřuji v tom, že tento nástroj (metodika) může přispět k šíření povědomí o této problematice a rozvíjet podnikovou gramotnost malých a středních podniků v této oblasti nebo alespoň upozornit na její potřebu.

Formální úprava a jazyková úroveň

Po formální stránce má práce dobrou a jasně čitelnou strukturu. Jednotlivé části jsou na sobě pěkně provázané. Práce je celkově čtivá a na solidní stylistické úrovni (samozřejmě leckde se neúplně formulované věty objeví, ale lze si bez problémů domyslet, co je jimi myšleno). Prezentované obrázky a tabulky mají v práci svůj význam a je na ně řádně odkazováno. Větší pozornost nicméně mohla být věnována ozdrojování obrázků pro rozlišení toho, co je převzato a co je vlastní zpracování autora. Použitá literatura je relevantní a řádně citovaná.

Celkové hodnocení a otázky k obhajobě

Celkově hodnotím předloženou práci pozitivně. Postup zpracování tématu dizertační práce, stanovení odpovídajících cílů, volba použitých metod je dobře promyšlena a v práci korektně aplikována. Práce a její cíl je solidně ukotven v současné literatuře a z dosažených výsledků je patrný přínos k vědeckému poznání zejména v aplikační rovině.

V rámci obhajoby mám následující okruhy otázek k diskuzi:

1. Z jakého důvodu byly v rámci dotazníku z portálu ZEFIS využity jen čtyři otázky zmiňované v příloze? Nebylo možné získat i další užitečné charakteristiky firem a jak by se daly využít pro vyhodnocení pravděpodobnosti kybernetických incidentů a faktorů, které je mohou ovlinit?
2. Jaká omezení či zkreslení může přinášet ukazatel počtu koncových bodů? Nabízely by se nějaké jiné a relativně snadno dostupné či reportované ukazatele?
3. Jaká omezení či zkreslení může přinášet ukazatel technologické efektivity (vztah 9)? Jakou roli zde může hrát např. typ výrobního podniku?
4. Jaká omezení či zkreslení může přinášet ukazatel produktivity kyberbezpečnosti (vztah 10)? Dá se říct, že je vyšší či nižší ukazatel lepší? A jakou metodikou vyhodnotit, kdo je „zaměstnancem v oblasti kybernetické bezpečnosti"?

5. Na jakém základě vznikla tabulka 4.6 (váhy procesů na mitigaci rizika), jaká míra homogenity či heterogenity je s nimi v dílčích položkách spojena napříč podniky a jak by se to případně mělo či dalo zohlednit v navrhované metodice?

Předložená dizertační práce „Metodika hodnocení úrovně kybernetické bezpečnosti" **splňuje** formální i obsahové požadavky kladené na dizertační práci v programu Ekonomika a management (obor Řízení a ekonomika podniku), neboť obsahuje původní a uveřejněné výsledky nebo výsledky přijaté k uveřejnění v oboru. Po úspěšné obhajobě **doporučuji** udělit titul Ph.D.

doc. Ing. Daniel Němec, Ph.D.

V Brně, dne 6. 10. 2024