Význam pozice a umístění bezpečnostního manažera v instituci

Viktor Porada – Policejní akademie ČR, Praha
Roman Rak – Policejní akademie ČR, Praha
Ingrid Matoušková – Bankovní institut Vysoká škola a. s., Praha

---

Kontinuální úspěšné prosazování bezpečnosti v instituci (malé či velké firmě, ve státní nebo neziskové organizaci) není zpravidla nikterak triviální záležitostí. Začínáme-li s bezpečností, dříve či později se zcela zákonitě dostaneme k bezpečnostní politice a bezpečnostnímu manažerovi. V okamžiku, kdy se tuto pozici (popř. celý útvar) rozhodneme vytvořit, vzniká nerudovská otázka „Kam s ním?“. Jedním z důležitých faktorů úspěšnosti prosazovaní bezpečnosti je právě začlenění bezpečnostního manažera v hierarchické organizační struktuře konkrétní instituce. K začlenění pochopitelně patří i pravomoci, vazby atd.

Následující text pomůže managementu různých institucí nalézt orientaci v dané problematice. Není ani tak podstatné, zda se teprve rozhodujeme bezpečnost vytvářet, nebo již se touto problematikou dále zabýváme. Tak jak se rozvíjí instituce vnitřně a zároveň se neustále mění i vnější bezpečnostní situace, dochází i ke změnám pohledu na práci bezpečnostního manažera, na úkoly, které jsou na něj ve stále větší míře nově kladeny.

V praxi existuje řada modelů, které objektivně závisejí na velikosti instituce, jejím předmětu podnikání (core business) a (někdy subjektivně) na vnímání významu bezpečnosti vrcholovým managementem nebo majiteli (akcionáři) instituce. Podívejme se proto na základní modely začlenění bezpečnostního manažera, na typické „plusy“ a „mínusy“, které jsou pro ně charakteristické. Kromě typických situací při řešení nejrůznějších úkolů existují i typické situace v mezilidských vztazích, které musí bezpečnostní manažer poměrně často řešit a které kladou velmi náročné požadavky na jeho osobnost.

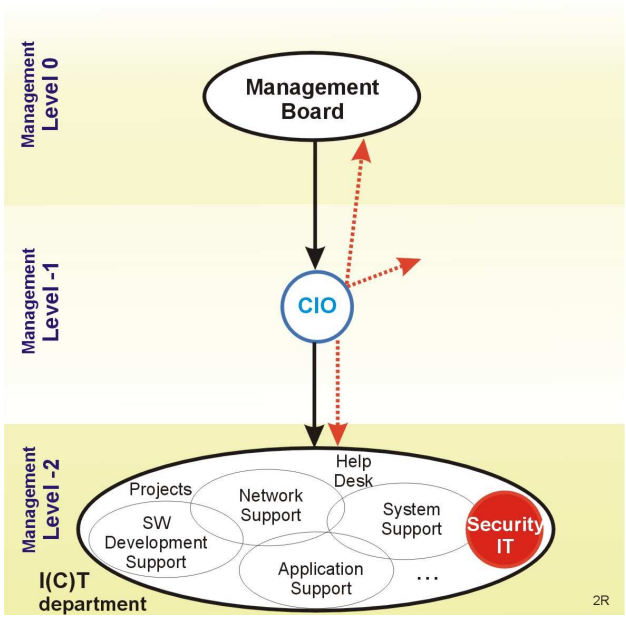
Pro názornost a zjednodušení úvah o začlenění bezpečnostního manažera do instituce uvažujeme jen tři základní úrovně řízení, pozici „šéfa“ informatiky (CIO – Chief Information Officer) zařazujeme záměrně o úroveň (level) níže než je vrcholový management (což nemusí být vždy pravda), nespecifikujeme různé detailní organizační uspořádání vrcholového managementu ani velikosti a struktury složení jednotlivých organizačních struktur I(C)T apod. Při začlenění CIO do úrovně 0 se všechny vazby a úvahy ve vztahu k bezpečnostním manažerovi IT (CSO_{IT} – Chief Security IT) přesouvají taktéž o jednu úroveň výše analogicky našemu výkladu. Neuvažujeme ani rozdíl mezi klasickým, podnikovým IT a komunikačními službami (telefony, faxy, IP telefonie atd.) nebo výrobně-řídícími, technologickými systémy, které jsou v různých (především výrobně orientovaných) institucích různě organizačně členěny a tedy i řízeny. Reálnou skutečností je ale fakt, že tyto technologie se na úrovni HW a SW s přihlédnutím k moderním technologickým trendům neustále sbližují a tedy vyžadují jednotné bezpečnostní řízení a kontrolu. U větších organizací kromě klasického bezpečnostního manažera I(C)T naopak předpokládáme existenci obecné pozice bezpečnostního manažera (Chief Security Officer - CSO), který je zodpovědný za komplexní ochranu objektu, zaměstnanců i zákazníků, celkovou informační bezpečnost (např. Desk Policy atd.).

Základní organizační umístění bezpečnostního manažera v instituci rozebereme na následujících osmi typových modelech. Musíme si ale uvědomit, že neexistuje žádný universální, jediný a správný model, který bychom si mohli jen jednoduše vybrat a formálně aplikovat na řešení bezpečnosti v té či jiné instituci. Protože každá instituce se liší jiným předmětem základních činností, kulturou zaměstnanců a managementu atd., existují jen určité

„best practises“, ze kterých si můžeme brát inspirativní příklad, ale musíme si je vždy s citem „dopilovat“ pro své vlastní potřeby. A u bezpečnosti to platí obzvlášť.

Model ignorativní bezpečnosti

V instituci nejsou žádné pozice, které by se zabývaly bezpečností informačních systémů. O bezpečnost se nikdo nezajímá nebo ji (zatím) vůbec nerealizuje. Aplikace jsou malé, nemají žádný rozhodující vliv na základní procesy v instituci nebo je bezpečnost managementem nebo zástupci IT ignorována. V některých případech se může tvrdit, že protože se dosud nic nestalo, nemá smysl do bezpečnosti vůbec investovat. Tato situace může být typická i pro nové malé firmy ve stavu zrodu, krátce po něm. Veškeré úsilí je zaměřeno na realizaci základního podnikatelského plánu, získání prvních zákazníků a na bezpečnost není v této chvíli vůbec čas a prostor. Pro takovéto firmy jsou často typické dodávky malých aplikací na klíč, vytvořených levnými pracovními silami studentů nebo rodinných příslušníků či příbuzných. „IT“ bývá často i jednomužné, v některých případech na částečný pracovní úvazek.

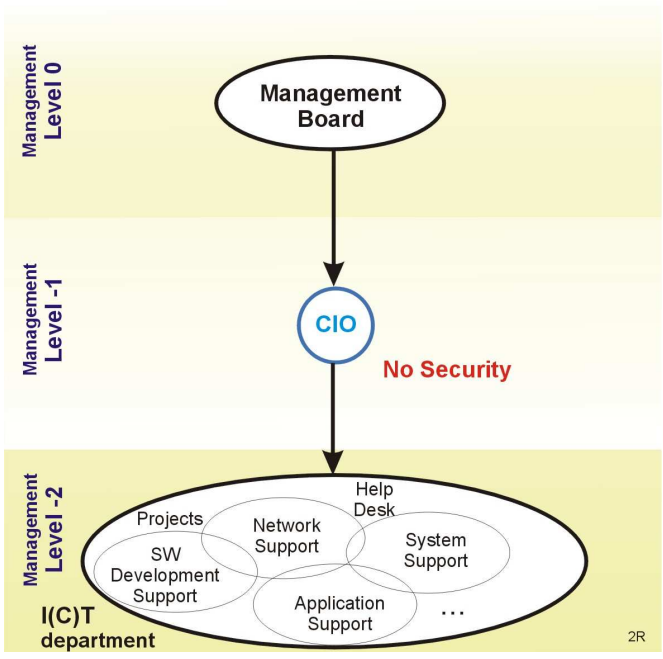


Obr. 2 Model minimální technologické bezpečnosti. Přerušované čáry formálně zobrazují komunikaci s okolím.

Tento stav trvá zpravidla do prvního bezpečnostního incidentu nebo dalšího kvalitativního růstu instituce.

Model minimální technologické bezpečnosti

Organizační složka IT technologií instituce má již oproti předchozímu modelu více zaměstnanců na trvalý pracovní úvazek a dobře si uvědomuje nutnost určité úrovně bezpečnosti. IT bezpečnost je ale většinou vnímána jako pouze technologická záležitost, řízená pouze uvnitř útvaru IT s minimální komunikací a součinností s ostatními organizačními prvky instituce, se zaměstnanci. Instituce neprovádí pravděpodobně finanční audity u velké auditorské čtyřky. Tito auditoři při vyhodnocování způsobů zpracování finančních operací vyhodnocují i bezpečnost technologie jejich zpracování a bývají poměrně často silným prvopočátečním impulsem pro přechod na vyšší model bezpečnosti. Chybí navíc obvykle bezpečnostní politika a z ní vyplývající závazné řídící dokumenty bezpečnosti. Řízením

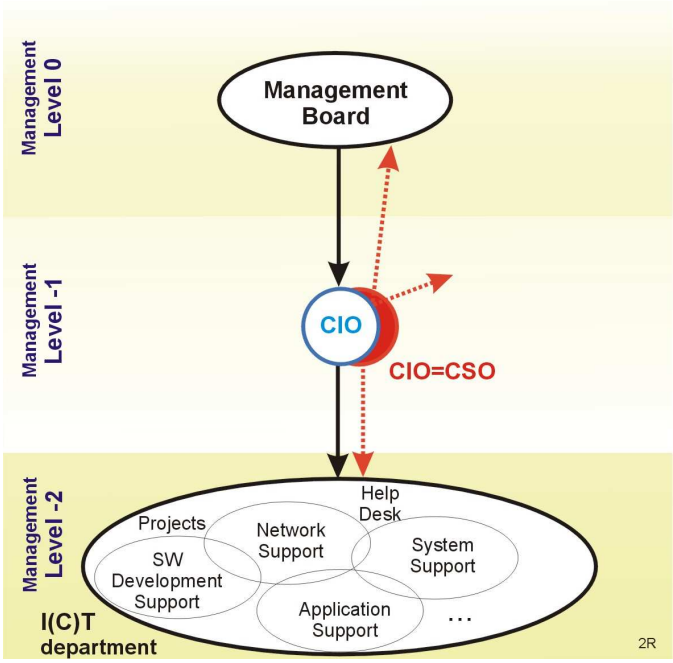


Obr. 1 Model ignorativní bezpečnosti.

bezpečnosti není v IT obvykle pověřena žádná osoba na plný pracovní úvazek. Jedná se spíše o administrátory sítě, databází, aplikací, kteří na sebe přebírají určitou odpovědnost za bezpečnost, která není ale jasně koncepčně vymezena. Realizace bezpečnosti je uplatňována spíše intuitivně v interní součinnosti IT specialistů na neformální úrovni ve které se odrážejí bezpečnostní znalosti a povědomí některé z neformálních „guru“ osobností IT. CIO praktikuje minimální komunikaci na téma IT bezpečnosti s okolím na stejné nebo vyšší organizační úrovni. Při takto pojaté bezpečnosti obvykle absentuje i rozpočtová kapitola na bezpečnost v budgetu IT. I přesto však technologická úroveň bezpečnosti může být poměrně vysoká a navíc schopná agilních změn proti bezpečnostním incidentům vycházejícím ze slabin používaných technologií. Instituce je ale velice slabě zabezpečena proti selhání nebo pokušení vlastních zaměstnanců, sociotechnické útoky proti takto chápané bezpečnosti jsou vysoce účinné a instituce je z tohoto pohledu obnažená. Absolutně chybí intenzivní personální práce se zaměstnanci v oblasti bezpečnosti stejně jako obecně pojatá informační bezpečnost. V institucích, vycházejících z tohoto modelu není často realizována ani rozsáhlejší objektová ochrana fyzického charakteru.

Model formální bezpečnosti

Tento model se zásadně neliší od předchozího. Instituce může i nemusí být větší; totéž platí i o velikosti IT a rozsahu spravovaných aplikací. Zásadní rozdíl spočívá však v tom, že v instituci došlo již k uvědomění si faktu pověřit někoho bezpečností IT. Vedoucí (CIO) organizačního celku informačních technologií se stává (dobrovolně nebo naopak a zásadně proti své vůli) oficiálně osobou zodpovědnou za bezpečnost IT. „Z ekonomických důvodů“ nevzniká ale ještě plnohodnotný bezpečnostní manažer IT, který by se zabýval svěřenou problematikou „full time“. Tento model může být modifikován pomocí předchozího modelu, tj. pro praktickou realizaci bezpečnosti IT jsou využíváni, a šéfem IT koordinováni nebo úkolováni jednotliví specialisté nebo vedoucí organizačních celků IT. Neexistuje ale zatím žádná stálá skupina specialistů, kteří by se zabývali jen a jen bezpečností. S ustanovením zodpovědnosti za bezpečnost s poměrně velkou pravděpodobností vznikají i předpoklady a účinné nástroje pro možnost plnit svěřené úkoly. Při takto pojaté bezpečnosti lze tedy očekávat už samostatnou rozpočtovou kapitolu v IT rozpočtu (investičním i nákladovém). Jinak zůstávají všechna další omezení a nedostatky, popsaná v modelu minimální technologické bezpečnosti. Klíčem k prosazování bezpečnosti je v tomto případě osobnost CIO, která může sehrát jak velice pozitivní nebo i zásadně negativní roli. Můžeme zde nalézt opravdu osvíceného IT manažera, který plně chápe a prosazuje bezpečnost IT, stejně tak odpůrce, který v bezpečnosti vidí nechtěné dítě a snaží se jen formálně naplnit zodpovědnost směrem k nadřízeným a svému okolí. Pravdou zůstává, že čistých manažérů IT majících plné pochopení pro bezpečnost, ve které nevidí jen nejrůznější provozní omezení, je pořád jak šafránu. Další

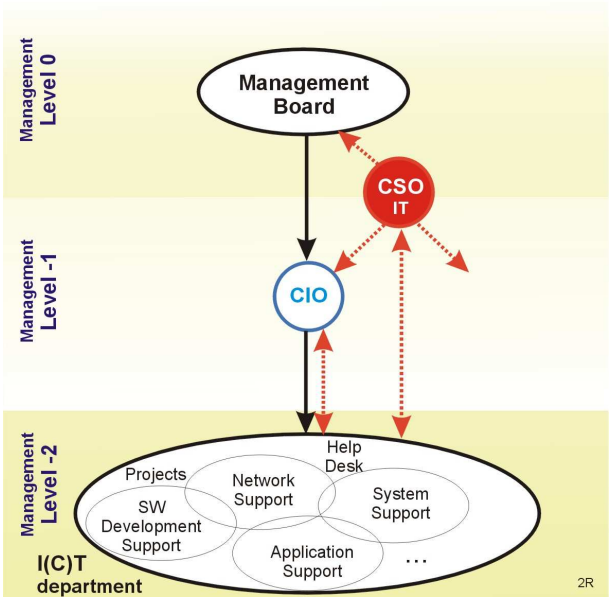


Obr. 3 Model formální bezpečnosti.

skutečností ale je i fakt, že IT bezpečnost (vezmeme-li v úvahu problematiku bezpečnosti sítí, databází, aplikací, autentizace, šifrování atd.) je velice sama nesmírně odborná a rozsáhlá, je jen minimální pravděpodobnost, že CIO při svých základních povinnostech je schopen vědomostně obsáhnout i tuto oblast a dokázat zabezpečit její praktické naplnění, kontrolu a další koncepční rozvoj. Jen tvorba a aktualizace příslušné bezpečnostní dokumentace, nejrůznější komplexní bezpečnostní analýzy, osvěta zaměstnanců instituce pohltí nesmírné množství nejen času a energie, ale i elánu. Základním nedostatkem takto chápaného modelu bezpečnosti vždy zůstává střet zájmů: ten, kdo zodpovídá za rozvoj IT a provoz aplikací nemůže nikdy plnit i roli gestora za bezpečnost, protože jsou zde potřeny základní zodpovědnostní a kontrolní mechanismy. CIO nemá navíc nikdy dostatek prostoru ani času pro bezpečnostní osvětu a výchovu zaměstnanců instituce.

Model odtržené bezpečnosti

V historii vnímání bezpečnosti v instituci (ve firmě) dochází k zásadnímu zlomu. Vedení instituce nebo vlastníci dospívají k rozhodnutí, že je nezbytně nutné vytvořit samostatnou tabulkovou pozici bezpečnostního manažera IT. Pozice je organizačně začleněna podle učebnicových doporučení mimo útvar IT. Bezpečnostní manažer IT je na stejné nebo vyšší organizační úrovni než osoba zodpovědná za IT. Role vedení IT a bezpečnosti jsou teoreticky správně mezi sebou odděleny aby nevznikal střet zájmů. V organizaci existuje bezpečnostní politika, na bezpečnost jsou vyčleňovány finanční prostředky. Na pozici bezpečnostního manažera má zásadní vliv hned několik faktorů. K největším patří skutečnost, zda má pod sebou nějaký vlastní útvar či nikoliv. Jen velmi silné instituce mají vlastní bezpečnostní útvary IT. V ekonomické sféře to jsou zejména finanční, přepravní instituce, velké výrobní podniky apod. U malých a středních podniků bývá bezpečnostní manažer IT zcela osamocen. Často je jeho funkce kumulována se zodpovědností za fyzickou, personální aj. bezpečnost a situace je analogická kumulace pozice CIO s CSO. Ve skutečnosti, při profesionálním přístupu k řešení bezpečnosti, se ale jedná o dvě zcela odlišné profese, které mají jen určité společné rozhraní (informační bezpečnost, která má část technologickou a část lidskou, týkající se všech zaměstnanců). Již na úrovni středních podniků nelze bezpečnostní problematiku obsáhnout jediným manažerem a to jak rozsahem činností, tak i profesionální připraveností.



Obr. 4 Model odtržené bezpečnosti.

Osobnost bezpečnostního manažera je ve velice nepříjemné situaci, ve „dvojím ohni“. V tomto modelu jsou na bezpečnostního manažera kladeny největší psychologické a odborné nároky. Z hlediska požadavku na vysoké životní zkušenosti, autoritu, schopnost vytvářet nebo aktualizovat metodiky (předpisy, směrnice atd.) je pozice obsazována osobami minimálně středního věku. Technologie se vyvíjejí ale neustále mimořádně bouřlivě. I když v okamžiku nástupu do pozice může být bezpečnostní manažer na vysoké odborné úrovni, časem je zcela odtržen od IT světa. Tento fakt je navíc ovlivněn mezilidskými vztahy mezi zaměstnanci IT a bezpečnostním manažerem. Pokud CSO prosazuje bezpečnost necitlivě, direktivně vůči

útvaru IT, informatici časem zcela odříznou („vyštípou“) bezpečnostního manažera od reálných technologií v instituci. Bezpečnostní manažer zůstává teoretikem. Musí se případně neustále školit v IT technologií u externích subjektů a jeho personální náklady narůstají.

Velice může záležet i na vztazích CIO a CSO. Pro jednání kontrolních orgánů (např. auditů) bývá někdy typické, že nectí organizační hierarchii a svým způsobem při získávání informací obcházejí určité řídící úrovně (v našem případě CIO) a vzniká dvojkolejnost informačních toků, v horším případě i řízení či vedení. Mezilidské vztahy se pak silně narušují. Pokud ale naopak je postupováno zcela formálně, mohou i zde nastat patové situace. Stačí, aby CIO odborně zpochybnil požadavky nebo návrhy CSO, které mohou pramenit nejen z nedostatků technologických znalostí CSO, ale především z nedostatečných interních informací z útvarů IT, které nejsou tímto útvarem záměrně poskytovány a máme na světě těžko řešitelnou situaci.

Problematickým se může stát i sestavování a hospodaření s IT rozpočtem. Stěží lze předpokládat, že ojediněle začleněný bezpečnostní manažer IT má svůj rozpočet, který by byl schopen nějak zásadně ovlivňovat úroveň bezpečnosti ve firmě. Pokud nejsou vyčleněny finanční prostředky na bezpečnost, a bezpečnost je jen řízena direktivně na základě administrativních aktů, výsledná bezpečnost bývá formální a nepružná. Skřípou-li vztahy mezi bezpečnostním manažerem a útvarem IT, a to i v případě, že existují finanční prostředky na bezpečnost, nemusí být rozumně vynakládány.

Naopak pozitivem tohoto modelu je blízkost CSO managementu společnosti a tedy větší úspěšnost při prosazování bezpečnostní politiky. Pozice bezpečnostního manažera byla zřízena vedením společnosti s určitým cílem a je nelogické zároveň s tím popírat základní úkoly bezpečnostního manažera.

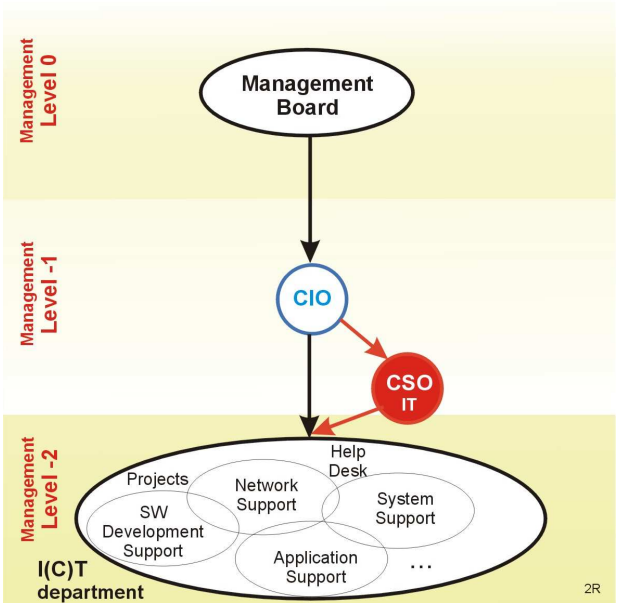
Bezpečnost bývá v instituci metodicky, teoreticky dobře rozpracována. Jsou rovněž předpoklady, že bezpečnostní osvěta a školení uživatelů a následné bezpečnostní povědomí je na vysoké úrovni. Formální bezpečnost převažuje nad bezpečností technologickou, výsledkem může být bezpečnost, která není dostatečně agilní, tj. schopna adekvátními způsoby reagovat na reálné bezpečnostní hrozby. Bezpečnostní manažer instituce se může stát pouze jejím „bezpečnostním maskotem“.

Model utopené bezpečnosti

Tento model je v praxi českých útvarů IT nejběžnější. Podle statistik z Průzkumu stavu informační bezpečnosti v ČR z roku 2003 celých 78% institucí je informační bezpečnost řízena útvarem IT. Ve středně velkých firmách se bezpečností zabývají 1 až 3 specialisté, většinou to je ale pouze bezpečnostní manažér IT, který vykonává svou profesi na plný pracovní úvazek. CSO je vzat pod křídla CIO. Mezi oběma manažery se předpokládají podobné názory na bezpečnost. Tento model odstraňuje nedostatky modelu předchozího, ale přináší zase jiné nevýhody. Bezpečnostní manažer je velice blízko informačním technologiím a lidem z IT, úzce spolupracuje s vedoucími jednotlivých IT týmů. Pokud jsou dobře nastaveny mezilidské vazby, technologická bezpečnost bývá na velmi vysoké úrovni. Nejsou zpravidla problémy ani s rozpočtem a financováním IT projektů, u kterých je bezpečnost dnes integrální součástí. Technologická bezpečnost je velice agilní a schopná včas reagovat na technologicky vedené útoky.

Externí auditoři často tomuto modulu vytýkají závislost CSO na CIO, případný střet zájmů. Pokud totiž neexistuje základní názorová shoda mezi CSO a CIO, manager IT teoreticky může brzdit rozvoj bezpečnosti. Nutno si však uvědomit proti argument, že pokud CIO nepřeje bezpečnosti, takovýto model nemůže v praxi vůbec vzniknout (pokud ovšem není vychytralou taktikou CIO).

Důležitým aspektem je i začátek budování bezpečnosti v instituci. Pokud útvar IT existuje a neexistuje bezpečnost jako taková, model utopené (pod vedoucím IT) bezpečnosti dává podstatně vyšší šance na budování bezpečnosti než model odtržené bezpečnosti. Bezpečnostní manažer IT v modelu odtržené bezpečnosti zůstává „kůlem v plotě“ a bez přímé podpory IT jsou jeho šance na nastartování bezpečnosti v instituci velmi malé.



Obr. 5 Model utopené bezpečnosti.

Model utopené bezpečnosti může vzniknout přirozenou evolucí z modelu minimální technologické bezpečnosti. Neformální zaměstnanec IT, guru, který při výkonu jiných IT profesí koordinoval bezpečnost uvnitř útvaru IT se může stát za předpokladu splnění manažerských požadavků dobrým bezpečnostním manažerem.

Nedostatkem tohoto modelu je často špatná komunikace a personální práce směrem vně útvaru IT, protože CIO je zbytečným mezičlánkem. Zrovna tak se můžou těžkou prosazovat bezpečnostní opatření (v tomto modelu obvykle vycházející ze způsobů myšlení technologicky orientovaných specialistů IT). Problematická bývá i integrace IT bezpečnosti s obecnou bezpečnostní politikou instituce. Komunikace mezi bezpečnostním manažerem a managementem v tomto modelu bývá složitější než v ostatních modelech a tiše se předpokládá pomoc CIO pro výměnu názorů v obou směrech.

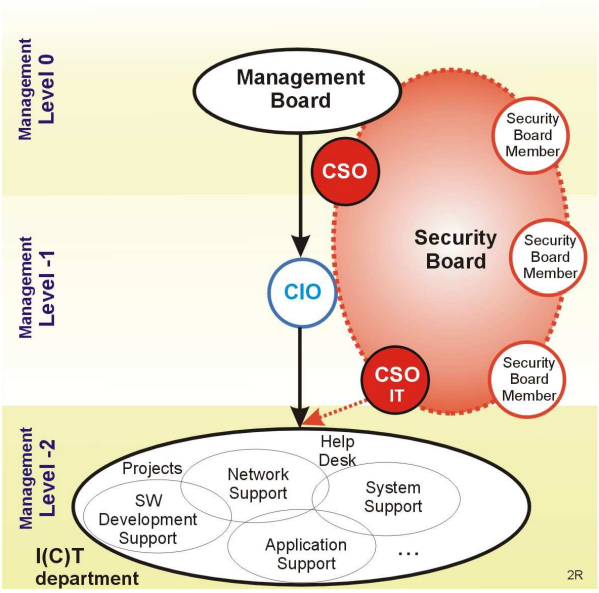
Má-li instituce pouze jediného bezpečnostního manažera IT (a žádné další specialisty), pak z praktického pohledu bývá model utopené bezpečnosti úspěšnější než model odtržené bezpečnosti, což je v rozporu s teoretickým přístupem, upřednostňujícím nezávislost realizace bezpečnosti v instituci.

Model agilní bezpečnosti

Model agilní bezpečnosti vychází z pozitiv předchozích modelů a odstraňuje negativa, typické pro jednotlivé modely. Model je charakteristcký pro středně velké instituce, které nemají žádné vlastní rozsáhlé bezpečnostní útvary s početným personálním obsazením, zajišťující bezpečnost. V instituci kromě osoby zodpovědné za bezpečnost informačních technologií může existovat navíc další manažer, odpovídající za fyzickou, personální, ekologickou bezpečnost apod.

V instituci je vytvořena tzv. bezpečnostní rada, která má podobu virtuální struktury napříč vrcholovým a středním managementem, jmenovaná vedením instituce (např. generálním ředitelem). Členové bezpečnostní rady jsou nominováni dle konkrétních potřeb instituce. Bezpečnostní rada může mít stále členy i externí, přizvané specialisty (z instituce nebo mimo ní). Členy mohou být jednotliví odborní ředitelé, personalisté, technici atd. a pochopitelně oba bezpečnostní manažeři.

Při takto pojatém modelu odpadají komunikační problémy mezi managementem a odbornými specialisty, koordinace mezi jednotlivými organizačními složkami nebo jednotlivci, kteří mají určitý vztah k bezpečnosti bývá na vysoké úrovni. Nebývá ani problém při prosazování bezpečnostních projektů, jejich financování. Bezpečnostní rada je kolektivním orgánem, který má trojí základní funkci: funkci „legislativní“, tj. tvorba a schvalování bezpečnostní politiky a s ní souvisejících dokumentů. Pak je tu funkce kontrolní, která zjišťuje stav implementovaných opatření a jejich funkcionalitu a pak funkci řídící v době ohrožení instituce, mimořádných bezpečnostních incidentech apod.



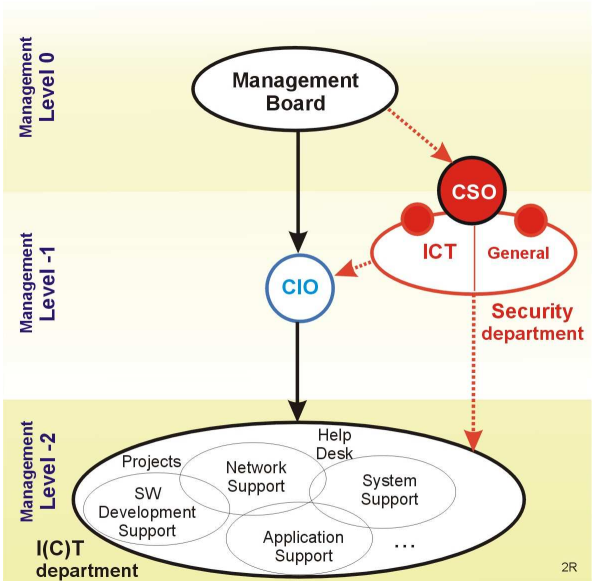
Obr. 6 Model agilní bezpečnosti.

Bezpečnost bývá vysoce agilní. Spokojeni bývají i auditoři, protože CSO není řízen jen CIO. CSO využívá všech výhod vyplývajících z blízkosti k útvaru IT v instituci. Na vysoké úrovni bývá i komunikace se zaměstnanci, jejich seznamováním s nezbytnými opatřeními a doporučeními. V bezpečnostní radě je dobré mít představitele personální složky instituce. Jednak je dobře otevřena cesta ke školením, jednak se dobře realizuje i personální bezpečnost.

Model rozsáhlé institucionální bezpečnosti

Uvedený model je typický pro velké instituce (jako jsou např. banky, velké průmyslové podniky, silové resorty státu) apod.

V těchto institucích již existují profesionální bezpečnostní útvary čítající více zaměstnanců, kteří se dále profesně specializují. Řeší se jak technologická bezpečnost, tak i bezpečnost informační a obecná (fyzická ostraha objektů atd.).



Obr. 7 Model rozsáhlé institucionální bezpečnosti.

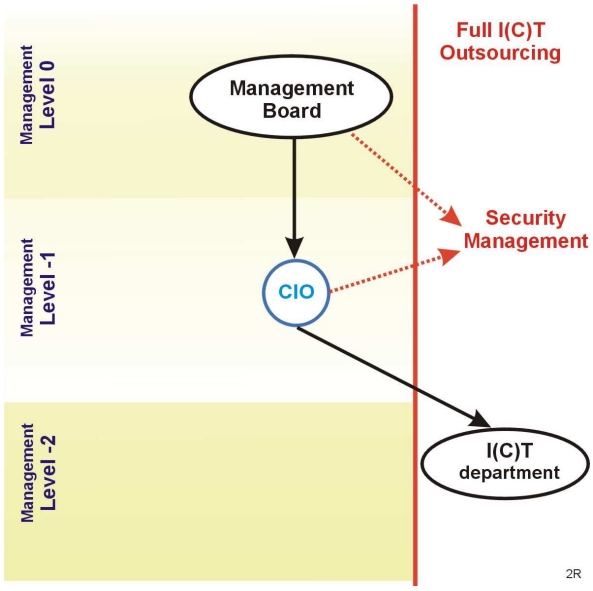
Tento model má řadu variant. Může se jednat o dva samostatné organizační celky, které mají své manažery pro technologickou (ICT) bezpečnost a obecnou bezpečnost, nebo o jediný organizační útvar ve vedení s jediným bezpečnostním manažerem, který se dále vnitřně člení podle jednotlivých oblastí a specializací.

Bezpečnost je již plně procesně formalizována a instituce buduje bezpečnost podle definovaných (mezi)národních standardů a doporučení, které byly pro instituci vybrány jako závazné. Veškeré IT projekty jsou důsledně řízeny i z pohledu bezpečnosti. Státní nebo polostátní organizace se obvykle navíc řídí závaznou národní (mezinárodní) legislativou na ochranu utajovaných skutečností, které kladou na instituci další požadavky a zároveň i omezení.

Pravidla financování bezpečnostních projektů jsou jasně determinována, potíže bývají obvykle v nedostatku finančních zdrojů na rozsáhlé projekty. V těchto institucích bývá na výši nejenom technologická bezpečnost, ale i bezpečnost personální. Zaměstnanci jsou pravidelně školeni a připraveni čelit i sociotechnickým útokům vedeným z venku. Bezpečnost ve velkých institucích se silně formalizovanými metodami a postupy nemusí být však dostatečně agilní na některé typy hrozeb. Hlavním problémem bývá jak velikost organizace, tak i někdy zkostnatělý nebo vžitý způsob myšlení ve „vyjetých kolejích“, nebo dokonce alibismus. V myšlení lidí, zaměstnanců může převládat názor: „Máme rozsáhlé bezpečnostní struktury, tak ať se starají!“

Model outsorcované bezpečnosti

O outsourcingu se poměrně často hovoří jako o cestě rozvoje a provozování ICT v instituci. Řada institucí využívá řady služeb svých dodavatelů pro řešení určitých okruhů činností (tedy lze hovořit o částečném outsourcingu). Plného outsourcingu ICT využívá zatím minimum institucí. Jsou proto malé praktické zkušenosti z pohledu bezpečnostního. Je zřejmé, že v instituci musí vždy ale zůstat osoba zodpovědná za koordinování informačních potřeb společnosti a řízení dodavatelské organizace.



Obr. 8 Model outsourcované bezpečnosti.

Komplexní řešení bezpečnosti se rozpadá do dvou okruhů. Všeobecná bezpečnostní politika zůstává vždy na straně instituce. Ta definuje své základní požadavky v souladu se strategickými plány svého rozvoje.

Technologická bezpečnost vychází z bezpečnostní politiky a je na straně dodavatele.

Outsourcovat lze leccos. Jedině co není možné outsourcovat, je vlastní strategické rozhodování a zodpovědnost za něj. Za bezpečnost organizace musí proto celkově zodpovídat vždy její zaměstnanec, bezpečnostní manažer, který musí zajistit definovanou úroveň dodavatelských služeb a koordinovat je se všemi procesy v instituci. Z tohoto pohledu jsou na bezpečnostního manažéra kladeny extremní nároky na jeho odbornost a manažerské znalosti a dovednosti, psychickou odolnost. Ve své pozici zůstává stejně osamocen jako v modelu odtržené bezpečnosti, bez možnosti blízkého přístupu k technologiím, které jsou dodavatelsky provozovány.

Základní otázkou vždy ale je, zda lze veškerou bezpečnost zajistit externími službami nebo zda to je ekonomicky nebo politicky přijatelné.

Faktem zůstává skutečnost, že outsourcing podstatně zvyšuje nároky na přesné zadání požadovaných služeb a obslužných procesů a je komunikačně náročný ve vztahu k dodavateli. V případě bezpečnosti se může jednat o kritický moment při rozhodování, protože složitá a zdlouhavá komunikace v případě ohrožení je sama o sobě nebezpečná.

Musí být i vyjasněny otázky, jakým způsobem kontrolovat úroveň bezpečnosti, když v zadavatelské organizaci je minimum (nebo žádní) specialisté na ICT nebo bezpečnost. Objektivní cestou v tomto případě je nezávislá kontrola, audit jiné instituce, specializující se na danou problematiku. To představuje další náklady, se kterými je nutno počítat.

Závěr

Žádný z výše uvedených modulů nemusí být universálně použitelný pro jakoukoliv instituci. Záleží na mnoha specifických podmínkách, které determinují praktický výsledek. Konečný, pro nás vhodný model může být i kombinací typických modelů, které jsme právě představili.

Při výkladu jsme se zaměřili především na instituce, jejichž organizační struktura je silně hierarchická a převažuje vertikální členění. Pro tyto instituce je typická štábní kultura a bezpečnost bývá organizována vojenským způsobem.

Pro moderní instituce je typická efektivní plochá struktura organizovaná maticovým způsobem. Při tomto uspořádání je kladen primární důraz na procesy. Takto je vnímána i bezpečnost. Bezpečnostní manažer pak zodpovídá za definované procesy v instituci a jejich bezpečnost.

Literatura:

[1] 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 80-86813-00-2

[2] Matoušková, I.: *Psychologie a taktika prosazování investic do informační bezpečnosti ve firemní sféře.* Security Magazín, č.4/2004, str. 48-49

[3] Nečas, S., Porada,V.: *Teoretická východiska a principy bankovní bezpečnosti*. Brno : VŠKE, 2002

[4] Nečas, S., Porada, V., Seiler, M.: *Bezpečnost banky ve vztahu k bezpečnostnímu managementu*. Sborník II. vědecké konference s mezinárodní účastí, Košice : ŽU - FŠI - pracovisko Košice, 2002, s. 250 - 262. ISBN 80-88922-78-X, EAN 9788088922780.

[5] Porada,V., Nečas, S.: *Bankovní bezpečnost jako součást bezpečnostní politiky organizace.* Bezpečnostní teorie a praxe, zvl. číslo. Praha : PA ČR, 2001 s. 437-448

[6] Rak, R.: *Homo sapiens jako nejsilnější i nejslabší článek v získávání a ochraně informací*, Data Security Management, 2004, č. 4, str. 10-13

[7] Rak, R., Matoušková, I.: *Tvůrčí bariéry, část I. – Bezpečnost, lidský intelekt a vliv sociálního prostředí*, DSM č.3/2004, str. 26-28, Tate International, Praha

[8] Rak, R., Matoušková, I.: *Tvůrčí bariéry, část II. – Bezpečnost, emoce a interpersonální komunikace*, DSM č.4/2004, str. 28-30, Tate International, Praha

[9] Spurný, J.: *O psychologickém přístupu k ochraně informací*. In. Psychologie v ekonomické praxi, 1999, roč. XXXIV. Č.3-4. s 199-203

Dr.h.c. prof. JUDr. Ing. Viktor Porada, DrSc, Policejní akademie ČR Praha, Lhotecká 559/7, Praha 4, E-mail: porada@polac.cz

Doc. Ing. Roman Rak, Ph.D., externí spolupracovník katedry kriminalistiky Policejní akademie ČR Praha, Lhotecká 559/7, Praha 4, E-mail: roman.rak@ct.cz

Mgr. Ingrid Matoušková, Bankovní institut Vysoká škola a.s., Ovenecká 9/380, Praha 7, E-mail: imatouskova@bivs.cz