ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
PROVOZNĚ EKONOMICKÁ FAKULTA

Ing. Jiří Urbanec
pracoviště: katedra informačního inženýrství

HODNOCENÍ BEZPEČNOSTI INFORMACÍ V INFORMAČNÍCH SYSTÉMECH

vědní obor: Informační management

Autoreferát k získání vědecké hodnosti Ph.D.

Školitel: doc. Ing. Prokop Toman, CSc.
katedra informačního inženýrství
Provozně ekonomická fakulta ČZU Praha

Oponenti:

Obhajoba se koná dne ------- v ------- hodin v zasedací místnosti PEF -----.

S disertací je možno se seznámit na odd. vědy a výzkumu Provozně ekonomické fakulty ČZU v Praze.

prof. Ing. Ivan Vrana, DrSc.
Předseda komise pro obhajoby disertačních prací

2015

OBSAH

1 CÍLE DISERTAČNÍ PRÁCE

Hlavní výzkumná otázka v disertační práci zní: jak stanovit vhodné charakteristiky a atributy informačního systému a jak identifikovat míry pro hodnocení informačního systému z pohledu zachování kritických bezpečnostních charakteristik informací?

Hlavním cílem disertační práce je návrh metodiky pro hodnocení bezpečnosti informací zpracovávaných v informačním systému a formulace závěrů a doporučení pro její využití v praxi. Praktickým přínosem práce je využití jejích závěrů ke snížení bezpečnostních rizik souvisejících s informacemi v informačních systémech organizací. Detekce odchylek a zaměření se na konkrétní slábnoucí oblasti umožní minimalizaci rizik působících na informace v informačních systémech (např. zneužití osobních, obchodních a strategických informací, intelektuálního vlastnictví apod.). Pomocí identifikovaných měr a jejich použití při stanovení tzv. bezpečnostní pozice informačního systému a v procesu auditu lze přispět k vyšší kvalitě ochrany informací a tím přispět ke zvyšování jistoty při správě a řízení investic do bezpečnosti informací. Systematizací hodnocení pozice informačního systému měřením lze dosáhnout opakované použitelnosti systému měr a vytvořit tak základ obchodního modelu Security-As-A-Service.

Formulované cíle vyplynuly z průzkumu teoretických východisek v problematice zajišťování bezpečnosti informací v informačních systémech organizací a z požadavků praxe na aplikaci metodiky hodnocení informačních systémů měřením v modelech řízení informační bezpečnosti.

Dílčí cíle práce jsou:

- identifikovat aktuální stav hodnocení bezpečnosti informací v organizacích v České republice realizací a vyhodnocením primárního výzkumu (kvantitativní a kvalitativní),
- charakterizovat míry pro hodnocení bezpečnosti informací,
- navrhnout a popsat vlastní metodiku pro identifikaci měr a prezentaci bezpečnostní pozice informačního systému,
- validovat navržený postup v konkrétní organizaci na stanovených reálných informačních systémech,
- zhodnotit vhodnost metodiky pro účely řízení informační bezpečnosti.

2 METODIKA PRÁCE

Disertační práce je rozdělena do dvou hlavních částí, které na sebe logicky navazují.

První část je tvořena rešerší současného stavu z literárních zdrojů týkající se bezpečnosti informací, zahrnující současnou českou i zahraniční literaturu včetně norem a standardů. Z literárních východisek jsou na základě dedukce vyvozeny pracovní závěry, z nichž plyne stanovený hlavní cíl a dílčí cíle práce, na jejichž základě byla zpracována praktická část disertační práce.

K vypracování disertační práce byly použity metody teoretické, empirické a srovnávací. Syntézou definovaných literárních východisek, získaných výsledků výzkumu, identifikovaných rizik spojených s informacemi, identifikovaných měr pro hodnocení bezpečnosti informací v informačním systému byl formulován a popsán model chování organizace v České republice a formulován návrh metodiky pro hodnocení bezpečnosti informací v informačním systému měřením. Tato metodika byla následně validována v konkrétní organizaci.

Cílem druhé, praktické části je odpovědět na stanovenou hlavní výzkumnou otázku. Praktická část disertační práce vychází z metodického modelu Stevenson (1989), jež je autorem upraven pro účely práce. Využívaný metodický model je tvořen čtyřmi hlavními částmi – vymezení problému, konstrukce modelu, analýza modelu a syntéza závěrů a implementace.

V disertační práci byl proveden kvantitativní a kvalitativní výzkum zaměřený na identifikaci faktorů ovlivňujících bezpečnost informací a identifikaci měření jako prostředku hodnocení informačních systémů s cílem statisticky vyhodnotit stav hodnocení bezpečnosti informací ve vybraném odvětví. Cílem kombinace kvantitativního a kvalitativního výzkumu je docílení triangulace výsledků, vyjasnění kvantitativně odvozených závěrů a rovněž získání nových poznatků. Dále bylo provedeno vyhodnocení získaných výsledků faktorovou a shlukovou analýzou.

Na základě syntézy výstupů rešerše současného stavu, výstupů analýzy dat získaných v rámci provedených výzkumů a přímého pozorování byl formulován metodický postup pro hodnocení bezpečnosti informací. Metodický postup je ověřen na reálné organizaci a je v práci prezentován ve formě dvou případových studií.

Ze závěrů disertační práce jsou formulovány přínosy pro další rozvoj vědního oboru a přínosy pro ekonomickou praxi.

Kvantitativní výzkum

Cílem kvantitativního výzkumu bylo analyzovat úroveň hodnocení informačních systémů z pohledu bezpečnosti zpracovávaných informací, testovat stanovené hypotézy, provést analýzu kontingenčních tabulek, identifikovat rizika spojená s informacemi zpracovanými v informačním systému, identifikovat míry pro hodnocení bezpečnosti informací v informačním systému. Kvantitativní výzkum respektoval Zákon č. 101/2000 Sb. o ochraně osobních údajů a oblast etiky ve výzkumu.

Výběrový soubor tvořily organizace se sídlem v České republice využívající IT a v rámci organizace byl osloven specialista v oblasti bezpečnosti informací. Výběrový soubor organizací, které byly zahrnuty do výzkumu, byl vytvořen náhodným kvótním výběrem z organizací se sídlem v České republice prezentovaných na internetu. Organizace byly rozděleny do homogenních skupin dle výběrových kritérií odpovídajících ČSÚ tak, aby byla zajištěna reprezentativnost organizací a zobecnitelnost výsledků na výběrový vzorek. Kritéria výběru v rámci výzkumu byla stanovena tak, aby přibližně odpovídala procentnímu zastoupení organizací dle odvětví ekonomiky a velikosti organizace.

- dle odvětví ekonomiky: 15 % z primárního, 15 % ze sekundárního, 70 % z terciálního sektoru,
- dle velikosti organizace dle počtu zaměstnanců: 70 % z malých, 20 % ze středních, 10 % z velkých organizací.

Celkově bylo osloveno 785 organizací, dotazník vyplnilo 101 organizací.

Kvalitativní výzkum

Cílem **polostrukturovaných rozhovorů** bylo podle seznamu otázek, které byly rozděleny do skupin Práce s informacemi, zralost procesů informační bezpečnosti a hodnocení vyvodit nové poznatky, resp. potvrdit poznatky z kvantitativního výzkumu.

Výběrový soubor: 3 respondenti vybraní dle výběrových kritérií.

Sběr dat: polostrukturovaný rozhovor, průměrná doba trvání 30 – 45 minut, nahrávání na diktafon.

Výběrový soubor: záměrný výběrový soubor, specialisté v oblasti bezpečnosti informací v bankovních institucích.

Způsob zpracování dat: naplnění saturace u výzkumných otázek.

Přímé pozorování je výzkumná metoda, při níž se sleduje a zaznamenává nebo popisuje činnost lidí, předmětů, se kterými manipulují, prostředí aj. Jde o subjektivní metodu (Disman, 2008). V průběhu výzkumu bylo umožněno v rámci zpracování disertační práce přímé pozorování v organizaci.

Cílem této metody bylo podpořit výsledky předchozích metod. Jedná se o výzkumnou metodu, při níž se sleduje a zaznamenává nebo popisuje činnost lidí, předmětů, se kterými manipulují, prostředí aj. Jde o subjektivní metodu (Disman, 2008).

Sběr dat: přímé zúčastněné pozorování.

Výběrový soubor: Specialisté v oblasti bezpečnosti informací v bankovních institucích a společnostech

Způsob zpracování dat: případová studie zahrnující doporučení a návrhy pro hodnocení informačních systémů z pohledu bezpečnosti zpracovávaných informací.

Tvorba metodického postupu

Cílem bylo vytvoření metodického postupu pro hodnocení bezpečnosti informací v informačním systému kompatibilního se konstruktem měření dle standardu ISO/IEC 27004 (2009).

Stanovená kritéria: aplikovatelnost měr v procesu měření dle ISO/IEC 27004 (2009), přínosy v oblasti řízení rizik pro informace v informačních systémech organizace a v procesu auditu pro stanovení slábnoucí oblasti.

Postup tvorby: na základě syntézy výstupů analýzy sekundárních zdrojů a výstupů analýzy dat získaných v rámci provedených výzkumů byl formulován metodický postup. Metodický postup je ověřen na reálné organizaci.

Případové studie

Cílem případových studií byl návrh a validace metodiky hodnocení bezpečnosti informací v informačním systému pro vybranou organizaci v bankovním sektoru v rámci ČR.

Procedura zpracování případové studie:

- Na vybrané organizaci v ekonomickém odvětví „finanční služby“ byla zvolena oblast jako cíl hodnocení. Hranice oblasti je zvolena tak, aby byla uzavřená z pohledu použitých informačních a komunikačních technologií, tj. např. samostatnou organizační jednotkou. Oblastí je Přímé bankovnictví. Okolí oblasti je považováno za ideální z pohledu zkoumané problematiky.

- Na vybrané organizaci v terciálním sektoru byla zvolena oblast jako cíl hodnocení bezpečnosti informací. Hranice oblasti je zvolena tak, aby byla uzavřená z pohledu použitých informačních a komunikačních technologií, tj. např. samostatnou organizační jednotkou.
- V rámci oblasti byly identifikovány informační systémy, byly dekomponovány a byl aplikován metodický postup hodnocení a identifikovány míry do formálního analytického modelu. Identifikace systémů, míry a hodnoty parametrů vyplynuly z výzkumu a přímého pozorování.
- Metodický postup a výstupy formálního analytického modelu byly validovány proti očekávaným hodnotám na základě informací z vybrané oblasti.

3 DOSAŽENÉ VÝSLEDKY

3.1 ZÁVĚRY KVANTITATIVNÍHO VÝZKUMU

Pro zajišťování bezpečnosti informací organizace nejčastěji využívají *zákonné normy* nezávisle na sektoru a velikosti organizace a *vlastní interní směrnice a standardy* nezávisle na sektoru. Standardy rodiny *ISO 27000* využívají téměř výhradně organizace z terciálního sektoru a jsou to většinou organizace velké. *Ostatní standardy* na bázi ISO se vyskytují v menšině organizací a jsou to vždy organizace velké.

V rámci všech organizací lze shrnout, že nejsou aplikovány postupy a standardy na bázi ISO standardů.

Organizace za nejvlivnější považují jednoznačně *lidský faktor* a následně *kvalitu technických prostředků ochrany důvěrnosti, integrity a dostupnosti informací*. Tento výsledek lze očekávat, lidský faktor je dlouhodobě identifikován jako nejkritičtější část informačních systémů a lidé jako prvek informačního systému mají nejvíce zranitelností. Faktor *identifikace rizik pro informace* označovali za vlivný převážně respondenti z organizací v terciálním sektoru nezávisle na velikosti organizace. Faktor bezpečnostní *klasifikace informací*, tedy přiřazení hodnoty a rizika konkrétním informacím, považuje za vlivný převážně střední organizace působící v terciálním sektoru. **Pozice faktoru klasifikace informací ve středu spektra vlivnosti však neodpovídá jeho teoretickému významu** pro dříve uváděné faktory, protože klasifikace informací jako výstup analýzy rizik by měla být vstupem jak pro identifikaci rizik, tak pro realizaci procesů informační bezpečnosti a aplikaci opatření, tedy nasazení technických prostředků.

Organizace z terciálního sektoru v závislosti na velikosti organizace z větší části označují za vlivné také faktory *monitoring osob* a *měření charakteristik informačního systému*. *Měření bezpečnostních charakteristik informací* je v terciálním sektoru vnímáno také jako vlivný faktor (u 90,9 %) nezávisle na velikosti organizace a sektoru. Faktory měření bezpečnosti (informačních systémů i informací) považuje za vlivné především velká organizace v terciálním sektoru. Vliv těchto faktorů je však považován za nejmenší. **Vnímání kvantitativního hodnocení bezpečnosti informací (měření) jako nejméně vlivného faktoru potvrzuje trvání nízké priority měření v současné bezpečnostní praxi** V komparaci s faktorem monitoringu osob a technických prostředků je považován za faktor s nižším vlivem.

Organizace si stanovují priority v oblasti dosahování bezpečnosti informací. Splnění legislativních cílů je pro organizace v ČR nejdůležitější a dále pak splnění personálních cílů. Nejmenší prioritu mají technické cíle, což odpovídá ekonomickému chápání cíle informačního systému.

Výsledky ukázaly, že v současné době **nadpoloviční většina zkoumaných organizací hodnotí informační systémy z pohledu rizika pro hodnotné informace** (58,49 %). Nejčastěji realizují hodnocení bezpečnosti informací organizace v terciálním sektoru (77,4 %) a nejméně organizace v sektoru primárním (3,2 %).

Ty organizace, které informační systém nehodnotí (malé a střední organizace), uváděly nejčastěji důvod, že *předpokládají, že informační systém a informace v něm jsou bezpečné* a *spoléhají na svého dodavatele systému* (29 organizací). Výskyt uvedeného předpokladu klesá s velikostí organizace a většinou se jedná se o malé organizace. Menší část malých a středních organizací *nezná postupy pro hodnocení* nebo *hodnocení nepovažuje za důležité*.

Organizace, které bezpečnost informací hodnotí, tak provádějí nejčastěji s cílem **identifikovat slabiny a vznikající problémy** (41,5 %). V rámci výzkumu byla prokázána střední závislost mezi hodnocením bezpečnosti informací a velikostí.

Hodnocení bezpečnosti informací provádí primárně velké organizace nezávisle na sektoru.

Nezávisle na sektoru platí, že s rostoucí velikostí organizace je hodnocení primárně vnímáno jako prostředek pro *identifikaci vznikajících problémů a slabin*. Dále má hodnocení za cíl *zlepšování procesů informační bezpečnosti*, *pokrytí legislativních požadavků*, *potvrzení účinnosti nastavených protiopatření* a nejméně často má za cíl *porozumění bezpečnostním rizikům*. Od hodnocení tedy organizace očekávají schopnost vyhodnocovat trend v charakteristikách bezpečnosti a očekává se, že budou identifikovány slábnoucí prvky zakládající nová rizika.

Měření podle výsledků výzkumu provádí velké organizace v terciálním sektoru. Za metodu měření označuje 76,5 % organizací jimi aplikovaný monitoring procesů a chování lidské obsluhy s cílem identifikovat odchylky od nastavených bezpečnostních politik. Přesně definované charakteristiky měří a vyhodnocuje 17,6 %.

Z výsledků vyplývá, že více než 80 % organizací ve skutečnosti neaplikuje měření bezpečnostních charakteristik informací. Aplikaci monitoringu nelze považovat za jejich měření, neboť monitoring vypovídá o dodržování bezpečnostních politik organizace, resp.

schopnosti odhalit jejich porušení (např. porušení pravidla přístupu k informacím, nepovolené přihlášení se k technickému prostředku nebo jeho zneužití, pokus o útok), nemusí však vypovídat o stavu konkrétních informací a rozsahu jejich ohrožení.

Faktorová analýza identifikovala 2 faktory, které mají vliv na bezpečnost informací. Tyto faktory autor interpretuje jako „bezpečnostní procesy“ a „bezpečnostně kritické prvky“. Shluková analýza identifikovala 7 shluků.

Důraz na lidský faktor a klasifikaci informací je zřetelný především u organizací v pokročilém stupni rozvoje informační bezpečnosti (organizace, které aplikují některou z norem informační bezpečnosti). Aplikace monitoringu je pak trend pozorovatelný u bezpečnostně rozvinutých organizací se silným finančním zázemím.

Kvantitativní výzkum identifikoval hlavní oblasti zájmu:

- měření jako prostředek hodnocení bezpečnosti informací,
- posílení prostředků pro dosažení legislativních cílů,
- snížení rozdílu v přístupu k hodnocení mezi velkými a malými organizacemi,
- prokazatelné snížení rozdílu ve vnímání rizika pro informační aktiva vlastníkem a zpracovatelem,
- další snižování vystavení informací zranitelnostem lidského faktoru plněním informační potřeby (v malých organizacích bezpečnost informací závisí zásadně na lidském faktoru).
- vyvážení významu podceňované klasifikace informací a přeceňovaných technických opatření.

Uvedené oblasti zájmu byly dále zpřesněny v rámci kvalitativního výzkumu.

3.2 ZÁVĚRY KVALITATIVNÍHO VÝZKUMU

Zástupci organizací účastnící se polostrukturovaných rozhovorů společně uvádí, že organizační rizika jsou unikátní, je díky tomu limitován reuse a tedy komoditizace. Jako komodita jsou však jednotlivá protiopatření, což je efektivní.

U organizace A je na projektech menšího rozsahu zřejmá simplifikace bezpečnostních problémů, hlavní výběrové kritérium je cena. Existuje snaha systematizovat správu informačních aktiv přejímáním metodik od mateřské organizace, předchozí pokusy však v několika případech nemají očekávaný přínos. U organizace B dokonce nejsou přímo stanovena informační aktiva ani jejich obchodní hodnota (ani business chain value). Existuje velký rozdíl v povědomí zaměstnanců o aplikaci bezpečnostních opatření. Snahy o zavedení

bezpečnostních opatření většinou naráží na jejich uživatelskou nepřívětivost, které snižují akceptovatelnost informačního systému a které se pak snaží zaměstnanci obejít. Pomocí informačních kampaní a povinných školení se daří stav zlepšovat, což se poměřuje hladkostí průchodu auditem. Vzhledem k tomu, že audit je namátkový, nemusí zcela vypovídat o celkovém stavu v organizaci B, navíc případná certifikace morálně zastarává (pozbývá validity).

Hlavní problémový bod je poskytnutí důkazu, že konkrétní data byla kompromitována během detekovaného incidentu, resp. samotná detekce incidentu. Vnímání rizik u zaměstnanců neodpovídá rizikům nastaveným organizací, což umožňuje útočníkům využít rozdílu ve vnímání k lepšímu využití zranitelností. Klasifikace informací a jejich ohodnocení je vnímáno jako podružné.

Kvantitativní výzkum zpřesnil oblast zaměření:

- ochrana informačních aktiv,
- podpora klasifikace informací,
- odlišné vnímání rizik na straně vlastníka (subjektu odpovědného za informace) a zpracovatele (uživatele, systému, dodavatele služby), resp. odlišného cenění hodnoty aktiv.

Na uvedené oblasti byly v rámci disertační práce zaměřeny instrumentální případové studie.

3.3 NÁVRH MODELU A METODIKY PRO HODNOCENÍ BEZPEČNOSTI INFORMACÍ V INFORMAČNÍCH SYSTÉMECH

Jako jeden z výstupů práce byl na základě kvalitativního a kvantitativního výzkumu sestaven **konstrukt vnitřních organizačních faktorů ovlivňujících bezpečnost informací** v informačních systémech. Konstrukt faktorů zahrnuje:

- Zhodnocení závažnosti a rizik působících na informační aktiva
- Zajištění ochrany kritických charakteristik informací
- Procesy řízení informační bezpečnosti a stanovená bezpečnostní politika
- Priority organizace v oblasti bezpečnosti informací a orientace zájmových skupin
- Modelový přístup organizace k řízení bezpečnosti informací
- Měření bezpečnosti informací
- Zobecněný model chování organizací

Efektivita procesů řízení bezpečnosti informací v organizaci je hodnocena podle schopnosti realizovat cíle informační bezpečnosti aplikací ochranných opatření. Problémem je pak získat důkazy, že efektivita těchto procesů se odráží v bezpečnostních charakteristikách organizace jako produktu těchto procesů a nedochází k redukci ochranných opatření. Faktorem, který tuto efektivitu ovlivňuje je požadavek být optimální z perspektivy ekonomické (z pohledu nákladů na mitigaci rizik a eliminace zranitelností) při zachování souladu s externími regulacemi.

Jako podpůrný nástroj použití v metodice stanovení měr byl použit autorem **rozšířený konceptuální model bezpečnosti informací** dle Hanáček, Staudek (2000, s. 2), Smejkal, Rais (2006, s. 84), Jaquith (2007, s. 232), Kouns, Minoli (2010, s. 159), CCRA (2012, s. 39, s. 40). Rozšíření autorem spočívá konkrétně v doplnění chybějící entity „Zpracovatel“ a doplnění relací propojujících novou entitu s původními entitami. Cílem rozšíření je podchytit faktory v modelu, které nejsou pod kontrolou vlastníka informace. Rozšířený konceptuální bezpečnostní model je v rámci práce experimentálně použit jako základna pro verifikaci stanovených cílů a otázek jako výstupů metody GQM a prostředek pro hodnocení bezpečnostní pozice systému.

GQM přístup je použit jako hlavní nástroj pro identifikaci bezpečnostních měr pro fázi návrhu metodického postupu. Systém měr jako výstup procesu zahrnuje konkrétní formálně popsanou identifikovanou sadu měr pro definovaný cíl při zachování kritérií pro míry. Obecný **konceptuální nástroj GQM** je autorem rozšířen o verifikační fázi stanoveného cíle G, otázky Q a míry M. Verifikační fáze mají zajistit schopnost zachovat vazbu na riziko a současně na sadu bezpečnostních opatření podle zvoleného konstruktu měření, stejně jako kvalitativní parametry míry. V případě nesplnění verifikačního kritéria je zapojena korekční zpětná vazba.

Z literárních zdrojů a provedeného průzkumu byl navržen **zobecněný model chování organizace** v České republice doplněný o aktivity měření úrovně bezpečnosti informací metodou stanovení bezpečnostní pozice konkrétního informačního systému. Účelem modifikace zobecněného modelu je zajistit v procesu pokrytí informační potřeby při provádění auditu úrovně bezpečnosti informací v informačním systému vytvořením konkrétního systému měr, referenčních hodnot a stanovením indikátorů.

Z pohledu **volby** aplikace uvedených **norem pro měření** byl autorem vybrán konstrukt měření dle ISO 27004, který je vhodný z důvodu své mezinárodní platnosti a vychází z normativních a vědeckých postupů. Lze také očekávat jeho další rozvoj.

Syntézou komponent realizačního rámce je autorem definován v práci popsaný **metodický postup pro hodnocení bezpečnostní pozice informačního systému**, který byl ověřen v podmínkách konkrétních organizací v ČR.

Vyhodnocení bezpečnostní pozice systému využívá jeden z možných způsobů agregace výsledků měření a následného modelování podle rozšířeného bezpečnostního modelu. Navržený výpočet bezpečnostní pozice využívá k výpočtu techniku celkového ohodnocení vztahů v rozšířeném konceptuálním bezpečnostním modelu. Předpokládá se, že ohodnocení konkrétní kritické charakteristiky (C, I, A) informace *I* v čase *t* je funkcí účinnosti relací mezi entitami a současně nejslabší množina relací identifikuje nejhorší bezpečnostní pozici informačního systému v čase *t*. Na model a jemu odpovídající instance entit je pohlíženo jako na neorientovaný ohodnocený graf, kde nejslabší posloupnost relací je možno vypočítat funkcí nejmenší kostry grafu (angl. minimal spanning tree). Výpočet je realizován aplikací Kruskalova algoritmu pro hledání nejmenší kostry v grafu. Odhad hodnoty bezpečnostních charakteristik C (Důvěrnost, angl. "confidentiality“), I (Integrita, angl. „integrity“), A (dostupnost, angl. „availability“) je dán souborem ochranných opatření příslušných ke každé hraně v nejmenší kostře a odhadem vlivu tohoto opatření na kritické charakteristiky informací na základě odhadu podle abstraktního stroje Reference Monitoru.

3.4 ZÁVĚRY Z PŘÍPADOVÝCH STUDIÍ

Proces hodnocení bezpečnosti informace navrženým postupem ukázal především silnou stránku grafické prezentace pozice informačního systému pro logickou skupinu „klasifikovaná data“ a „klasifikované emaily“. Pozitivně působí možnost posoudit účinek relace a schopnost reagovat v oblasti lidských zdrojů (zpracovatel) např. školením. Pozitivní vliv na schopnost stanovovat cíle má taktéž použitý rozšířený konceptuální model, který minimálně v oblasti zkoumaných relací transformovaných do charakteristik systému působí jako efektivní nástroj pro stanovení cílů a otázek ve formě návrhu, což následně usnadňuje identifikací míry, což je v souladu s cílem práce.

Problematickou se jeví aplikace samotného **vývoje míry**, kdy nastavení analytického modelu, naplnění definovaných konstruktů může mít stejnou složitost jako vývoj

softwarového produktu a vyžaduje použití softwarových nástrojů. Vyžaduje taktéž jisté matematicko-statistické znalosti a schopnost analýzy.

Aplikovaný postup pracoval s třídami opatření v kontextu části informačního systému (web rozhraní, emailový systém). Výběr tříd opatření, které jsou do hodnocení zahrnuty, je v tomto případě kvalitativní a zavádí do měření subjektivitu. Exaktní přístup stanovující konkrétní sadu opatření a nad ním stanovenou míru je schopen subjektivitu výrazně snížit.

Případové studie indikují ve zkoumaných oblastech očekávanou rozdílnou sílu relací „Vlastník cení informace“ a „Zpracovatel cení informace“. Indikuje jej sice nízká, nicméně stabilně opakovaná míra **email** a **web application leakage**. Rozdíl je v případě lidských zdrojů minimalizovatelný nasazením nástrojů, které vynucují provedení akce s vazbou na klasifikaci informace na straně zpracovatele.

4 ZÁVĚR

4.1 PLNĚNÍ CÍLŮ DISERTAČNÍ PRÁCE

Hlavním výstupem práce bylo stanovení metodiky pro hodnocení bezpečnosti informací v informačním systému. Bezpečnost informací jako produkt vyplývá z bezpečnostní pozice tohoto informačního systému v daném čase. Metodika vychází z identifikovaného modelu chování české organizace rozšířeného o proces měření podle ISO 27004. Rozšíření je voleno tak, aby zajistilo potřebný vliv výstupů měřicího procesu na proces zlepšování bezpečnosti informací v organizaci. Toho je dosaženo poskytnutím informací do zpětné vazby s možností ovlivnění modelu chování organizace směrem k riziku a minimalizace redukce výběrového souboru bezpečnostních opatření způsobené organizačními prioritami.

Pro naplnění hlavního cíle práce byl zvolen top-down přístup k identifikaci měr zaměřených na bezpečnost informací s využitím obecného konceptuálního nástroje Goal-Question-Metric autorem rozšířeného o verifikační fáze pro oblast bezpečnosti informací. Pro usnadnění identifikace otázek a měr byla zavedena metoda verifikace výstupů kroků vývoje měr postavená na rozšířeném bezpečnostním modelu informace a na ochranných opatřeních definovaných vybraným standardem ISO 27004. Verifikace účinně zajišťuje uchování potřebných vazeb na rizika a na opatření.

Pro naplnění dílčích cílů práce byl realizován kvantitativní a kvalitativní výzkum, kdy byla zaměřena oblast zájmu případových studií v českých organizacích, která byla formulována jako „snížení vystavení informací zranitelnostem vycházejících z lidského

faktoru“, „klasifikace informace“ a „odlišné vnímání rizik ve vztahu vlastník-informace a zpracovatel-informace“.

Pro realizaci měření podle navrženého modelu byl navržen a na konkrétní organizaci ověřen postup měření. Pomocí postupu byly iterativním přístupem vyvinuty tři míry, které jsou prezentovány v rámci praktické části práce jako případové studie. Výsledky měření realizovaného v dané organizaci jsou závislé především na použitém měřicím nástroji (specifický experimentální vývoj).

4.2 VĚDECKÝ PŘÍNOS PRÁCE

Vědecký přínos se předpokládá v odhalení závislostí mezi entitami na základě rozšířeného bezpečnostního modelu a na základě měření s využitím vytvořeného modelu chování organizace. Přínosem je i posílení významu abstraktního modelu Reference monitor jako základny pro hodnocení informačních systémů v různých podobách (počítačové systémy, lidé, manuální systémy).

Návazná výzkumná činnost může využít možnost kategorizace organizací podle modelového přístupu a směřovat k vytvoření konkrétního systému měr pro konkrétní přístup. Po kompletním ohodnocení a agregaci výstupů lze provést statickou vizualizaci bezpečnostní pozice informačního systému v organizaci na bázi změřených hodnot. Lze taktéž zapojit další oblast bezpečnosti informačních systémů (výpočetních a komunikačních systémů, spolehlivosti, pravděpodobnosti selhání a vzájemné závislosti) propojením s doménou kontinuity činnosti ICT.

4.3 PRAKTICKÝ PŘÍNOS PRÁCE

Přínos pro praxi autor spatřuje v přehledu a analýze aktuálního stavu měření v oblasti informační bezpečnosti v České republice. Následné navržení postupu může být použito v iniciálních fázích zavádění ISO 27004 do praxe podniků, stejně po rozšíření a adaptaci jako realizaci povinností organizace vyplývajících z legislativních podmínek, konkrétně Zákona o kybernetické bezpečnosti. Metodika v podmínkách českých organizací přináší jednu z možných metod pro zpřístupnění procesů informační bezpečnosti veřejnosti. Poskytnuté výstupy umožňují zvýšení povědomí o oblasti řízení informačních rizik v dalších sektorech ekonomiky. Hlavní přínos je pak podpoření a zvýšení efektivnosti fáze ACT a auditní fáze CHECK v rámci procesů řízení informační bezpečnosti na operativní úrovni a podporu rozhodování za jistoty o organizačních prioritách v oblasti bezpečnosti informací. Díky obecnosti lze metodiku po revizi ověřit v ostatních ekonomických sektorech.

Systematický vývoj měr navrženým postupem potenciálně umožňuje vývoj znovupoužitelného a do dalších organizací přenositelného systému měr, což zakládá možnost realizace moderního přístupu Security as a service. Vstupem do metodiky mohou být již existující kvantitativní metodiky, např. CVSS (Common Vulnerability Scoring System) a jiné.

5 SEZNAM POUŽITÉ LITERATURY

[1] CCRA: *Common Criteria for Information Technology Security Evaluation*. CCRA, 2012.
Dostupný z:
https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf
https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf
https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf
[Citováno: 25.4.2015]

[2] DISMAN, M. *Jak se vyrábí sociologická znalost.* Nakladatelství Karolinum, Praha 2008, ISBN 978-80-246-0139-7.

[3] HANÁČEK, P., STAUDEK, J.: *Bezpečnost informačních systémů: Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. Praha: Úřad pro státní informační systém, 2000. Dostupný z: <http://www.micr.cz/files/479/uvis-Bezpecnost-20000701.pdf>. [Citováno: 15.6.2013]

[4] ISO/IEC 27004:2009 – Information technology – Security techniques – Information security management measurements.

[5] JAQUITH, A.: *Security Metrics. Repacing Fear, Uncertainty, and Doubt.* USA: Pearson Education Inc., 2009. ISBN 978-0-32-134998-9.

[6] KOUNS, J., MINOLI, D.: *Information Technology Risk Management in Enterprise Environments*. USA: Wiley Publishing, 2010. ISBN 978-0-471-76254-6.

[7] STEVENSON, W. J.: *Introduction to Management Science*. Homewood: IRWIN, 1989. ISBN: 0-256-03660-8.

[8] SMEJKAL, V., RAIS, K.: *Řízení rizik ve firmách a jiných organizacích.* 2. vydání. Praha: Grada Publishing, 2006. ISBN 80-247-1667-4.

6 SEZNAM PUBLIKAČNÍ ČINNOSTI

VĚDECKÉ PUBLIKACE BEZ IF - SCOPUS

[1] URBANEC, Jiří a URBANCOVÁ, Hana. THE BENEFITS OF BUSINESS CONTINUITY MANAGEMENT IN CZECH ORGANIZATIONS. Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis, 2015, Vol. 63, Issue 3, pp. 1061-1071. ISSN: 1211-8516.

[2] URBANEC, Jiří a Hana URBANCOVÁ. ADOPTION OF BUSINESS CONTINUITY MANAGEMENT STANDARDS IN CZECH ORGANIZATIONS. Scientia Agriculturae Bohemica, 2014, roč. 45, č. 1, s. 66-74. ISSN: 1211-3174.

[3] URBANCOVÁ, Hana a Jiří URBANEC. INTERNAL FACTORS INFLUENCING THE KNOWLEDGE CONTINUITY ENSURING. Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis, 2012, roč. LX, č. 4, s. 387-396. ISSN: 1211-8516.

ODBORNÉ PUBLIKACE:

[1] URBANCOVÁ, Hana a Jiří URBANEC. THE SURVEY OF TACIT KNOWLEDGE SHARING IN ORGANISATION. Scientific Papers of the University of Pardubice. Series D. Faculty of Economics and Administration, 2011, roč. XVII, č. 19 (1/2011), s. 220-229. ISSN 1211-555X.

[2] URBANCOVÁ, Hana, Martina KÖNIGOVÁ, Jiří URBANEC a Jiří FEJFAR. The influence of new management disciplines on the innovation in organizations. Trendy ekonomiky a managementu, 2012, roč. VI, č. 10, s. 105-115. ISSN 1802-8527.

KONFERENCE - THOMSON REUTERS

[1] URBANEC, J. – ŠVARCOVÁ, I. Information security characteristics in non-trivial models of e-mail communication. In Agrarian Perspectives XX 13.09.2011, CULS Prague. CULS Prague: CULS Prague, 2011. s. 431-437.

[2] URBANCOVÁ, Hana a Jiří URBANEC. LEARNING METHODS IN THE CZECH AND SLOVAK ORGANIZATIONS. In: Efficiency and Responsibility in Education 2013: Proceedings of the 10th International Conference. Czech University of Life Sciences Prague, 2013. s. 618-625. ISBN 978-80-213-2378-0.

OSTATNÍ VÝSLEDKY

[1] URBANEC, J. Přístupy k hodnocení bezpečnosti informací v organizacích v České republice. 2014, Ekonomické listy, 01/2014, str. 42 - 51, ISSN 1801-4166.

[2] URBANEC, J. Hodnocení bezpečnosti informací v informačních systémech a návratnost investic. 2013, Ekonomické listy, 3/2013 k 31. 12. 2013, str. 24 - 40, ISSN 1801-4166.

[3] URBANEC, J. Bezpečnost informací v informačních systémech. In Think Together 2011 07.02.2011, PEF ČZU v Praze. PEF ČZU v Praze: PEF ČZU v Praze, 2011. s. 1-5.

[4] URBANEC, J. Ako zašifrovať zdieľanú skupinovú schránku. 2011, INFOWARE magazín IT profesionálov, ITnews.sk, 10/2011, strana 26, ISSN: 1335-4787-

[5] URBANEC, J. Šifrovaná spolupráce v korporátním prostředí. 2011, Security World, 2/2011, IDG Czech Republic, a. s., strana: 18-19, ISSN 1802-4505.

[6] URBANCOVÁ, Hana a Jiří URBANEC. Knowledge Continuity as a part of Business Continuity Management. In: ICIBM 2013: International Conference on Innovation, Business and Management, World Academy of Science, Engineering and Technology. Venice: World Academy of Science, Engineering and Technology, 2013, Issue 76, s. 255-259. ISSN 2010-376X.

[7] URBANCOVÁ, Hana a Jiří URBANEC. STAFF NUMBER REDUCTION IN THE CZECH AND SLOVAK REPUBLIC. In: Zborník vedeckých príspevkov z medzinárodnej vedeckej konferencie: „Young V4 Science 2013“. Bratislava: Vysoká škola ekonómie a manažmentu verejnej správy v Bratislave, 2013, s. 172-178. ISBN 978-80-89654-01-7.

7 SOUHRN

Informace jsou pro organizace cenným aktivem a zdrojem konkurenční výhody. Proto je nezbytné zajistit a udržovat bezpečnostní charakteristiky procesů a systémů v požadovaných mezích a průběžně kvantitativně hodnotit stav na bázi měření. Problémem při samotném procesu měření se ukazuje výběr vhodných charakteristik a měr procesů a produktů, které by byly předmětem měření. Hlavním cílem disertační práce je návrh metodiky pro hodnocení bezpečnosti informací v informačních systémech organizací měřením a formulovat závěry a doporučení pro její využití v praxi. Situace v Českých organizacích byla zjištěna na základě kvantitativního průzkumu, ve kterém byla data sbírána pomocí dotazníkového šetření (N=785, n=101) a následný kvalitativní výzkum proběhl ve 3 organizacích z finančního sektoru v České republice. Výsledky ukázaly, že v současné době nadpoloviční většina zkoumaných organizací hodnotí informační systémy z pohledu rizika pro hodnotné informace (58,49 %). Organizace, které bezpečnost informací hodnotí, tak provádějí nejčastěji s cílem identifikovat slabiny a vznikající problémy (41,5 %). Pouze 17,6 % organizací hodnotí bezpečnost informací měřením. Práce identifikuje model chování organizace, navržený metodický postup definuje vlastní měřitelné charakteristiky systému identifikované pomocí rozšířeného bezpečnostního modelu, definuje proces vývoje měr v organizaci na bázi nástroje GQM, navrhuje měření kompatibilní s ISO 27004 a prezentuje hodnocení výsledků na základě změřených výstupů. Navržené postupy a konstrukty se zaměřily na zlepšení výzkumem identifikované oblasti „klasifikace informací“ a „rozdílné vnímání hodnoty informace vlastníkem a zpracovatelem“. Ověřeny byly na dvou anonymních organizacích a jsou prezentovány ve formě případové studie. Jedním ze závěrů je, že navržená metodika je použitelná organizacemi se silným technickým a finančním zázemím, kde je možno překonat náročné požadavky procesu vývoje měr a aplikace měření. Metodika samotná má pak své vlastní limity pro aplikaci.

KLÍČOVÁ SLOVA

bezpečnost informací, informační systém, informace, metodika, GQM, výzkum, organizace, model, případová studie

8 SUMMARY

Evaluation of information security in information systems

Information is a valuable asset for organizations and a source of competitive advantage nowadays. Therefore it is necessary to retain information security characteristics of processes and systems in required limits and continuously evaluate the state using measurement. The problem in measurement shows to be in the selection of suitable characteristics and measures of the processes or the products, which are subject to measurement. The main aim of the dissertation thesis is to design methodic for evaluating information security in information systems and formulate conclusions and recommendations for its use in practice. The situation in The Czech Republic was obtained based on a quantitative survey in which data was collected by means of a questionnaire survey (N=785; n=101) and qualitative research was conducted in the 3 organizations from financial sector in the Czech Republic. Results showed that at present an absolute majority of surveyed organizations evaluate information systems from the perspective of risk to valuable information (58.49%). Organizations evaluating information security are most often to identify weaknesses and emerging issues (41.5%). Only a 17.6% of them measure. The designed methodic identifies behavioral model of the organization, defines measurable characteristics of the system and the organization based on extended security model, defines process of development of the measures based on GQM tool, engages measurement process compatible with ISO 27004 and presents evaluation procedure using measured values. The proposed procedures and constructs focused on improvement of field detected by the survey, the “information classification” and “difference between perception of information value between owner and processor”. The procedures were validated on two anonymous organizations and are presented in form of case studies. One of the conclusions is, that proposed methodic is applicable mostly in organizations with strong technical and financial base, where it is possible to overcome requirements of measures development processes and measurement application. Also the methodic of evaluation has its own limits of applicability.

KEY WORDS

information security, information system, information, methodics, GQM, survey, model, organization, case study