UNIVERZITA PARDUBICE
FAKULTA EKONOMICKO-SPRÁVNÍ

BAKALÁŘSKÁ PRÁCE

2009 Martin Kameník

Univerzita Pardubice
Fakulta ekonomicko-správní

Informační výhoda jako součást informační bezpečnosti

Martin Kameník

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: **Martin KAMENÍK**

Studijní program: **B6209 Systémové inženýrství a informatika**

Studijní obor: **Informační a bezpečnostní systémy**

Název tématu: **Informační výhoda jako součást informační bezpečnosti**

Zásady pro vypracování:

1. Informace jako výhoda v konkurenčním boji
2. Ofenzivní komerční zpravodajství
3. Defenzivní komerční zpravodajství
4. Možná opatření a jejich dopad při zajišťování informační výhody

Rozsah grafických prací:

Rozsah pracovní zprávy:

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

Seznam odborné literatury:

[1]Security magazín. Praha: Family media, 2008, 5-6. ISSN 1210-8723.
[2]Mitnick,K.D, Simon, W.,L. Umění klamu. Gliwice: Helion, 2003, 348 s. ISBN 83-7361-210-6.
[3]Brabec, F. Ochrana bezpečnosti podniku. Praha : Eurounion, 1996. 203 s. ISBN 80-85858-29-0.
[4]Kameník, J. a kol. Komerční bezpečnost: soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur. Praha: ASPI, 340s. ISBN 978-80-7357-309-6.

Vedoucí bakalářské práce: **doc. Ing. Jiří Křupka, 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 19. 4. 2009

Martin Kameník

ANOTACE

Práce se věnuje významu informací a jejich zabezpečení. Představuje moderní nástroje pro získání informační výhody a jejich možnou provázanost. Zahrnuje průzkum názoru firem na danou problematiku.

KLÍČOVÁ SLOVA

informace, bezpečnost, knowledge management, business intelligence, konkurenční zpravodajství

TITLE

Information advantage as a part of information security

ANNOTATION

This work deals with the meaning of information and their security. It presents modern tools for obtaining information advantage and their possible cohesion. It contains research of companies' opinion at given questions.

KEYWORDS

information, security, knowledge management, business intelligence, competitive intelligence

OBSAH

Seznam tabulek a obrázků

1. Úvod

Cílem práce je komplexní pohled na pojem informační bezpečnosti. Představení moderních nástrojů k získání informační výhody a jejich vzájemnou možnou provázanost. Praktická část se poté zabývá informační výhodou z defenzivního pohledu (tj. zajištění vlastních dat) a stavem povědomí této problematiky z různých úhlů malých i velkých firem. Téma práce bylo zvoleno s ohledem na svou aktuálnost.

Nemělo by již být pochyb o tom, že informace jsou jednou z klíčových složek úspěchu nejen pro státní, ale i soukromý sektor. Že tomu tak bylo i v letech minulých, dokazuje následující citát čínského filosofa z doby přibližně 500 let př. n. l.

„To, co pomohlo osvíceným vládcům a schopným generálům k vítězství, co jim umožnilo předstihnout tisíce dalších, byly včasné informace.“[1]

Výrok se pochopitelně týkal vojenství, ale velmi snadno jej lze vztáhnout na moderní ekonomický svět. Právě toho si jsou dnešní podniky dobře vědomy nebo by alespoň měly být, chtějí-li se prosadit v sílící konkurenci. Jednotlivé firmy používají takřka shodných prostředků a prvkem, který je dělí na prosperující a ztrátové, je kvalita a včasnost relevantních informací.

Vznikají ucelené metody, které se zabývají buď ziskem nových informací, nebo z již získaných informací další skryté souvislosti dolují. Dochází však k tzv. informační explozi. Pro manažery je tato situace stejně špatná, ne-li horší, než nedostatek informací. Je tedy vhodné filtrovat pouze podstatné informace, které pomohou v procesu rozhodování.

Při získávání informací by se firma měla stranit praktik ekonomické špionáže, jejíž amorální stránka koliduje s právním řádem většiny zemí. Nicméně při zajištění vlastní bezpečnosti je nezbytné počítat s možností využití špionáže ze strany konkurenčních podniků. Pro zisk informační výhody je možné použít některý z legálních nástrojů, jako jsou relativně nové směry business intelligence, konkurenční zpravodajství, knowledge management, atd. Jejich podstatou je zisk informací, jejich správa a efektivní použití v souladu se společenskými a právními normami.

Tyto „nové“ nástroje má management k dispozici, ale přesto zatím nejsou zcela doceněny. Zároveň s tím, jak firmy začaly zjišťovat důležité informace o svých konkurentech, objevila se potřeba chránit vlastní aktiva. Podniky o sobě často (mnohdy z vlastních zdrojů) propagují zbytečně mnoho faktů, které lze zpravodajem využít pro konkurenci. Na některé z těchto problémů bude v práci poukázáno.

[1] SUN-C\', PIN, Sun. *Umění války*. [s.l.] : [s.n.], 2005. 296 s., s.38

2. Informace

V následujících textech bude často zmíněn pojem informace, informační výhoda, bezpečnost informací, zisk informací atd. Je tedy vhodné stanovit, z jakého pohledu je informace chápána.

2.1.Definování pojmu

V závislosti na prostředí se definice mění. Lze nalézt charakteristiku pro filosofii, komunikaci, kybernetiku či matematiku. Jednotlivé výroky jsou uvedeny ve výše jmenovaném pořadí.

„Poznatek o určité skutečnosti, předmětu nebo jevu zachyceném ve zpřístupnitelné formě využitelný při přizpůsobování se člověka životnímu prostředí.“[2] Cigánik

„Objektivní obsah komunikace mezi souvisejícími hmotnými objekty, projevující se změnou stavu těchto objektů.“[3] Brillouin

„Název pro obsah toho, co se vymění s vnějším světem, když se mu přizpůsobujeme a působíme na něj svým přizpůsobováním. Proces přijímání a využívání informace je procesem našeho přizpůsobování k nahodilostem vnějšího prostředí a aktivního života v tomto prostředí.“[4] Wiener

„Energetická veličina, jejíž hodnota je úměrná zmenšení entropie systému.“[5]

V tomto textu se ovšem bude jednat převážně o pohled ekonomický, kdy je informace brána jako aktivum firmy. Může to být know-how, personální záznamy zaměstnanců, dodavatelů, klientů, ale také vývoj nového výrobku, účetní knihy atd.

„Podnikatelské informace jsou informace obíhající v podnikatelské sféře a využívané v ovlivňování výrobních, obchodních a jiných procesů. Týkají se především vztahů lidí k podnikatelské aktivitě, vztahů mezi sebou, jejich vzájemného působení, potřeb, zájmů, cílů, atd.“[6]

Informační výhoda je poté nejčastěji chápána jako spojení zajištění vlastních dat a znalosti podstatných informací o konkurenci nebo konkurenčním prostředí. Aby bylo výhody dosaženo je tedy potřeba vhodně používat ofenzivních i defenzivních technik. Ty budou představeny dále v textu.

Informace mohou být v různých formách. Elektronické - dvd, cd, disketa, data na pevném disku nebo písemné záznamy – výroční zprávy, účetní knihy, seznamy dodavatelů, atd.

[2] KUČEROVÁ. *Teorie informace* [online]. 2006 [cit. 2009-02-22]. Dostupný z WWW: <http://web.sks.cz/users/ku/uis/inform1.htm>.
[3] KUČEROVÁ. *Teorie informace* [online]. 2006 [cit. 2009-02-22]. Dostupný z WWW: <http://web.sks.cz/users/ku/uis/inform1.htm>.
[4] KUČEROVÁ. *Teorie informace* [online]. 2006 [cit. 2009-02-22]. Dostupný z WWW: <http://web.sks.cz/users/ku/uis/inform1.htm>.
[5] KUČEROVÁ. *Teorie informace* [online]. 2006 [cit. 2009-02-22]. Dostupný z WWW: <http://web.sks.cz/users/ku/uis/inform1.htm>.
[6] BRABEC, František, et al. *Bezpečnost pro firmu, úřad, občana*. [s.l.] : [s.n.], 2001. 400 s., s. 211

2.2.Důvod ochrany informací

Důvody ochrany jsou v některých případech zřejmé. Například vyzrazení tajemství vede k finanční ztrátě podniku. V těchto případech obvykle bývá stupeň zabezpečení vysoký. Jakmile se však nejedná o snadno prohlédnutelnou příčinu, bývá zabezpečení podceňováno. Seznam zákazníků a jejich charakteristika může být pro konkurenční podnik velmi cenná. Stačí se zaměřit na méně spokojené zákazníky a tím snížit pozici konkurence na trhu. Také je možné takto získané informace zveřejnit, a tak vystavit podnik žalobě ze strany zákazníků. Ztráta důvěryhodnosti v mnoha odvětvích zapříčiní celkový pád podniku, čímž opět získá konkurence.

Z výše uvedených důvodů vznikaly a vznikají nové obory jako počítačová bezpečnost či bezpečnost informačních systémů. Je nutné si uvědomit, že stát sice data chrání pomocí zákonů a vyhlášek, ale to konkurenci nemusí vadit.

Jaké okruhy je třeba chránit a jak jsou zajištěny zákonem? Jedná se o tyto oblasti:

- obchodní tajemství
- zvláštní skutečnost
- osobní a citlivé údaje
- utajované informace

Obchodní tajemství je v obchodním zákoníku vymezeno následovně:

„Předmětem práv náležejících k podniku je i obchodní tajemství. Obchodní tajemství tvoří veškeré skutečnosti obchodní, výrobní či technické povahy související s podnikem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu, nejsou v příslušných obchodních kruzích běžně dostupné, mají být podle vůle podnikatele utajeny a podnikatel odpovídajícím způsobem jejich utajení zajišťuje.“[7]

Obchodním tajemstvím se myslí informace o provozech a provozních činnostech, know-how, obchodních aktivitách, apod.

Zvláštní skutečnost je v právním systému České republiky řešena v zákonu 240/2000Sb., o krizovém řízení a změně některých zákonů. V oblasti osobní a administrativní bezpečnosti vydala vláda ČR Nařízení vlády č. 462/2000 Sb.

[7] HAVIT, S.R.O.. *Zákony, vyhlášky, nařízení vlády a jiné právní normy* [online]. 2009 [cit. 2009-03-01]. Dostupný z WWW: < http://business.center.cz/business/pravo/zakony/obchzak/cast1.aspx#par17>, § 17.

Osobní a citlivé údaje dříve ochraňoval zákon č. 256/1992Sb., o ochraně osobních údajů v informačních systémech. Ten byl zrušen a nahrazen zákonem č. 101/2000Sb., o ochraně osobních údajů. Tento zákon je významný z hlediska globální informační bezpečnosti. Únik osobních údajů může být zneužit v mnoha podobách – vydírání, korupce, ztráta jména (goodwill),…

Přesná definice osobního nebo citlivého údaje jsou uvedeny v §4 odstavce a) a b).

„a) osobním údajem jakýkoliv údaj týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze na základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho identitu. O osobní údaj se nejedná, pokud je třeba ke zjištění identity subjektu údajů nepřiměřené množství času, úsilí či materiálních prostředků“[8]

„b) citlivým údajem osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v politických stranách či hnutích nebo odborových či zaměstnaneckých organizacích, náboženství a filozofickém přesvědčení, trestné činnosti, zdravotním stavu a sexuálním životě subjektu údajů“[9]

Utajované informace jsou ošetřeny v zákoně č. 412/2005SB, Zákon o ochraně utajovaných informací a bezpečnostní způsobilosti. Zákon upravuje, které informace mohou být vedeny jako utajované, podmínky přístupu k nim, jak mají být zabezpečeny, atd.

[8] NAKLADATELSTVÍ SAGIT. *Sbírka zákonů* [online]. 1996-2009 [cit. 2009-03-01]. Dostupný z WWW: <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00101&cd=76&typ=r>.
[9] NAKLADATELSTVÍ SAGIT. *Sbírka zákonů* [online]. 1996-2009 [cit. 2009-03-01]. Dostupný z WWW: <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00101&cd=76&typ=r>.

3. Competitive intelligence

Vývoj competitive intelligence je možné, s trochou nadsázky, sledovat s vývojem lidské společnosti. Nicméně tehdejší praktiky by se dnes považovaly za různé druhy špionáže. V podobě, jak je známo dnes, se formovalo od 80. let 20. století. Vzniká ve Spojených státech jako nutný následek sílící konkurence východních zemí, převážně Japonska. Americký trh nebyl připraven potýkat se s jinou než tuzemskou konkurencí. Tamní obchodníci nepovažovali ostatní země za výraznějšího konkurenta. V roce 1986 již byla založena první profesní organizace sdružující informační zpravodaje pod označením Society of Competitive Intelligence Professional (SCIP). V roce 1990 měla svou pobočku na evropském kontinentu a teprve v relativně nedávné době i v České republice pod označením SCIP CZECH. Výraz competitive intelligence se v české literatuře nejčastěji objevuje pod označením konkurenční zpravodajství. Takto bude nejčastěji označován i v tomto textu.

3.1.Charakteristika konkurenčního zpravodajství

Definic charakterizující konkurenční zpravodajství je více. Pro porovnání jsou níže uvedeny dvě definice.

„Pojem "Competitive Intelligence" (CI) se používá pro označení činnosti nebo procesu sloužícího pro získávání a interpretaci informací umožňujících rozhodování subjektů v konkurenčním prostředí (rozumí se dosažení, udržení nebo zvýšení konkurenční výhody firmy). V podstatě se jedná o postupy a metody běžně užívané zpravodajskými službami (Intelligence services) s tím, že jsou zde respektována právní a etická pravidla platná pro komerční prostředí."[10]

Terminologická databáze TDKIV definuje konkurenční zpravodajství jako *„zjišťování, sledování a vyhodnocování konkurenčního prostředí (firmy, organizace) s cílem odhalit slabé a silné stránky konkurence, rozpoznat její strategické záměry. Zahrnuje analýzu a syntézu dat, resp. informací, které se transformují do strategických znalostí, shromažďování informací o konkurenci a sledování subjektů firemního okolí (trh, stát, právo a legislativa, politické a demografické souvislosti).* [PAPÍK-1998:4-5]"[11]

Obě definice hovoří o konkurenčním zpravodajství zjednodušeně jako o cíleném získávání informací z konkurenčního prostředí v souladu s etickými a právními normami. Jedná se multidisciplinární obor zahrnující matematiku, ekonomii, statistiku, psychologii či informatiku.

[10] BRABEC, František, et al. *Bezpečnost pro firmu, úřad, občana*. [s.l.] : [s.n.], 2001. 400 s., s.267

[11] KUČEROVÁ. *Česká terminologická databáze knihovnictví a informační vědy* [online]. 2005 [cit. 2009-03-01]. Dostupný z WWW: <http://sigma.nkp.cz/F/TAELM253K8MN7Y6CDDHP338BFKCKK26IM3SIFXUEUP4RNDF616-00167?func=full-set-set&set_number=028974&set_entry=000002&format=999>.

Odkud tedy zpravodajové získávají informace? Pro nalezení odpovědi je uvedeno dělení zdrojů informací z pohledu deontologie.

- Otevřené zdroje
    - Publikované
    - Nepublikované
- Uzavřené zdroje
    - Důvěrné
    - Chráněné

Otevřené zdroje jsou volně dostupné. Jejich poskytnutí se děje s vědomím zdroje. Liší se v úrovni obtížnosti jejich získání. Oproti tomu uzavřené zdroje nelze získat jinak, než porušením jedné či obou rovin - etičnost a legalita. Důvěrné, též označované jako privátní zdroje lze získat legálně, ale jejich použití se považuje za neetické. K chráněným neboli tajným zdrojům se lze dostat jen porušením zákona nebo ochrany prováděné vlastníkem.

Následující tabulka 1 znázorňuje srovnání přínosů a nákladů na jednotlivé typy. Patrná je dominance množství informace u otevřených publikovaných zdrojů a náklady u uzavřených chráněných zdrojů. Z toho plyne význam a široké uplatnění konkurenčního zpravodajství, které pracuje s otevřenými zdroji.

Tabulka 1: Přínosy a náklady na zisk informace, Zdroj: [1]

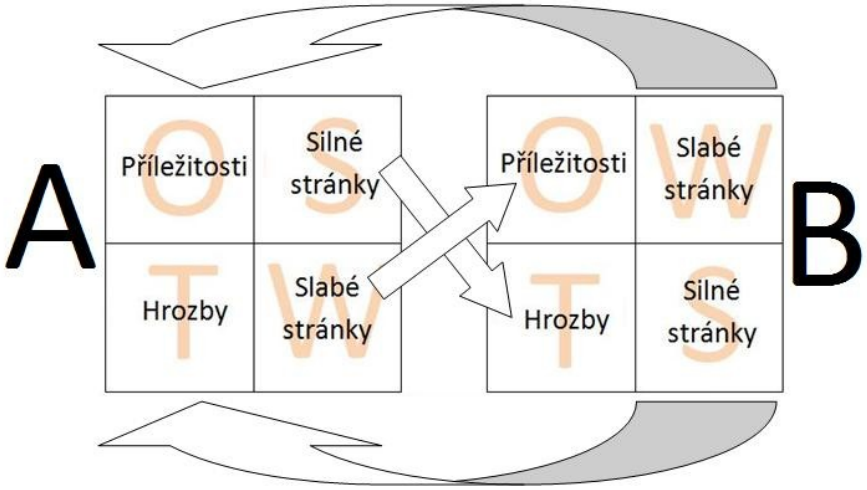
Typ zdroje	Množství informace	Náklady
Otevřené publikované informace	80%	20%
Otevřené nepublikované informace	5%	10%
Uzavřené důvěrné informace	5%	20%
Uzavřené chráněné informace	10%	50%

Jednou z nejčastějších metod v marketingu pro svou snadnost a názornost je SWOT analýza. Její zjednodušený model je na obrázku 1.

Obrázek 1: SWOT analýza

Metoda SWOT spočívá v analýze a klasifikaci jednotlivých faktorů, které se dělí do čtyř oblastí. Jsou jimi silné a slabé stránky podniku, příležitosti a hrozby. Na tomto modelu lze velmi dobře ukázat zaměření konkurenčního zpravodajství z hlediska managementu.

Otázka silné a slabé stránky se zjišťuje pomocí interní analýzy, kterou zabezpečuje směr zvaný business intelligence. Jeho propojení s konkurenčním zpravodajstvím bude vysvětleno později. Příležitosti a hrozby jsou naopak předmětem zájmu externí analýzy a tedy konkurenčního zpravodajství. Tyto dvě oblasti nezjišťuje podnik jen analýzou sebe sama, ale také zaměřením se na SWOT analýzu konkurenčního prostředí. Vazba dvou SWOT analýz konkurenčních podniků je ukázána na obrázku 2.



Obrázek 2: Vztah SWOT analýz konkurence

Provázanost je nasnadě. Silné stránky konkurence znamenají hrozby, slabé stránky poté příležitost. Vztah je samozřejmě obousměrný.

Konkurenční zpravodajství se dělí na dva hlavní směry podle předmětu zájmu.

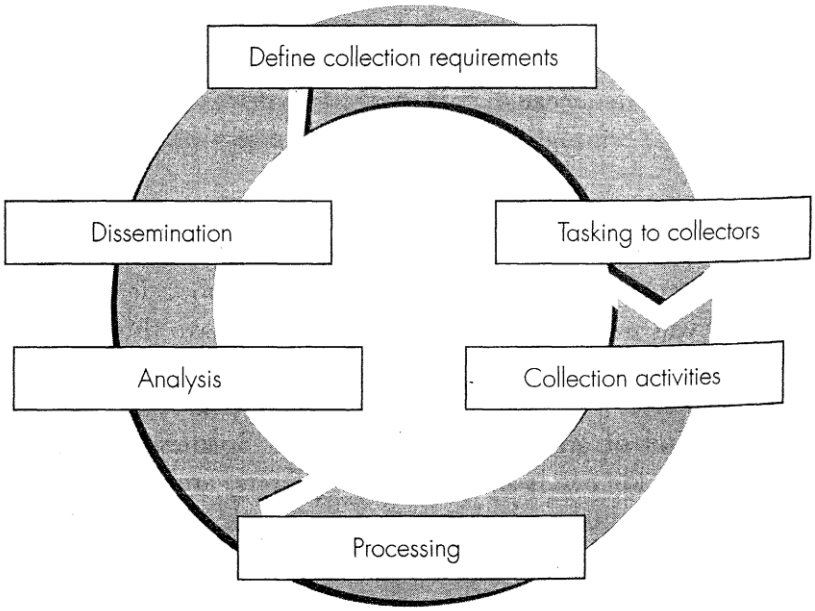
- Ofenzivní směr
- Defenzivní směr

V dalším textu jsou tyto oblasti rozepsány blíže včetně jejich vzájemného vztahu. Pro firmy je nezbytné přijmout skutečnost, že bez tohoto nástroje rapidně klesá konkurenceschopnost.

3.2.Ofenzivní konkurenční zpravodajství

Cílem ofenzivní stránky je zisk relevantních informací o prostředí a konkurenci. Nejde o zisk zbytečně velkého množství dat, které vytvoří informační chaos. Proto je vhodné činnost zahájit otázkami stylu:, oč má zadavatel konkrétně zájem, kolik času je k dispozici a jaké jsou finanční prostředky. John Nolan ve své knize Confidential uvádí jako základní právě tyto tři veličiny - finance, rychlost a kvalitu. Platí, že chce-li klient informace rychle a kvalitně, bude to drahé. Žádá-li to levně a rychle, nebude to kvalitní. Je tedy vhodné najít rovnováhu přijatelnou pro klienta.

Jak bylo řečeno výše, konkurenční zpravodajství je kontinuální proces. Na obrázku 3 je tento cyklus zachycen.



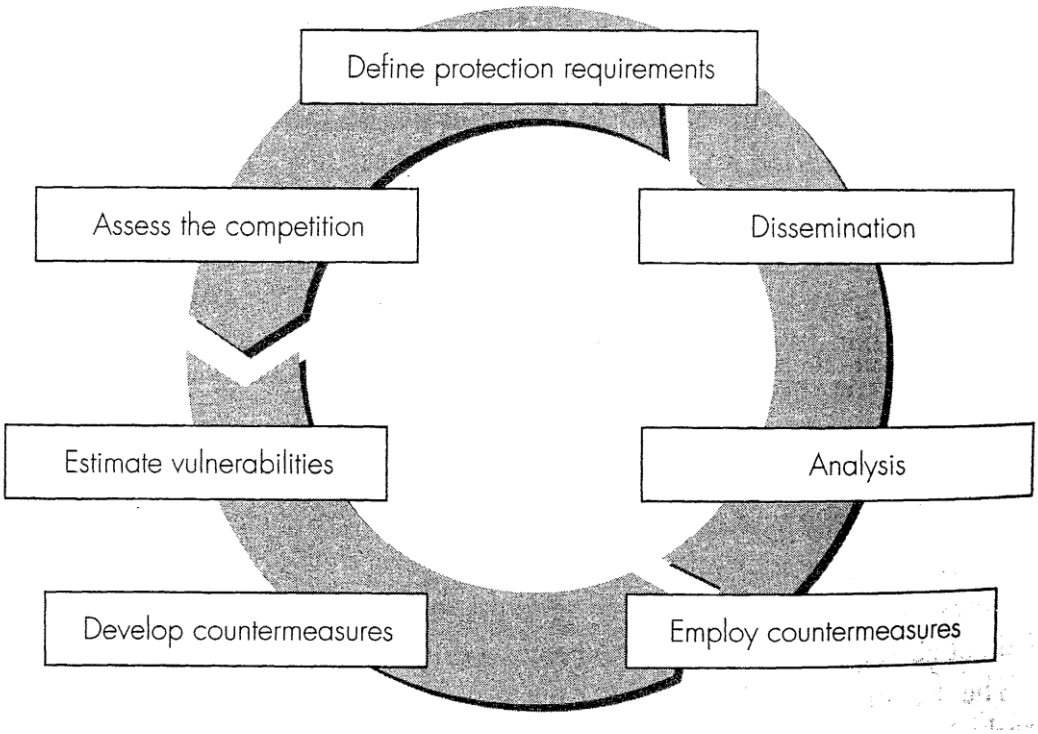
Obrázek 3: Cyklus ofenzivního zpravodajství, Zdroj: [14]

- První částí je definování požadavků, cílů (Define collection requirements). Tato fáze obsahuje určení směrů, způsobů a postupů, kterými bude informace opatřena. Plán využívá zpětné vazby pro pravidelnou aktualizaci odpovědí na následující otázky: co už firma ví a co potřebuje zjistit, z jakého důvodu to potřebuje zjistit a dokdy to potřebuje zjistit.
- Následuje rozdělení úloh pro zpravodaje (Tasking to collectors). Tento bod je zejména u rozsáhlejších úloh, na kterých pracuje více lidí současně.
- Třetí částí je samotný sběr informací (Collection activities). Zde se specialista snaží nalézt odpovědi na dříve stanovené otázky. K tomu využívá primárních a sekundárních zdrojů. Je důležité informace ověřovat pro zajištění jejich spolehlivosti.
- Po třídění a porovnávání následuje zpracování (Processing). Specialista se snaží informacím porozumět.
- V další fázi dochází k analýze (Analysis) pomocí analyticko-syntetických procesů, data-miningu, atd. Snahou je najít latentní informace.
- Poslední fází je distribuce (Dissemination). Zde je již předána komplexní zpráva klientovi v přehledné podobě. Často na základě závěrů vyvstanou nové otázky a cyklus se opakuje.

3.3.Defenzivní konkurenční zpravodajství

Je třeba si uvědomit, že konkurenční zpravodajství není výsadou jedné firmy. Naopak jej využívá, ač zvolna, čím dál více podniků, které si uvědomují jeho význam. Jak roste jeho používání konkurencí, je analogicky větší pravděpodobnost, že bude domovská firma podrobena analýze některým z řady konkurentů. Neměla by se podcenit ani možnost kybernetického útoku nebo špionáže. Také z těchto důvodu je potřeba vlastní citlivé údaje vhodně zabezpečit. I v tomto případě se jedná o cyklus, který by měl být neustále aktualizovaný pomocí zpětné vazby.

Průběh je podobný jako v případě ofenzivního zpravodajství. Na obrázku 4 je cyklus naznačen.



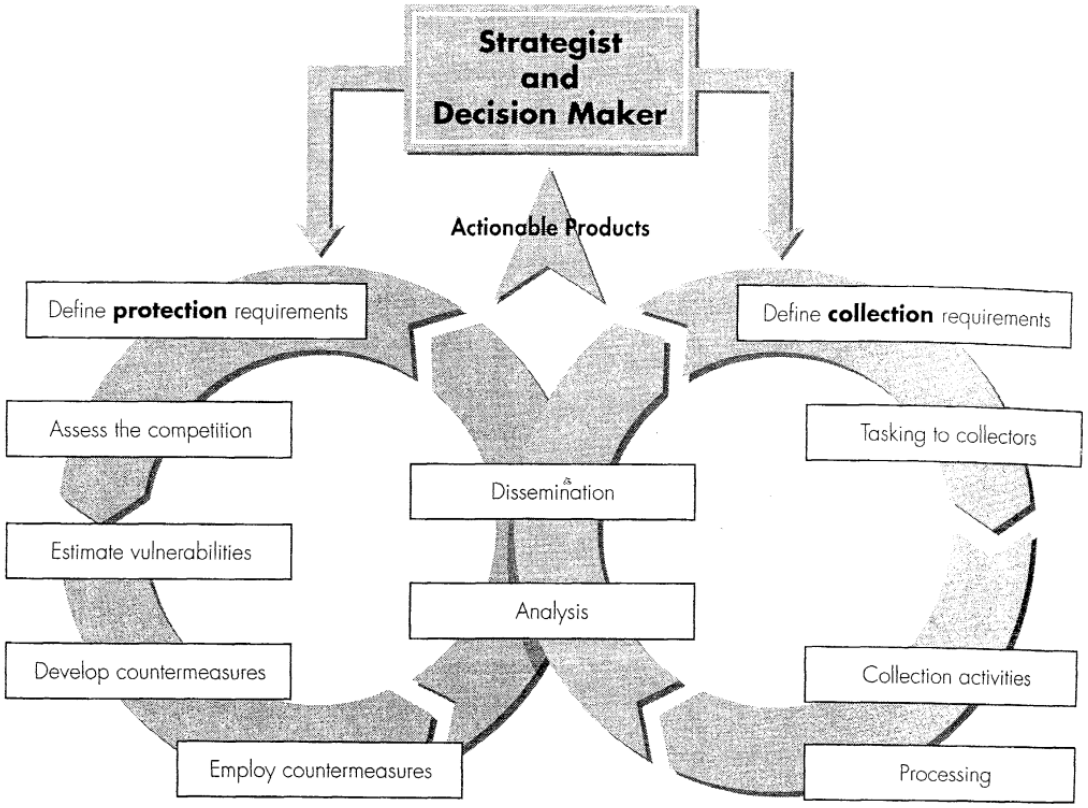
Obrázek 4: Cyklus defenzivního zpravodajství, Zdroj: [14]

- Hlavní je definovat vlastní požadavky na ochranu (Define protection requirements). Je vhodné si opět položit základní otázky. U defenzivního zpravodajství znějí - Co chránit, jak to chránit a jak dlouho to chránit? Již v této části bývají časté nedostatky. Zveřejnění dokumentu po uzavřeném kontraktu, zbytečné množství chráněných údajů nebo údajů, které již není nutno chránit. Tyto nedostatky v samotném návrhu vedou buď k nadbytečným výdajům za bezpečnostní prvky nebo nedostatečnému střežení informací.
- Druhým bodem je odhadnout konkurenci (Assess the competition). Proti komu se vlastně firma brání. Jedná-li se o firmu v odvětví, která má minimální konkurenci (tzv. modré okno oceánu), není nutné uvolnit na bezpečnost tolik nákladů.
- Následuje odhad vlastní zranitelnosti (Estimate vulnerabilities). Ten by měl být realistický nebo pesimistický. Optimistický vede k pozdější otevřenosti systému. John Nolan radí, jako jednu z efektivních metod pro nalezení nedostatků ve vlastním obranném systému, provést útok sám na sebe. Těmito penetračními testy lze zavčasu odhalit slabá místa.
- Jsou-li známy odpovědi na výše uvedené otázky, začíná tvorba protiopatření (Develop countermeasures).

- Poslední dvě fáze jsou totožné s ofenzivním zpravodajstvím. Analýza (Analysis) a distribuce (Dissemination) vzniklé bezpečnostní politiky.

3.4.Vztah ofenzivního a defenzivního konkurenčního zpravodajství

Nyní jsou jasně definovány dvě složky konkurenčního zpravodajství. Z uvedených popisů se dá usoudit, že defenzivní zpravodajství je aplikováno uvnitř podniku, zatímco ofenzivní zpravodajství sahá do vnějšího prostředí. Bylo by však chybou vést je odděleně v domnění, že mezi nimi není žádná spojitost. Naopak je vhodné obě složky provázat, jak je znázorněno na obrázku 5. Závěry z ofenzivního zpravodajství lze uplatnit i ve vlastní firmě a je možné, že stejné trhliny v bezpečnosti, které odhalí defenzivní zpravodajství, budou i u konkurence.



Obrázek 5: Vztah ofenzivního a defenzivního CI, Zdroj: [14]

Vzájemný vztah si lze představit jako dvě ozubená kola, přičemž činnost prvního ovlivňuje druhé. Teprve informace takto získané lze pokládat za správný výstup konkurenčního zpravodajství (Actionable products), který podporuje vrcholná, strategická rozhodování firmy (Strategist and

decision maker). S informacemi této úrovně by měl být kvůli zajištění vyšší bezpečnosti obeznámen pouze top management.

3.5.Rozdíl a vztah mezi business intelligence a competitive intelligence

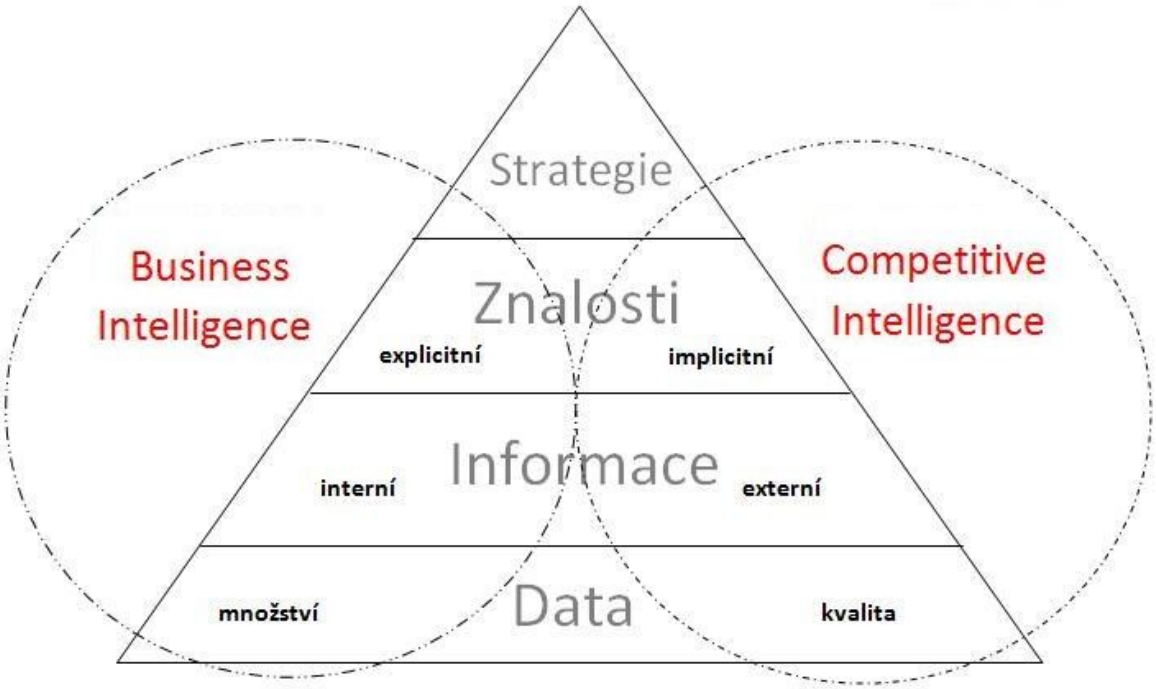
Výše v textu byl zmíněn pojem business intelligence. V této části bude více přiblížen a dán do kontextu s konkurenčním zpravodajstvím. Pro základní představu, co business intelligence znamená, je uvedena definice:

„Business Intelligence je sada procesů, aplikací a technologií, jejichž cílem je účinně a účelně podporovat rozhodovací procesy ve firmě. Podporují analytické a plánovací činnosti podniků a organizací a jsou postaveny na principech multidimenzionálních pohledů na podniková data.“[12]

Business intelligence se snaží o prognózu vývoje podnikání na základě zkušeností a odhadů aplikovaných na získané informace. Charakteristika je obdobná jako u konkurenčního zpravodajství. Jak se tedy liší business intelligence od competitive intelligence? V mnohé literatuře jsou tyto pojmy zaměňovány či udávány jako totožné. Tomu přispívá i fakt, že tyto směry vznikly přibližně ve stejnou dobu. V dnešní podobě se začíná objevovat na konci 70. let 20. století. V 80. letech jsou již publikovány první práce. Podoba této disciplíny se pochopitelně stále vyvíjí a v mnoha oblastech se s konkurenčním zpravodajstvím překrývají. Odlišnosti tam nicméně přeci jen jsou.

Hlavní rozdíl mezi těmito zpravodajstvími je v informacích, které používají. Zatímco business intelligence čerpá hlavně z vnitřních zdrojů za podpory nástrojů data-miningu či text-miningu, konkurenční zpravodajství se snaží nalézt relevantní zdroje dat v externím prostředí. Tato myšlenka včetně zobrazeného vztahu competitive a business intelligence je znázorněna na obrázku 6.

[12] NOVOTNÝ, Ota, POUR, Jan, SLÁNSKÝ, David. *Business Intelligence : Jak využít bohatství ve vašich datech*. [s.l.] : [s.n.], 2005. 255 s., s.19



Obrázek 6: Vztah konkurenčního zpravodajství a business intelligence

Ačkoli se oba okruhy zabývají shodnými stupni vyobrazené pyramidy (budou rozebrány v další kapitole), jedná se vždy o odlišný přístup. Business inteligence se zaměřuje na explicitní znalosti a již zmíněné interní informace, zatímco konkurenční zpravodajství pracuje s externími zdroji a implicitními znalostmi. Firma by se měla snažit o aplikaci obou typů zpravodajství a podporovat jejich kooperaci.

Výstupem je schopnost informovat poslední a nejvyšší typ zpravodajství. To se nachází nad nimi a stará se o strategická rozhodnutí. Obvykle bývá nazýváno podnikové zpravodajství.

4. Knowledge management

Knowledge management též často překládaný jako „řízení znalostí“, „správa znalostí“ či „znalostní management“ je dalším nástrojem v rukou firmy. Jeho detailní popis vydá na samostatnou práci. Zde bude charakterizován a spojen v kontextu s bezpečnosti informací a konkurenčním zpravodajstvím.

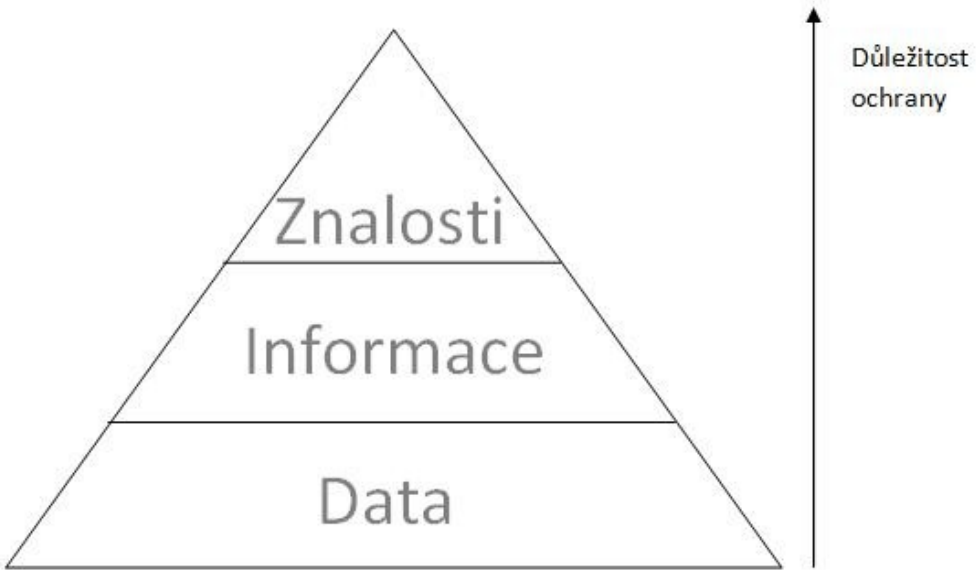
4.1.Charakteristika knowledge management

Sdílení informací v rámci kooperujících firem je osvědčená praxe. Postupem času se ale vývoj od nalezení informace, jejího pochopení a aplikace ukázal příliš zdlouhavý. Řešením této otázky je knowledge management, který nesdílí jen data či informace, ale přímo znalosti.

Nejprve je vhodné stanovit rozdíl mezi znalostí a informací. Jedním z možných hierarchických dělení je následující:

- Data (text, fakta, obrazy, zvuk)
- Informace (organizovaná, strukturovaná, interpretovaní, shrnutá data)
- Znalosti (případ, pravidlo, proces, model)

První stupeň je libovolná skutečnost nebo její interpretace. V druhém je důležité zdůvodnění, abstrakce, vztahy a aplikace. Znalosti navíc zahrnují zkušenost, principy a učení se. Definice pro jednotlivé body se různí, navíc někdy následuje další krok – moudrost, zpravodajství. Zde však postačuje dělení toto. Na obrázku 7 je závislost jednotlivých stupňů na významu zabezpečení.



Obrázek 7: Vztah bezpečnosti a stupňů dat

Závislost je přímo úměrná. Znalosti by měly být chráněny maximálně. Získá-li ale útočník dostatečný počet dat, sám si je na informace a poté znalosti převede. Význam ochrany dat by se proto neměl podceňovat.

Jak tedy definovat knowledge management? Je obtížné najít všeobsahující definici, níže uvedená nabízí dobrou představu.

„Praktická odborná činnost zaměřená na využití znalostí v rozhodovacích a řídících procesech za podpory informačních a komunikačních technologií. Zabývá se navrhováním, implementací a provozem systémů správy znalostí, jež zahrnují procesy získávání, reprezentace a zpracování, ukládání, vyhledávání a odvozování, prezentace, sdílení a distribuce znalostí. Teoretické zázemí tvoří kognitivní vědy a aplikační obory umělé inteligence (např. znalostní inženýrství), metody a techniky práce jsou odvozeny z praxe informačního managementu.“[13]

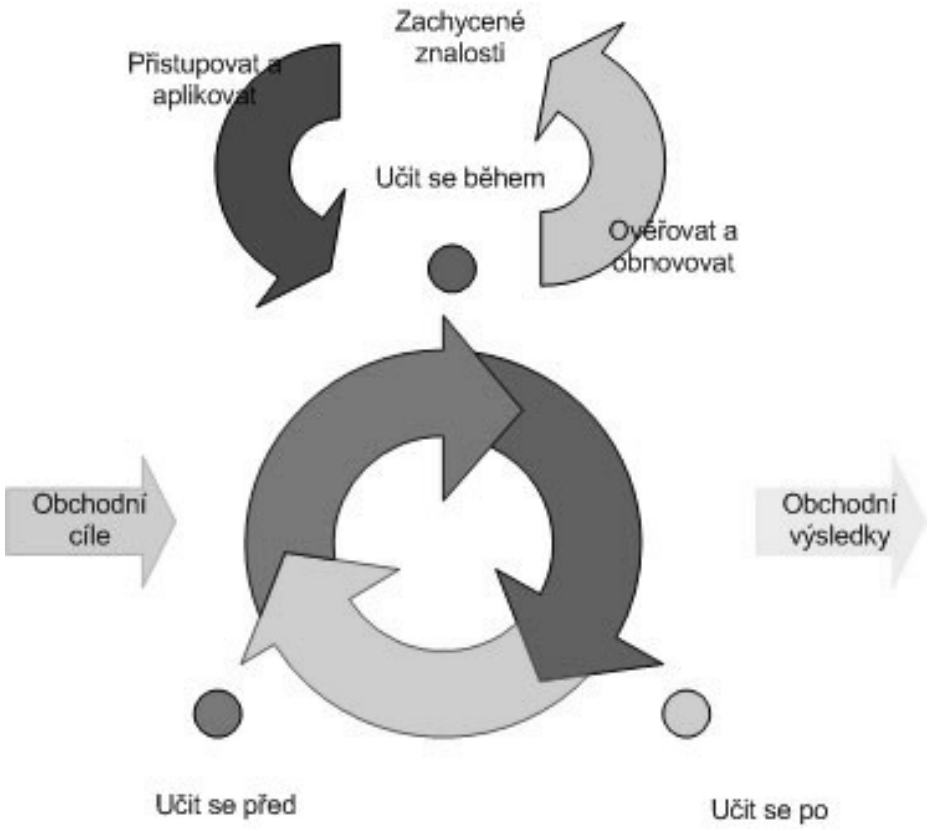
Knowledge management se snaží spojit znalosti jednotlivců do širšího celku pro efektivnější řešení úloh. Dalo by se říci, že se snaží z implicitních znalostí (nekodifikované znalosti v hlavách lidí) utvořit explicitní (zaznamenané). Děje se tak z prostého důvodu. Sdílení znalostí umožňuje jednak rychlejší řešení nového problému, tak také zamezuje, aby tým lidí zbytečně řešil již úspěšně vyřešený problém. Knowledge management je chápán jako hybridní disciplína. Nelze určit, zda se jedná o vědu či dovednost.

4.2.Souvislost mezi knowledge management a competitive intelligence

Lze využít knowledge management v konkurenčním zpravodajství? Konkurenční zpravodajství stejně jako management znalostí zahrnuje více disciplín. Nelze je přesně zařadit a jejich hranice se logicky překrývají. Bylo by zbytečné omezovat se v získávání konkurenční výhody jen na úzkou oblast možností. Odpověď na úvodní otázku je tedy určitě kladná a to hned v několika směrech.

Modely a metodiky používané v knowledge managementu lze poměrně úspěšně aplikovat do konkurenčního zpravodajství. Vhodným příkladem je holistický model na obrázku 8.

[13] KUČEROVÁ. *Česká terminologická databáze knihovnictví a informační vědy* [online]. 2001 [cit. 2009-03-01]. Dostupný z WWW: <http://sigma.nkp.cz/F/G8JPQQ9EAXK7XJNVDM6HMA5MPCQRI1497EVL8DGF8BYKJK1T6N-07053?func=find-b&find_code=WTD&x=0&y=0&request=knowledge+management&adjacent=N>.



Obrázek 8: Holistický model, Zdroj: [6]

Model znázorňuje průběh mezi zadáním obchodních cílů a obchodních výsledků. I při získávání informací panuje obdobný postup.

- Učit se před – je možné, že obdobnou věc již někdo řešil. Proč tedy nevyužít jeho poznatků? Před další činností by měl zpravodaj zjistit dostupné informace.
- Učit se během – tzv. průběžné učení. Tato fáze umožňuje reflexi získaných poznatků a stanovení dalších postupů.
- Učit se po akci – proces učení se po akci významně napomáhá při plnění dalšího úkolu či projektu. Původní znalosti jsou zlepšovány a optimalizovány.
- Zachycené znalosti – zde je snaha o uchování znalosti v takové podobě, aby se dala znovu použít. Zůstane-li znalost implicitní, hrozí její ztráta s odchodem zaměstnance. Efektivním způsobem pro zachycení znalostí je systematické budování znalostních bází společnosti.

Poslední bod má dvě stránky. Je v konkurenčním zpravodajství vhodné vytvářet znalostní bázi? Zde již odpověď tak jednoznačná není. Její existence je zatím třeba ve formě přednášek a konferencí například společnosti SCIP CZECH. V rámci společnosti či společností spolupracujících je to vhodné i přes to, že lidé ztrácejí svou jedinečnou. Jakmile něco vytvoří, vymyslí, stává se to vlastnictvím podniku. Pro zabezpečení a růst firmy je to však značná výhoda.

Dalším směrem může být uvědomění si existence takového managementu. Jakmile se do báze znalostí získá přístup třeba pomocí informátora, je k dispozici rozsáhlé množství zdrojů. V knihách o knowledge management se tvorba bází propaguje, ale již ne tolik jejich zabezpečení. Přitom průměrný sociotechnik zde získá dokonalý přehled o vnitřních poměrech firmy, které lze využít.

4.3.Využití knowledge management při ochraně informací

Knowledge management je tedy možné použít pro zefektivnění zisku informací. Nyní je otázkou, zda také pro zlepšení defenzivní složky konkurenčního zpravodajství.

Defenzivní konkurenční zpravodajství má hlavně funkci preventivní. Zde je možné poučit se z případů úniku informací v jiných společnostech. Jak postupovali, kde se stala chyba a na základě jejich znalosti vylepšit vlastní obrannou linii. Méně přívětivá je druhá možnost, že došlo k narušení informační bezpečnosti u domovské firmy. I zde lze však získat cenné znalosti do budoucnosti. Využít se dá metoda AAR používaná u americké armády a převzatá do knowledge managementu.

AAR neboli After Action Report se používá pro zpětné hodnocení právě vykonané akce, projektu, atd. Jedná se o okamžitou odezvu, dokud si všichni zúčastnění pamatují přesně detaily. Zatímco v prostředí knowledge managementu tato metoda slouží pro srovnání skutečných a plánovaných výsledků, v oblasti konkurenčního zpravodajství ji lze užít například pro bezpečnostní incident. Okamžitě se tak napraví zjištěné nedostatky a nebude poskytnut prostor pro další útoky po dobu oslabení.

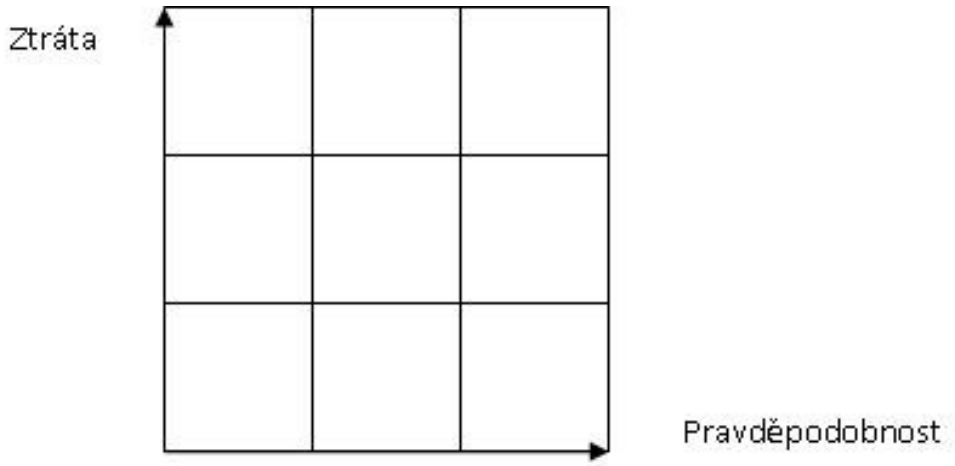
Znalostní báze se dá také využít jako výchozí bod pro tvorbu bezpečnostní politiky nově vznikající pobočky. Například firma vytvářející dceřinný podnik v kulturně odlišném prostředí může predikovat možné potíže a jak jim předejít.

5. Zajišťování informační výhody

Zajištění informační výhody lze chápat buď jako průzkum konkurenčního prostředí nebo jako zabezpečení vlastních firemních dat. V následujících analýzách jsou využita data převzatá z průzkumů profesionálních firem. Název zdroje, rok průzkumu, relevantní otázky a počet respondentů je vždy uveden. Důvodem pro tento způsob zisku dat je citlivost zjišťovaných údajů. I tato data nebudou zcela odpovídat realitě obzvlášť v otázkách bezpečnostních incidentů. Skutečnost, že byla ukradena data osobní povahy, by měla další dopad na ztráty, kterým se snaží firma předejít.

5.1.Stanovení rizik

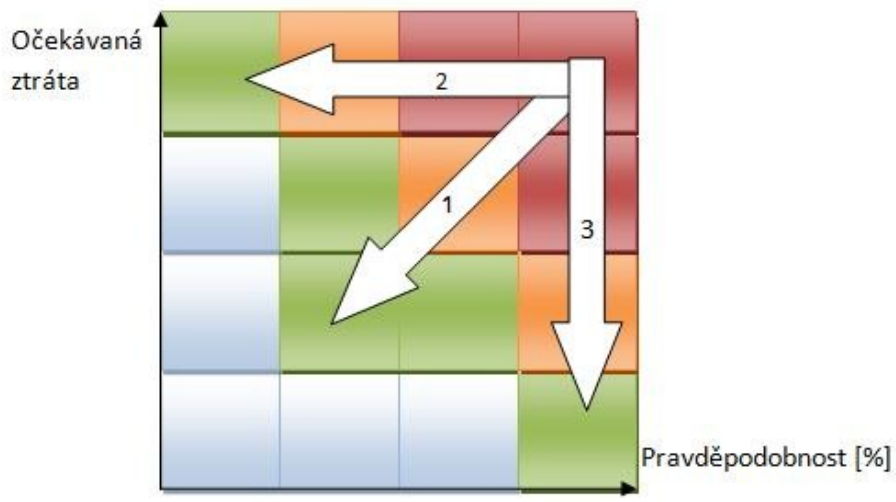
Jednou z možností sledování rizik ohrožujících prosperitu firmy je matice rizik též známá jako krizová matice Klause Winterlinga. Základní varianta je uvedena níže na obrázku 9.



Obrázek 9: Matice Klause Winterlinga

Matice je v podstatě Kartézskou soustavou souřadnic, jejíž osy znázorňují pravděpodobnost, s jakou nastane některá z krizových situací a v případě jejího vzniku, jaké jsou očekávané ztráty. Kvadrant je pro přehlednost rozdělen na jednotlivé shluky, které budou dále blíže vysvětleny.

Z matematického hlediska je riziko R funkcí několika proměnných. Lze jej vyjádřit rovnicí R = f(Z, p, t, x1, x2, ...,xn). Přičemž Z = ztráta, p = pravděpodobnost, t = čas a x jsou další faktory. Pro zjednodušení se počítá pouze s očekávanou ztrátou a pravděpodobností. Tedy R = p*Z. Tímto se získává bodové ohodnocení pro každou z krizových situací. Na obrázku 10 jsou znázorněny možnosti reakce na krizi.



Obrázek 10: Reakce na krizi

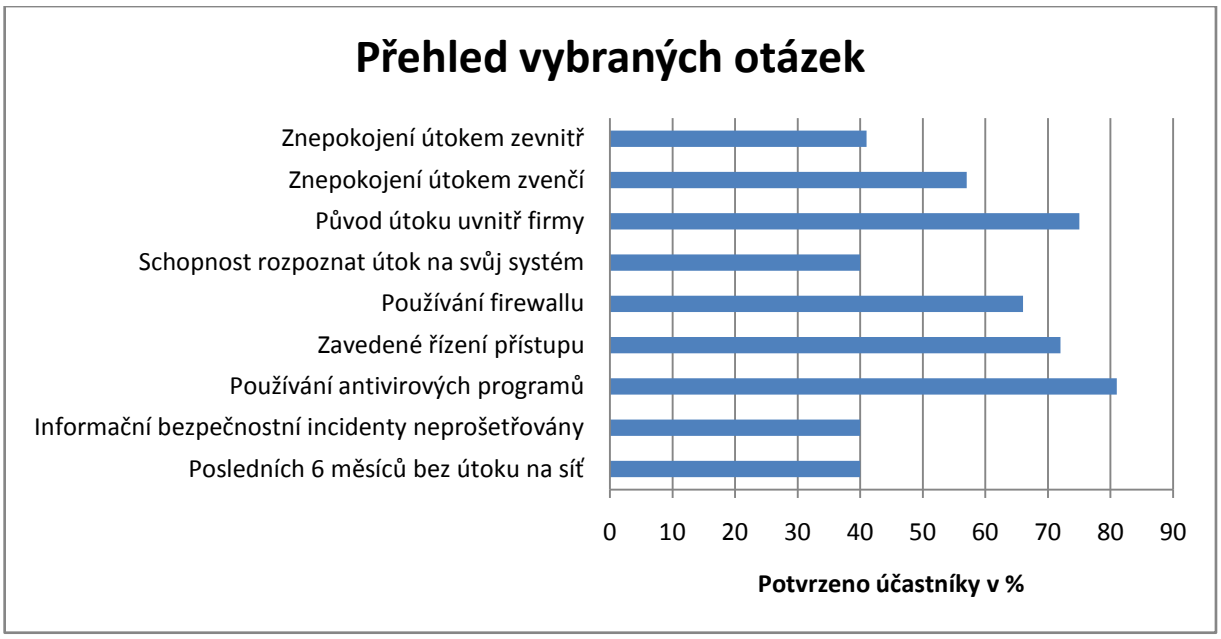
Na tomto obrázku je již upravená matice zahrnující barevně odlišené oblasti dle stupně rizika. Snahou je dostat se z červené oblasti do modré. Z výše uvedeného matematického zápisu je jasné, že možnosti jsou tři. Snížit prvního, druhého nebo oba činitele. Jako nejvhodnější se jeví snížit pravděpodobnost vzniku události. V případě informační bezpečnosti tedy jejich zajištění vhodnými, dříve uvedenými, prostředky. To ilustruje i následující příklad 1.

Příklad 1

V roce 2008 došlo u slovenského portálu Azet.sk k bezpečnostnímu incidentu. Na poskytované službě Zoznamka.sk bylo možné získat emailové adresy uživatelů. Celkem mohlo být získáno 900 000 emailů, které mohly být dále zneužity ke spamování (nevyžádané masově šířené sdělení) nebo phishingu (podvodná technika používaná k získávání citlivých údajů). Správnou analýzou situace se dalo problému snadno předejít. Bezpečnost portálu byla častokrát vytýkána.

V tomto konkrétním případě se dala použít metoda CAPTCHA. Jedná se o Turingův test, který se snaží rozpoznat skutečné uživatele od robotů. Jednou z podob je opisování textu z vygenerovaného obrázku. Tím by se snížila pravděpodobnost úspěšného útoku a redukci rizika. Ztráta se v tomto případě snižuje hůře. Portál utrpěl na pověsti a vystavuje se riziku žaloby. Možností snížení ztráty by bylo uvést riziko v podmínkách při registraci. Předešlo by se tak případné žalobě.

Během října a listopadu roku 2001 provedla společnost Ernst & Young celosvětový průzkum bezpečnosti informačních systémů. Proběhly osobní a telefonické rozhovory s celkem 459 vedoucími pracovníky této oblasti v jednotlivých společnostech. V následujícím grafu na obrázku 11 jsou zpracovány některé ze zjištěných relevantních údajů.



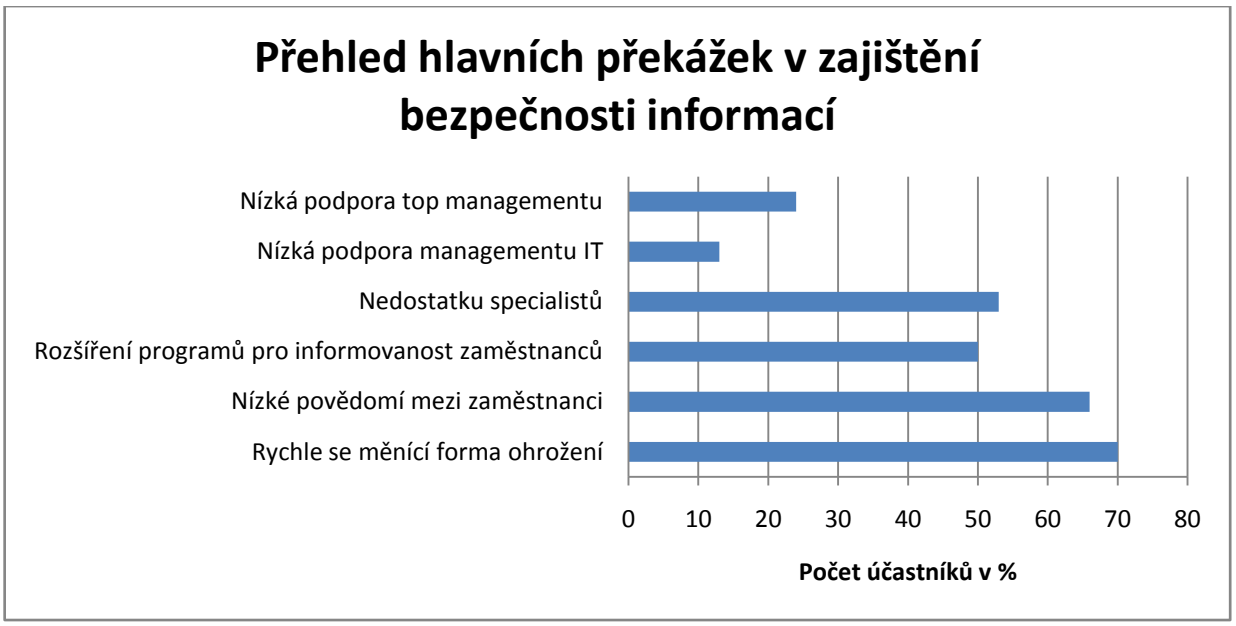
Obrázek 11: Vybrané otázky z průzkumu bezpečnosti firem

V grafu jsou zaznamenány skutečnosti a procento firem, kterých se týkají. Je-li tedy uvažována hypotetická matice, toto je jedna její osa. Hodnota je odvozena ze statistických údajů. Výše ztráty je subjektivním hodnocením firmy.

Z výzkumu plyne několik závěrů. Je-li dokázáno, že 75% útoků na bezpečnost informací společnosti je zevnitř, neměla by se tato oblast podceňovat. Útoku zevnitř se z dotazovaných 459 firem obává pouhých 188. Jako opatření by posloužila lepší informovanost zaměstnanců, ale o to se snaží jen polovina respondentů. Druhou možností je zvýšit povědomí pracovníků pomocí vhodných materiálů a školení. Toho je využito u 44% podniků. Je třeba pochopit, že útokem zevnitř se nemyslí jen zamýšlená sabotáž, ale také nechtěné smazání údajů, vyzrazení tajemství atd. Častější obava z kybernetického útoku z vnějšího prostředí vedla k poměrně vysokým četnostem u používání řízení přístupu (330), firewallu (303) a antivirového softwaru (372).

Moderní útoky na data, jako metoda sociálního inženýrství popsaná v knize Umění klamu autora Kevina Mittnicka, jsou stavěny tak, aby subjekt nerozpoznal, že byl vůbec nějaký útok proveden. Také pouhých 40% si je jisto, že by případné narušení bezpečnosti rozpoznalo. Poměrně velké procento firem ani útoky neprošetřuje, což ústí v permanentní zranitelnost.

Obrázek 12 znázorňuje názor samotných firem na příčinu problémů spojených se zajištěním bezpečnosti.



Obrázek 12: Přehled překážek při zajištění informační bezpečnosti

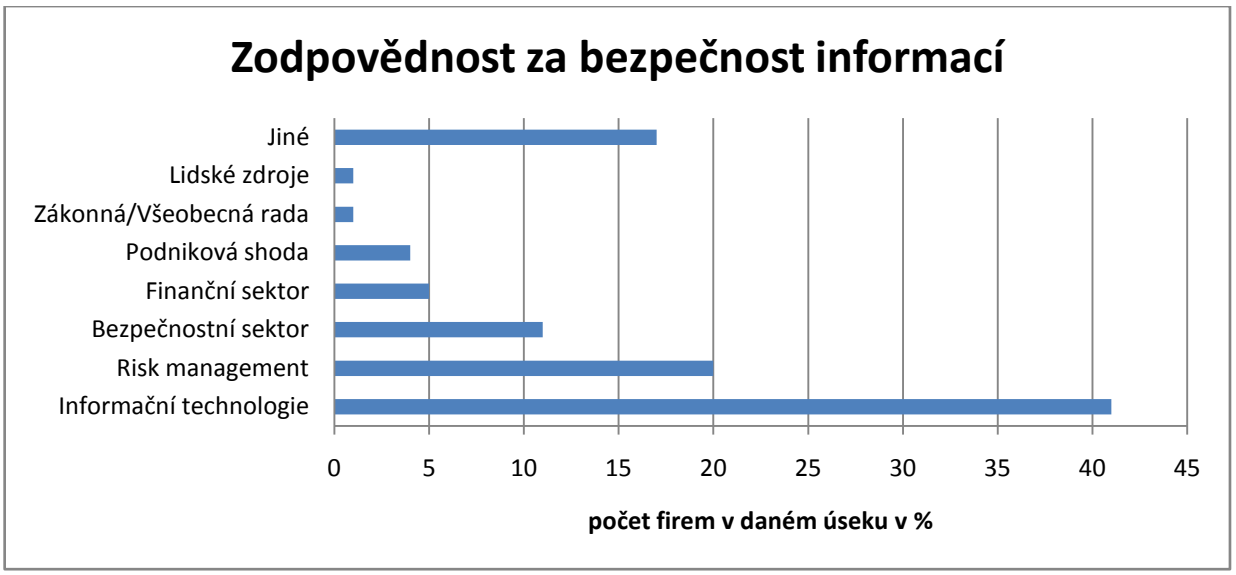
Výsledky v podstatě nabádají k zavedení specializovaného útvaru pro bezpečnost informací. Předpokladem by byl tým specialistů, který je schopný rychleji reagovat na variabilitu prostředí a může pořádat pravidelná školení o zacházení s citlivými daty společnosti.

5.2.Zodpovědnost za bezpečnost informací

Je otázkou, který firemní úsek by měl být zodpovědný za bezpečnost informací. Nejčastější přístup je delegace těchto povinností na úsek informačních technologií. Vychází to z historického vývoje, kdy počítače byly stěžejním bodem podniku a jejich zajištění bylo prioritou. Dnes je však tato představa zčásti mylná. Oddělení IT nemá ve valné většině případů k dispozici bezpečnostní politiku. Neví tedy, která data je třeba ochraňovat, jak dlouho a do jaké míry. Nevyhnutelným následkem neznalosti odpovědí na tyto otázky je neekonomické chování pro podnik - zbytečné náklady, chybné odhadnutí potřeb společnosti. Ochrana informací je většinou logicky propojena s krizovým managementem. Ztráta dat je jednou z nejhorších krizových situací, ke kterým může ve firmě dojít.

Tuto problematiku lze doložit průzkumem společnosti Ernst & Young's z roku 2008, který byl prozatím publikován pouze na anglických webových stránkách[14]. České firmy světový trend dohánějí, ale mnoho jich stále tuto oblast podceňuje. Počet respondentů průzkumu byl v tomto případě 1400. Pro vyšší objektivnost se jednalo o zástupce velkých a středních podniků z celého světa.

[14] ERNST & YOUNG'S. *GISS_2008_EN* [online]. 2009 [cit. 2009-03-30]. Dostupný z WWW: <https://www.aotalliance.org/docs/GISS_2008_EN.pdf>.



Obrázek 13: Zodpovědnost za bezpečnost informací

Patrná je dominance (41%) zodpovědnosti v sektoru IT. Risk Management, který je již vhodnější má pouze pětinový podíl. Přímo určené oddělení má pouhých 11%, což představuje 154 firem. Další úseky jsou pod 5 %. Jiná oddělení používá 17% podniků. Nicméně v tomto údaji jsou zahrnuty i podniky, které se o bezpečnost svých dat nestarají vůbec.

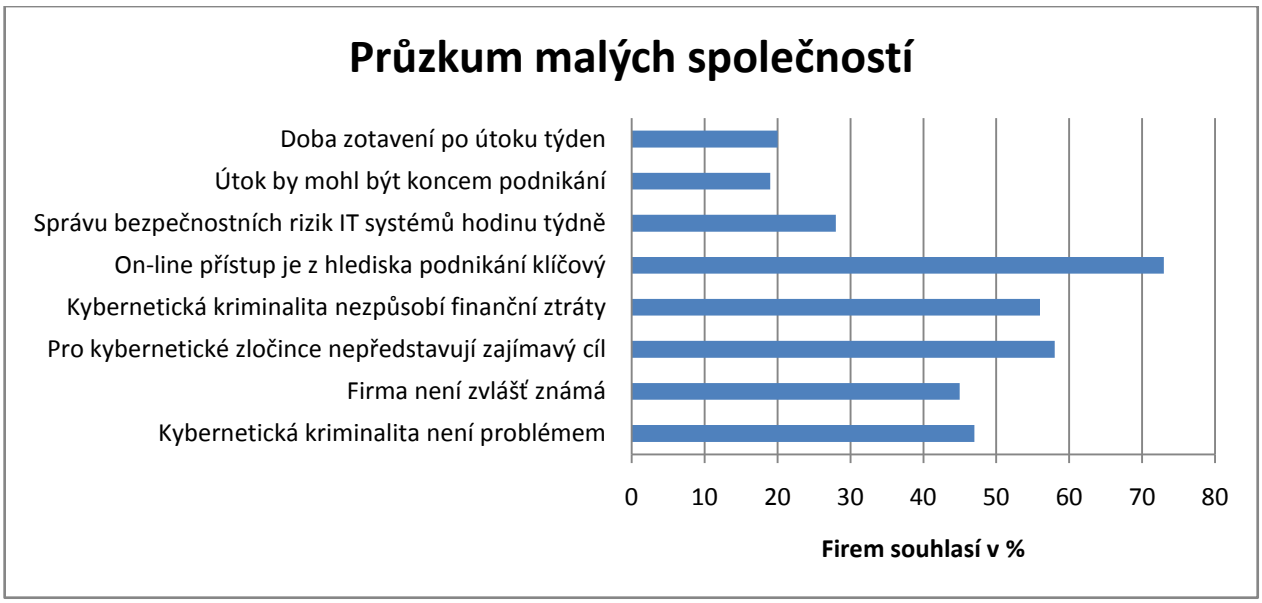
Porovnání mezi roky 2001[15] a 2008[16] nevykazuje velké zlepšení. V roce 2001 za kontinuitu provozu zodpovídalo oddělení IT ve 45%. A přitom neočekávané přerušení provozu zaznamenalo 75% podniků.

5.3.Rozdíl v přístupu k bezpečnosti v závislosti na velikosti firmy

V tomto bodě je hledána odpověď na otázku, zda a jak se liší přístup k ochraně informací u malých a velkých podniků. Malé podniky jsou stejně závislé na informacích jako velké, ale přesto mají pocit, že svou nevýrazností nepředstavují cíl kybernetického útoku.

Graf na obrázku 14 ukazuje názory zástupců malých firem dle průzkumu, který provedla firma McAfee v roce 2007[17]. Počet dotazových firem je 600. Velikost firmy je brána z hlediska počtu zaměstnanců. Malá firma se pohybuje v rozmezí 2-500.

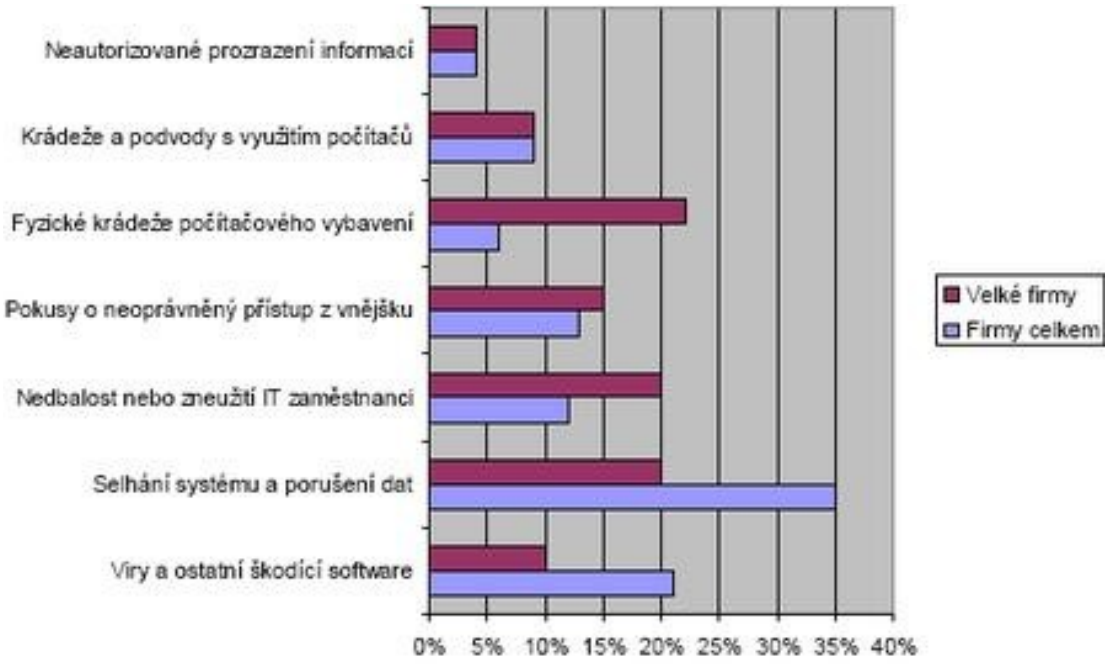
[15] ZONER SOFTWARE, S.R.O.. Většina útoků na informační systém má svůj původ uvnitř firem -- Interval.cz [online]. 2002 [cit. 2009-03-30]. Dostupný z WWW: <http://interval.cz/tiskove-zpravy/vetsina-utoku-na-informacni-system-ma-svuj-puvod-uvnitr-firem/>.
[16] ERNST & YOUNG'S. *GISS_2008_EN* [online]. 2009 [cit. 2009-03-30]. Dostupný z WWW: <https://www.aotalliance.org/docs/GISS_2008_EN.pdf>.
[17] IT SYSTEMS. *Kyberneticka-kriminalita-ve-firmach-z* [online]. 2007 [cit. 2009-03-30]. Dostupný z WWW: <http://www.systemonline.cz/zpravy/kyberneticka-kriminalita-ve-firmach-z.htm>.



Obrázek 14: Názor malých firem na bezpečnost

Jak je patrné, velké množství malých podniků si hrozbu kybernetických útoků nepřipouští nebo připouští, ale nemá prostředky pro svou ochranu. Téměř polovina účastníků (47%) se domnívá, že kybernetická kriminalita je problémem pouze velkých společností. 45% si myslí, že není významná a celých 58%, že nejsou důležitým cílem. 56% je názoru, že případný útok nezpůsobí finanční ztráty. Všechna čísla jsou opravdu vysoká a přitom 73 respondentů uvedlo, že on-line přístup je pro jejich podnikání klíčový. Pětina (20%) dokonce případný útok považuje za konec jejich podnikání. Přibližně stejný počet (20%) odhaduje dobu zotavení své firmy po kybernetickém útoku na dobu jednoho týdne. Finanční ztráty jsou v těchto případech značné.

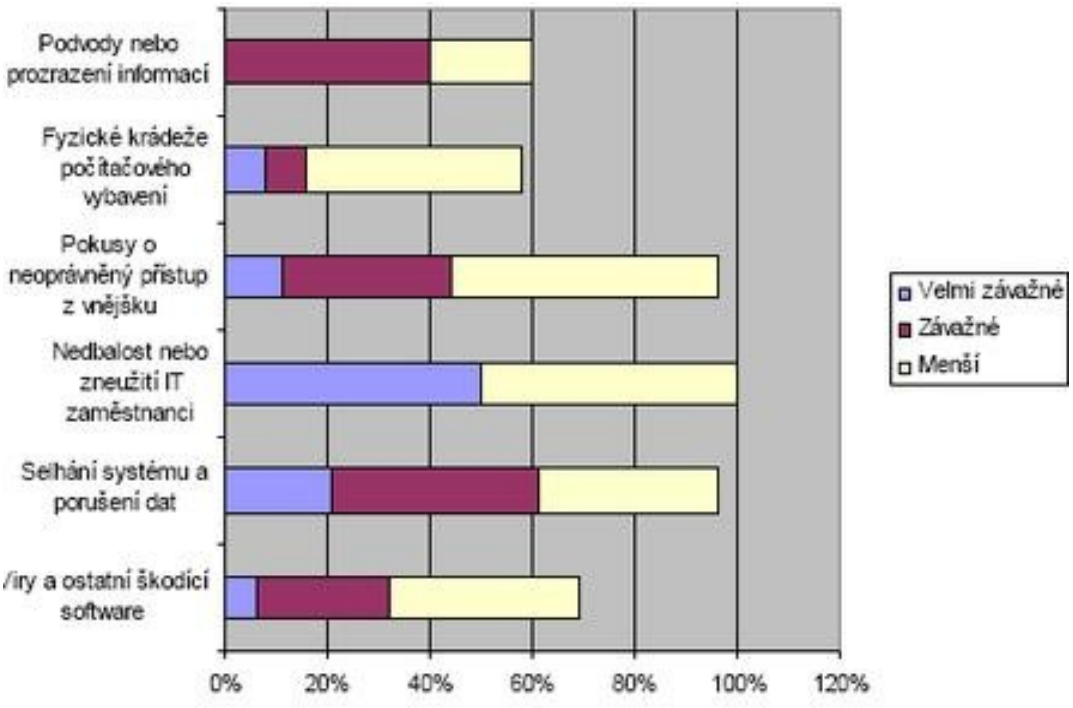
Další graf na obrázku 15 ilustruje procento bezpečnostních incidentů velkých firem k celku. I zde je vidět, že velké firmy mají takřka stejné procento útoků na své systémy jako ostatní společnosti. Hlavní rozdíl je v krádeži majetku. Ten je pochopitelně vyšší u majetných velkých firem. Podceňování bezpečnostních prvků vede k podstatně vyšším údajům u selhání systému, porušení dat, napadení viry a škodlivým softwarem.



Obrázek 15: Porovnání velkých a ostatních firem z hlediska počtu útoků, Zdroj: [8]

V této sekci poslední obrázek 16 zobrazuje stupeň závažnosti, který způsobily výše uvedené bezpečnostní incidenty. Velmi závažné jsou hlavně incidenty spojené s nedbalostí nebo zneužitím IT zaměstnanci. Vychází to z výše uváděné nízké povědomosti zaměstnanců. Závažné jsou také podvody, prozrazení informací, selhání systému a viry s jiným škodlivým softwarem. Je patrné, že každá sekce má i nemalý počet záznamů o menší závažnosti. Právě na nich by se měl zapojit model AAR nebo holistický model, aby se v těchto případech bezpečnostní politika upravila a nedocházelo dále k závažnějším problémům.

Patrné je také, že firmy většinou investují do fyzické ochrany. Krádeže majetku se tak týkají méně podstatných zařízení. Je také vidět značná snaha o neoprávněný přístup z vnějšího prostředí. Velmi často to ovšem bývají začínající hackeři, kteří pouze touží po adrenalinové zábavě a nepředstavují velké riziko pro firmu. Velmi závažných útoků je „pouhých“ 8%.



Obrázek 16: Přehled výše závažnosti pro bezpečnostní incidenty, Zdroj: [8]

Závěry této části dobře znázorňuje níže uvedený příklad 2[18]. Jedná se o skutečnou situaci, která vznikla v malé (11 zaměstnanců) středočeské společnosti. Management firmy zcela ignoroval bezpečnost datových toků a výdaje v tomto směru považoval za zbytečné ztráty.

Příklad 2

Firma vlastnila vysokorychlostní připojení, HW firewall a antivirový program ve free verzi. Právní vědomí bylo na nízké úrovni. To bylo patrné z faktů, že v polovině případů nebyly k dispozici oficiální doklady o legálnosti softwaru, zaměstnanci si na server i osobní počítače volně stahovali a instalovali libovolné programy. Přístup k firemním datům nebyl (kromě účetních dat) omezen. Dohled nad správou firemního HW ani SW neexistoval.

Tato situace zdánlivě nepůsobila žádné potíže v rozvoji firmy a v pokračování úspěšně se rozvíjející obchodní činnosti. Během období osmi měsíců došlo důsledkem laxnosti managementu společnosti k následujícímu porušením bezpečnosti:

Rozbalením zavirované přílohy došlo k napadení firemní sítě. Její obnova si důsledkem omezených možností jediného pracovníka IT vyžádala téměř 10 dní. Některá důležitá obchodní data nebylo možné obnovit vůbec.

[18] TUESDAY BUSINESS NETWORK; BROADBAND MONEY. *Bezpečnost firemní komunikace* [online]. 2006 [cit. 2009-04-21]. Dostupný z WWW: <http://redakce.abchistory.cz/download-ke-stazeni/2006-broadband-studie-03-komunikace.pdf>.

Zaměstnanec, který se s vedením společnosti nerozešel v dobrém, předal podle různých indicií část firemní databáze klientů konkurenční firmě, na základě čehož došlo k určitému odlivu zákazníků ke konkurenci.

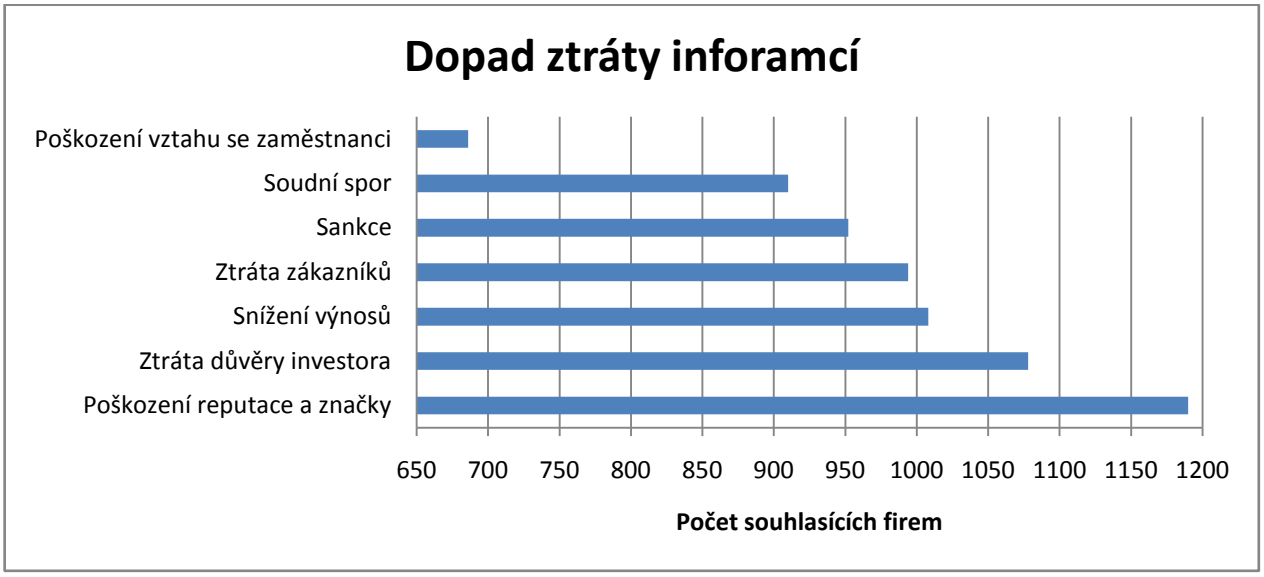
Původně předpokládané základní investice pro vznik nezbytné bezpečnostní politiky, standardizovaní firemní komunikace a zajištění bezpečnosti firemních dat by přitom v době rozkvětu firmy nemusely přesáhnout 10–30 % měsíčního zisku.

5.4.Dopady spojené se ztrátou informací

Kde se nejvíce projevují dopady při ztrátě informací? Odpověď na tuto otázku částečně přináší průzkum provedený v roce 2008 společností Ernst & Young's[19]. 1400 odborníků mohlo pro větší objektivnost a přehled označit více variant. Na výběr bylo ze sedmi možností.

Zde by se mělo ukázat, že výsledkem není jednorázová finanční ztráta. Dopady mohou být a často jsou dlouhodobějšího rázu. Je třeba mít stále na paměti nehmotný majetek firmy jako je například dobrá pověst.

Na obrázku 17 je přehled četností pro jednotlivé možnosti.



Obrázek 17: Místa dopadu při ztrátě informací

Na první pohled je patrné, že dopadů je více. Nejčastěji se jedná o poškození renomé společnosti, tento bod uvedlo 85% dotázaných. Druhá nejčastější možnost byla ztráta důvěry investora (77%), což rovněž znamená dlouhodobé finanční ztráty. Na třetím a čtvrtém místě jsou snížení výnosů (72%) a ztráta zákazníka (71%). Další je finanční postih buď v podobě sankcí 68%, nebo soudního sporu (65%). Poškození vztahu se zaměstnanci již není tak velký (49%) v porovnání s ostatními, ale přesto není zanedbatelný.

[19] ERNST & YOUNG'S. *GISS_2008_EN* [online]. 2009 [cit. 2009-03-30]. Dostupný z WWW: <https://www.aotalliance.org/docs/GISS_2008_EN.pdf>.

6. Závěr

Práce se zabývala významem informací převážně z ekonomického pohledu, tj. jako nedílné složky prosperující firmy. Byly ukázány důvody pro ochranu informací vlastní společnosti a důležitost včasného získání relevantních informací o konkurenci a konkurenčním prostředí.

Za tímto účelem byly rovněž představeny tři moderní ekonomické nástroje a některé jejich metody sloužící pro získání informační výhody. Jmenovitě knowledge management, business inteligence a konkurenční zpravodajství. Poslední uvedené bylo v této práci stěžejní. I proto bylo rozvedeno v širším kontextu. Snahou bylo jasně definovat tyto oblasti a jejich možnou vzájemnou provázanost nejen ve smyslu oblasti působení, ale také používaných metod. Obohacením konkurenčního zpravodajství o postupy jako jsou AAR nebo holistický model lze zefektivnit získávání informační výhody.

V poslední části byly vybrány čtyři okruhy tematicky spojené s informační bezpečností. Prvním bylo stanovení rizik společnosti a jeho možné snížení. Zde byly ukázány hlavní překážky při zajišťování dat, byla představena matice rizik (Klause Winterlinga) a zároveň byly demonstrovány časté chyby při zabezpečování informací. Dále: kdo zodpovídá za bezpečnost dat. V této části se hlavní myšlenka týkala oblasti, pod kterou by měla spadat správa citlivých dat společnosti. Rozdílné přístupy k bezpečnosti informací velkých a malých firem byl třetím okruhem. Poměrně jasně je demonstrován rozdílný přístup k problematice u velkých a malých společností včetně důsledků, které z toho plynou. Posledním okruhem byla otázka - jaké jsou dopady bezpečnostního incidentu. Snahou bylo ukázat, že okamžitá finanční ztráta není jediným problémem, ale dopady jsou mnohem širší. Některé ze závěrů byly poté ilustrovány na skutečných událostech. Při práci byla mimo jiné použita metoda komparace, kdy byly srovnávány jednotlivé zjištěné údaje.

Bezpečnost informací je oblastí, která bude stále aktuálnější. Stejně je tomu u nutnosti získání informační výhody. Práce poskytuje náhled do problematiky a dává odpovědi na některé z mnoha otázek. Na základě daného zadání a dosažených výsledků lze tvrdit, že cíl práce byl splněn.

7. Použitá literatura

[1] BRABEC, František, et al. *Bezpečnost pro firmu, úřad, občana*. [s.l.] : [s.n.], 2001. 400 s.

[2]BRABEC, František, et al. *Soukromé detektivní služby*. [s.l.] : [s.n.], 1995. 63 s.

[3] BRABEC, František. Ochrana bezpečnosti podniku. Praha : Eurounion Praha, 1996. 203 s. ISBN 80-85858-29-0.

[4] BYLOKOVÁ, Kateřina, ČECH, Martin, MASAŘÍKOVÁ, Gabriela. *Competitive-intelligence-portal-ci* [online]. 2009 [cit. 2009-02-22]. Dostupný z WWW: <https://www.inflow.cz/competitive-intelligence-portal-ci>.

[5] COLLISON, Chris, PARCELL, Geoff. *Knowledge management*. [s.l.] : [s.n.], 2005. 236 s.

[6] *Crm-a-knowledge-management* [online]. 2005 [cit. 2009-03-01]. Dostupný z WWW: <http://www.crmportal.cz/redakcni/crm-a-knowledge-management>.

[7] ERNST & YOUNG'S. GISS_2008_EN [online]. 2009 [cit. 2009-03-30]. Dostupný z WWW: <https://www.aotalliance.org/docs/GISS_2008_EN.pdf>.

[8] GOGELA, Robert . Asseco-bezpecnost-dat [online]. 2008 [cit. 2009-03-30]. Dostupný z WWW: <http://www.itbiz.cz/asseco-bezpecnost-dat>.

[9] HAVIT, S.R.O.. *Zákony, vyhlášky, nařízení vlády a jiné právní normy* [online]. 2009 [cit. 2009-03-01]. Dostupný z WWW: <http://business.center.cz/business/pravo/zakony/>.

[10]IT SYSTEMS. Kyberneticka-kriminalita-ve-firmach-z [online]. 2007 [cit. 2009-03-30]. Dostupný z WWW: <http://www.systemonline.cz/zpravy/kyberneticka-kriminalita-ve-firmach-z.htm>.

[11] Kameník, J. a kol. Komerční bezpečnost. Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur. 1.vyd. Praha: ASPI, a.s., 340 s.

[12] KUČEROVÁ. *Teorie informace* [online]. 2006 [cit. 2009-02-22]. Dostupný z WWW: <http://web.sks.cz/users/ku/uis/inform1.htm>.

[13] MITNICK, Kevin, SIMON, William; Umění klamu. Rafal Lazarczyk; Ludek Vašta. 1. vyd. Gliwice : Helion, 2003. 348 s. ISBN 83-7361-210-6.

[14] NOLAN, John. *Confidential*. [s.l.] : [s.n.], 1999. 360 s.

[15] NOVOTNÝ, Ota, POUR, Jan, SLÁNSKÝ, David. *Business Intelligence : Jak využít bohatství ve vašich datech*. [s.l.] : [s.n.], 2005. 255 s.

[16] RODRYČOVÁ, Danuše, STAŠA, Pavel. *Bezpečnost informací jako podmínka prosperity firmy*. [s.l.] : [s.n.], 2000. 143 s.

[17] Security magazín, FAMily media, Praha, 2008, 5-6, ISSN 1210-8723

[18] SUN-C\', PIN, Sun. *Umění války*. [s.l.] : [s.n.], 2005. 296 s.

[19] TUESDAY BUSINESS NETWORK; BROADBAND MONEY. *Bezpečnost firemní komunikace* [online]. 2006 [cit. 2009-04-21]. Dostupný z WWW: <http://redakce.abchistory.cz/download-ke-stazeni/2006-broadband-studie-03-komunikace.pdf>.

[20] WINTERLING, Klaus. Jak se provádí krizový management. [s.l.] : [s.n.], 1992. 39 s.

[21] ZONER SOFTWARE, S.R.O.. *Většina útoků na informační systém má svůj původ uvnitř firem -- Interval.cz* [online]. 2002 [cit. 2009-03-30]. Dostupný z WWW: <http://interval.cz/tiskove-zpravy/vetsina-utoku-na-informacni-system-ma-svuj-puvod-uvnitr-firem/>.