Univerzita Pardubice
Fakulta ekonomicko-správní

Místo, úloha a význam bezpečnostního manažera v organizaci

Leoš Gramskopf

Bakalářská práce
2009

Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky
Akademický rok: **2008/2009**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Leoš GRAMSKOPF**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Místo,úloha a význam bezpečnostního manažera v organizaci**

Zásady pro vypracování:

Pojetí bezpečnostního managementu
Obsah informační bezpečnosti
Hlavní kroky implementace systému řízení bezpečnosti informací
Bezpečnostní manažer v instituci
Osobnost bezpečnostního manažera
Pozice bezpečnostního manažera - typové modely

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

BRABEC, František. Bezpečnost pro firmu, úřad, občana. 1.vyd. Praha: Public History, 2001. 210 s. ISBN 80-86445-04-06.

BRABEC, FRANTIŠEK A KOL. Soukromé detektivní služby. 1. vyd. Praha : Eurounion, 1995. 253 s.

BRABEC, FRANTIŠEK. Ochrana bezpečnosti podniku. 1. vyd. Praha : Eurounion, 1996. 203 s.

NEČAS, Stanislav - Hála, Milan. Bezpečnost v podmínkách organizací a institucí ČR - sborník z mezinárodní konference. 1. vyd. Praha: Soukromá vysoká škola ekonomických studií, 2005. 208 s. ISBN 80-86744-49-3.

URL<http://www.svses.cz/skola/akce/konf/bezp05/texty/sbornik.pdf> materiály poskytnuté JUDr. Františkem Brabcem ke studiu předmětu Úvod do IBS na Univerzitě Pardubice

Vedoucí bakalářské práce: **doc. Ing. Pavel Petr, Ph.D.**
Ústav systémového inženýrství a informatiky

Konzultant bakalářské práce: **JUDr. František Brabec**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **6. října 2008**

Termín odevzdání bakalářské práce: **1. května 2009**

doc. Ing. Renáta Myšková, Ph.D.
děkanka

L.S.

doc. Ing. Jiří Křupka, Ph.D.
vedoucí ústavu

V Pardubicích dne 6. října 2008

Prohlašuji:
Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 28. 4. 2009

Leoš Gramskopf

PODĚKOVÁNÍ

Rád bych touto cestou poděkoval doc. Ing. Pavlu Petrovi, PhD. za pomoc a vedení při tvorbě bakalářské práce a JUDr. Františku Brabcovi za poskytnutí cenných rad, podnětů a materiálů z praxe.

SOUHRN

Bakalářská práce se zabývá problematikou bezpečnostního managementu v organizaci. Popisuje obecné oblasti bezpečnosti, kde vyzdvihuje důležitost informační bezpečnosti, a představuje hlavní kroky zavádění systémů řízení informační bezpečnosti v instituci. Dále se zaměřuje na osobu bezpečnostního manažera, jeho význam a úlohu v organizaci, způsoby začlenění bezpečnostního manažera do organizační struktury podniku a aspekty ovlivňující činnost bezpečnostního manažera.

KLÍČOVÁ SLOVA

bezpečnostní manažer, informační bezpečnost, systém řízení informační bezpečnosti, bezpečnostní analýza, bezpečnostní projekt

TITLE

Position and role of security manager in company

ABSTRACT

The work deals with company security management questions. It describes general security areas, highlighting the importance of information security, and presents main steps in information security management system implementation. Then it focuses on the position of a security manager, his importance and role in a company, the ways of security manager incorporation within the company organizational structure and the aspects affecting a security manager activity.

KEYWORDS

security manager, information security, information security management system, security analysis, security project

OBSAH

Úvod

Současná doba je charakterizována neustále se měnícími podmínkami a turbulentními změnami, které působí na činnosti organizací, institucí či podnikatelských subjektů. Ne všechny subjekty se ovšem umí s proměnami tržního prostředí úspěšně vyrovnat. V právě probíhající ekonomické krizi se ukazuje, že nezáleží na velikosti společnosti, její historii, tradici nebo jakých úspěšných hospodářských výsledků dosáhla v minulých letech, ale naopak jak se dokáže vyrovnat se svými neúspěchy a zda na ně byla dostatečně připravena, případně jak umí využít neúspěchů svých konkurentů. Aktuální cíle jednotlivých organizací se mohou lišit podle postavení na trhu. Některé chtějí udržet chod společnosti a přečkat nepříznivou situaci, některé chtějí naopak posílit svůj význam a odstranit z cesty své soupeře. I když jsou cíle různých společností často rozdílné a protichůdné, jedno mají společné. K naplňování svých cílů potřebují informace. Informace včasné, relevantní, kvalitní, užitečné a cenné.

Většina organizací se pomocí nejrůznějších prostředků zaměřuje především na získávání informací, málokterá ale obrací pozornost na ochranu svých důležitých aktiv a na zabránění úniku citlivých informací. Oba obranné mechanismy jsou jednou z hlavních náplní bezpečnostního manažera. Společnosti se shodnou na nesporném významu informační bezpečnosti, ale jen některé se zabývají celkovým bezpečnostním managementem. Ty, které se bez něj obejdou, oponují zbytečně vynaloženými náklady, za které nedostanou očekávaný efekt. Neuvědomují si ale, že kdyby došlo k úniku informací, mohou ztráty daleko převyšovat náklady, které by vložily do řešení bezpečnostního managementu. Jedním z důvodů může být i neznalost této problematiky či nedostatek kvalifikovaných pracovníků, kteří by dokázali tyto činnosti zajistit.

Je vidět, že na tuto situaci zareagovaly i vysoké školy, které začaly nabízet studium v oborech informačních a bezpečnostních systémů. Já sám studuji tento obor a jeho náplň mě natolik zaujala, že jsem si zvolil profesi bezpečnostního managera jako téma své bakalářské práce.

Cílem práce je seznámit se s problematikou bezpečnostního managementu a na základě těchto znalostí najít vhodný postup implementace systémů řízení informační bezpečnosti v podniku, definovat profesi bezpečnostního manažera a nalézt univerzální model začlenění bezpečnostního manažera do organizační struktury podniku.

Práce by měla být vodítkem či pomocnou rukou všem neopatrným subjektům, které doteď váhají se zapojením bezpečnostního managementu do své organizace, ale může doplnit i znalosti zodpovědných subjektů, které tak mají možnost ověřit si, zda při zabezpečení svých informací něco neopomněly. V neposlední řadě by si měl čtenář uvědomit, jak náročná je profese bezpečnostního manažera a že by tato funkce měla být lépe ohodnocena v souvislosti s významem své pozice a s celkovým přínosem pro organizaci, instituci či podnikatelský subjekt.

1 Pojetí bezpečnostního managementu

Termín management vychází z anglického *to manage* – řídit, původem z francouzského *ménagement*, které má zase svůj kořen v latinském slovu *manus* - ruka, a jeho prazákladem bylo ruční ovládání koní. Management je umění řízení, působení na určitou soustavu (například společnost) a ovládaní její činnosti [11]. V českém jazyce má několik významů, nejčastěji bývá překládán jako řízení nebo vedení, píše se i vyslovuje anglicky.

Rozlišujeme tři významy tohoto zdomácnělého slova, tři základní pojetí managementu [10]:

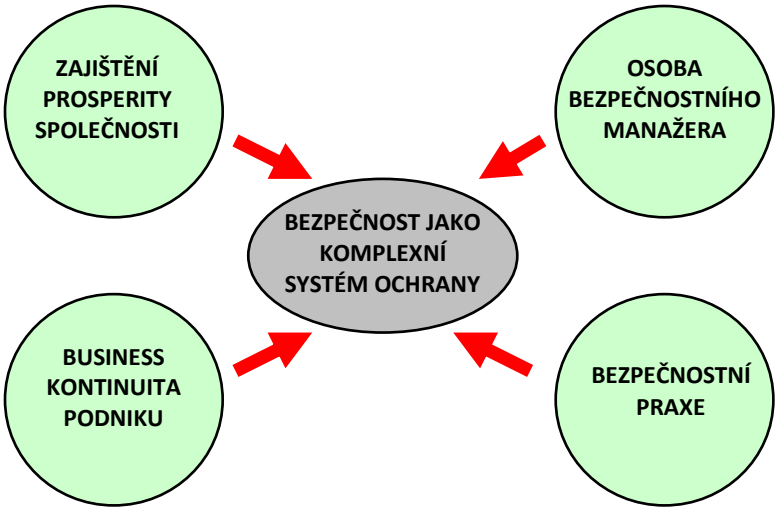
- management jsou vedoucí pracovníci – manažeři,
- management představuje škálu manažerských činností či funkcí (plánování, organizování, rozhodování atd.),
- management je vědní disciplína i praktický obor.

Obecný, teoretický management, podobně jako obecná ekonomická teorie implikuje speciální oborové, odvětvové disciplíny (ekonomika dopravy, zdravotnictví, stavebnictví). Speciální disciplínou, která je uznávána, se nestane každé nové téma hned. Proto také z jisté profesionální opatrnosti hovoříme o bezpečnostním managementu spíše jako o tématu managementu. Při stále více uvědomovaných společenských rizicích v globálním světě současného století se stále více zabýváme bezpečností. Objevují se publikační příspěvky a výzkumy, které signalizují potřebu systematického shromažďování bezpečnostních poznatků v množině bezpečnostních věd. V této souvislosti se rozvíjí také nové téma managementu - bezpečnostní management. [10]

1.1 Bezpečnost jako ucelený systém

Komplexní řešení problematiky ochrany managementu je poměrně rozsáhlou oblastí bezpečnosti a zahrnuje plánování preventivních opatření, vzdělávání manažerů, vytvoření materiálně-technické základní ochrany, komerční obranné zpravodajství, fyzický výkon ochrany a řešení bezpečnostních incidentů a ohrožení. Je v zájmu manažerů se o tuto problematiku začít velmi vážně zajímat. Bezpečnost jako systém ochrany sloužící k poznání a eliminaci vnějších a vnitřních bezpečnostních rizik,

vystupuje ve vztahu k roli manažera, vlastníka, vedoucího apod. v několika rovinách [7]. Pro představu jsou jednotlivé roviny uvedeny na obrázku 1, za kterým následuje detailnější popis jednotlivých rovin.



Obrázek 1 Roviny vystupující ve vztahu k bezpečnosti podniku [vlastní]

První a základní rovina chápe bezpečnost jako nezbytnou podmínku zajištění prosperity společnosti, kontinuity činnosti úřadu, instituce nebo naplnění cílů projektu, produktu, služby. Odpovědnost za bezpečnost má vždy manažer – vedoucí organizace. Tato odpovědnost je v obecné rovině stanovena právními předpisy a vyplývá z komplexní odpovědnosti vedoucího. Zároveň však logicky pramení z odpovědnosti a ze zájmu manažera o funkčnost organizace jako celku. V současných podmínkách si funkčnost bez bezpečnosti nelze představit. Nejde však pouze o bezpečnost práce, ale o bezpečnost v nejširším významu slova, tj. bezpečnost komplexní. [7]

Druhá rovina je rovinou osobní a je bezprostředně spojena s výkonem činnosti manažera, jeho dalšími aktivitami i soukromým životem. Patří sem především události a jednání, které mohou být zneužity k diskreditaci manažera a v konečném důsledku ohrozí kontinuitu jeho působení ve funkci či podnikání. Zajímavé přitom je, že velká část obvinění klíčových státních úředníků a top manažerů nemá příčinu v úmyslném jednání, ale v nedbalosti. Ta vyplývá z nedostatečné znalosti legislativy nebo podceňování rizik souvisejících s řešením dané situace. V některých případech se pak trestná činnost manažera či úředníka neprokáže, ale vlivem medializace dojde k poškození jeho dobrého jména a dobrého jména úřadu či společnosti. S odstupem času se někdy navíc ukazuje, že problém vznikl uměle na základě úniku informací, které neměly být veřejnosti přístupné. Nejsou výjimkou ani případy, kdy se celý problém

odehraje na základě komerční objednávky. Zdrojů incidentů může být celá řada, od konkurenčních vlivů přes záležitosti vyplývající z minulosti manažera až po osobní ambice podřízených nebo aktivity propuštěných zaměstnanců. Ideální možností je zavedení specializovaného bezpečnostního vzdělávání pro top management. Základním krokem může být vystoupení bezpečnostního experta nebo znalce na poradě vedení či představenstva společnosti. [7]

Třetí rovinou je rovina business kontinuity. Obvykle chápeme, že společnost by měla mít krizové scénáře pro řešení nejrůznějších problémů a incidentů. Ne vždy se však dokážeme odpoutat od mýtu, že se toto dotýká pouze ekonomické úrovně řešení. Bezpečnostní opatření spojená s kontinuitou podnikání jsou nadále podceňována, řešení ohrožené bezpečnostního charakteru schází nebo jsou nedostatečně rozpracována. Přitom nemusí jít o nákladná opatření technického charakteru, ale o opatření organizační. Příkladem jsou rozpracované a zvládnuté postupy při vzniku incidentů bezpečnostního charakteru s minimalizací jejich dopadu. Pro subjekty kritické infrastruktury je povinnost zpracování krizové dokumentace stanovena legislativou. Ta je však vázána na vyhlášení tzv. krizového stavu. Ne vždy si uvědomujeme, že neřeší, a ani řešit nemůže, situace, které ještě nedosáhly uvedeného rozměru, nebo vnitřní incidenty. [7]

Čtvrtá rovina, ve které se promítají roviny předchozí, je rovinou bezpečnostní praxe. Její výslednicí je reálná úroveň bezpečnosti podniku, úřadu, instituce. Základní otázkou přitom je, jakým způsobem je ochrana osob, hmotného a nehmotného majetku (informací) organizována a zajištěna. Je zde na místě položit si několik základních otázek [7]:

- Splňujeme veškeré požadavky, které pro bezpečnost stanovuje platná legislativa ČR?
- Řídíme se při zajišťování bezpečnosti odbornými technickými normami?
- Byl váš bezpečnostní systém navržen na základě analýzy rizik? Kdy byla analýza naposledy aktualizována?
- Má vaše společnost, instituce, úřad bezpečnostní politiku? Je bezpečnostní politika pravidelně aktualizována?

- Jaké je postavení bezpečnostního managementu a místo bezpečnostního manažera v organizační struktuře?
- Je účinnost bezpečnostního systému ověřována auditní a kontrolní činností?
- Existuje pro oblast bezpečnosti a krizového řízení samostatný rozpočet? Víme, kolik nás bezpečnost stojí?
- Je hodnocení bezpečnosti součástí porad vedení? Je součástí hodnocení podřízených manažerů?

Obdobných otázek bychom mohli položit ještě mnoho. Cílem však není podat vyčerpávající přehled problémů, ale nastartovat proces uvědomění bezpečnosti.

Další podrobnosti jsou pak plně záležitostí bezpečnostního managementu nebo společnosti, která bude bezpečnost komplexně posuzovat. Pokud je na většinu výše uvedených otázek odpovědí NE nebo NEVÍM, pak je na místě začít se bezpečností zabývat na úrovni vrcholového vedení společnosti nebo úřadu. Jednou z možností je zadání posouzení současného stavu bezpečnosti specializované společnosti nebo expertnímu týmu. Řešením je také postupná realizace úkolů, které jednotlivé otázky prezentují. [7]

1.2 Rozsah bezpečnosti

Rozsah bezpečnosti si lze představit podle zjednodušeného schématu domu, který je znázorněn na obrázku 2.

Obrázek 2 Schéma domu s rozsahem bezpečnosti [7]

Náš virtuální dům na obrázku tvoří ucelený bezpečnostní systém. Jeho základem je personální bezpečnost. Pod tímto pojmem se skrývají veškeré otázky spojené s bezpečnostními podmínkami pro výběr top managementu, zaměstnanců a ověřování splňování těchto podmínek po celou dobu trvání zaměstnaneckého nebo jiného poměru u organizace. Pod personální bezpečnost dále zahrnujeme proces bezpečnostního vědomí (spoluodpovědnosti za bezpečnost) a bezpečnostní vzdělávání. [7]

Dům je dále rozdělen do dvou hlavních částí bezpečnosti. Části safety (provozní a technologická bezpečnost) a security (klasická bezpečnost). Oběma částmi bezpečnosti se pak prolínají jednotlivá bezpečnostní opatření (oblasti, prostředky, druhy zajištění apod.), kterými jsou zejména [7]:

- fyzická bezpečnost,
- informační bezpečnost,
- administrativní bezpečnost.

Nástavbou a střechou virtuálního domu je pak bezpečnostní politika a bezpečnostní management. Bezpečnostní politikou v tomto případě nechápeme pouze vlastní základní dokument řídící dokumentace v oblasti bezpečnosti, tj. komplexní bezpečnostní politiku, ale veškerou navazující bezpečnostní dokumentaci. Rovněž bezpečnostní management není chápán pouze jako bezpečnostní manažer nebo tým, ale také vedoucí zaměstnanci jednotlivých úrovní, kteří jsou za bezpečnost ve svých funkcích odpovědni.

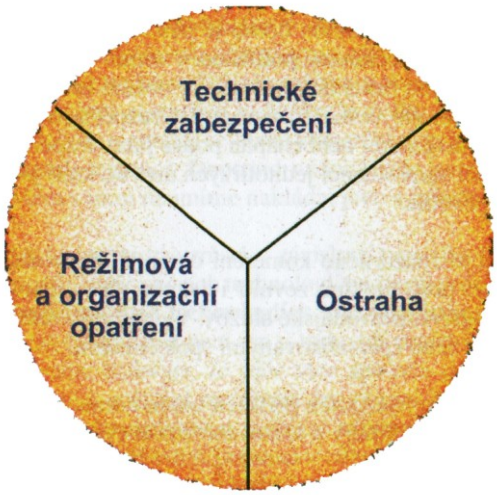
Jako bleskosvod je znázorněno komerční obranné zpravodajství, jehož účelem je chránit organizaci proti útokům zevnitř i zvenku. Pro orgány státu zajišťují roli obranného zpravodajství zpravodajské služby. V privátním sektoru se toto zajišťuje vlastními specialisty nebo specializovanými společnostmi.

Přerušovanou čarou je znázorněn perimetr okolo domu, který představuje ochranu ve smyslu business kontinuity a krizového řízení.

Obdobně jako u stavby či rekonstrukce domu je nezbytné si uvědomit, že i bezpečnost se musí řídit legislativou a odbornými technickými normami. Tak jako vydání stavebního povolení předchází analýza řady vlivů, tak musí být před návrhem bezpečnostního systému provedena bezpečnostní analýza. Tak jako se stavba realizuje na základě projektu, tak se realizuje bezpečnost podle bezpečnostního projektu. Kolaudací a revizí bezpečnostního domu je bezpečnostní audit. Ten je nezbytné po periodách provozu domu opakovat a provést následnou korekci bezpečnostních opatření. [7]

Fyzická bezpečnost

Schéma znázorňující opatření fyzické bezpečnosti je znázorněno na obrázku 3.



Obrázek 3 Schéma opatření fyzické bezpečnosti [7]

Bezpečnostní opatření jsou dnes velmi širokou problematikou, která je průsečíkem řady významných vědních disciplín. Nejsložitější oblastí je technické zabezpečení, které zahrnuje pohled o stovkách technologií a možnostech jejich implementace. Její využívání předpokládá vysokou úroveň odborných znalostí, ale i periodické vzdělávání v oblasti vývoje standardů a nových výrobků na trhu. Proto je doménou úzkého okruhu specialistů a až na výjimky outsourcovanou činností. Bezpečnostní management však nemůže ztratit přehled o technických možnostech, protože jinak by byl ve vleku zájmu dodavatelů. I přesto, že systémy technického zabezpečení jsou dodávány renomovanými společnostmi s nezbytnou praxí, dochází při návrhu, realizaci i provozu k chybám a nedostatkům. V jejich důsledku se pak snižuje spolehlivost, využitelná hodnota a uživatelský komfort. Problémem je především výběr zabezpečení podle jediného kritéria, kterým je cena. V případě, že jednoznačně nespecifikujeme minimální technické parametry a požadavky na uživatelský komfort, dochází nejen k upřednostnění méně kvalitních systémů, ale v konečném důsledku i ke snížení efektivnosti bezpečnostní instituce. Technické parametry nabídek by u větších zakázek měla posuzovat specializovaná a nezávislá společnost nebo soudní znalec. Je vhodné, aby se tito specialisté podíleli rovněž na technickém dozoru a přejímce zabezpečení. [7]

Neméně závažným problémem je bezpečnostní správa instalovaných technologií a výkon funkce odpovědné osoby za provoz systému technického zabezpečení. U některých organizací není tato otázka řešena vůbec. Výsledkem je pak neutěšený stav provozu bezpečnostních technologií. Výjimkou není ani formálně provedená funkční zkouška nebo periodická revize. Uvedený stav je rovněž výsledkem nekvalitního výběru dodavatele a upřednostňování ceny před kvalitou. [7]

Nedoceněnou otázkou zůstávají režimová a organizační opatření. Bez nich nemůže být funkční technické zabezpečení ani ostraha. Chybí provozní řády a zásady chování při mimořádných událostech. Školení zaměřené na dodržování režimových a organizačních opatřeních jsou výjimečnou záležitostí. Mezi nejčastější závady zjišťované bezpečnostními audity patří chyby v klíčovém režimu a vstupu osob do objektu v mimoprovozní době. V řadě případů zcela schází režim provozu technického zabezpečení. Obdobný stav je v oblasti kontroly režimových opatření. Ty se provádějí pouze výjimečně a často formálně. Obyčejně se kontroly nařídí až po vzniku mimořádné události. Příčina je často ve vytížení bezpečnostního managementu velkým množství činností, které není schopen kvůli kapacitním možnostem zvládnout. [7]

Bezproblémové není ani zajišťování fyzické ostrahy objektů a ostrahy formou dálkového monitoringu a dohledu. Trend snižování závislosti fyzické bezpečnosti na ostraze je sice správný, ale není nekonečným příběhem. Bezpečnost objektů bez ostrahy je bohužel nereálná. Ostraha zůstává i z důvodu nízkého finančního ohodnocení zaměstnanců stále nejslabším článkem bezpečnostního systému. Nedostatky přetrvávají ve smluvních vztazích, které neposkytují dostatek nástrojů pro quality monitoring služeb. [7]

Situace ve fyzické bezpečnosti vyžaduje přehodnocení stávajících opatření a jejich optimalizaci. Ty činnosti, které bezpečnostní management pro své vytížení nezvládá, je nezbytné outsourcovat. Možným prostorem pro outsourcing je činnost odpovědné osoby za provoz bezpečnostních technologií, quality monitoring technického zabezpečení a ostrahy, zpracování a aktualizace provozních řádů a další chybějící bezpečnostní dokumentace. [7]

Administrativní bezpečnost

Podcenění bezpečnosti vede dříve nebo později k závažnému poškození funkčnosti organizace. Výjimkou nejsou ani hospodářské škody značného rozsahu, a dokonce konkurzy podniků. Zvláštností není ani trestně právní postih statutárních orgánů. Nejvíce problémů má svůj původ v nedostatcích v oblasti personální bezpečnosti. Významnou roli hraje i úroveň dokumentace bezpečnostních opatření. Při jejím podcenění je obtížné vyžadovat dodržování těchto opatření a stejně tak je kontrolovat.

V první rovině je možné argumentovat množstvím příkladů, kdy opomenutí nebo podhodnocení bezpečnosti ohrozilo podnikatelské aktivity nebo vedlo ke značným ekonomickým ztrátám. Patří sem například úniky důležitých informací a know-how v případech krachu významných telekomunikačních a softwarových společností v USA. Velmi častým problémem je nedůslednost v personální bezpečnosti. Typickým příkladem takového problému je neodhalení gamblerství finančního ředitele jednoho významného potravinářského holdingu, které vedlo ke ztrátě desítek milionů Kč, nebo problémy spojené s pokusy o vytunelování jednoho z nejvýznamnějších českých provozovatelů produktovodů. [7]

Informační bezpečnost

Závažné dopady mohou mít nedostatky v oblasti fyzické a informační bezpečnosti. Význam fyzické bezpečnosti se zvyšuje v návaznosti na fyzickou bezpečnost informačních systémů, zvýšená rizika terorismu a aktuálnost fyzického zabezpečení ochrany proti nasazení operativní techniky. V úvahu je zde nutné vzít nejen to, že i špičková technika se stala komerčním produktem, ale i rizika zneužití techniky státních institucí. Doposud nedokážeme nejen docenit hodnotu informací, ale především s nimi neumíme nakládat jako s informacemi. Význam informační bezpečnosti vzrůstá v závislosti na riziku úniku citlivých informací a rostoucím podílu informačních technologií na řízení procesů. Čím závislejšími se stáváme na informačních technologiích, tím více jsme ovlivňováni jejich bezpečností. Informační bezpečnost není jen o tom, zda používáme špičkové informační technologie a legální software. Je stále více způsobů používán technologií, bezpečnostního monitoringu a řešení incidentů. I v oblasti informační bezpečnosti vzrůstá význam personální bezpečnosti a vzdělání uživatelů. Většina postupů, standardů a zásad informační bezpečnosti je popsaná v odborných normách v oblasti informačních a komunikačních technologií. Tématu

informační bezpečnosti se budeme více věnovat v samostatné kapitole. [7]

1.3 Obsah informační bezpečnosti

Ze všech funkcí bezpečnostního managementu je potřeba vyzdvihnout funkci v dnešní době nejdůležitější – řízení bezpečnosti informačních systémů. Obor informační bezpečnosti můžeme stručně vymezit jako specializaci zabývající se ochranou informací. Pod termínem "informační bezpečnost" tak máme na mysli celý soubor aktivit směřujících k zajištění důvěrnosti (k našim informacím se nedostane nikdo nepovolaný), integrity (naše informace nebudou změněny nebo porušeny) a dostupnosti (vždy budeme mít ke svým informacím přístup) informací. Ve své podstatě a ve své šíři je informační bezpečnost multidisciplinární obor nabízející komplexní pohled na problematiku ochrany informací, jež se zabývá otázkami organizačními, řídícími, metodickými, technickými, právními, sociálními a dalšími [13].

O významu řešení informační bezpečnosti pro organizace nemá smysl diskutovat. Skutečně se dnes těžko najde manažer, který by si mohl dovolit oblast informační bezpečnosti zcela ignorovat. Informace jsou stále více ceněným zbožím a to si uvědomují všichni. Od uvědomění si významu bezpečnosti až k efektivní ochraně informací je nicméně cesta dlouhá a trnitá. [13]

Od vzniku prvních počítačů se lidé postupně začali vážně zabývat informační bezpečností. Za tu dobu se nahromadila již řada zkušeností a praktických příkladů, které umožňují pojmenovat to, co by rozhodně společnosti měly do řešení informační bezpečnosti zahrnout [13]:

- **Bezpečnostní politika** - označení pro základní a klíčový bezpečnostní dokument schválený nejvyšším vedením společnosti a závazný pro celou společnost, v němž společnost deklaruje své základní cíle v oblasti ochrany informací. Politika pojmenovává to, co má být chráněno, a stanovuje, byť v základních rysech, jak toho má být dosaženo. Dále je cílem politiky definovat příslušné zodpovědnosti a pravomoci.

- **Bezpečnostní management** - organizační struktura společnosti obecně zajišťující prosazování plnění bezpečnostní politiky do života společnosti a chránící organizaci před bezpečnostními riziky. Klíčovou postavou je bezpečnostní manažer -

člověk zodpovědný za bezpečnost - u něhož se musí rovným dílem skloubit manažerské schopnosti s odbornými vědomostmi.

- **Systém hlášení bezpečnostních incidentů** - zahrnuje eskalační procedury, které zajistí mobilizaci v případě problémů vyžadujících okamžitou reakci, a centrální evidenci hlášení o bezpečnostních incidentech. Distribuovaná prostředí IT mají za následek distribuovanou zodpovědnost, musí proto existovat jednotný systém umožňující včasnou reakci a podporující měření účinnosti bezpečnostních opatření a pro zjišťování trendů.

- **Bezpečnostní vzdělávání** - systém pravidelného vzdělávání vlastních zaměstnanců v oblasti informační bezpečnosti. Prostředí IS/IT se rychle mění, mění se legislativa, mění se i samotné společnosti, jejich strategie a obchodní plány, lidé ve společnosti mění své pozice, přicházejí a odcházejí. To jsou hlavní argumenty pro to, aby se školení týkající se informační bezpečnosti periodicky opakovala.

- **Plány obnovy funkčnosti** - příprava na eliminaci dopadů v případě vážné neočekávané události. Jedná se o přípravu na eliminaci dopadů hrozeb, které ze své podstaty společnost ovlivnit nemůže (přírodní katastrofa) nebo nechce (preventivní opatření by byla neúměrně nákladná). Filozofie je zde stejná jako u pojištění - příprava na něco špatného, co mě může potkat, ale nemusí, a co nemohu ovlivnit.

Všech pět zmíněných skutečností uplatněných při řešení informační bezpečnosti neznamená automaticky pro společnost bezproblémový život. Ovšem ani absence některého či dokonce všech neznamená automaticky zkázu. Zkušenosti ale ukazují, že společnosti "se všemi pěti pohromadě" mají s informační bezpečností a ve svém důsledku s naplňováním svých strategických obchodních cílů menší problémy, než společnosti jiné. [13]

Ochrana informací v komplexním – systémovém pojetí představuje systém s řadou subsystémů – rovin. Informační bezpečnost se musí odehrávat v následujících rovinách:

- rovina metodologická a koncepční;

- rovina bezpečnostně organizační, bezpečnostně režimová a bezpečnostně technologická;

- rovina prosazování a uplatňování informační bezpečnosti – bezpečnostních postupů a opatření;

- rovina bezpečnostních auditů;
- rovina personální;
- rovina technických řešení.

Je třeba vycházet ze skutečností, že existují dvě možnosti úniku informací [5]:

1. nespolehlivost a selhání lidského faktoru,
2. nespolehlivost a selhání technických systémů (včetně softwarových subsystémů).

Lidský faktor je ale stěžejní a primární. Technická a softwarová spolehlivost či nespolehlivost (stupeň spolehlivosti) je koneckonců výsledkem lidské činnosti. Hovoříme-li o problematice ochrany informací, dat, komunikačních a počítačových systémů v podniku, můžeme jinými slovy hovořit o obranném zpravodajství či podnikové kontrašpionáži. Obsah je ale stejný. Jestliže se všeobecně uznává, že v rámci soutěživého zpravodajství (Competitive intelligence) jsou hlavní devizou lidé – tj. lidské zdroje, pak z hlediska vlastního obranného zpravodajství jsou též největším problémem. Lidé jsou nejčastějším problémem úniku informací a dat a jejich neznalost, nedbalost, neopatrnost a mnohdy i záměr ovlivňují spolehlivost počítačových a komunikačních systémů.

Při definování požadavků na ochranu informací je třeba si odpovědět na následující okruhy otázek [5]:

- Které informace, data, počítačové a komunikační systémy je třeba považovat za důvěrné, které jsou hlavní elementy těchto chráněných systémů a proč?
- Jak dlouho je třeba určité informace a data uchovávat v tajnosti a proč?
- Co je již známo nebo o čem lze předpokládat, že je známo a proč?
- Které útvary organizace a které osoby budou s daným okruhem informací seznámeny, v jakém rozsahu a proč je to nutné?
- Které osoby spadají do okruhu pracovníků, kteří vytvářejí rozhodnutí, strategii, pracují na vývoji, výzkumu?

1.3.1 Prvky informační bezpečnosti

Celková bezpečnost informací je dána jednotlivými prvky, zejména stupněm ochrany jeho nejslabších článků. Prvky informační bezpečnosti lze rozdělit na [1]:

- **Personální bezpečnost** – jedná se o ochranu informačních systémů z hlediska jednání a konkrétních událostí způsobených pracovníky, a to především z pohledu prevence. Personální bezpečnost musí být zajišťována jednak detektivními prověrkami budoucích (potenciálních) zaměstnanců podniku a jednak periodickými detektivními prověrkami stávajících zaměstnanců. Bezpečnost v oblasti personálních opatření předpokládá vymezení rozsahu prověrky nových i stávajících zaměstnanců, zejména pak vedoucích pracovníků z oblasti středního a vrcholového managementu a obzvláště těch, kteří přicházejí nebo budou přicházet do styku s důvěrnými a utajovanými informacemi. Dále je potřeba vymezit rozsah a způsob dohledu nad osobami, které z podniku odešly a byly seznámeny s důvěrnými a především s utajovanými skutečnostmi či informacemi.

  Detektivní prověrky zaměstnanců příslušného podnikatelského subjektu musí poskytnout informace minimálně z okruhů, jako jsou celková zpráva o pověsti (závislé na budoucím zařazení zaměstnance, informace z evidencí a posledního bydliště, ale i z dřívějších bydlišť a pracovišť, informace o rodičích, sourozencích, o činnostech ve formálních i neformálních kolektivech apod.), informace o kontaktech (stycích) prověřované osoby (cílem je odhalit rizikové styky a kontakty), informace o detektivní prověrce situací, činností a jednání, na která jsou k prověřované osobě signály. Někdy dochází k prověrce i pomocí fyziodetekčního vyšetření, které je zvláště významné v oblasti bankovnictví, pojišťovnictví a u organizací zabývajících se výzkumem a vývojem u institucí, kde se pracuje s utajovanými skutečnostmi (daty, informacemi).

- **Režimová bezpečnost** – vytvoření pravidel z hlediska zásad práce s informacemi, daty, komunikačními a počítačovými systémy. Jde o významný prvek prevence. Režimová bezpečnost zahrnuje kontrolu dodržování pravidel, režim práce s písemnostmi, režim ukládání datových médií, vymezení okruhu osob pro práci s výběrovými, důvěrnými a utajovanými informacemi a daty, opatření pro případ mimořádné události apod. Vymezuje, co je v rámci podniku považováno za důvěrné a utajované informace, stanovuje okruh lidí, kteří k těmto informacím mají přístup a

v jakém rozsahu, určuje režim a kontrolu pohybu zaměstnanců a cizích osob v objektu organizace, stanovuje režim a kontroly přijímání návštěv.

- **Bezpečnost technických prostředků** – jde o jejich výběr a spolehlivost, kontrolu přístupu k těmto prostředkům, ochranu před elektromagnetickým zářením a elektrostatickou elektřinou, stanovení rozsahu a následnou realizaci komplexních a dílčích, základních a periodických prohlídek, stanovení prověrek míst určených k důležitým jednáním, vybavení prostor technickými prostředky průběžného zjišťování odposlechů.

- **Bezpečnost programových prostředků** – kontrola přístupu k nim, autentičnost a identifikace uživatele, rozdělení pravomocí mezi uživatele, výběr a spolehlivost programů, ochrana proti virům, ochrana proti zneužití programového vybavení, ochrana proti zničení nebo poškození.

- **Bezpečnost dat** – předpokládá ochranu dat v souborech a databázích, ať již elektronických či písemných, ochrana proti chybám a virům, zvláštní ochrana citlivých dat, autorizace a rozlišení přístupu k datům a databázím.

- **Bezpečnost komunikačních systémů a cest** – představuje především ochranu mezi jednotlivými částmi komunikačních a počítačových systémů.

- **Fyzická bezpečnost** – zajišťuje ochranu informací, dat, komunikačních a počítačových systémů proti neoprávněnému přístupu k nim, proti protiprávnímu vniknutí do prostor, kde se nacházejí.

- **Aktivní ochrana proti úniku informací a dat** (proti podnikové či firemní špionáži – proti aktivnímu soutěživému či konkurenčnímu zpravodajství) – jde o systém opatření směřujících k získání informací o aktivitách konkurenčních útvarů (agentur) zabývajících se konkurenčním (soutěživým) zpravodajstvím (informační pronikání do takovýchto útvarů či agentur).

1.3.2 Informace a její cena

Každá informace má svou cenu, která je vyjádřena hodnotou, jakou má pro příjemce tím, že snižuje neurčitost a umožňuje rozhodování a řízení. Neexistuje informace, která by neměla cenu. Potřeba nějak změřit cenu informací vzniká ze dvou důvodů. Jednak jde o důležitý údaj při oceňování aktiv organizace jako celku v souvislosti s oceněním

nehmotného vlastnictví, jednak jde o rozhodující argument pro stanovení adekvátních ochranných opatření. Vyjádření ceny informace přímo v peněžních jednotkách není až na výjimky možné. Hlavním důvodem je vícerozměrnost hodnoty informace, která se obvykle vyjadřuje v její dostupnosti, důvěrnosti a integritě. Je zřejmé, že dočasně nedostupná nebo příliš brzy prozrazená nebo nesprávná informace ztrácí cenu. Nejčastěji používanou metodou oceňování informací je expertní hodnocení následků – co by se stalo, kdyby určitá informace byla po nějakou dobu nedostupná, vyzrazená, úmyslně nebo náhodně změněná nebo podvržená? Možné následky vystihuje následující výčet [14]:

- **Ohrožení života a zdraví** - v důsledku vyzrazení, modifikace a nedostupnosti informací mohou být ohroženy životy a zdraví osob, vyzrazení může mít za následek vydírání, modifikace a nedostupnost informací je nebezpečná ve zdravotnictví, při řízení dopravních a technologických prostředků.

- **Vyzrazení osobních údajů** - informace o soukromí osob, jejich zdravotním stavu, majetkových poměrech, rasovém původu, náboženství, osobním hodnocení, sexuální orientaci, musí být určitým způsobem chráněny. Následkem vyzrazení může být újma na vážnosti dotčené osoby, ale také postih provozovatele informačního systému. Současně je třeba ručit za správnost těchto informací, protože neautorizovaná změna muže mít podobné následky jako vyzrazení.

- **Poškození dobrého jména** - nedostupnost, vyzrazení nebo modifikace informace může mít za následek poškození dobrého jména, pověsti, důvěryhodnosti jednotlivce nebo organizace.

- **Porušení zákonů, předpisů a smluvních závazků** - dostupnost a důvěrnost informací chráníme i z důvodu, právních předpisů a smluvních závazků. Zpravidla jde o povinnost nebo závazek mlčenlivosti, ochrany důvěrných údajů, know-how, obchodního tajemství, bankovního nebo jiného tajemství nebo utajovaných skutečností.

- **Narušení řízení chodu organizace** - nedostupnost, poškození nebo úplné zničení informace může způsobit omezení činnosti nebo neefektivní řízení organizace. Předčasné zveřejnění informací o připravovaných změnách (reorganizaci) vyvolá takovou reakci, že tyto změny nebude možné provést.

- **Poškození obchodních zájmů** - hodnota informací v konkurenční soutěži se zpravidla měří cenou, kterou by byla ochotna zaplatit konkurence za získání, poškození, nedostupnost nebo zničení informací.

- **Přímé finanční ztráty** - informace související zejména s finančními transakcemi a finanční bilancí mohou v případě vyzrazení, neautorizované modifikace, nedostupnosti nebo zničení vést k přímým finančním ztrátám. Situace po havárii informačního systému nebo jeho části vyžaduje náklady na obnovu, kterou lze vyjádřit cenou práce a ostatními náklady.

- **Nepřímé finanční ztráty** - souvisí s ohrožením života a zdraví osob, poškozením dobrého jména, porušením smluvních závazků, narušením řízení a chodu organizace.

- **Maření zákonnosti** - informace týkající se vyšetřování trestných činů by neměly být předčasně vyzrazeny, modifikovány nebo nedostupné. Může jít o úmysl zahladit stopy, varovat podezřelé, činit nátlak na svědky.

1.4 Bezpečnostní rozměr managementu

Přesvědčování o nutnosti brát bezpečnost jako nedílnou součást řízení firmy, organizace nebo instituce by se na tomto místě mohlo zdát jako příslovečné nošení dříví do lesa. Bohužel, zdaleka tomu tak není. A to i přes nesporný růst frekventovanosti této problematiky, ať už v obecném povědomí, tak v odborné diskuzi, nebo na stránkách tisku jako součást hodnocení stavu společenského prostředí v národním a můžeme říci, že i v globálním rámci.

Svět není bezpečný. Stojíme tváří v tvář novým hrozbám, v jejichž důsledku máme nové bezpečnostní potřeby. Pokud chceme efektivně dosahovat svých cílů, musíme se chovat racionálně a brát tyto skutečnosti s přiměřenou vážností. Můžeme říci, že každý manažer je konfrontován s řadou neformálních i formálních důvodů, které ho nutí zamyslet se nad bezpečností, jejím místem v životě firmy, organizace nebo instituce i jejím místem v systému vlastní práce.

V této souvislosti je na místě vyjmenovat tyto důvody [7]:

a) Důvody neformální

- Politické důvody (hrozba mezinárodního terorismu: radikalizace některých politických subjektů a mezinárodních hnutí; prorůstání organizovaného zločinu do politických a ekonomických struktur; slábnoucí státní paternalismus nás nutí více se i v oblasti bezpečnosti starat vlastními silami).

- Hospodářské důvody (extrémní konkurence a vypjaté formy konkurenčního boje, v jehož rámci jsou nezřídka využívány nelegální prostředky).

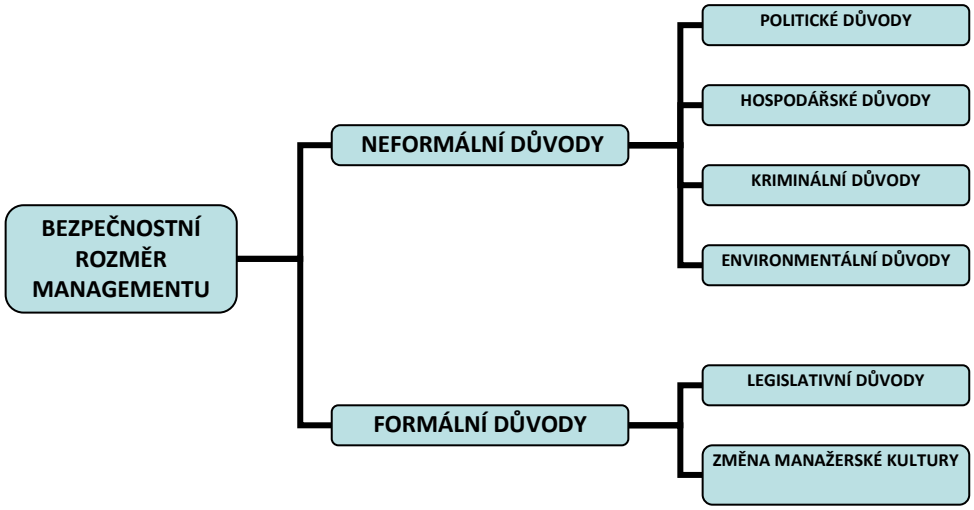
- Kriminální důvody (její nové formy, zahrnující stále širší škálu prostředků, od klasického násilí, nelegálního obchodu, obchodu s nelegálním zbožím a podvodu, po velmi sofistikované, zahrnující zneužití finančně ekonomických mechanismů, prvků informační společnosti a dalších).

- Enviromentální důvody (globální změny klimatu a enviromentální důsledky neuvážené lidské činnosti v minulosti ústí ve zvýšený výskyt živých hrozeb).

b) Důvody formální

- Legislativní důvody (objektivně působící bezpečnostní hrozby nacházejí svůj odraz v právu, ze kterého plyne řada nových závazných povinností, jejichž plnění je zatíženo sankcí).

- Změna manažerské kultury (k ní dochází pod tlakem EU, řady nadnárodních profesních družení a orgánů, mateřských firemních central či zahraničního managementu pracujícího v českém prostředí; pokud je aspekt bezpečnosti přejímán tvořivě a s ohledem na skutečné potřeby a podmínky českého prostředí, je vše v pořádku; pokud je pouze pasivně implementován soubor bezpečnostních procedur podle zahraničního manuálu, nepřispívá to ani k pozitivní změně bezpečnostní kultury, ani k efektivnímu řešení bezpečnostních potřeb, často právě naopak; a naopak jen váhavě a na škodu věci je přijímána myšlenka komplexního outsourcingu bezpečnostního managementu [3]. Neformální a formální důvody jsou také zobrazeny na obrázku 4.



Obrázek 4 Formální a neformální důvody působící na bezpečnostní management [vlastní]

1.5 Srovnání bezpečnosti ve veřejné správě a v komerční sféře

Realizace bezpečnosti ve státním sektoru a v komerční sféře má svá specifika. Následující srovnání se zaměřuje na oba sektory z pohledu specifičnosti úkolů v oblasti bezpečnosti, v oblasti disponibilních zdrojů, prostředků a nástrojů a v oblasti sociálního klimatu a kultury práce.

1.5.1 Bezpečnost ve veřejné správě

Zajišťování bezpečnosti ve státní veřejné správě má svoje zvláštnosti, plynoucí především z těchto skutečností [7]:

a) Specifičnosti úkolů v oblasti bezpečnosti

- stát a státní správa vychází z pojetí bezpečnosti jako veřejného statku a jako jednoho ze základních práv občana;
- stát a státní správa v přístupu k bezpečnosti musí rozlišovat hranici mezi veřejnými a privátními bezpečnostními potřebami;
- stát zajišťuje bezpečnost makrosystému a v rámci něho podmínky pro uplatnění bezpečnostních zájmů privátních subjektů jako podsystém státního makrosystému (jednotlivce i společenství, fyzických i právnických osob, měst a obcí;

- plní svou roli na poli tvorby bezpečnostní legislativy (legislativní iniciativy);
- plní svou roli na poli zajišťování průchodu práva;
- se stále větší naléhavostí se ukazuje bezpečnostní potřeba osobní ochrany osob (před fyzickým útokem, před skandalizačním sběrem informací, rodinných příslušníků apod.).

b) Specifičnost disponibilních zdrojů, prostředků a nástrojů

- stát v otázkách makrosystémových souvislostí bezpečnosti disponuje vrcholnou odpovědností a pravomocí, kterou naplňuje prostřednictvím orgánů státní správy;
- stát disponuje výlučnými nástroji prevence (zdroji informací, nástroji vlastních preventivních bezpečnostních opatření) i represe (retroaktivních bezpečnostních opatření);
- stát může za mimořádných okolností zmobilizovat totální nasazení všech zdrojů a prostředků země. V tomto směru má již za standardní situace k dispozici řadu legislativních a institucionálních nástrojů k řízení a zabezpečení přípravy na takovou eventualitu;
- stát má v souladu se zákonem v zájmu bezpečnosti právo dočasně omezit práva fyzických a právnických osob, nařídit nebo zakázat určité konání;
- stát na základě práva deleguje přiměřenou část svých pravomocí a odpovědnosti na orgány samosprávy. V zájmu toho jim poskytuje organizační a materiální podporu, má právo kontroly, případně i represe;
- za standardní bezpečnostní situace využívá v zájmu bezpečnosti zdrojů státního rozpočtu, včetně případného práva rozpočtové změny v případě potřeby;
- v souladu se zákonem a v kontextu s bezpečnostní situací intervenuje ve prospěch naplnění bezpečnostních potřeb fyzických a právnických osob;
- v souladu s Bezpečnostní strategií a v souladu s platnou bezpečnostní legislativou soustřeďuje svoji pozornost na otázky makrosystémové bezpečnosti, mezi které patří:
  - obrana země (vojenská, diplomatická, informační);

- ochrana vnitřního pořádku a zákonnosti;
- ochrana klíčových materiálních aktiv (hmotných a finančních statků, prvků kritické infrastruktury) i nemateriálních aktiv (životy a zdraví obyvatelstva, životní prostředí, informace, dobrá pověst země) v souladu s platnou bezpečnostní legislativou.

c) Specifičnosti sociálního klimatu a kultury práce

- práce státních orgánů a institucí je i v bezpečnostních otázkách pod vlivem rozporného vztahu správní kontinuity a politické diskontinuity. K překonání této rozpornosti slouží:
  - kontinuita práva;
  - kontinuita politické a správní kultury;
  - kontinuita mezinárodních závazků;
  - personální a organizační kontinuita práce odborného bezpečnostního aparátu, včetně bezpečnostního managementu ústředních správních orgánů a krajských správních orgánů;
- vrcholným nástrojem prosazení této kontinuity je systém volební demokracie, v jehož rámci bezpečnost vystupuje jako vrcholné politikum. V tomto smyslu je bezpečnost ve všech úrovních věcí v pravém slova smyslu veřejného zájmu (a musí jí být stále více, což představuje jeden z důležitých úkolů bezpečnostní komunity).

1.5.2 Bezpečnost v komerčním sektoru

Realizace bezpečnosti v komerční sféře vychází z těchto specifik [7]:

a) Specifičnost úkolů v oblasti bezpečnosti

- jádrem úkolů bezpečnostní práce v komerční sféře je zajistit kontinuitu podnikání a v maximální míře eliminovat ztráty vznikající v důsledku bezpečnostně nestandardních stavů. V tomto smyslu je možné chápat smysl bezpečnostní práce v komerční sféře jako do jisté míry protiklad bezpečnostní práce ve státní a místní správě. V této práci se projevuje rys jisté „sobeckosti“. Bezpečnost je v komerčním sektoru implicitní součástí konkurenčního boje;

- aby tento všudypřítomný duch „dravé, soutěživé sobeckosti“ zcela nepotlačil smysl bezpečnosti jako celospolečenského zájmu, je pro komerční subjekty řada úkonů bezpečnostní práce závazná ze zákona. Jedná se především o povinnosti na úseku:
  - ochrany zdraví a života lidí;
  - ochrany životního prostředí;
  - prevence závažných havárií a přípravy na řešení krizových situací;
  - požární ochrany;
  - ochrany stanoveného okruhu informací;
  - pravidel činnosti pro specifické komerční oblasti (výroba zbraní, bezpečnostního materiálu, nakládání a obchod s nimi; nakládání se zdroji ionizujícího záření; nakládání s infekčním materiálem…)
- do značné míry limitujícím faktorem rozvoje bezpečnosti v komerčním sektoru je absence specializované legislativní normy, která by komplexně řešila problematiku ochrany majetku hmotného i nehmotného (především obchodního tajemství). V důsledku toho panuje:
  - nejednotnost ve výkladu šíře kategorie oprávněného zájmu;
  - značná nejednotnost v přístupech (od budování velmi sofistikovaných bezpečnostních systémů až po absolutní rezignaci na bezpečnost za rámec splnění (často jen formální) povinnosti ze zákona;
  - značná nejednotnost ve výkladu oprávněnosti či neoprávněnosti některých realizovaných bezpečnostních opatření;
  - nadměrná normativní vůle v práci komerčních bezpečnostních služeb (na které řada komerčních subjektů deleguje svoje obecné právo ochraňovat své oprávněné zájmy, avšak zprostředkovaně na ně současně přenáší právní odpovědnost za způsob, jak tento zájem ochrání);
  - bezpečnostní režimová opatření vytvářejí často latentní zdroje konfliktního vztahu v mnoha rovinách: zaměstnanec – zaměstnavatel, prodejce – zákazník, odběratel - dodavatel apod.

b) Specifičnosti disponibilních zdroj, prostředků, nástrojů

- komerční subjekty využívají ve prospěch bezpečnosti kombinace veřejných a privátních zdrojů. Těžiště však spočívá ve využití zdrojů privátních;

- většina komerčních subjektů vnímá bezpečnost jako důležitý problém, avšak, a to na prvním místě, jako problém mimo hranice svého core-business;

- bezpečnost je vnímána jako hodnota nezbytná, ale současně jako hodnota zvyšující náklady core-business. Proto jsou zdroje vyčleněné pro budování bezpečnostního systému firmy (finanční, materiální, lidské i organizační) často poníženy na hranici funkčního minima;

- v důsledku již vzpomenutého legislativního stavu panují značně rozporuplné přístupy k využívání prostředků a nástrojů bezpečnostní práce. Většina firem se v této souvislosti omezuje na:

  - využívání fyzické ostrahy v kombinaci s využitím mechanických zábranných prostředků, poplachových systémů a kamerových systémů. Jejich nasazení se soustřeďuje na ochranu perimetru;

  - bezpečnostní režimová opatření zaostávají;

  - stále je věnována malá pozornost využívání možných synergií (především v souvislostech mezi fungováním režimu obecné bezpečnosti – režimem zaměstnanecké kázně – režimem technologické a provozní kázně, bezprostředně se promítající do objemu a kvality produkce, popřípadě služeb);

  - v oblasti bezpečnostní práce se stále jen ojediněle využívají moderní organizační formy komplexního outsourcingu.

c) Specifičnosti sociálního klimatu a kultury práce

- v komerční sféře se z objektivních důvodů uplatňují velmi progresivní způsoby managementu. To do značné míry otevírá cestu i pro uplatnění progresivních forem bezpečnostního managementu;

- v rozhodovacích procesech mají největší váhu ekonomické kalkulace, což klade před bezpečnostní management potřebu naučit se přesvědčivě argumentačně využívat kategorie z oblasti podnikové ekonomiky a výkaznictví;

- většina komerčních subjektů učinila významný pokrok v zkvalitnění odborné úrovně zaměstnanců působících v oblasti firemního bezpečnostního managementu. Jen v některých případech dosud převažují jiná, např. sociální hlediska;

- v rámci firem v majetku, nebo s majoritou zahraničního vlastníka, nebo firem pracujících na principu komplexní licence („franchisingu“) činí někdy problémy harmonizace bezpečnostní kultury mateřské společnosti s místními potřebami, podmínkami a možnostmi.

Obecně můžeme říci, že je to právě prostředí komerčních subjektů, ve kterém došlo k nejvýraznějším posunům v oblasti bezpečnostní kultury. A to jak ve smyslu docenění významu bezpečnosti, tak i ve smyslu využívání progresivních metod bezpečnostního managementu. Především z této sféry je možno čerpat nové podněty. Jedním z problémů, na který by se bezpečnostní komunita měla soustředit, je zobecňování a šíření těchto podnětů, a zejména zvýšení tlaku na tvorbu dosud chybějících legislativních norem. [7]

1.6 Shrnutí

Tuto kapitolu je potřeba chápat jako vstup do problematiky bezpečnostního managementu. Bezpečnost zde byla představena jako komplexní systém, do kterého zasahují čtyři roviny. První rovina chápe bezpečnost jako nezbytnou podmínku zajištění prosperity společnosti, druhá rovina je spojena s osobou bezpečnostního manažera a výkonem jeho činnosti, třetí rovina je rovina business kontinuity a čtvrtá rovina je rovinou bezpečnostní praxe.

Na schématu virtuálního domu byl demonstrován rozsah bezpečnosti se svými hlavními částmi, mezi které patřily fyzická, informační a administrativní bezpečnost. Důležitost informační bezpečnosti byla detailněji rozebrána v následující podkapitole. Obsahem informační bezpečnosti jsou bezpečnostní politika, bezpečnostní management, systém hlášení bezpečnostních incidentů, bezpečnostní vzdělávání a plány obnovy funkčnosti. Prvky informační bezpečnosti jsou personální bezpečnost, režimová bezpečnost, bezpečnost technických prostředků, bezpečnost programových prostředků, bezpečnost dat, bezpečnost komunikačních systémů a cest, fyzická bezpečnost a aktivní ochrana proti úniku informací a dat.

Následující podkapitola se zabývala cenou informace a následky, které by mohla způsobit nedostupná, vyzrazená nebo změněná informace.

Z pohledu bezpečnostního rozměru managementu byly vyjmenovány neformální a formální důvody, které ovlivňují činnost bezpečnostního manažera. Mezi neformální důvody patří politické, hospodářské, kriminální a enviromentální důvody. Mezi formální důvody řadíme potom legislativní důvody a změnu manažerské kultury.

Poslední kapitola se zabývala srovnáním bezpečnosti ve veřejné správě a v komerčním sektoru, a to z pohledu specifičnosti úkolů v oblasti bezpečnosti, specifičnosti disponibilních zdrojů, prostředků a nástrojů a specifičnosti sociálního klimatu a kultury práce.

2 Hlavní kroky implementace ISMS

Základem systému řízení informační bezpečnosti ISMS (Information Security Management System), zvaného též Systém řízení bezpečnosti informací, jsou normy informační bezpečnosti. Je to něco podobného jako všeobecně známé ISO v řízení kvality, ale v tomto případě jde o řízení bezpečnosti informačních systémů. Důvodů proč je dobré zavádět tyto normy do praxe je víc. Především se tím zavádí pořádek do informací, informačních systémů a jejich vazeb. Zajišťuje se tak i ochrana informací před zničením, odcizením či zneužitím, což zvyšuje důvěryhodnost organizace a zlepšuje její image na veřejnosti. Navíc tím firma získává výhodu při výběrových řízeních. [8]

2.1 Rozhodnutí o zavedení ISMS

Všechno začíná rozhodnutím managementu o zavádění ISMS. Jde o strategické rozhodnutí, neboť se jedná o řídicí systém, který je velmi silně integrován do nejdůležitějších procesů organizace. Bez účinné podpory managementu by nebylo možné ISMS zavést, provozovat a udržovat, natož pak dále zlepšovat a rozvíjet. Při zavádění ISMS by se měl management řídit zásadami, které lze shrnout do 13 bodů:

1. Bezpečnost informací se musí stát prioritou vrcholového vedení.
2. Bezpečnost informací "něco stojí"; investované prostředky by měly produkovat výsledek a ne pouze nákladný konzultační proces.
3. Míra bezpečnosti by měla být úměrná škodě, která může být způsobena.
4. Bezpečnost informací není jednorázový akt, ale nikdy nekončící proces, který musí být řízený.
5. Přehnané nároky na bezpečnost jdou na úkor funkcionality a ve svých důsledcích spíše škodí, než pomáhají.
6. Nejúčinnější je bezpečnost, která se řeší od začátku implementace informačního systému a je jeho integrální součástí.
7. Prolomení bezpečnosti může zabránit kombinace opatření na několika vrstvách (organizační, personální, objektová, technická, komunikační, provozní, programová).

8. Bezpečnost informací je multioborová problematika, kterou nezvládne běžný správce informačních systémů, administrátor ani programátor.
9. Bez důkladného a kontinuálního vzdělávání zaměstnanců v oblasti ISMS nelze provozovat sebelépe implementovaný systém.
10. Bezpečnost informací nesmí být překážkou podnikání a naopak úspěšné podnikání není možné bez zajištění bezpečnosti informací.
11. Bezpečnostní manažer musí být podřízen pouze vrcholovému vedení nebo musí být nezávislý, rozhodně nelze tuto funkci spojovat s provozem informačních technologií nebo informačních systémů.
12. Implementace technologických prostředků není implementací ISMS.
13. Je třeba mít se na pozoru před firmami a jednotlivci, kteří o sobě prohlašují, že ISMS rozumí, většinou to není pravda. [8]

2.2 Stanovení rozsahu a struktury ISMS

Druhým krokem je stanovení rozsahu a struktury ISMS. Jde o to, co se bude chránit a na které oblasti organizace se bude ISMS vztahovat. K tomu je potřebné shromáždit řadu informací a podkladů.

Obecně je potřeba v každé organizaci zajistit vnější ochranu objektů organizace včetně kontrolních propustkových míst. Jedná se o bezpečnostně technické zabezpečení objektů spolu s fyzickou ochranou – službou ochrany majetku a osob. Zkušenosti ukazují, že i u velkých společností je vhodné si tyto služby sjednat smluvně na komerční bázi. Je ale potřeba zaměřit se i na vnitřní ochranu - organizační a režimové zajištění bezpečnosti organizace (podniku). Jedná se o operativní (detektivní či zpravodajskou) ochranu ekonomických zájmu, aktivit a vztahů organizací. [8]

2.3 Bezpečnostní analýza

Základním podkladem pro stanovení bezpečnostního rámce, rozsahu a struktury ISMS by měla být úvodní (vstupní) analýza ISMS.

Bezpečnostní analýza je nezbytným východiskem pro proces syntézy získaných poznatků a vypracování bezpečnostního projektu, jehož úkolem je stanovit naprosto konkrétní opatření, kterými bude dosaženo cíle definovaného bezpečnostní politikou.

Přitom bezpečnost nelze chápat jen jako prostý souhrn použitých prostředků, opatření a postupů, ale jako určitý celek – systém, který je vytvořen za účelem dosažení konkrétního cíle. Prvky tohoto systému vytvářejí a jsou spojeny logickými vazbami, které mají své zákonitosti. Aby tento systém byl funkční, musí být schopen reagovat na změny vnějších podmínek tak, že se jim operativně přizpůsobí, aniž by tím jeho funkčnost byla snížena. Musí však být schopen reagovat nejen na změny, které již proběhly nebo právě probíhají, ale i na změny, které mají nebo mohou nastat v budoucnu. Ten, kdo systém vytváří, realizuje jej a obsluhuje, musí být schopen analyzovat veškeré dostupné údaje nejen ke zjištění stávajícího stavu, ale i ke zjištění budoucího vývoje podmínek. Výsledkem takové analýzy je tedy kromě zjištění současného stavu věcí i zjištění předpokládaného budoucího vývoje formulovaného v podobě bezpečnostní prognózy. [5]

Pro provádění bezpečnostní analýzy obecně nebyly vypracovány žádné speciální techniky a standardy a každá poradenská firma kombinuje běžně používané techniky s vlastními postupy. Je třeba si uvědomit, že v oblasti zabezpečení organizací nedostává analytik všechny informace v podobě, která by se dala přesně kvantifikovat. Zásadní informace pro bezpečnostní expertízu organizací nejsou v podobě přesných čísel, což samozřejmě omezuje možnosti výběru a použití různých technik analýzy a prognózy. Lze říci, že každá odborná poradenská organizace v oblasti zabezpečení si vypracovala vlastní postupy, které jsou modifikací běžně užívaných technik strategické analýzy v jiných oblastech (např. v oblasti ekonomické a finanční). Mezi takové analýzy patří např. analýza PEST, modifikovaná analýza zdrojů a zejména analýza SWOT. Velmi dobře použitelné jsou i některé metody popisné statistiky, např. Paretův diagram a jiné druhy diagramů.

Součástí bezpečnostní analýzy jsou [5]:

- **Situační analýza** - situační analýza umožňuje orientaci v problému, který má být z bezpečnostního hlediska řešen.

- **Analýza rizik** - každá bezpečnostní činnost, má li být prováděna kvalifikovaně na profesionální bázi, a má-li být tedy úspěšná, musí vycházet z komplexní bezpečnostní analýzy, kde prioritní je analýza rizik – tedy ocenění rizik. Bez provedení této části analýzy by bezpečnostní analýza nebyla ani kompletní ani použitelná pro funkční řešení problému bezpečnosti. Analýza rizik je použitelná (a

nutná) při posuzování a analyzování celkové bezpečnosti organizace či instituce. Analýza rizik musí dát odpověď na tři základní otázky:

- jaká rizika – hrozby mohou nastat
- jaká je pravděpodobnost, že rizika nastanou a dojde k bezpečnostnímu konfliktu
- jaké budou následky, když bezpečnostní konflikt nastane

Rizikovou bezpečnostní analýzu je třeba provádět z následujících hledisek:

- hmotný majetek
- nehmotný majetek
- osoby
- režim -veřejný pořádek
- organizace provozu
- požární podmínky
- bezpečnost zdraví při práci a hygiena práce
- životní prostředí

- **Hodnotová analýza** - hodnotová analýza by měla zahrnout zhodnocení hodnot, které mají být nebo jsou předmětem ochrany, jaké hodnoty lze příslušným bezpečnostním opatřením zajistit, předpokládané nebo stávající náklady na ochranu, a v neposlední řadě vyhodnocení těchto vzájemných vztahů, tedy zhodnocení efektivity a lukrativity bezpečnostních opatření.

Bezpečnostní analýzy, a následně i prognózy, plány či projekty lze dělit na:

a) Komplexní - komplexní analýzy (rovněž prognózy, plány a projekty) řeší celý komplex zajištění ochrany bezpečnosti a s tím spojených rizik.

b) Dílčí - dílčí analýzy (prognózy, plány a projekty) tvoří výsek určitého komplexu ochrany bezpečnosti. Jsou realizovány v různých úrovních. Může se jednat např. o dílčí analýzu (prognózu, plán, projekt apod.) vnější ochrany objektu, vnitřní ochrany objektu, ochrany utajovaných skutečností, ochrany informací, ochrany personální bezpečnosti apod.

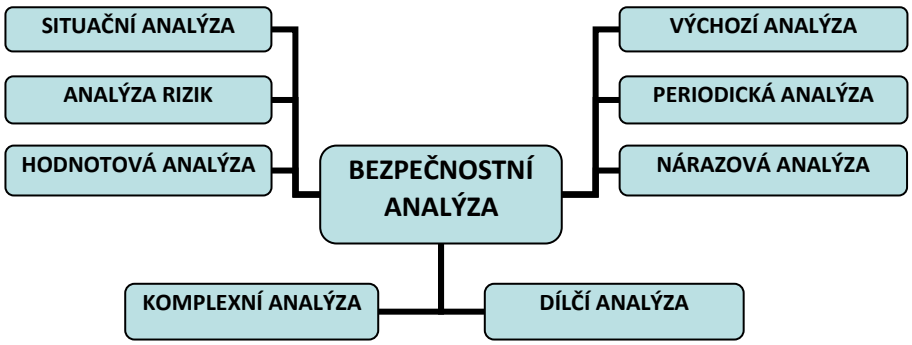
Z hlediska toho, kdy bezpečnostní analýzu provádíme, můžeme tyto dělit na:

a) Výchozí - jedná se o analýzu (prognózu, plán, projekt) na počátku řešení daného problému ochrany majetku a osob.

b) Periodická - analýzu (prognózu, plán, projekt) nestačí provést na počátku řešení předmětného úkolu ochrany majetku a osob, ale je nutné tuto v určitých periodách opakovat.

Nárazová - jedná se o analýzu (prognózu, plán či projekt) prováděnou v souvislosti s nastalou změnou bezpečnostní situace, v souvislosti se vznikem mimořádných událostí apod. [5].

Jednotlivé typy a druhy analýz jsou pro zopakování znázorněny na obrázku 5.



Obrázek 5 Rozdělení bezpečnostní analýzy z různých pohledů [vlastní]

2.4 Bezpečnostní audit

V případě bezpečnostního auditu uvažujeme spíše o ocenění kvality již vykonávaných bezpečnostních opatření. Audit bezpečnostních opatření se provádí pro potřeby sjednání pojištění, při pojistné události, při rozhodování, zda si ponechat stávající bezpečnostní službu či uzavřít smluvní vztah s jinou apod. Bezpečnostní audit je třeba periodicky opakovat a je třeba jej opětovně provést vždy při vzniku nových bezpečnostních rizik, hrozeb a ohrožení. Je žádoucí, aby bezpečnostní manažer – bezpečnostní management zajistil nezávislý bezpečnostní audit na smluvním (komerčním základě) specializovanou firmou (společností, agenturou, kanceláří). Významnými subsystémy bezpečnostního auditu jsou subsystém ochrany majetku, ochrany osob – personální bezpečnosti, ochrany KNOW HOW, ochrany technologických provozů a ochrany obchodní bezpečnosti. Nejvýznamnějším subsystémem pro ochranu podnikatelského subjektu je

ovšem ochrana informační bezpečnosti – informačních systémů. [5]

Při řešení problematiky bezpečnostních auditů, stejně jako při bezpečnostních analýzách, je třeba vycházet z jistého jejího obsahu, stanoveného postupu. Nejprve je potřeba formulovat problém, tedy k čemu má být bezpečnostní audit směrován, jakým způsobem bude bezpečnostní audit zajišťován, zda bude bezpečnostní audit řešen jako komplexní, či dílčí. Následuje úvaha, na základě které bychom se měli zamyslet nad tím, jakým způsobem přistoupíme k řešení problému. Je potřeba stanovit si zásady a požadavky kladené na řešený problémový okruh a na bezpečnostní zájmy klienta s ohledem na právní řád dané problematiky. Odtud postoupíme ke sběru informací, který můžeme rozdělit do tří oblastí, a to informací od vedení organizace (společnosti, firmy), informací od zaměstnanců firmy a informací zvenčí firmy. Tyto informace je dále nutné roztřídit a vybrat podle kritérií vycházejících z formulace problémů a vytyčených cílů a z úvahy o přístupu k řešení problémů. Dalším krokem je studium a rozbor vytříděných informací. Součástí tohoto kroku je rozbor hledisek a kritérií kladených na ochranu bezpečnosti a bezpečnostních zájmů; analýza rizik, ke kterým je třeba přihlížet a která je třeba považovat za kritéria hrozícího nebezpečí pro bezpečnost a bezpečnostní zájmy klienta; analýza současného stavu v zajišťování bezpečnosti a bezpečnostních zájmů; zhodnocení skutečného stavu naplňování bezpečnostních cílů, mezi které patří objektivní zhodnocení rizik, žádoucí bezpečnostní efekt, požadovaný objem bezpečnostních služeb a způsob, kvalita i kvantita poskytovaných bezpečnostních služeb. Posledním krokem je zobecnění a interpretace zpracovaných informací s ohledem na vypracování výstupu bezpečnostního auditu. Součástí výstupu je stanovení hledisek a kritérií žádoucího stavu bezpečnosti a naplňování bezpečnostních zájmů; zjištění kvantity a intenzity rizik hrozících bezpečnosti a jednotlivým bezpečnostním zájmům; zjištění a posouzení souladu mezi stavem skutečným (zjištěným) a stavem žádoucím zjištění rozpornosti mezi těmito stavy a navržení opatření. [5]

2.5 Bezpečnostní prognóza

Bezpečnostním prognózováním rozumíme proces (činnost) směřující k vypracování bezpečnostní prognózy. Bezpečnostní prognózu je pak třeba chápat jako výsledný produkt procesu nazývaného bezpečnostní prognózování. Jde tedy o více či méně přesný odhad vývoje v oblasti zajištění ochrany bezpečnosti a bezpečnostních zájmů

podnikatelského subjektu (v některých případech i občana – klienta). Nelze se ale omezit pouze na stanovený objekt, pro nějž má být zajišťována soukromě bezpečnostní ochrana, ale je třeba brát v úvahu i prognózu vývoje bezpečnosti a veřejného pořádku v okolí chráněného objektu. Bezpečnostní prognóza je pokračováním bezpečnostní analýzy. [5]

Schopnost prognózovat přesně a konzistentně je velmi důležitá, avšak naprostá přesnost je nedosažitelná (v opačném případě by potřeba formulace bezpečnostní politiky – bezpečnostního plánu byla výrazně nižší). Je nutné udělat maximum toho, co za daných podmínek je subjekt, který formuluje svoji bezpečnostní politiku a realizuje ji, schopen udělat. Prognóza také nemůže být zredukována jen na mechanické cvičení. Je naivní se domnívat, že budoucnost bude připomínat minulost a současnost, na jejichž základě formulujeme své cíle a prostředky jejich dosažení, v budoucnosti. Problém kvalitního a účinného zajištění bezpečnosti spočívá ve schopnosti těch, co rozpracovávají bezpečnostní politiku do podoby konkrétního bezpečnostního projektu a kteří se zabývají realizací bezpečnostního projektu, že se zabývají nejen pravděpodobnými budoucími situacemi (proces prognózování), ale i situacemi méně pravděpodobnými nebo nepravděpodobnými (proces posouzení hrozeb – analýza rizik). Jestliže dokážou předvídat možné budoucí problémy, je pravděpodobné že nepřehlédnou a nepodcení signál nebezpečí v okamžiku, kdy přijde a jejich reakce bude rychlejší. [5]

Prognózu bezpečnosti podniku je třeba chápat jako pokračující proces s informacemi získanými jako výstup bezpečnostní analýzy či bezpečnostního auditu, jako odůvodněné předvídání vývoje bezpečnosti a to na podkladě informací získaných bezpečnostní analýzou nebo bezpečnostním auditem. Prognóza napomáhá sociální kontrole a rozšiřuje sféru sociální kontroly, určuje možnosti zajištění souladnosti stavu skutečného a stavu žádoucího, přičemž napomáhá odstraňování rozporností mezi těmito stavy. Pomocí prognózy je možné stanovit důsledky různých přístupů k zajišťování ochrany bezpečnosti a bezpečnostních zájmů klienta. [5]

2.6 Stanovení bezpečnostní politiky

Dokument Bezpečnostní politika tvoří základní materiál, od něhož se odvíjejí další projekty zajištění ochrany bezpečnosti podniku, podnikatelského subjektu. Účelem dokumentu je prosadit důvěryhodný informační systém. Bezpečnostní politika by měla definovat strukturu správy programového systému, zodpovědnosti jednotlivců i skupin,

resp. týmů v organizaci a celkové bezpečnostní cíle. Důležitou roli zde hraje zdůraznění úlohy jednotlivce a osobní zodpovědnosti každého zaměstnance organizace zavádějící bezpečný informační systém, proto je žádoucí zavést detailní účtování činností jednotlivců. Bezpečnostní politika by měla pokrýt všechny zdroje informačního systému v organizaci, tj. technické a programové vybavení, informace, personál atd. Jsou-li některé kritičtější, mělo by to být jednoznačně stanoveno. Výsledkem řešení by měl být Program informační bezpečnosti, což chápeme jako dokument koncepčního charakteru, který určuje metody a podmínky reálného řešení informační bezpečnosti a je schválený vrcholovým vedením organizace zadavatele.

Program by měl obecně zahrnovat [3]:

- cíle v oblasti ISMS, celkovou strategii a rámec zásad ISMS;
- odpovědnost za naplňování cílů, prostředky k jejich naplňování a časové období pro jejich naplňování;
- požadavky vyplývající z hlavních činností organizace, legislativní, normativní požadavky a smluvní závazky;
- organizační a odpovědnostní struktura a vazby informační bezpečnosti v systému řízení organizace;
- specifikace platných oprávnění a jiných předpisů;
- metody a způsoby ochrany majetku a osob, informací a informačního sytému na fyzické úrovni, ale i na úrovni organizační a logické;
- způsoby a postupy řešení, časové a finanční podmínky řešení;
- zásady havarijního plánování a řízení bezpečnostních incidentů.

Velmi významnou součástí bezpečnostní politiky podnikatelského subjektu, organizace či instituce je bezpečnostní informační politika. Bezpečnostní informační politikou v rámci řízení organizace budeme rozumět souhrn organizačních a řídících opatření, norem, standardů a pravidel, jejichž východiskem je ohodnocení informací jako jednoho z aktiv organizace, zhodnocení jejich ohrožení, stanovení rizik a návrh jejich ochrany v rámci technických, technologických, organizačních, personálních a dalších opatření jako nedílné součásti systému řízení organizace a koncepce jejího rozvoje. Předmětem nebo objektem ochrany je tedy informace a informační systém. V této souvislosti je

vhodné si uvědomit rozdíl mezi obecnou bezpečnostní politikou organizace a bezpečnostní informační politikou. Pojem bezpečnostní politika organizace je pojmem obecnějším, zahrnujícím i jiné stránky bezpečnosti organizace než bezpečnost informací. V praxi dochází k tomu, že smíšení pojmů neumožňuje dostatečně postihnout odlišnosti informační technologie od ostatních bezpečnostních funkcí a charakteristik organizace. Je tedy třeba přesně vymezit informace a informační systém v dané organizaci a určit souvislosti s jinými prvky komplexu organizace. Bezpečnostní politika nepochybně specifikuje míru závažnosti a obsah určité složky ochrany pro konkrétní informační systém. Bezpečnostní politika systému zabývajícího se citlivými daty (např. zpravodajské instituce) bude asi klást největší důraz na důvěrnost, naproti tomu bezpečnostní politika systému komerční firmy na integritu, telefonní společnosti na dostupnost apod. Bezpečnostní politika má obvykle charakter povinných zásad, měnitelných pouze několika správci. Můžeme na ni pohlížet jako na normy, pravidla a praktiky definující způsob zpracování, ochrany a distribuce citlivé informace v rámci činnosti informačního systému. [3]

2.7 Bezpečnostní projekt

Bezpečnostní projekt představuje nezbytnou dokumentaci (písemnou i grafickou) důvěryhodného, účinného a efektivního systému zabezpečení ochrany bezpečnostních zájmů příslušného konkrétního podnikatelského subjektu nebo jeho organizační části. [4]

Rozsah a složitost přípravy a sestavení plánu (projektu) jsou přímo závislé na velikosti a složitosti plánovaného cíle. Protože se zabýváme otázkou komplexního zabezpečení organizace, jde nám především o komplexní bezpečnostní projekt organizace, který bude zahrnovat řadu dílčích cílů. K jeho dokončení bude potřeba více lidí, v rámci něj bude řešeno více úkolů a některé i souběžně, což si vyžádá vysoké nároky na koordinaci jednotlivých činností. Bezpečnostní projekty, podobně jako ostatní druhy projektů, se vyznačují některými charakteristickými znaky. Jedná se především o tyto hlavní znaky [9]:

- projekty mají přesně a srozumitelně definované cíle,
- projekty obsahují jednoznačné termíny k jejich dokončení,
- obsahují množinu činností (úkolů) propojenou vzájemnými vazbami,

- pro jejich realizaci jsou vyčleněny zdroje (obvykle v podobě rozpočtu),
- obsahují seznamy pracovníků odpovědných za realizaci projektu,
- realizují se zpravidla projektové týmy (protože jejich splnění nelze zajistit jediným člověkem).

Cíle projektu vychází z cíle definovaného již při zpracování bezpečnostního auditu. Projekt musí určit, jaké konkrétní technické prostředky a režimová opatření budou pro ochranu objektu použity a jaký bude jejich vzájemný poměr a rozsah. Tento poměr a rozsah je zcela závislý na specifických podmínkách organizace, cíli, kterého má být dosaženo, a dalších aspektech. [9]

V souvislosti s realizací bezpečnostních opatření vyvstává otázka, kdo fakticky v rámci realizace tato opatření provede a co k realizaci bude zapotřebí, tedy jaké materiální a personální požadavky jsou kladeny a z jakých zdrojů je organizace získá. Příslušné zdroje mohou být buď vlastní, nebo externí a v praxi je nejčastěji použito obou v různém poměru. Je pravděpodobné, že např. zpracování bezpečnostního projektu i jeho realizace bude zčásti nebo zcela ponechána na expertních dodavatelích. Není ale vyloučeno, že organizace zrealizuje projekt z vlastních zdrojů, a sníží tak jeho ekonomickou náročnost. Využití vlastních zdrojů také může usnadnit a zjednodušit realizaci projektu, Je třeba ale mít na mysli, že využití vlastních sil nesmí být na úkor kvality provedené práce. [9]

Pro zdárnou realizaci bezpečnostního projektu musí být určeny konkrétní osoby k provedení jednotlivých úkolů obsažených v bezpečnostním projektu. Zde je určení konkrétních osob a jejich odpovědnosti za včasnou realizaci konkrétních úkolů naprosto nezbytné, protože v realizační fázi musí být všem jasné, kdo a kdy bude určitý úkol vykonávat a kdo za splnění bude odpovědný. Konkretizace úkolů nepředstavuje atomizaci jednotlivých dílčích úkolů (nejde tedy o popis jednotlivých kroků např. při montáži zařízení), ale jedná se o konkretizaci na jednotlivá technická a režimová opatření, ze kterých bude vybudován celek. Jestliže je součástí projektu realizovat systém funkční ostrahy objektu, pak jednotlivé dílčí úkoly budou představovat např. vypracování směrnic pro výkon ostrahy, provedení školení osob, zavedení kontrolního systému výkonu ostrahy apod. [9]

2.8 Implementace a provoz ISMS

První zatěžkávací zkouškou správné realizace bezpečnostního projektu bývá jeho implementace. Fáze přijetí a ztotožnění se určených osob a ostatních zaměstnanců organizace s bezpečnostním projektem je velmi citlivá. Musíme se uvědomovat, že realizace takového projektu, jakým je bezpečnostní projekt představuje provedení řady změn v zavedených stereotypech organizace. Změny mají v mnoha případech povahu organizačních změn dosavadních režimových postupů, zvýšení odpovědnosti a povinností řadě zaměstnanců, zavedení určitých omezení pro pracovníky (režim vstupu a pohybu v objektu) apod. Ukazuje se, že při implementaci výsledků projektu musí být zvolen správný způsob použití dvou prostředků, a to komunikace a osvěty. Cílem komunikace s příslušnými osobami v organizaci je přenést na ně znalost o bezpečnostní politice a seznámení s provedenými změnami. Cílem podnikové osvěty je příslušným osobám vysvětlit způsoby, jak efektivně a bezbolestně aplikovat zavedená opatření do jejich každodenní praxe. Aby implementace byla úspěšná, je vhodné o smyslu a významu bezpečnostního projektu s příslušnými osobami mluvit již od okamžiku, kdy začínají práce na jeho přípravě. Organizace se dříve seznámí s argumenty, které jsou namítány proti projektu a získá tak více času na přesvědčení zaměstnanců o správnosti realizace projektu. [9]

Aby mohl být ISMS úspěšně zaveden do praxe, je nutno zajistit minimálně toto [8]:

- zpracovat plán zvládání rizik, s ohledem na priority, odpovědnost a pravomoci
- zajistit lidské zdroje a finanční prostředky pro plnění jednotlivých programů řízení rizik, provoz a implementaci ISMS
- připravit programy vzdělávání a zvyšování bezpečnostního povědomí zaměstnanců
- implementovat zvolená opatření prostřednictvím programů řízení rizik
- popsat procesy pro řízení informační bezpečnosti a uplatnit je v provozu organizace
- řídit lidské a finanční zdroje

- implementovat postupy a procesy včetně nezbytných kontrol pro denní monitorování a kontrolu informační bezpečnosti, zajistit rychlou detekci a reakci na bezpečnostní incidenty a zvyšovat účinnost ISMS.

2.9 Monitorování a přezkoumávání ISMS

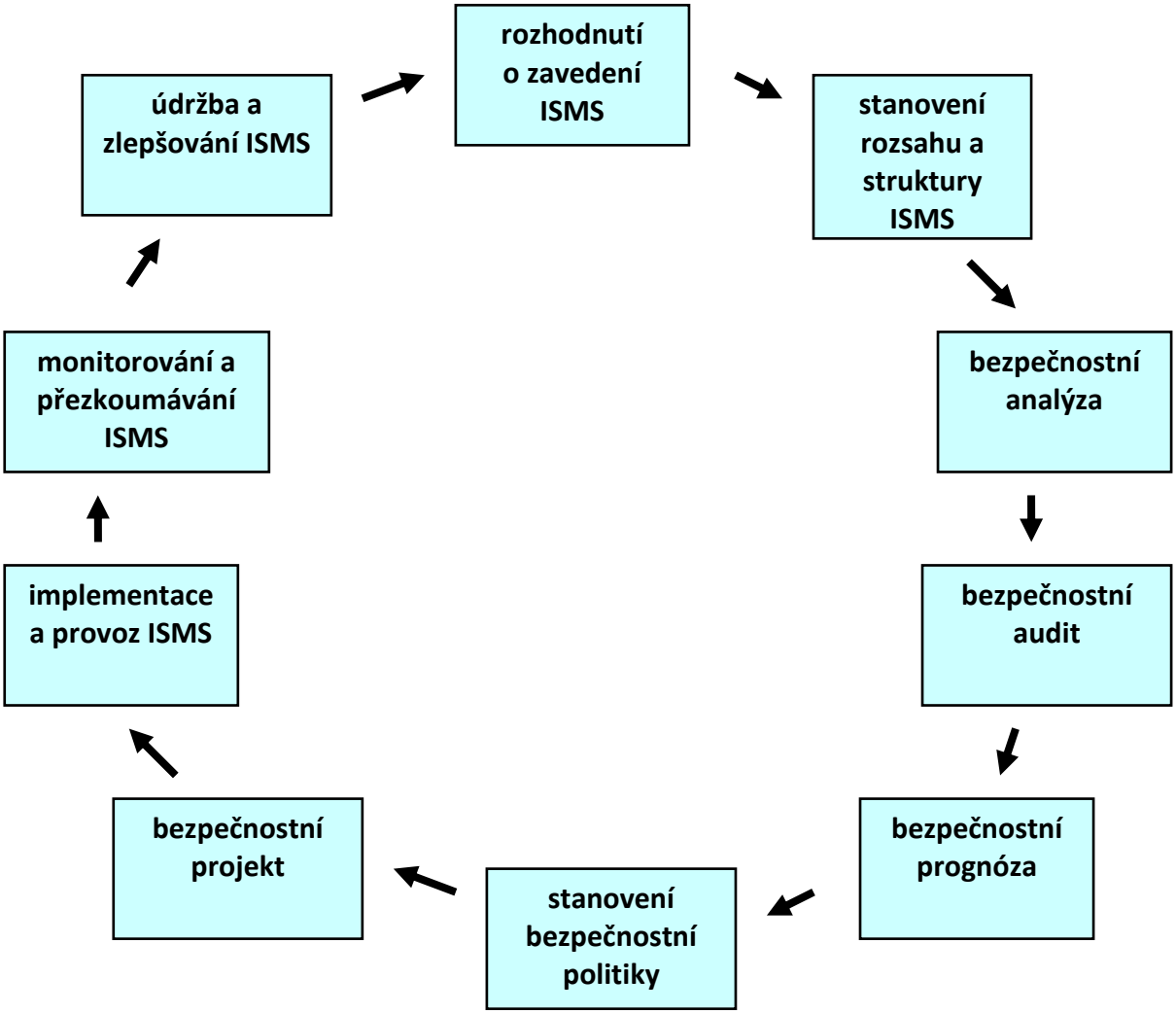
Monitorování a přezkoumávání ISMS je dalším důležitým krokem. Organizace musí monitorovat a provádět další kontroly a testy tak, aby se především identifikovaly chyby ve zpracování informací a odhalily bezpečnostní incidenty i pokusy o narušení bezpečnosti. Monitorováním se odhalí též slabá místa v ISMS a zjistí se, zda nastavené bezpečnostní procesy a činnosti fungují správně. Poté lze určit způsob eliminace bezpečnostních problémů s ohledem na priority organizace.

Je vhodné používat různé druhy testování pro odhalování bezpečnostních problémů, např. penetrační testy apod. Také je nutné pravidelně ověřovat ISMS z hlediska plnění bezpečnostní politiky, cílů a programů pro snižování rizik a s ohledem na výsledky bezpečnostních auditů, incidentů, příp. podnětů zákazníků a jiných stran. Rovněž pravidelně je třeba hodnotit úroveň přijatých rizik s ohledem na změny v organizaci, technologiích, podnikatelských cílech a procesech i změnách vnějšího prostředí. Požadavkem je také pravidelně provádět interní audity ISMS - sestavit plán auditů (povinný záznam), provádět přezkoumávání ISMS vedením (minimálně 1 x ročně) a zaznamenávat všechny činnosti a incidenty, které by mohly mít vliv na efektivitu nebo výkon ISMS. [8]

2.10 Údržba a zlepšování ISMS

Údržba a zlepšování ISMS je posledním krokem a subsystémem ISMS. Zahrnuje identifikaci a evidenci možností pro zlepšování, realizaci nápravných a preventivních opatření na základě zjištěných neshod v ISMS. Také je nutné projednávat a seznamovat všechny zainteresované strany s výsledky přijatých opatření, zajistit, aby navrhovaná zlepšení dosáhla předpokládaných cílů. Proto je třeba popsat a zavést procesy, které umožní provádět nápravná opatření zaměřená na identifikaci neshod, nedostatků a bezpečnostních incidentů, zjišťování jejich příčin a přijímání a kontrolu takových nápravných opatření, aby se jejich opakování stalo méně pravděpodobným. A také přijímání preventivních opatření na základě analýzy rizik a zkušeností z jiných organizací. [8]

Schéma hlavních kroků implementace systémů řízení bezpečnosti informací znázorňuje obrázek 6. Na obrázku jsou uvedeny jednotlivé kroky, které byly detailně popsány v předchozích kapitolách, a posloupnost jednotlivých kroků, jak by měly následovat za sebou v rámci celého procesu implementace.



Obrázek 6 Schéma hlavních kroků implementace ISMS [vlastní]

2.11 Shrnutí

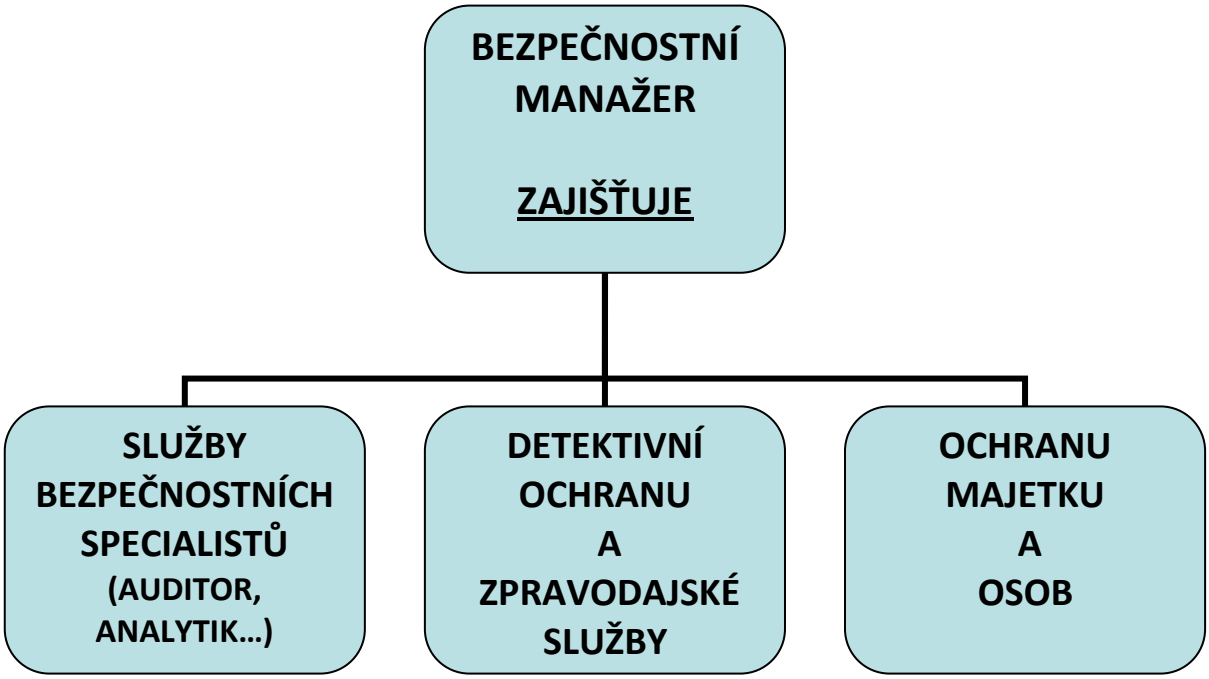
V rámci této kapitoly byly důkladně vysvětleny a popsány hlavní kroky při implementaci systému řízení bezpečnosti informací v organizaci. Byl nalezen vhodný postup celého procesu, který je reprezentován pevně danou posloupností jednotlivých kroků. Vše začíná rozhodnutím managementu společnosti o zavádění ISMS, kde je potřeba řídit se třinácti důležitými body, jež jsou uvedené v podkapitole 2.1. Následuje stanovení rozsahu a struktury ISMS, tedy co se bude chránit a v na které oblasti organizace se bude ISMS vztahovat. Dalším krokem je bezpečnostní analýza, která se skládá ze situační analýzy, analýzy rizik a hodnotové analýzy. Čtvrtým krokem je bezpečnostní audit uvažovaný jako ocenění kvality již vykonávaných bezpečnostních opatření pro potřeby sjednání pojištění apod. Dalším v pořadí je bezpečnostní prognóza, tedy více či méně přesný odhad vývoje v oblasti zajištění ochrany bezpečnosti a bezpečnostních zájmů organizace. Ze všech předchozích kroků potom vychází stanovení bezpečnostní politiky jako základního materiálu, od něhož se odvíjí další projekty zajištění ochrany bezpečnosti podniku. Z bezpečnostní politiky vyplyne bezpečnostní projekt, který určí, jaké konkrétní technické prostředky a režimová opatření budou pro ochranu objektu použity a jaký bude jejich vzájemný poměr a rozsah. Součástí bezpečnostního projektu jsou osoby zodpovědné za realizaci dílčích plánů projektu a posloupnosti těchto plánů včetně časových termínů. Na základě bezpečnostního projektu se potom přistupuje k implementaci ISMS a zavedení do provozu. Po úspěšném dokončení tohoto kroku je potřeba zahájit monitorování celého systému a přezkoumávání jeho nastavení. Z těchto zkoumání vyplynou návrhy na zlepšování ISMS, které jsou předány k posouzení managementu a pokud dojde ke schválení předložených inovací, následuje znovu přesně daná posloupnost jednotlivých kroků obecné implementace systému řízení bezpečnosti informací.

3 Bezpečnostní manažer v instituci

Bezpečnostní manažer je specializovaná funkce s touto pracovní náplní [6]:

1. Tvorba a správa bezpečnostních politik organizace a souvisejících norem.
2. Dohled nad výběrem programových prostředků pro organizaci.
3. Podpora implementace a správy bezpečnostních informačních softwarových systémů.
4. Poskytování rad, návodů a pomoci uživatelům IS v oblasti bezpečnosti IS.
5. Určování běžných bezpečnostních funkčních procesů IS a pomoc při vývoji automatizovaných nástrojů pro jejich podporu.
6. Dohled nad informačním systémem, kontrola aplikací.
7. Monitoring sítě a jednotlivých složek IS. Kontrola dodržování interních norem pro IS, smluv a zákonů v organizaci.
8. Příprava, řešení a kontrola bezpečnostních projektů v organizaci.
9. Pomoc při analýze manuálních bezpečnostních funkcí IS a poskytování podkladů pro doporučení a zpráv pro vedení organizace.
10. Udržování, modifikace a vylepšování automatických funkčních bezpečnostních systémů pro testování, hodnocení, správu rizik, hodnocení hardware a software a řízení přístupu.
11. Provádí analýzu rizik a navrhuje účinná opatření k minimalizaci rizik a hrozeb pro organizaci.
12. Provádí vyšetřování bezpečnostních incidentů, tvorba dokumentace a incidenčních zpráv. Navrhuje účinná opatření k minimalizaci ztrát.
13. Shromažďování, kompilování a generování informačních zpráv o bezpečnostních funkcích a instruktážních školení pro zaměstnance organizace.

Obecnou představu o oblastech činností, které zajišťuje bezpečnostní manažer, může poskytnout obrázek 7.



Obrázek 7 Náplň činností bezpečnostního manažera [2]

3.1 Formální a neformální stránka jmenování bezpečnostního manažera do funkce

Účinnost a efektivita bezpečnostního managementu a v důsledku toho i bezpečnostní práce ve firmě, organizaci či instituci je přímo podmíněna rolí odpovědného manažera.

Síla role bezpečnostního manažera firmy, organizace či instituce odvisí od dvou základních skutečností [7]:

1. od způsobu začlenění bezpečnostního manažera do organizační struktury firmy, organizace, instituce;
2. od síly osobnostních předpokladů k sehrání této role na straně manažera samého.

Způsob začlenění bezpečnostního manažera do organizační struktury firmy, organizace, instituce je různý. V každém případě je nutno vidět vždy dvě stránky tohoto začlenění – **formální a neformální**.

Formální stránku rozhodujících podmínek pro sehrání role bezpečnostního manažera firmy, organizace, instituce v systému bezpečnostního managementu tvoří [7]:

- přiměřený akt jeho formálního jmenování a uvedení do pozice;
- stanovení odpovědnosti a pravomocí;
- přiměřená vnitřní publicita věnovaná tomuto aktu, veřejná deklarace jeho postavení z hlediska odpovědnosti a pravomocí;
- striktní stanovení jeho pozice v organizační struktuře firmy, organizace, instituce především z hlediska subordinace (jeho podřízenosti a nadřízenosti);
- organizační zařazení do vrstvy top managementu, nebo alespoň zajištění formálního i neformálního práva volné a přímé komunikace s touto organizační vrstvou.

V praxi tyto podmínky nejsou vždy zdaleka naplněny. Jen z pohledu formálního „názvu“ funkce a jejího personálního zajištění. Nejčastěji se setkáváme s těmito variantami [7]:

a) bezpečnostní manažer je oficiálně bezpečnostním manažerem a plní svoji roli v managementu bezpečnosti firmy, organizace či instituce ve větší či menší shodě s tím, co bylo řečeno výše;

b) ve firmě, organizaci či instituci je jmenován bezpečnostní ředitel v souladu s požadavky zákona 412/2005 Sb. a souběžně s tím plní funkci bezpečnostního manažera shoda popsaném širším rámci;

c) určení zaměstnanci, zastávající jinou odbornou pozici v managementu firmy, organizace či instituce, plní funkci bezpečnostního manažera i bezpečnostního ředitele jako tzv. kumulovanou funkci (bezpečnostní manažer není výhradním obsahem jejich práce);

d) bezpečnostní management je roztříštěn obsahově (zpravidla po „tradičních“ bezpečnostních odbornostech – PO, BOZP, ostraha a bezpečnostní technologie, bezpečnost IS, ochrana utajovaných informací, ochrana osobnících údajů, vnitrofiremní bezpečnostní investigativní činnost atd.) i personálně. Roli bezpečnostního manažera v takto nebo jinak vymezených dílčích obsahových rámcích plní různí zaměstnanci

v manažerských pozicích (personální manažer, manažer IT, manažer správy objektu, manažer vnitrofiremních služeb apod.).

Neformální stránka začlenění bezpečnostního manažera do organizační struktury firmy, organizace, instituce spočívá [7]:

- ve váze, která je otázkám bezpečnosti přisouzena, a jak citlivé je celé top vedení na podněty v této oblasti;
- v ochotě top managementu z toho plynoucí vyčlenit na adresu bezpečnosti přiměřený objem sil a prostředků;
- v reálných možnostech uplatnění funkčního a odborného vlivu na život, především na průběh a řízení bezpečnostních procesů.

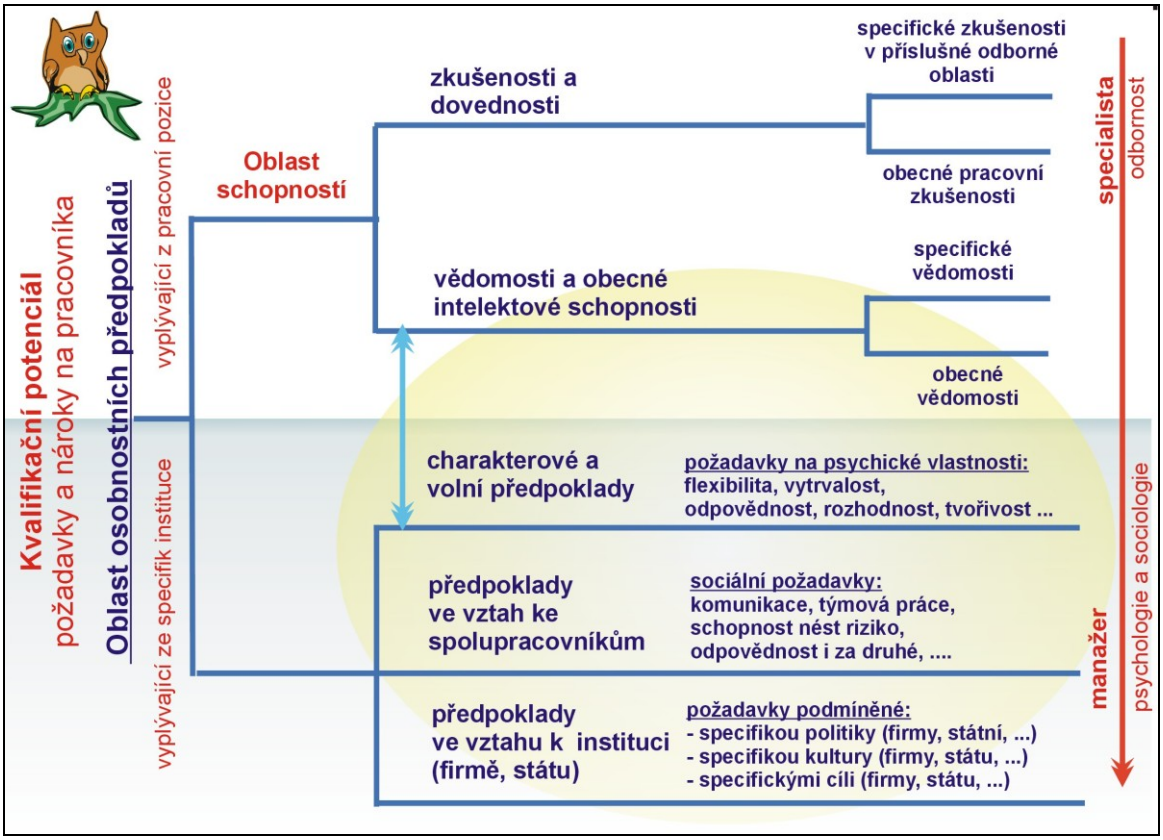
Řešení otázek, které tvoří základ obsahu neformální i formální stránky začlenění bezpečnostního manažera do organizační struktury firmy, organizace, instituce, se přímo odvíjí od míry strategického zaměření na bezpečnost, což představuje koncentrát funkcí Bezpečnostní politiky. S jistou mírou zjednodušení můžeme konstatovat, že absence Bezpečnostní politiky jako strategického programového dokumentu na úrovni top managementu firmy, organizace, instituce je symptomem všech shora naznačených problémů.

Samozřejmě, že i v případě silné zaměřenosti firmy, organizace, instituce na bezpečnost, dobré Bezpečnostní politiky rozpracované do reálného a systematicky realizovaného harmonogramu její praktické implementace a při optimálním začlenění bezpečnostního manažera do organizační struktury záleží mnohé od síly jeho osobnostních předpokladů. [7]

3.2 Aspekty ovlivňující výkon bezpečnostního manažera

Bezpečnostní manažeři společností (firem, organizací a institucí) tvoří zvláštní skupinu soukromě bezpečnostních specialistů. Zajišťují bezpečnost uvnitř vlastní organizace. Nejedná se tedy o poskytování služeb zákazníkům (klientům), ale jde o zaměstnanecký poměr v příslušné organizaci. Role bezpečnostního manažera je velmi zodpovědná, náročná a nevděčná. Je doprovázena vysokými nároky kladenými na něho a zároveň vysokým stupněm samoty. Tyto aspekty vychází ze samotné povahy bezpečnosti – je

složitá a komplexní (technologie, management, lidé uvnitř i vně organizace, vysoká vynalézavost a účinné prostředky protivníků), dynamická, s vysokou mírou neurčitosti, neuspořádanosti a chaosu, těžko ekonomicky zdůvodnitelná a obhajitelná. Pro výběr bezpečnostního manažera neexistují žádná univerzální pravidla. Klademe na něj požadavky jako na každého jiného manažera a zároveň musíme brát v úvahu všechny aspekty instituce, ve které má působit [3]. Obrázek 8 demonstruje různorodost požadavků a nároků na kvalifikační potenciál bezpečnostního manažera. Na obrázku jsou schopnosti pracovníka rozděleny do dvou oblastí podle toho, zda vyplývají z pracovní pozice nebo ze specifik instituce. Jednotlivé oblasti jsou potom podrobněji popsány.



Obrázek 8 Kvalifikační potenciál [3]

Bezpečnostní manažer musí být osoba, která disponuje rozsáhlými a různorodými znalostmi a zkušenostmi. K jejich získání musí využívat všech možných zdrojů, mezi které patří rozsáhlé interdisciplinární teoretické vědomosti, osobní, životní a profesní zkušenosti, psychologické znalosti a zkušenosti, zprostředkované zkušenosti zachycené v literatuře a jiných informačních zdrojích. Práce bezpečnostního manažera vyžaduje všestrannou vzdělanost a celkovou kulturnost. V souvislosti s výkonem „soukromé

detektivní činnosti organizace“ by se měl orientovat ve vědních disciplinách, jako jsou právo, kriminalistika, kriminologie, logika, informační technologie, sociologie, pedagogika, psychologie a další. Postup bezpečnostního manažera musí směřovat nikoli k obecnému poznání, ale k zaměření se na získání určitých znalostí, které přímo či nepřímo souvisejí s profesionálními zájmy a cíly činnosti. Tyto vlastnosti se zpravidla nazývají plasticitou. Plasticita zaručuje bezpečnostnímu manažerovi stálou připravenost a schopnost získávat nutné znalosti, tedy schopnost učení a schopnost promptně využívat a aplikovat naučené. Co se týče morálních aspektů, předpokládá se především bezúhonnost, beztrestnost, absolutně žádná závislost, transparentní jednání. Jako každý manažer, těžištěm jeho činnosti je práce s informacemi (získávání, zpracování, analýza, hodnocení, využití a ochrana), ovšem na rozdíl od běžné manažerské pozice je pozice bezpečnostního manažera specifická ve způsobu získávání informací a zacházení s nimi (využívání). Z dalších vlastností bych vyzdvihl schopnost komunikace a kooperace, řešení problémů, samostatnost, odpovědnost, argumentace a v neposlední řadě charisma. [3]

Vedle schopností a dovedností bezpečnostního manažera je potřeba zmínit i psychologické aspekty jeho činností. Psychologické aspekty zaujímají ve vědomostech a zkušenostech bezpečnostního manažera a tedy i v jeho činnosti nezastupitelné místo. Důvody jsou zřejmé, neboť náplní činností bezpečnostního manažera je práce s lidmi a to s lidmi různého zaměření, různého chování a jednání. Protože práce bezpečnostního manažera je převážně duševního charakteru, je potřeba, aby se bezpečnostní manažer věnoval své duševní hygieně, aby byl odolný vůči stresu. Měl by dokonale znát sám sebe, uvědomit si své silné stránky a ty potom účelně využít ve své každodenní činnosti. Je také potřeba, aby dokázal využít schopností a předností jednotlivých pracovníků úseku bezpečnostního managementu. [3]

Pokud se zaměříme na psychologické aspekty vlastních postupů a opatření, které jsou prováděny v rámci činností bezpečnostního manažera, nalezneme potom hlediska, mezi která patří požadavek na rychlé tempo práce a na vysoké psychické nároky na tuto činnost, zejména zvyknout si na řešení náročných a složitých situací, dokázat se v nich orientovat a dokázat je řešit. Významnou úlohu zde sehrává i motivace. Z dalších aspektů, které souvisejí s výkonem práce bezpečnostního manažera, s jeho postupy, opatřeními a úkoly, je vhodné osvojit si schopnost poznat lidi a umět je odhadnout, umět komunikovat s lidmi, ovlivňovat lidi (působit na lidi) a uspořádat pracovní

prostředí podle potřeb vlastních záměrů a cílů. Je třeba posoudit i následující okruhy, které souvisejí s psychologickými hledisky náplně činností bezpečnostního manažera. Jedná se o schopnosti, jako jsou řešení problémů (identifikace úkolu, jeho pochopení, analýza), rychlé a jednoznačné rozhodování (předvídavost, stanovení priorit), tvořivost (alternativní přístupy, přijímaní nových myšlenek, nadhled), vytrvalost (překonání odporu, získávání druhých) a zvládání zátěže (několik problémů najednou, zdrženlivost v reakcích, přijímání konstruktivní kritiky). [3]

Pedagogická hlediska lze opět posuzovat z několika okruhů. Z komunikačních dovedností jsou to jasné a výstižné vyjadřování, vhodná slovní zásoba, stylistika a gramatika, srozumitelný projev, vyjadřování, volba komunikace odpovídající typu příjemce, vyhýbání se žargonu a slangu a umění naslouchat. V oblasti mezilidských vztahů se jedná o umění taktu a diplomacie při jednání a ve složitých situacích, vnímavost, citlivost a vstřícnost k názorům a pocitům jiných, zájem o účinky svého chování směrem k jiným lidem a schopnost vést tým. Mezi prezentační a pedagogické schopnosti patří přesvědčivá prezentace myšlenek, plánů, činností a rozhodnutí, umění prodat sebe a svůj tým, řešený problém či projekt, schopnost vyložit složité a odborné věci jasně a srozumitelně laikům i managementu, trpělivost, tvorba jasných, srozumitelných a závazných dokumentů, využití moderních technologií a metod pro účinné prezentace. [3]

3.3 Shrnutí

Bezpečnostní manažer je specializovaná funkce, která v organizaci zajišťuje služby bezpečnostních specialistů (auditor, analytik apod.), detektivní ochranu a zpravodajské služby a v neposlední řadě ochranu majetku a osob. Síla role bezpečnostního manažera závisí na způsobu začlenění bezpečnostního manažera do organizační struktury podniku a na síle osobnostních předpokladů manažera samého. Podle způsobu začlenění bezpečnostního manažera do organizační struktury vznikají formální a neformální vazby mezi bezpečnostním manažerem a ostatními zaměstnanci. Z oblasti osobnostních předpokladů jsou na bezpečnostního manažera kladeny požadavky vyplývající z pracovní pozice, ale i ze specifik instituce. Obecně musí být bezpečnostní manažer osoba, která disponuje rozsáhlými a různorodými znalostmi a zkušenostmi. Kromě toho na jeho činnost působí psychologické aspekty vystupující při řešení problémů, rychlém rozhodování, tvořivosti a zvládání zátěže. Z pedagogických hledisek doprovázejí profesi bezpečnostního manažera mimo jiné komunikační dovednosti, umění taktu a diplomacie a prezentační dovednosti.

4 Začlenění bezpečnostního manažera do organizační struktury podniku

Ve společnosti nebo úřadě s funkčním bezpečnostním systémem je bezpečnostní management uznávanou součástí managementu společnosti a bezpečnostní manažer partnerem vedení. Nejvhodnějším řešením je přímá podřízenost bezpečnostního manažera vedení společnosti, obvykle generálnímu řediteli nebo prezidentu společnosti, u úřadu vedoucímu úřadu. U akciových společností je možnou formou řízení bezpečnostního manažera podřízenost členu představenstva, který je odpovědný za bezpečnost. U subjektů, které podléhají režimu zákona o ochraně utajovaných informací, je jednoznačně stanovena podřízenost bezpečnostního ředitele odpovědné osobě. Ne vždy však tato osoba řídí celou bezpečnost, ale pouze ochranu utajovaných informací. Pokud nemá bezpečnostní manažer přístup k vedení, pak může jen stěží naplňovat své poslání včetně vlastní ochrany top managementu. [7]

U velkých společností, ale i u středních a menších firem, je možnou formou řešení outsourcing bezpečnostního managementu. Některé činnosti a pozice bezpečnostního managementu je možné outsourcovat i u veřejné správy. Základními otázkami je výběr dodavatele outsourcingu, míra jeho úrovně a supervize celého procesu. Obvyklým řešením je realizace outsourcingu na základě projektu a analýzy rizik. Není vhodné, aby dodavatel outsourcingu bezpečnostního managementu byl subjekt, který současně zajišťuje fyzickou ostrahu nebo instalace bezpečnostních technologií. Proces řízení outsourcingu bezpečnostního managementu musí být řízen osobou odpovědnou za bezpečnost nebo bezpečnostním manažerem. [7]

Možným řešením outsourcingu u velkých společností nebo centrálních úřadů s regionální strukturou poboček je outsourcing bezpečnostního managementu v regionech a vlastní bezpečnostní management v ústředí. Rovněž vybrané činnosti v ústředí je možné outsourcovat. U středních a menších firem se postupně prosazuje úplný outsourcing. U malých firem naopak může jeden bezpečnostní manažer zajišťovat činnosti pro několik subjektů. Součástí každého smluvního vztahu o outsourcingu bezpečnosti by měla být dohoda včetně sankcí za porušení ochrany poskytovaných informací. [7]

V praxi existuje **řada modelů**, které objektivně závisí na velikosti instituce, předmětu podnikání, na vnímání významu bezpečnosti vrcholovým managementem nebo na majiteli instituce. Nastíníme si proto základní modely začlenění bezpečnostního manažera, ukážeme si typické „plusy“ a „mínusy“, které jsou pro ně charakteristické.

Pro zjednodušení úvah uvažujme pouze tři základní úrovně řízení [12]:

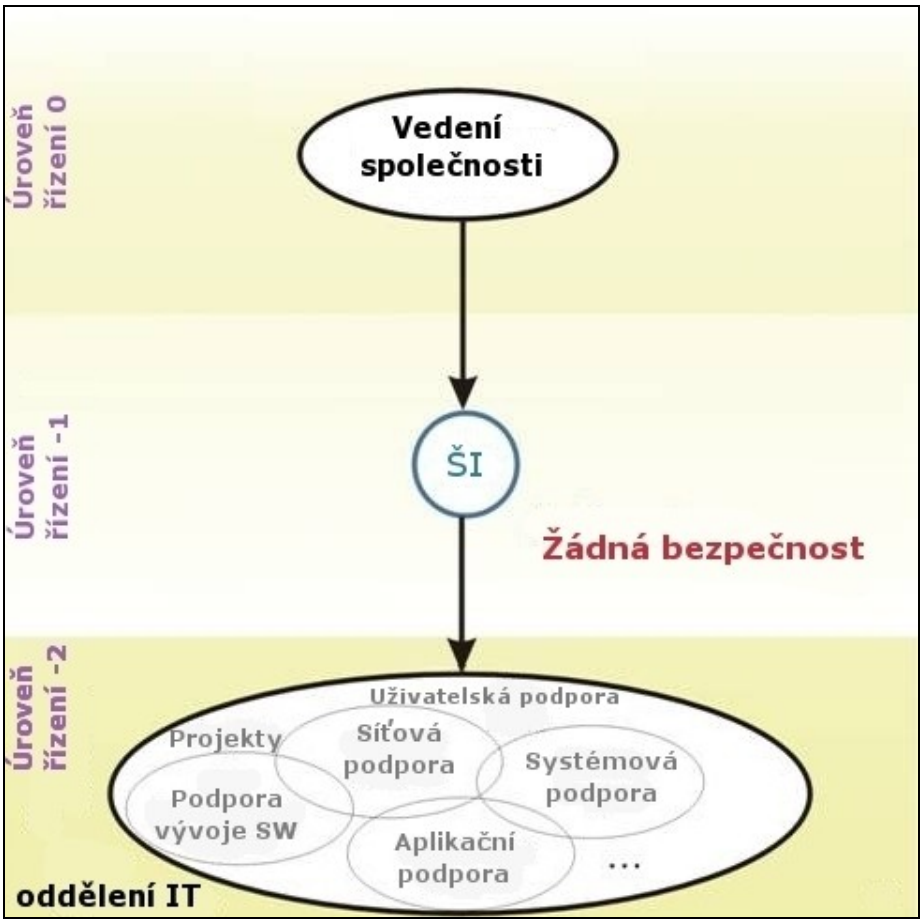
- vrcholový management – není potřeba specifikovat detailní organizační uspořádání;
- pozice „šéfa“ informatiky (ŠI) – původně z anglického CIO – Chief Information Officer;
- oddělení IT – jednotlivé organizační struktury využívající informační technologie (IT), není nutné specifikovat jejich složení, velikosti apod.

Na následujících osmi typových modelech si ukážeme, jak lze umístit, začlenit pozici obecně bezpečnostního manažera (BM – z anglického CSO – Chief Security Officer) nebo bezpečnostního manažera IT (BM_{IT} – z anglického CSO_{IT} – Chief Security Officer) do organizační hierarchie společnosti. [12]

4.1 Model ignorativní bezpečnosti

V rámci tohoto modelu v instituci neexistují žádné pozice, které by se zabývaly bezpečností IS. O bezpečnost nikdo nemá zájem nebo ji nerealizuje. Aplikace nemají žádný rozhodující vliv na základní procesy v instituci. V podstatě zde existuje názor, že dosud se nic nestalo, a tak nemá smysl do bezpečnosti investovat.

Tento model (viz. obrázek 9) je typický pro malé firmy, které jsou teprve u zrodu nebo krátce po něm. Hlavní pozornost je zatím zaměřena na realizaci základního podnikatelského plánu a získání prvních zákazníků. IT bývá často řešeno jednomužně, někdy i na částečný pracovní úvazek. Tento stav zpravidla trvá do prvního bezpečnostního incidentu nebo dalšího kvalitativního růstu instituce. [12]



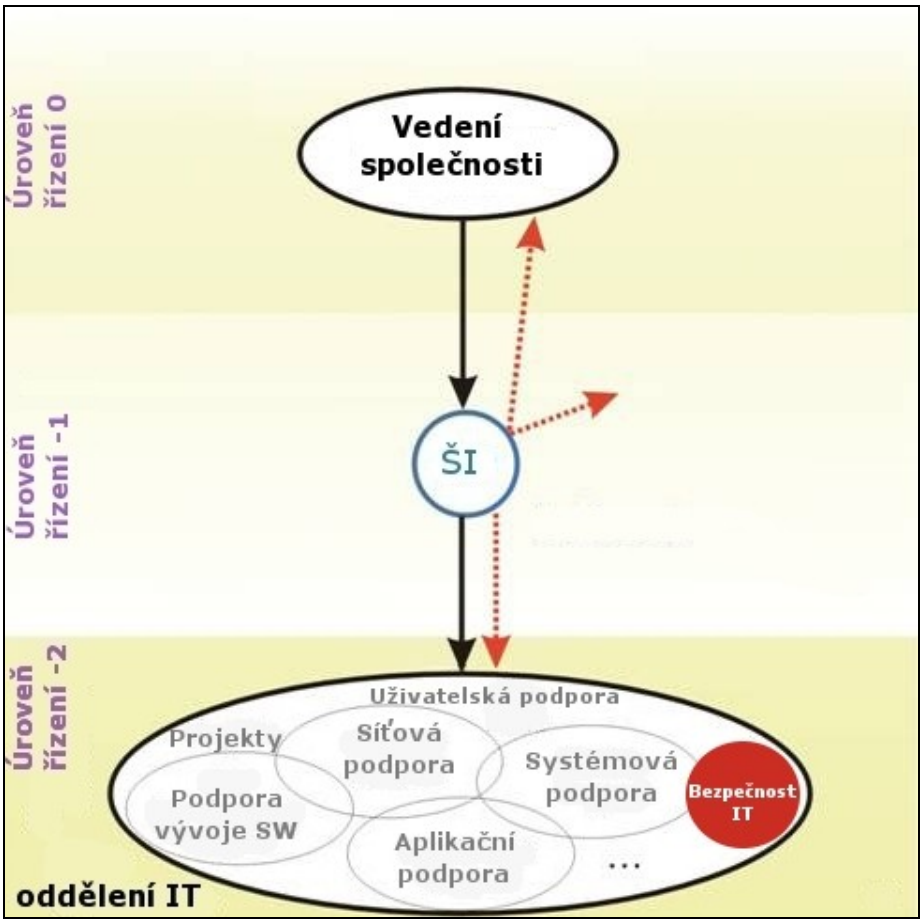
Obrázek 9 Model ignorativní bezpečnosti [upraveno s využitím 12]

4.2 Model minimální technologické bezpečnosti

Oproti předchozímu modelu pracuje v této struktuře již několik zaměstnanců IT na trvalý pracovní úvazek. Ti si uvědomují nutnost určitého zabezpečení, ovšem z jejich pohledu bývá bezpečnost vnímána pouze jako technologická záležitost řízená uvnitř útvaru IT. Komunikace a součinnost s ostatními organizačními složkami je minimální. Chybí zde bezpečnostní politika a z ní vyplývající závazné řídící dokumenty bezpečnosti. Řízením bezpečnosti není v IT obvykle pověřena konkrétní osoba na plný pracovní úvazek. Jedná se spíše o administrátory sítě, databází, aplikací, kteří spíše intuitivně realizují bezpečnostní praktiky na neformální úrovni.

Šéf informatiky praktikuje minimální komunikaci na téma IT bezpečnosti s okolím na stejné nebo vyšší organizační úrovni. Tímto pojetím zde absentuje i rozpočtová kapitola na bezpečnost v budgetu IT. Přesto ovšem může být poměrně vysoká technologická úroveň bezpečnosti vycházející ze slabin používaných aplikací a napadení „zvenku“, instituce ale postrádá ochranu proti selhání nebo pokušení vlastních zaměstnanců. V institucích vycházejících z tohoto modelu není často realizována ani rozsáhlejší

objektová ochrana fyzického charakteru [12]. Model je zobrazen na obrázku 10.



Obrázek 10 Model minimální technologické bezpečnosti [upraveno s využitím 12]

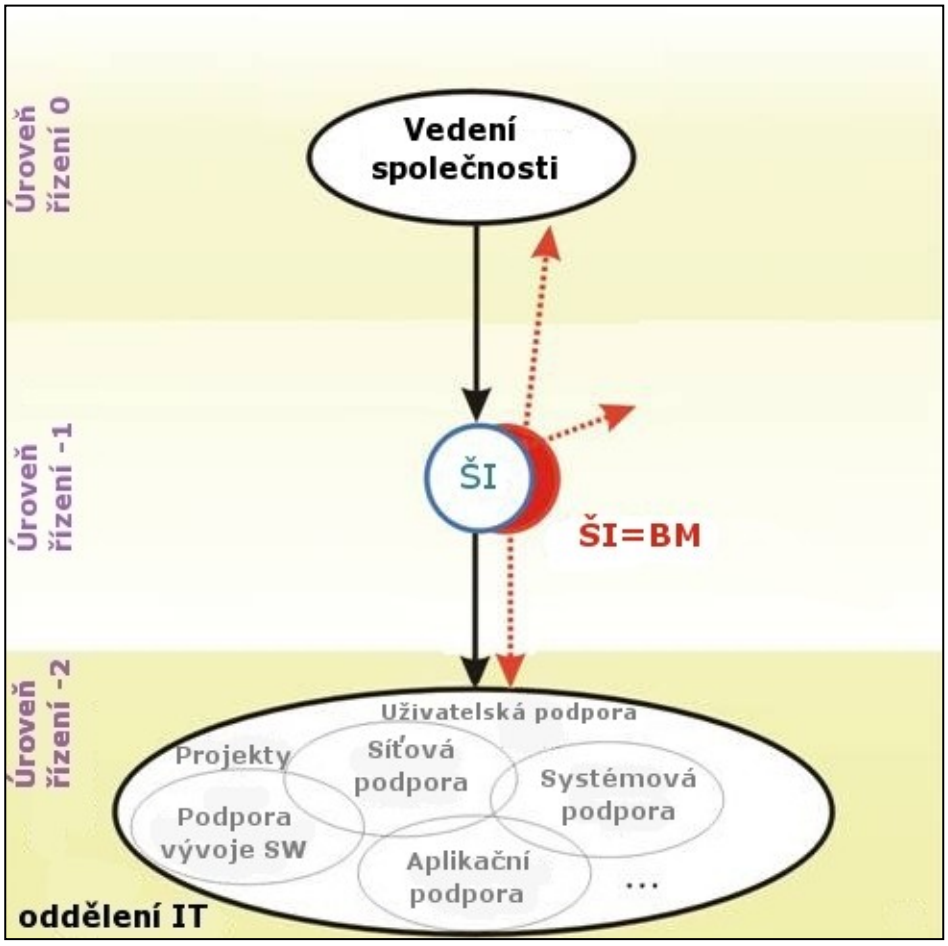
4.3 Model formální bezpečnosti

Tento model se v zásadě neliší od předchozího, co se týká velikosti instituce či IT a rozsahu spravovaných aplikací. Zásadní rozdíl spočívá v tom, že v organizaci již došlo k uvědomění si faktu pověřit někoho bezpečností IT. Šéf informatiky (ŠI) se tak stává chtě nechtě touto osobou. Z ekonomického hlediska tak nevzniká plnohodnotný bezpečnostní manažer (BM), který by se plnohodnotně zabýval svěřenou problematikou. Pro realizaci bezpečnosti IT jsou využíváni a úkolováni jednotliví specialisté či vedoucí organizačních celků IT, kteří jsou koordinováni osobou šéfa informatiky. Neexistuje ale zatím žádná specializovaná skupina, která by se zabývala jen a jen bezpečností.

V tomto pojetí bezpečnosti lze očekávat už samostatný rozpočet pro bezpečnost v rozpočtu IT. Klíčem k prosazování bezpečnosti je osobnost ŠI. Ta může sehrát jak

velice pozitivní nebo i zásadně negativní roli. Můžeme zde nalézt jak osvíceného IT manažera, stejně tak odpůrce, který jen formálně naplňuje svou funkci směrem k vedení společnosti i okolí. Na obhajobu ŠI existuje ale důležitý fakt, že IT bezpečnost je nesmírně odborná a obsáhlá. ŠI tak při svých o povinnostech IT manažera nemůže být schopen vědomostně obsáhnout i tuto oblast a dokázat zajistit její praktické naplnění, kontrolu a další rozvoj.

Základním nedostatkem tohoto modelu zůstává střet zájmů: ten, kdo zodpovídá za rozvoj IT a provoz aplikací nemůže nikdy plnit i roli gestora za bezpečnost, protože se zde potírají základní zodpovědnostní a kontrolní mechanismy. ŠI navíc nemá dostatek prostoru ani času pro bezpečnostní osvětu a výchovu zaměstnanců instituce [12]. Obrázek 11 znázorňuje tento typ modelu.



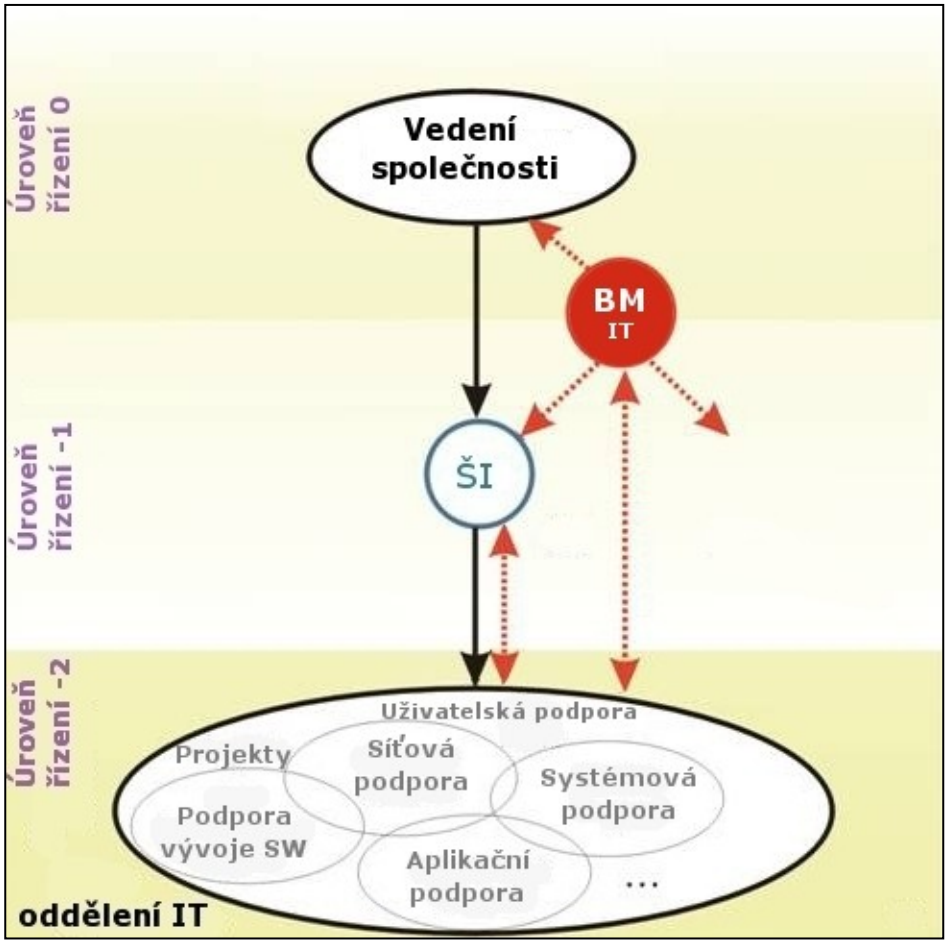
Obrázek 11 Model formální bezpečnosti [upraveno s využitím 12]

4.4 Model odtržené bezpečnosti

V tomto modelu dochází k zásadnímu zlomu – vedení instituce (vlastníci) dojdou k rozhodnutí, že je nezbytné vytvořit samostatnou tabulkovou pozici bezpečnostního manažera IT (BM_{IT}). Jeho pozice je začleněna mimo útvar IT a je na stejné nebo vyšší úrovni než šéf informatiky (ŠI). V organizaci existuje bezpečnostní politika, na bezpečnost jsou vyčleňovány finanční prostředky. Jejich objem potom závisí na velikosti podniku a podle toho padne také rozhodnutí, zda vytvořit vlastní bezpečnostní útvary IT (finanční, přepravní instituce, velké výrobní podniky apod.) nebo pouze pozici samostatného (BM_{IT}), jak je běžné u malých a středních podniků. Často je jeho pozice spojena i se zodpovědností za fyzickou personální aj. bezpečnost a tak dochází ke kumulaci pozice analogicky jako v předchozím modelu v případě ŠI a BM. Ve skutečnosti jde o dvě naprosto odlišné pozice a již na úrovni středních podniků nelze celou bezpečnostní problematiku obsahově zvládnout jediným manažerem.

BM se tak dostává do nepříjemné situace. Jsou na něj kladeny největší psychologické a odborné nároky, požadují se po něm vysoké životní zkušenosti, a tak je tato pozice obsazena osobou minimálně středního věku. Otázkou zůstává, jak je potom schopný sledovat neustále se vyvíjející technologie a jak dokáže vycházet se zaměstnanci IT. Pokud BM prosazuje bezpečnost necitlivě, direktivně vůči útvaru IT, může se stát, že ti ho časem zcela odříznou od reálných technologií v instituci.

Stejně tak je velice důležitá vazba mezi (BM_{IT}) a ŠI. Stačí, aby ŠI zpochybňoval názory a návrhy BM_{IT} a nerespektoval jej a hned tu máme neřešitelnou situaci. Stejně tak se to může odrazit i na sestavování rozpočtu, neboť je velmi pravděpodobné, že BM_{IT} nebude mít svůj vlastní rozpočet, ale bude odkázaný na rozpočet IT. Pozitivem tohoto modelu je na druhou stranu blízkost BM k managementu společnosti a tím vzniká předpoklad pro úspěšné prosazování bezpečnostní politiky v organizaci [12]. Přesnější představu o modelu poskytuje obrázek 12.



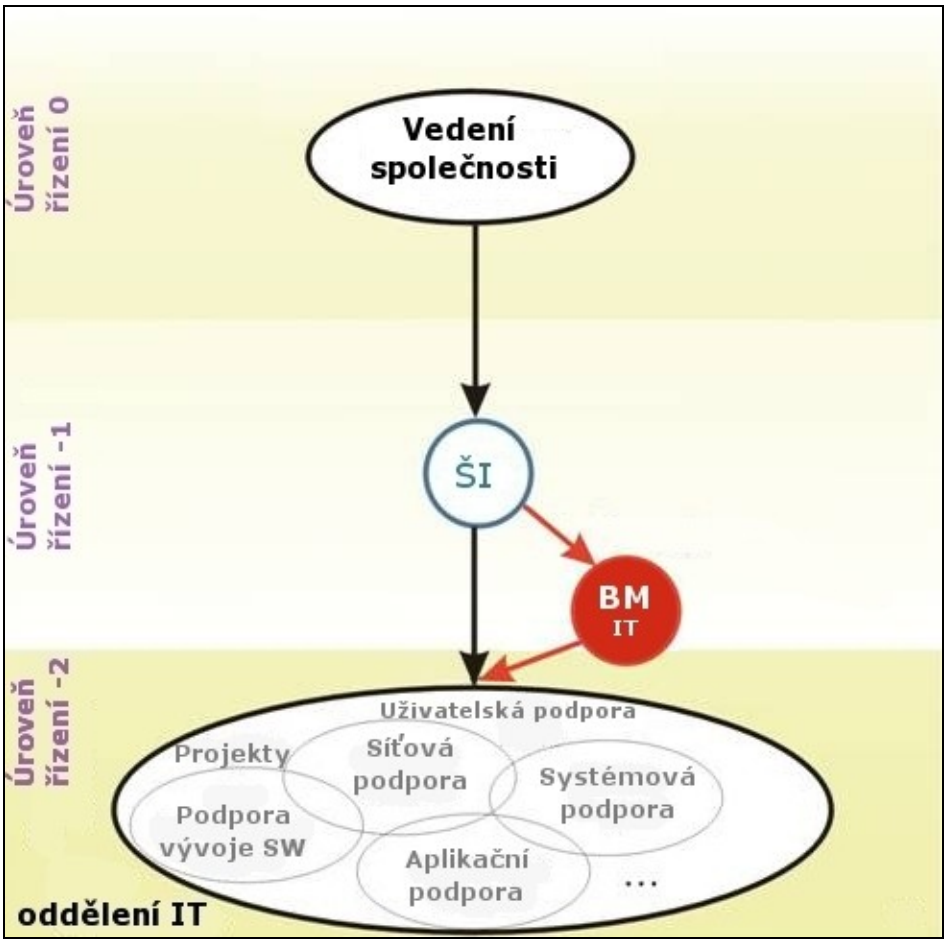
Obrázek 12 Model odtržené bezpečnosti [upraveno s využitím 12]

4.5 Model utopené bezpečnosti

V praxi českých útvarů IT je tento model nejběžnější. Ve středně velkých firmách se bezpečností zabývají 1 až 3 specialisté, většinou ale jen bezpečnostní manažer IT vykonává svou profesi na plný úvazek. BM je vzat pod křídla ŠI. Předpokládají se zde podobné názory na bezpečnost mezi oběma manažery. Tím se odstraní problémy předchozího modelu, ale zase se objeví nevýhody jiné. BM má velmi blízko k IT a k lidem z IT, úzce spolupracuje s vedoucími jednotlivých IT týmů. Jestliže jsou dobře nastaveny mezilidské vztahy, technologická bezpečnost bývá na vysoké úrovni. Nejsou zde ani problémy s rozpočtem a financováním IT projektů. Technologická bezpečnost je velice agilní a schopná včas reagovat na technologicky vedené útoky.

Externí auditoři tomuto modelu ale vytýkají závislost BM na ŠI. Pokud zde totiž neexistuje základní názorová shoda, může teoreticky ŠI bránit rozvoji bezpečnosti. V tom případě by ale v podstatě nedošlo vůbec vytvoření pozice BM v instituci.

Model utopené bezpečnosti může vzniknout přirozenou evolucí z modelu minimální technologické bezpečnosti. Neformální zaměstnanec IT, který koordinoval spolu s ostatními procesy IT i bezpečnost uvnitř útvaru IT, se může stát za splnění manažerských požadavků dobrým BM. Nedostatkem modelu je často špatná komunikace a personální práce směrem vně útvaru IT, protože ŠI je zbytečným mezičlánkem. Problémem bývá i integrace IT bezpečnosti s obecnou bezpečnostní politikou instituce. Má-li organizace pouze jediného BM_{IT}, pak z praktického pohledu bývá model utopené bezpečnosti úspěšnější než model odtržené bezpečnosti, i když je to v rozporu s teoretickým přístupem, který upřednostňuje nezávislost realizace bezpečnosti v instituci [12]. Model lze shlédnout na obrázku 13.



Obrázek 13 Model utopené bezpečnosti [upraveno s využitím 12]

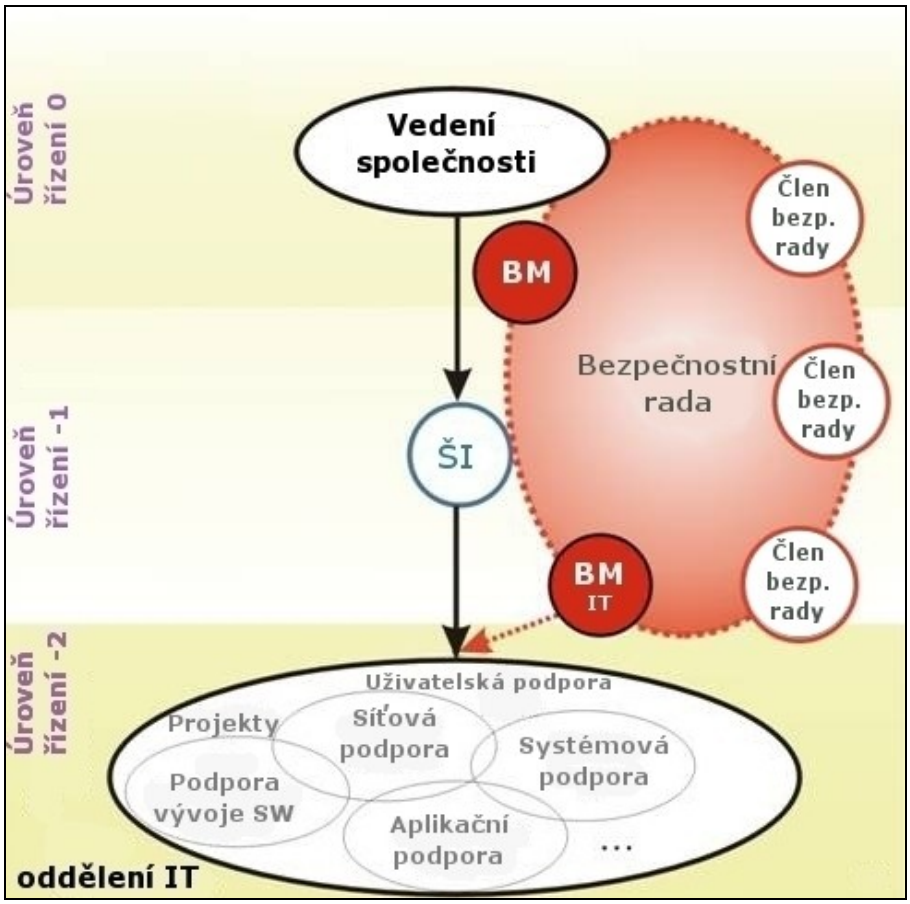
4.6 Model agilní bezpečnosti

Model agilní bezpečnosti vychází z pozitiv předchozích modelů a odstraňuje jejich typická negativa. Model je typický pro středně velké podniky bez vlastních rozsáhlých bezpečnostních útvarů s početným personálním obsazením, zajišťující bezpečnost. V instituci může kromě osoby BM_{IT} existovat i další manažer, který zodpovídá za fyzickou, personální, ekologickou bezpečnost apod. – bezpečnostní manažer (BM).

V instituci je vytvořena bezpečnostní rada jmenovaná vedením instituce, která má podobu virtuální struktury napříč vrcholovým a středním managementem. Členové jsou jmenováni podle konkrétních potřeb, mohou to být i externí, přizvaní specialisté, ale i jednotliví odborní ředitelé, personalisté, technici a samozřejmě oba bezpečnostní manažeři.

V tomto pojetí modelu odpadají komunikační problémy mezi managementem a odbornými specialisty, koordinace bývá na vysoké úrovni. Není problém ani při prosazování bezpečnostních projektů a jejich financování. Bezpečnostní rada je tak kolektivním orgánem, který zajišťuje tvorbu a schvalování bezpečnostní politiky a s tím souvisejících dokumentů (legislativní funkce), kontroluje stav implementovaných opatření a jejich funkcionalitu (kontrolní funkce) a řeší mimořádné bezpečnostní situace v době ohrožení organizace (řídící funkce). Bezpečnost bývá vysoce agilní.

Na vysoké úrovni je i komunikace se zaměstnanci, jejich seznamování s opatřeními a doporučeními. V bezpečnostní radě je proto vhodné mít i zástupce personální složky instituce – jednak se dobře otevírá cesta ke školením, jednak se dobře realizuje i personální bezpečnost [12]. Model je znázorněn na obrázku 14.



Obrázek 14 Model agilní bezpečnosti [upraveno s využitím 12]

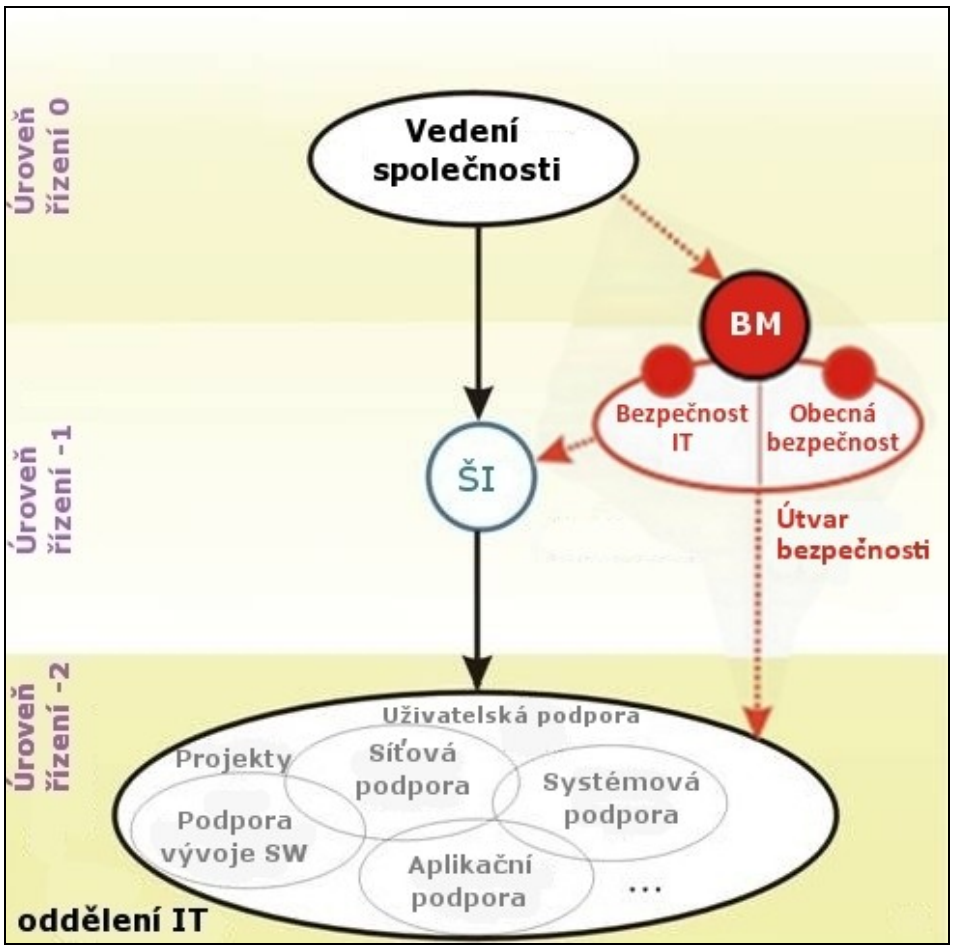
4.7 Model institucionální bezpečnosti

Uvedený model je typický pro velké instituce (banky, velké průmyslové podniky, silové resorty státu). Existují zde již profesionální bezpečnostní útvary obsahující více zaměstnanců, kteří se dále profesně specializují. Řeší se jak technologická bezpečnost, tak i bezpečnost informační a obecná (fyzická ostraha objektů aj.).

Model (viz. obrázek 15) má řadu variant. Může se jednat o dva samostatné organizační celky (jeden má svého manažera pro technologickou bezpečnost a druhý pro obecnou bezpečnost) nebo o jeden organizační útvar (ten vede jediný BM), který se dále dělí do jednotlivých oblastí a specializací. Bezpečnost je již plně procesně formalizována a instituce buduje bezpečnost podle (mezi)národních standardů a doporučení, které si instituce vybere za závazné.

Pravidla financování jsou jasně determinována, potíže se obvykle objevují v nedostatku finančních zdrojů na rozsáhlé projekty. Na vysoké úrovni je jak technologická, tak i personální bezpečnost, zaměstnanci jsou pravidelně školeni proti útokům zvenku. Jedinou nevýhodou tohoto modelu by tak mohla být nedostatečná agilita na některé

typy hrozeb nebo samotná velikost organizace, ve které funguje vžitý způsob myšlení ve „vyjetých kolejích“ nebo dokonce alibismus.[12]



Obrázek 15 Model institucionální bezpečnosti [upraveno s využitím 12]

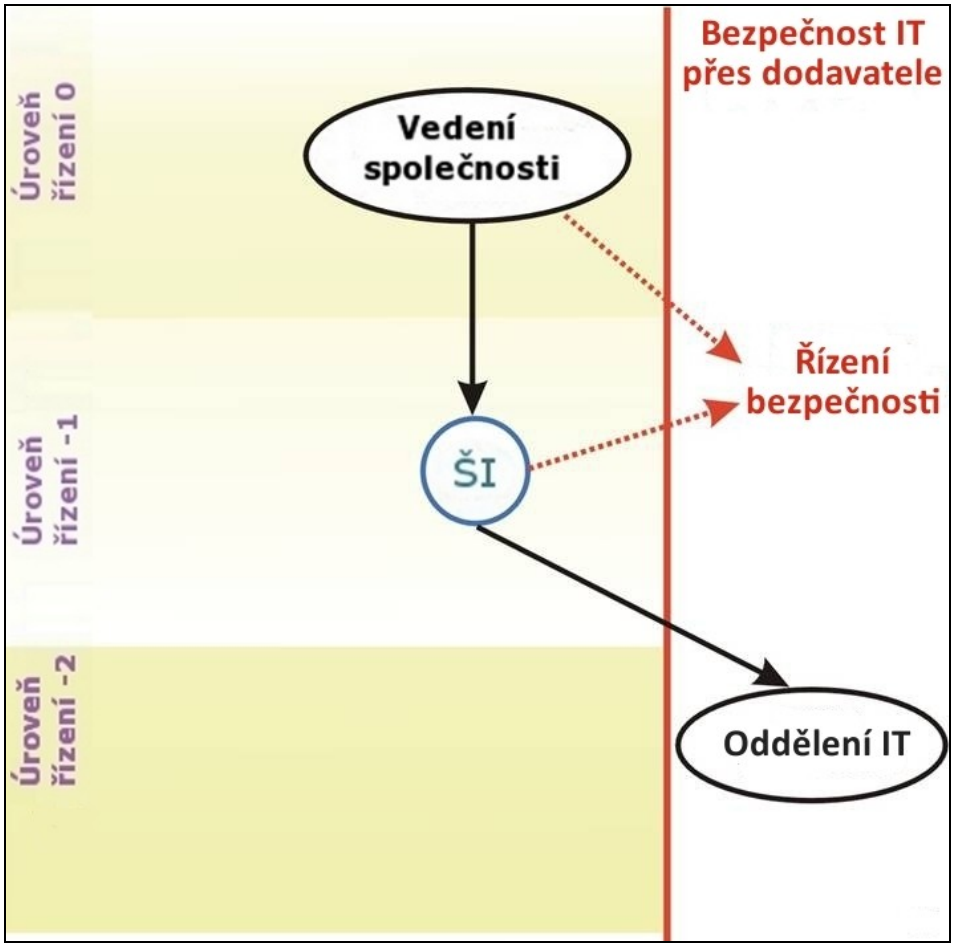
4.8 Model outsourcované bezpečnosti

Řada institucí využívá služeb svých dodavatelů pro řešení určitých okruhů činností. Plného outsourcingu využívá zatím minimum institucí. Z toho důvodu jsou k dispozici malé informace o praktických zkušenostech z bezpečnostního pohledu.

Určitě musí vždy v instituci existovat osoba zodpovědná za koordinaci informačních potřeb společnosti a řízení dodavatelské organizace. Komplexní řešení bezpečnosti se rozpadá do dvou okruhů – všeobecná bezpečnostní politika zůstává na straně instituce (je v souladu s firemní strategií), zatímco technologická bezpečnost vychází z bezpečnostní politiky a je na straně dodavatele.

Outsourcovat lze v podstatě cokoli kromě vlastního strategického rozhodování a zodpovědnosti za něj. Za bezpečnost organizace proto musí vždy celkově zodpovídat její zaměstnanec – bezpečnostní manažer. Ten zajišťuje požadovanou úroveň služeb u dodavatele a koordinuje je se všemi institucionálními procesy. Z tohoto důvodu jsou na BM kladeny mimořádné nároky na odbornost, manažerské schopnosti a psychickou odolnost. Ve své pozici je osamocen podobně jako v modelu odtržené bezpečnosti, bez blízkého přístupu k technologiím, jež jsou provozovány dodavatelsky.

Outsourcing zvyšuje nároky na přesné zadání požadovaných služeb a obslužných procesů a je komunikačně náročný ve vztahu k dodavateli. Musí být i vyjasněny otázky, jakým způsobem kontrolovat úroveň bezpečnosti, když v zadavatelské organizaci je minimum specialistů informační bezpečnosti. Objektivní cestou je v tomto případě nezávislá kontrola (audit jiné instituce specializující se na danou problematiku). Potom je ale nutné počítat s dalšími náklady, kterou tato kontrola s sebou nese [12]. Model outsourcované bezpečnosti představuje obrázek 16.



Obrázek 16 Model outsourcované bezpečnosti [upraveno s využitím 12]

4.9 Shrnutí

Zařazení bezpečnostního manažera v instituci (malé či velké firmě, ve státní nebo neziskové organizaci) není vůbec jednoduchá záležitost. Je potřeba si uvědomit, že právě začlenění bezpečnostního manažera v hierarchické organizační struktuře je důležité pro úspěšné prosazování jak bezpečnostního manažera, tak i případně celého oddělení bezpečnostního managementu. S tím pochopitelně souvisí i stanovení pravomocí, vazeb atd. [3]. Pro lepší orientaci v uvedených modelech uvádí tabulka 1 srovnání jednotlivých modelů, kde poukazuje na hlavní rozdíly ze tří pohledů. Nejprve z pohledu existence funkce bezpečnostního manažera v organizaci, potom znázorňuje, komu je bezpečnostní manažer v podniku podřízen a nakonec ukazuje, ve kterém typu podniku se příslušný model nejčastěji uplatňuje.

Tabulka 1 Srovnání typových modelů [vlastní]

Model	Funkce BM ve firmě	Podřízenost BM	Uplatnění modelu
Ignorativní bezpečnosti	NE	-	malé podniky
Minimální technické bezpečnosti	NE	-	malé podniky
Formální bezpečnosti	NE	-	malé a středně velké podniky
Odtržené bezpečnosti	ANO	vedení společnosti	malé a středně velké podniky
Utopené bezpečnosti	ANO	šéf informatiky	středně velké podniky
Agilní bezpečnosti	ANO	vedení společnosti	středně velké a velké podniky
Institucionální bezpečnosti	ANO	vedení společnosti	velké podniky
Outsourcované bezpečnosti	NE	vedení společnosti, šéf informatiky	malé, středně velké i velké podniky

Z tabulky vyplývá, že menší organizace zpravidla neřeší problematiku bezpečnostního managementu. Je zřejmé, že s prosazováním bezpečnostního managementu v organizaci rostou i náklady. Potom tedy záleží na tom, nakolik si menší organizace cení svých aktiv a zda se jim vyplatí ušetřit za neřešení bezpečnosti v porovnání s případnou

finanční ztrátou v důsledku úniku důležitých informací. U středně velkých a velkých organizací je už bezpečnost řešena, hlavním problémem je ale úskalí začlenění bezpečnostního manažera do organizační struktury a nastavení správných vazeb v rámci organizační struktury. V této souvislosti je vhodné obrátit pozornost na tabulku 2, která vyzdvihuje hlavní výhody a nevýhody jednotlivých modelů.

Tabulka 2 Výhody a nevýhody modelů [vlastní]

Model	Výhody	Nevýhody
Ignorativní bezpečnosti	žádné	neřeší se bezpečnost, vysoké riziko úniku informací, ztráty aktiv
Minimální technické bezpečnosti	řeší se alespoň bezpečnost IT	chybí řešení obecné bezpečnosti, chybí pozice BM v podniku
Formální bezpečnosti	začíná se řešit bezpečnostní management, zavedení rozpočtu na bezpečnost	bezpečnostní manažer je zároveň šéf informatiky, záleží na jeho schopnostech, vzniká střet zájmů mezi zodpovědností a kontrolou
Odtržené bezpečnosti	zavedení samostatné pozice BM (zodpovědného převážně za bezpečnost IT), přímá vazba na vedení společnosti	často má BM zodpovědnost za IT a za obecnou bezpečnost, vysoká vytíženost BM, šéf informatiky je rozpočtově vázán na BM
Utopené bezpečnosti	BM je přímo napojen na IT, kde si koordinuje bezpečnost IT, dobré financování IT projektů	závislost BM na šéfovi informatiky (zhoršení komunikace BM směrem k vedení)
Agilní bezpečnosti	zavedení bezpečnostní rady, členové jsou napříč všemi útvary podniku, zavedení BM a BM_{IT},dobrá komunikace BM směrem k ostatním útvarům, prosazování rozpočtu na bezpečnost	vyšší vytížení členů bezpečnostní rady v rámci svých povinností a v rámci povinností vyplývajících z členství v bezpečnostní radě
Institucionální bezpečnosti	zavedení samostatného bezpečnostního útvaru, který je zodpovědný za obecnou bezpečnosti i za IT bezpečnost, podřízenost vedení společnosti	vysoké náklady na získání kvalifikovaných pracovníků do útvaru bezpečnosti
Outsourcované bezpečnosti	převedení zodpovědnosti na dodavatele, ušetření nákladů	zvýšené nároky na přesné zadání požadavků, koordinaci a kontrolu nastavení procesů

Každá organizace se liší jiným předmětem základních činností, kulturou zaměstnanců a managementu, a tak nelze považovat žádný z modelů za univerzální, jediný či správný. Lze se ovšem nechat jimi inspirovat a s citem je upravit pro své vlastní potřeby [14]. Pro malé společnosti se hodí v porovnání s náklady nejlépe model formální bezpečnosti, pro středně velké podniky je obecně vyhovující model utopené společnosti (bývá nejčastěji používán v praxi) a model agilní bezpečnosti, ve velkých podnicích by měl být potom uplatňován model institucionální bezpečnosti.

5 Závěr

V této práci jsem se pokusil představit problematiku bezpečnostního managementu ze všech možných úhlů pohledu. Práce se skládá ze čtyř celistvých celků, přičemž každá část se zabývá vždy určitým náhledem, který je odlišný od části jiné.

První celek se zabývá teoretickou podstatou činnosti bezpečnostního manažera. Začíná zařazením bezpečnostního managementu v soustavě ostatních věd a postupně přechází ke komplexnímu náhledu na bezpečnost a rozsahu bezpečnosti aplikovaném na modelu virtuálního domu. Vyzdvihuje důležitost informační bezpečnosti a závěrem porovnává řešení bezpečnosti ve státním sektoru a komerční sféře. V rámci této kapitoly se podařilo splnit cíl seznámit se s problematikou a získat tak potřebné znalosti pro plnění dalších vytyčených cílů.

Druhý celek se zabývá hlavními kroky implementace systémů řízení informační bezpečnosti. V rámci tohoto celku byl nalezen vhodný postup implementace systému řízení informační bezpečnosti (ISMS – information security management system) v organizaci, čímž byl splněn další z cílů. Mezi hlavní kroky tohoto postupu patří rozhodnutí o zavedení ISMS, stanovení rozsahu a struktury ISMS, bezpečnostní analýza, bezpečnostní audit, bezpečnostní prognóza, stanovení bezpečnostní politiky, bezpečnostní projekt, implementace a provoz ISMS monitorování a přezkoumávání ISMS a údržba a zlepšování ISMS.

Poté se práce zaměřuje na osobu bezpečnostního manažera a podstatu této profese, kterou se podařilo definovat a tím splnit jeden z cílů této práce. Bezpečnostní manažer je specializovaná funkce, která v organizaci zajišťuje služby bezpečnostních specialistů (auditor, analytik apod.), detektivní ochranu a zpravodajské služby a v neposlední řadě ochranu majetku a osob. Síla role bezpečnostního manažera závisí na způsobu začlenění bezpečnostního manažera do organizační struktury podniku a na síle osobnostních předpokladů manažera samého. Obecně musí být bezpečnostní manažer osoba, která disponuje rozsáhlými a různorodými znalostmi a zkušenostmi. Kromě toho na jeho činnost působí psychologické aspekty vystupující při řešení problémů, rychlém rozhodování, tvořivosti a zvládání zátěže. Z pedagogických hledisek doprovázejí profesi bezpečnostního manažera mimo jiné komunikační dovednosti, umění taktu a diplomacie a prezentační dovednosti.

Závěrečný celek se zabývá začleněním bezpečnostního manažera do organizační struktury organizace. Popisuje řešení začlenění manažera v různých typech společností a představuje teoretické modely zařazení manažera do podniku. Cílem této kapitoly bylo nalézt univerzální model, podle kterého je vhodné začlenit bezpečnostního manažera do organizační struktury podniku. Tento cíl se nepodařilo splnit. Zjistilo se, že každá společnost má svá specifika, na základě kterých nelze jednoznačně vytvořit obecný model. Všechny organizace řešící informační bezpečnost ale mohou čerpat z představených modelů a přizpůsobit si je podle potřeb daného subjektu. Výsledky srovnání jednotlivých modelů ukázaly, že pro malé společnosti se hodí v porovnání s náklady nejlépe model formální bezpečnosti, pro středně velké podniky je obecně vyhovující model utopené společnosti (bývá nejčastěji používán v praxi) a model agilní bezpečnosti, ve velkých podnicích by měl být potom uplatňován model institucionální bezpečnosti.

V rámci bakalářské práce se podařilo splnit téměř všechny cíle, které byly stanoveny v úvodu. Na osobu bezpečnostního manažera jsou kladeny ty nejvyšší nároky, a to snad ze všech možných oblastí. Tato funkce obnáší jak obrovské odborné předpoklady, tak ale i schopnosti psychologické a odolnost proti stresu. Měla by to být osoba, která má za sebou řadu životních zkušeností, ale zároveň je ochotná a schopná se neustále vzdělávat. Musí zůstat ve firmě osamocena z podstaty své práce, ale zároveň musí mít nejvřelejší vztahy se svým okolím, aby dokázala prosazovat zásady bezpečnostní politiky v instituci. Musí unést břemeno zodpovědnosti, ale na druhou stranu působit sebejistě. Zkrátka musí umět sloučit věci zdánlivě neslučitelné a přitom vypadat, jako by to nebylo nijak obtížné. Z toho důvodu chovám k pozici bezpečnostního manažera nesmírnou úctu. Jeho životní a pracovní pozice je velice složitá, v moderním světě ovšem hraje velmi významnou a nezastupitelnou roli.

6 Seznam použité literatury

[1] BRABEC, František. *Bezpečnost pro firmu, úřad, občana.* 1.vyd. Praha: Public History, 2001. 210 s. ISBN 80-86445-04-06.

[2] BRABEC, František. *Bezpečnostní manažer* [elektronický dokument MS PowerPoint]. Vytvořen 1.10.2006, poslední revize 5.12.2007 [cit. 2007-12-20]. Přednášky k předmětu KUIBS na Univerzitě Pardubice, dostupné ze systému STAG Univerzity Pardubice.

[3] BRABEC, František. *Bezpečnostní manažer ve firmě* [elektronický dokument MS Word]. Vytvořen 11.7.2005, poslední revize 10.10.2006 [cit. 2007-01-09]. Přednášky k předmětu KUIBS na Univerzitě Pardubice, dostupné ze systému STAG Univerzity Pardubice.

[4] BRABEC, František. *Ochrana bezpečnosti podniku*. 1. vyd. Praha: Eurounion, 1996. 203 s. ISBN 8085858-29-0.

[5] BRABEC, František. *Úvod do studijního oboru informační a bezpečnostní služby*. [elektronický dokument MS Word]. Vytvořen 27.3.2005, poslední revize 10.10.2006 [cit. 2007-01-10]. Přednášky k předmětu KUIBS na Univerzitě Pardubice, dostupné ze systému STAG Univerzity Pardubice.

[6] ČZU. *Bezpečnostní manažer – OIKT* [online]. c2006, [cit.2009-04-15]. URL: < http://www.oikt.czu.cz/?r=93 >.

[7] FRYŠAR, Miroslav a kolektiv. *Bezpečnost pro manažery, podnikatele a politiky*. 1. vyd. Praha: Public history, 2006.176 s. ISBN 80-86445-22-4.

[8] *Jak se buduje systém informační bezpečnosti* [online]. c1996-2008, poslední revize 8.9.2006 [cit. 2009-04-15]. URL: < http://managerweb.ihned.cz/c3-19237600-T00000_d-jak-se-buduje-system-informacni-bezpecnosti >.

[9] KAMENÍK, Jiří - BRABEC, František a kolektiv. *Komerční bezpečnost: Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*. 1.vyd. Praha: ASPI, 2007. 340 s. ISBN 978-80-7357-309-6.

[10] KNÝ, Milan. *Bezpečnostní management* [online]. c2005 – 2008, poslední revize 28.11.2006 [cit. 2009-04-15]. URL: < http://www.trivis.info/view.php?cisloclanku=2006112801 >.

[11] *Management – Wikipedie, otevřená encyklopedie* [online]. Poslední revize 27.3.2009 [cit 2009-04-15]. URL: < http://cs.wikipedia.org/wiki/Management >.

[12] NEČAS, Stanislav - HÁLA, Milan. *Bezpečnost v podmínkách organizací a institucí ČR: sborník z mezinárodní konference*. [online] 1. vyd. Praha: Soukromá vysoká škola ekonomických studií, 2005. 208 s. ISBN 80-86744-49-3. [cit. 2009-04-15].
URL: < http://www.svses.cz/skola/akce/konf/bezp05/texty/sbornik.pdf >.

[13] SEIGE, Viktor. Informační bezpečnost – pojem (ne)známý. *IT system* [online]. 2001, roč. 2, č. 1-2 [cit 2009-04-15].
URL: < http://www.systemonline.cz/clanky/informacni-bezpecnost-pojem-ne-znamy.htm >.

[14] TRIVIS-CPP. *Ochrana informací a utajovaných informací* [elektronický dokument MS Word]. Vytvořen 26.11.2006, poslední revize 12.12.2006 [cit. 2006-12-19]. Přednášky k předmětu KUIBS na Univerzitě Pardubice, dostupné ze systému STAG Univerzity Pardubice.

7 Seznam obrázků

8 Seznam tabulek