Sustainability - Environment - Safety ´2016
Zborník z medzinárodnej vedeckej konferencie, Bratislava, 6. december 2016
Proceedings of the International Scientific Conference, Bratislava, December 6, 2016, Slovak Republic
■ Žilina: Strix. Edícia ESE-30, Prvé vyd., ISBN 978-80-89753-08-6 ■ Rusko, M.- Kollár, V. [Eds.] ■

TYPOVÉ MODELY ZAMERANÉ NA ZVÝŠENIE BEZPEČNOSTI V PODNIKU

Alojz BARTEK - Miroslav RUSKO

TYPE MODELS AIMED AT IMPROVING SAFETY IN AN ENTERPRISE

ABSTRAKT
Bezpečnostná politika podniku je základným a východiskovým dokumentom podniku. Podnik ňou deklaruje svoj záujem na implementáciu bezpečnosti do všetkých sfér činnosti podniku. Predstavuje komplexný pohľad na všetky aspekty bezpečnosti. Bezpečnostná politika definuje chránené záujmy podniku, stanovuje princípy, možné ohrozenia a rizika a systém riadenia bezpečnosti v podniku. Kontinuálne úspešné presadzovanie bezpečnosti v inštitúcií je náročný proces. Jedným z dôležitých faktorov úspešnosti presadzovania bezpečnosti je začlenenie bezpečnostného manažéra v hierarchickej organizačnej štruktúre konkrétnej inštitúcie. K začleneniu patria okrem iného právomoci a väzby na horizontálnej aj vertikálnej úrovni. Príspevok sa zaoberá problematikou organizačného umiestnenia bezpečnostného manažéra v inštitúcií, ktoré je prezentované na ôsmych typových modeloch.

KĽÚČOVÉ SLOVÁ: *bezpečnosť, podnik*

ABSTRACT
Continuous and successful promotion of safety in the enterprise is a demanding process. One of the key factors of promotion of safety is the inclusion of a safety manager in a hierarchical organizational structure of the same institution. The integration include, among others, competence and bonds on both the horizontal and the vertical level. The OHS policy is one of the basic documents of enterprises. Enterprise through it, declaring its intention to implement safety in all spheres of activities of the enterprise. It represents a comprehensive view of all aspects of safety. The OHS policy defines protected interests of enterprise, sets out the principles, possibilities of hazards and risks and safety management system in the enterprise. This contribution deals with the issue of organizational allocation of the safety manager in an institution, which is presented by eight type models.
KEY WORDS: *safety, enterprise*

ÚVOD

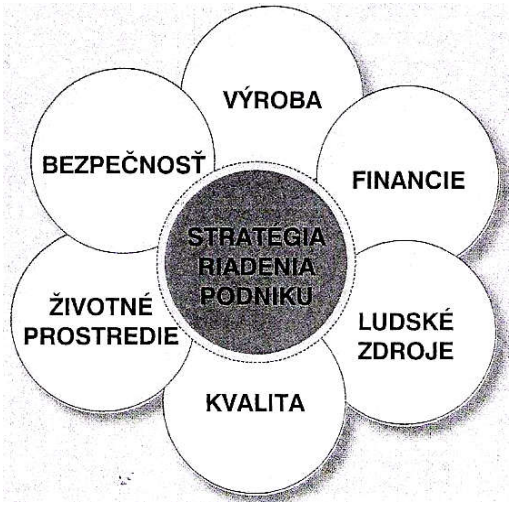
Motívom pre vrcholový manažment podniku na riešenie otázok bezpečnosti podniku okrem reakcie na vytvorené bezpečnostné prostredie je i plnenie platných právnych noriem. Riešenie otázok bezpečnosti vytvára predpoklady na ochranu ľudského činiteľa, majetku a ostatných aktív podniku. To prispieva k vyššej kvalite života v podniku a k vyššej efektivite samotného podniku. Zvyšuje sa pocit bezpečia zamestnancov podniku, vytvára sa optimálna pracovná atmosféra a verejná mienka, čo vedie k vyššej výkonnosti podniku. V konečnom dôsledku to vytvára image, know-how a goodwill podniku na trhu. Bezpečnostná politika podniku je základným a východiskovým dokumentom podniku. Podnik ňou deklaruje svoj záujem na implementáciu bezpečnosti do všetkých sfér činnosti podniku. Predstavuje komplexný pohľad na všetky aspekty bezpečnosti. Bezpečnostná politika definuje chránené záujmy podniku, stanovuje princípy, možné ohrozenia a rizika a systém riadenia bezpečnosti v podniku.
Súčasné analýzy i samotný vývoj bezpečnosti vo svete ukazuje prudký nástup nevojenských ohrození, ktoré sa dotýkajú nielen jednotlivých štátov ale aj regiónov. K takýmto ohrozeniam patria napríklad terorizmus, kriminalita, extrémizmus rôzneho druhu, nekontrolovateľná migrácia, nedostatok strategických surovín, prírodné katastrofy, poškodzovanie životného prostredia a p. Tieto nevojenské ohrozenia spolu s ostatnými faktormi môžu mať vplyv na celkovú bezpečnosť vo svete, v Slovenskej republike, ale tiež na bezpečnosť regiónov a jednotlivých subjektov, ku ktorým je možné zaradiť i podnik, organizácie a inštitúcie (ďalej len podnik). Zaručenie

bezpečnosti podniku má dôležitý spoločenský význam. Predchádza možným negatívnym dopadom, prináša optimalizáciu pracovného procesu a pozitívny ekonomický efekt, vyššiu produktivitu, efektívnosť a kvalitu práce. Lepšia prosperita podniku prispieva k prosperite celej spoločnosti. Zaručenie bezpečnosti podniku má aj dôležitý humánny aspekt, ktorý prezentujú kultúrnu a spoločenskú úroveň a prispieva k celkovej kvalite života spoločnosti.

Motívom pre vrcholový manažment podniku na riešenie otázok bezpečnosti podniku okrem reakcie na vytvorené bezpečnostné prostredie je i plnenie platných právnych noriem.

Je skutočnosťou, že síce existuje rada prístupov, noriem a štandardov, ktorých aplikáciou sa zaisťuje bezpečnosť kritických objektov, ale havárie sa vyskytujú stále, a preto sa hľadajú ďalšie účinnejšie prístupy pre ich konštrukciu a riadenie počas ich prevádzky. [1]

Riešenie otázok bezpečnosti vytvára predpoklady na ochranu ľudského činiteľa, majetku a ostatných aktív podniku. To prispieva k vyššej kvalite života v podniku a k vyššej efektivite samotného podniku. [2]Zvyšuje sa pocit bezpečia zamestnancov podniku, vytvára sa optimálna pracovná atmosféra a verejná mienka, čo vedie k vyššej výkonnosti podniku. V konečnom dôsledku to vytvára image, know-how a goodwill podniku na trhu. V riadení bezpečnosti podniku je potrebné si uvedomovať, že bezpečnosť je nákladná, nikdy nie je stopercentná, nikdy nie je končená a je úlohou predovšetkým najvyššieho manažmentu. Platí zásada, že len približne 15 % problémov je vhodné ponechať na riešenie zamestnancom a ostatok, to je približne 85 % problémov by malo byť zabezpečených systémom riadenia[3]. Na zabezpečenie trvalej prosperity podniku je dôležité, aby bol zavedený riadiaci mechanizmus, ktorý zabezpečí optimálne fungovanie podniku. Súčasťou takéhoto riadenia podniku je i riadenie bezpečnosti (obr. č. 1).



Obr. 1: Stratégia riadenia podniku

Bezpečnosť práce možno charakterizovať ako stav pracoviska, ktorý poskytuje vysokú mieru istoty, že pri dodržaní pravidiel (bezpečnostných požiadaviek, technologických a pracovných postupov a pod.) vzťahujúcich sa na príslušné pracovisko a pracovný proces a bez pôsobenia nepredvídateľných vonkajších vplyvov, bude vylúčená alebo znížená možnosť ohrozenia života a zdravia osôb, poškodenia alebo zničenia ich majetku. [4]

Zavedenie realizácie systémových prvkov bezpečnosti a ochrany zdravia pri práci predpisuje zamestnávateľom zákon č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci. Podnikový dokument „Politika BOZP“ je zameraný na celkovú orientáciu riadenia a vzťahov a podnikovú stratégiu v oblasti ochrany zamestnancov. Zamestnávatelia sú povinní podľa zákona vypracovať takýto dokument obsahujúci základné zámery, ktoré sa majú dosiahnuť v oblasti bezpečnosti a ochrany zdravia pri práci.

Dokument „Politika bezpečnosti a ochrany zdravia pri práci“ predstavuje formálny záväzok organizácie, stanovuje ciele na zlepšenie pracovných podmienok, bezpečnosti a ochrany zdravia pri práci. Podnikový dokument „Politika bezpečnosti a ochrany zdravia pri práci“ je kľúčovým prvkom systému riadenia, pretože

[1] PROCHÁZKOVÁ, D., 2015: Řízení rizik zacílené na bezpečnost kritických onjektů. – In: Rusko, M. [Ed.] 2015: *Integrovaná bezpečnosť 2015*. - Zborník z medzinárodnej vedeckej konferencie konanej 18.semtembra 2015 v Rajeckej doline, 1. vyd., Edícia ESE-22, ISBN 978-80-89753-04-8, 182 s.

2 GAŠPIERIK,L. - REITŠPÍS, J.: Bezpečnosť podniku (organizácie, inštitúcie), ALARM magazín, č.1/2006

3 RAK, R., MATOUŠKOVÁ, I.: Tvůrči bariéry, část II. - Bezpečnost, emoce a interpersonální komunikace, DSM č.4/2004, str. 28-30, Tate International, Praha

[4] BALOG, K. – TUREKOVÁ, I. – TURŇOVÁ, Z., 2006. Inžinierstvo pracovného prostredia. Trnava : MTF STU, skriptá

udáva:

- základnú orientáciu,
- požadovaný smer vývoja bezpečnosti a ochrany zdravia pri práci,
- prezentuje podnikovú filozofiu kultúry práce a celkový prístup vedenia a zamestnancov.

KRITICKÁ INFRAŠTRUKTÚRA PODNIKU

Kritické objekty sú zložité technologické objekty a infraštruktúry, t.j. technologické (resp. presnejšie socio-technologické) systémy, zahŕňajúce budovy a infršstruktúry, sú nutné pre životy ľudí v dnešnom svete. Je ale pravdou, že na jednej strane uľahčujú život ľudí, ale na druhej strane ho ohrozujú, keď dôjde k haváriám. Najväčšie riziká sú spojené s objekami a infraštruktúrami, ktoré sú zložité a obsahujú navyše nebezpečné chemické látky. Predmetné objekty sú viac jako len množinou technických častí zariadení a súčiastok. Sú odrazom organizačnej štruktúry, managementu, prevádzokých predpisov a kultúry konštrukčných organizácií, ktoré ich vytvorily a tiež sú spravidla i odrazom spoločnosti, v ktorej boli vytvorené. [5], [6], [7] Pre bezpečnosť sledovaných objektov je dôležitá interoperabilita za podmienok normálnych, abnormálnych i kritických. [8]

Kritickú infraštruktúru podniku je možné rozdeliť na vonkajšiu a vnútornú. Vonkajšia kritická infraštruktúra bude pôsobiť spravidla nezávisle na podniku. Vnútorná kritická infraštruktúra bude spravidla riadená a ovplyvniteľná podnikom. [9]

Kontinuálne úspešné presadzovanie bezpečnosti v inštitúcií (malej či veľkej firme, v štátnej alebo neziskovej organizácií) nie je spravidla triviálnou záležitosťou. Ak začíname s bezpečnosťou, skôr či neskôr sa celkom zákonite dostaneme k bezpečnostnej politike a bezpečnostnému manažérovi. V okamihu, keď sa túto pozíciu (poprípade celý útvar) rozhodneme vytvoriť, vzniká nerudovská otázka: „Kam s ním?" Jedným z dôležitých faktorov úspešnosti presadzovania bezpečnosti je práve začlenenie bezpečnostného manažéra v hierarchickej organizačnej štruktúre konkrétnej inštitúcie. K začleneniu pochopiteľne patria i právomoci, väzby atď.

Tak, ako sa rozvíjajú inštitúcie vnútorne, a zároveň sa neustále menia i vonkajšie bezpečnostné situácie, dochádza aj k zmenám pohľadu na prácu bezpečnostného manažéra, na úlohy, ktoré sú na nich v stále väčšej miere kladené. V praxi existuje rad modelov, ktoré objektívne závisia na veľkosti inštitúcie, jej predmete podnikania (core business) a (niekedy subjektívne) na vnímaní významu bezpečnosti vrcholovým manažmentom alebo majiteľom (akcionárom) inštitúcie. [10] Pozrime sa preto na základné modely začlenenia bezpečnostného manažéra, na typické „plusy" a „mínusy", ktoré sú pre ne charakteristické.

Okrem typických situácií pri riešení najrôznejších úloh existujú aj typické situácie v medziľudských vzťahoch, ktoré musí bezpečnostný manažér pomerne často riešiť a kladú veľmi náročné požiadavky na jeho osobnosť. [11], [12]

Pre názornosť a zjednodušenie úvah o začlenení bezpečnostného manažéra do inštitúcie, zvažujeme len tri základné úrovne riadenia, pozíciu „šéfa" informatiky[13] (CIO - Chief Information Officer) zaraďujeme zámerne o úroveň (level) nižšie než je vrcholový manažment (čo nemusí byť vždy pravda), nešpecifikujeme rôzne detailné organizačné usporiadania vrcholového manažmentu ani veľkosť a štruktúry zloženia jednotlivých organizačných štruktúr l(C)T apod. Pri začlenení CIO do úrovne 0 sa všetky väzby a úvahy vo vzťahu k bezpečnostnému manažérovi IT (CSOIT - Chief Security IT) presúvajú taktiež o jednu úroveň vyššie analogicky nášmu výkladu. Neuvažujeme ani rozdiel medzi klasickým podnikovým IT a komunikačnými službami (telefóny, faxy, IP telefonovanie atď.) alebo výbornými riadiacimi, technologickými systémami, ktoré sú v rôznych (predovšetkým výborne orientovaných) inštitúciách rôzne organizačne členené, a vtedy aj riadené. Reálnou skutočnosťou je ale fakt, že tieto technológie sa na úrovni HW a SW s prihliadnutím k moderným technologickým trendom neustále zbližujú, a vtedy vyžadujú jednotné bezpečnostné riadenie a kontrolu. U väčších organizácií okrem klasického bezpečnostného manažéra l(C)T naopak predpokladáme existenciu všeobecnej pozície bezpečnostného manažéra (Chief Security Officer - CSO), ktorý je zodpovedný za komplexnú ochranu objektu, zamestnancov aj zákazníka, celkovú informačnú bezpečnosť (napr. Desk Policy atď.).[14]

---

[5] PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace*. Praha: ČVUT 2011, 483p. ISBN 978-80-01-04844-3.

[6] OECD. *Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Communities for developing SPI Programmes related to Chemical Accident Prevention, Preparedness and Response*. OECD, 2002, Paris, 191p.

[7] PROCHÁZKOVÁ, D. *Bezpečnost kritické infrastruktury*. Praha: ČVUT 2012, 318p. ISBN: 978-80-01-05103-0.

[8] PROCHÁZKOVÁ, D. *Základy řízení bezpečnosti kritické infrastruktury*. Praha: ČVUT 2013, 223p. ISBN 978-80-01-05245-7.

9 KELLEOVÁ, E. - BALOG, K. - RUSKO, M.: Rizikové faktory a indikátory vnútorného prostredia budov. In: Monitorovanie a hodnotenie stavu životného prostredia V : Časť B. - Zvolen : Technická univerzita vo Zvolene, 2004. ISBN 80-228-1332-X., s. 81-86

10 RUSKO, M.: Bezpečnostné a environmentálne manažérstvo. - 1.vyd. - Žilina : STRIX, 2006. - 389 s.

11 RUSKO, M. - BALOG, K. - TUREKOVÁ, I.: Vybrané kapitoly z environmentálneho a bezpečnostného manažérstva. 1.vyd., Bratislava : VeV, 2006. 160 s., ISBN 80-969257-5-X.

[12] MATOUŠKOVÁ, I., RAK, R.: The role of the safety manager when enforcing comprehensive information security, 5th International Conference Information Security Summit, 2004, s. 85-98, Tate International, ISBN 80-868113-00-2

13 SPURNÝ, J.: O psychologickém přísutupu k ochrane informací. In. Psychológie v ekonomické praxi, 1999, roč. XXXIV. Č. 3-4. s 199-203

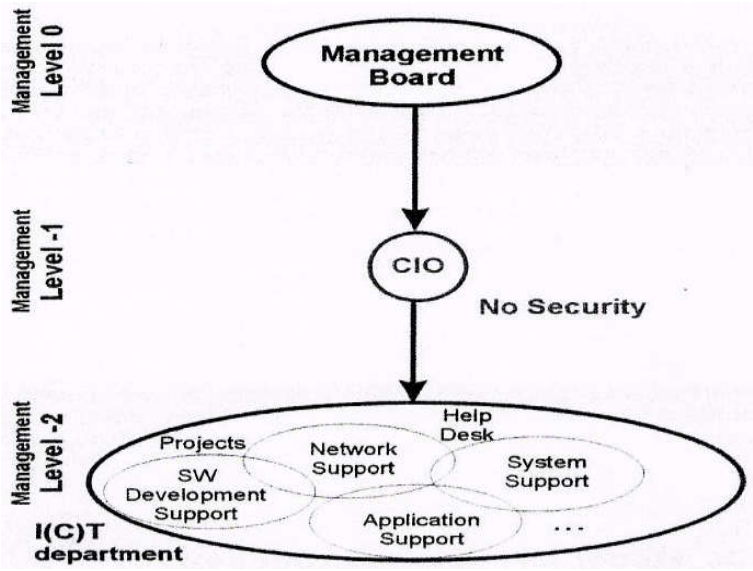
[14] BARTEK, A., 2014: Definovanie kritickej infraštruktúry podniku. – In: Rusko,M. - Balog, K. - Harangozó, J. [Eds.] 2014: Integrovaná bezpečnosť 2014. - Zborník z medzinárodnej vedeckej konferencie konanej 18.-19. decembra 2014 v Bratislave, 1. vydanie, Edícia ESE-17,

TYPOVÉ MODELY ZAMERANÉ NA PROBLEMATIKU BEZPEČNOSTI V PODNIKU

Základné organizačné umiestnenie bezpečnostného manažéra v inštitúcií rozoberieme na nasledujúcich osem typových modeloch. Musíme si ale uvedomiť, že neexistuje žiadny univerzálny, jediný a správny model, ktorý by si mohli len jednoducho vybrať a formálne aplikovať na riešenie bezpečnosti v tej či inej inštitúcií. Pretože každá inštitúcia sa líši iným predmetom základných činností, kultúrou zamestnancov a manažmentu atd., existujú len určité „best practices", z ktorých si môžeme brať inšpiratívny príklad, ale musíme si ich vždy s citom „dopiľovať" pre svoje vlastné potreby. A u bezpečnosti to platí obzvlášť.

MODEL IGNORATÍVNEJ BEZPEČNOSTI

V inštitúcií nie sú žiadne pozície, ktoré by sa zaoberali bezpečnosťou informačných systémov[15]. O bezpečnosť sa nikto nezaujíma alebo ju (zatiaľ) vôbec nerealizuje. Aplikácie sú malé, nemajú žiadny rozhodujúci vplyv na základné procesy v inštitúcií alebo je bezpečnosť manažmentom alebo zástupcami IT ignorovaná.
V niektorých prípadoch sa môže tvrdiť, že pretože sa doteraz nič nestalo, nemá zmysel do bezpečnosti vôbec investovať. Táto situácia môže byť typická i pre nové malé firmy v stave zrodu i krátko po ňom. [16] Všetko úsilie je zamerané na realizáciu základného podnikateľského plánu, získanie prvých zákazníkov, a na bezpečnosť nie je v tejto chvíli vôbec čas a priestor. Pre takéto firmy sú často typické dodávky malých aplikácií na kľúč, vytvorených lacnými pracovnými silami študentov alebo rodinných príslušníkov či príbuzných. „IT" býva často i jedno možné, v niektorých prípadoch na čiastočný pracovný úväzok.
Tento stav trvá spravidla do prvého bezpečnostného incidentu alebo ďalšieho kvalitatívneho rastu inštitúcie.



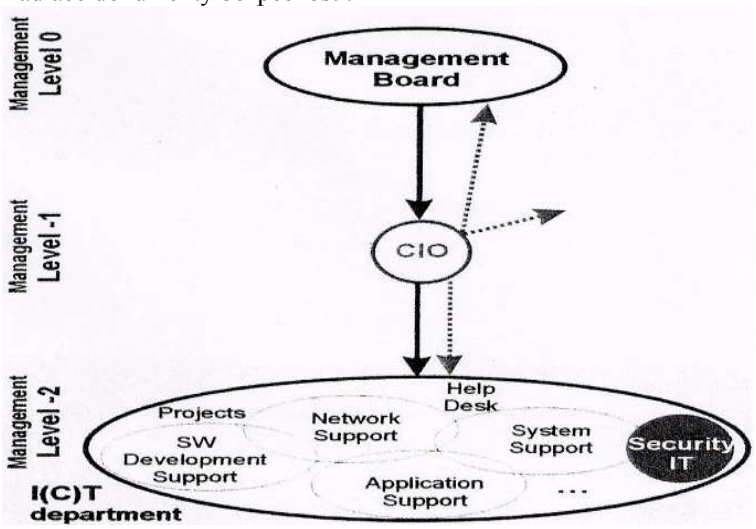
Obr. 2 Model ignoratívnej bezpečnosti.

MODEL MINIMÁLNEJ TECHNOLOGICKEJ BEZPEČNOSTI

Organizačná zložka IT technológií inštitúcie má teraz oproti predchádzajúcemu modelu viac zamestnancov na trvalý pracovný úväzok a dobre si uvedomuje nutnosť určitej úrovne bezpečnosti. IT bezpečnosť je ale väčšinou vnímaná ako len technologická záležitosť riadená len vo vnútri útvaru IT s minimálnou komunikáciou a súčinnosťou s ostatnými organizačnými prvkami inštitúcie, so zamestnancami. Inštitúcia neprevádza pravdepodobne finančné audity u veľkej audítorskej štvorky. Títo audítori pri vyhodnocovaní spôsobov spracovania finančných

ISBN 978-80-89753-00-0. 205 s.
15 RAK, R. - MATOUŠKOVÁ, I.: Tvúrči bariéry, část II. - Bezpečnost, emoce a interpersonální komunikace, DSM č.4/2004, str. 28-30, Tate International, Praha
[16] NEČAS, S., PORADA, V, SEILER, M.: Bezpečnosť banky ve vztahu k bezpečnostnímu managementu. Sborník II, vedecké konfe-rence s mezinárodní účastí, Košice: ŽU - FŠI - pracovisko Košice, 2002, s. 250 - 262. ISBN 80-88922-78-X, EAN 9788088922780.

operácií vyhodnocujú aj bezpečnosť technológie ich spracovania a bývajú pomerne často silným prvopočiatočným impulzom pre prechod na vyšší model bezpečnosti. Chýba na viac obvykle bezpečnostná politika a z nej vyplývajúce záväzné riadiace dokumenty bezpečnosti.



Obr. 3 Model minimálnej technologickej bezpečnosti.
Poznámka:Tenké (prerušované) čiary formálne zobrazujú komunikáciu s okolím.

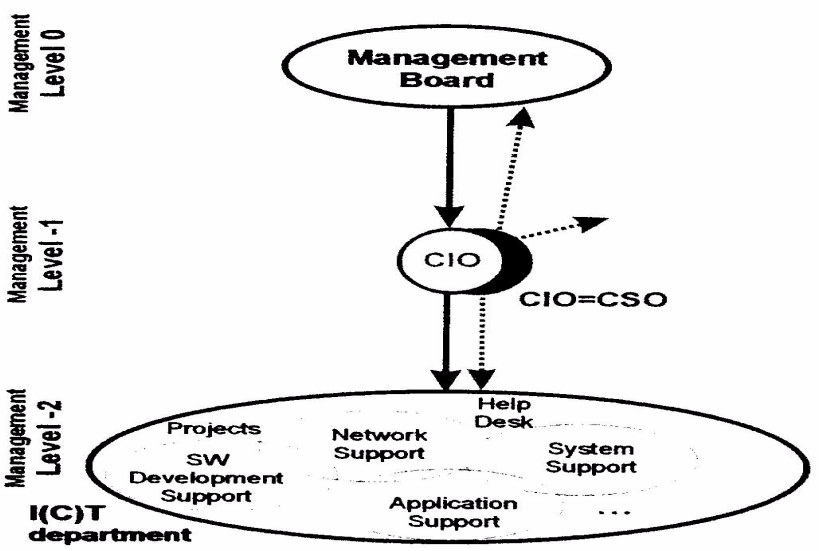
Riadením bezpečnosti nie je v IT obvykle poverená žiadna osoba na plný pracovný úväzok. Jedná sa skôr o administrátorov siete, databáz, aplikácií, ktorí na seba preberajú určitú zodpovednosť za bezpečnosť, ktorá nie je ale jasne koncepčne vymedzená. Realizácia bezpečnosti je uplatňovaná skôr intuitívne v internej súčinnosti IT špecialistov na neformálnej úrovni, v ktorej sa odrážajú bezpečnostné vedomosti a povedomie niektorých z neformálnych „guru" osobností IT CIO praktikuje minimálnu komunikáciu na tému IT bezpečnosti s okolím na rovnakej alebo vyššej organizačnej úrovni. Pri takto poňatej bezpečnosti obvykle absentuje aj rozpočtová kapitola na bezpečnosť v budgetu IT[17]. Aj tak technologická úroveň bezpečnosti môže byť pomerne vysoká, a na viac schopná agilných zmien proti bezpečnostným incidentom vychádzajúcich zo slabín používaných technológií. Inštitúcia je ale veľmi slabo zabezpečená proti zlyhaniu alebo pokušeniu vlastných zamestnancov, sociotechnické útoky proti takto chápanej bezpečnosti sú vysoko účinné a inštitúcia je z tohto pohľadu obnažená. Absolútne chýba intenzívna personálna práca so zamestnancami v oblasti bezpečnosti rovnako ako všeobecne poňatá informačná bezpečnosť. V inštitúciách, vychádzajúcich z tohto modelu nie je často realizovaná ani rozsiahlejšia objektová ochrana fyzického charakteru.

MODEL FORMÁLNEJ BEZPEČNOSTI

Tento model sa zásadne nelíši od predchádzajúceho. Inštitúcia môže aj nemusí byť väčšia; to isté platí o veľkosti IT a rozsahu spravovaných aplikácií. Zásadný rozdiel spočíva však v tom, že v inštitúcií došlo už k uvedomeniu si nutnosti poveriť niekoho bezpečnosťou IT Vedúci (CIO) organizačného celku informačných technológií sa stáva (dobrovoľne alebo naopak a zásadne proti svojej vôli) oficiálne osobou zodpovednou za bezpečnosť IT „Z ekonomických dôvodov" nevzniká ale ešte plnohodnotný bezpečnostný manažér IT, ktorý by sa zaoberal zverenou problematikou „full time". Tento model môže byť modifikovaný pomocou predchádzajúceho modelu, t.j. pre praktickú realizáciu bezpečnosti IT sú využívaní a šéfom IT koordinovaní alebo poverovaní úlohami jednotliví špecialisti alebo vedúci organizačných celkov IT. Neexistuje ale zatiaľ žiadna stála skupina špecialistov, ktorí by sa zaoberali len a len bezpečnosťou. So stanovením zodpovednosti za bezpečnosť s pomerne veľkou pravdepodobnosťou vznikajú aj predpoklady a účinné nástroje pre možnosť plniť zverené úlohy. Pri takto poňatej bezpečnosti môžeme teda očakávať už samostatnú rozpočtovú kapitolu v IT rozpočte (investičnom aj nákladovom). Inak ostávajú všetky ďalšie obmedzenia a nedostatky opísané v modeli minimálnej technologickej bezpečnosti. Kľúčom k presadzovaniu bezpečnosti je v tomto prípade osobnosť CIO, ktorá môže zohrať ako veľmi pozitívnu, tak aj zásadne negatívnu rolu. Môžeme tu nájsť naozaj osvieteného IT manažéra, ktorý úplne chápe a presadzuje bezpečnosť IT, rovnako tak odporca, ktorý v bezpečnosti vidí nechcene dieťa a

17 PORADA, V. - NEČAS, S.: Bankovní bezpečnost jako součást bezpečnostní politiky organizace Bezpečnostní teórie a praxe, zvl. číslo. Praha: PA ČR, 2001 s. 437 - 448

snaží sa len formálne naplniť zodpovednosť smerom k nadriadeným a svojmu okoliu. Pravdou zostáva, že čistých manažérov IT majúcich plné pochopenie pre bezpečnosť, v ktorej nevidí len najrôznejšie prevádzkové obmedzenie, je stále ako šafranu. Ďalšou skutočnosťou ale je aj fakt, že IT bezpečnosť (ak vezmeme do úvahy problematiku bezpečnosti sietí, databáz, aplikácií, autentizácie, šifrovania atd.) je sama veľmi odborná a rozsiahla, je len minimálna pravdepodobnosť, že CIO pri svojich základných povinnostiach je schopný vedomostne obsiahnuť i túto oblasť a dokázať zabezpečiť jej praktické naplnenie, kontrolu a ďalší koncepčný rozvoj.



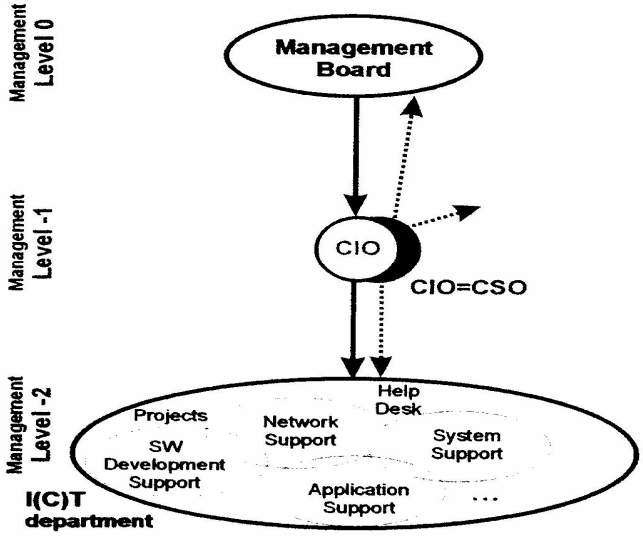
Obr. 4 Model formálnej bezpečnosti.

Len tvorba aktualizácia príslušnej bezpečnostnej dokumentácie, najrôznejšie komplexné bezpečnostné analýzy a osveta zamestnancov inštitúcie pohltí nesmierne množstvo nie len času a energie, ale aj elánu. Základným nedostatkom takto chápaného modelu bezpečnosti vždy zostáva stret záujmov: ten, kto zodpovedá za rozvoj IT a prevádzku aplikácií, nemôže nikdy plniť aj rolu gestora za bezpečnosť, pretože sú tu potrebné základné zodpovednostné a kontrolne mechanizmy. CIO nemá nikdy dostatok priestoru ani času pre bezpečnostnú osvetu a výchovu zamestnancov inštitúcie.

MODEL ODTRHNUTEJ BEZPEČNOSTI

V histórii vnímania bezpečnosti v inštitúcií (vo firme) dochádza k zásadnému zlomu. Vedenie inštitúcie alebo vlastníci dospievajú k rozhodnutiu, že je nutné vytvoriť samostatnú tabuľkovú pozíciu bezpečnostného manažéra IT Pozícia je organizačne začlenená podlá učebnicových doporučení mimo útvar IT. Bezpečnostný manažér IT je na rovnakej alebo na vyššej organizačnej úrovni než osoba zodpovedná za IT. Úlohy riadenia IT a bezpečnosti sú teoreticky správne medzi sebou oddelené, aby nevznikal stred záujmov. V organizácií existuje bezpečnostná politika, na bezpečnosť sú vyčleňované finančné prostriedky. Na pozíciu bezpečnostného manažéra má zásadný vplyv hneď niekoľko faktorov. K najväčším patrí skutočnosť, či má pod sebou nejaký vlastný útvar alebo nie. Len veľmi silné inštitúcie majú vlastné bezpečnostné útvary IT. V ekonomickej sfére to sú finančné a prepravné inštitúcie, veľké výrobné podniky apod. U malých a stredných podnikoch býva bezpečnostný manažér IT celkom osamotený. Často je jeho funkcia kumulovaná so zodpovednosťou za fyzickú aj personálu bezpečnosť a situácia je analogická kumulácia pozície CIO a CSO. V skutočnosti pri profesionálnom prístupe k riešeniu bezpečnosti sa ale jedná o dve celkom odlišné profesie, ktoré majú len určité spoločné rozhranie (informačná bezpečnosť, ktorá má časť technologickú a časť ľudskú, týkajúcu sa všetkých zamestnancov). Dnes na úrovni stredných podnikov sa nedá bezpečnostnú problematiku obsiahnuť jediným manažérom, a to ako rozsahom činností, tak aj profesionálnou pripravenosťou.
Osobnosť bezpečnostného manažéra je vo veľmi nepríjemnej situácií, vo „dvojakom ohni". V tomto modeli sú na bezpečnostného manažéra kladené najväčšie psychologické a odborné nároky. Z hľadiska požiadaviek na vysoké životné skúsenosti, autoritu, schopnosť vytvárať alebo aktualizovať metodiky (predpisy, smernice atď.) je pozícia obsadzovaná osobami minimálne stredného veku. Technológie sa vyvíjajú neustále mimoriadne búrlivo. Aj keď v okamihu nástupu do pozície môže byť bezpečnostný manažér na vysokej odbornej úrovni, časom je celkom odtrhnutý od IT sveta. Tento fakt je ovplyvnený medziľudskými vzťahmi medzi zamestnancami IT a bezpečnostným manažérom. Pokiaľ CSO presadzuje bezpečnosť necitlivo, direktívne voči

útvaru IT, informatici časom celkom odrežú (vyštiepu) bezpečnostného manažéra od reálnych technológií v inštitúcií. Bezpečnostný manažér zostáva teoretikom. Musí sa prípadne neustále školiť v IT technológiách u externých subjektov a jeho personálne náklady narastajú.



Obr. 5 Model odtrhnutej bezpečnosti

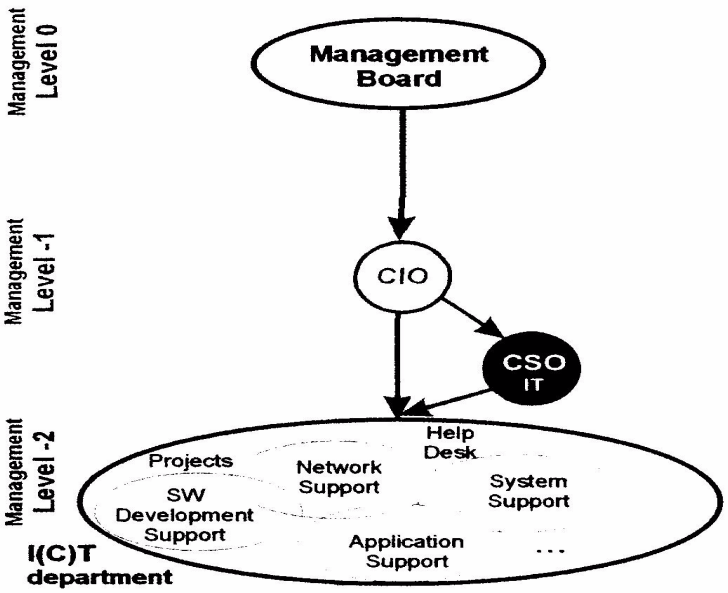
Veľmi môže záležať aj na vzťahoch CIO a CSO. Pre jednanie kontrolných orgánov (napr. audítorov) býva niekedy typické, že nectia organizačnú hierarchiu a svojim spôsobom pri získavaní informácií obchádzajú určité riadiace úrovne (v našom prípade CIO) a vzniká dvojkoľajnosť informačných tokov, v horšom prípade aj riadenia či vedenia. Medziľudské vzťahy sa potom silne narúšajú. Pokiaľ ale naopak je postupované celkom formálne, môžu i tu nastať patové situácie. Stačí, aby CIO odborne spochybnil požiadavky alebo návrhy CSO, ktoré môžu prameniť nie len z nedostatkov technologických znalostí CSO, ale predovšetkým z nedostatočných interných informácií z útvarov IT, ktoré nie sú týmto útvarom zámerne poskytované, a máme na svete ťažko riešiteľnú situáciu.
Problematickým sa môže stať aj zostavovanie a hospodárenie s IT rozpočtom. Ťažko sa dá predpokladať, že ojedinelé začlenený bezpečnostný manažér IT má svoj rozpočet, ktorý by bol schopný nejako zásadne ovplyvňovať úroveň bezpečnosti vo firme. Pokiaľ nie sú vyčlenené finančné prostriedky na bezpečnosť, a bezpečnosť je len riadená direktívne na základe administratívnych aktov, výsledná bezpečnosť býva formálna a nepružná. Ak škrípu vzťahy medzi bezpečnostným manažérom a útvarom IT, a to i v prípade, že existujú finančné prostriedky na bezpečnosť, nemusia byť rozumne vynakladané.[18]
Naopak pozitívom tohto modelu je blízkosť CSO manažmentu spoločnosti a teda väčšia úspešnosť pri presadzovaní bezpečnostnej politiky. Pozícia bezpečnostného manažéra bola zriadená vedením spoločnosti, s určitým cieľom a je nelogické zároveň tým popierať základné úlohy bezpečnostného manažéra. Bezpečnosť býva v inštitúcií metodicky, teoreticky dobre rozpracovaná. Sú rovnako predpoklady, že bezpečnostná osveta a školenie používateľov a následné bezpečnostné povedomie je na vysokej úrovni. Formálna bezpečnosť prevažuje nad bezpečnosťou technologickou, výsledkom môže byť bezpečnosť, ktorá nie je dostatočne agilná, t.j. schopná adekvátnymi spôsobmi reagovať na reálne bezpečnostné hrozby. Bezpečnostný manažér inštitúcie sa môže stať iba jej „bezpečnostným maskotom".

MODEL UTOPENEJ BEZPEČNOSTI

Tento model je v praxi IT najbežnejší. Podľa štatistík z Prieskumu stavu informačnej bezpečnosti v ČR z roku 2003 v celých 78% inštitúcií je informačná bezpečnosť riadená útvarom IT. V strede veľkých firiem sa bezpečnosťou zaoberajú 1 až 3 špecialisti, väčšinou je to ale len bezpečnostný manažér IT, ktorý vykonáva svoju profesiu na plný pracovný úväzok. CSO je vzatý pod krídla CIO. Medzi oboma manažérmi sa predpokladajú podobné názory na bezpečnosť. Tento model odstraňuje nedostatky modelu predchádzajúceho, ale prináša zase iné nevýhody. Bezpečnostný manažér je veľmi blízko informačným technológiám a ľuďom z IT, úzko spolupracuje s vedúcimi jednotlivých IT tímov. Pokiaľ sú dobre nastavené medziľudské väzby, technologická

[18] MATOUŠKOVÁ, I.: Psychológie a taktika presadzovaní investic do informační bezpečnosti ve firemní sféře, Security Mgazín, č. 4/2004, str. 48-49

bezpečnosť býva na veľmi vysokej úrovni. Nie sú spravidla problémy ani s rozpočtom a financovaním IT projektov, ktorých je bezpečnosť dnes integrálnou súčasťou. Technologická bezpečnosť je veľmi agilná a schopná v čas reagovať na technologicky vedené útoky.

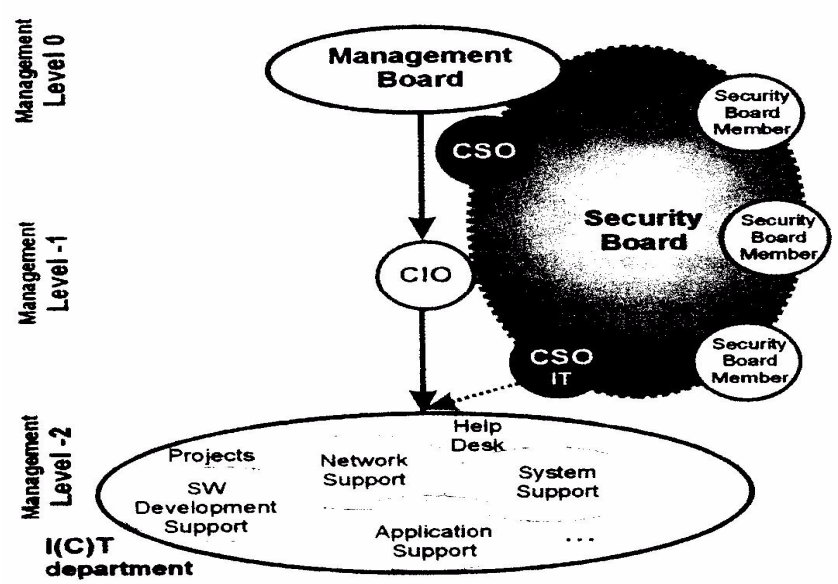


Obr. 6 Model utopenej bezpečnosti

Externí audítori často tomuto modelu vytýkajú závislosť CSO na CIO, prípadný stret záujmov. Pokiaľ totiž neexistuje základná názorová zhoda medzi CSO a CIO, manažér IT teoreticky môže brzdiť rozvoj bezpečnosti. Je nutné si však uvedomiť protiargument, že pokiaľ CIO neprejde bezpečnosťou, takýto model nemôže v praxi vôbec vzniknúť (pokiaľ však nie je vychytralou taktikou CIO).
Dôležitým aspektom je i začiatok budovania bezpečnosti v inštitúcií. Pokiaľ útvar IT existuje, a neexistuje bezpečnosť ako taká, model utopenej (pod vedúcim IT) bezpečnosti dáva podstatne menšie šance na budovanie bezpečnosti než model odtrhnutej bezpečnosti. Bezpečnostný manažér IT v modeli odtrhnutej bezpečnosti ostáva „kolom v plote" a bez priamej podpory IT sú jeho šance na naštartovanie bezpečnosti v inštitúcií veľmi malé.
Model utopenej bezpečnosti môže vzniknúť prirodzenou evolúciou z modelu minimálnej technologickej bezpečnosti. Neformálny zamestnanec IT, guru, ktorý pri výkone iných IT profesií koordinoval bezpečnosť vo vnútri útvaru IT, sa môže stať za predpokladu splnenia manažérskych požiadaviek dobrým bezpečnostným manažérom.
Nedostatkom tohto modelu je často zlá komunikácia a personálna práca smerom do vnútra útvaru IT, pretože CIO je zbytočným medzičlánkom. Tak isto sa môžu ťažko presadzovať bezpečnostné opatrenia (v tomto modeli obvykle vychádzajúcom zo spôsobov myslenia technologicky orientovaných špecialistov IT). Problematická býva aj integrácia IT bezpečnosti so všeobecnou bezpečnostnou politikou inštitúcie. Komunikácia medzi bezpečnostným manažérom a manažmentom v tomto modeli býva zložitejšia než v ostatných modeloch a ticho sa predpokladá pomoc CIO pre výmenu názorov v oboch smeroch.
Ak má táto inštitúcia len jediného bezpečnostného manažéra IT (a žiadnych ďalších špecialistov), potom z praktického pohľadu býva model utopenej bezpečnosti úspešnejší než model odtrhnutej bezpečnosti, čo je v rozpore s teoretickým prístupom uprednostňujúcim nezávislosť realizácie bezpečnosti inštitúcie.

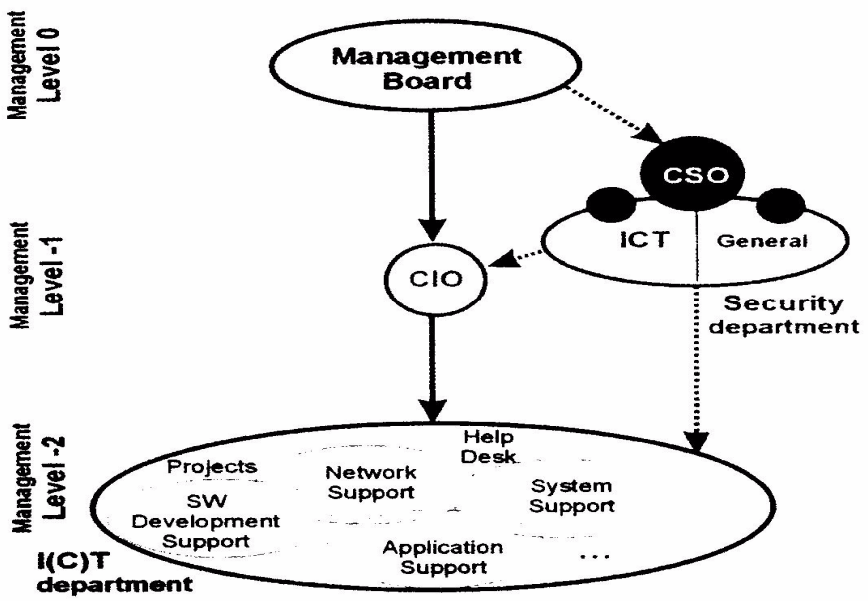
MODEL AGILNEJ BEZPEČNOSTI

Model agilnej bezpečnosti vychádza z pozitív predchádzajúcich modelov a odstraňuje negatíva typické pre jednotlivé modely. Model je charakteristický pre stredne veľké inštitúcie, ktoré nemajú žiadne vlastné rozsiahle bezpečnostné útvary s početným personálnym obsadením zaisťujúcim bezpečnosť. V inštitúcií okrem osoby zodpovednej za bezpečnosť informačných technológií môže existovať na viac ďalší manažér zodpovedajúci za fyzickú, personálnu, ekologickú bezpečnosť apod.



Obr. 7 Model agilnej bezpečnosti

V inštitúcií je vytvorená tzv. bezpečnostná rada, ktorá má podobu virtuálnej štruktúry naprieč vrcholovým a stredným manažmentom, menovaná vedením inštitúcie (napr. generálnym riaditeľom). Členovia bezpečnostnej rady sú nominovaní podľa konkrétnych potrieb inštitúcie. Bezpečnostná rada môže mať stálych aj externých členov, prizvaných špecialistov (z inštitúcie alebo mimo nej). Členmi môžu byť jednotliví odborní riaditelia, personalisti, technici atď., a pochopiteľne obaja bezpečnostní manažéri.



Obr. 8 Model rozsiahlej inštitucionálnej bezpečnosti.

Pri takto pojatom modeli odpadajú komunikačné problémy medzi manažmentom a odbornými špecialistami, koordinácia medzi jednotlivými organizačnými zložkami alebo jednotlivcami, ktorí majú určitý vzťah k bezpečnosti býva na vysokej úrovni. Nebýva ani problém pri presadzovaní bezpečnostných projektov a ich financovaní. Bezpečnostná rada je kolektívnym orgánom, ktorý ma trojitú základnú funkciu: funkciu „legislatívnu" t.j. tvorba a schvaľovanie bezpečnostnej politiky a s ňou súvisiacich dokumentov. Potom je tu funkcia kontrolná, ktorá zisťuje stav implementovaných opatrení a ich fungovanie, a potom funkcia riadiaca v dobe ohrozenia inštitúcie, mimoriadnych bezpečnostných incidentov apod. Bezpečnosť býva vysoko agilná. Spokojní bývajú audítori, pretože CSO nie je riadený len CIO. CSO využíva všetky výhody vyplývajúce z blízkosti k útvaru IT v inštitúcií. Na vysokej úrovni býva i komunikácia sa zamestnancami, ich zoznamovanie s

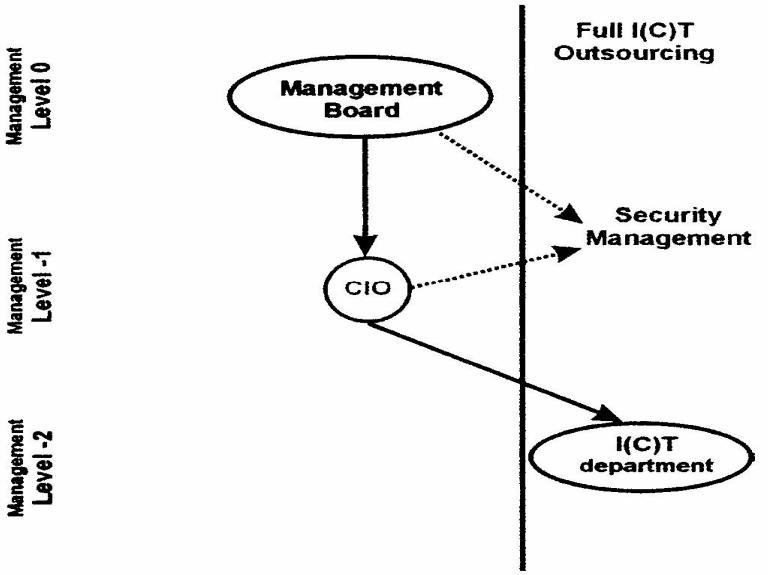
neodkladnými opatreniami a odporúčaniami. V bezpečnostnej rade je dobre mať predstaviteľa zložky inštitúcie. Jednak je dobre otvorená cesta ku školeniam, jednak sa dobre realizuje i personálna bezpečnosť.

MODEL ROZSIAHLEJ INŠTITUCIONÁLNEJ BEZPEČNOSTI

Uvedený model je typický pre veľké inštitúcie (ako napr. banky, veľké priemyselné podniky, silové rezorty štátu) apod. V týchto inštitúciách už existujú profesionálne bezpečnostné útvary čítajúce viac zamestnancov, ktorí sa ďalej profesijné špecializujú. Rieši sa ako technologická bezpečnosť, tak aj bezpečnosť informačná a všeobecná (fyzická ochrana objektov atď.).
Tento model má rad variant. Môže sa jednať o dva samostatné organizačné celky, ktoré majú svojich manažérov pre technologickú ICT bezpečnosť a všeobecnú bezpečnosť, alebo o jediný organizačný útvar vo vedení s jedným bezpečnostným manažérom, ktorý sa ďalej vnútorne člení podľa jednotlivých oblastí a špecializácií.
Bezpečnosť je teraz úplne profesijné formalizovaná a inštitúcia buduje bezpečnosť podľa definovaných (medzi)národných štandardov a odporúčaní, ktoré boli pre inštitúciu vybrané ako záväzné. Akékoľvek IT projekty sú dôsledne riadené i z pohľadu bezpečnosti. Štátna alebo polo štátna organizácia sa obvykle na viac riadi záväznou národnou (medzinárodnou) legislatívou na ochranu utajovaných skutočností, ktorá kladie na inštitúciu ďalšie požiadavky, a zároveň aj obmedzenia.
Pravidla financovania bezpečnostných projektov sú jasne determinované, problémy bývajú obvykle v nedostatku finančných zdrojov na rozsiahle projekty. V týchto inštitúciách býva na výške nie len technologická bezpečnosť, ale aj bezpečnosť personálna. Zamestnanci sú pravidelne školení a pripravení čeliť i sociotechnickým útokom vedeným z vonka. Bezpečnosť vo veľkých inštitúciách so silno formalizovanými metódami a postupmi nemusí byť však dostatočne agilná na niektoré typy hrozieb. Hlavným problémom býva ako veľkosť organizácie, tak niekedy aj skostnatený alebo vžitý spôsob myslenia vo „vyjazdených koľajach", alebo dokonca alibizmus. V myslení ľudí, zamestnancov, môže prevládať názor: „Máme rozsiahle bezpečnostné štruktúry, tak nech sa starajú!"

MODEL OUTSORCOVANEJ BEZPEČNOSTI

O outsourcingu sa pomerne často hovorí ako o ceste rozvoja a prevádzkovaní ICT v inštitúcií. Mnoho inštitúcií využíva rad služieb svojich dodávateľov pre riešenie určitých okruhov činností (teda sa dá hovoriť o čiastočnom outsourtingu). Plného outsourtingu ICT využíva zatiaľ minimum inštitúcií. Sú preto malé praktické skúsenosti z pohľadu bezpečnostného. Je zrejmé, že v inštitúcií musí vždy ale zostať osoba zodpovedná za koordinovanie informačných potrieb spoločnosti a riadenie dodávateľskej organizácie.
Komplexné riešenie bezpečnosti sa rozpadá do dvoch okruhov. Všeobecná bezpečnostná politika zostáva vždy na strane inštitúcie. Tá definuje svoje základné požiadavky v súlade so strategickými plánmi svojho rozvoja. Technologická bezpečnosť vychádza z bezpečnostnej politiky a je na strane dodávateľa. [19]



Obr. 9 Model outsorcovanej bezpečnosti.

[19] NEČAS, S., PORADA, V.: Teoretická východiska a principy bankovní bezpečnosti. Brno: VŠKE, 2002, 12s.

Outsourcovať sa dá všeličo. Jediné čo nie je možné outsourcovať, je vlastné strategické rozhodovanie a zodpovednosť za neho. Za bezpečnosť organizácie musí preto celkovo zodpovedať vždy jej zamestnanec, bezpečnostný manažér, ktorý musí zaistiť definovanú úroveň dodávateľských služieb a koordinovať ich so všetkými procesmi v inštitúcií. Z tohto pohľadu sú na bezpečnostného manažéra kladené extrémne nároky na jeho odbornosť a manažérske vedomosti a schopností a psychickú odolnosť. Vo svojej pozícií zostáva rovnako osamotený ako v modeli odtrhnutej bezpečnosti, je bez možnosti blízkeho prístupu k technológiám, ktoré sú dodávateľsky prevádzkované. Základnou otázkou vždy ale je, či sa dá akúkoľvek bezpečnosť zaistiť externými službami alebo je to ekonomicky alebo politicky prijateľné[20].
Faktom ostáva skutočnosť, že outsourcing postupne zvyšuje nároky na presné zadanie požadovaných služieb a obslužných procesov a je komunikačné náročný vo vzťahu k dodávateľovi. V prípade bezpečnosti sa môže jednať o kritický moment pri rozhodovaní, pretože zložitá a zdĺhavá komunikácia v prípade ohrozenia je sama o sebe nebezpečná. Musia byť aj vyjasnené otázky, akým spôsobom kontrolovať úroveň bezpečnosti, keď v zadávateľskej organizácií je minimum (alebo vôbec nie sú) špecialisti na ICT alebo bezpečnosť. Objektívnou cestou v tomto prípade je nezávislá kontrola, audit inej inštitúcie, špecializujúci sa na danú problematiku. To predstavuje ďalšie náklady, s ktorými je nutné počítať.

ZÁVER

Pre moderné inštitúcie je typická efektívna plochá štruktúra organizovaná maticovým spôsobom. Pri tomto usporiadaní je kladený primárny dôraz na procesy. Takto je vnímaná aj bezpečnosť. Bezpečnostný manažér potom zodpovedá za definované procesy v inštitúcií a ich bezpečnosť. Zaručenie bezpečnosti podniku má dôležitý spoločenský význam. Predchádza možným negatívnym dopadom, prináša optimalizáciu pracovného procesu a pozitívny ekonomický efekt, vyššiu produktivitu, efektívnosť a kvalitu práce. Lepšia prosperita podniku prispieva k prosperite celej spoločnosti. Zaručenie bezpečnosti podniku má aj dôležitý humánny aspekt, ktorý prezentujú kultúrnu a spoločenskú úroveň a prispieva k celkovej kvalite života spoločnosti. Žiadny z modelov prezentovaných v príspevku nemusí byť univerzálne použiteľný pre akúkoľvek inštitúciu. Záleží na mnohých špecifických podmienkach, ktoré determinujú praktický výsledok. Konečný, pre nás vhodný model, môže byť aj kombináciou typických modelov, ktoré sme práve predstavili. Pri výklade sme sa zamerali predovšetkým na inštitúcie, ktorých organizačná štruktúra je silno hierarchická a prevažuje vertikálne členenie. Pre tieto inštitúcie je typická štábna kultúra a bezpečnosť býva organizovaná vojenským spôsobom.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

BALOG, K. – TUREKOVÁ, I. – TURŇOVÁ, Z., 2006. Inžinierstvo pracovného prostredia. Trnava : MTF STU, skriptá

BARTEK, A., 2014: Definovanie kritickej infraštruktúry podniku. – In: Rusko,M. - Balog, K. - Harangozó, J. [Eds.] 2014: Integrovaná bezpečnosť 2014. - Zborník z medzinárodnej vedeckej konferencie konanej 18.-19. decembra 2014 v Bratislave, 1. vydanie, Edícia ESE-17, ISBN 978-80-89753-00-0. 205 s.

GAŠPIERIK,L. - REITŠPÍS, J.: Bezpečnosť podniku (organizácie, inštitúcie), ALARM magazín, č.1/2006

KELLEOVÁ, E. - BALOG, K. - RUSKO, M.: Rizikové faktory a indikátory vnútorného prostredia budov. In: Monitorovanie a hodnotenie stavu životného prostredia V : Časť B. - Zvolen : Technická univerzita vo Zvolene, 2004. ISBN 80-228-1332-X., s. 81-86

MATOUŠKOVÁ, I., RAK, R.: The role of the safety manager when enforcing comprehensive information security, 5th International Conference Information Security Summit, 2004, s. 85-98, Tate International, ISBN 80-868113-00-2

MATOUŠKOVÁ, I.: Psychológie a taktika presadzovaní investic do informační bezpečnosti ve firemní sfére, Security Mgazín, č. 4/2004, str. 48-49

NEČAS, S., PORADA, V, SEILER, M.: Bezpečnosť banky ve vztahu k bezpečnostnímu managementu. Sborník II, vedecké konfe-rence s mezinárodní účastí, Košice: ŽU - FŠI - pracovisko Košice, 2002, s. 250 - 262. ISBN 80-88922-78-X, EAN 9788088922780.

NEČAS, S., PORADA, V.: Teoretická východiska a principy bankovní bezpečnosti. Brno: VŠKE, 2002, 12s.

OECD. *Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Communities for developing SPI Programmes related to Chemical Accident Prevention, Preparedness and Response*. OECD, 2002, Paris, 191p.

PORADA, V. - NEČAS, S.: Bankovní bezpečnost jako součást bezpečnostní politiky organizace Bezpečnostní teórie a praxe, zvl. číslo. Praha: PA ČR, 2001 s. 437 - 448

20 RAK, R.: Homo sapiens jako nejsilnejší i nejslabší článek v získavaní a ochrane informací, Data Security Management, 2004, č. 4, str. 10-13

PROCHÁZKOVÁ, D. *Bezpečnost kritické infrastruktury*. Praha: ČVUT 2012, 318p. ISBN: 978-80-01-05103-0.
PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace*. Praha: ČVUT 2011, 483p. ISBN 978-80-01-04844-3.
PROCHÁZKOVÁ, D. *Základy řízení bezpečnosti kritické infrastruktury*. Praha: ČVUT 2013, 223p. ISBN 978-80-01-05245-7.
PROCHÁZKOVÁ, D., 2015: Řízení rizik zacílené na bezpečnost kritických onjektů. – In: Rusko, M. [Ed.] 2015: *Integrovaná bezpečnosť 2015*. - Zborník z medzinárodnej vedeckej konferencie konanej 18.semtembra 2015 v Rajeckej doline, 1. vyd., Edícia ESE-22, ISBN 978-80-89753-04-8, 182 s.
RAK, R. - MATOUŠKOVÁ, I.: Tvúrči bariéry, část II. - Bezpečnost, emoce a interpersonální komunikace, DSM č.4/2004, str. 28-30, Tate International, Praha
RAK, R., MATOUŠKOVÁ, I.: Tvúrči bariéry, část II. - Bezpečnost, emoce a interpersonální komunikace, DSM č.4/2004, str. 28-30, Tate International, Praha
RAK, R.: Homo sapiens jako nejsilnejší i nejslabší článek v získavaní a ochrane informací, Data Security Management, 2004, č. 4, str. 10-13
RUSKO, M. - BALOG, K. - TUREKOVÁ, I.: Vybrané kapitoly z environmentálneho a bezpečnostného manažérstva. 1.vyd., Bratislava : VeV, 2006. 160 s., ISBN 80-969257-5-X.
RUSKO, M.: Bezpečnostné a environmentálne manažérstvo. - 1.vyd. - Žilina : STRIX, 2006. - 389 s.
SPURNÝ, J.: O psychologickém přísutupu k ochrane informací. In. Psychológie v ekonomické praxi, 1999, roč. XXXIV. Č. 3-4. s 199-203

ADRESY AUTOROV

Ing. Alojz BARTEK, PhD.
Wüstenrot stavebná sporiteľňa, a. s., Grösslingova 77, 824 68 Bratislava, Slovenská republika
e-mail: alojz.bartek@gmail.com

Doc. RNDr. Miroslav RUSKO, PhD.
Slovenská technická univerzita v Bratislave, Materiálovotechnologická fakulta Trnava, Ústav integrovanej bezpečnosti, Botanická 49, 917 01 Trnava, Slovenská republika
e-mail: mirorusko@centrum.sk

RECENZIA TEXTOV V ZBORNÍKU
Recenzované dvomi recenzentmi, členmi vedeckej rady konferencie. Za textovú a jazykovú úpravu príspevku zodpovedajú autori.

REVIEW TEXT IN THE CONFERENCE PROCEEDINGS
Contributions published in proceedings were reviewed by two members of scientific committee of the conference. For text editing and linguistic contribution corresponding authors.