Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky

DISERTAČNÍ PRÁCE

VÝZNAM OCHRANY A BEZPEČNOSTI IS/IT PRO KONKURENCESCHOPNOST PODNIKU

THE POINT OF IS/IT PROTECTION AND SECURITY FOR THE FIRM COMPETITIVENESS

Autor: Ing. Milan Kafka

Obor: 6208V038 Management a ekonomika

Školitel: prof. Ing. Zdeněk Molnár, CSc.

Listopad 2007

PODĚKOVÁNÍ

Rád bych poděkoval svému školiteli prof. Ing. Zdeňku Molnárovi, CSc. zejména za cenné rady, komentáře, konzultace a odborné vedení, které mi poskytoval v průběhu vytváření této disertační práce.

ABSTRAKT

Název práce	Význam ochrany a bezpečnosti IS/IT pro konkurenceschopnost podniku.
Klíčová slova	Bezpečnost IS/IT, konkurenceschopnost, incidenty, rizika

Informace se stávají v období globalizace obchodu s větší mírou spolupráce, dynamičnosti a vzájemné integrace firem velmi ceněnou komoditou se strategickým významem. Uvedené skutečnosti přináší nový pohled a význam přiměřené bezpečnosti informací v IS/IT zejména v souvislostech s jejich elektronizací a elektronickou výměnou. Ochrana a bezpečnost IS/IT tedy pro společnosti nabývá aktuálně stále většího významu a je jedním z klíčových faktorů konkurenceschopnosti a ekonomické úspěšnosti společnosti. Zájem managementu o bezpečnost IS/IT a informací tím vyplývá nejenom z ohrožení prosperity a konkurenceschopnosti ale v případě extrému i vlastní existence podniku.

Předkládaná disertační práce se zamýšlí nad problematikou bezpečnosti IS/IT z několika pohledů:

- Tendence v oblasti bezpečnosti a hrozeb,
- manažerský náhled,
- technologický náhled,
- ekonomický náhled.

Hlavním cílem disertační práce je na základě teoretického a terénního výzkumu a praktických zkušeností identifikovat a analyzovat příčiny současných bezpečnostních incidentů a rizikových faktorů z výše uvedených pohledů a souvislostí.

Vedlejší cíli práce je stanovení přiměřené bezpečnosti IS/IT organizace ve vztahu ke konkurenceschopnosti společnosti a firem.

V disertační práci bylo také využito dlouholetých vlastních praktických zkušeností z realizovaných bezpečnostních projektů doplněných o srovnání celosvětových i personálních průzkumů informační bezpečnosti.

V závěru práce jsou výsledky konfrontovány se stanovenými hypotézami. Výsledky práce všeobecně přispějí k rozvoji problematiky ochrany a bezpečnosti IS/IT z pohledu konkurenceschopnosti společnosti.

ABSTRACT

Title	The point of IS/IT protection and security for the firm competitiveness.
Keywords	Security of IS/IT, Competitiveness, Incidents, Risks.

In the period of business globalization and with higher degree of cooperation, dynamism and mutual integration of firms information become valuable commodity with strategic importance. The given facts present a new view of appropriate security of information IS/IT, especially in the sphere of electronization and electronic exchange.

The protection and security of IS/IT become more and more important for the company and it is one of the key factors of competitiveness and company's business success. The interest of management in IS security and information arises not only from the fact that prosperity and competitiveness might be jeopardized but also the existence of the company itself might be put in jeopardy.

The dissertation thesis deal with security IS/IT in these levels:

- trends in the field of security and threats,
- opinions of the management,
- technological opinion,
- economic opinion.

The main goal of this thesis is to identify and analyze the causes of contemporary security incidents and risk factors from the points of view mentioned above.

The secondary goal of this thesis is to determine appropriate degree of security IS/IT in the company in relation to the competitiveness of the company and firms.

The dissertation thesis is based on long-standing practical experiences of the author resulting from implemented security projects that were supplemented by comparisons of worldwide and personal surveys of information security.

Results are confronted with defined hypotheses at the end of the thesis. The results of the thesis will generally contribute to the development of problems of protection and IS/IT security mainly from the point of view of company’s competitiveness.

OBSAH

SEZNAM OBRÁZKŮ, GRAFŮ A TABULEK

Seznam obrázků:

Seznam grafů:

Seznam tabulek:

SEZNAM ZKRATEK A ZNAČEK

AR	Průměrný příjem firmy za standardních podmínek
ARbezinf	Průměrný příjem firmy s konstantní informační ztrátou
ARsinf	Průměrný příjem firmy s konstantním informačním ziskem
BCM	Označení řízení nepřetržitosti obchodních činností (Business Continuity)
BCP	Označení plánování nepřetržitosti obchodních operací (Business Continuity Plan)
BSI	British Standards Institute
CCTA	Centrální agentura pro počítače a telekomunikace (Central Computer and Telecomunications Agency)
CISA	Certifikace v oblasti auditu, kontroly, řízení a bezpečnosti informačních technologií (Certified Information Systems Auditor)
CISM	Certifikace pro manažery informační bezpečnosti (Certified Information Security Manager)
CRAMM	CCTA Risk Analysis and Management Method
GROUPWARE	poštovní systém
ICT	Informační a komunikační systém
IDS	Detekční informační systém
IPS	Prevenční informační systém
IS	Informační systém
ISACA	Mezinárodní profesní asociace se zaměřením na oblast auditu, řízení, kontroly a bezpečnosti informačních systémů (Information Systems Audit and Control Association)
ISMS	Systém řízení bezpečnosti informací (Information Security Management Systems)
ISO	International Standards Organization
IT	Informační technologie
ITIL	Knihovna infrastruktury informačních technologií (IT Infrastructure Library)
K	Výrobní faktor - kapitál
kinf	Koeficient informací firmy
L	Výrobní faktor - práce
MR	Mezní příjem firmy za standardních podmínek
MRbezinf	Mezní příjem firmy s konstantní informační ztrátou
MRsinf	Mezní příjem firmy s konstantním informačním ziskem
P	Cena finální produkce
PATCH	Záplata, odstranění chyby nebo zranitelnosti SW
PDCA	“Plánuj-Dělej-Kontroluj-Jednej“ (Plan-Do-Check-Act)
Q	Množství výrobků a služeb, výstup firmy

R	Cena kapitálu
SOX	SARBANES-OXLEY
SLA	Úroveň garance služby (Service Level Agreement)
T	Čas
TCRR	Total Cost of Remove Risk
TEED	Total Economic Estimate of Damage
TR	Celkový příjem firmy za standardních podmínek
TRbezinf	Celkový příjem firmy s konstantní informační ztrátou
TRsinf	Celkový příjem firmy s konstantním informačním ziskem
W	Cena práce
$f(k\,\mathrm{inf})$	Funkce vlivu informací
Π	Zisk firmy

1 ÚVOD

Informace se stávají v období globalizace obchodu s větší mírou spolupráce, dynamičnosti a vzájemné integrace firem velmi ceněnou komoditou se strategickým významem. Uvedené skutečnosti přináší nový pohled a význam přiměřené bezpečnosti informací v IS/IT zejména v souvislostech s jejich elektronizací a elektronickou výměnou. Ochrana a bezpečnost IS/IT tedy pro společnosti nabývá aktuálně stále většího významu a je jedním z klíčových faktorů konkurenceschopnosti a ekonomické úspěšnosti společnosti. Zájem managementu o bezpečnost IS/IT a informací tím vyplývá nejenom z ohrožení prosperity a konkurenceschopnosti ale v případě extrému i vlastní existence podniku.

I přes obsáhlé množství současné odborné literatury bezpečnostní problematiky IS/IT zabývající se otázkami norem, standardy, metodologií, procesy bezpečnosti, terminologii, dílčími bezpečnostními řešeními, profilem a postavením bezpečnostního manažera IS/IT a řadou doložených analyzovaných případových studií bezpečnostních incidentů v IS/IT stále dochází k dalším a dalším bezpečnostním případům ohrožující činnost společností a firem.

K oblasti bezpečnostních incidentů IS/IT a vlivu bezpečnosti IS/IT na konkurenceschopnost se snaží přispět i tato disertační práce. Hlavním cílem disertační práce je identifikace a analýza příčin současných bezpečnostních incidentů v IS/IT a rizikových faktorů IS/IT a jejich vliv na konkurenceschopnost podniků.

Primární hypotézy disertační práce byly formulovány prostřednictvím následujících tezí:

- Hypotéza číslo 1:

  „Podstatným prvkem eliminace příčin současných bezpečnostních incidentů je lidský faktor.“

- Hypotéza číslo 2:

  „Přiměřená bezpečnost IS/IT závisí:

  a. Na lidském faktoru,
  b. na konkrétní aplikaci norem a metodologií v organizaci (Management procesní bezpečnosti),
  c. na aplikaci bezpečnostních technologických prvků (Management technologické bezpečnosti).“

§ Hypotéza číslo 3

„Bezpečnost IS/IT zvyšuje konkurenceschopnost společnosti.“

Přínos disertační práce pro teorii spatřuji v přehledu a analýze nových trendů v oblasti bezpečnosti IS/IT se zaměřením na management, ekonomii a technologickou rovinu.

Přínos práce pro vědu vidím v hledání nových možností jak reagovat na bezpečnostní rizika IS/IT a chránit konkurenceschopnost společností.

2 SOUČASNÝ STAV ŘEŠENÉ PROBLEMATIKY

Aktuální situaci problematiky podnikové bezpečnosti IS/IT můžeme charakterizovat jako velmi dynamickou oblast poznání s řadou vývojových tendencí a trendů. Na stav poznání řešené problematiky budu nahlížet zejména prostřednictvím následujících zdrojů:

- Literární prameny,
- praktické zkušenosti.

2.1 Literární prameny

K problematice bezpečnosti IS/IT existuje řada odborné literatury, dokumentace, přednášek, sborníků, metodologií a norem. Podstatným a klíčovým vstupním prvkem uvedené problematiky jsou zejména standardy, normy, metodologie a procesní analýza. Mezinárodní normy pro systémy managementu bezpečnosti informací patří mezi základní soubory norem technické normalizace. Bezpečnostní normy jsou podstatným prvkem informační bezpečnosti, který sjednocuje formu bezpečnostních opatření a přístupů k informační bezpečnosti.

Standardy v oblasti bezpečnosti IS/IT se zabývají nastavením, řízením a posuzováním bezpečnosti informací. Podle zaměření je můžeme dělit do následujících skupin:

- Osvědčené bezpečnostní praktiky,
- Standardy v oblasti řízení bezpečnosti IS,
- Standardy pro posuzování bezpečnostních vlastností jednotlivých komponent IS/IT.

Zásadní pro manažery IS/IT a bezpečnostní manažery jsou první dvě kategorie. Poslední kategorie je určena pro organizace vyvíjející komponenty pro ICT, nebo architekty speciálně zaměřených IS/IT. K osvědčeným bezpečnostním praktikám aplikovaných pro české prostředí patří standard ISO/IEC 17799:2005 (1). Ke standardům pro oblast řízení bezpečnosti informací pro české prostředí přináleží například standardy ISO/IEC 27001:2005 (2), ČSN ISO/IEC TR 1335-1 (3), ČSN ISO/IEC TR 1335-2 (4), ČSN ISO/IEC TR 1335-3 (5), ČSN ISO/IEC TR 1335-4 (6).

2.1.1 **Osvědčené bezpečnostní praktiky IS/IT**

V disertační práci v rámci literární rešerše jsem zvolil osvědčené bezpečnostní praktiky podle standardu ISO/IEC 17799:2005 (1). ISO přepracovává standard 17799 a zavádí nové řady norem v oblasti bezpečnosti informací pod označením ISO/IEC 27000. Cílem této řady norem označených ISO/IEC 27000 je sjednotit požadavky, návody a doporučení na systémy řízení informační bezpečnosti, které se vyskytují v různých normách. Nový standard ISO/IEC 17799:2005 (1) by měl mít označení v připravované řadě norem ISO 2700x označení ISO/IEC 27002:2005. K výběru osvědčených bezpečnostních praktik IS/IT ISO/IEC 17799:2005 mne vedli okolnosti rozšířenosti na území české republiky a dále, že vychází z ověřeného britského standardu BS 7799-2. Bohužel, vzhledem k rozsahu disertační práce není možné a reálné detailněji rozebrat další bezpečnostní praktiky.

ISO/IEC 17799:2005 je sbírka nejlepších bezpečnostních praktik a může být využita jako kontrolní seznam všeho dobrého, co je nutno pro bezpečnost informací v organizaci udělat.

Bezpečnostní manažeři IS/IT dlouho čekali na někoho, kdo vytvoří prověřitelný soubor globálně uznávaných standardů IS/IT. Standard ISO 17799 se po svém publikování Mezinárodní organizací pro standardizaci (ISO) v prosinci 2000 postupně vyvinul v uznávaný celosvětový standard informační bezpečnosti. ISO 17799 je definován jako „komplexní soubor opatření sestávající z nejlepších praktik k zajištění informační bezpečnosti“.

British Standards Institute (BSI) vydala v roce 1995 první bezpečnostní standard – BS 7799, který byl napsán s úmyslem najít řešení bezpečnostních otázek souvisejících s elektronickým obchodováním. Nicméně standard BS 7799 byl vnímán jako těžkopádný a navíc bezpečnostní otázky v té době nevzbuzovaly velký zájem. V roce 1999 vydal BSI druhou verzi svého standardu BS 7799. Právě v této době zareagovala ISO a začala pracovat na revizi standardu BS 7799.

International Standards Organization (ISO) v prosinci 2000 přijala první část standardu BS 7799 a publikovala jej jako vlastní standard pod názvem ISO/IEC 17799:2000. Přibližně ve stejnou dobu byly přijaty formální prostředky akreditace a certifikace podle tohoto standardu. V roce 2005 bylo přijato druhé vydání ISO/IEC 17799:2005 (1).

ISO/IEC 17799:2005 (1) je sbírkou doporučení pro nejlepší bezpečnostní praktiky a tato doporučení může aplikovat každá organizace bez ohledu na svoji velikost nebo obor, v němž působí. Standard byl záměrně napsán jako flexibilní a ty, kdo se jím řídí, nikdy nenavádí k tomu, aby dali přednost konkrétnímu bez-

pečnostnímu řešení před jiným. Doporučení obsažená ve standardu ISO/IEC 17799:2005 (1) zůstávají technologicky neutrální a nijak nepomáhají při hodnocení ani chápání existujících bezpečnostních opatření. Nicméně existuje řada technologických i procesních bezpečnostních specialistů IS/IT, kteří hovoří o tom, že ISO/IEC 17799:2005 (1) je příliš volně strukturovaný a bez reálného významu. Subjektivně se domnívám, že určitá neurčitost standardu ISO/IEC 17799:2005 (1) je však záměrná, protože jeden standard může jen obtížně pokrývat širokou řadu IS/IT prostředí a rozvíjet se spolu s dynamicky se měnícími technologiemi IS/IT.

Norma ISO/IEC 17799:2005 (1) obsahuje celkem 11 základních oddílů bezpečnosti IS/IT, které jsou dále rozděleny do 39 cílů (kontrolních) opatření pro ochranu IS/IT aktiv proti porušení jejich důvěrnosti, dostupnosti a integrity. Obecně opatření zahrnují funkční požadavky pro architekturu bezpečnosti IS/IT. Cíle opatření se mohou stát stavebními prvky pro stanovení bezpečnostní politiky. Nicméně ne vše lze aplikovat v každé organizaci. Každá organizace má svá specifika a uvedená opatření může přeformulovat podle aktuálních potřeb organizace. Příslušná opatření jsou vybírána na základě hodnocení rizik a jejich implementace je závislá na konkrétní situaci.

Forma popisu opatření je uvedena v následující tabulce.

Tab. 2.1.1 Forma popisu opatření
[(1)*]*

Opatření
Formulace konkrétního opatření vedoucího k naplnění cíle
Doporučení k realizaci
Doporučení na implementaci konkrétního opatření
Opatření
Doplňující informace. Např. odkazy na normy

Základní členění ISO/IEC 17799:2005 (1):

- Bezpečnostní politika,
- organizace bezpečnosti,
- klasifikace a řízení aktiv,
- bezpečnost lidských zdrojů,
- fyzická bezpečnost a bezpečnost prostředí,

- řízení komunikací a řízení provozu,
- řízení přístupu,
- vývoj, údržba a rozšíření informačního systému,
- zvládání bezpečnostních incidentů,
- řízení kontinuity činností organizace,
- soulad s požadavky.

Bezpečnostní politika

Vedení organizace by mělo stanovit jasný směr postupu v oblasti bezpečnosti informací, ukázat její podporu vydáním a aktualizací bezpečnostní politiky informací platné v celé organizaci. (1)

Organizace bezpečnosti

Měl by být vytvořen řídící rámec pro zahájení a řízení implementace bezpečnosti informací v organizaci. Vedení organizace by mělo schválit politiku bezpečnosti informací, přiřadit role v oblasti bezpečnosti informací a koordinovat implementaci bezpečnosti v organizaci. (1)

Bezpečnost informací a zařízení pro zpracování informací by neměla být snížena při zavedení produktů a služeb třetích stran. Přístup externích subjektů k zařízení pro zpracování informací a k informacím by měl být kontrolován. (1)

Klasifikace a řízení aktiv

U všech důležitých informačních aktiv by měla být stanovena odpovědnost a určen jejich vlastník. (1)

Informace by měly být klasifikovány tak, aby byla naznačena jejich potřebnost, důležitost a stupeň ochrany. (1)

Bezpečnost lidských zdrojů

Odpovědnosti za bezpečnost by měly být zohledněny v rámci přijímacího řízení, měly by být zahrnuty v pracovních smlouvách a popisech práce. Všichni zaměstnanci, smluvní a třetí strany, využívající prostředky organizace pro zpracování informací, by měli podepsat dohodu odpovídající jejich rolím a povinnostem. (1)

Měly by být jasně definovány odpovědnosti vedoucích zaměstnanců, aby se zajistilo dodržování bezpečnosti ze strany jednotlivců během celé doby trvání pracovního vztahu. Zaměstnanci, smluvní a třetí strany by měli být školeni v bezpečnostních postupech a ve správném používání prostředků pro zpracování informací, aby byla minimalizována bezpečnostní rizika. Měla by být vytvořena formalizovaná pravidla pro disciplinární řízení v případě narušení bezpečnosti. Měly by být určeny jednoznačné odpovědnosti za řádný průběh ukončení pracovního vztahu zaměstnanců, smluvních a třetích stran, za odevzdání přiděleného vybavení a odejmutí přístupových práv. (1)

Fyzická bezpečnost a bezpečnost prostředí

Prostředky IT, zpracovávající kritické nebo citlivé informace organizace, by měly být umístěny v zabezpečených zónách chráněných definovaným bezpečnostním perimetrem s odpovídajícími bezpečnostními bariérami a vstupními kontrolami. Tyto prostředky by měly být fyzicky chráněny proti neautorizovanému přístupu, poškození a narušení. Jejich ochrana by měla odpovídat zjištěným rizikům. (1)

Zařízení by měla být fyzicky chráněna proti bezpečnostním hrozbám a působení vnějších vlivů. (1)

Řízení komunikací a řízení provozu

Měly by být stanoveny odpovědnosti a postupy pro řízení a správu prostředků zpracovávajících informace. Zahrnuje to vytváření vhodných provozních instrukcí a postupů. (1)

Pro zajištění toho, že služby dodávané třetími stranami jsou v souladu s dohodnutými požadavky, by organizace měla kontrolovat realizaci dohod, monitorovat míru souladu jejich dodržování a v případě potřeby zajistit nápravu.

Pro zajištění odpovídající kapacity a zdrojů a výkonu systému je nutné provést odpovídající přípravu a plánování. (1)

Pro prevenci a detekování škodlivých programů a nepovolených mobilních kódů jsou vyžadována patřičná opatření. (1)

Měly by být vytvořeny rutinní postupy realizující schválenou politiku zálohování a strategii pro vytváření záložních kopií dat a testování jejich včasného obnovení. (1)

Pozornost vyžaduje správa bezpečnosti počítačových sítí, které mohou přesahovat hranice organizace. Pro zabezpečení citlivých dat přenášených veřejnými sítěmi mohou být požadována dodatečná opatření. (1)

Měly by být stanoveny náležité provozní postupy týkající se zabezpečení dokumentů, počítačových médií (např. pásky, disky), vstupních/výstupních dat a systémové dokumentace před neoprávněným prozrazením, modifikací, odstraněním nebo poškozením. (1)

Výměna informací a programů mezi organizacemi by měla být založena na formální politice, prováděna v souladu s platnými dohodami a měla by být ve shodě s platnou legislativou. (1)

Měly by být zváženy bezpečnostní dopady a požadavky na opatření spojené s použitím služeb podporujících elektronický obchod, včetně on-line transakcí. Pozornost by měla být věnována ochraně integrity a dostupnosti elektronicky publikovaných informací na veřejně přístupných systémech. (1)

Systémy by měly být monitorovány a bezpečnostní události zaznamenávány. Pro zajištění včasné identifikace problémů informačních systémů by měl být používán operátorský deník a záznamy předchozích selhání. (1)

Řízení přístupu

Přístup k informacím, prostředkům pro zpracování informací a procesům organizace by měl být řízen na základě provozních a bezpečnostních požadavků.

Měly by existovat formální postupy pro přidělování uživatelských práv k informačním systémům a službám. (1)

Pro účinné zabezpečení je nezbytná spolupráce oprávněných uživatelů. Uživatelé by si měli být vědomi odpovědnosti za dodržování účinných opatření kontroly přístupu, zejména s ohledem na používání hesel, a bezpečnosti jim přidělených prostředků. (1)

Přístup k interním externím sítovým službám by měl být řízen. (1)

Pro omezení přístupu k prostředkům počítače by měly být použity bezpečnostní prostředky na úrovni operačního systému. Tyto prostředky by měly být schopné:

a) Autentizace oprávněných uživatelů v souladu se stanovenou politikou řízení přístupu,

b) zaznamenávat úspěšné a neúspěšné pokusy o autentizaci,

c) zaznamenávat využití systémových privilegií,

d) spouštět varování při porušení systémových bezpečnostních politik,

e) poskytovat vhodné prostředky pro autentizaci,

f) v případě potřeby omezit dobu připojení uživatele.

Pro omezení přístupu k aplikačním systémům by měly být použity bezpečnostní prostředky. Logický přístup k programům a informacím by měl být omezen na oprávněné uživatele. (1) Aplikační systémy by měly:

a) Kontrolovat přístup uživatelů k datům a funkcím aplikačního systému v souladu s definovanou politikou řízení přístupu,

b) poskytovat ochranu před neoprávněným přístupem ke všem nástrojům a systémovým programům, které mohou obejít systémové a aplikační kontrolní mechanizmy,

c) nenarušit bezpečnost jiných systémů, se kterými jsou sdíleny informační zdroje.

Při použití mobilních výpočetních prostředků by mělo být zváženo riziko práce v nechráněném prostředí a měla by být zajištěna vhodná ochrana. (1)

Vývoj, údržba a rozšíření informačního systému

Bezpečnost se musí stát neodlučitelnou součástí informačních systémů. To zahrnuje provozní systémy, infrastrukturu, interní aplikace organizace, zakoupené produkty, služby a uživatelsky vyvinuté aplikace. Návrh a implementace informačního systému na podporu procesů organizace může být z hlediska bezpečnosti kritický. Bezpečnostní požadavky by měly být stanoveny a odsouhlaseny ještě před zahájením vývoje informačního systému. (1)

Pro zajištění bezchybného zpracování by do aplikačních systémů, včetně těch, které jsou vytvořeny uživatelsky, měly být zahrnuty vhodné kontroly. Měly by zahrnovat potvrzení platnosti vstupních dat, interního zpracování a výstupních dat. (1)

Měla by být vytvořena pravidla pro použití kryptografických opatření. K podpoře používání kryptografických technik by měl v organizaci existovat systém jejich správy. (1)

Přístup k systémovým souborům a zdrojovým kódům programů by měl být řízen, projekty IT a podpůrné činnosti by měly být prováděny bezpečným způsobem. Měla by být přijata opatření zabraňující prozrazení citlivých informací v testovacím prostředí. (1)

Vedoucí a správci, kteří jsou odpovědní za aplikační systémy, by měli mít také odpovědnost za bezpečnost projektového a podpůrného prostředí. Měli by zajistit, že všechny plánované změny systému budou podrobeny kontrole, aby nenarušily bezpečnost systému nebo provozního prostředí. (1)

Řízení (správa) technických zranitelností by mělo být zavedeno efektivním, systematickým a opakovatelným způsobem, s využitím metrik pro ověření její účinnosti. Toto by mělo zahrnovat všechny operační systémy a použité programové vybavení. (1)

Zvládání bezpečnostních incidentů

Měly by být ustaveny formální postupy pro hlášení bezpečnostních událostí a pro zvyšování stupně jejich důležitosti. Všichni zaměstnanci, smluvní strany a uživatelé třetích stran by měli znát postupy hlášení různých typů událostí a slabin, které mohou mít dopad na bezpečnost aktiv organizace. Zjištěné bezpečnostní události a slabiny by měli zaměstnanci ihned hlásit na určené místo. (1)

Pro účinné zvládání bezpečnostních útoků a slabin by měly být stanoveny odpovědnosti a zavedeny formalizované postupy umožňující okamžitou reakci. Měl by být nastaven proces neustálého zlepšování reakce, monitorování, vyhodnocování a celkového zvládání bezpečnostních incidentů. (1)

Řízení kontinuity činností organizace

Pro minimalizaci následků a zotavení se ze ztráty informačních aktiv (které může být např. výsledkem přírodních pohrom, nehod, chyb zařízení a úmyslného jednání) na přijatelnou úroveň, za pomoci preventivních a zotavovacích opatření, by měl být zaveden proces řízení kontinuity činností organizace. Tento proces by měl identifikovat kritické činnosti organizace a začlenit požadavky řízení bezpečnosti informací s ohledem na požadavky provozní, personální, materiální, dopravní a požadavků na zařízení. (1)

Soulad s požadavky

Návrh, provoz a používání informačních systémů může být předmětem zákonných, podzákonných nebo smluvních bezpečnostních požadavků. (1)

Jako pozitivní u standardu ISO/IEC 17799:2005 osvědčených praktik hodnotím možnost selekce vhodných opatření. Vhodná opatření jsou vybírána na základě hodnocení rizik a jejich implementace je závislá na konkrétní situaci. Uvedený přístup zajišťuje, že norma je široce aplikovatelná a je při implementaci velmi flexibilní. Nicméně toto přináší obtíže při certifikaci, zda aktuální bezpečnostní opatření jsou v souladu s normou.

2.1.2 **Standardy v oblasti řízení bezpečnosti IS**

Systém řízení bezpečnosti informací (ISMS) je dokumentovaný systém prokazující, že popsaná informační aktiva jsou chráněna, rizika bezpečnosti informací jsou řízena, jsou zavedena opatření s požadovanou úrovní záruk a ta jsou kontrolována. ISMS může být zaveden pro IS/IT nebo může zahrnovat celou organizaci. (2)

V rámci literární rešerše jsem zvolil ISMS ISO/IEC 27001:2005. (2) K výběru ISMS ISO/IEC 27001:2005 mne vedli okolnosti působnosti na území české republiky a dále, že vychází z ověřeného britského standardu.

Mezinárodní norma ISO/IEC 27001:2005 byla připravena proto, aby poskytla podporu pro ustavení, zavedení, provozování, monitorování, udržování a zlepšování systému řízení bezpečnosti informací. Přijetí ISMS by mělo být strategickým rozhodnutím organizace. Návrh a zavedení ISMS v organizaci je podmíněno potřebami a cíli činností organizace a z toho vyplývajících požadavků na bezpečnost, dále pak používanými procesy a velikostí a strukturou organizace. Všechny tyto a jejich podpůrné systémy podléhají změnám v čase. (2)

Při použití procesního přístupu ISO/IEC 27001:2005 je kladen důraz na:

a) Pochopení požadavků na bezpečnost informací a potřebu stanovení politiky a cílů bezpečnosti informací,

b) zavedení a provádění kontrol v kontextu s řízením celkových rizik činností organizace,

c) monitorování a přezkoumání funkčnosti a efektivnosti ISMS,

d) neustálé zlepšování založené na objektivním měření.

Model ISMS ISO/IEC 27001:2005 můžeme označit jako “Plánuj-Dělej-Kontroluj-Jednej (Plan-Do-Check-Act nebo PDCA).

Základní procesní části modelu ISMS ISO/IEC 27001:2005:

a) Plánuj (ustavení ISMS)

   - Ustavení politiky ISMS, cílů, procesů a postupů souvisejících s řízením rizik a zlepšováním bezpečnosti informací tak, aby poskytovaly výsledky v souladu s celkovou politikou a cíli organizace.

b) Dělej (zavádění a provozování ISMS)

- § Zavedení a využívání politiky ISMS, opatření, procesů a postupů.

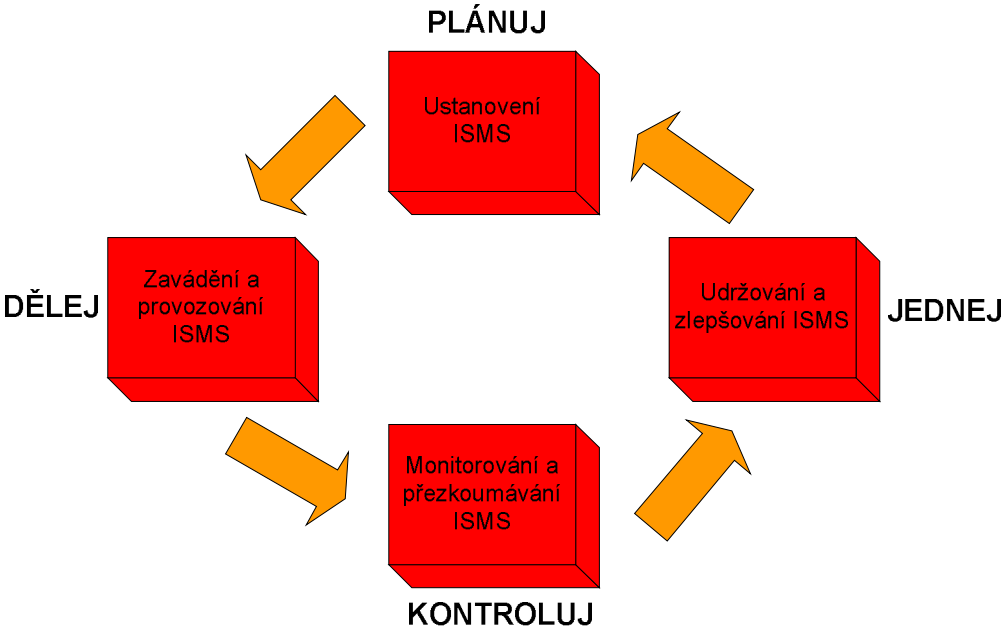
c) Kontroluj (monitorování a přezkoumání ISMS)

- § Posouzení, kde je to možné i měření výkonu procesu (respektive jeho funkčnosti a efektivnosti) vůči politice ISMS, cílům a praktickým zkušenostem a hlášení výsledků vedení organizace k přezkoumání.

d) Jednej (udržování a zlepšování ISMS)

- § Provedení opatření k nápravě a preventivních opatření, založených na výsledcích interního auditu ISMS a přezkoumání systému řízení ze strany vedení organizace tak, aby bylo dosaženo neustálého zlepšování ISMS.

Obr 2.1.2 znázorňuje, jak ISMS přijímá požadavky bezpečnosti informací a očekávání zainteresovaných stran jako vstup, a jak pomocí nezbytných činností a procesů vytváří výstupy bezpečnosti informací, které splňují tyto požadavky a očekávání.



Obr. 2.1.2 Model PDCA
[(2)]

ISMS ISO/IEC 27001:2005 dává procesní návod a vede k řízení informační bezpečnosti IS.

2.1.3 **Další standardy a normy**

Mimo standardy a normy uvedené v předchozí kapitole, existuje řada dalších norem, standardů, metod a metodologií. V rámci literárních pramenů disertační práce jsem zvolil pro přiblížení reprezentativní vzorek dalších hlavních norem a standardů používaných ve firmách v České republice.

Seznam vybraných standardů a norem, doporučení zasahující do oblasti bezpečnosti IS/IT:

- Řada ČSN ISO/IEC TR 1335-1 (3), ČSN ISO/IEC TR 1335-2 (4), ČSN ISO/IEC TR 1335-3 (5), ČSN ISO/IEC TR 1335-4 (6),
- ITIL (7) (8),
- řada ISO/IEC 20000-1:2005, ISO/IEC 20000-2:2005,
- COBIT,
- CRAMM,
- SARBANES-OXLEY.

Normy ČSN ISO/IEC TR 1335-1-4

Účelem norem ČSN ISO/IEC TR 1335-1-4 je poskytnout směrnice pro řídící aspekty bezpečnosti IT.

Hlavní cíle této normy jsou:

- Definovat a popsat pojetí spojená s řízením bezpečnosti IT,
- identifikovat vztahy mezi řízením bezpečnosti IT a mezi řízením IT všeobecně,
- prezentovat několik modelů, které mohou být použity k vysvětlení bezpečnosti IT,
- poskytnout všeobecnou směrnici o řízení bezpečnosti IT.

ISO/IEC TR 13335 je organizována do více částí. Hlavní části:

- ČSN ISO/IEC TR 1335-1 (Část 1: Pojetí a modely bezpečnosti IT) (3),

- ČSN ISO/IEC TR 1335-2 (Část 2: Řízení a plánování bezpečnosti IT) (4),
- ČSN ISO/IEC TR 1335-3(Část 3: Techniky pro řízení bezpečnosti IT) (5),
- ČSN ISO/IEC TR 1335-4 (Část 4: Výběr ochranných opatření) (6).

Část 1 poskytuje přehled základních pojetí a modelů, použitých k popisu řízení bezpečnosti IT. Tento materiál je vhodný pro manažery odpovědné za bezpečnost IT a pro ty, kdo jsou zodpovědní za celkový bezpečnostní program organizace. Část 2 popisuje řídící a plánovací aspekty. Tyto aspekty mají význam pro manažery s odpovědnostmi souvisejícími se systémy IT organizace. Část 3 popisuje bezpečnostní techniky vhodné pro použití pracovníky, kteří jsou zapojeni do manažerských činností v průběhu životního cyklu projektu, jako je plánování, návrh, implementace, testování, získání nebo provozování. Část 4 poskytuje směrnice pro výběr ochranných opatření a jak muže být tento výběr podporován použitím základních modelů a kontrol. (3) (4) (5) (6)

ITIL (IT Infrastructure Library)

ITIL představuje rámec nejlepších praktických zkušeností („best practices“) pro poskytování IT služeb. ITIL je mezinárodně uznávaný standard pro řízení IT služeb, který začal vznikat ve Velké Británii v 80. letech minulého století. ITIL se zaměřuje u jednotlivých procesů na klíčové principy, hlavní aktivity, výkonnostní kritéria a kvalitativní indikátory.

Knihovna ITIL je rozdělena do několika částí, zaměřených na specifickou oblast řízení IT služeb, které odpovídají klíčovým procesům v IT a vzájemně se prolínají.

Seznam částí ITIL v2:

- Obchodní pohled (Business Perspectives);
- Správa aplikací IT (Application Management);
- Dodávka IT služeb (IT Services Delivery);
- Podpora IT služeb (IT Services Support);
- Správa IT infrastruktury (IT Infrastructure Management);
- Správa bezpečnosti (Security Management);

- Řízení IT projektů IT (Project Management).

Propojení mezi ITIL a bezpečností informací je logické. Jestliže předmětem ITIL je oblast IT, pak nelze opomenout ani bezpečnost IT. Z tohoto důvodu ITIL řeší také oblast bezpečnosti informací. (7)

ISO/IEC 20000-1-2:2005

Norma ISO/IEC 20000 je mezinárodním standardem, v rámci kterého jsou shrnuty základní postupy ITIL do standardizovaných kritérií. Norma ISO/IEC 20000 existuje v několika částech:

- ISO/IEC 20000-1:2005 (Information technology – Service management – Part 1: Specification)

- ISO/IEC 20000-2:2005 (Information technology – Service management – Part 2: Code of practice)

Jak vyplývá z názvu, první část je určena pro posuzování a případně certifikaci kvality IT služby, druhá část slouží jako návod pro zavedení funkčního systému. Součásti této normy je také Management bezpečnosti informací.

COBIT

COBIT (Control Objectives for Information and related Technology) je metodika sloužící k systematickému řízení ITC podporující dlouhodobý rozvoj organizace, dosažení obchodních a strategických cílu organizace při minimalizaci rizik a optimalizaci nákladu. Využívá soubor všeobecně uznávaných praktik řízení ICT. Tuto metodiku lze použít jako alternativu nebo doplnění ITIL, je však více orientovaná na obchodní procesy.

CRAMM

Další ze standardů ISMS je metodika CRAMM (CCTA Risk Analysis and Management Method). CRAMM je metodika pro zavádění a podporu systému řízení bezpečnosti informací pro provádění analýzy rizik informačních systémů a sítí, k návrhu bezpečnostních protiopatření, určování havarijních požadavků na informační systém a k návrhům na řešení havarijních situací.

SARBANES-OXLEY (SOX)

Zákon SOX je synonymem boje proti zneužívání moci manažery k vlastnímu obohacení. Tento zákon ukládá všem společnostem, jejichž akcie jsou veřejně obchodovány na americkém akciovém trhu, povinnost zavést a udržovat rámec interních kontrol a procedur pro zajištění transparentnosti finančního výkaznic-

tví. Zároveň klade zvýšené požadavky na zodpovědnost managementu za jakákoliv zkreslení zveřejňovaných výsledků, za něž ukládá mnohem tvrdší postihy.

V praxi to znamená zavedení nových úrovní kontrol a schvalování, aby bylo zaručeno, že finanční výkaznictví transparentně uplatňuje principy plného zveřejňování (full disclosure) a podnikové řízení (corporate governance). K zákonu vyšla celá řada opatření a doporučení vydaných americkou Securities and Exchange Comision (SEC) a dalšími organizacemi upravující takové věci, jako jsou formuláře pro měsíční, čtvrtletní a roční reporty, uzávěrky, doporučení, jak provádět audit a podobně. (9)

Mnoho firem tak v současnosti stojí před problémem, jak se přizpůsobit Sarbanes-Oxley. V této souvislosti se hovoří o zvýšené zodpovědnosti generálního a finančního ředitele za kontrolu systému vykazování finančních výsledků a o povinnosti ustanovit výbor pro audit. Méně často se však hovoří o dopadu tohoto zákona na IT, procesy a infrastrukturu organizací. Bereme-li v potaz skutečnost, že v dnešním světě prakticky neexistují podnikové procesy, které by nebyly postavené na příslušné IT infrastruktuře, pak je zřejmé, že zajištění kontrol ve finančních tocích se neobejde bez sladění s technologickým zázemím společnosti. (9)

Zajištění shody se SOX proto vyžaduje mimo jiné ověření, případně zavedení kontrol v oblasti IT. Auditoři mají omezené zkušenosti s interním fungováním IT v organizaci. Naopak IT manažeři většinou neznají konkrétní potřeby nutné k zajištění souladu s legislativou. Vzniká tak nová situace, v níž auditoři a IT management musí začít spolupracovat. Obě strany přitom vstupují do oblastí, které jim nejsou z podstaty jejich práce příliš známé. (9)

IT manažeři, zvláště ti, co působí na rozhodovací úrovni, by se měli dobře vyznat v provádění kontrolního a schvalovacího procesu. Společně s ostatními vedoucími pracovníky by se měli podílet na analyzování aktiv firmy a potenciálních rizik, které mohou mít významný finanční dopad. Tato analýza pak slouží jako východisko pro definování plánu, který by postupně promítl podmínky SOX do změn v IT. (9)

2.1.4 **Ostatní literární zdroje**

Ostatní literární prameny mimo hlavní normy, standardy a metodologii můžeme rozdělit do několika hlavních částí a jejich vzájemných kombinací:

- Procesní management bezpečnosti IS/IT,
- technologický management a technologické prvky bezpečnosti IS/IT,

- oblast hrozeb a zranitelností IS/IT

- Ostatní.

Procesní management bezpečnosti IS/IT a význam bezpečnosti IS/IT

Literární zdroje procesního managementu bezpečnosti IS/IT se zabývají především problematikou procesního řízení bezpečnosti IS/IT a dávají srozumitelnější návod při porovnání s normami pro management IS/IT jakým způsobem procesně vybudovat řízení bezpečnosti IS/IT. Uvedené zdroje se zabývají zjednodušeným popisem postupu plánování, implementací a průběžným hodnocením účinnosti a výkonnosti bezpečnostní politiky IS/IT. (10) (11) (12) (13) (14) (15) (16) (17) (18) (19) (20) (21)

Několik vybraných doporučení z oblasti procesní bezpečnosti IS/IT:

- Bezpečnost je proces, který nelze koupit jako hotový produkt v krabici. Musí se vytvořit, instalovat a hlavně udržovat. (11)

- Za bezpečnost musí někdo osobně zodpovídat a stejná osoba musí mít pravomoc bezpečnost prosadit. Bezpečnost není možné postavit na dobrovolnosti. (11)

- Komplexní řešení bezpečnosti IS/IT ano, postupujte od bezpečnostní studie přes politiku až k projektu. Bezpečnostní projekt ne, pokud nevíte, jak zapadá do koncepce bezpečnosti. (11)

- Bezpečnost informací je víc než bezpečnost IS. (11)

K významu bezpečnosti IS/IT: „Vzhledem k zostřující se konkurenci v naší informační ekonomice se data o zákaznících stávají stále cennějším aktivem.“ (16)

Technologický management a technologické prvky bezpečnosti IS/IT

Literární zdroje této kategorie se zabývají především problematikou technologického managementu bezpečnosti IS/IT, provozní bezpečnosti IS/IT a dílčích prvků technologické bezpečnosti IS/IT.

Často u těchto literárních zdrojů se objevují tendence pro nadsazení technologii nebo jejich dílčích částí nad ostatními aspekty managementu bezpečnosti IS/IT.

„Současná vize bezpečnosti je založena na převážně technických řešeních. Využívány jsou velmi sofistikované metody implementace v antivirových pro-

gramech, IDS/IPS systémech, firewallech a dalších aplikacích, které mají za úkol udržet chráněné informace pod pokličkou.“ (17)

Oblast hrozeb a zranitelností IS/IT

Literární zdroje této kategorie se zabývají především problematikou hrozeb a zranitelností bezpečnosti IS/IT, popisem technologických útoků a charakterem útočníků. (18) (19) (26)

„Po letech, která lze nazvat „dobou bezpečnostní nevědomosti“, se zabezpečení sítí stává otázkou dne. Málokdy uplyne týden, aniž by se ve zpravodajství ze světa IT neobjevila zpráva o napadení významného internetového serveru. Přesto jsou napadány stále další a další firmy a organizace, a zpřísněná opatření podnikají až poté, co si protrpěly ostudu v podobě přesměrované úvodní WWW stránky, ztráty z odstavení zahlceného internetového serveru, zcizení dat, zneužití účtů či bankovních transakcí. Tato nepřipravenost nepadá ani tak na vrub nedbalosti administrátorů, ale hlavně toho, že nemají informace o nenápadných bezpečnostních dírách v operačních systémech, aplikacích a síťových zařízeních a neznají důmyslné nástroje a postupy, které hackeři používají.“ (19)

Ostatní

Ostatní zdroje se zabývají náhledem na bezpečnost z různých pohledů: právní, personální, účetní a další. Celkem podstatnějším pohled nabízí právní stránka bezpečnosti IS/IT. (20)

2.2 Praktické zkušenosti

Mimo finanční sféru a strategické průmyslové firmy v ČR byla od počátku let 2000 chápána informační bezpečnost z pohledu managementu společností jako jen pouze okrajová část a více méně ztotožněna pouze s technologickou ochranou nejčastěji – antivirovou ochranou a firewally. S postupem času se situace změnila a mění zejména z pohledu chování managementu a majitelů společností.

2.2.1 **Management bezpečnosti IS/IT z pohledu praxe**

Řada komerčních společností systémově řeší management bezpečnosti IS/IT dle následujících logických kroků:

a) Stanovení cílů bezpečnosti IS/IT

Co přesně bude hlavním cílem a jaká cesta k tomuto cíli povede.

b) Analýza rizik IS/IT

Výsledkem je dokument obsahující popis systému a výsledky analýzy, tedy úroveň hrozeb, zjištěné zranitelnosti, úroveň stávajících ochranných opatření a distribuci výsledných rizik.

c) Bezpečnostní politika a standardy IS/IT

Dokument, který je po přijetí managementem závazný pro celou společnost a který definuje východiska pro všechny další aktivity společnosti v oblasti informační bezpečnosti. Hlavním cílem bezpečnostní politiky je:

- Definovat hlavní cíle při ochraně informací,
- Stanovit způsob jak bezpečnost řešit,
- Určit pravomoci a zodpovědnosti.

Hlavní oblasti a principy informační bezpečnosti definované v bezpečnostní politice IS se dále rozpracovávají do detailní podoby bezpečnostních standardů. Zatímco bezpečnostní politika IS je relativně neměnným dokumentem, u bezpečnostních standardů se předpokládá častější frekvence úprav.

d) Implementace bezpečnosti IS/IT

Implementace bezpečnosti IS představuje více či méně větších nebo menších projektů, které je třeba realizovat, aby se bezpečnostní politika IS spolu s bezpečnostními standardy uvedly do praxe.

e) Monitoring a audit

Provedením analýzy rizik, přijetím bezpečnostní politiky IS/IT, vytvořením bezpečnostních standardů a implementací bezpečnosti do života společnosti proces řešení bezpečnosti nekončí, ale dostává se do kvalitativně nového stádia. Ve chvíli, kdy jsou hlavní problémy vyřešeny a prostředí, alespoň do určité míry, připraveno, nastává čas pro důležité rutinní činnosti. Jde o průběžné sledování (monitoring) a průběžnou kontrolu (audit). Z monitoringu a auditu se může vracet k implementaci bezpečnosti, bezpečnostní politice IS/IT, analýze rizik a dokonce na samotný začátek řešení bezpečnosti IS/IT.

V oblasti praktického řešení bezpečnostní problematiky dochází k prolínání zejména dvou skupin hájících své postavení a hranice.

Jedna skupina vytváří tzv. papírovou bezpečnost (například bezpečnostní politiku a standardy IS/IT), která vychází zejména z norem, metodologií a jejich

aplikací zejména v knižní podobě. Problémem této skupiny profesionálních odborníků je značná nadřazenost a nadsazenost tzv. papírových výstupů nad praktickou realizací a rutinním zavedením řešení bezpečnosti do každodenního života společnosti. Proto je důležité položit si občas otázku, zda ochrana informací je prováděna přiměřeně k aktuálním hrozbám a zda prakticky pokrývá komplexně všechny oblasti nezbytné pro zajištění adekvátní ochrany informací.

Druhá skupina z pohledu praktické bezpečnosti nahlíží na problematiku zejména z tzv. technologické bezpečnosti IS/IT nebo kroku implementace bezpečnosti IS/IT což znamená degradaci řešení na technologickou úroveň. V případě extrémní preference výrazného nadřazení technické a technologické bezpečnosti IS může dojít vzhledem k potlačení ostatních bezpečnostních aspektů nad ostatní faktory (organizační, lidské, normy) k neočekávaným bezpečnostním incidentům. Dalším neduhem je prosazování tzv. dílčích nekoncepčních technologických řešení zejména u výrobců disponujících pouze jednou nebo několika bezpečnostními technologiemi. Obrazně můžeme přirovnat k zabezpečenému domu s extrémně chráněnými dveřmi nicméně za stavu plně otevřených oken.

Další nejčastější chyby v procesu řešení informační bezpečnosti je nízká podpora ze strany nejvyššího vedení. Například management deklaruje svůj zájem o informační bezpečnost, je ochoten provést první, nebo několik prvních kroků, ale přijetím bezpečnostní politiky IS jeho podpora končí. Takováto společnost pak končí s bezpečnostní politikou, která zůstává nenaplněna. Výsledkem pak bývá zklamání lidí zapojených do řešení informační bezpečnosti, celková zmatenost týkající se bezpečnostní politiky a ve svém důsledku celková neúcta zaměstnanců k interním předpisům - interní legislativě.

2.3 Sumarizace aktuálního stavu

Současný aktuální stav můžeme hodnotit z několika hledisek:

- Literární prameny,
- praktické zkušenosti.

Literární prameny

V literárních pramenech můžeme nahlížet zjednodušeně na aktuální stav ze dvou zdrojů:

- Osvědčené bezpečnostní praktiky a standardy v oblasti řízení bezpečnosti IS,
- ostatní literární zdroje.

Osvědčené bezpečnostní praktiky a standardy v oblasti řízení bezpečnosti IS se věnují zejména procesním řízením bezpečnosti IS/IT.

Subjektivně v této oblasti vidím problémy ve dvou základních rovinách:

- Selekce normy, standardu bezpečnosti IS/IT a jeho vlivu na ostatní procesy společnost,
- značné formálnosti.

Domnívám se, že nemá smysl používat jednotlivé metodiky a normy odděleně. Můžeme být svědky řady diskusí ve společnostech: Například: „Dle ISO/IEC 27001:2005 by to mělo být tak a tak …, Ne, ne COBIT říká, že je to jinak …, Ale ne dle ITIL je to správně tak a tak…“ Uvedené diskuse jsou velmi kontraproduktivní. Podstatné je třeba si uvědomit, kam jsou jednotlivé normy a standardy bezpečnosti IS/IT ve společnosti cíleny. Je nutné hledat soulad norem a možnosti vhodných vazeb mezi nimi. Například: „Stanovit rozhraní (hranice působnosti) vedení, řízení IS/IT a řízení bezpečnosti informací, vytvořit procesní vazby tak, aby požadované činnosti byly vždy dokončeny s předpokládaným výsledkem atd.“ Subjektivně toto vidím jako zásadní problémy při aplikaci norem do praxe. Jako vedlejší značnou formálnost a přílišnou variabilitu norem a standardů.

Ostatní literární prameny se zabývají zejména procesním managementem bezpečnosti IS/IT, technologickým managementem a technologickými prvky bezpečnosti IS/IT a dalšími aspekty souvisejícími s bezpečností IS/IT. Některé výstupy z těchto zdrojů příliš zjednodušují situace, jiné příliš varují a odrazují manažery IS/IT k nějakým zásadním řešením.

Praktické zkušenosti

V oblasti praktického řešení bezpečnostní problematiky dochází k prolínání zejména dvou skupin hájících své postavení a hranice.

Jedna skupina vytváří tzv. papírovou bezpečnost, která vychází zejména z norem, metodologií a jejich aplikací zejména v knižní podobě. Problémem této skupiny profesionálních odborníků je značná nadřazenost a nadsazenost tzv. papírových výstupů nad praktickou realizací a rutinním zavedením řešení bezpečnosti do každodenního života společnosti. Druhá skupina z pohledu praktické bezpečnosti nahlíží na problematiku zejména z tzv. technologické bezpečnosti IS nebo kroku implementace bezpečnosti IS/IT což znamená degradaci řešení na technologickou úroveň. Dalším neduhem je tzv. prosazování tzv. dílčích nekoncepčních technologických řešení zejména u výrobců disponujících pouze jednou

nebo několika bezpečnostními technologiemi. Obrazně můžeme přirovnat k zabezpečenému domu s extrémně chráněnými dveřmi nicméně za stavu plně otevřených oken.

Další nejčastější chyby v procesu řešení informační bezpečnosti je nízká podpora ze strany nejvyššího vedení. Například management deklaruje svůj zájem o informační bezpečnost, je ochoten provést první, nebo několik prvních kroků, ale přijetím bezpečnostní politiky IS jeho podpora končí. Takováto společnost pak končí s bezpečnostní politikou, která zůstává nenaplněna. Celkem velkým problémem je prosazovaní norem a metodologií bezpečnosti IS/IT z teoretické do praktické roviny.

3 CÍLE DISERTAČNÍ PRÁCE

Cíle disertační práce byly formulovány tak, aby respektovaly zadání a téma práce, přičemž výsledky řešení mohly být využity nejen v rámci profese autora v praktické rovině, ale byly přínosem i v oblasti výzkumu bezpečnosti IS/IT. Pro potřeby disertační práce byly cíle rozděleny následujícím způsobem:

Hlavním cílem *disertační práce* je na základě teoretického, terénního výzkumu a praktických zkušeností identifikovat a analyzovat příčiny současných bezpečnostních incidentů a rizikových faktorů IS/IT a jejich vliv na konkurenceschopnost podniků.

Vedlejšími cíli práce jsou:

- Určení směrů a trendů v oblasti bezpečnosti IS/IT
- Mikroekonomické modelace vlivu bezpečnosti IS/IT na konkurenceschopnost
- Stanovení optimálního modelu managementu bezpečnosti IS/IT
- Stanovení optimálního profilu manažera bezpečnosti IS/IT
- Aplikace teoretických znalostí z rešerše do praktické roviny

3.1 Hypotézy disertační práce

Na základě studia specializované literatury zabývající se problematikou bezpečnosti IS/IT a vlastních odborných znalostí a zkušeností byly stanoveny následující hypotézy disertační práce.

- **Hypotéza číslo 1**

  Podstatným prvkem eliminace příčin současných bezpečnostních incidentů je lidský faktor.

- **Hypotéza číslo 2**

  Přiměřená bezpečnost IS/IT závisí:

  a. Na lidském faktoru,
  b. na konkrétní aplikaci norem a metodologií v organizaci (Management procesní bezpečnosti),

c. na aplikaci bezpečnostních technologických prvků (Management technologické bezpečnosti).

§ Hypotéza číslo 3

Bezpečnost IS/IT zvyšuje konkurenceschopnost společnosti.

4 ZVOLENÉ METODY ZPRACOVÁNÍ

Globální zpracování disertační práce bylo založeno na analyticko-syntetické metodě a postupu, kdy známé teoretické prvky poznání bezpečnosti IS/IT jsou rozšířené o aktuální výstupy bezpečnostních kvalitativních a kvantitativních průzkumů a zkušeností z řešení bezpečnostních projektů.

4.1 Metody a techniky použité v řešení disertační práce

Za účelem co nejefektivnějšího dosažení stanovených hlavních a vedlejších cílů a ověření uvedených hypotéz disertační práce byly zvoleny následující metody šetření:

- *Problémová analýza.* Hledání odpovědí na otázky k uvedenému tématu:
  - Jaké jsou problémy teoretického poznání bezpečnosti IS/IT?
  - Jaké jsou problémy při aplikaci teoretického poznání bezpečnosti IS/IT do praxe?
  - Jak eliminovat bezpečnostní rizika a hrozby?
  - Jak stanovit přiměřenou bezpečnost z pohledu technologií, managementu a ekonomické roviny?
  - Jaký by měl být optimální profil bezpečnostního manažera IS/IT?
  - Jaké jsou problémy vazeb a vztahů manažerů bezpečnosti IS/IT a manažerů IS/IT?
  - Jak může ovlivnit bezpečnost IS/IT konkurenceschopnost?
- *Kritická analýza* teoretických pramenů vztahujících se k tématu bezpečnosti IT/IS a vztahu ke konkurenceschopnosti především z metodologií, norem, specializovaných odborných domácích i zahraničních zdrojů.
- *Kvantitativní výzkum* ve formě telemarketingového dotazníkového šetření na reprezentativním vzorku menších a středních společností splňující následující kritéria:
  - Sídlo v lokalitě Zlínského kraje,
  - minimální počet zaměstnanců 25,

- komerční organizace,
- společnosti nepůsobící v IT,
- ekonomická stabilita.

Kontaktováno bylo 194 společností, odpovědi poskytlo 161 společností. Oslovení byli pracovníci odpovědní za problematiku bezpečnosti IT. Otázky byly směřovány ke zvolení jedné z nabízených odpovědí. Data byla vyhodnocena metodou deskriptivní statistiky.

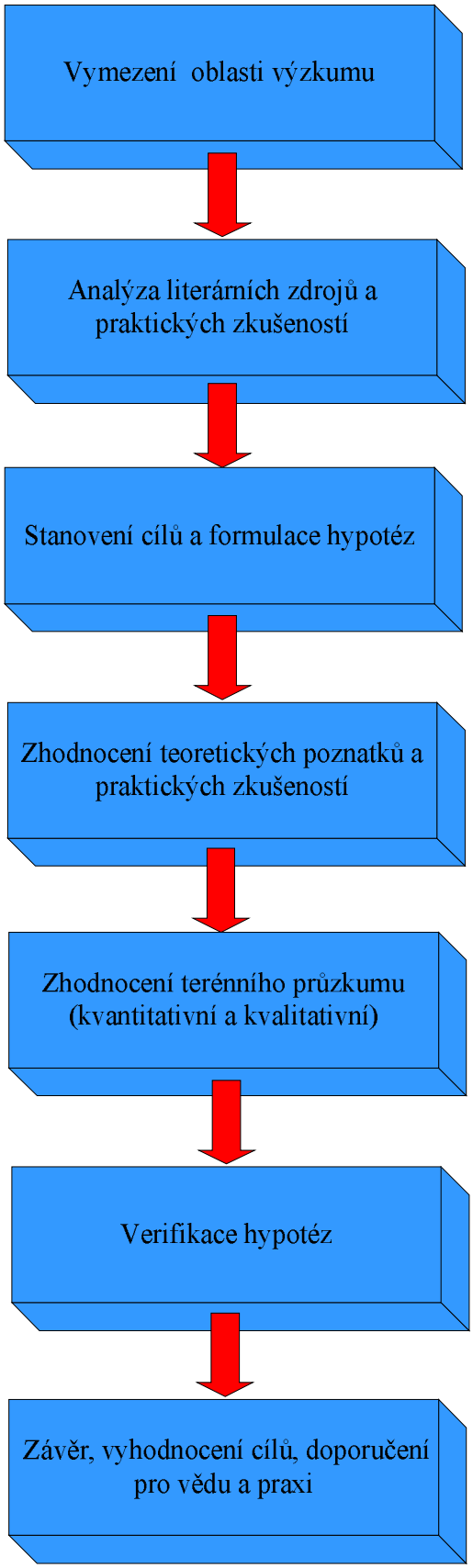
- *Kvalitativní výzkum* ve formě hloubkového interview na reprezentativním vzorku velkých společností s představiteli managementu IT a managementu bezpečnosti IT. Kvalitativní výzkum představuje analýzu vztahů, závislostí a příčin přímo u zkoumaného subjektu a jejich zobecnění. Tento typ výzkumu vyžaduje použití náročnějších postupů, nicméně umožňuje provést výzkum na menším vzorku než u kvantitativního. Kvalitativní výzkum probíhal v následujících organizacích:
  - Obchodní,
  - finanční.

  Subjektivně velmi ceněnou skutečností kvalitativního výzkumu byly neformální průběhy hloubkového individuálního interview. Bez uvedeného přístupu, zejména z pohledu při práci s velmi citlivými údaji ve vazbě na ohrožení konkurenceschopnosti a případně negativních dopadů na společnost v případě úniku dat, by nebylo možné získat otevřený stav zkoumané problematiky. Při práci s kvalitativními daty byla uplatněna obsahová analýza.

- *Případové studie.* K doplnění problematiky tématu byly doplněny subjektivní analýzy bezpečnostních incidentů na konkrétních případech.

4.2 Postup řešení disertační práce

Pro zpracování disertační práce byl zvolen následující postup typický pro řešení většiny vědeckých prací:



Obr. 4.2 Postup řešení disertační práce [Vlastní zpracování]

5 HLAVNÍ VÝSLEDKY PRÁCE

Práce přinesla celou řadu výsledků a poznání, které mají přímý vztah k podnikové praxi i vazbu na teoretický výzkum. Hlavní výsledky a přínosy mé práce vidím v následujících kapitolách.

5.1 Kvantitativní průzkum bezpečnosti IS/IT ve firmách Zlínského kraje

Pro ověření požadavku společností a aktuálnosti navržené problematiky jsem v rámci vnitrofiremní informační strategie realizoval během listopadu a prosince 2004 tržní kvantitativní průzkum menších a středních společností formou telemarketingu. Jednou z významných částí uvedeného kvantitativního výzkumu byla problematika bezpečnosti dat a IS/IT.

5.1.1 **Rozsah**

Primárním vstupním podkladem pro uvedený průzkum a následnou analýzu dat byla databáze Albertina - Firemní monitor 11/2004. Byla selektována skupina společností splňující zejména následující kritéria:

- Sídlo v lokalitě Zlínského kraje,
- minimální počet zaměstnanců 25,
- komerční organizace,
- společnosti nepůsobící v IT,
- ekonomická stabilita.

Výsledkem uvedených selektivních parametrů byla informační databáze 153 komerčních organizací Zlínského kraje.

5.1.2 **Informační tematické okruhy**

Telemarketing byl zaměřen na monitoring stavu vybraných společností dle kritérií uvedených v předchozí kapitole z pohledu infrastruktury a bezpečnosti IS/IT. Oslovení byli administrátoři a odpovědní pracovníci za problematiku bezpečnosti IS/IT. V rámci kvantitativního výzkumu byly vyhodnoceny čtyři stěžejní otázky související s danou problematikou a to:

- Preferujete bezpečnost IS/IT z pohledu konkurenceschopnosti vlastní společnosti?

- ANO
- NE

- Zajímá Vás možnost získání včasných informací o aktuálních bezpečnostních hrozbách?

  - ANO
  - NE

- Měli byste zájem o zjištění aktuálního stavu bezpečnosti IT ve Vaší společnosti?

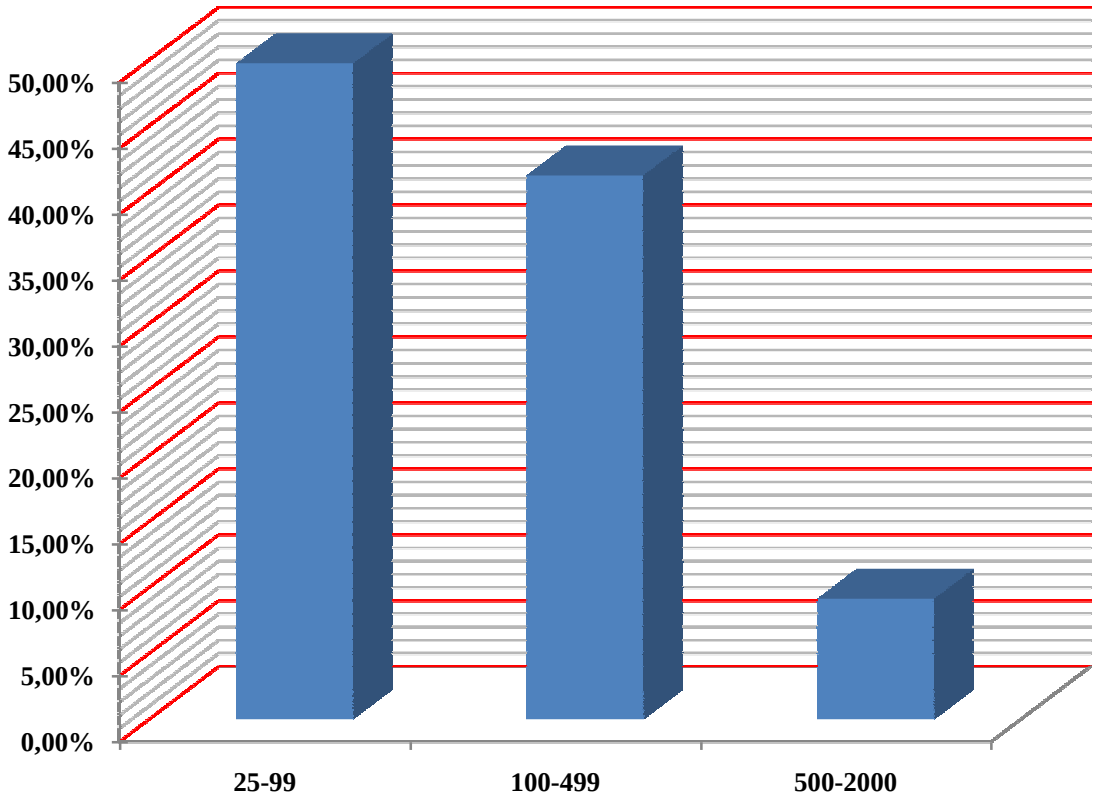
  - ANO
  - NE

- Měli byste zájem o externí správu a monitoring bezpečnostních technologií IS/IT?

  - ANO
  - NE

5.1.3 **Metodologie zpracování**

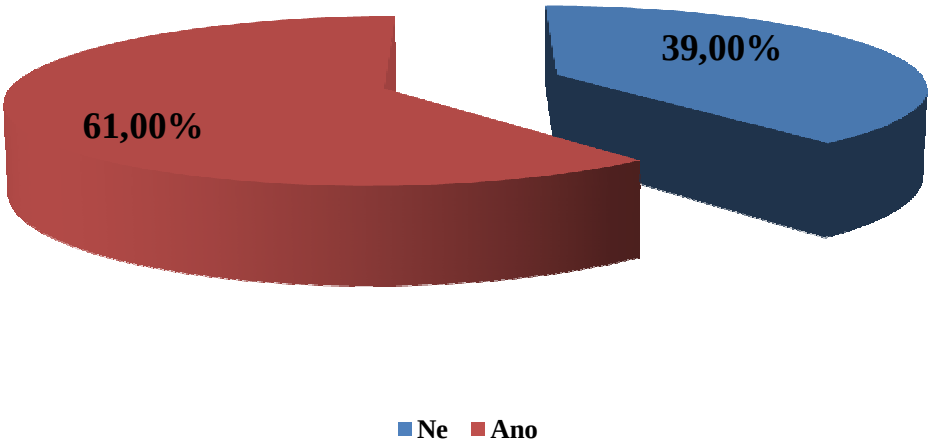
Sběr dat byl uskutečněn formou telemarketingu ze 194 společností, odpovědi poskytlo 161 společností. Otázky byly směřovány ke zvolení jedné z nabízených odpovědí. Zpětným ověřením správnosti informací bylo vyřazeno 8 společností. Data byla vyhodnocena metodou deskriptivní statistiky. Segmentace dotazovaných ukázala strukturu, kterou tvořily společnosti 49,7% s počtem zaměstnanců 25-99, 41,2% s počtem zaměstnanců 100-499 a 9,1% s počtem zaměstnanců 500-2000.



Graf 5.1.3 Struktura dotazovaných společností
[Vlastní zpracování]

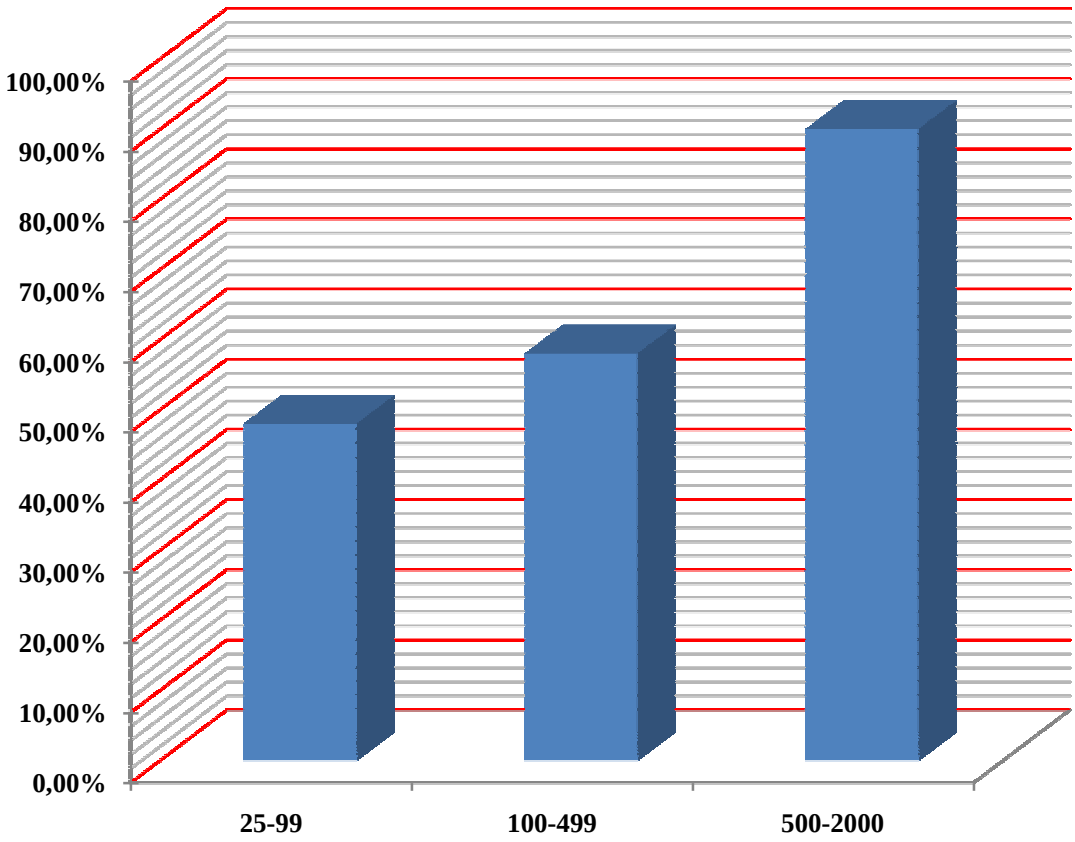
5.1.4 **Selektované výstupy kvantitativního výzkumu**

Prvním ze selektivního výstupu kvantitativního výzkumu byla data vztažená k preferenci bezpečnosti IS/IT z pohledu konkurenceschopnosti vlastní společnosti. Dle toho výstupu vnímá vážnost vazby bezpečnosti IS/IT a vlastní konkurenceschopnost 61% společností. Pro 39% společností není bezpečnost IS/IT z pohledu konkurenceschopnosti významná.



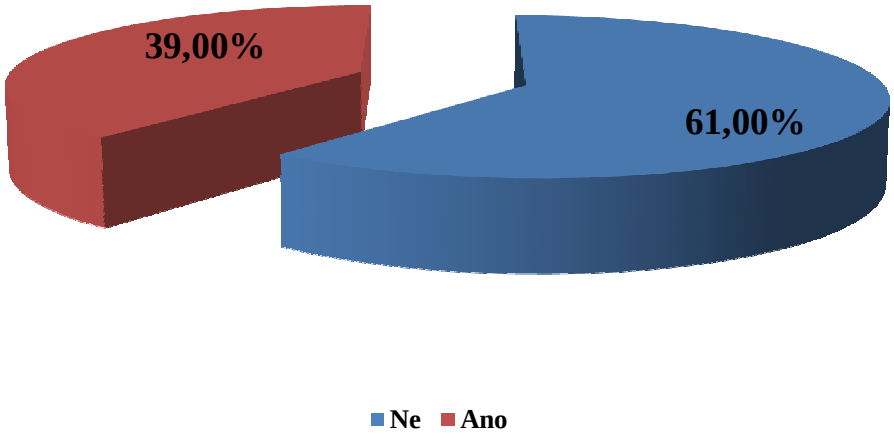
Graf 5.1.4.1 Preference bezpečnosti z pohledu konkurenceschopnosti vlastní společnosti
[Vlastní zpracování]

Pokud se podíváme na strukturu preferenci bezpečnosti IS/IT z pohledu konkurenceschopnosti vlastní společnosti dle velikosti společnosti podle počtu zaměstnanců, největší preferenci bezpečnosti IS/IT přikládají společnosti s počtem zaměstnanců nad 500. S menším počtem zaměstnanců se preference bezpečnosti IS/IT výrazně snižuje. Uvedený výstup potvrzuje, že menší společnosti (s počtem zaměstnanců 25-99) nedoceňují význam svých informací uložených v IS/IT a nepředpokládají jejich zneužití.



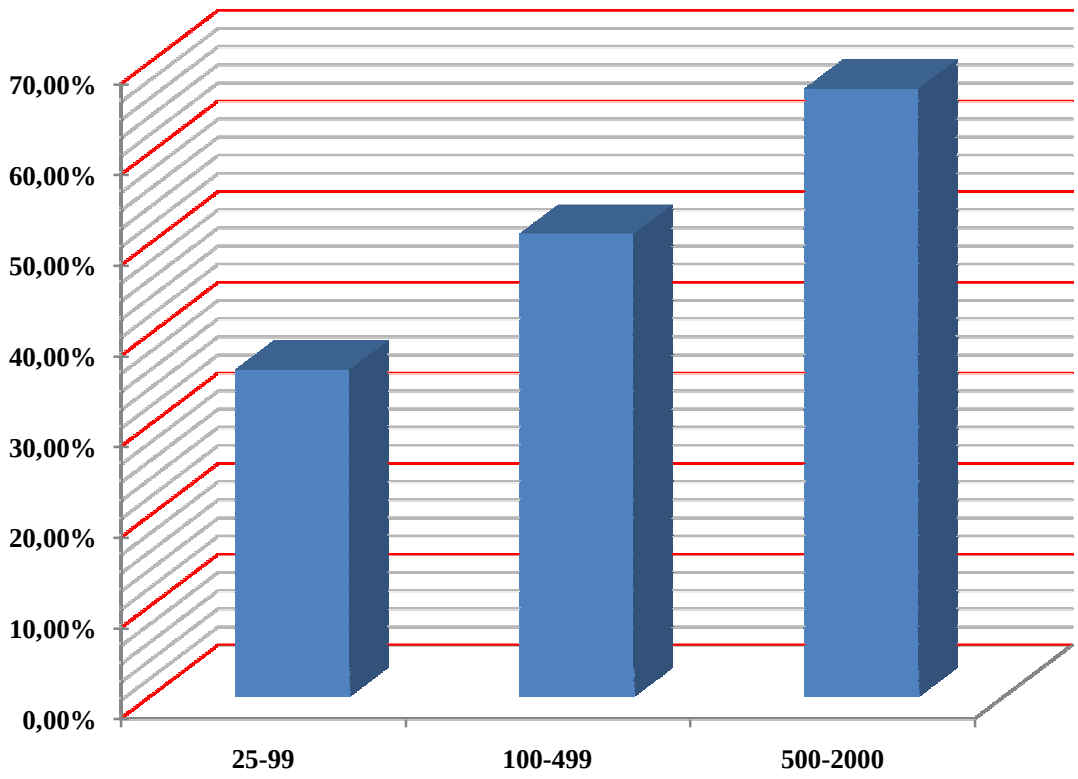
Graf 5.1.4.2 Preference bezpečnosti z pohledu konkurenceschopnosti vlastní společnosti dle velikosti společnosti
[Vlastní zpracování]

Druhým vybraným výstupem kvantitativního výzkumu byla data vztažená k problematice poskytování včasných informací o aktuálních bezpečnostních hrozbách. Bezpečnostními hrozbami byly míněny zejména technologické aspekty: „Antivirové nákazy, kritické zranitelnosti infrastruktury IS/IT, cílené útoky na infrastrukturu“. Překvapivým výstupem je nezájem nadpoloviční části společností o doručování informací bezpečnostních hrozeb IS/IT. 61% společností nemá zájem dostávat včasné informace o aktuálních kritických bezpečnostních hrozbách. Pouze 39% společností má zájem o informační službu aktuálních kritických bezpečnostních hrozeb.



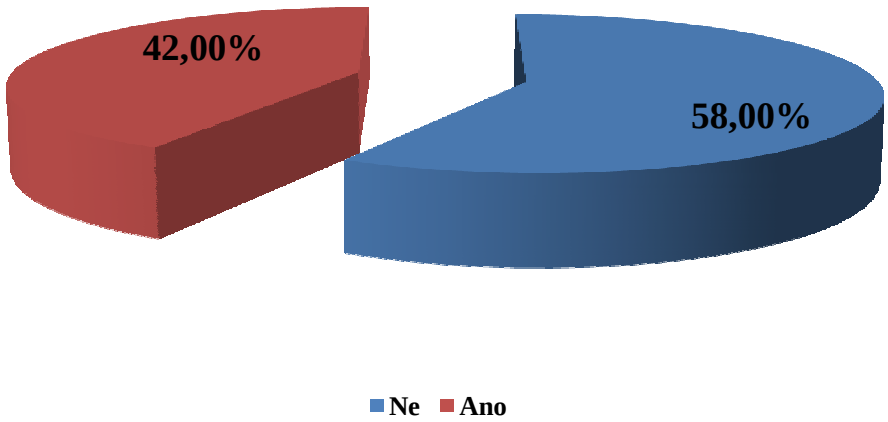
Graf 5.1.4.3 Zájem získání včasných informací o aktuálních bezpečnostních hrozbách [Vlastní zpracování]

Pokud se podíváme na strukturu společností z pohledu zájmu poskytování včasných informací o aktuálních bezpečnostních hrozbách dle velikosti společnosti podle počtu zaměstnanců, největší zájem mají společnosti s počtem zaměstnanců nad 500. S menším počtem zaměstnanců se zájem služby poskytování včasných informací o aktuálních bezpečnostních hrozbách výrazně snižuje. U společností mezi 25-99 zaměstnanci nezájem o včasné informace aktuálních bezpečnostních hrozeb dosahuje téměř 70%. Subjektivně se domnívám, že menší společnosti (s počtem zaměstnanců 25-99) nedoceňují význam svých informací uložených v IS/IT a nepředpokládají jejich zneužití.



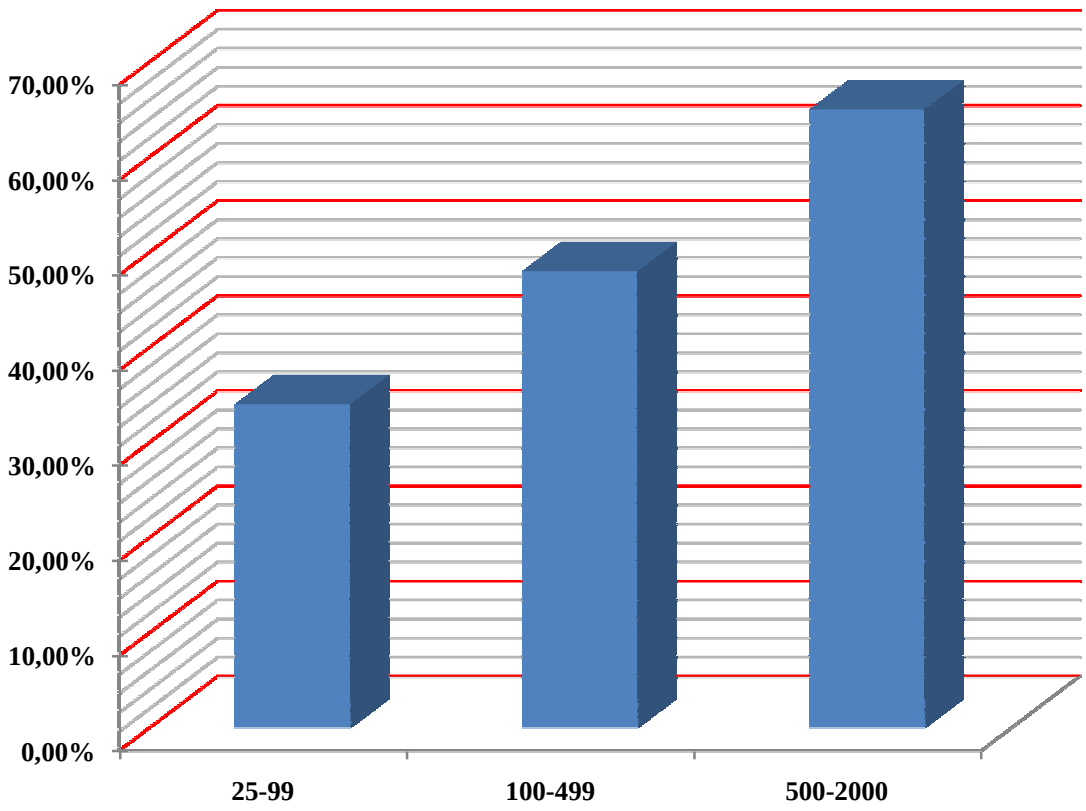
Graf 5.1.4.4 Zájem získání včasných informací o aktuálních bezpečnostních hrozbách dle velikosti společnosti
[Vlastní zpracování]

Třetím vybraným výstupem kvantitativního výzkumu byla data vztažená k problematice zjištění aktuálního stavu bezpečnosti IS/IT ve společnosti. Zjištěním aktuálního stavu byly míněny technologické aspekty bezpečnosti IS/IT: „Provedení základních penetračních testů na selektivní část infrastruktury“. Překvapivým výstupem je nezájem nadpoloviční části společností o zjištění vlastního aktuálního stavu bezpečnosti IS/IT. 58% společností nemá zájem o zjištění vlastního aktuálního stavu bezpečnosti IS/IT. Pouze 42% společností projevuje zájem o zjištění vlastního aktuálního stavu bezpečnosti IS/IT.



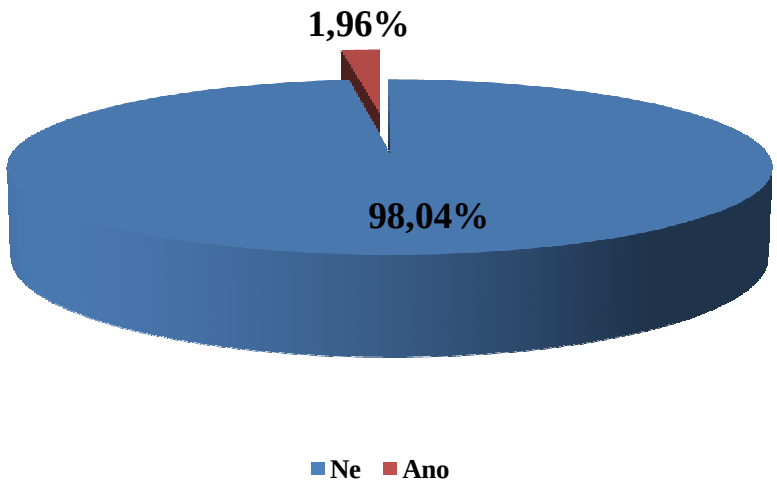
Graf 5.1.4.5 Zájem o zjištění aktuálního stavu bezpečnosti IT ve společnosti [Vlastní zpracování]

V případě analýzy zájmu zjištění aktuálního stavu bezpečnosti IS/IT ve společnosti podle počtu zaměstnanců, největší zájem mají opět společnosti s počtem zaměstnanců nad 500. S menším počtem zaměstnanců se zájem o zjištění vlastního aktuálního stavu bezpečnosti IS/IT výrazně snižuje. Společnosti s počtem 25-99 zaměstnanců nemají zájem o zjištění vlastního aktuálního stavu bezpečnosti IS/IT. Opět se potvrzuje, že menší společnosti (s počtem zaměstnanců 25-99) nedoceňují význam svých informací uložených v IS/IT a nepředpokládají jejich zneužití. U společností nad 500 zaměstnanců zájem o zjištění vlastního aktuálního stavu bezpečnosti IS/IT přesahuje 60 %. U společností s počtem zaměstnanců mezi 100-499 je poměr zájmu a nezájmu téměř shodný.



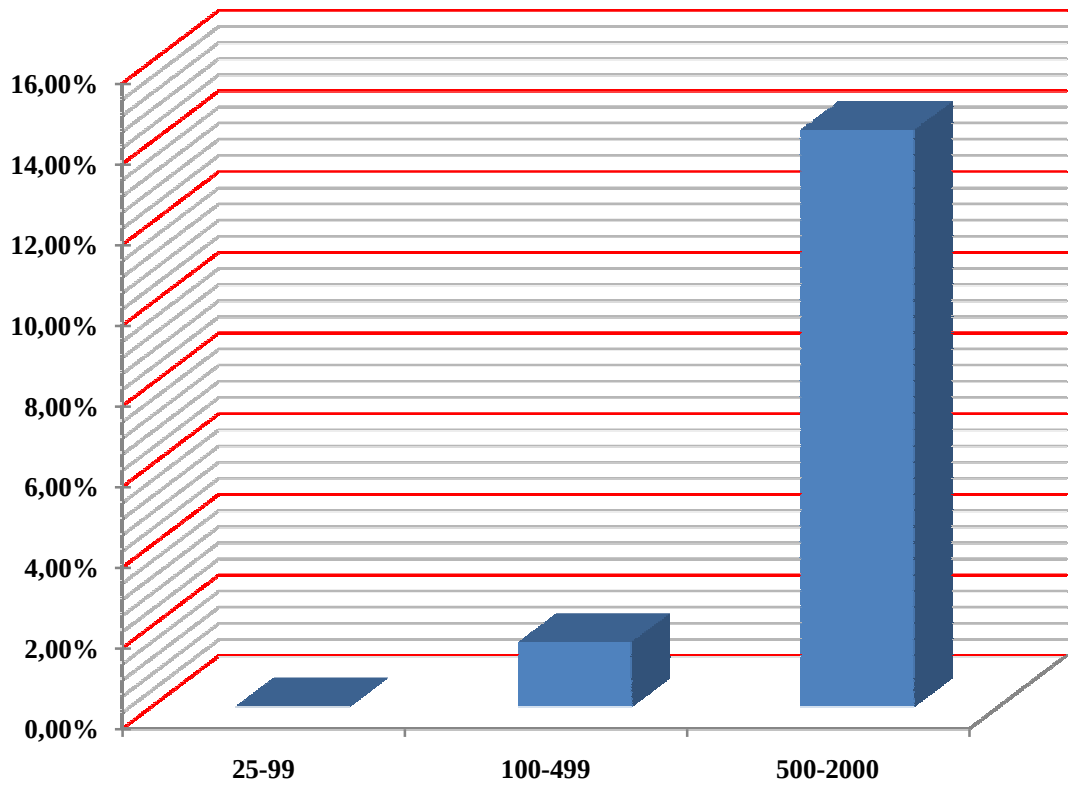
Graf 5.1.4.6 Zájem o zjištění aktuálního stavu bezpečnosti IT ve společnosti dle velikosti společnosti
[Vlastní zpracování]

Čtvrtým vybraným výstupem kvantitativního výzkumu byla data vztažená k problematice externí správy a monitoringu bezpečnostních technologií IS/IT. Monitoringem a správou bezpečnostních technologií IS/IT byly myšleny technologické aspekty bezpečnosti IS/IT: „Monitoring a správa primárních prvků bezpečnosti – správa a údržba antivirové a antispamové ochrany, centrální firewally“. Překvapivým výstupem je absolutní nezájem společností o externí správu a monitoring bezpečnostních technologií IS/IT. Více jak 98% společností nemá zájem o externí správu a monitoringu bezpečnostních technologií IS/IT. Pouze necelá 2% společností projevuje zájem o externí správu a monitoringu bezpečnostních technologií IS/IT.



Graf 5.1.4.7 Zájem o externí správu a monitoring bezpečnostních technologií IS/IT ve společnosti
[Vlastní zpracování]

V případě porovnání zájmu o externí správu a monitoring bezpečnostních technologií IS/IT ve společnosti podle počtu zaměstnanců, zájem projevují spíše společnosti s počtem zaměstnanců nad 500. S menším počtem zaměstnanců se zájem o externí správu a monitoring bezpečnostních technologií IS/IT blíží k nule. Společnosti s počtem 25-99 zaměstnanců nemají žádný zájem o externí správu a monitoring bezpečnostních technologií IS/IT. U společností nad 500 zaměstnanců zájem o externí správu a monitoring bezpečnostních technologií IS/IT dosahuje 14 %. U společností s počtem zaměstnanců mezi 100-499 se zájem o externí správu a monitoring bezpečnostních technologií IS/IT výrazně snižuje a je roven téměř 2%.



Graf 5.1.4.8 Zájem o externí správu a monitoring bezpečnostních technologií IS/IT ve společnosti dle velikosti
[Vlastní zpracování]

5.1.5 Sumarizace kvantitativního průzkumu a porovnání s jinými průzkumy

Z analýzy výsledků kvantitativního výzkumu vyplývá a potvrzuje aktuálnost problematiky a zájem a preference společností Zlínského kraje o problematiku bezpečnosti IS/IT.

Preferenci bezpečnosti IS/IT z pohledu konkurenceschopnosti vlastní společnosti výstupu vnímá vážnost vazby bezpečnosti IS/IT a vlastní konkurenceschopnost 61% společností. Pouze pro 39% společností není bezpečnost IS/IT z pohledu konkurenceschopnosti významná. Pokud se podíváme na strukturu preferenci bezpečnosti IS/IT z pohledu konkurenceschopnosti vlastní společnosti dle velikosti společnosti podle počtu zaměstnanců, největší preferenci bezpečnosti IS/IT přikládají společnosti s počtem zaměstnanců nad 500.

Překvapivým výstupem je nezájem nadpoloviční části společností o doručování informací bezpečnostních hrozeb IS/IT. 61% společností nemá zájem dostávat včasné informace o aktuálních kritických bezpečnostních hrozbách. Pouze

39% společností má zájem o informační službu aktuálních kritických bezpečnostních hrozeb. Pokud se podíváme na strukturu společností z pohledu zájmu poskytování včasných informací o aktuálních bezpečnostních hrozbách dle velikosti společnosti podle počtu zaměstnanců, největší zájem mají společnosti s počtem zaměstnanců nad 500. S menším počtem zaměstnanců se zájem služby poskytování včasných informací o aktuálních bezpečnostních hrozbách výrazně snižuje. U společností mezi 25-99 zaměstnanci nezájem o včasné informace aktuálních bezpečnostních hrozeb dosahuje téměř 70%. Subjektivně se domnívám, že menší společnosti (s počtem zaměstnanců 25-99) nedoceňují význam svých informací uložených v IS/IT a nepředpokládají jejich zneužití.

Dalším překvapivým výstupem je nezájem nadpoloviční části společností o zjištění vlastního aktuálního stavu bezpečnosti IS/IT. 58% společností nemá zájem o zjištění vlastního aktuálního stavu bezpečnosti IS/IT. Pouze 42% společností projevuje zájem o zjištění vlastního aktuálního stavu bezpečnosti IS/IT. V případě analýzy zájmu zjištění aktuálního stavu bezpečnosti IS/IT ve společnosti podle počtu zaměstnanců, největší zájem mají opět společnosti s počtem zaměstnanců nad 500. S menším počtem zaměstnanců se zájem o zjištění vlastního aktuálního stavu bezpečnosti IS/IT výrazně snižuje.

Celkem zajímavým výsledkem kvantitativního výzkumu je absolutní nezájem společností o externí správu a monitoringu bezpečnostních technologií IS/IT. Více jak 98% společností nemá zájem o externí správu a monitoring bezpečnostních technologií IS/IT. V případě porovnání zájmu o externí správu a monitoring bezpečnostních technologií IS/IT ve společnosti podle počtu zaměstnanců, zájem projevují spíše společnosti s počtem zaměstnanců nad 500. S menším počtem zaměstnanců se zájem o externí správu a monitoring bezpečnostních technologií IS/IT blíží k nule.

Část výstupů kvantitativního průzkumu je možné porovnat s Průzkumem stavu informační bezpečnosti v ČR 2003 a 2005 (21) a (22) zejména v části významu informační bezpečnosti. Podle (21) celkem 95% organizací uvedlo, že informační bezpečnost pro ně má význam nebo dokonce velký význam. Uvedený průzkum (21) potvrdil, že s rostoucím počtem zaměstnanců stoupá pro organizace význam informační bezpečnosti. Tento závěr plně i potvrzují výstupy kvantitativního průzkumu. Dle (21) pro pouhé 1% organizací nad 1000 zaměstnanců má informační bezpečnost malý význam. Přestože podle (21) čísla ukazují, že pro drtivou většinu organizací má informační význam, pouhých 53% organizací je přesvědčeno, že se u nich praktické realizaci informační bezpečnosti věnuje dostatečná pozornost.

Ostatní prvky kvantitativního průzkumu představují odlišný pohled na bezpečnost IS/IT uvnitř společností než u standardních průzkumů stavu bezpečnosti

IS/IT. Hlavní rozdíl spočívá v monitoringu zájmu společností o zajištění bezpečnosti IS/IT externími společnostmi a to jak technologické tak i procesní. V oblast technologické správa technologické bezpečnosti IS/IT od formy konzultací až po outsourcing technologické bezpečnosti s přesně definovanými pravidly a úrovní (SLA) poskytovaných služeb. V oblasti metodické a procesní konzultace se zavedením a praktickým prosazením managementu bezpečnosti.

5.2 Kvalitativní průzkum bezpečnosti IS/IT ve vybraných firmách ČR

V rámci disertační práce byl vedle průzkumu kvantitativního proveden také průzkum kvalitativní, jehož cílem bylo zjistit názory na bezpečnost IS/IT od následujících odpovědných a zainteresovaných pracovníků:

- Manažerů IS/IT,
- bezpečnostních manažerů IS/IT,
- administrátorů IS/IT,
- běžných uživatelů.

Kvalitativní průzkum byl proveden formou řízeného individuálního interview na reprezentativním vzorku dvou společností. Původním záměrem bylo uskutečnění kvalitativního průzkumu na větším vzorku společností. Bohužel ze strany odpovědných pracovníků vybraných společností nebylo dáno kladné stanovisko k provedení průzkumu. Subjektivně uvedená stanoviska chápu, neboť v oblasti bezpečnosti IS/IT se jedná o velmi citlivá data a informace, která by mohla za určitých podmínek a okolností negativně dopadnout v přinejmenším na vnější profil společnosti. Druhým aspektem by mohlo být zakrývání objektivního stavu bezpečnosti IS/IT. Vzhledem k uvedeným okolnostem nebudu také uvádět bližší podrobnosti ke společnostem, u kterých byl proveden kvalitativní průzkum.

Pro doplnění výstupů kvalitativního průzkumu u reprezentativního vzorku dvou společností, přikládám zobecnění stavů a názorů ve zkoumané oblasti na fiktivní společnosti. Zobecnění stavů vychází z více jak pětileté praxe v oblasti bezpečnosti i znalosti prostředí jiných společností.

Kvalitativní průzkum byl zaměřen na řízená individuální interview s předem připravenými otázkami, které korelují s tématem disertační práce. Schéma interview je uvedeno v příloze B.

Na následujících podkapitolách uvádím shrnutí nejdůležitějších poznatků získaných z kvalitativního průzkumu separovaných do několika základních náhledů:

- Význam bezpečnosti IS/IT a konkurenceschopnost,
- bezpečnostní hrozby a trendy,
- procesní management bezpečnosti IS/IT,
- technologická bezpečnost IS/IT,
- ekonomická část bezpečnosti IS/IT.

5.2.1 **Rozsah**

Pro potvrzení případně vyvrácení hypotéz, splnění hlavních i vedlejších cílů jsem realizoval během druhé poloviny 2006 a roku 2007 kvalitativní průzkum na reprezentativním vzorku dvou společností:

- Minimální počet zaměstnanců 1500,
- komerční organizace,
- společnosti nepůsobící v IT,
- ekonomická stabilita.

Výsledkem uvedených selektivních parametrů byly společnosti uvedené v následující tabulce. Společnosti byly dle výše uvedených důvodů pojmenovány následujícím způsobem: ABC a.s. , DEF a.s. a XYZ a.s.. U společností ABC a.s. a DEF a.s. se uskutečnil kvalitativní průzkum; společnost XYZ a.s. představuje zobecnění stavů a názorů ve zkoumané oblasti na základě více jak pětileté vlastní praxe v oblasti bezpečnosti IS/IT i znalosti prostředí IS/IT společností.

Tab. 5.2.1 Vybrané společnosti pro kvalitativní průzkum
[Vlastní zpracování]

Název společnosti	**Segment**
ABC a.s.	Finance
DEF a.s.	Obchod
XYZ a.s.	Zobecněná fiktivní společnost (komerční sféra mimo oblast IT)

5.2.2 **Informační tematické okruhy a metodologie zpracování**

Kvalitativní průzkum byl proveden na reprezentativním vzorku dvou společností a jedné fiktivní zobecňující společnosti se zaměřením na otázky korelující k tématu disertační práce. Otázky byly rozděleny podle role a pozice pracovníků společnosti.

Osloveni byli následující reprezentativní zástupci společností:

- Manažer IS/IT,
- bezpečnostní manažer IS/IT,
- administrátor IS/IT,
- běžný uživatel.

Bohužel se ne na všech pozicích podařilo uskutečnit interview se zástupcem na požadované pozici. Proto uvádím přiřazovací tabulky odpovídající navrhované pozici pro interview a skutečné odpovídající pozici. Upřesňující struktura oslovených zástupců společnosti ABC a.s. včetně pozic je uvedena v následující tabulce.

Tab. 5.2.2.1 Struktura oslovených zástupců společnosti ABC a.s. [Vlastní zpracování]

Navrhovaná pozice	**Skutečná pozice**
Manažer IS/IT	Ředitel provozu infrastruktury IS/IT
Bezpečnostní manažer IS/IT	Ředitel bezpečnosti IS/IT
Administrátor IS/IT	Administrátor provozní bezpečnosti IS/IT
Běžný uživatel IS/IT	Administrativní pracovník

Upřesňující struktura oslovených zástupců společnosti DEF a.s. včetně pozic je uvedena v následující tabulce.

Tab. 5.2.2.2 Struktura oslovených zástupců společnosti DEF a.s. [Vlastní zpracování]

Navrhovaná pozice	Skutečná pozice
Manažer IS/IT	Vedoucí infrastruktury
Bezpečnostní manažer IS/IT	Manažer bezpečnosti IS/IT
Administrátor IS/IT	Specialista
Běžný uživatel IS/IT	Administrativní pracovník

Upřesňující struktura fiktivních zástupců společnosti XYZ a.s. včetně pozic je uvedena v následující tabulce.

Tab. 5.2.2.3 Struktura oslovených zástupců společnosti XYZ a.s. [Vlastní zpracování]

Role	Pozice
Manažer IS/IT	Ředitel IS/IT
Bezpečnostní manažer IS/IT	Ředitel bezpečnosti IS/IT
Administrátor IS/IT	Systémový administrátor
Běžný uživatel IS/IT	Obchodní zástupce

V rámci kvalitativního výzkumu bylo uskutečněno globální hodnocení v oblastech souvisejících s danou problematikou:

- Význam bezpečnosti IS/IT a konkurenceschopnost,
- bezpečnostní hrozby a trendy,
- procesní management bezpečnosti IS/IT,
- technologická bezpečnost IS/IT,
- ekonomická část bezpečnosti IS/IT.

Kvalitativní průzkum proběhl formou řízených interview s předem připravenými otázkami, které korelují s tématem disertační práce. Dle jednotlivých odpovědí bylo na místě interview dále doplňováno dalšími komplementárními dotazy. Základní schéma interview je uvedeno v příloze B.

5.2.3 **Význam bezpečnosti IS/IT a konkurenceschopnost**

V části významu bezpečnosti IS/IT a konkurenceschopnosti byly šetřeny odpovědi a jejich subjektivní váha přikládající významu bezpečnosti IS/IT a jeho vlivu na konkurenceschopnost společnosti. Do interview byly zahrnuty všechny pozice:

- Manažer IS/IT,
- bezpečnostní manažer IS/IT,
- administrátor IS/IT,
- běžný uživatel.

Odpovědi dle jednotlivých pozic jsou uvedeny v níže uvedených čtyřech tabulkách.

Tab. 5.2.3.1 Význam bezpečnosti IS/IT a konkurenceschopnost – pohled manažerů IS/IT.
[Vlastní zpracování]

Jaký přikládáte význam obecně bezpečnosti IS/IT pro Vaši společnost?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
má význam	běžný	významný
Může bezpečnost IS/IT ovlivnit prvky konkurenceschopnosti ve Vaší společnosti?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
ano	částečně	ano

Tab. 5.2.3.2 Význam bezpečnosti IS/IT a konkurenceschopnost – pohled bezpečnostních manažerů IS/IT.
[Vlastní zpracování]

Jaký přikládáte význam obecně bezpečnosti IS/IT pro Vaši společnost?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
velký	velký	velký
Může bezpečnost IS/IT ovlivnit prvky konkurenceschopnosti ve Vaší společnosti?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
ano	ano	ano

Tab. 5.2.3.3 Význam bezpečnosti IS/IT a konkurenceschopnost – pohled administrátorů IS/IT.
[Vlastní zpracování]

Jaký přikládáte význam obecně bezpečnosti IS/IT pro Vaši společnost?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
velký	velký	velký
Může bezpečnost IS/IT ovlivnit prvky konkurenceschopnosti ve Vaší společnosti?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
ano	pravděpodobně ano	ano

Tab. 5.2.3.4 Význam bezpečnosti IS/IT a konkurenceschopnost – pohled běžného uživatele.
[Vlastní zpracování]

Jaký přikládáte význam obecně bezpečnosti IS/IT pro Vaši společnost?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
má význam	běžný	běžný

Výstupy kvalitativního průzkumu k problematice významu bezpečnosti IS/IT a vazby na konkurenceschopnost společnosti potvrdily, že pro společnosti bezpečnost IS/IT je významná a má přímé vazby na konkurenceschopnost společnosti. Je cenné, že vliv bezpečnosti IS/IT a jeho význam potvrdili zejména pozice manažerů IS/IT, částečně i zástupci běžných uživatelů.

5.2.4 **Bezpečnostní hrozby a trendy**

V této části kvalitativního výzkumu bezpečnosti IS/IT byly shromažďovány informace k problematice příčin bezpečnostních hrozeb a aktuálních trendů bezpečnosti IS/IT. Interview se účastnily následující pozice:

- Manažer IS/IT,
- bezpečnostní manažer IS/IT,
- administrátor IS/IT,

Odpovědi dle jednotlivých pozic jsou uvedeny v níže uvedených čtyřech tabulkách.

Tab. 5.2.4.1 Bezpečnostní hrozby a trendy – pohled manažerů IS/IT.
[Vlastní zpracování]

Jaké vidíte hlavní příčiny bezpečnostních hrozeb a incidentů v oblasti IS/IT ve Vaší společnosti?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
Lidé; Finance; Technologie.	Technologie; Lidé; Zaneprázdněnost pracovníků; Nedostatek kvalifikovaných pracovníků;	Lidský faktor - uživatel, administrátor; Nedostatky v technologiích; Chybějící finance; Kvalifikovaný personál; Aplikace procesní bezpečnosti do praxe.

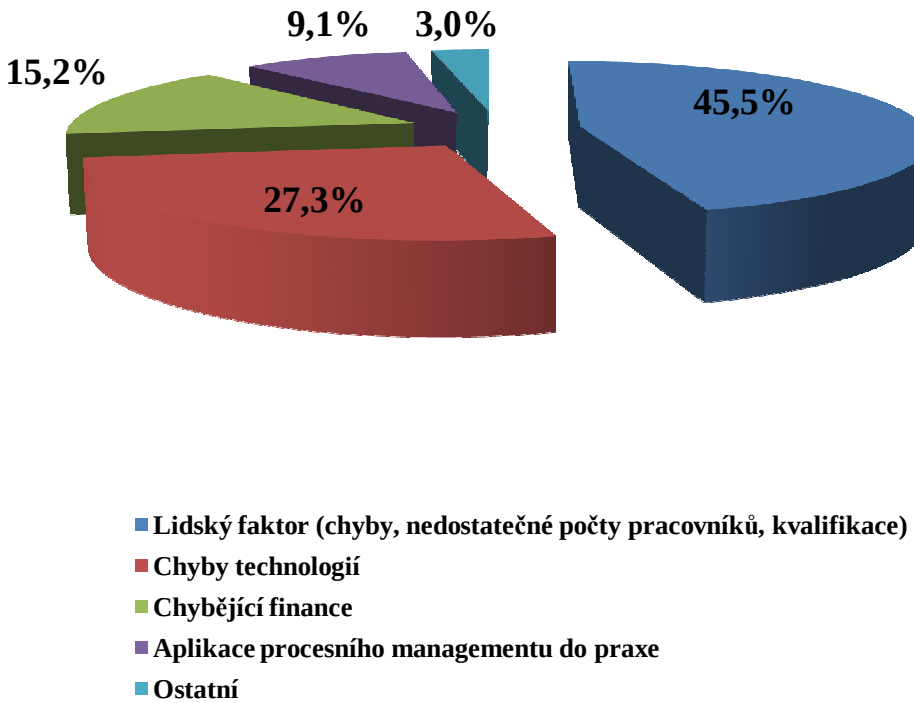
Tab. 5.2.4.2 Bezpečnostní hrozby a trendy – pohled bezpečnostních manažerů IS/IT.
[Vlastní zpracování]

Jaké vidíte hlavní příčiny bezpečnostních hrozeb a incidentů v oblasti IS/IT ve Vaší společnosti?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
Omezené finance; Nedostatek kvalifikovaného personálu; Chyby v technologiích a jejich odstraňování; Globalizace komunikace.	Chyby v technologiích a jejich odstraňování; Zaneprázdněnost pracovníků; Nedostatek kvalifikovaných pracovníků; Prosazování procesů	Shodné jako u manažera IS/IT
Jakým způsobem sledujete trendy bezpečnosti IS/IT?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
ON-Line přístupy do proaktivních systémů varování; Školení CISA, CISM; ISACA výměna názorů	Odbornými školeními	Odbornými školeními; Informace ze systémů proaktivní ochrany.

Tab. 5.2.4.3 Bezpečnostní hrozby a trendy – pohled administrátorů IS/IT. [Vlastní zpracování]

Jaké vidíte hlavní příčiny bezpečnostních hrozeb a incidentů v oblasti IS/IT ve Vaší společnosti?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
Chyby v technologiích a jejich odstraňování; Lidský faktor.	Chyby v technologiích a jejich odstraňování; Zaneprázdněnost;	Shodné jako u manažera IS/IT

Sumarizace odpovědí všech pozic (Manažer IS/IT, bezpečnostních manažer IS/IT, administrátor IS/IT) k otázce příčin bezpečnostních hrozeb je zpracována v níže uvedeném grafu.



Graf 5.2.4 Sumarizace bezpečnostních hrozeb [Vlastní zpracování]

K hlavním příčinám bezpečnostních hrozeb dle výstupu sumarizací odpovědí patří: lidský faktor (lidské chyby, nedostatečná kvalifikace, zaneprázdněnost a nedostatečný počet pracovníků), chyby v technologiích (aplikace i infrastruktura), nedostatek financí do bezpečnostních technologií IS/IT a prosazování bezpečnostního managementu IS/IT. Pro sledování trendů bezpečnosti využívají bezpečnostní manažeři IS/IT odbornými školení a „workshopy“ a sledováním „on-line zdrojů“ a systémů proaktivní ochrany.

5.2.5 **Procesní management bezpečnosti IS/IT**

V části kvalitativního výzkumu bezpečnosti IS/IT byly shromažďovány informace k problematice procesní management bezpečnosti IS/IT. Do interview poskytly odpovědi následující pozice:

- Manažer IS/IT,
- bezpečnostní manažer IS/IT,
- administrátor IS/IT,
- běžný uživatel.

Odpovědi dle jednotlivých pozic jsou uvedeny v níže uvedených čtyřech tabulkách.

Tab. 5.2.5.1 Procesní management bezpečnosti IS/IT – pohled manažerů IS/IT. [Vlastní zpracování]

Máte ve formě dokumentu formálně definovanou a nejvyšším vedením přijatou bezpečnostní politiku?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
Ano	Ano	Ano
Jaké je postavení oddělení bezpečnosti IS/IT ve Vaší společnosti?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
Procesní bezpečnost IS/IT přímo podřízená vrcholovému managementu; provozní ve struktuře managementu IS/IT	Procesní i provozní pod vedením IS/IT, metodicky řízena ze zahraničí	Procesní bezpečnost pod vedením obecné bezpečnosti a auditu; technologická pod část IS/IT

Jaké vlastnosti by měl mít manažer bezpečnosti IS/IT?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
Autorita, důslednost, odbornost, znalost prostředí	Odbornost, manažerské schopnosti, analytické schopnosti	Autorita, odbornost, manažerské schopnosti, prezentační schopnosti, znalost prostředí

K podstatným výstupům odpovědí manažerů IS/IT v oblasti procesní bezpečnost IS/IT patří existence formálně definované a nejvyšším vedením přijaté bezpečnostní politiky. Sekce bezpečnosti IS/IT dle výstupů odpovědí je přímo podřízena vrcholovému managementu, část technologické bezpečnosti vedení IS/IT. Podstatné vlastnosti manažerů bezpečnosti jsou sumarizovány za tabulkou odpovědí bezpečnostních manažerů IS/IT. Na dalších čtyřech obrázcích s blokovými diagramy je zobrazena zjednodušená organizační struktura společnosti ABC a.s., DEF a.s. a XYZ a.s. ve vazbě na bezpečnost IS/IT. U společnosti ABC a.s. navíc zjednodušená struktura Výboru pro řízení bezpečnosti ABC a.s. ve vazbě na bezpečnost IS/IT.

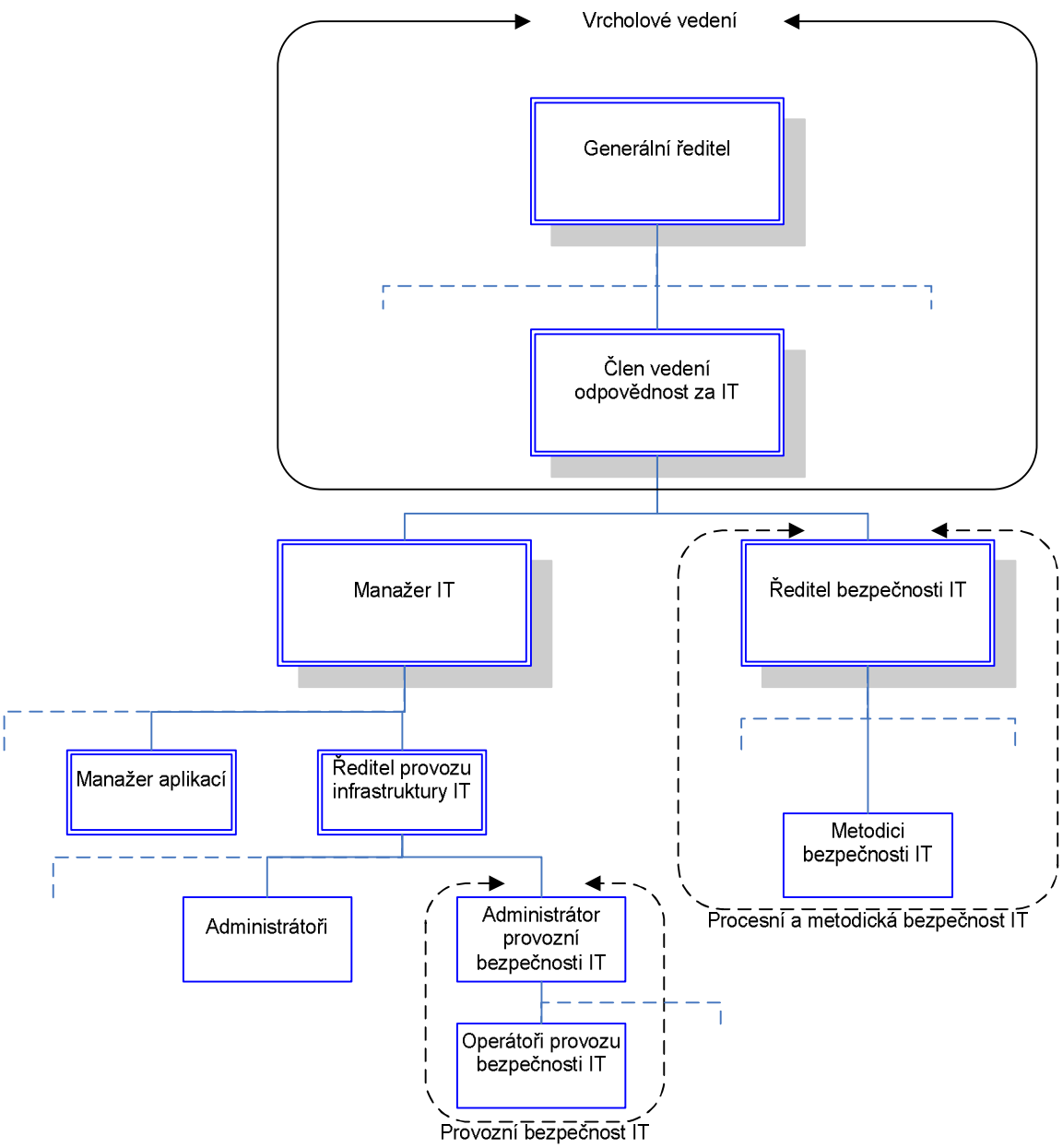
V případě detailního pohledu na zjednodušenou organizační strukturu společnosti ABC a.s. pozorujeme přímé řízení procesní bezpečnosti IS/IT vrcholovým vedením společnosti. Provozní bezpečnost IS/IT je podřízena provozu infrastruktury. Mírně negativně vnímám odtržení provozní bezpečnosti IS/IT od vedení bezpečnosti IS/IT. Příčinou je procesní rychlost a organizační řídící distance mezi procesní a technologickou bezpečností.

Ve společnosti ABC a.s. byl také vytvořen pomocný řídící orgán „Výbor pro řízení celkové bezpečnosti společnosti ABC a.s.“. Výbor zajišťuje řešení problematiky komplexního pohledu na celkovou bezpečnost společnosti tedy nejen bezpečnosti IS/IT ale i náhled právní, personální, provozu, ostatní bezpečnosti ve vazbě na vrcholové vedení společnosti.

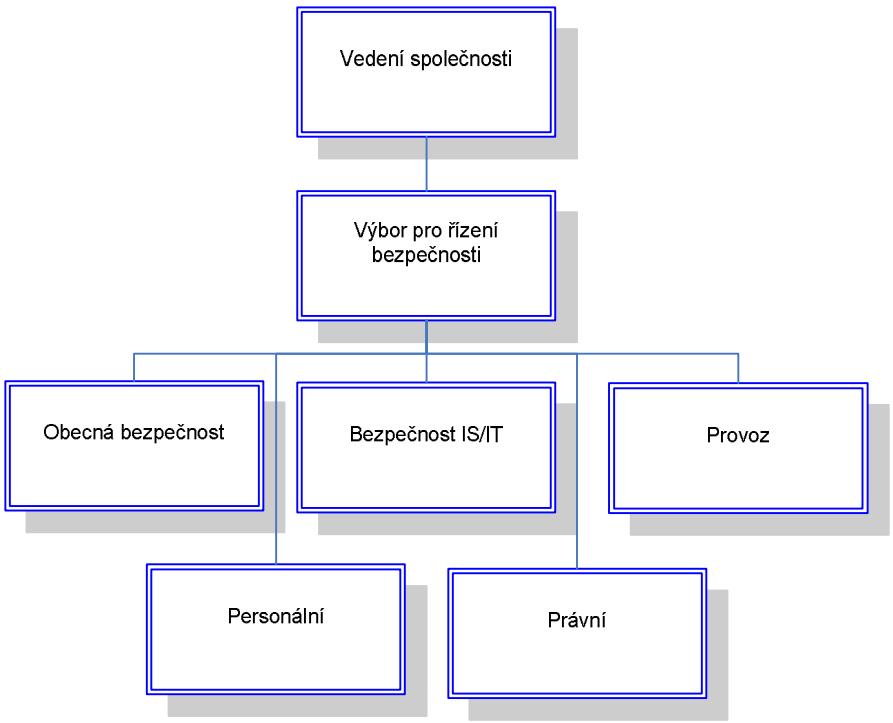
Náhledem na zjednodušenou organizační strukturu společnosti DEF a.s. vidíme také přímé řízení procesní bezpečnosti IS/IT vrcholovým vedením společnosti. Rozdílem jsou zásahy z vnější nadnárodní organizační struktury jako např. definice standardů, ověřené metodiky atd. Provozní bezpečnost IS/IT je podřízena části administrace. Mírně negativně vnímám také odtržení provozní bezpečnosti IS/IT od vedení bezpečnosti IS/IT, navíc negativa jsou prohloubena současnou činností administrace tak i monitoringem technologické bezpečnosti IS/IT.

V případě detailního pohledu na zjednodušenou organizační strukturu společnosti XYZ a.s. pozorujeme také přímé řízení procesní bezpečnosti IS/IT vrcholovým vedením společnosti. Provozní bezpečnost IS/IT je podřízena manažeru

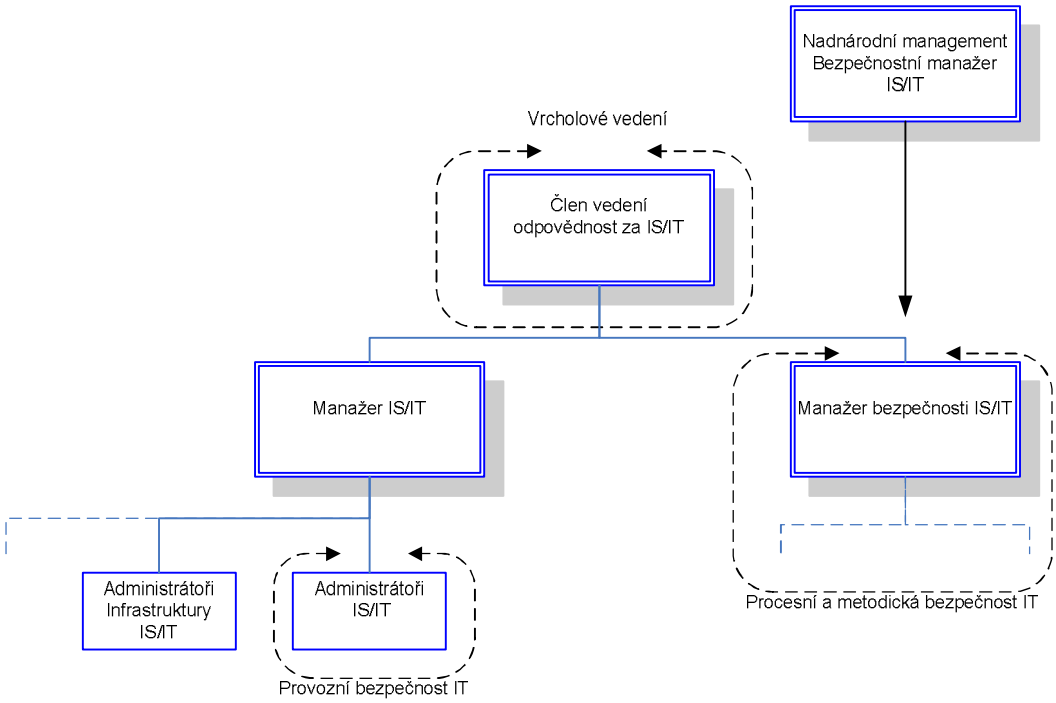
IS/IT. Mírně negativně vnímám opět odtržení provozní bezpečnosti IS/IT od vedení bezpečnosti IS/IT.



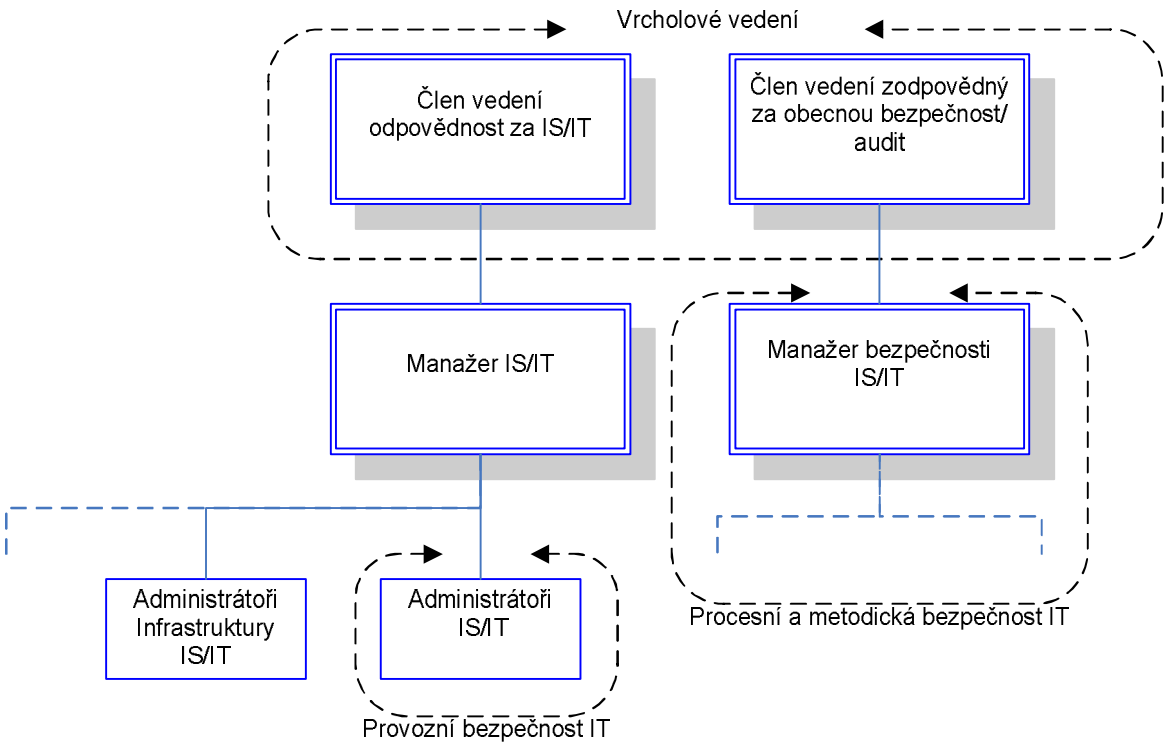
Obr. 5.2.5.1 Zjednodušená organizační struktura společnosti ABC a.s. ve vazbě na bezpečnost IS/IT
[Vlastní zpracování]



Obr. 5.2.5.2 Zjednodušená struktura Výboru pro řízení bezpečnosti ABC a.s. ve vazbě na bezpečnost IS/IT
[Vlastní zpracování]



Obr. 5.2.5.3 Zjednodušená organizační struktura společnosti DEF a.s. ve vazbě na bezpečnost IS/IT
[Vlastní zpracování]



Obr. 5.2.5.4 Zjednodušená organizační struktura společnosti XYZ a.s. ve vazbě na bezpečnost IS/IT
[Vlastní zpracování]

Tab. 5.2.5.2 Procesní management bezpečnosti IS/IT – pohled bezpečnostních manažerů IS/IT.
[Vlastní zpracování]

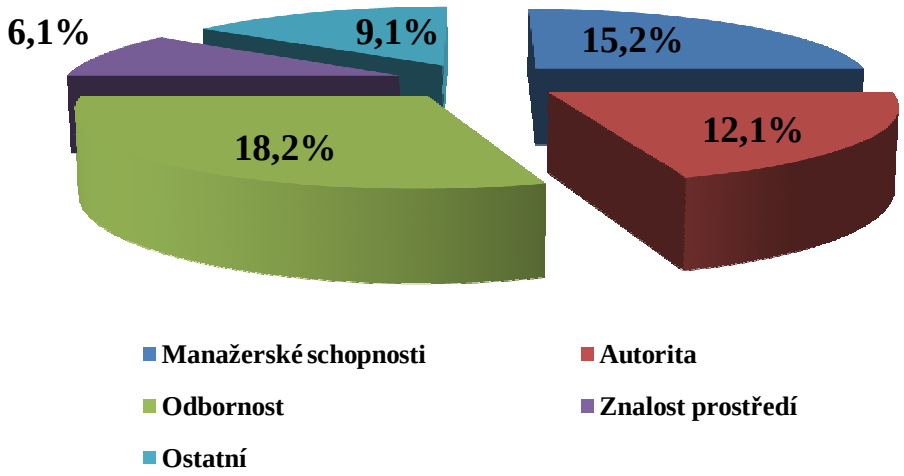
Jakými hlavními bezpečnostními normami, metodologii a standardy pro IS/IT se řídíte?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
ISO/IEC 17799:2005; ISO IEC 27001:2005; ISO/IEC TR 13335; ITIL Cobit CRAMM	BS 7799-1; BS 7799-2; ISO/IEC TR 13335 Cobit	BS 7799 ISO/IEC TR 13335

Jak vnímáte vazby mezi managementem IS/IT a managementem bezpečnosti IS/IT?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
Konfliktní při prosazování bezpečnostních projektů a politik	Standardní	Konfliktní
Jaké vlastnosti by měl mít manažer bezpečnosti IS/IT?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
Odbornost, manažerské schopnosti, autorita, cílevědomost	Manažerské schopnosti, certifikace CISM (CISA)	Manažerské schopnosti, odbornost a znalosti, autorita
Co by bylo možné udělat pro zlepšení bezpečnosti IS/IT ve Vaší společnosti?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
Více financí, větší podpora vedení,	Finance, personál, školení zaměstnanců	Podpora vedení, finance, školení zaměstnanců

K podstatným výstupům odpovědí bezpečnostních manažerů IS/IT v oblasti procesní bezpečnost IS/IT patří seznam metodik, standardů a norem pro management bezpečnosti IS/IT. Hlavními jsou normy a standardy plynoucí z BS 7799, ISO/IEC TR 13335, ITIL, Cobit a CRAMM.

Cenným výstupem jsou rozporné vazby mezi managementem IS/IT a bezpečností IS/IT. K podstatným vlastnostem manažerů bezpečnosti patří: „Odbornost, manažerské vlastnosti, autorita a znalost prostředí.“

Uvedená sumarizace podstatných vlastností je zobrazena v následujícím grafu 5.2.5. Pro zlepšení stavu bezpečnosti IS/IT dle odpovědí je třeba: „Více financí, větší podpora vedení, školení zaměstnanců a specialistů.“



Graf 5.2.5 Profil manažera bezpečnosti IS/IT
[Vlastní zpracování]

Tab. 5.2.5.3 Procesní management bezpečnosti IS/IT – pohled administrátorů IS/IT.
[Vlastní zpracování]

Jak vnímáte vazby mezi administrací IS/IT a managementem bezpečnosti IS/IT?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
Komplikace při administraci, procesní žádosti o povolení úkonů	normální	Výrazné ztížení činnosti administrátorů
Probíhají školení v oblasti bezpečnost IS/IT?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
Ano	Nevím	Ano
Víte o existenci směrnic a politik bezpečnosti IS/IT ve Vaší společnosti?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
Ano	Ano	Ano

Cenným výstupem odpovědí administrátorů IS/IT v oblasti procesní bezpečnosti IS/IT jsou také rozporné vazby mezi administrací IS/IT a bezpečností IS/IT. Významné pro management bezpečnosti IS/IT jsou školení i znalost existence směrnic a politik bezpečnosti IS/IT u administrátorů IS/IT.

Tab. 5.2.5.4 Procesní management bezpečnosti IS/IT – pohled běžného uživatele. [Vlastní zpracování]

Probíhají školení v oblasti bezpečnost IS/IT?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
Ano	Ne	Ano

5.2.6 Technologická bezpečnost IS/IT

V části kvalitativního výzkumu bezpečnosti IS/IT byly shromažďovány informace k problematice technologické bezpečnosti IS/IT. Do interview poskytly odpovědi následující pozice:

- Manažer IS/IT,
- bezpečnostní manažer IS/IT,
- administrátor IS/IT.

Odpovědi dle jednotlivých pozic jsou uvedeny v níže uvedených třech tabulkách.

Tab. 5.2.6.1 Technologická bezpečnosti IS/IT – pohled manažerů IS/IT. [Vlastní zpracování]

Jakým způsobem je řízena technologická bezpečnost IS/IT?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
Prostřednictvím bezpečnostního provozu IS/IT	Administrace infrastruktury IS/IT	Bezpečnostní provozní dohled IS/IT

Tab. 5.2.6.2 Technologická bezpečnosti IS/IT – pohled bezpečnostních manažerů IS/IT. [Vlastní zpracování]

Jaký máte názor na preferenci technologické bezpečnosti IS/IT?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
Procesní bezpečnost je rámcově nadřazená nad technologickou	Z procesní musí metodicky řídit technologickou	Procesní by měla udávat směr, technologická realizovat v oblasti technologické

Tab. 5.2.6.3 Technologická bezpečnosti IS/IT – pohled administrátorů IS/IT. [Vlastní zpracování]

Jaký máte názor na preferenci technologické bezpečnosti IS/IT?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
Preference technologické nad procesní	Preference technologické nad procesní	Technologická je významná

Pro zabezpečení technologické bezpečnost IS/IT existuje provoz (dohled) provozní bezpečnosti viz potvrzení předchozích odpovědí. Zajímavým výstupem jsou rozporuplné výstupy jednotlivých pozic manažerů bezpečnosti IS/IT versus administrátorů IS/IT. Manažeři bezpečnosti zastávají ve většině názor opodstatněnosti úlohy procesního managementu IS/IT. Administrátoři IS/IT jsou přesvědčeni o větší váze technologické bezpečnosti IS/IT.

5.2.7 **Ekonomická část bezpečnosti IS/IT**

V této části kvalitativního výzkumu bezpečnosti IS/IT byly shromažďovány informace k problematice ekonomické části bezpečnosti IS/IT. Do interview jsem zařadil následující pozice:

- Manažer IS/IT,
- bezpečnostní manažer IS/IT.

Odpovědi dle jednotlivých pozic jsou uvedeny v níže uvedených dvou tabulkách.

Tab. 5.2.7.1 Ekonomická část bezpečnosti IS/IT – pohled manažerů IS/IT. [Vlastní zpracování]

Jaký je procentuální poměr investic do oblasti bezpečnosti IS/IT versus investice do IS/IT?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
Odhad cca do 5%	Těžko rozlišitelné, některé technologické prvky přímo provázané	Odhady 2-6%

Tab. 5.2.7.2 Ekonomická část bezpečnosti IS/IT – pohled bezpečnostních manažerů IS/IT.
[Vlastní zpracování]

Jaký by měl být procentuální poměr investic do oblasti bezpečnosti IS/IT versus investice do IS/IT?		
ABC a.s.	**DEF a.s.**	**XYZ a.s.**
Cca 10%	5-8%	Do 10%

Investice cíleně určené pouze pro bezpečnost IS/IT je velmi problematické identifikovat. Investice do bezpečnosti IS/IT se výrazně prolínají s investicemi do celkové infrastruktury. Poměr investic do bezpečnosti IS/IT dle odpovědí činí v rozmezí 2-6%. Přiměřený poměr dle vyjádření bezpečnostních manažerů IS/IT by měl být cca okolo 10%.

5.2.8 Sumarizace kvalitativního průzkumu a porovnání s jinými průzkumy

Kvalitativní průzkum přinesl celou řadu výsledků vztažených k hlavním i vedlejším cílům disertační práce.

Význam bezpečnosti IS/IT a konkurenceschopnost

Výstupy kvalitativního průzkumu k problematice významu bezpečnosti IS/IT a vazby na konkurenceschopnost společnosti potvrdily, že pro společnosti bezpečnost IS/IT je významná a má přímé vazby na konkurenceschopnost společnosti. Je cenné, že vliv bezpečnosti IS/IT a jeho význam potvrdili zejména pozice manažerů IS/IT, částečně i zástupci běžných uživatelů.

Bezpečnostní hrozby a trendy

K hlavním příčinám bezpečnostních hrozeb dle výstupu sumarizací odpovědí patří: lidský faktor (lidské chyby, nedostatečná kvalifikace, zaneprázdněnost a nedostatečný počet pracovníků), chyby v technologiích (aplikace i infrastruktura), nedostatek financí do bezpečnostních technologií IS/IT a prosazování bezpečnostního managementu IS/IT. Pro sledování trendů bezpečnosti využívají bezpečnostní manažeři IS/IT odbornými školení a „workshopy“ a sledováním on-line zdrojů a systémů proaktivní ochrany.

Procesní management bezpečnosti IS/IT

K podstatným výstupům odpovědí manažerů IS/IT v oblasti procesní bezpečnost IS/IT patří existence formálně definované a nejvyšším vedením přijaté bezpečnostní politiky. Sekce bezpečnosti IS/IT dle výstupů odpovědí je přímo podřízena vrcholovému managementu, část technologické bezpečnosti vedení IS/IT.

K podstatným výstupům odpovědí bezpečnostních manažerů IS/IT v oblasti procesní bezpečnost IS/IT patří seznam metodik, standardů a norem pro management bezpečnosti IS/IT. Hlavními jsou normy a standardy plynoucí z BS 7799, ISO/IEC TR 13335, ITIL, Cobit a CRAMM. Cenným výstupem jsou rozporné vazby mezi managementem IS/IT a bezpečností IS/IT. K podstatným vlastnostem manažerů bezpečnosti patří: Odbornost, manažerské vlastnosti, autorita a znalost prostředí. Pro zlepšení stavu bezpečnosti IS/IT dle odpovědí je třeba: více financí, větší podpora vedení, školení zaměstnanců a specialistů.

Cenným výstupem odpovědí administrátorů IS/IT v oblasti procesní bezpečnosti IS/IT jsou také rozporné vazby mezi administrací IS/IT a bezpečností IS/IT. Významné pro management bezpečnosti IS/IT jsou školení i znalost existence směrnic a politik bezpečnosti IS/IT u administrátorů IS/IT.

Technologická bezpečnost IS/IT

Pro zabezpečení technologické bezpečnost IS/IT existuje provoz (dohled) provozní bezpečnosti viz potvrzení předchozích odpovědí. Zajímavým výstupem jsou rozporuplné výstupy jednotlivých pozic manažerů bezpečnosti IS/IT versus administrátorů IS/IT. Manažeři bezpečnosti zastávají ve většině názor opodstatněnosti úlohy procesního managementu IS/IT. Administrátoři IS/IT jsou přesvědčeni o větší váze technologické bezpečnosti IS/IT.

Ekonomická část bezpečnosti IS/IT

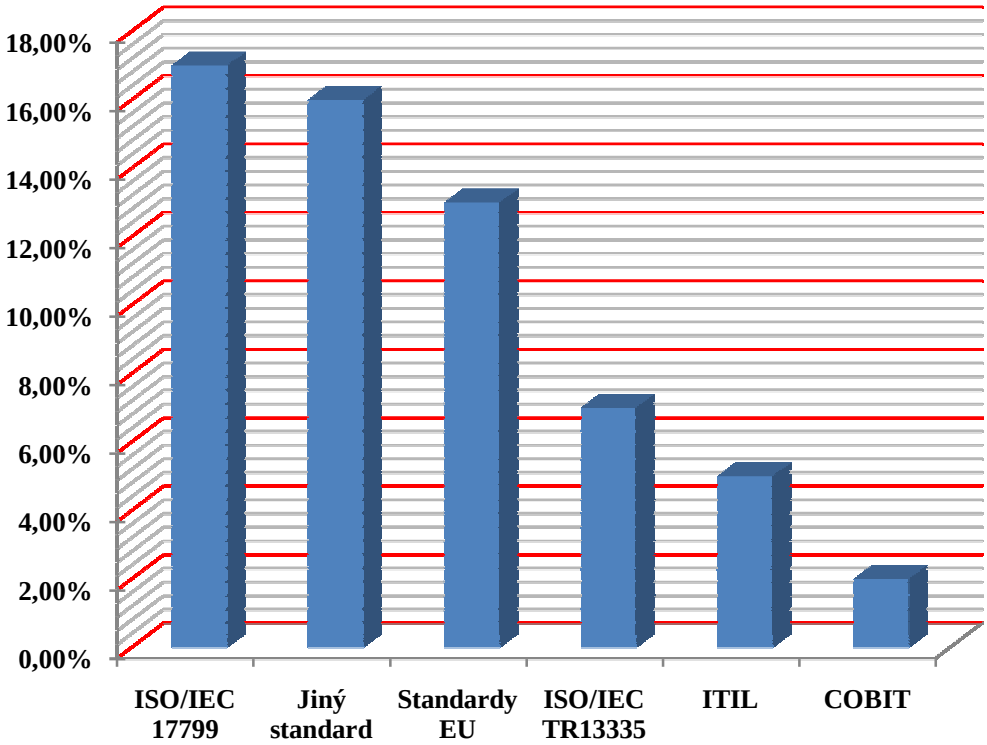
Investice cíleně určené pouze pro bezpečnost IS/IT je velmi problematické identifikovat. Investice do bezpečnosti IS/IT se výrazně prolínají s investicemi do celkové infrastruktury. Poměr investic do bezpečnosti IS/IT dle odpovědí činí v rozmezí 2-6%. Přiměřený poměr dle vyjádření bezpečnostních manažerů IS/IT by měl být cca okolo 10%.

Porovnání s jinými průzkumy

Srovnání organizační struktury bezpečnosti IS/IT kvalitativního průzkumu. Dle (22): "Nejčastějším způsobem organizačního zajištění bezpečnosti je využití útvaru IT/IS, což využívá 78 procent oslovených společností. Dalšími možnostmi jsou například útvar bezpečnosti nebo ekonomický útvar.“. Výstupem kvalitativního průzkumu jsou částečně oddělené útvary bezpečnosti IS/IT.

Dle (22) od průzkumu z roku 1999 počet společností disponujících bezpečnostní politikou vzrostl z 35 procent na současných 48 procent. Dle odpovědí kvalitativního průzkumu společnosti mají formálně definovanou a nejvyšším vedením přijatou bezpečnostní politiky. Přehled využívání konkrétních standardů bezpečnosti IS/IT dle průzkumu (22) se nachází v následujícím grafu.

Dle odpovědí kvalitativního průzkumu společnosti využívají normy a standardy plynoucí z BS 7799, ISO/IEC TR 13335, ITIL, Cobit a CRAMM. Porovnáním kvalitativního průzkumu s (22) společnosti mají zavedeny nejrozšířenější standardy bezpečnosti IS/IT.



Graf 5.2.8 Přehled využívání konkrétních standardů [(7)]

5.3 Analýzy bezpečnostních incidentů v IS/IT

Podstatným aspektem pro management bezpečnosti IS/IT obvykle bývá rozbor bezpečnostních incidentů a událostí v IS/IT. Společnosti samozřejmě z objektivních příčin se snaží o odvrácení medializace těchto negativních událostí, nicméně uvedené případy jsou ponaučením nejen pro odborné spektrum ale i pro odpovědné manažery společností a firem. Na několika případech bych se chtěl subjektivně pokusit o analýzu bezpečnostních incidentů v oblasti IS/IT dle jednotlivých částí:

- Obecné údaje organizace
- Popis incidentu

§ Proč došlo k incidentu?

§ Jakým způsobem se mohlo předejít?

§ Ponaučení

5.3.1 První bezpečnostní incident

První bezpečnostní incident se zabývá problematikou neomezených přístupových práv vývojového programátora a chybějícího kontrolního oddělení a mechanismů auditu a kontroly.

§ Obecné údaje organizace

- § Sídlo v ČR,
- § počet zaměstnanců větší než 1000,
- § komerční organizace finančního charakteru,
- § společnost nepůsobí v IT.

§ Popis incidentu

V popisu incidentu jsem zaměnil název organizace na název BANKA. Hlavní postavou bezpečnostního incidentu byl programátor hlavního účetního systému BANKY. Do BANKY nastoupil před 10 ti lety, získal nesmírné zkušenosti a pověst velkého odborníka a specialisty v oblasti IS/IT. Vzhledem k těmto okolnostem samozřejmě i nesmírnou důvěru. V době před odhalením bezpečnostního incidentu měl na starosti opravy a vychytávání chyb v hlavním účetním systému BANKY. Programátor zjistil, že systém má jednu nepatrnou mezeru, díky níž se z BANKY dají bez povšimnutí odčerpávat peníze. Napoprvé poslal na své soukromé konto sedm milionů. Podařilo se, nikdo na nic nepřišel. Stejný krok zkusil znovu. Tentokrát se zastavil na částce 193 milionů. Peníze, které "tunelem" poslal z BANKY na své účty, pocházely z rezervy, která BANCE kryje ztráty při poklesu měnových kurzů. BANKA si je odečetla jako ztrátu. Programátor dostal strach. Vytunelované peníze byly přece jen velká suma, a tak se je rozhodl alespoň částečně vrátit. Jenže jakkoli si v BANCE nikdo nevšiml, že peníze mizí, náhlý přírůstek milionové částky pozornosti neunikl. Rozjela se kontrola, která na všechno přišla.

§ Proč došlo k incidentu?

- § Neomezená práva programátora,

- chybějící systém pravidelných kontrol a kontrolních mechanismů,
- chybějící kontrolní oddělení.

§ Jakým způsobem se mohlo předejít?

- Omezením práv programátora,
- víceúrovňovým testováním oprav a chyb v účetním systému,
- nasazením kontrolních mechanismů,
- vytvořením kontrolního oddělení.

§ Ponaučení z incidentu

Pro zamezení uvedeného typu incidentu je třeba nastavit procesně i technicky kontrolní mechanismy uvnitř organizace. Navíc kontroly je nutné v čase měnit a přizpůsobovat v souvislosti s rozvojem systému IS/IT případně i se změnou organizační struktury. Na závěr tohoto bezpečnostního incidentu připojuji lidové pořekadlo: „Důvěřuj, ale prověřuj“.

5.3.2 Druhý bezpečnostní incident

Druhý bezpečnostní incident se zabývá problematikou podceněním provozních personálních potřeb pro administraci provozní bezpečnosti IS/IT.

§ Obecné údaje organizace

- Sídlo v ČR,
- počet zaměstnanců větší než 1000,
- komerční organizace,
- společnost nepůsobí v IT.

§ Popis incidentu

V popisu incidentu jsem zaměnil název organizace na název FIRMA. FIRMA vypsala výběrové řízení na dodávku a implementaci bezpečnostních technologií. Konkrétně se jednalo o antivirové a antispamové řešení pro koncové zařízení (počítače, notebooky). Systém byl naimplementován externí společností a předán firmě do provozu. Bohužel při přebírání systému FIRMA zjistila, že

pro provoz nemá dostatečné volné personální a finanční zdroje. Zodpovědnost provozu uvedeného systému předala na již tak více jinými úkoly přetížené infrastrukturní administrátory IS/IT. Během krátké doby byla odhalena u implementovaného bezpečnostního antivirového a antispamového řešení pro koncové zařízení zranitelnost. Výrobce poskytl ihned po zjištění „patch“ pro odstranění zranitelnosti. Bohužel administrátoři vzhledem k jinému vytížení „patch“ neaplikovali na svůj systém. Po půl roce od zveřejnění zranitelnosti došlo k zneužití uvedené zranitelnosti ve FIRMĚ. Výsledkem byla několik dnů přetížená infrastruktura s velmi problematickou funkčností a nedostupností řady zdrojů IS/IT. Ztráty nedostupnosti způsobené tímto incidentem byly pro FIRMU podstatným argumentem pro změnu stanoviska a následné promptní řešení situace.

- **Proč došlo k incidentu?**
  - Podcenění provozních nákladů IS/IT,
  - přetíženost správců,
  - pochybení u manažera bezpečnosti.
- **Jakým způsobem se mohlo předejít?**
  - Zdůvodnění výjimečných potřeb u managementu společnosti,
  - personálním řešením,
  - přenesením činnosti, odpovědnosti a sankcí na externí společnost.
- **Ponaučení z incidentu**

Pro zamezení uvedeného typu incidentu je třeba schopnost manažera bezpečnosti IS/IT přesvědčit management společnosti o preferenci v těchto situací. Tedy uvolnění finančních rezerv pro personální vyřešení situace nebo přenesením činnosti, odpovědnosti a sankcí na externí společnost.

5.3.3 Třetí bezpečnostní incident

Třetí bezpečnostní incident se zabývá problematikou ochranou autorských práv.

- **Obecné údaje organizace**
  - Sídlo v ČR,

- komerční organizace,
- výroba a vývoj.

§ Popis incidentu

V popisu incidentu jsem zaměnil název organizace na název AUTO. AUTO byla společností charakteru více vývojovou a výrobní než obchodní. Do společnosti AUTO vstoupil zahraniční vlastník, který měl několik dalších společností obdobného charakteru v zahraničí. Došlo ke změnám v celkové organizační struktuře AUTO. Společnost AUTO měla v převážné míře dodávat výrobky a komponenty do jiné společnosti vlastněné tímtéž majitelem. Na straně této jiné společnosti pracoval zaměstnanec nákupního oddělení zajišťující nákup výrobků a komponent ze společnosti AUTO. Společnost AUTO investovala do vývoje a výrazným způsobem zinovovala komponenty. Inovované komponenty včetně cen nabídla nákupnímu oddělení. Zpětná odezva z nákupního oddělení byla negativní. Po nějaké době zjistila společnost AUTO, že na trhu se objevily jejich inovované komponenty. Uvedené komponenty měly svá konstrukční specifika, dle kterých nebylo možné, aby byly jiné komponenty plně shodné s jejími. Auto zpřísnilo bezpečnostní režim v IS/IT a to jak procesní tak i technologický. Navíc spustila bezpečnostní monitorovací systém v počítačové síti. Zjištění bylo vcelku překvapivé. Dotyčný pracovník nákupního oddělení zahraniční společnosti byl přistižen, jak vzdáleným přístupem do IS AUTO se snažil získat technickou dokumentaci k dalším komponentům. Důvodem jeho počínání byl osobní zájem o odměny za úspory při nákupu vyrobených komponent. Technickou dokumentaci společnosti AUTO předával jiným konkurenčním zahraničním společnostem s levnější pracovní silou. Cena těchto komponent byla nižší o nezapočítání ceny vývoje a samozřejmě byla ponížena o levnější pracovní sílu.

§ Proč došlo k incidentu?

- Nízké zabezpečení konstrukční dokumentace,
- nedostatečná ochrana proti interním hrozbám,
- Chybějící monitorovací systém,
- Špatný motivační systém uvnitř nadnárodních společností.

§ Jakým způsobem se mohlo předejít?

- Zabezpečením elektronické technické dokumentace,

- nasazením monitorovacího systému,
- zabezpečením proti vnitřním hrozbám,
- změnou motivačního systému.

§ Ponaučení z incidentu

Pro zamezení uvedeného typu incidentu je třeba provést důslednou analýzu rizik a na jejím základě zajistit přiměřeným způsobem bezpečnostní opatření. Podstatným prvkem je také „ON-LINE“ monitoring bezpečnostních událostí.

5.3.4 Čtvrtý bezpečnostní incident

Čtvrtý bezpečnostní incident představuje jiný typ bezpečnostního incidentu. Zabývá se společností poskytující služby v oblasti IS/IT, která kvůli své nedbalosti v této oblasti musela ukončit svou činnost.

§ Obecné údaje organizace

- Sídlo v USA,
- komerční organizace,
- společnost působící v oboru IT.

§ Popis incidentu

V popisu incidentu jsem zaměnil název organizace na název PODNIK. PODNIK byl významným americkým IT kontraktorem v oblasti zdravotnictví. Spravoval a udržoval webové aplikace řady nemocnic v USA. Před krachem byl zasažen několika bezpečnostními incidenty. Dle konzultační společnosti podstatné pro krach byl bezpečnostní incident u zákazníků, jehož výstupem bylo zanedbání ochrany dat téměř 100 tisíc osob. Technickou příčinou údajně dle konzultační společnosti bylo vypnutí firewallu pro transfer dat z jednoho serveru na jiný a jeho následná neaktivace. Data byla nechráněná několik týdnů. Nemocnice následně zrušily kontrakty s uvedenou společností. PODNIK musel ukončit svou činnost.

§ Proč došlo k incidentu?

- Nedbalost a přetíženost správců,
- Kvalifikace a zodpovědnost pracovníků IS/IT.

- **Jakým způsobem se mohlo předejít?**
  - Interní postupy a kontrolními mechanismy pro poskytování kvalifikovaných služeb,
  - školením pracovníků IS/IT,
  - dostatečný personální počet specialistů.
- **Ponaučení z incidentu**

Pro zamezení uvedeného typu incidentu je třeba zavést management jakosti v poskytování IS/IT služeb (postupy a kontrolními mechanismy pro poskytování kvalifikovaných služeb, projektové řízení atd.)

5.4 Vybrané tendence a trendy v oblasti bezpečnosti IS/IT

Kapitola tendence a trendy v oblasti bezpečnosti IS/IT sumarizuje vybrané tendence a trendy zejména v oblasti technologické bezpečnosti IS/IT. Hlavním podkladem pro vypracování tendencí a trendů v oblasti bezpečnosti, zranitelnosti a bezpečnostních hrozeb byla vybrána datová základna nejrozsáhlejší monitorovací sítě Symantec Global Intelligence Networks. (23)

Základní údaje sítě Symantec Global Intelligence Networks:

- 40 000 monitorovacích senzorů,
- senzory sítě umístěny ve více než 180 zemích,
- databáze dokumentující více než 22 000 zranitelných míst,
- zranitelná místa postihují více než 50 000 technologií,
- technologie a systémy více než 8 000 dodavatelů.

Datové výstupy sítě Symantec Global Intelligence Networks jsou aktualizovány formou zpráv Internet Security Threat Report (ISTR) společnosti Symantec, které jsou vydávány v časovém horizontu půl roku. Poslední zpráva shrnovala první pololetí roku 2007. (23) Další použité zdroje jsou doplněním případně potvrzením datové základny společnosti Symantec. (25) (32) (33)

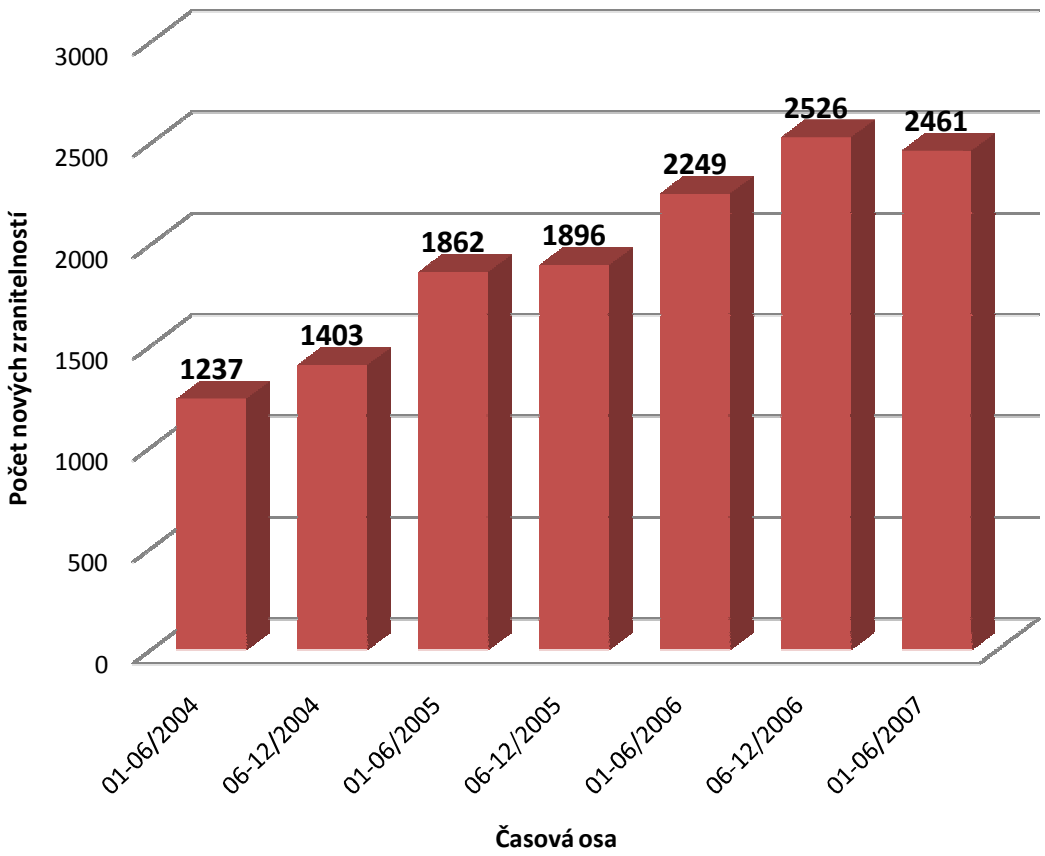
Vzhledem k obsáhlosti, počtu hodnot, metrických veličin a oblastí bezpečnosti IS/IT, které by bylo možné monitorovat a trendově analyzovat, a které není reálné z pohledu rozsahu plně obsáhnout v této disertační práci, zvolil jsem následující reprezentativní výsek trendové oblasti bezpečnosti IS/IT:

- Trendy zranitelnosti systémů IS/IT škodlivými kódy,
- trendy útoků a nové motivace počítačových zločinců,
- trendy nebezpečných kódů a kombinovaných hrozeb,
- trendy v oblasti technologické bezpečnosti IS/IT.

5.4.1 **Trendy zranitelnosti systémů IS/IT škodlivými kódy**

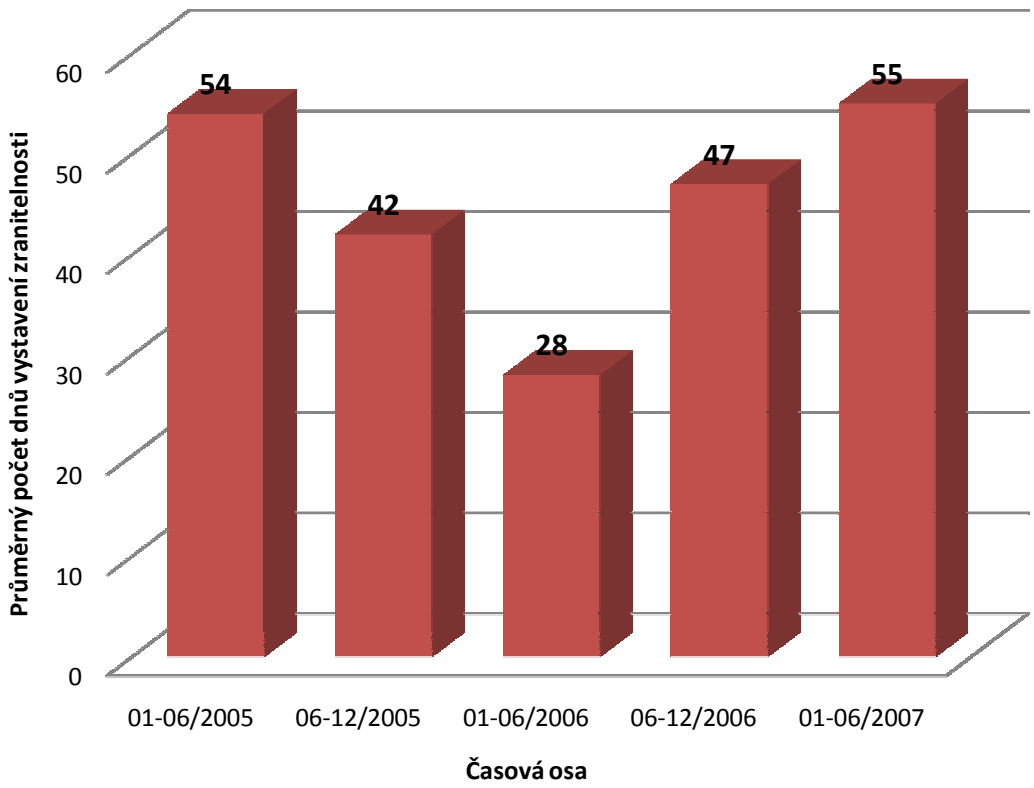
Zranitelnost systému je jedním z podstatných parametrů a vlastností v oblasti bezpečnosti IS/IT. Zranitelnost můžeme definovat jako nedostatek, slabinu nebo stav analyzovaného aktiva (případně subjektu nebo jeho části; v našem případě systému), který může hrozba využít pro uplatnění svého nežádoucího vlivu. Tato veličina je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby. Zranitelnost vznikne všude tam, kde dochází k interakci mezi hrozbou a aktivem. Zjednodušeně hlavními příčinami zranitelností jsou skryté chyby při vytváření nových systémů, nedostatečné odladění, ekonomické aspekty a tlak trhu na výrobce systému.

Graf 5.4.1.1 symbolizuje trendy v oblasti technologické zranitelnosti systémů IS/IT. Od roku 2004 do konce roku 2006 je vidět lineární růst počtu nových zjištěných zranitelností. V prvním pololetí roku 2007 došlo k mírnému snížení počtu nových zjištěných zranitelností systémů. Subjektivně se však domnívám, že trend růstu bude i nadále pokračovat.



Graf 5.4.1.1 Počty nových zjištěných zranitelností
[(23), (24), (25), (26), (27), (28), (29), (30), (31)*]*

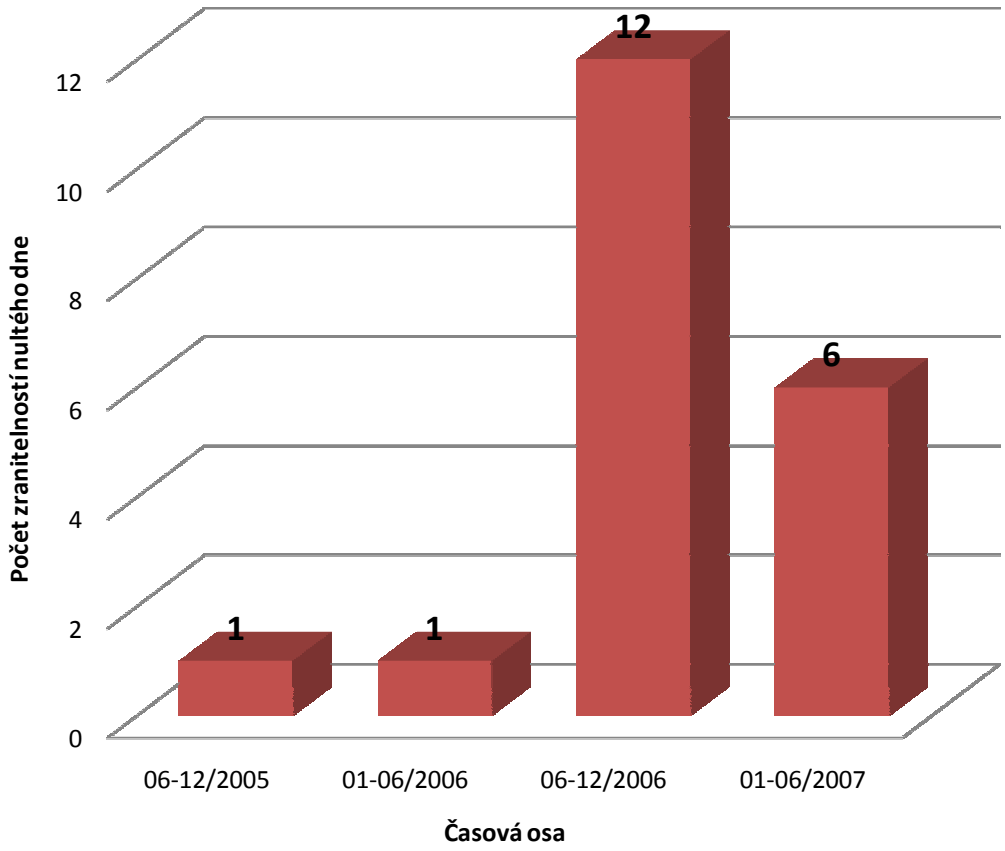
Graf 5.4.1.2 rozkrývá hlouběji problematiku zranitelností systémů IS/IT. V uvedeném grafu jsou uvedeny trendy průměrného počtu dnů vystavení hrozbě zjištěné zranitelnosti systémů IS/IT. Prakticky to znamená, že patch pro odstranění zranitelnosti systému IS/IT, výrobce systému vytvoří a uvede na trh až po jistém časovém období. Nejideálnější situace byla v prvním pololetí roku 2006, kdy průměrná doba bez „záplat“ pro odstranění zjištěné zranitelnosti byla 28 dnů ve sledovaném časovém úseku. Nejhorší situace byla zatím v prvním pololetí roku 2007, kdy průměrná doba bez „záplat“ pro odstranění zjištěné zranitelnosti byla 55 dnů ve sledovaném časovém úseku. Uvedený trend znamená, že výrobci v současných podmínkách nejsou schopni dynamicky reagovat na růstový trend nově zjištěných zranitelností. Tímto dostávají manažery bezpečnosti IS/IT do velmi problematických situací.



Graf 5.4.1.2 Průměrný počet dnů vystavení společností zranitelnosti
[(23), (24), (25), (26), (27), (28), (29), (30), (31)*]*

Novým prvkem v oblasti zranitelností systémů IS/IT se stala definice nultého dne. Zranitelnost nultého dne znamená, že tentýž den zjištěná nová zranitelnost systému IS/IT byla globálně zneužita. To dává novou dimenzi pohledu bezpečnostních manažerů IS/IT na oblast technologické bezpečnosti IS/IT. Z neformálních rozhovorů s manažery bezpečnosti IS/IT vyplynulo, že danou problematiku v nynějších podmínkách nejsou schopni plnohodnotně řešit. Manažeři bezpečnosti IS/IT o problematice nultého dne ví a prognózují, že by mohlo jít o další budoucí směr a negativní trend v oblasti bezpečnosti IS/IT.

V grafu 5.4.1.3 je zobrazen aktuální stav a trend od druhé poloviny roku 2005 až po první pololetí 2007. Zatím nejvíce zranitelností nultého dne zachycuje druhé pololetí roku 2006 a to celkem 12. V první polovině roku 2007 zatím 6 prokazatelných zranitelností nultého dne. Celkem zarážející je i struktura zranitelností nultého dne. Ve zranitelnostech nultého dne figurují i výrobci bezpečnostních řešení IS/IT.

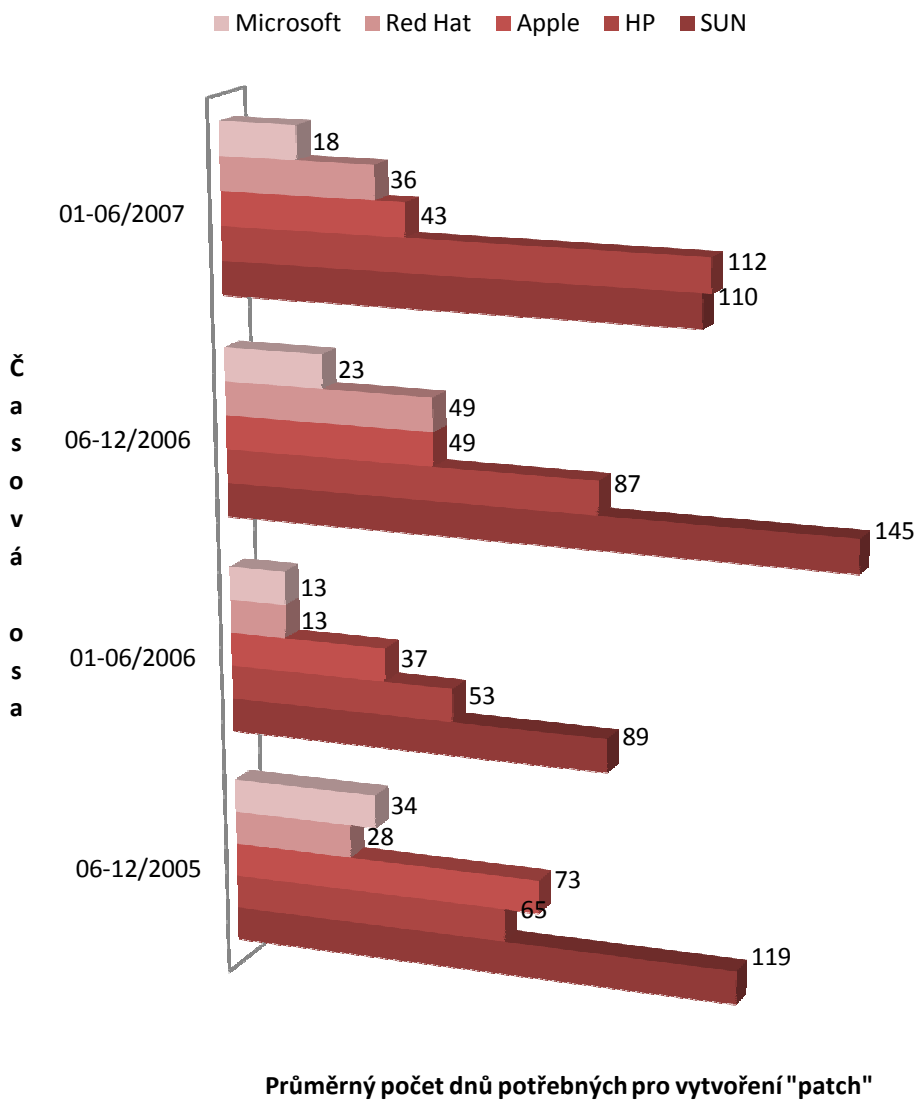


Graf 5.4.1.3 Počet zranitelností nultého dne
[(23), (24), (25), (26), (27), (28), (29), (30), (31)*]*

Důležitým prvkem v oblasti technologické bezpečnosti jsou koncová zařízení: Pracovní stanice, notebooky, přenosná mobilní zařízení a další. Koncová zařízení jsou cílem řady napadení jak cíleně tak i náhodně. Pro doložení trendů složité problematiky tzv. záplatování systémů, přikládám vybrané operační systémy a průměrný počet dnů potřebný k vytvoření záplaty na odstranění zjištěné zranitelnosti systému IS/IT. Trendově jsou zpracovány následující operační systémy:

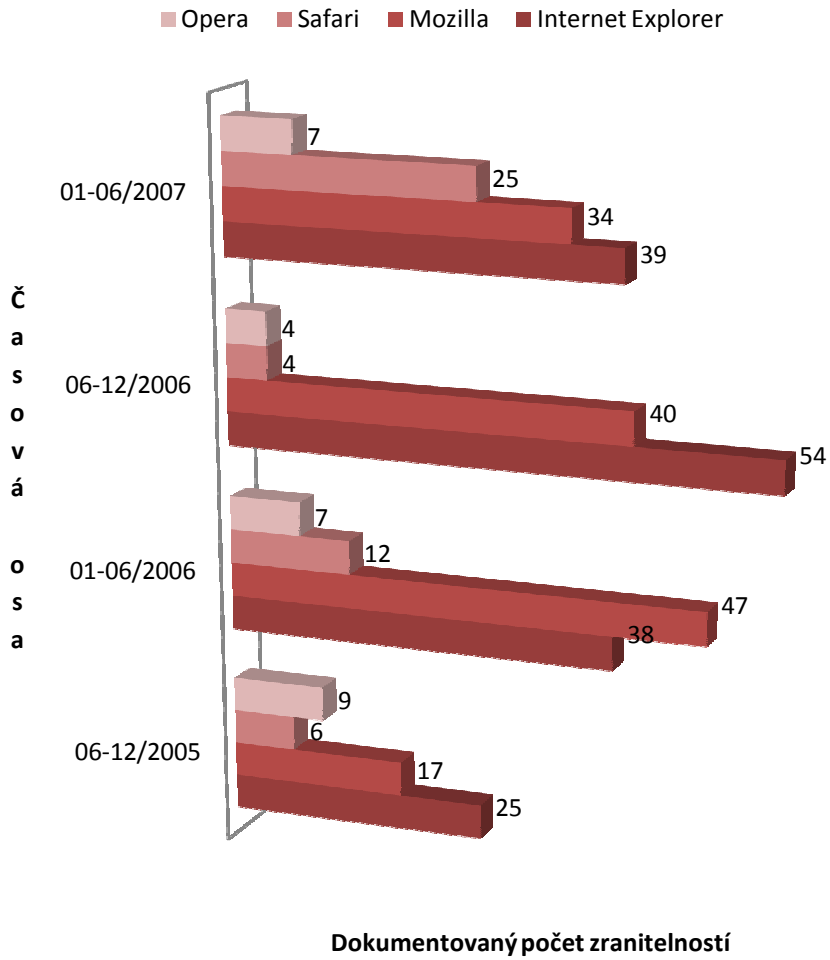
- Microsoft
- Red Hat
- Apple
- HP
- SUN

Zatím nejdelší průměrný čas potřebný k zajištění záplaty představuje operační systém SUN. Překvapivě dobře v uvedeném srovnání si vedou operační systémy Microsoft.



Graf 5.4.1.4 Průměrný počet dnů pro vytvoření záplat pro jednotlivé operační systémy [(23), (24), (25), (26), (27), (28), (29), (30), (31)*]*

Významnou roli mají v oblasti bezpečnosti IS/IT webové prohlížeče. Webové prohlížeče jsou jednou z nejčastěji používaných aplikačních částí. Mohou sloužit jako terminály pro aplikace, poštovní služby atd. V grafu 5.4.1.5 je zobrazen aktuální stav a trend od druhé poloviny roku 2005 až po první pololetí 2007. Nejvíce zjištěných nových zranitelností představuje prohlížeč Microsoft Internet Explorer, nejméně Opera. Uvedený trend počtu zjištěných zranitelností souvisí zejména s počtem požívaných instalací příslušného prohlížeče.



Graf 5.4.1.5 Dokumentovaný počet zranitelností prohlížečů
[(23), (24), (25), (26), (27), (28), (29), (30), (31)*]*

5.4.2 Trendy útoků a nové motivace počítačových zločinců

V oblasti trendů útoků dle (23) dochází během několika let k velmi významným změnám. Hackeři zvyšují úspěšnost nebezpečných činností pomocí nových taktik založených na principech obchodních strategií. Počítačoví zločinci se při vývoji, distribuci a použití nebezpečného kódu a služeb stále více profesionalizují a dokonce komercionalizují. Počítačová zločinnost je nadále motivována finančním ziskem a počítačoví zločinci nyní při provádění nebezpečných činností využívají profesionálnější metody útoku, nástroje a strategie. Řada počítačových zločinců pochopila své role a zůstává u části technické a technologické tzn. zcizení dat, přístupových práv, identity, získání čísla účtů a kódů atd. Obchodní rovinu zajišťují další obchodní specialisté, kteří na trhu podzemní ekonomiky hledají obchodní protistranu, která je ochotna za získané informace

a data příslušně zaplatit. Dle Arthura Wonga[1]: „Hrozby z Internetu a nebezpečné činnosti, které v současné době sledujeme, ukazují, že hackeři pozvedají tento trend na vyšší úroveň a počítačová zločinnost se stává jejich povoláním. K úspěšnému dosažení tohoto cíle používají praktiky známé z obchodní činnosti.“

Původní motivace hackerů:

- Útoky jsou prováděny s cílem proslavit se a vyniknout,
- útoky jsou viditelné a plošné,
- útoky jsou destruktivní a zpravidla viditelné.

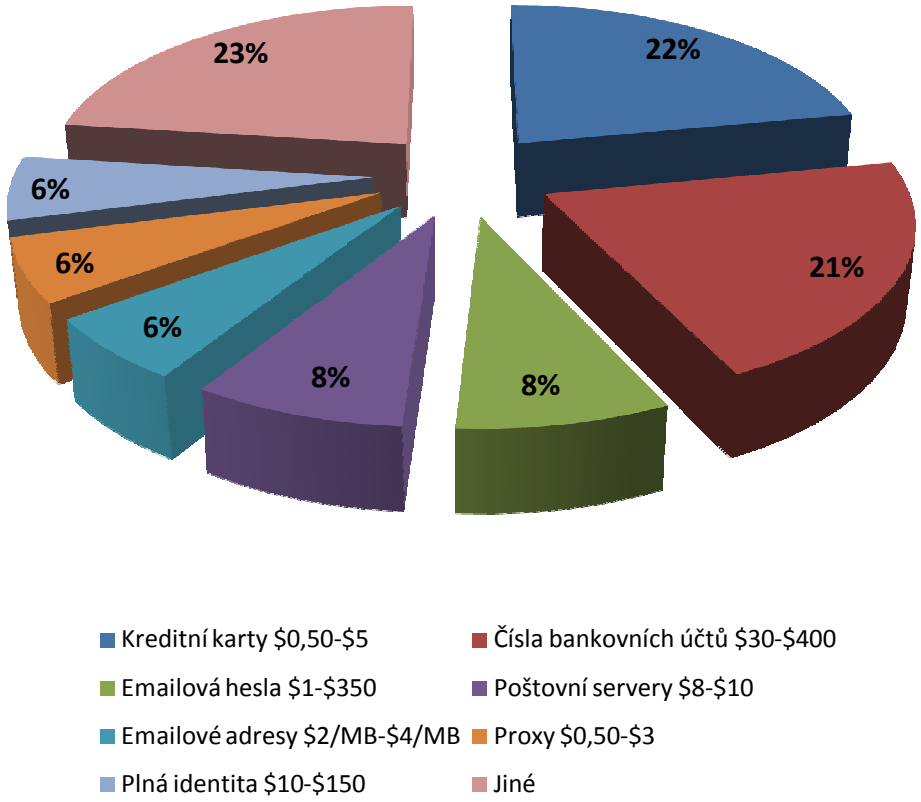
Nové motivace hackerů (zejména období po roce 2006):

- Útoky jsou navrženy s cílem finančního obohacení,
- útoky jsou tiché a vysoce cílené,
- útoky vykrádají data,
- dopad není hned jasný.

Dle (23) bylo zjištěno zvýšení počtu počítačových zločinců, kteří při provádění nebezpečných útoků využívají důmyslné sady nástrojů. Příkladem této strategie byla profesionálně vyvinutá sada nástrojů prodávaná v podzemní ekonomice. Útočníci mohli nainstalovat zakoupenou kolekci softwarových součástí a s jejich pomocí nainstalovat nebezpečný kód do tisíců počítačů po celém světě. Úspěšnost útoku mohli sledovat pomocí různých metrik na online konzole pro řízení a správu. Uvedená sada je také příkladem koordinovaného útoku využívající kombinaci nebezpečných činností.

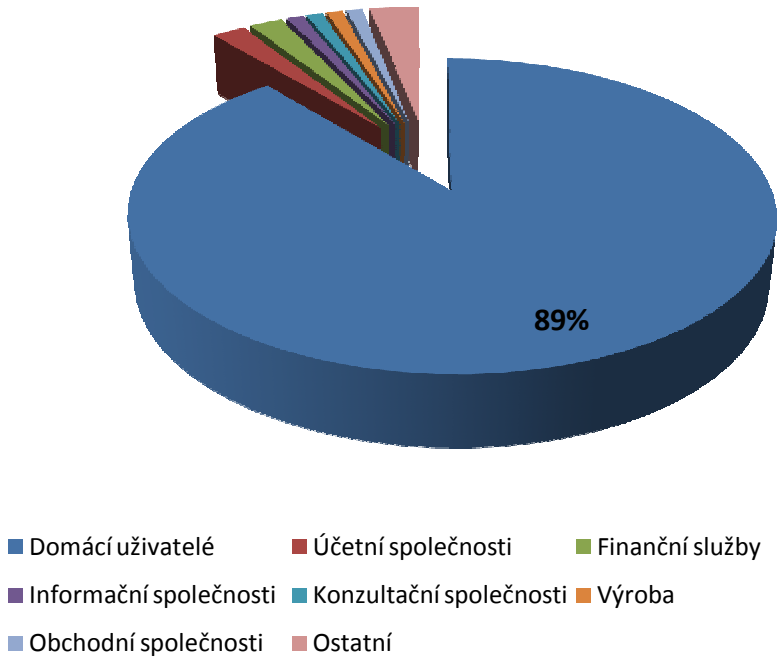
Graf 5.4.2.1 dokumentuje nabízené komodity na serverech podzemní ekonomiky včetně cenové nabídky za 1 ks tzv. zboží. Nejčastěji nabízenou komoditou na serverech podzemní ekonomiky byly kreditní karty, na které připadalo 22 % všech nabídek. Na druhém místě byly s těsným odstupem bankovní účty s 21 %.

[1] *Senior vice president, Symantec Security Response and Managed Services*



Graf 5.4.2.1 Nabízené komodity na serverech podzemní ekonomiky včetně cenové nabídky
[(23)*]*

Oblast aktuálního trendu směřování útoků dle sektoru je uvedena v grafu 5.4.2.2. Dle uvedeného grafu plyne, že cílem útoků jsou především domácí uživatelé a to celkem v počtu 89%. Útoky na domácí uživatele subjektivně mají však sekundární význam. Primárně je získáni identity domácích uživatelů a s její pomocí získání přístupu k firemním datovým zdrojům. Řada domácích uživatelů se připojuje k firemním sítím z domu prostřednictvím vzdáleného připojení, zabezpečené linky případně k poštovnímu serveru. Tímto způsobem se nahrávají příležitosti pro útočníky.

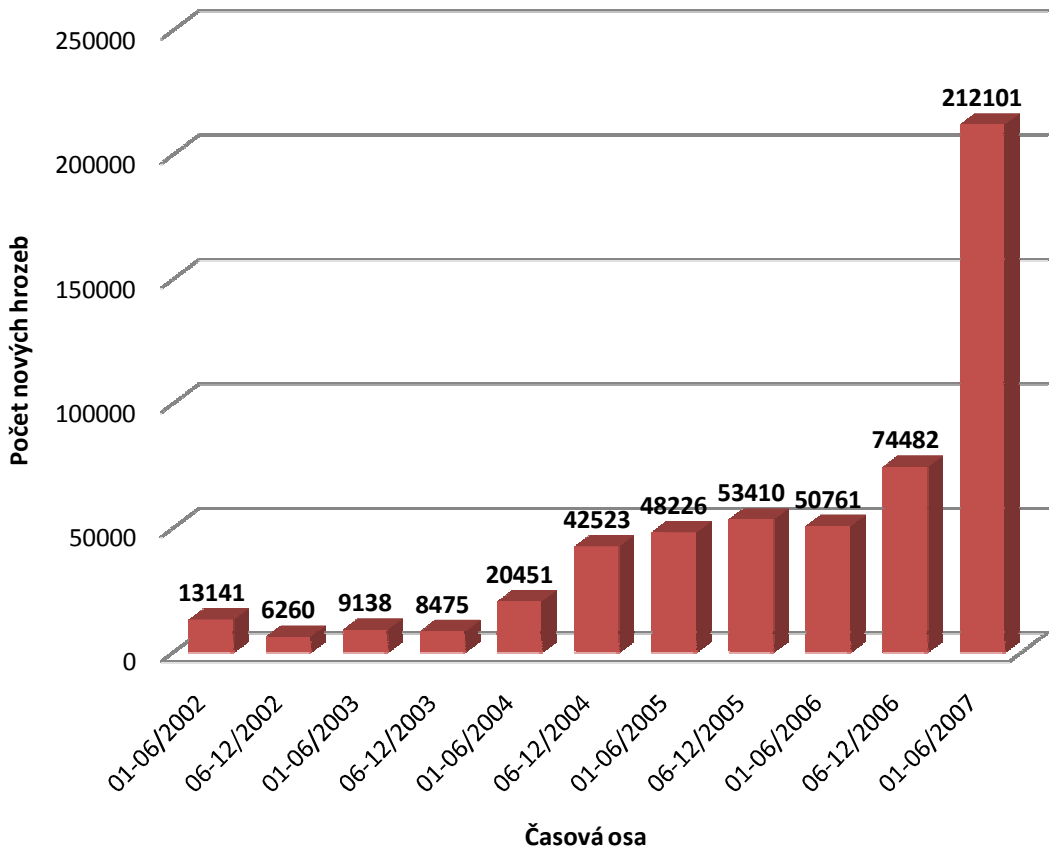


Graf 5.4.2.2 Demografie útoků dle sektorů
[(23)*]*

5.4.3 **Trendy nebezpečných kódů a kombinovaných hrozeb**

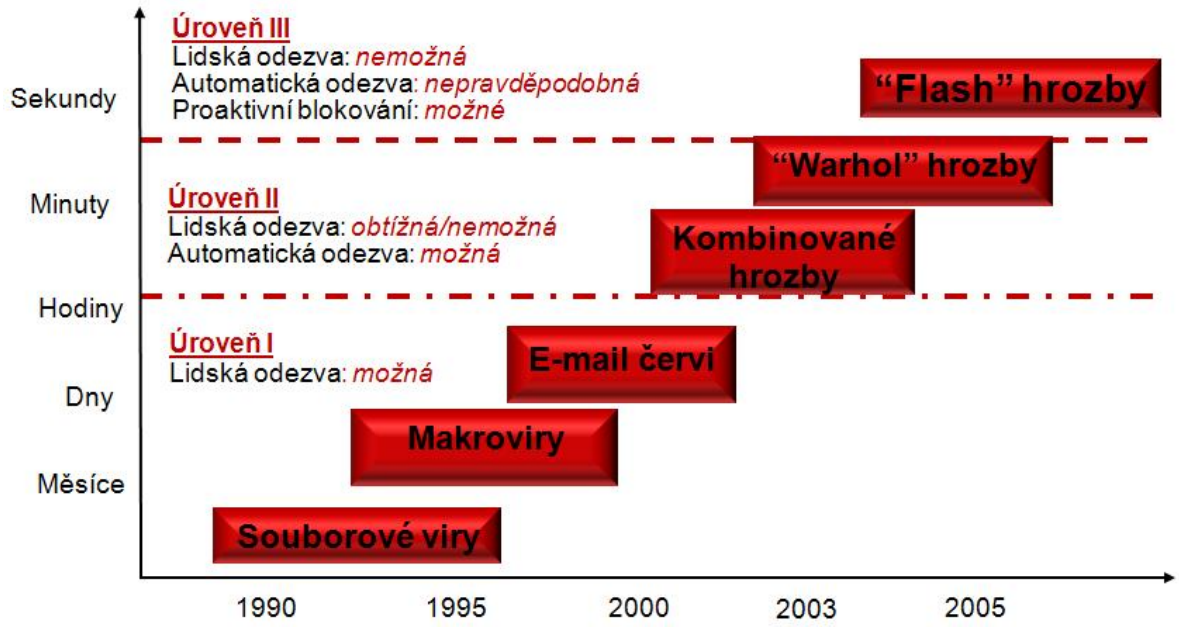
Nebezpečné kódy jsou škodlivé programové kódy, jejichž prostřednictvím může dojít až ke krádeži identity a kompromitace počítačového zařízení včetně zneužití uživatelských dat.

V grafu 5.4.3.1 je zobrazen aktuální stav a trend nově zjištěných nebezpečných hrozeb od první poloviny roku 2002 až po první pololetí 2007. Překvapivým zjištěním je obrovský nárůst škodlivých kódů v prvním polovině roku 2007. Ten dosahuje počtu 212101 a představuje nárůst proti předchozímu pololetí roku 2006 o 186%. Situace dle počtu nově zjištěných hrozeb od druhého pololetí 2002 do konce roku 2003 byla stabilizovaná. Od konce roku 2004 do prvního pololetí 2006 mírně oscilovala okolo počtu 50000 nově zjištěných hrozeb. Tendence výrazného růstu nově zjištěných hrozeb naznačilo druhé pololetí roku 2006.



Graf 5.4.3.1 Počet nových hrozeb škodlivých kódů
[(23), (24), (25), (26), (27), (28), (29), (30), (31)*]*

Trendy v oblasti typů generačního vývoje škodlivých kódů včetně vazby na reakční dobu jsou uvedeny v grafu 5.4.3.2. V úrovni I. jsou uvedeny škodlivé kódy typu: souborové viry, makroviry a e-mail červi. U této úrovně byl ještě lidský zásah možný. U úrovně II. kombinovaných hrozeb a typu „Warhol“ hrozeb byl lidský zásah téměř nemožný, bylo nutné řešit formou automatických odezev. U úrovně III je možné již jen proaktivní blokování.



Graf 5.4.3.2 Trend bezpečnostních hrozeb škodlivých kódů
[Vlastní zpracování]

5.4.4 Trendy v oblasti technologické bezpečnosti IS/IT

V oblasti trendů technologické bezpečnosti IS/IT bych chtěl poukázat na následující aktuální vybrané tendence a trendy:

- Proaktivní bezpečnost IS/IT,
- víceúrovňové a kombinované ochrany bezpečnosti IS/IT,
- dynamické kontroly přístupu bezpečnosti IS/IT k datovým zdrojům,
- nové technologie pro „patch".

Proaktivní bezpečnost IS/IT

Proaktivní bezpečnost IS/IT je aktuálním trendem v oblasti bezpečnosti IS/IT. Proaktivní bezpečnost IS/IT znamená proaktivní přístup k řešení otázky bezpečnosti IS/IT. Cílem proaktivní bezpečnosti je proaktivně spravovat hrozby, slabiny a incidenty v oblasti IS/IT a minimalizovat tak potenciální dopady na společnosti. V kontrastu s reaktivními mechanismy, které se pokoušejí zdolat útoky a incidenty až v okamžicích, kdy už zasáhly infrastrukturu, proaktivní správa bezpečnosti IS/IT přidává metody, technologie a služby, které se soustřeďují na nalezení a ošetření slabin již před útokem. Zjednodušeně systémy proaktivní bezpečnosti IS/IT pomáhá zesílit a zocelit odolnost IS/IT. Část prvků technologií proaktivní bezpečnosti IS/IT je uvedena v části kapitoly přiměřené

technologické bezpečnosti IS/IT. Cílem disertační práce nebyl detailní popis a identifikace technologických prvků proaktivní bezpečnosti IS/IT.

Víceúrovňové a kombinované ochrany bezpečnosti IS/IT

Dlouhodobým trendem v oblasti technologické bezpečnosti IS/IT je aplikace víceúrovňové a kombinované ochrany bezpečnosti IS/IT. Víceúrovňovou a kombinovanou ochranu bezpečnosti IS/IT je možné chápat jako určitou specifickou podmnožinu systémů proaktivní bezpečnosti IS/IT. Podstatou víceúrovňové a kombinované ochrany bezpečnosti IS/IT je nasazování více typů, druhů a technologických úrovní vzájemně provázaných a kooperujících systémů bezpečnosti IS/IT. V případě nedostatečné identifikace bezpečnostní hrozby nebo výpadku určité úrovně technologického systému bezpečnosti IS/IT přebírá roli jiný systém bezpečnosti IS/IT s jinou úrovní a podrobností.

Dynamické kontroly přístupu bezpečnosti IS/IT k datovým zdrojům

Trendem bezpečnosti IS/IT v několika posledních letech se stala dynamická kontrola přístupu bezpečnosti IS/IT k datovým zdrojům. Dynamické kontroly přístupu bezpečnosti IS/IT k datovým zdrojům je možné také chápat jako určitou specifickou podmnožinu systémů proaktivní bezpečnosti IS/IT. Podstatou dynamické kontroly přístupu bezpečnosti IS/IT je dynamické přidělování úrovní přístupových práv za určitých specifických podmínek a stanovování procesních činností stavů.

Stanovování úrovní přístupu k datovým zdrojům podle hlavních kritérií:

- Kdo žádá o přístup (identifikace uživatele),
- kde žádá o přístup (identifikace lokality),
- kdy žádá o přístup (identifikace času),
- s jakým zařízením žádá o přístup (identifikace zařízení).

Podle uvedených kritérií je dynamicky přiřazována úroveň přístupových práv. Například u zařízení, které nesplňuje při přihlašování v danou chvíli bezpečnostní firemní standardy, bude postupováno dle bezpečnostních směrnic organizace.

Nové technologie pro „patch“

Velkým problémem pro společnosti z pohledu zajištění bezpečnosti IS/IT je problematika „patch“ neboli tzv. záplatování zranitelností systémů IS/IT. V letošním roce se objevily první impulsy naznačující možnosti řešení. Principem těchto nových technologií je nepřetržité monitorování a sledování chování sys-

tému ve standardním režimu, na jehož základě dochází k přidělování tzv. skórování systému. Dle úrovně skórování systému IS/IT je pak možné ihned v zárodku rozpoznat a identifikovat nebezpečné a škodlivé pokusy a následně jim zabránit, i přesto, že systém nemá aplikovanou příslušnou záplatu nebo případně výrobce systému ji ještě nemá.

5.4.5 Sumarizace vybraných trendů v oblasti bezpečnosti IS/IT

Sumarizace vybraných trendů reprezentuje následující výsek trendové oblasti bezpečnosti IS/IT:

- Trendy zranitelnosti systémů IS/IT škodlivými kódy,
- trendy útoků a nové motivace počítačových zločinců,
- trendy nebezpečných kódů a kombinovaných hrozeb,
- trendy v oblasti technologické bezpečnosti IS/IT.

Trendy zranitelnosti systémů IS/IT škodlivými kódy

Zranitelnost systému je jedním z podstatných parametrů a vlastností v oblasti bezpečnosti IS/IT. Zjednodušeně hlavními příčinami zranitelností jsou skryté chyby při vytváření nových systémů, nedostatečné odladění, ekonomické aspekty a tlak trhu na výrobce systému.

Od roku 2004 do konce roku 2006 lineárně roste počet nových zjištěných zranitelností.

Podstatnou rolí v oblasti zranitelnosti hraje počet dnů, kdy nová zranitelnost nemá záplatu na odstranění této zranitelnosti. Nejideálnější situace byla v prvním pololetí roku 2006, kdy průměrná doba bez „záplat“ pro odstranění zjištěné zranitelnosti byla 28 dnů ve sledovaném časovém úseku. Nejhorší situace byla zatím v prvním pololetí roku 2007, kdy průměrná doba bez „záplat“ pro odstranění zjištěné zranitelnosti byla 55 dnů ve sledovaném časovém úseku. Uvedený trend znamená, že výrobci v současných podmínkách nejsou schopni dynamicky reagovat na růstový trend nově zjištěných zranitelností. Tímto dostávají manažery bezpečnosti IS/IT do velmi problematických situací.

Novým prvkem v oblasti zranitelností systémů IS/IT se stala definice nultého dne. Zranitelnost nultého dne znamená, že tentýž den zjištěná nová zranitelnost systému IS/IT byla globálně zneužita. To dává novou dimenzi pohledu bezpečnostních manažerů IS/IT na oblast technologické bezpečnosti IS/IT.

Důležitým prvkem v oblasti technologické bezpečnosti jsou koncová zařízení a jejich operační systémy. Zatím nejdelší průměrný čas potřebný k zajištění záplaty představuje operační systém SUN. Překvapivě dobře v uvedeném srovnání

Významnou roli mají v oblasti bezpečnosti IS/IT webové prohlížeče. Nejvíce zjištěných nových zranitelností představuje prohlížeč Microsoft Internet Explorer, nejméně Opera. Uvedený trend počtu zjištěných zranitelností souvisí zejména s počtem požívaných instalací příslušného prohlížeče.

Trendy útoků a nové motivace počítačových zločinců

V oblasti trendů útoků dle (23) dochází během několika let k velmi významným změnám. Hackeři zvyšují úspěšnost nebezpečných činností pomocí nových taktik založených na principech obchodních strategií. Počítačoví zločinci se při vývoji, distribuci a použití nebezpečného kódu a služeb stále více profesionalizují a dokonce komercionalizují. Počítačová zločinnost je nadále motivována finančním ziskem a počítačoví zločinci nyní při provádění nebezpečných činností využívají profesionálnější metody útoku, nástroje a strategie.

Nejčastěji nabízenou komoditou na serverech podzemní ekonomiky byly kreditní karty, na které připadalo 22 % všech nabídek. Na druhém místě byly s těsným odstupem bankovní účty s 21 %.

Cílem útoků jsou především domácí uživatelé a to celkem v počtu 89%. Útoky na domácí uživatele subjektivně mají však sekundární význam. Primárně je získáni identity domácích uživatelů a s její pomocí získání přístupu k firemním datovým zdrojům.

Trendy nebezpečných kódů a kombinovaných hrozeb

Nebezpečné kódy jsou škodlivé programové kódy, jejichž prostřednictvím může dojít až ke krádeži identity a kompromitace počítačového zařízení včetně zneužití uživatelských dat.

Překvapivým zjištěním je obrovský nárůst škodlivých kódů v prvním pololetí roku 2007. Ten dosahuje počtu 212101 a představuje nárůst proti předchozímu pololetí roku 2006 o 186%.

Trendy v oblasti technologické bezpečnosti IS/IT

V oblasti trendů technologické bezpečnosti IS/IT byly zvoleny následující aktuální vybrané tendence a trendy:

- Proaktivní bezpečnost IS/IT,
- víceúrovňové a kombinované ochrany bezpečnosti IS/IT,

- § dynamické kontroly přístupu bezpečnosti IS/IT k datovým zdrojům,
- § nové technologie pro patch.

a) Proaktivní bezpečnost IS/IT

Proaktivní bezpečnost IS/IT je aktuálním trendem v oblasti bezpečnosti IS/IT. Cílem proaktivní bezpečnosti je proaktivně spravovat hrozby, slabiny a incidenty v oblasti IS/IT a minimalizovat tak potenciální dopady na společnosti. V kontrastu s reaktivními mechanismy, které se pokoušejí zdolat útoky a incidenty až v okamžicích, kdy už zasáhly infrastrukturu, proaktivní správa bezpečnosti IS/IT přidává metody, technologie a služby, které se soustřeďují na nalezení a ošetření slabin již před útokem.

b) Víceúrovňové a kombinované ochrany bezpečnosti IS/IT

Dlouhodobým trendem v oblasti technologické bezpečnosti IS/IT je aplikace víceúrovňové a kombinované ochrany bezpečnosti IS/IT. Víceúrovňovou a kombinovanou ochranu bezpečnosti IS/IT je možné chápat jako určitou specifickou podmnožinu systémů proaktivní bezpečnosti IS/IT. Podstatou víceúrovňové a kombinované ochrany bezpečnosti IS/IT je nasazování více typů, druhů a technologických úrovní vzájemně provázaných a kooperujících systémů bezpečnosti IS/IT.

c) Dynamické kontroly přístupu bezpečnosti IS/IT k datovým zdrojům

Trendem bezpečnosti IS/IT v několika posledních letech se stala dynamická kontrola přístupu bezpečnosti IS/IT k datovým zdrojům. Dynamické kontroly přístupu bezpečnosti IS/IT k datovým zdrojům je možné také chápat jako určitou specifickou podmnožinu systémů proaktivní bezpečnosti IS/IT. Podstatou dynamické kontroly přístupu bezpečnosti IS/IT je dynamické přidělování úrovní přístupových práv za určitých specifických podmínek a stanovování procesních činností stavů.

d) Nové technologie pro patch

Velkým problémem pro společnosti z pohledu zajištění bezpečnosti IS/IT je problematika patch neboli tzv. záplatování zranitelností systémů IS/IT. Principem těchto nových technologií je nepřetržité monitorování a sledování chování systému ve standardním režimu, na jehož základě dochází k přidělování tzv. skórování systému. Dle úrovně skórování systému IS/IT je pak možné ihned v zárodku rozpoznat a identifikovat nebezpečné a škodlivé pokusy a následně

jim zabránit, i přesto, že systém nemá aplikovanou příslušnou záplatu nebo případně výrobce systému ji ještě nemá.

5.5 Mikroekonomická modelace vlivu bezpečnosti IS/IT

V této kapitole bych chtěl za určitých hypotetických předpokladů ukázat modelací vliv bezpečnostních faktorů IS/IT na mikroekonomické aspekty menších a středních firem.

5.5.1 Celkové, mezní a průměrné příjmy v nedokonalé konkurenci

Společnosti vyrábí zejména v podmínkách, kdy je některý z rysů dokonalé konkurence porušen, proto v mikroekonomických analýzách předpokládám podmínky nedokonalé konkurence.

Dle (32) hlavním rysem nedokonalé konkurence je, že firma vyrábí identifikovatelný produkt, u kterého může stanovit cenu. Míra volnosti a ovlivňování ceny závisí především na formě konkurence. Za hlavní příčiny směřující ke vzniku nedokonalé konkurence jsou zejména faktory: Nákladové podmínky, bariéry konkurence a ostatní. Nákladové podmínky vedou ke vzniku nedokonalé konkurence v podobě úspor z velkého rozsahu výroby. Při výrobě velkého objemu produkce se náklady rozpočítávají na větší množství výrobků, takže průměrné náklady s růstem výroby klesají, což samozřejmě vede k potlačení slabších konkurentů ze specifikovaného trhu.

K ostatním faktorům směřující k nedokonalosti trhu jsou:

- nedostatečné informace tržních subjektů
- zásahy státu
- kartelové dohody
- a další

K analýze jsem navrhl faktor tzv. nedostatečné informace tržních subjektů. Ztráta, získání (zcizení informací, získání informací náhodným způsobem, ztráta informací) nebo standardní informovanost může mít globálně firmu ovlivnit.

Předpokládejme hypoteticky firmu, která bude s rostoucím objemem produkce snižovat cenu z 10 jednotek Kč na 1 jednotku Kč. Zaveďme $f(k\,\mathrm{inf})$ s následujícími konstantními hodnotami:

$f(k\,\mathrm{inf}) = 0{,}9$ *znamená, že společnost utrpěla konstantní informační ztrátu 10%,*

$f(k\,\mathrm{inf}) = 1$ *znamená, že společnost má standardní znalosti,*

$f(k\,\mathrm{inf}) = 1{,}1$ *znamená, že společnost získala konstantní informace v rozsahu 10% navíc.*

Celkový příjem firmy (TR):

$$TR = P \cdot Q \cdot f(k\,\mathrm{inf}) \tag{5.5.1.1}$$

Průměrný příjem firmy (AR):

$$AR = \frac{TR}{Q} = \frac{P \cdot Q \cdot f(k\,\mathrm{inf})}{Q} = P \cdot f(k\,\mathrm{inf}) \tag{5.5.1.2}$$

Mezní příjem firmy (MR):

$$MR = \frac{\Delta TR}{\Delta Q} \tag{5.5.1.3}$$

Tab. 5.5.1.1 Celkový příjem hypotetické firmy v nedokonalé konkurenci [Vlastní zpracování]

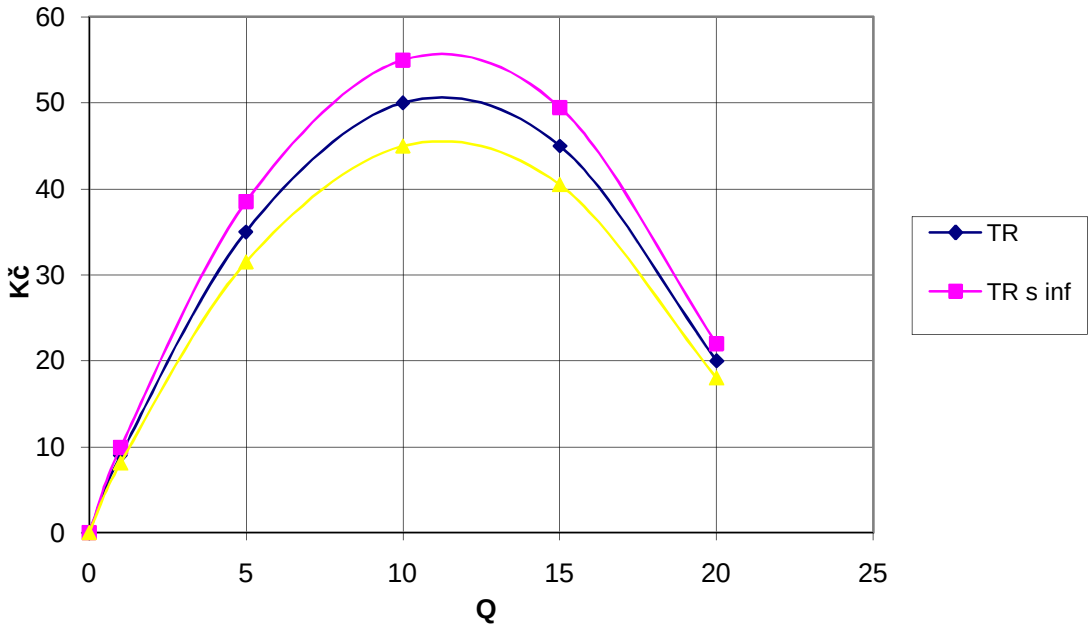
Q	P	TR	TRsinf	TRbezinf
0	10	0	0	0
1	9	9	9,9	8,1
5	7	35	38,5	31,5
10	5	50	55	45
15	3	45	49,5	40,5
20	1	20	22	18

kde pro:

TR s hodnotou f (Kinf)=1

TRsinf s hodnotou f (Kinf)=1,1

TRbezinf s hodnotou f (Kinf)=0,9



Graf 5.5.1.1 Celkový příjem firmy hypotetické firmy v nedokonalé konkurenci [Vlastní zpracování]

Z grafu 5.5.1.1 plyne, že vývoj TR může být s rostoucím Q různý. Za předpokladu lineární poptávkové funkce TR nejprve roste a pak od cca Q=11,5 klesá. Grafickým vyjádřením je konkávní křivka TR, která závisí na elasticitě poptávky:

- elastická poptávka pro Q=<0;11,5>, procentní růst prodaného Q je vyšší než procentní pokles P, TR roste.
- jednotková elastická poptávka pro Q=;11,5, procentní růst prodaného Q je stejný jako procentní pokles P
- neelastická poptávka pro Q>11,5, procentní růst prodaného Q je menší než procentní pokles P, TR klesá.

Při porovnání jednotlivých funkcí TR, TRsinf a TRbezinf samozřejmě plyne, že maximální celkový hypotetický příjem dosahuje TRsinf, nejmenší TRbezinf. Tedy hypoteticky při funkci $f(k\,\text{inf})$ s konstantní hodnotou je logicky výhodné mít informační výhodu. Ještě zajímavější to může být pro společnost v případě nekonstantní hodnoty Kinf například s možností posunutí jednotkové elastické poptávky.

Tab. 5.5.1.2 Mezní a průměrný příjem hypotetické firmy v nedokonalé konkurenci [Vlastní zpracování]

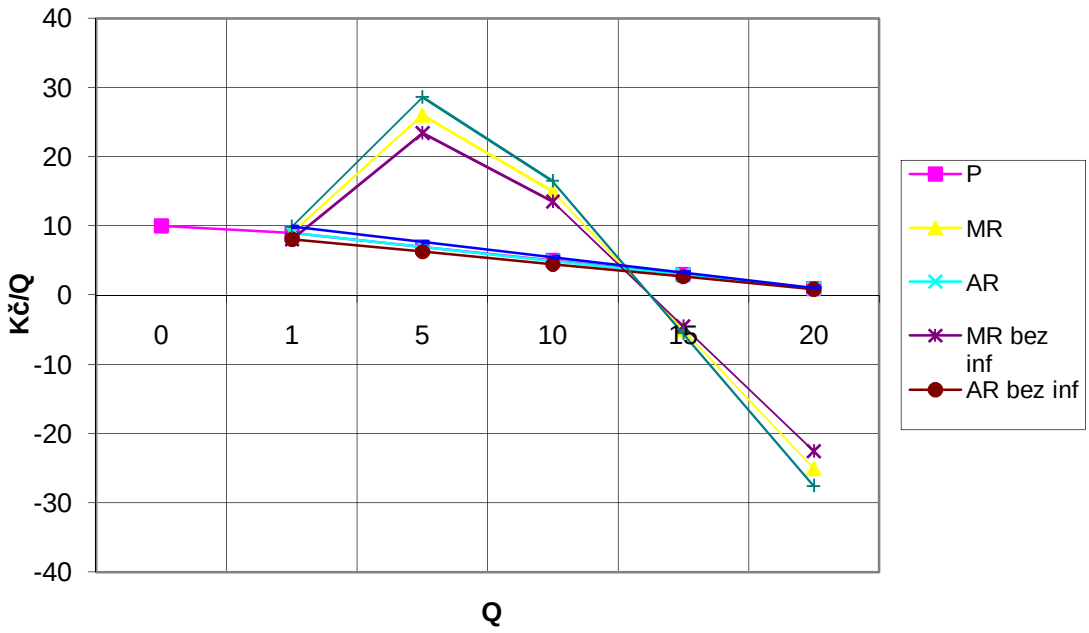
Q	**P**	**MR**	**AR**	**MR bezinf**	**AR bezinf**	**MR sinf**	**AR sinf**
0	10						
1	9	9	9	8,1	8,1	9,9	9,9
5	7	26	7	23,4	6,3	28,6	7,7
10	5	15	5	13,5	4,5	16,5	5,5
15	3	-5	3	-4,5	2,7	-5,5	3,3
20	1	-25	1	-22,5	0,9	-27,5	1,1

kde pro:

MR, AR s hodnotou f (Kinf)=1

MRsinf, ARsinf s hodnotou f (Kinf)=1,1

MRbezinf, ARbezinf s hodnotou f (Kinf)=0,9



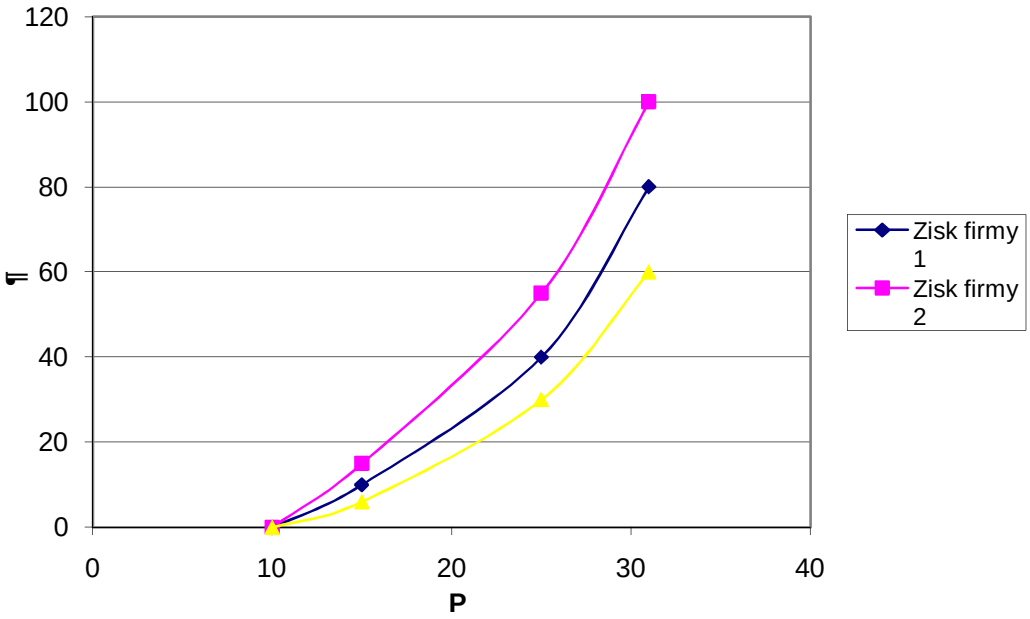
Graf 5.5.1.2 Mezní a průměrný příjem hypotetické firmy v nedokonalé konkurenci [Vlastní zpracování]

Z grafu 5.5.1.2 plyne, že za zjednodušeného předpokladu lineární poptávkové funkce, je grafickým vyjádřením AR křivka se zápornou směrnicí. Porovnáním AR, ARsinf a ARbezinf, opět plyne, že průměrný celkový hypotetický příjem dosahuje společnost s informační výhodou. Uvedená fakta platí také pro srovnání MR, MRsinf a MRbezinf.

5.5.2 **Zisk a výrobní náklady**

Funkce zisku je funkcí cen výrobních faktorů a ceny finální produkce. Funkci můžeme zapsat v následujícím tvaru:

$$\Pi = f(w, r, P) \qquad (5.5.2.1)$$



Graf 5.5.2 Funkce zisku v závislosti na P
[Vlastní zpracování]

Firma maximalizující zisk podřizuje volbu vstupů i výstupů dosažení maximálního ekonomického zisku. Pokud se cena finální produkce zvýší a ceny všech výrobních faktorů se sníží, potom se zisk nutně zvýší.

Předpokládejme hypoteticky tři společnosti. Společnosti 1 maximalizuje zisk při cenách P1, w1, r1 nakupuje optimální množství výrobních faktorů K1, L1 a vyrábí tak optimální objem finální produkce Q1; společnost 2 maximalizuje zisk při cenách P2, w2, r2 nakupuje optimální množství výrobních faktorů K2, L2 a vyrábí tak optimální objem finální produkce Q2 a společnost 3 maximalizuje zisk při cenách P3, w3, r3 nakupuje optimální množství výrobních faktorů K3, L3 a vyrábí tak optimální objem finální produkce Q3. Pak zisk jednotlivých společností je následující:

$$\Pi 1 = P1Q1 - w1L1 - r1K1 \qquad (5.5.2.2)$$

$$\Pi 2 = P2Q2 - w2L2 - r2K2 \qquad (5.5.2.3)$$

$$\Pi 3 = P3Q3 - w3L3 - r3K3 \qquad (5.5.2.4)$$

Při podmínkách:

$$P1 = P2 = P3 \tag{5.5.2.5}$$

$$w1 \leq w2 \leq w3 \tag{5.5.2.6}$$

$$r1 \leq r2 \leq r3 \tag{5.5.2.7}$$

$$Q1 \geq Q2 \geq Q3 \tag{5.5.2.8}$$

musí platit:

$$\Pi 1 \geq \Pi 2 \geq \Pi 3 \tag{5.5.2.9}$$

Změny množství výrobních faktorů výrazným způsobem ovlivňují zisk společností. Za předpokladu platnosti předchozích podmínek zobrazuje závislost zisku na P graf 5.5.2. Uvedené skutečnosti jsou logické a samozřejmé. Představme si, však jak snížení množství výrobních faktorů může přispět ztráta dat a informací z vývojových oddělení. Například společnost 1 s průběhem zisku získává nepřetržitě informace pro výrobu nových progresivních technologických zařízení využitím dat z vývojového oddělení společnosti 3. Tedy společnost 3 dostatečně nezabezpečila data svého vývojového oddělení, musí dále investovat do následného vývoje, což přináší větší náklady než u společnosti 1, která se chová na trhu neseriózně, neinvestuje do vývoje tak velký objem prostředků jak společnost 3. Společnost 3 za předpokladu menší ziskovosti může dále existovat, společnost 1 musí však své parazitní chování také tržně regulovat, aby společnost 3 plně nezlikvidovala. Uvedené skutečnosti se promítají zejména u společností výrobních, technologických ale i krátkodobě mají svůj význam i u společností obchodních.

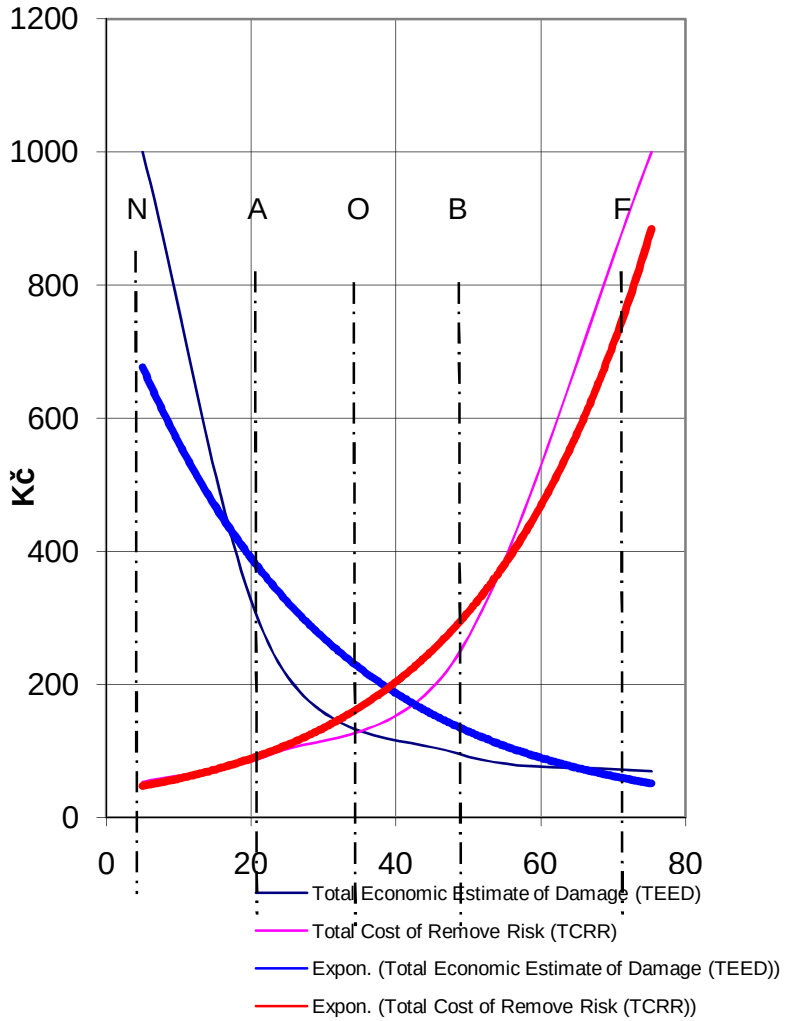
5.5.3 **Ekonomická přiměřenost v rozhodování firem**

Důležitým faktorem pro rozhodování společnosti k uvedené problematice jsou zejména následující otázky: „Kdy, kolik a pak následně periodicky přiměřeně investovat do bezpečnosti IT i zejména vzhledem k dostupným financím, možnostem společnosti a ve vztahu k charakteru společnosti, P, Q, Π a dalším faktorům?“.

Bezpečnost IT společnosti, která není ve společnosti řešena, znamená ve svém důsledku vícenásobné výdaje. V případě, že uniknou data, přijde společnost tímto například o těžce vybudovanou pozici na trhu, tedy přichází o část příjmů. Ihned musí zacelit příčinu a přijmout okamžité řešení tzn. další náklady. V dal-

ším kroku je potřeba vydat investice na technické a organizační řešení, aby nedošlo k zopakování takových bezpečnostních incidentů.

Účelnost nákladů na řešení bezpečnosti můžeme srovnat jako poměr nákladů Total Cost of Remove Risk (TCRR) potřebných na snížení pravděpodobnosti zranitelností a hrozeb firmy, které se získaly analýzou rizik Total Economic Estimate of Damage (TEED). V následujícím grafu 5.5.3.1 Analýza Total Economic Estimate of Damage (TEED) a Total Cost of Remove Risk (TCRR), firemní optimalizace je porovnání nákladů na bezpečnost TEED v závislosti na škodách TCRR (odhadnuté analýzou rizik).



Graf 5.5.3.1 Analýza Total Economic Estimate of Damage (TEED) a Total Cost of Remove Risk (TCRR)
[Vlastní zpracování]

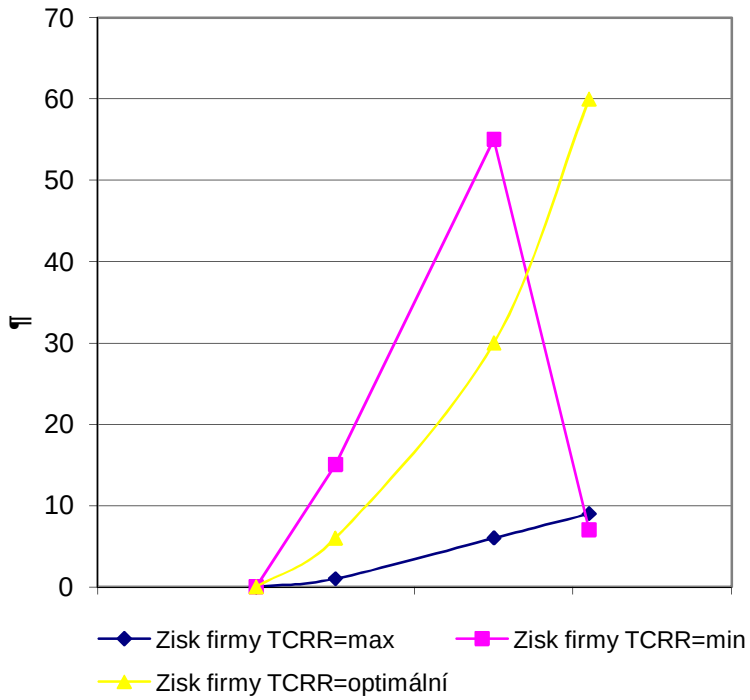
Z grafu 5.5.3.1 je vidět, že v bodě A čase t1 se vynaložily náklady TCRR1 na odstranění ohodnoceného rizika TEED1, tzn. náklady TCRR1 byly nižší než ohodnocení rizika TEED1. Ve druhém případě v bodě B čase t2 se vynaložily

náklady TCRR2 na odstranění ohodnoceného rizika TEED2, tzn. náklady TCRR2 byly podstatně vyšší než ohodnocení rizika TEED2. Je optimální jít maximálně do takové časové polohy, kdy náklady se rovnají ohodnocenému riziku. Dle uvedené hypotézy je z pohledu společnosti optimální rozhodnutí oscilovat v nejbližším okolí bodu O. V grafu jsou vytvořeny exponenciální křivky, které zobrazují tendence TEED a TCRR. Uvedená hypotetická úvaha je výrazně závislá na analýze rizik a jejich ohodnocení.

V případě, že budeme chtít maximálně zabezpečený systém, tzn. hodnotu všech dostupných firemních informací a dat oceníme značnou hodnotou viz bod F (Full), náklady na bezpečnost IS TCRR horentně stoupnou a systém zabezpečení bude značně neekonomický při realizaci a použití. Navíc nastanou problémy s přístupem k firemním datům, výrazně se stíží dynamické reakce společnosti v jednotlivých obchodních případech. Z pohledu mikroekonomického spotřebuje společnost výrazný objem nákladových investic, tím samozřejmě se následně výrazně sníží svůj zisk Π.

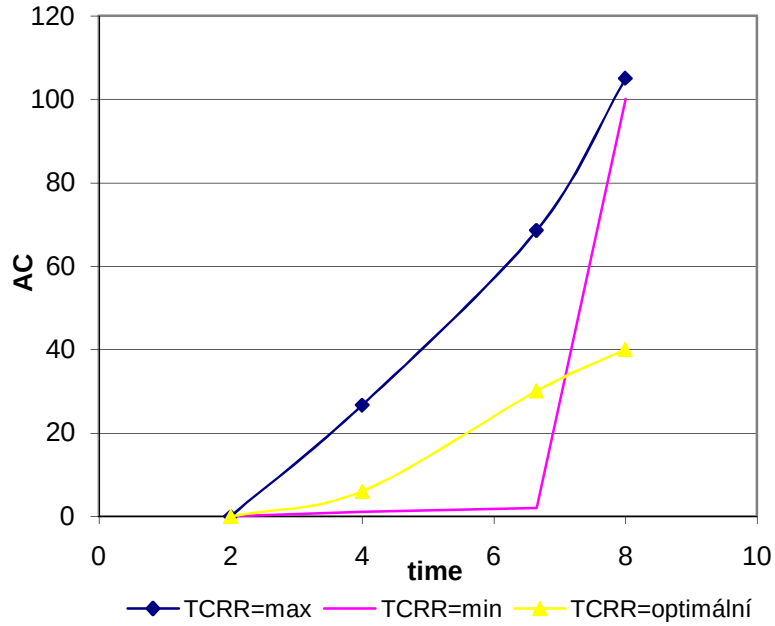
Druhým extrémem je podhodnocení jednotlivých dat a informací viz bod N. V tomto případě budou investice TCRR do zabezpečení IS minoritní a je otázkou, kdy dojde k výraznému bezpečnostnímu incidentu, který ohrozí konkurenceschopnost společnosti nebo dokonce její likvidaci.

Oba extrémní případy jsou zobrazeny v grafu 5.5.3.2. V případě maximalizujícího TCRR zisk roste pomalu, v případě minimalizující TCRR zisk roste výrazně až do situace bezpečnostního incidentu, kdy dojde k dramatickému snížení zisku ohrožující postavení společnosti. V grafu je také zobrazen zisk při optimálním TCRR.



Graf 5.5.3.2 Analýza zisku za podmínek TCRR
[Vlastní zpracování]

Optimalizace řešení bezpečnosti znamená porovnání účelnosti nákladů na přiměřenou míru ochrany a bezpečnosti IS/IT. Absolutní hodnota nákladů TCRR na řešení bezpečnosti IS/IT závisí zejména: na velikosti společnosti, množství heterogenních systémů IS, množství informací, počtu pracovníků a různých postupů práce s informacemi, propojení centra s pobočkami, formou obchodování atd. Vliv nákladů na TCRR je analyzován v grafu 5.5.3.3 Analýza nákladů za podmínek TCRR. Za situace maximalizujícího TCRR náklady rostou extrémně rychle, v případě minimalizující TCRR jsou téměř nulové až do situace bezpečnostního incidentu, kdy dojde k dramatickému zvýšení nákladů; tzn. náklady na odstranění důsledků bezpečnostního incidentu a nákladů na zabezpečení společnosti, aby se situace neopakovala. V grafu je zobrazen průběh nákladů při optimálním TCRR.



Graf 5.5.3.3 Analýza nákladů za podmínek TCRR
[Vlastní zpracování]

Bezpečnost informačních systémů není a nemůže z podstaty být nikdy dokonalá, je na ni stále co zlepšovat. Na druhou stranu rozsah možných opatření je tak obrovský, že vždy je možno vybrat více variant s různou úrovní zabezpečení a samozřejmě tím i v různé cenové hladině.

5.6 Přiměřená firemní bezpečnost IS/IT

Na základě teoretické rešerše, kvalitativního a kvantitativního průzkumu, dlouholetých praktických zkušeností a výstupů světových průzkumů se v rámci disertační práce pokusím subjektivně stanovit části prvků přiměřené firemní bezpečnosti IS/IT. Stavební prvky přiměřené bezpečnosti IS/IT jsem subjektivně rozdělil do třech základních částí:

- Přiměřený procesní management bezpečnosti IS/IT a profil manažera bezpečnosti IS/IT,
- přiměřená technologická bezpečnost IS/IT,
- ekonomická část přiměřené bezpečnosti IS/IT.

5.6.1 **Přiměřený procesní management bezpečnosti IS/IT a profil manažera bezpečnosti IS/IT**

V případě přiměřeného procesního managementu bezpečnosti IS/IT a profilu manažera bezpečnosti IS/IT jsem se zaměřil na následující dva elementy:

- Přiměřený procesní management bezpečnosti IS/IT,
- ideální osobnostní profil manažera bezpečnosti IS/IT.

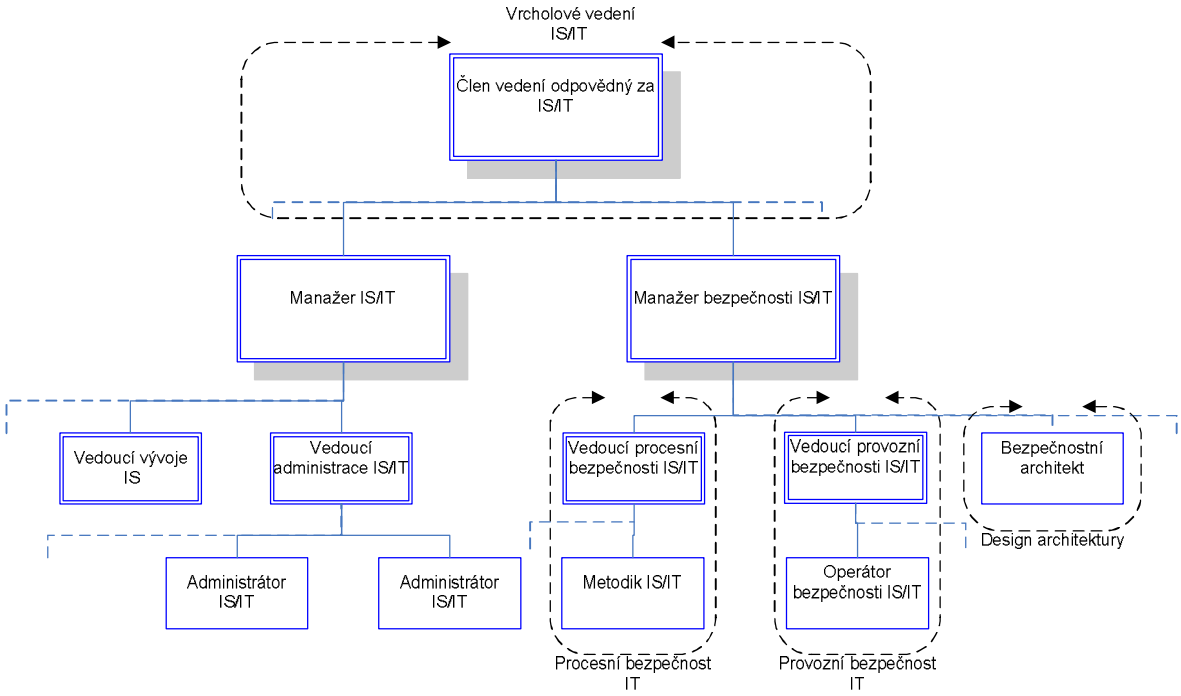
Zjednodušený popis obou elementů bezpečnosti IS/IT je uveden v následujících částech této kapitoly.

Přiměřený procesní management bezpečnosti IS/IT

V přiměřeném procesním managementu bezpečnosti IS/IT jsem se zaměřil na organizační strukturu managementu IS/IT ve vazbě na bezpečnost IS/IT. Organizační strukturu přiměřeného procesního managementu bezpečnosti IS/IT modeluji na typ organizace s těmito parametry:

- Minimální počet zaměstnanců 2000 s přístupem do IS organizace,
- komerční obchodní organizace,
- společnosti nepůsobí v IS/IT.

Přiměřeným procesním managementem bezpečnosti IS/IT rozumím optimalizaci procesních vazeb bezpečnosti IS/IT v organizační struktuře společnosti. Zjednodušenou organizační strukturu subjektivní modelace přiměřeného procesní managementu bezpečnosti IS/IT uvádím na obrázku Obr. 5.6.1. V případě detailního pohledu na tuto zjednodušenou organizační strukturu pozorujeme přímé řízení bezpečnosti IS/IT i IS/IT členem vedení odpovědným za IS/IT. Manažer bezpečnosti IS/IT řídí jak procesní bezpečnost IS/IT tak i dohled provozní bezpečnosti IS/IT. Bezpečnostní manažer IS/IT přímo řídí i další pozice jako například bezpečnostního architekta IS/IT a další. Výhodou modelu je direktivní organizační řízení procesní i technologické bezpečnosti IS/IT. Určitým nedostatkem může být však koordinace provozu IS/IT ve vazbě na tuto organizační strukturu.



Obr. 5.6.1 Zjednodušená struktura managementu bezpečnosti IS/IT [Vlastní zpracování]

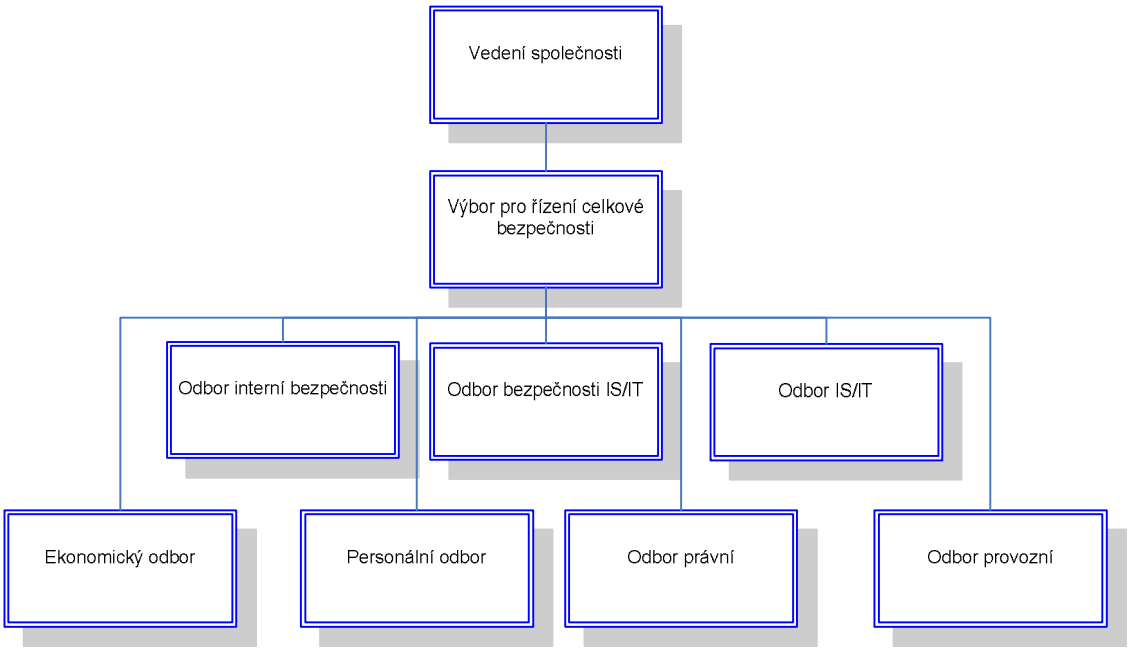
Pro zajištění managementu celkové bezpečnosti v modelaci doporučuji vytvoření řídícího orgánu: „Výboru pro řízení celkové bezpečnosti společnosti“, který by dohlížel a řešil další aspekty celkové bezpečnosti: „Právní, bezpečnost budov a prostor, personální otázky a další v přímé vazbě na vrcholové vedení společnosti.“

Výbor pro řízení celkové bezpečnosti společnosti by měl zajišťovat zejména následující:

- Návrhy a doporučení bezpečnostní politiky v oblastech bezpečnosti zaměstnanců, majetku a IS/IT,
- dohled na naplňování bezpečnostní politiky,
- koordinace prosazování bezpečnostních opatření v praxi,
- vyhodnocování závěrů analýz provozních rizik, spojených s oblastí bezpečnosti a včetně opatření k jejich nápravě,
- doporučování zásad, pravidel a postupů pro užívání IS/IT,

- doporučení pravidel proti ztrátě, modifikaci a zneužití dat v rámci IS/IT,
- doporučení pravidel pro třetí strany pro přístup k informacím nebo do fyzických prostor společnosti,
- doporučení plánů pro řízení kontinuity podnikatelských činností,
- vyhodnocení mimořádných událostí včetně opatření k jejich nápravě,
- a další.

Návrh struktury Výbor u pro řízení celkové bezpečnosti společnosti je uvedena na obrázku Obr. 5.6.2.



Obr. 5.6.2 Výbor pro řízení celkové bezpečnosti společnosti [Vlastní zpracování]

Porovnáním subjektivního modelu přiměřené bezpečnosti IS/IT a výstupů kvalitativního průzkumu bezpečnosti IS/IT, se uvedený model nejvíce blíží zjednodušené organizační struktuře společnosti ABC a.s. uvedené na Obr 5.2.5.1. Rozdíl spočívá v podřízenosti provozní bezpečnost IS/IT. Shodným prvkem u modelace přiměřené bezpečnosti IS/IT a výstupu kvalitativního průzkumu ve společnosti ABC a.s. je řídící orgán „Výbor pro řízení celkové bezpečnosti společnosti ABC a.s.“, uvedený na Obr 5.2.5.2.

Ideální osobnostní profil manažera bezpečnosti IS/IT

Na základě teoretické rešerše, kvalitativního a kvantitativního průzkumu, dlouholetých praktických zkušeností a výstupů průzkumů jsem se pokusil subjektivně stanovit ideální osobnostní profil manažera bezpečnosti IS/IT.

Mezi podstatné vlastnosti manažera bezpečnosti IS/IT by měly patřit:

- Manažerské schopnosti,
- přirozená autorita,
- morální vlastnosti,
- prezentační a komunikační schopnosti ve vazbě na vedení společnosti,
- analytické schopnosti.

K hlavním odborným předpokladům manažera bezpečnosti IS/IT by měly přináležet:

- Manažerská procesní metodická odbornost (CISM, CISA),
- základní ekonomické znalosti,
- znalost prostředí organizace,
- technologická odbornost.

Sumarizace ideálního osobnostního profilu manažera bezpečnosti IS/IT je uvedena na obrázku Obr. 5.6.3. Ze svého subjektivního pohledu nejvíce preferuji manažerské schopnosti a charisma, z odbornosti metodickou procesní bezpečnost IS/IT.

Porovnáním subjektivního modelu osobnostního profilu manažera bezpečnosti IS/IT a výstupů kvalitativního průzkumu bezpečnosti IS/IT, dochází ke shodě u preference manažerských schopností a autority. Z kvalitativního průzkumu plyne, že z vlastností více chybí prezentační a komunikační vlastnosti. Z pohledu odbornosti je plná shoda výstupů kvalitativního průzkumu i subjektivního modelu osobnostního profilu manažera bezpečnosti IS/IT. Preferovanou částí je zejména metodická odbornost procesní bezpečnosti IS/IT (CISM, CISA).

Obr. 5.6.3 Profil manažera bezpečnosti IS/IT
[Vlastní zpracování]

5.6.2 **Přiměřená technologická bezpečnost IS/IT**

Na základě teoretické rešerše, kvalitativního a kvantitativního průzkumu, dlouholetých praktických zkušeností a výstupů průzkumů jsem se pokusil subjektivně definovat pravidla přiměřené technologické bezpečnosti IS/IT. Pravidla modeluji na typ organizace s těmito parametry:

- Minimální počet zaměstnanců 2000 s přístupem do IS organizace,
- komerční obchodní organizace,
- společnost nepůsobí v IS/IT.

Vzhledem k tomu, že společnosti mají velmi odlišná technologická portfolia technické infrastruktury IS/IT, nebudu se zabývat detailním rozborem infrastruktury, což není cílem této disertační práce, ale stanovením základních stavebních prvků přiměřené technologické bezpečnosti IS/IT a definováním ze svého subjektivního pohledu podstatných pravidel pro oblast přiměřené technologické bezpečnosti IS/IT.

Podstatné technologické prvky bezpečnosti IS/IT:

- Aplikační firewally na vnitřním a vnějším perimetru,
- antivirové systémy pro gateway a groupware,
- antispamové systémy pro gateway a groupware,
- systémy filtrace nebezpečného a nežádoucího obsahu,
- systémy proaktivní ochrany (IPS, IDS),
- systémy pro zabezpečené vzdálené připojení,
- systémy ochrany přístupu k síti,
- systémy pro zabezpečení bezdrátové komunikace,
- systémy kontroly shody s bezpečnostními politikami,
- systému controllingu a dohledu,
- korelační systémy pro analýzu bezpečnostních událostí,
- systémy pro zálohování, archivaci a rychlou obnovu včetně šifrovaného ukládání a přístupu,
- systémy záložního napájení
- systémy pro zajištění dostupnosti (HA/LB)
- ochrana koncových bodů,
    - Transparentní šifrování pevných disků,
    - antivir,

- antispam,
- kontrola přenosných médií (USB),
- antispyware,
- aplikační obousměrný personální firewall,
- prevence narušení,
- dvoufaktorová autentizace.

Vybraná pravidla technologické bezpečnosti IS/IT:

- Dílčí bezpečnostní technologické projekty musí být v souladu s analýzou rizik a výstupů z penetračních testů,
- používání víceúrovňových technologií,
- definice a zařazení uživatel do bezpečnostních skupin,
- minimalizace bezpečnostních technologických konzol,
- dynamické přiřazování bezpečnostních politik podle přihlašovacího místa uživatele: v zaměstnání, doma, služební cestě,

5.6.3 **Ekonomická část přiměřené bezpečnosti IS/IT**

Na základě teoretické rešerše, kvalitativního a kvantitativního průzkumu, dlouholetých praktických zkušeností a výstupů průzkumů jsem se pokusil subjektivně definovat sumarizovat několik podstatných informací k ekonomické části přiměřené bezpečnosti IS/IT. Ekonomická rovina byla za určitých hypotetických předpokladů modelována v kapitole 5.5 Mikroekonomická modelace vlivu bezpečnosti IS/IT.

Výše financí výrazným způsobem ovlivňuje obě části zkoumané bezpečnosti IS/IT tedy technologickou i procesní bezpečnost IS/IT. Je nutné diverzifikovat finance na část technologickou i procesní. V případě procesní nebo technologické by nemělo dojít k vyčerpání všech financí na jednu nebo druhou stranu. Přiměřený poměr do bezpečnosti IS/IT by měl činit minimálně 5%.

5.6.4 **Sumarizace přiměřené firemní bezpečnosti**

Přiměřená firemní bezpečnost IS/IT byla zkoumána ze třech základních pohledů:

- Přiměřený procesní management bezpečnosti IS/IT a profil manažera bezpečnosti IS/IT,
- přiměřená technologická bezpečnost IS/IT,
- ekonomická část přiměřené bezpečnosti IS/IT.

Přiměřený procesní management bezpečnosti IS/IT a profil manažera bezpečnosti IS/IT

V případě přiměřeného procesního managementu bezpečnosti IS/IT a profilu manažera bezpečnosti IS/IT jsem se zaměřil na následující dva elementy:

- Přiměřený procesní management bezpečnosti IS/IT,
- ideální osobnostní profil manažera bezpečnosti IS/IT.

a) Přiměřený procesní management bezpečnosti IS/IT

V přiměřeném procesním managementu bezpečnosti IS/IT jsem se zaměřil na organizační strukturu managementu IS/IT ve vazbě na bezpečnost IS/IT. Přiměřeným procesním managementem bezpečnosti IS/IT rozumím optimalizaci procesních vazeb bezpečnosti IS/IT v organizační struktuře společnosti. Zjednodušenou organizační strukturu subjektivní modelace přiměřeného procesní managementu bezpečnosti IS/IT uvádím na obrázku Obr. 5.6.1.

b) Ideální osobnostní profil manažera bezpečnosti IS/IT

Mezi podstatné vlastnosti manažera bezpečnosti IS/IT by měly patřit:

- Manažerské schopnosti,
- přirozená autorita,
- morální vlastnosti,
- prezentační a komunikační schopnosti ve vazbě na vedení společnosti,
- analytické schopnosti.

K hlavním odborným předpokladům manažera bezpečnosti IS/IT by měly přináležet:

- Manažerská procesní metodická odbornost (CISM, CISA),
- základní ekonomické znalosti,
- znalost prostředí organizace,
- technologická odbornost.

Přiměřená technologická bezpečnost IS/IT

V rámci přiměřené technologické bezpečnosti IS/IT jsem se pokusil subjektivně definovat pravidla a stavební prvky přiměřené technologické bezpečnosti IS/IT.

Podstatné technologické prvky bezpečnosti IS/IT:

- Aplikační firewally na vnitřním a vnějším perimetru,
- antivirové systémy pro gateway a groupware,
- antispamové systémy pro gateway a groupware,
- systémy filtrace nebezpečného a nežádoucího obsahu,
- systémy proaktivní ochrany (IPS, IDS),
- systémy pro zabezpečené vzdálené připojení,
- systémy ochrany přístupu k síti,
- systémy pro zabezpečení bezdrátové komunikace,
- systémy kontroly shody s bezpečnostními politikami,
- systému controllingu a dohledu,
- korelační systémy pro analýzu bezpečnostních událostí,
- systémy pro zálohování, archivaci a rychlou obnovu včetně šifrovaného ukládání a přístupu,

- systémy záložního napájení
- systémy pro zajištění dostupnosti (HA/LB)
- ochrana koncových bodů,
    - Transparentní šifrování pevných disků,
    - antivir,
    - antispam,
    - kontrola přenosných médií (USB),
    - antispyware,
    - aplikační obousměrný personální firewall,
    - prevence narušení,
    - dvoufaktorová autentizace.

Vybraná pravidla technologické bezpečnosti IS/IT:

- Dílčí bezpečnostní technologické projekty musí být v souladu s analýzou rizik a výstupů z penetračních testů,
- používání víceúrovňových technologií,
- definice a zařazení uživatel do bezpečnostních skupin,
- minimalizace bezpečnostních technologických konzol,
- dynamické přiřazování bezpečnostních politik podle přihlašovacího místa uživatele: v zaměstnání, doma, služební cestě,

Ekonomická část přiměřené bezpečnosti IS/IT

V rámci ekonomická části přiměřené bezpečnosti IS/IT jsem se pokusil subjektivně definovat několik pravidel pro ekonomickou část bezpečnosti IS/IT.

Výše financí výrazným způsobem ovlivňuje obě části zkoumané bezpečnosti IS/IT tedy technologickou i procesní bezpečnost IS/IT. Je nutné diverzifikovat

finance na část technologickou i procesní. V případě procesní nebo technologické by nemělo dojít k vyčerpání všech financí na jednu nebo druhou stranu.

5.7 Sumarizace hlavních výsledků práce

Disertační práce byla zaměřena na problematiku bezpečnosti IS/IT a její vazby na konkurenceschopnost společnosti. Hlavní výsledky a přínosy mé práce sumarizuji do následujících podkapitol.

5.7.1 **Sumarizace kvantitativního průzkumu**

Z analýzy výsledků kvantitativního výzkumu vyplývá a potvrzuje aktuálnost problematiky a zájem a preference společností Zlínského kraje o problematiku bezpečnosti IS/IT.

Preferenci bezpečnosti IS/IT z pohledu konkurenceschopnosti vlastní společnosti výstupu vnímá vážnost vazby bezpečnosti IS/IT a vlastní konkurenceschopnost 61% společností.

Překvapivým výstupem je nezájem nadpoloviční části společností o doručování informací bezpečnostních hrozeb IS/IT. 61% společností nemá zájem dostávat včasné informace o aktuálních kritických bezpečnostních hrozbách. S menším počtem zaměstnanců se zájem služby poskytování včasných informací o aktuálních bezpečnostních hrozbách výrazně snižuje. Subjektivně se domnívám, že menší společnosti (s počtem zaměstnanců 25-99) nedoceňují význam svých informací uložených v IS/IT a nepředpokládají jejich zneužití.

Dalším překvapivým výstupem je nezájem nadpoloviční části společností o zjištění vlastního aktuálního stavu bezpečnosti IS/IT.

Celkem zajímavým výsledkem kvantitativního výzkumu je absolutní nezájem společností o externí správu a monitoringu bezpečnostních technologií IS/IT. Více jak 98% společností nemá zájem o externí správu a monitoring bezpečnostních technologií IS/IT.

Část výstupů kvantitativního průzkumu je možné porovnat s Průzkumem stavu informační bezpečnosti v ČR 2003 a 2005 (21) a (22) zejména v části významu informační bezpečnosti.

Ostatní prvky kvantitativního průzkumu představují odlišný pohled na bezpečnost IS/IT uvnitř společností než u standardních průzkumů stavu bezpečnosti IS/IT. Hlavní rozdíl spočívá v monitoringu zájmu společností o zajištění bezpečnosti IS/IT externími společnostmi a to jak technologické tak i procesní.

5.7.2 **Sumarizace kvalitativního průzkumu**

Kvalitativní průzkum přinesl celou řadu výsledků vztažených k hlavním i vedlejším cílům disertační práce.

Význam bezpečnosti IS/IT a konkurenceschopnost

Výstupy kvalitativního průzkumu k problematice významu bezpečnosti IS/IT a vazby na konkurenceschopnost společnosti potvrdily, že pro společnosti bezpečnost IS/IT je významná a má přímé vazby na konkurenceschopnost společnosti. Je cenné, že vliv bezpečnosti IS/IT a jeho význam potvrdili zejména pozice manažerů IS/IT, částečně i zástupci běžných uživatelů.

Bezpečnostní hrozby a trendy

K hlavním příčinám bezpečnostních hrozeb dle výstupu sumarizací odpovědí patří: lidský faktor (lidské chyby, nedostatečná kvalifikace, zaneprázdněnost a nedostatečný počet pracovníků), chyby v technologiích (aplikace i infrastruktura), nedostatek financí do bezpečnostních technologií IS/IT a prosazování bezpečnostního managementu IS/IT. Pro sledování trendů bezpečnosti využívají bezpečnostní manažeři IS/IT odbornými školení a „workshopy“ a sledováním on-line zdrojů a systémů proaktivní ochrany.

Procesní management bezpečnosti IS/IT

K podstatným výstupům odpovědí manažerů IS/IT v oblasti procesní bezpečnost IS/IT patří existence formálně definované a nejvyšším vedením přijaté bezpečnostní politiky. Sekce bezpečnosti IS/IT dle výstupů odpovědí je přímo podřízena vrcholovému managementu, část technologické bezpečnosti vedení IS/IT.

K podstatným výstupům odpovědí bezpečnostních manažerů IS/IT v oblasti procesní bezpečnost IS/IT patří seznam metodik, standardů a norem pro management bezpečnosti IS/IT. Hlavními jsou normy a standardy plynoucí z BS 7799, ISO/IEC TR 13335, ITIL, Cobit a CRAMM. Cenným výstupem jsou rozporné vazby mezi managementem IS/IT a bezpečností IS/IT. K podstatným vlastnostem manažerů bezpečnosti patří: Odbornost, manažerské vlastnosti, autorita a znalost prostředí. Pro zlepšení stavu bezpečnosti IS/IT dle odpovědí je třeba: více financí, větší podpora vedení, školení zaměstnanců a specialistů.

Cenným výstupem odpovědí administrátorů IS/IT v oblasti procesní bezpečnosti IS/IT jsou také rozporné vazby mezi administrací IS/IT a bezpečností IS/IT. Významné pro management bezpečnosti IS/IT jsou školení i znalost existence směrnic a politik bezpečnosti IS/IT u administrátorů IS/IT.

Technologická bezpečnost IS/IT

Pro zabezpečení technologické bezpečnost IS/IT existuje provoz (dohled) provozní bezpečnosti viz potvrzení předchozích odpovědí. Zajímavým výstupem jsou rozporuplné výstupy jednotlivých pozic manažerů bezpečnosti IS/IT versus administrátorů IS/IT. Manažeři bezpečnosti zastávají ve většině názor opodstatněnosti úlohy procesního managementu IS/IT. Administrátoři IS/IT jsou přesvědčeni o větší váze technologické bezpečnosti IS/IT.

Ekonomická část bezpečnosti IS/IT

Investice cíleně určené pouze pro bezpečnost IS/IT je velmi problematické identifikovat. Investice do bezpečnosti IS/IT se výrazně prolínají s investicemi do celkové infrastruktury. Poměr investic do bezpečnosti IS/IT dle odpovědí činí v rozmezí 2-6%. Přiměřený poměr dle vyjádření bezpečnostních manažerů IS/IT by měl být cca okolo 10%.

Porovnání s jinými průzkumy

Srovnání organizační struktury bezpečnosti IS/IT kvalitativního průzkumu. Dle (22): "Nejčastějším způsobem organizačního zajištění bezpečnosti je využití útvaru IT/IS, což využívá 78 procent oslovených společností. Dalšími možnostmi jsou například útvar bezpečnosti nebo ekonomický útvar.“. Výstupem kvalitativního průzkumu jsou částečně oddělené útvary bezpečnosti IS/IT.

5.7.3 Sumarizace analýzy čtyř incidentů

Podstatným aspektem pro management bezpečnosti IS/IT obvykle bývá rozbor bezpečnostních incidentů a událostí v IS/IT. Společnosti samozřejmě z objektivních příčin se snaží o odvrácení medializace těchto negativních událostí, nicméně uvedené případy jsou ponaučením nejen pro odborné spektrum, ale i pro odpovědné manažery společností a firem.

První bezpečnostní incident se zabývá problematikou neomezených přístupových práv vývojového programátora a chybějícího kontrolního oddělení a mechanismů auditu a kontroly. Pro zamezení uvedeného typu incidentu je třeba nastavit procesně i technicky kontrolní mechanismy uvnitř organizace. Navíc kontroly je nutné v čase měnit a přizpůsobovat v souvislosti s rozvojem systému IS/IT případně i se změnou organizační struktury.

Druhý bezpečnostní incident se zabývá problematikou podceněním provozních personálních potřeb pro administraci provozní bezpečnosti IS/IT. Pro zamezení uvedeného typu incidentu je třeba schopnost manažera bezpečnosti IS/IT přesvědčit management společnosti o preferenci v těchto situací. Tedy uvolnění finančních rezerv pro personální vyřešení situace nebo přenesením činnosti, odpovědnosti a sankcí na externí společnost.

Třetí bezpečnostní incident se zabývá problematikou ochranou a zcizováním autorských práv. Pro zamezení uvedeného typu incidentu je třeba provést důslednou analýzu rizik a na jejím základě zajistit přiměřeným způsobem bezpečnostní opatření. Podstatným prvkem je také ON-LINE monitoring bezpečnostních událostí.

Čtvrtý bezpečnostní incident představuje jiný typ bezpečnostního incidentu. Zabývá se společností poskytující služby v oblasti IS/IT, která kvůli své nedbalosti v této oblasti, musela ukončit svou činnost. Pro zamezení uvedeného typu incidentu je třeba zavést management jakosti v poskytování IS/IT služeb (postupy a kontrolními mechanismy pro poskytování kvalifikovaných služeb, projektové řízení atd.)

5.7.4 Sumarizace tendence a trendů v oblasti bezpečnosti IS/IT

Sumarizace vybraných trendů reprezentuje následující výsek trendové oblasti bezpečnosti IS/IT:

- Trendy zranitelnosti systémů IS/IT škodlivými kódy,
- trendy útoků a nové motivace počítačových zločinců,
- trendy nebezpečných kódů a kombinovaných hrozeb,
- trendy v oblasti technologické bezpečnosti IS/IT.

Trendy zranitelnosti systémů IS/IT škodlivými kódy

Zranitelnost systému je jedním z podstatných parametrů a vlastností v oblasti bezpečnosti IS/IT. Zjednodušeně hlavními příčinami zranitelností jsou skryté chyby při vytváření nových systémů, nedostatečné odladění, ekonomické aspekty a tlak trhu na výrobce systému.

Od roku 2004 do konce roku 2006 lineárně roste počet nových zjištěných zranitelností.

Podstatnou rolí v oblasti zranitelnosti hraje počet dnů, kdy nová zranitelnost nemá záplatu na odstranění této zranitelnosti. Nejideálnější situace byla v prvním pololetí roku 2006, kdy průměrná doba bez „záplat“ pro odstranění zjištěné zranitelnosti byla 28 dnů ve sledovaném časovém úseku. Nejhorší situace byla zatím v prvním pololetí roku 2007, kdy průměrná doba bez „záplat“ pro odstranění zjištěné zranitelnosti byla 55 dnů ve sledovaném časovém úseku. Uvedený trend znamená, že výrobci v současných podmínkách nejsou schopni

dynamicky reagovat na růstový trend nově zjištěných zranitelností. Tímto dostávají manažery bezpečnosti IS/IT do velmi problematických situací.

Novým prvkem v oblasti zranitelností systémů IS/IT se stala definice nultého dne. Zranitelnost nultého dne znamená, že tentýž den zjištěná nová zranitelnost systému IS/IT byla globálně zneužita. To dává novou dimenzi pohledu bezpečnostních manažerů IS/IT na oblast technologické bezpečnosti IS/IT.

Důležitým prvkem v oblasti technologické bezpečnosti jsou koncová zařízení a jejich operační systémy. Zatím nejdelší průměrný čas potřebný k zajištění záplaty představuje operační systém SUN. Překvapivě dobře v uvedeném srovnání

Významnou roli mají v oblasti bezpečnosti IS/IT webové prohlížeče. Nejvíce zjištěných nových zranitelností představuje prohlížeč Microsoft Internet Explorer, nejméně Opera. Uvedený trend počtu zjištěných zranitelností souvisí zejména s počtem požívaných instalací příslušného prohlížeče.

Trendy útoků a nové motivace počítačových zločinců

V oblasti trendů útoků dle (23) dochází během několika let k velmi významným změnám. Hackeři zvyšují úspěšnost nebezpečných činností pomocí nových taktik založených na principech obchodních strategií. Počítačoví zločinci se při vývoji, distribuci a použití nebezpečného kódu a služeb stále více profesionalizují a dokonce komercionalizují. Počítačová zločinnost je nadále motivována finančním ziskem a počítačoví zločinci nyní při provádění nebezpečných činností využívají profesionálnější metody útoku, nástroje a strategie.

Nejčastěji nabízenou komoditou na serverech podzemní ekonomiky byly kreditní karty, na které připadalo 22 % všech nabídek. Na druhém místě byly s těsným odstupem bankovní účty s 21 %.

Cílem útoků jsou především domácí uživatelé a to celkem v počtu 89%. Útoky na domácí uživatele subjektivně mají však sekundární význam. Primárně je získáni identity domácích uživatelů a s její pomocí získání přístupu k firemním datovým zdrojům.

Trendy nebezpečných kódů a kombinovaných hrozeb

Nebezpečné kódy jsou škodlivé programové kódy, jejichž prostřednictvím může dojít až ke krádeži identity a kompromitace počítačového zařízení včetně zneužití uživatelských dat.

Překvapivým zjištěním je obrovský nárůst škodlivých kódů v prvním pololetí roku 2007. Ten dosahuje počtu 212101 a představuje nárůst proti předchozímu pololetí roku 2006 o 186%.

Trendy v oblasti technologické bezpečnosti IS/IT

V oblasti trendů technologické bezpečnosti IS/IT byly zvoleny následující aktuální vybrané tendence a trendy:

- Proaktivní bezpečnost IS/IT,
- víceúrovňové a kombinované ochrany bezpečnosti IS/IT,
- dynamické kontroly přístupu bezpečnosti IS/IT k datovým zdrojům,
- nové technologie pro patch.

a) Proaktivní bezpečnost IS/IT

Proaktivní bezpečnost IS/IT je aktuálním trendem v oblasti bezpečnosti IS/IT. Cílem proaktivní bezpečnosti je proaktivně spravovat hrozby, slabiny a incidenty v oblasti IS/IT a minimalizovat tak potenciální dopady na společnosti. V kontrastu s reaktivními mechanismy, které se pokoušejí zdolat útoky a incidenty až v okamžicích, kdy už zasáhly infrastrukturu, proaktivní správa bezpečnosti IS/IT přidává metody, technologie a služby, které se soustřeďují na nalezení a ošetření slabin již před útokem.

b) Víceúrovňové a kombinované ochrany bezpečnosti IS/IT

Dlouhodobým trendem v oblasti technologické bezpečnosti IS/IT je aplikace víceúrovňové a kombinované ochrany bezpečnosti IS/IT. Víceúrovňovou a kombinovanou ochranu bezpečnosti IS/IT je možné chápat jako určitou specifickou podmnožinu systémů proaktivní bezpečnosti IS/IT. Podstatou víceúrovňové a kombinované ochrany bezpečnosti IS/IT je nasazování více typů, druhů a technologických úrovní vzájemně provázaných a kooperujících systémů bezpečnosti IS/IT.

c) Dynamické kontroly přístupu bezpečnosti IS/IT k datovým zdrojům

Trendem bezpečnosti IS/IT v několika posledních letech se stala dynamická kontrola přístupu bezpečnosti IS/IT k datovým zdrojům. Dynamické kontroly přístupu bezpečnosti IS/IT k datovým zdrojům je možné také chápat jako určitou specifickou podmnožinu systémů proaktivní bezpečnosti IS/IT. Podstatou dynamické kontroly přístupu bezpečnosti IS/IT je dynamické přidělování úrovní přístupových práv za určitých specifických podmínek a stanovování procesních činností stavů.

d) Nové technologie pro patch

Velkým problémem pro společnosti z pohledu zajištění bezpečnosti IS/IT je problematika patch neboli tzv. záplatování zranitelností systémů IS/IT. Principem těchto nových technologií je nepřetržité monitorování a sledování chování systému ve standardním režimu, na jehož základě dochází k přidělování tzv. skórování systému. Dle úrovně skórování systému IS/IT je pak možné ihned v zárodku rozpoznat a identifikovat nebezpečné a škodlivé pokusy a následně jim zabránit, i přesto, že systém nemá aplikovanou příslušnou záplatu nebo případně výrobce systému ji ještě nemá.

5.7.5 **Sumarizace mikroekonomické modelace vlivu bezpečnosti IS/IT**

Mikroekonomické modelace vlivu bezpečnosti IS/IT ukázala za určitých hypotetických předpokladů vliv bezpečnostních faktorů IS/IT na mikroekonomické aspekty menších a středních firem.

Důležitým faktorem pro rozhodování společnosti k uvedené problematice jsou zejména následující otázky: „Kdy, kolik a pak následně periodicky přiměřeně investovat do bezpečnosti IT i zejména vzhledem k dostupným financím, možnostem společnosti a ve vztahu k charakteru společnosti, P, Q, Π a dalším faktorům?“.

Bezpečnost IT společnosti, která není ve společnosti řešena, znamená ve svém důsledku vícenásobné výdaje. V případě, že uniknou data, přijde společnost tímto například o těžce vybudovanou pozici na trhu, tedy přichází o část příjmů. Ihned musí zacelit příčinu a přijmout okamžité řešení tzn. další náklady. V dalším kroku je potřeba vydat investice na technické a organizační řešení, aby nedošlo k zopakování takových bezpečnostních incidentů.

Optimalizace řešení bezpečnosti znamená porovnání účelnosti nákladů na přiměřenou míru ochrany a bezpečnosti IS/IT. Absolutní hodnota nákladů na řešení bezpečnosti IS/IT závisí zejména: na velikosti společnosti, množství heterogenních systémů IS, množství informací, počtu pracovníků a různých postupů práce s informacemi, propojení centra s pobočkami, formou obchodování atd.

5.7.6 **Sumarizace přiměřené firemní bezpečnosti IS/IT**

Přiměřená firemní bezpečnost IS/IT byla zkoumána ze třech základních pohledů:

- Přiměřený procesní management bezpečnosti IS/IT a profil manažera bezpečnosti IS/IT,

- přiměřená technologická bezpečnost IS/IT,
- ekonomická část přiměřené bezpečnosti IS/IT.

Přiměřený procesní management bezpečnosti IS/IT a profil manažera bezpečnosti IS/IT

V případě přiměřeného procesního managementu bezpečnosti IS/IT a profilu manažera bezpečnosti IS/IT jsem se zaměřil na následující dva elementy:

- Přiměřený procesní management bezpečnosti IS/IT,
- ideální osobnostní profil manažera bezpečnosti IS/IT.

a) Přiměřený procesní management bezpečnosti IS/IT

V přiměřeném procesním managementu bezpečnosti IS/IT jsem se zaměřil na organizační strukturu managementu IS/IT ve vazbě na bezpečnost IS/IT. Přiměřeným procesním managementem bezpečnosti IS/IT rozumím optimalizaci procesních vazeb bezpečnosti IS/IT v organizační struktuře společnosti. Zjednodušenou organizační strukturu subjektivní modelace přiměřeného procesní managementu bezpečnosti IS/IT uvádím na obrázku Obr. 5.6.1.

b) Ideální osobnostní profil manažera bezpečnosti IS/IT

Mezi podstatné vlastnosti manažera bezpečnosti IS/IT by měly patřit:

- Manažerské schopnosti,
- přirozená autorita,
- morální vlastnosti,
- prezentační a komunikační schopnosti ve vazbě na vedení společnosti,
- analytické schopnosti.

K hlavním odborným předpokladům manažera bezpečnosti IS/IT by měly přináležet:

- Manažerská procesní metodická odbornost (CISM, CISA),
- základní ekonomické znalosti,

- ü znalost prostředí organizace,
- ü technologická odbornost.

Přiměřená technologická bezpečnost IS/IT

V rámci přiměřené technologické bezpečnosti IS/IT jsem se pokusil subjektivně definovat pravidla a stavební prvky přiměřené technologické bezpečnosti IS/IT.

Podstatné technologické prvky bezpečnosti IS/IT:

- § Aplikační firewally na vnitřním a vnějším perimetru,
- § antivirové systémy pro gateway a groupware,
- § antispamové systémy pro gateway a groupware,
- § systémy filtrace nebezpečného a nežádoucího obsahu,
- § systémy proaktivní ochrany (IPS, IDS),
- § systémy pro zabezpečené vzdálené připojení,
- § systémy ochrany přístupu k síti,
- § systémy pro zabezpečení bezdrátové komunikace,
- § systémy kontroly shody s bezpečnostními politikami,
- § systému controllingu a dohledu,
- § korelační systémy pro analýzu bezpečnostních událostí,
- § systémy pro zálohování, archivaci a rychlou obnovu včetně šifrovaného ukládání a přístupu,
- § systémy záložního napájení
- § systémy pro zajištění dostupnosti (HA/LB)
- § ochrana koncových bodů,

- Transparentní šifrování pevných disků,
- antivir,
- antispam,
- kontrola přenosných médií (USB),
- antispyware,
- aplikační obousměrný personální firewall,
- prevence narušení,
- dvoufaktorová autentizace.

Vybraná pravidla technologické bezpečnosti IS/IT:

- Dílčí bezpečnostní technologické projekty musí být v souladu s analýzou rizik a výstupů z penetračních testů,
- používání víceúrovňových technologií,
- definice a zařazení uživatel do bezpečnostních skupin,
- minimalizace bezpečnostních technologických konzol,
- dynamické přiřazování bezpečnostních politik podle přihlašovacího místa uživatele: v zaměstnání, doma, služební cestě,

Ekonomická část přiměřené bezpečnosti IS/IT

V rámci ekonomická části přiměřené bezpečnosti IS/IT jsem se pokusil subjektivně definovat několik pravidel pro ekonomickou část bezpečnosti IS/IT.

Výše financí výrazným způsobem ovlivňuje obě části zkoumané bezpečnosti IS/IT tedy technologickou i procesní bezpečnost IS/IT. Je nutné diverzifikovat finance na část technologickou i procesní. V případě procesní nebo technologické by nemělo dojít k vyčerpání všech financí na jednu nebo druhou stranu.

6 PŘÍNOS PRÁCE PRO VĚDU A PRAXI

Disertační práce byla zaměřena na problematiku bezpečnosti IS/IT a její vazby na konkurenceschopnost společnosti.

Přínos disertační práce pro teorii vidím v přehledu a analýze nových trendů v oblasti bezpečnosti IS/IT se zaměřením na management, ekonomii a technologickou rovinu. Práce je proložena případovými studiemi reálných bezpečnostních incidentů v IS/IT a analýz příčin včetně subjektivních návrhů opatření pro zamezení replikace těchto negativních událostí. Pro oblast vědeckou a výzkumnou vidím přínosy zejména v oblasti analýzy vývojových tendencí a jejich závěrů. Přínos práce pro vědu vidím také v hledání nových možností jak reagovat na bezpečnostní rizika a tím zvyšovat tvůrčí potenciál podniku právě zabezpečením dobrého a bezpečného pracovního klimatu podniku. Z pohledu teorie spatřuji dále přínos na základě hypotetických předpokladů demonstraci finanční modelace vlivu bezpečnosti IS/IT na základní ekonomické parametry (P, Q, Π).

Praktická část disertační práce přinesla výsledky o stavu bezpečnosti IS/IT v reprezentativním vzorku společností v České republice. Ze syntézy analytických poznatků, které vyplynuly z kvalitativního a kvantitativního průzkumu, byly učiněny závěry a potvrzeny nebo vyvráceny stanovené hypotézy. Přínosy disertační práce spatřuji pro komerční praxi nejen ve zjištění primárních příčin, ale zejména v pokusu o eliminaci a odvrácení příčin, které jsou pro společnosti a firmy zásadní.

Velmi cennou částí práce je kvalitativní terénní průzkum, který přináší nové pohledy manažerů bezpečnosti IS/IT a manažerů IS/IT na problematiku bezpečnosti IS/IT. Z pohledu managementu bezpečnosti IS/IT považuji za cennou část subjektivní stanovení optimálního profilu osobnosti manažera bezpečnosti IS/IT a odkrytí vazeb a vztahů mezi managementem společnosti, bezpečnostním manažerem a manažerem IS/IT.

Vybrané přínosy pro praxi z pohledu přiměřené bezpečnosti IS/IT:

- Zvýšení důvěryhodnosti společnosti.
- Zabránění poškození dobrého jména společnosti medializací úniku dat.
- Ochrana stability organizace.
- Ochrana investic do výzkumu a vývoje před zneužitím konkurencí.

- Ochrana společnosti před útokem hackerů, počítačovými viry a spamy.
- Ochrana informací obchodního charakteru.
- Připravenost společnosti na selhání technických zařízení, plány obnovy.

Tuto práci považuji za počáteční stupeň k problematice nového náhledu na problematiku bezpečnosti IS/IT, která je svou podstatou velmi rozsáhlá a mnohé části a trendy nemohly být z nedostatku prostoru popsány.

7 ZÁVĚR

Disertační práce byla zaměřena na problematiku bezpečnosti IS/IT a její vazby na konkurenceschopnost společnosti.

Výsledky disertační práce lze rozdělit do několika částí:

A. Primární výsledek

- Identifikace a analýzy příčin současných bezpečnostních incidentů a rizikových faktorů IS/IT a jejich vliv na konkurenceschopnost podniků.

B. Sekundární výsledek

- Určení směrů a trendů v oblasti bezpečnosti IS/IT
- Mikroekonomické modelace vlivu bezpečnosti IS/IT na konkurenceschopnost
- Stanovení přiměřeného modelu managementu bezpečnosti IS/IT
- Stanovení optimálního profilu manažera bezpečnosti IS/IT
- Aplikace teoretických znalostí z rešerše do praktické roviny

C. Potvrzení nebo vyvrácení hypotéz

7.1 Primární výsledek

Hlavním cílem disertační práce byla identifikace a analýza příčin současných bezpečnostních incidentů a rizikových faktorů IS/IT a jejich vliv na konkurenceschopnost podniků.

Podle výstupů disertační práce k hlavním příčinám bezpečnostních incidentů patří:

a) Lidský faktor

- Chyby na různých úrovních,
- nedostatečná kvalifikace,
- zaneprázdněnost,
- nedostatečný počet pracovníků.

b) Procesní management bezpečnosti IS/IT

   - Prosazování procesního managementu bezpečnosti IS/IT do praktické roviny

c) Technologické aspekty bezpečnosti IS/IT

   - Zranitelnosti infrastruktury,
   - zranitelnosti IS/IT,
   - úroveň bezpečnostních technologií IS/IT,
   - škodlivé kódy.

d) nedostatek financí do bezpečnostních technologií IS/IT

Pro odstranění příčin bezpečnostních incidentů IS/IT neexistuje jednoznačné řešení. Každá společnost je navíc specifická z řady aspektů: svým oborem působnosti, počtem zaměstnanců, technologií, IS/IT atd. Snížením rizika příčin bezpečnostních incidentů je však možné předcházet přiměřenou kombinací procesního managementu bezpečnosti IS/IT a bezpečnostních technologií IS/IT. Podstatným prvkem ke snížení počtu bezpečnostních incidentů je lidský faktor. Každopádně ke snížení by mohly přispět bezpečnostní školení a vzdělávání zaměstnanců také ve smyslu významu bezpečnosti IS/IT pro konkurenceschopnost vlastní společnosti.

7.2 Sekundární výsledky

Vedlejšími výsledky disertační práce byly:

a) Vymezení směrů a trendů v oblasti bezpečnosti IS/IT

b) Mikroekonomické modelace vlivu bezpečnosti IS/IT na konkurenceschopnost

c) Stanovení přiměřeného modelu managementu bezpečnosti IS/IT

d) Stanovení optimálního profilu manažera bezpečnosti IS/IT

e) Aplikace teoretických znalostí z rešerše do praktické roviny

Tendence směrů a trendů v oblasti bezpečnosti IS/IT potvrdila výrazný nárůst bezpečnostních hrozeb a růst počtu nově zjištěných zranitelností. Bezpečnostní technologie IS/IT přichází adekvátně reakcí na nové hrozby a trend zranitelností systémů IS/IT technologiemi proaktivní ochrany.

Mikroekonomická modelace prokázala za určitých hypotetických podmínek vliv bezpečnosti IS/IT na konkurenceschopnost společností.

V disertační práci byl subjektivně vytvořen přiměřený model managementu bezpečnosti IS/IT z pohledu organizační struktury, technologické a ekonomické roviny. Obdobným způsobem byl stanoven optimální profil manažera bezpečnosti IS/IT.

7.3 Potvrzení nebo vyvrácení hypotéz

Na základě studia specializované literatury zabývající se problematikou bezpečnosti IS/IT, vlastních odborných znalostí a zkušeností, terénních kvalitativních a kvantitativních průzkumů a analýz bezpečnostních incidentů je možné vyjádřit stanovisko k hypotézám uvedeným v kapitole 3.1 této disertační práce:

Hypotéza číslo 1

„Podstatným prvkem eliminace příčin současných bezpečnostních incidentů je lidský faktor."

Na základě získaných výsledků je možné tuto hypotézu potvrdit. Lidský faktor ovlivňuje bezpečnost IS/IT na všech úrovních: straně uživatele, administrátora, manažera bezpečnosti IS/IT, manažera IS/IT tak i manažera společnosti. U uživatelů je to zejména chybějící povědomí, u administrátorů zejména časová zaneprázdněnost při aplikaci bezpečnostních technologií a podcenění bezpečnostních rizik, u manažerů IS/IT preference dostupnosti dat a služeb nad bezpečností, nedostatek finančních prostředků na technologickou bezpečnost a motivace, u manažerů bezpečnosti IS/IT nedostatečná argumentace, kvalita osobnosti a autority při praktickém prosazování bezpečnostních politik a u manažerů společnosti chybějící povědomí, velký tlak na úspory investic a provozu.

Hypotéza číslo 2

„Přiměřená bezpečnost IS/IT závisí:

a. Na lidském faktoru,
b. na konkrétní aplikaci norem a metodologií v organizaci (Management procesní bezpečnosti),
c. na aplikaci bezpečnostních technologických prvků (Management technologické bezpečnosti)."

Tuto hypotézu je možné potvrdit a to právě na základě uvedených bezpečnostních průzkumů, výsledků kvalitativního a kvantitativního průzkumu, analýzy bezpečnostních incidentů a bezpečnostních trendů.

Hypotéza číslo 3

„Bezpečnost IS/IT zvyšuje konkurenceschopnost společnosti.

Na základě získaných výsledků jsem dospěl ke změně a upřesnění znění této hypotézy:

„Přiměřená bezpečnost IS/IT zvyšuje konkurenceschopnost společnosti.“

Uvedenou hypotézu je možné potvrdit zejména na základě výsledků kvalitativního výzkumu, analýzy bezpečnostních incidentů a modelace přiměřené bezpečnosti IS/IT.

Na závěr své disertační práce bych rád uvedl, že se domnívám, že cíle práce jsem splnil a věřím, že tato práce bude i v budoucnu sloužit jak mně tak i studentům, pedagogům a v praxi nejen odpovědným pracovníkům za bezpečnost IS/IT tj. manažerům bezpečnosti IS/IT ale i manažerům IS/IT a manažerům společností. Předpokládám, že i nadále budu problematiku bezpečnosti IS/IT dále prohlubovat a zabývat a to nejen v praktické rovině.

8 PŘÍLOHY

PŘÍLOHA A – Obsah kvantitativního telemarketingového průzkumu

Dobrý den,

Dovolujeme si Vás oslovit jako zástupce reprezentativního vzorku vybraných významných společností Zlínského kraje.

Naše společnost IMPROMAT-COMPUTER s.r.o. bude pořádat v regionu Zlínského kraje v nejbližší době cyklus odborných prezentací za účasti zástupců předních výrobců a odborných specialistů na téma infrastruktury a bezpečnosti IS/IT. Proto se na Vás jako významné firmy v regionu Zlínského kraje obracíme s prosbou na zodpovězení několika dotazů, které by pomohly co nejoptimálněji vybrat pro Vás nejvhodnější a nejaktuálnější témata.

Společnosti, které poskytnou údaje a potvrdí svou účast na odborných seminářích, obdrží výhody jako např.: výrazné slevy na služby v oblasti bezpečnostních technologií IS/IT, vybraným společnostem bude poskytnuta zdarma konzultace našich specialistů, vylosovaní obdrží zdarma bezpečnostní licenční programy a mnoho dalších „benefitů“.

I. Ověření kontaktních informací společnosti:

Verifikace a potvrzení kontaktních údajů společnosti.

Zařazení společnosti dle počtu zaměstnanců:

- 25-99
- 100-499
- 500-2000

II. Oblast infrastruktury:

Oblast otázek infrastruktury nebyla součástí zpracování kvantitativní průzkumu této disertační prače.

III. Oblast bezpečnosti IS/IT:

Vybraná část otázek použitá pro kvantitativní průzkum a další zpracování:

- Preferujete bezpečnost IS/IT z pohledu konkurenceschopnosti vlastní společnosti?
  - ANO
  - NE
- Zajímá Vás možnost získání včasných informací o aktuálních bezpečnostních hrozbách?
  - ANO
  - NE
- Měli byste zájem o zjištění aktuálního stavu bezpečnosti IT ve Vaší společnosti?
  - ANO
  - NE
- Měli byste zájem o externí správu a monitoring bezpečnostních technologií IS/IT?
  - ANO
  - NE

Další otázky k problematice bezpečnosti IS/IT nebyly v disertační práci dále použity.

IV. Upřesnění tématu odborných specializovaných prezentací ve Zlínském kraji:

Oblast otázek upřesnění tématu odborných specializovaných prezentací ve Zlínském kraji nebyla součástí zpracování kvantitativní průzkumu této disertační prače.

V. Potvrzení zasílání pravidelných informací z oblasti bezpečnosti IS/IT

Oblast otázek zasílání pravidelných informací z oblasti bezpečnosti IS/IT nebyla součástí zpracování kvantitativní průzkumu této disertační prače.

Termíny odborných prezentací Vám zašleme v dostatečném předstihu zpět na Váš email, případně Vás budeme kontaktovat telefonicky. Děkujeme Vám za spolupráci a přejeme hezký den.

Pracovník telemarketingu
IMPROMAT-COMPUTER s.r.o.

PŘÍLOHA B – Obsah kvalitativního průzkumu

Vážení kolegové,

Dovoluji si Vás oslovit jako zástupce reprezentativního vzorku vybraných společností s prosbou o spolupráci na výzkumu v rámci zpracování disertační práce na téma: „Význam ochrany a bezpečnosti IS/IT pro konkurenceschopnost podniku.“

Tento výzkum si klade za cíl globálně analyzovat současnou reálnou situaci v oblasti bezpečnosti IS/IT a měl by přispět k jejímu dalšímu rozvoji v České republice. Zavazuji se, že uvedené výstupy nebudu svazovat s konkrétním jménem Vaší společnosti a budou použity pouze pro oblast této disertační práce. S globálními výstupy kvalitativního průzkumu Vás v případě Vašeho zájmu budu informovat.

Děkuji Vám za spolupráci.

Ing. Milan Kafka
Ředitel projektů
IMPROMAT-COMPUTER s.r.o.

Manažer IS/IT:

I. Význam bezpečnosti IS/IT a konkurenceschopnost

- Jaký přikládáte význam obecně bezpečnosti IS/IT pro Vaši společnost?
- Může bezpečnost IS/IT ovlivnit prvky konkurenceschopnosti ve Vaší společnosti?

II. Bezpečnostní hrozby a trendy

- Jaké vidíte hlavní příčiny bezpečnostních hrozeb a incidentů v oblasti IS/IT ve Vaší společnosti?

III. Procesní management bezpečnosti IS/IT

- Máte ve formě dokumentu formálně definovanou a nejvyšším vedením přijatou bezpečnostní politiku?
- Jaké je postavení oddělení bezpečnosti IS/IT ve Vaší společnosti?
- Jaké vlastnosti by měl mít manažer bezpečnosti IS/IT?

IV. Technologická bezpečnost IS/IT

- Jakým způsobem je řízena technologická bezpečnost IS/IT?

V. Ekonomická část bezpečnosti IS/IT

- Jaký je procentuální poměr investic do oblasti bezpečnosti IS/IT versus investice do IS/IT?

Bezpečnostní manažer IS/IT:

I. Význam bezpečnosti IS/IT a konkurenceschopnost

- Jaký přikládáte význam obecně bezpečnosti IS/IT pro Vaši společnost?
- Může bezpečnost IS/IT ovlivnit prvky konkurenceschopnosti ve Vaší společnosti?

II. Bezpečnostní hrozby a trendy

- Jaké vidíte hlavní příčiny bezpečnostních hrozeb a incidentů v oblasti IS/IT ve Vaší společnosti?
- Jakým způsobem sledujete trendy bezpečnosti IS/IT?

III. Procesní management bezpečnosti IS/IT

- Jakými hlavními bezpečnostními normami, metodologii a standardy pro IS/IT se řídíte?
- Jak vnímáte vazby mezi managementem IS/IT a managementem bezpečnosti IS/IT?
- Jaké vlastnosti by měl mít manažer bezpečnosti IS/IT?
- Co by bylo možné udělat pro zlepšení bezpečnosti IS/IT ve Vaší společnosti?

IV. Technologická bezpečnost IS/IT

- Jaký máte názor na preferenci technologické bezpečnosti IS/IT?

V. Ekonomická část bezpečnosti IS/IT

- Jaký by měl být procentuální poměr investic do oblasti bezpečnosti IS/IT versus investice do IS/IT?

Administrátor IS/IT:

I. Význam bezpečnosti IS/IT a konkurenceschopnost

- Jaký přikládáte význam obecně bezpečnosti IS/IT pro Vaši společnost?
- Může bezpečnost IS/IT ovlivnit prvky konkurenceschopnosti ve Vaší společnosti?

II. Bezpečnostní hrozby a trendy

- Jaké vidíte hlavní příčiny bezpečnostních hrozeb a incidentů v oblasti IS/IT ve Vaší společnosti?

III. Procesní management bezpečnosti IS/IT

- Jak vnímáte vazby mezi administrací IS/IT a managementem bezpečnosti IS/IT?
- Probíhají školení v oblasti bezpečnost práce v IS/IT?
- Víte o existenci směrnic a politik bezpečnosti IS/IT ve Vaší společnosti?

IV. Technologická bezpečnost IS/IT

- Jaký máte názor na preferenci technologické bezpečnosti IS/IT?

V. Ekonomická část bezpečnosti IS/IT

Oddíl bez otázek

Běžný uživatel:

I. Význam bezpečnosti IS/IT a konkurenceschopnost

- Jaký přikládáte význam obecně bezpečnosti IS/IT pro Vaši společnost?

II. Bezpečnostní hrozby a trendy

Oddíl bez otázek

III. Procesní management bezpečnosti IS/IT

- Probíhají školení v oblasti bezpečnost práce v IS/IT?

IV. Technologická bezpečnost IS/IT

Oddíl bez otázek

V. Ekonomická část bezpečnosti IS/IT

Oddíl bez otázek

PŘÍLOHA C – Vyjádření ředitele společnosti IMPROMAT-COMPUTER s.r.o.

IMPROMAT COMPUTER

Systémová řešení

Milan Kafka pracuje v současnosti ve společnosti IMPROMAT-COMPUTER s.r.o. na pozici ředitele projektů a zároveň je součástí výkonného managementu společnosti.

Od roku 1996, kdy nastoupil do společnosti IMPROMAT-COMPUTER s.r.o., úspěšně vedl řadu strategických projektů pro skupinu společností PPF a.s. a dalších středních i velkých společností. Od roku 2000 výrazným způsobem rozšířil portfolio poskytovaných služeb a komplexních SW řešení. Během posledních pěti let úspěšně prosazuje u zákazníků technologické i metodické procesní bezpečnostní prvky do praktické roviny.

Pod jeho vedením společnost IMPROMAT-COMPUTER s.r.o. dosáhla řady významných aplikačních ocenění v oblasti „security". Mimo jiné jako první společnost v ČR získala mezinárodní odborný certifikát Microsoft Gold Certified Partner for Security Solutions 2002. Tento certifikát obhájila společnost i pro období 2007/2008. Také v oblasti spolupráce se společností Symantec, vedoucí technologickou společností v oblasti bezpečnosti, dosahuje špičkové úrovně. IMPROMAT-COMPUTER s.r.o. opět potvrdila pro období 2007/2008 nejvyšší odbornou kompetenci v ČR - Symantec Platinum Partner.

Milan získal řadu významných personálních certifikátů a ocenění mimo jiné: MCP, CNE, MCSE, MSWAP.

Dle mého názoru splňuje dispozice k vědecké a odborné činnosti. Vzhledem k rozsáhlým praktickým zkušenostem, které si cílevědomě prohlubuje odborným studiem, uvedenou aktivitu podporuji. Získané teoretické informace cíleně využívá a úročí ve prospěch společnosti IMPROMAT-COMPUTER s.r.o..

Ve Zlíně 20.10 2007

IMPROMAT-COMPUTER s.r.o.

RNDr. Petr Kožela
Ředitel
IMPROMAT-COMPUTER s.r.o.

IMPROMAT-COMPUTER s.r.o., areál Svit, 41, budova, tř. T. Bati 5267, 762 02 Zlín
Zapsána V OR: KS V Brně, sp. zn. oddíl C, vložka 8573, IČO: 46992308, DIČ: 308-46992308
tel.: +420 577 213 151, fax: +420 577 211 870, mail: comp.sale@impromat.cz, www.impromat.cz

PŘÍLOHA D – Vyjádření ředitele pobočky společnosti Symantec pro ČR

symantec.

V Praze, dne 1. listopadu 2007

Symantec GmbH
Česká republika a Slovenská republika
Bucharova 2
150 00 Praha 5
Česká republika

Věc: Vyjádření výrobce bezpečnostních řešení

Společnost IMPROMAT-COMPUTER s.r.o. patří z pohledu referencí, odbornosti, certifikací a obchodní úspěšnosti našich bezpečnostních technologií k našim nejvýznamnějším partnerům v České a Slovenské republice.

IMPROMAT-COMPUTER s.r.o. je aktuálně certifikována pro období 2007/2008 na nejvyšší odborné kompetenci v ČR jako Symantec Platinum Partner.

Naše vzájemná spolupráce v oblasti bezpečnostních technologií IS/IT má již dlouholetou tradici. Jeden z prvních rozsáhlých bezpečnostních projektů IS/IT prostřednictvím našich bezpečnostních technologií ve společnosti s počtem nad 8000 koncových zařízení úspěšně realizovala společnost IMPROMAT-COMPUTER s.r.o. již v roce 1998. Od této první rozsáhlejší spolupráce uskutečnila společnost IMPROMAT-COMPUTER s.r.o. řadu dalších bezpečnostních projektů obdobného charakteru.

Milan Kafka pracuje v současnosti ve společnosti IMPROMAT-COMPUTER s.r.o. na pozici ředitele projektů a je primární osobou v oblasti naší spolupráce, vedení projektů a řízení obchodních případů. Milan postupnými kroky vybudoval od roku 1997 špičkový odborný tým v oblasti technologické bezpečnosti, který patří k nejlepším v České republice.

Věřím, že naše vzájemná spolupráce v oblasti bezpečnostních technologií se bude i nadále rozvíjet ve prospěch obou dvou stran.

Se srdečným pozdravem,

Radek Smolík
Country Manager
Symantec GmbH (Česká republika a Slovenská republika)

9 LITERATURA

V následujícím přehledu je uveden seznam použité literatury.

[1.] *ISO/IEC 17799:2005 Information Security Management Information Technology - Code of practice for information security management.* - : British Standards Institution, 2005. p. 106.

[2.] *ISO/IEC 27001:2005 Information Security Management Systems - Information technology - Security techniques - Information security management systems - Requirements Code of practice for information security management.* - : British Standards Institution, 2005. p. 32.

[3.] *ISO/IEC TR13335-1 Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 1:Pojetí a modely bezpečnosti.* - : Český normalizační institut, 1999. str. 41.

[4.] *ISO/IEC TR13335-2 Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 2: Řízení a plánování bezpečnosti.* - : Český normalizační ústav, 2000. str. 23.

[5.] *ISO/IEC TR13335-3 Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 3: Techniky pro řízení bezpečnosti.* - : Český normalizační ústav, 2000. str. 47.

[6.] *ISO/IEC TR13335-4 Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 4: Výběr ochranných opatření.* - : Český normalizační ústav, 2002. str. 72.

[7.] *ITIL Příloha časopisu Business World.* Praha : IDG Czech, a.s., 2007. str. 64.

[8.] ADÁMEK, M. Kvalitativní standardy v IS/ICT. Část 3. Koncept ITIL. *Moderni rizeni.* [Online] 8. 9 2006. [Citace: 20. 5 2007.] http://modernirizeni.ihned.cz/c4-10065470-19237620-600000_d-kvalitativni-standardy-v-is-ict-cast-3-koncept-itil.

[9.] FARFAN, J. a KUFNER, V. Sarbanes-Oxley: za vším hledej IT. *cvis.* [Online] 4. 5 2006. [Citace: 21. 8 2007.] http://www.cvis.cz/hlavni.php?stranka=novinky/clanek.php&id=449.

[10.] KOVACICH, GERALD L. *Průvodce bezpečnostního pracovníka informačních systémů. Zavádění a prosazování bezpečnostní politiky informačních systémů.* 1.vydání. Brno : UNIS Publishing s.r.o., 2000. str. 200. ISBN 80-86097-42-0.

[11.] RODRYČOVÁ D., STAŠA P. *Bezpečnost informací jako podmínka prosperity firmy.* 1.vydání. Praha : Grada Publishing, spol.s r.o., 2000. ISBN 80-7169-144-5.

[12.] HALOUZKA J., HUBNER M., KAPLAN Z.,RACKOVÁ E., SEIGE V. *Informační bezpečnost, Self Assessment, Příručka manažera.* Praha : DSM - Tate International, s.r.o., 2003. str. 154.

[13.] DOBDA, L. *Ochrana dat v informačních systémech.* Praha : Grada Publishing, 1998. ISBN: 80-7169-479-7.

[14.] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* Brno : Computer Press, 2004. str. 194. ISBN: 80-251-0106-1.

[15.] *Rizikovost lidského faktoru v bezpečnosti podnikových informačních systémů.* JAŠEK, R. Zlín : Univerzita Tomáše Bati ve Zlíně, 2002. Sbornik konference Internet a konkurenceschopnost podniku. stránky 139 - 142. ISBN 80-7318-060-X.

[16.] *Bezpečnost informací jako jeden z pilířů konkurenceschopnosti.* JAŠEK, R. Zlín : Univerzita T. Bati, 2001. Internet a konkurenceschopnost podniku . stránky 74-76. ISBN 80-238-6785-7.

[17.] HUMLOVÁ A., SEIGE V. *Vize informační bezpečnosti 2002/2003.* Praha : DSM - TATE International, s.r.o., 2002. str. 210.

[18.] MACEK J., NOVÁK L., RACKOVÁ E., SEIGE V. *Příručka manažera - Business Continuity Planning.* Praha : DSM - TATE International, s.r.o., 2004. str. 210.

[19.] RAK, R. Jak prosazovat investice do bezpečnosti? *Data Security Management.* 8. Duben 2004, stránky 30-32.

[20.] VÁŇA, P. Proč řešit bezpečnost informací. *Softwarové noviny.* 1 2001, Příloha, stránky 12-15.

[21.] SYNEK, M. *Manažerská ekonomika.* Praha : Grada Publishing, 1996. str. 455. ISBN 80-7169-211-5.

[22.] GATES, B. *Byznys rychlostí myšlenky*. 1.vydání. Praha : Management Press, Ringier ČR, a.s. , 1999. str. 354. ISBN 80-85943-97-2.

[23.] DROZD, M. Boj s lidským faktorem v informační bezpečnosti. *IT Systems*. Říjen 2007, stránky 54-56.

[24.] MCCARTHY, L. *IT Security - Risking the Corporation*. Prentice Hall PTR. USA : Pearson Education Inc., 2003. p. 246. ISBN 0-13-101112-X.

[25.] Deset největších bezpečnostních hrozeb v roce 2007. *SYSTEMONLINE*. [Online] 2006. http://www.systemonline.cz/it-security/deset-nejvetsich-bezpecnostnich-hrozeb-v-roce-2007.htm.

[26.] VOKŮRKOVÁ, L. Největší hrozby bezpečnosti IS/IT číhají uvnitř firmy. *CW*. [Online] 3 2006. [Citace: 20. 9 2007.] http://www.cw.cz/cwarchiv.nsf/print/56591F7E4594E180C125716A004EDA20?OpenDocument.

[27.] SCAMBRAY J., MCCLURE S., KURTZ G. *Hacking bez tajemství*. 1.vydání. Praha : Computer Press, 2001. str. 592. ISBN 80-7226-549-0.

[28.] MIKULEC, J. Bezpečnost v mezích zákona - pohled právníka na bezpečnost IT v podniku. *Chief Information Officer Magazine*. březen 2006, 3, stránky 10-13.

[29.] ERNST & YOUNG, DSM - DATA SECURITY MANAGEMENT, NBÚ. *Czech Information Security Survey 2003*. Praha : ERNST & YOUNG, DSM - DATA SECURITY MANAGEMENT, NBÚ, 2003. str. 32. ISBN 80-902858-8-0.

[30.] —. *Czech Information Security Survey 2005*. Praha : ERNST & YOUNG, DSM - DATA SECURITY MANAGEMENT, NBÚ, 2005. ISBN: 80-86813-07-X.

[31.] SYMANTEC. *Symantec Internet Security Threat Report. Trends for July - December 06*. [Dokument] s.l. : Symantec Corporation, March 2007.

[32.] RIPTECH. *Riptech Internet Security Threat Report. Attack Trends for Q1 and Q2 2002*. [Dokument] s.l. : Symantec Corporation, 2002.

[33.] —. *Riptech Internet Security Threat Report. Attack Trends for Q3 and Q4 2001*. [Dokument] s.l. : Symantec Corporation, 2002.

[34.] SYMANTEC. *Symantec Internet Security Threat Report. Trends for July - December 05.* [Dokument] s.l. : Symantec Corporation, March 2006.

[35.] —. *Symantec Internet Security Threat Report. Trends for July - December 04.* [Dokument] s.l. : Symantec Corporation, March 2005.

[36.] —. *Symantec Internet Security Threat Report. Trends for July - December 03.* [Dokument] s.l. : Symantec Corporation, 2004.

[37.] —. *Symantec Internet Security Threat Report. Trends for January 06 - June 06.* [Dokument] s.l. : Symantec Corporation, September 2007.

[38.] —. *Symantec Internet Security Threat Report. Attack Trends for Q3 and Q4 2002.* [Dokument] s.l. : Symantec Corporation, 2003.

[39.] —. *Symantec Internet Security Threat Report. September 2003.* [Dokument] s.l. : Symantec Corporation, 2003.

[40.] —. *Symantec Internet Security Threat Report. Trends for January - June 04.* [Dokument] s.l. : Symantec Corporation, 2004.

[41.] —. *Symantec Internet Security Threat Report. Trends for January 05 - June 05.* [Dokument] s.l. : Symantec Corporation, September 2005.

[42.] SOUKUP, J. *Mikroekonomická analýza.* Slaný : Melandrium, 2001. ISBN 80-86175-13-8.

10 SEZNAM PUBLIKACÍ AUTORA

10.1Publikace

[1.] KAFKA, M., JAŠEK R. Mikroekonomie a bezpečnost. In VIII. ročník mezinárodní konference INTERNET A BEZPEČNOST ORGANIZACÍ Zlín, 14. března 2006. Univerzita Tomáše Bati ve Zlíně. 2006. ISBN 80-7318-393-5

[2.] KAFKA, M., JAŠEK R. Cost optimatization for security. In Odborná príprava pre bezpečnostné služby. Súčasnosť a perspektívy. (projekt mezinárodní vědecko technické spolupráce ČR/SR/ŽU/04/2 - Nové prístupy k vzdelávaniu a výcviku pre sféru bezpečnostného priemyslu). Žilina, 2005. ISBN 80-969148-2-0

[3.] KAFKA, M., JAŠEK R. Requirements on it security managers. In Odborná príprava pre bezpečnostné služby. Súčasnosť a perspektívy. (projekt mezinárodní vědecko technické spolupráce ČR/SR/ŽU/04/2 - Nové prístupy k vzdelávaniu a výcviku pre sféru bezpečnostného priemyslu). Žilina, 2005. ISBN 80-969148-2-0

[4.] KAFKA, M. Aktuální pohled menších a středních společností na problematiku technologické bezpečnosti. In Sborník konference Internet a konkurenceschopnost podniku. VII. sborník přednášek. Univerzita Tomáše Bati ve Zlíně, 2005. ISBN 80-7318-269-6.

[5.] KAFKA, M. Současný stav a tendence v oblasti bezpečnosti. In Sborník konference Internet a konkurenceschopnost podniku. VI. sborník přednášek. Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-162-2.

[6.] KAFKA, M. Informační bezpečnost v komerční praxi. In Sborník konference Internet a konkurenceschopnost podniku. V. sborník přednášek. Univerzita Tomáše Bati ve Zlíně, 2003. ISBN 80-7318-112-6.

10.2Recenze

[1.] JAŠEK, R. Informační bezpečnost a ochrana zdraví při práci s výpočetní technikou. Ostravská univerzita. Repronis Ostrava 2003. ISBN 80–7042-275–0

10.3Projekty[2]

[1.] Česká pojišťovna a.s., Digitální zpracování dotazníků „Velké letní hry ČP – Bez nehody do pohody“ včetně převedení klientských dat do požadovaného datového tvaru pro další marketingové zpracování. Management projektu ze strany dodavatele – kompletní problematika včetně zajištění bezpečnostních opatření. 1999-2000 Česká republika.

[2.] Česká pojišťovna a.s., Digitální zpracování smluv. Management projektu ze strany dodavatele – kompletní problematika včetně zajištění bezpečnostních opatření. 2000 Česká republika.

[3.] Česká pojišťovna a.s., Zpracování formulářů denních aktivit obchodníků v rámci projektu zvýšení produktivity. Management projektu ze strany dodavatele – kompletní problematika včetně zajištění bezpečnostních opatření. 2000 Česká republika.

[4.] ZPS a.s., Digitalizace strategické technické dokumentace. Management projektu ze strany dodavatele – kompletní problematika včetně zajištění bezpečnostních opatření. 2000 Česká republika.

[5.] ČSSZ, Migrace infrastrukturního prostředí. Management projektu ze strany subdodavatele. 2005 Česká republika.

---

[2] *V této sekci je pouze několik vybraných projektů s velmi stručnou charakteristikou. Pro detailnější informace je nutný souhlas zákazníka. Nicméně většinu dalších projektů není možné zveřejnit zejména z pohledu bezpečnostní problematiky, zachování důvěrnosti a bezpečnosti zákaznických informací. Zveřejnění projektů nebo únik informací je navíc podmíněno vysokými finančními sankcemi plynoucí z možného informačního ohrožení zákazníka.*

11 CURRICULUM VITAE

Osobní údaje

Příjmení, jméno, titul:	Kafka, Milan, Ing.
Datum a místo narození:	30. 11. 1964, Zlín
Bydliště:	Ječmenná 647, Zlín Kostelec 76314
Telefon:	+420 603 888 082
e-mail:	Milan.Kafka@impromat.cz

Vzdělání

2002-	Univerzita Tomáše Bati ve Zlíně, Fakulta managementu a ekonomiky, postgraduální studium
1983- 1988	VUT Brno, Fakulta elektrotechnická
1980- 1983	Gymnázium Zlín

Profesionální praxe

1999 - současnost IMPROMAT-COMPUTER s.r.o., Zlín

Ředitel projektů – Vrcholový management společnosti – dále pověřen řízením oddělení SW a oddělením služeb

- Změna vizí společnosti směrem na systémovou integraci, „outsourcing“ a „enterprise“ projekty
- Management strategických projektů
- Orientace na řešení bezpečnosti velkých a středních společností

1996-1998 - IMPROMAT-COMPUTER s.r.o., Zlín

Vedoucí oddělení SW

- Založení nového oddělení
- Orientace na řešení, počátek velkých projektových řešení

1990 -1996 - SWS a.s., Slušovice

Specialista síťových technologií, obchodně technický konzultant

- odborný konzultant projektového týmu technologií zálohování dat a informací na ČSSZ

1989 -1990 - JZD AK Slušovice, Slušovice

Analytik, programátor

Personální certifikace

2005 **SWAP (Software Audit Professional)** – odborná auditní certifikace dle metodologie společnosti Microsoft (nepřetržitě od roku 2001)

2002 **člen ISACA (Information Systems Audit and Control Association)** - mezinárodní profesní asociace zaměřená na oblast auditu, kontroly a bezpečnosti informačních systémů.

2002 **MCSE (Microsoft Certified System Engineer)** – odborně technologický nejvyšší systémový certifikát technologií Microsoft

1997 **MCP (Microsoft Certified Professional)** – odborně technologický systémový certifikát technologií Microsoft

1991 **CNE (Certified NetWare Engineer)** certifikační update

1990 **CNE (Certified NetWare Engineer)** odborně technologický nejvyšší systémový certifikát technologií Novell získán ve Spolkové republice Německo – třetí občan ČR

Týmové certifikace

2002-2007 **Microsoft Gold Certified Partner for Security Solutions,** *IMPROMAT-COMPUTER s.r.o., Vedoucí týmu*

- § nejvyšší celosvětové partnerské ocenění společnosti Microsoft – pouze několik společností v EU; do roku 2003 pouze jediná společnost v ČR

2002 -2007 **Symantec Platinum Partner,**
IMPROMAT-COMPUTER s.r.o., Vedoucí týmu

- § nejvyšší celosvětové partnerské ocenění společnosti Symantec
- § Podmínkou je prokazatelné splnění aspektů: průkazné zkušenosti s poskytováním bezpečnostních řešení klientům z podnikové sféry, využití vlastních bezpečnostních strategií a postupů, disponování špičkových technologií.

Zájmy

Sport, IT technologie, lyžování, cyklistika