

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta managementu a ekonomiky
Ústav managementu výroby – průmyslového inženýrství

**PROJEKT ŘEŠENÍ BEZPEČNOSTI DAT A ŘÍZENÍ BEZPEČNOSTNÍCH RIZIK
V PODNIKOVÉM INFORMAČNÍM SYSTÉMU**

Diplomová práce

ABSTRAKT

Abstrakt česky

Práce je zaměřena na návrh a tvorbu optimálního projektového řešení informační bezpečnosti ve firmě LIMIRE, s r. o. V teoretické části je vysvětleno názvosloví a pojmy, které se v této oblasti objevují. Analytická část obsahuje rozbor současné situace informační bezpečnosti ve firmě včetně prezentace výsledků analýzy. V této části jsou dále odhaleny silné a slabé stránky současného stavu informační bezpečnosti. Projektová část již poskytuje konkrétní návrhy řešení pro zlepšení situace včetně analýzy efektů a možných rizik. Tato část práce vychází ze samotných výsledků analytické části.

Abstract in English language

The primary target of this work is to create an information security project solution in the LIMIRE, Ltd, company. In the theoretical part, the terminology and definitions that appears in this area are explained. Analytical part contains the analysis of the current situation concerning information security and presentation of the analysis results. In this part of the work, the strength and weak parts of the current information security situation are revealed. The project itself is giving suggestion for improving the situation. The project contains also the analysis of the effects and possible threats. The project part is based on the results of the analytical part of this work.

Rád bych touto cestou poděkoval vedoucímu této diplomové práce panu Mgr. Romanu Jaškovi, Ph.D. za odborné vedení, cenné informace, připomínky i materiály, které mi při vedení této diplomové práce poskytl.

Dále děkuji panu Ing. Vladimíru Dragounovi, konzultantovi mé diplomové práce za praktické rady a poskytnuté informace.

OBSAH

OBSAH.....	5
ÚVOD.....	8
1 TEORETICKÁ ČÁST.....	9
1.1 POJEM OCHRANA ZNALOSTÍ, DAT A INFORMACÍ	9
1.2 INFORMAČNÍ SYSTÉM V PODNIKU	10
1.3 INFORMAČNÍ BEZPEČNOST	11
1.3.1 Proces řešení informační bezpečnosti	12
1.3.2 Závislost prosperity firmy na bezpečnosti informací	12
1.3.3 Analýzy bezpečnosti informačního systému.....	13
1.3.4 Efekty bezpečnostní analýzy	13
1.3.5 Kdy je vhodné provádět analýzu bezpečnosti IS.....	14
1.3.6 Doporučené schéma řešení bezpečnosti IS dle normy ISO 13335	15
1.3.7 Cíle a strategie řešení bezpečnosti IS	15
1.3.8 Analýza rizik IS.....	16
1.3.9 Bezpečnostní politika IS	17
1.3.10 Bezpečnostní standardy IS.....	17
1.3.11 Implementace bezpečnosti IS.....	17
1.3.12 Monitoring a audit	18
1.3.13 Možnosti spolupráce s externími firmami	18
1.4 MOŽNOSTI OCHRANY DAT PŘED HROZBAMI	19
1.5 NĚKTERÉ PRVKY OCHRANY DAT V PODNIKOVÉM IS	19
1.5.1 Antivirové programy	20
1.5.2 Firewally	20
1.5.3 Hesla.....	20
1.6 NĚKTERÉ PROSTŘEDKY NUTNÉ PRO PŘENOS DAT MEZI PODNIKEM A OKOLÍM	21
1.6.1 Operační systémy	21
1.6.2 Internet	27
1.6.3 Počítačové sítě a důvody jejich zavádění.....	28
1.7 BEZPEČNOST DAT A INFORMACÍ A LEGISLATIVA	29
1.8 VYBRANÉ ISO NORMY BEZPEČNOSTNÍCH MECHANISMŮ	29
1.9 WORKSHOP PŘI ŘEŠENÍ INFORMAČNÍ BEZPEČNOSTI	30
1.10 ZHODNOCENÍ TEORETICKÝCH ZDROJŮ	31
1.11 TEORETICKÁ VÝCHODISKA PRO ANALYTICKOU ČÁST	31
2 ANALYTICKÁ ČÁST.....	32
2.1 PŘEDSTAVENÍ SPOLEČNOSTI.....	32
2.2 STAV INFORMAČNÍ BEZPEČNOSTI V ČR V ROCE 2003.....	34
2.3 VÝVOJ IT VE FIRMĚ	35
2.4 POSTUP AUDITU BEZPEČNOSTI VE FIRMĚ	37

2.5	CÍL TVORBY ZÁSAD ZABEZPEČENÍ	38
2.6	TYP DAT VYUŽÍVANÝCH V PODNIKU	38
2.7	MOŽNÉ ZDROJE ÚNIKU ČI ZTRÁTY INFORMACÍ A DAT V PODNIKU	40
2.8	TEST BEZPEČNOSTI.....	41
2.9	ZTRÁTA DAT DLE PŮVODCE OHROŽENÍ.....	43
2.10	DIAGNOSTICKÝ NÁSTROJ MBSA.....	45
2.11	PENETRAČNÍ TEST.....	46
2.12	SILNÉ A SLABÉ STRÁNKY SOUČASNÉHO ZABEZPEČENÍ DAT	47
2.12.1	Útočníci	47
2.12.2	Nehody a katastrofy	50
2.12.3	Interní ohrožení.....	52
2.12.4	Ohrožení zvenku	54
2.12.5	Výsledky analýzy aktuálního stavu zabezpečení	56
2.13	HROZBY NEDOSTATEČNĚ ZABEZPEČENÉHO INFORMAČNÍHO SYSTÉMU	56
2.14	SYNTÉZA ANALYTICKÉ ČÁSTI A VYTVOŘENÍ ZÁVĚRŮ PRO PROJEKTOVÉ ŘEŠENÍ.....	57
3	PROJEKTOVÁ ČÁST	59
3.1	CÍLE PROJEKTOVÉHO ŘEŠENÍ	59
3.2	PLÁNOVÁNÍ PROJEKTU	60
3.3	PROJEKT VYLEPŠENÍ ÚROVNĚ ZABEZPEČENÍ SÍTĚ (INTERNETU)	62
3.4	NÁVRH OPATŘENÍ PRO ÚČINNÉ ZÁLOHOVÁNÍ DAT.....	64
3.5	NÁVRH ŘEŠENÍ OCHRANY DAT A PRÁCE PROSTŘEDNICTVÍM ZÁLOŽNÍCH ZDROJŮ	65
3.6	VYTVOŘENÍ ZÁSAD PRO BEZPEČNÝ POHYB NA INTERNETU A OCHRANU DAT	69
3.7	KATALOG OPATŘENÍ PROJEKTOVÉ ČÁSTI.....	72
4	ANALÝZA EFEKTŮ A RIZIK PROJEKTOVÉHO ŘEŠENÍ.....	73
4.1	PŘÍNOS NAVRHOVANÝCH PROJEKTOVÝCH ŘEŠENÍ.....	73
4.2	VYLEPŠENÍ ÚROVNĚ ZABEZPEČENÍ SÍTĚ	74
4.3	NÁVRH OPATŘENÍ PRO ÚČINNÉ ZÁLOHOVÁNÍ DAT.....	75
4.4	NÁVRH ŘEŠENÍ OCHRANY DAT A PRÁCE PROSTŘEDNICTVÍM ZÁLOŽNÍCH ZDROJŮ	75
4.5	VYTVOŘENÍ ZÁSAD PRO BEZPEČNÝ POHYB NA INTERNETU A OCHRANU DAT	76
	ZÁVĚR.....	77
	SUMMARY.....	79
	SEZNAM POUŽITÉ LITERATURY	80
	SEZNAM OBRÁZKŮ	82
	SEZNAM TABULEK.....	83

SEZNAM PŘÍLOH.....84

ÚVOD

Informační technologie, informační systémy a další zařízení jakožto nositelé dat a informací zaznamenaly v poslední době nevídaný rozmach. O důvodech které k tomu vedly nemá smysl debatovat. Jsou totiž všeobecně známé a vyplývají z celosvětově rozpoznatelných globalizačních trendů. Do popředí se tak dostává fenomén, o kterém se mnoho let příliš nevědělo a o jehož důležitosti bohužel i dnes stále ještě mnoho lidí pochybuje. Jedná se o ochranu informací, znalostí a dat. Není nutné nikterak zdlouhavě debatovat o faktu, že informace proudící v podnikových sítích elektronicky i v papírové podobě mají mnohdy obrovskou cenu. Nikterak svou povahou, ale svou důležitostí pro jiné osoby. Takové osoby potom nabytím podobných dat mohou získat účinný nástroj pro svou cestu k porážení konkurence či k získání nečekaného profitu na úkor lidí, jež o data přišli, o data která byla chráněna nedostatečným, insuficietním způsobem.

Tak jako se zdokonalují způsoby, kterými se organizované skupiny či jednotlivci snaží data krást, se rovněž zdokonalují i postupy a nástroje, kterými lze svá data více nežli dostatečně chránit. Je však rovněž nezbytné si uvědomit, že nebezpečím pro svá data mohou být i samotní uživatelé, kteří nikterak neproškolení vstupují do procesu tvorby a výměny dat. Je potom jednoduché vlastní neukázněností či neznalostí způsobit nemalé finanční škody plynoucí z porušení datové integrity. Případů z minulosti, kdy ztráta dat díky nedisciplinovanosti uživatelů či zodpovědných osob znamenala obrovské ztráty a velkou ostudu existují jen v České republice desítky.

Problematicke ochrany znalostí a dat a samotnému řešení informační bezpečnosti jsem se již věnoval ve své bakalářské práci a byl jsem nesmírně potěšen, když jsem našel opět firmu, která byla ochotna se touto problematikou zabývat a já tímto způsobem mohl uplatnit některé poznatky z dřívějšíka a rovněž i aplikovat zcela nové postupy při tvorbě a řešení bezpečnostní politiky.

1 TEORETICKÁ ČÁST

1.1 Pojem ochrana znalostí, dat a informací

Pojem ochrana je jistě úzce spjat s pojmem bezpečnost či pojmem jistota a všechny tyto tři mají v podstatě za úkol snižovat ohrožení. Bezpečnostní politika provází člověka již od počátku jeho existence. Důvody a metody zabezpečení se ovšem v průběhu historie měnily, avšak objektem – předmětem zabezpečení či ochrany byly vždy tyto nejdůležitější následující tři skupiny:

- **Zdraví a život**
- **Majetek**
- **Informace, data a znalosti**

Subjektem zabezpečení či ochrany jsou všichni uživatelé informačních systémů, tedy lidé, v jejichž zájmu se zabezpečení a ochrana provádí – těmito subjekty mohou být zejména:

- **Fyzické osoby**
- **Právnícké osoby (podnikatelé, firmy, apod.)**

Zřejmě dojdeme k závěru, že některé tyto uvedené pojmy spolu úzce souvisí. Například porušení bezpečnosti informace v podniku může vyústit ve ztrátu majetku podniku a to například i ve smyslu budoucích příjmů a nikoliv jen ztráty současného bohatství. Ve své diplomové práci bych se rád věnoval té třetí oblasti zabezpečení: zabezpečení informací, dat a znalostí a to právě v konkrétním podniku. Pod pojmem zabezpečení bychom si mohli představit souhrn technických a programových prostředků a dále organizačních opatření pro zajištění dat, informací či znalostí oproti jejich zničení, ztrátě, znehodnocení či zneužití.

Je to však rovněž zodpovědnost za ochranu informací během jejich vzniku, zpracování, ukládání, přenosů a likvidace prostřednictvím logických, technických, fyzických a organizačních opatření, která musí působit proti ztrátě důvěrnosti, integrity (neporušenosti) a dostupnosti těchto hodnot. Řešení bezpečnostní politiky u konkrétních subjektů vždy vyžaduje individuální posouzení podmínek, požadavků a zájmů těchto subjektů. V zásadě je třeba, aby si subjekt odpověděl na následující otázky:

- **Zda a co má být chráněno**
- **Před čím to má být chráněno**
- **Jakými prostředky a jakým způsobem má být ochrana prováděna**

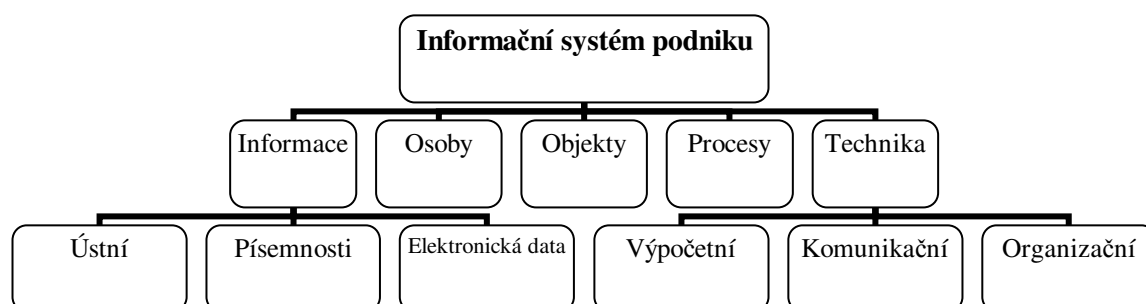
Mezi **vnější okolnosti**, které nás nutí data, znalosti a informace chránit patří zejména existence hrozeb a míra rizika s jakou se hrozby mohou uskutečnit.

Mezi **vnitřní okolnosti** patří například ekonomické možnosti subjektu realizovat nutná protipatření.

[1, str. 9]

1.2 Informační systém v podniku

Informační systém podniku (IS) je definován jako systém informací procházejících firmou. Za účelem uskutečnění cílů IS je využíváno IT (informačních technologií) což jsou podpůrné prostředky technického charakteru.

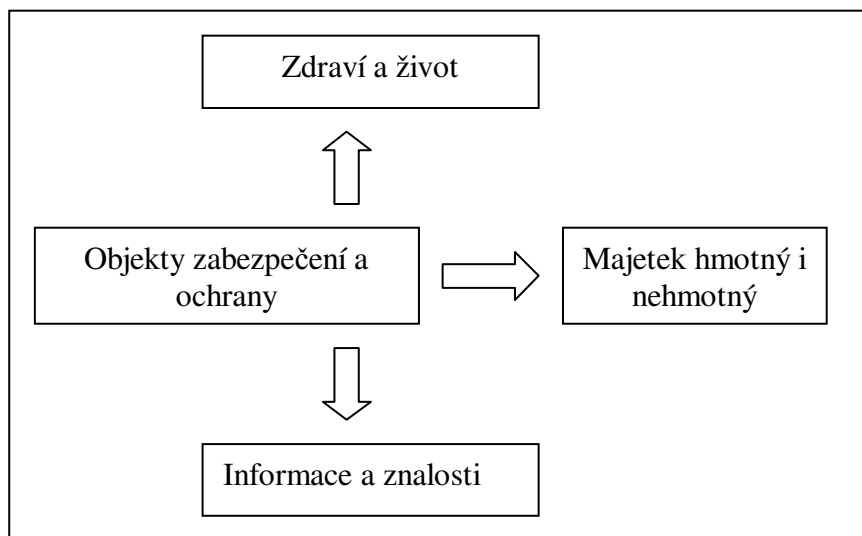


Obr. 1: Informační systém podniku [1, str. 62]

Dále se tady setkáváme z pojmem tzv. bezpečného informačního systému: **Bezpečný informační systém** definujeme jako systém, který chrání informace během jejich vstupu, zpracování, uložení, přenosu a výstupu proti ztrátě dostupnosti, integrity a důvěrnosti a při jejich likvidaci proti ztrátě důvěrnosti. Každý informační systém se skládá z více součástí, může být tedy bezpečně vybudován pouze aplikací celostních ochranných mechanismů. I zde je však nutné si uvědomit, že absolutní bezpečnost neexistuje a tedy vždy nutně existuje míra akceptovatelného rizika. [1, str. 11]

1.3 Informační bezpečnost

Jeden z prvních počítačů na světě ENIAC (*Electronic Numerator, Integrator, Analyzer and Computer*) byl chráněn prostě tím, že o něm svět několik měsíců nevěděl. Takovýto způsob ochrany by dnes již zcela jistě neuspěl. Proto se s rozmachem informačních technologií řeší i způsoby jejich zabezpečení a vzniká tak úplně nový pojem – **informační bezpečnost** (information security).



Obr. 2: Objekty zabezpečení a ochrany [vlastní zpracování]

Počátky tohoto pojmu je možno vysledovat v polovině 80. let v období, kdy se v masovém měřítku začínají přesouvat agendy a data všeho druhu do privátních výpočetních systémů. Tyto systémy, jejichž hodnotu v podstatě představovala pouze jejich pořizovací cena se rázem mění na systémy a centra nesmírných hodnot. Finanční domy vedou ve svých informačních systémech evidence účtů svých klientů, podniky je používají pro řízení výroby, armády do nich umisťují i ty nejutajovanější informace o obraně států.

V dnešní době pro dosažení maximálního účinku ochrany informačních systémů je nutná spolupráce na několika úrovních (informační, personální, majetková). Cílem provozovatele informačního systému je dosažení co největší bezpečnosti systému, který zaručuje minimální úniky a možnosti zneužití informací. V případě selhání některého z mechanismů zabezpečení pak požaduje co nejrychleji napravit vzniklé škody a v rámci možností dopadnout nebo identifikovat viníka. Bezpečnost je zde tedy chápána jako komplexní zajištění systému. [1, str. 10]

1.3.1 Proces řešení informační bezpečnosti

Prvním zlomem pro řešení informační bezpečnosti je vůbec rozhodnout se pro její řešení. Tomuto říkáme **mentální krok**. Až na výjimky, se management nerozhoduje na základě jasných a ověřitelných informací. Takové informace (výskyt hrozby v čase a jejich dopady na společnost) nejsou dopředu k dispozici a výpočty typu návratnosti investic jsou většinou spekulativní. Je zde nutné si pokládat otázky: „co by se stalo, kdyby to tam nebylo“, „jak vysoké by byly nutné náklady na návrat do původního stavu, bylo-li by to vůbec možné?“, atd. Je proto vhodné a užitečné, považovat náklady spojené s řešením a řízením informační bezpečnosti za určitý specifický druh pojištění. Komplikací pro rozhodnutí je dále fakt, že informační bezpečnost vyžaduje nezanedbatelnou finanční investici. Jakousi náplastí je ale fakt, že bez vynaložení těchto nákladů by společnost ztratila mnohem více. Cílem mentálního kroku je tedy rozhodnutí pro efektivní řešení informační bezpečnosti. To konkrétně znamená následující:

- Ochotu managementu společnosti se informační bezpečností seriózně zabývat
- Rozhodnutí managementu nastartovat proces řešení a přesně stanovit termíny splnění jednotlivých kroků
- Vyčlenění potřebných lidských zdrojů
- Ochotu managementu do projektů investovat
- Uvědomit si skutečnost, že je nutné spolupracovat s externími dodavateli bezpečnostních produktů a služeb
- Připravenost managementu na možné organizační změny

Informační bezpečnost je záležitostí čistě nákladovou, a to s velice obtížně vyjádřitelnými přínosy. V takové situaci je proto **naprosto nezbytná a klíčová podpora managementu firmy**. [3, str. 53]

1.3.2 Závislost prosperity firmy na bezpečnosti informací

Informační bezpečnost, bezpečnost informací, prosperita firmy, konkurenceschopnost podniku. Toto vše jsou slovní spojení vázající se k ochraně informací s cílem zabezpečit jejich přiměřené utajení. Cílem je zajištění, aby někdo jiný nezískal takové možnosti, které by mu umožnily získat na úkor „mé“ společnosti větší část pomyslného nabízeného tržního koláče v jeho podnikatelské působnosti,

aby nezískal konkurenční výhodu. Jde tedy o to, aby nedošlo k nechtěnému úniku významných informací, případně aby nedošlo k fyzickému odstavení informační bezpečnosti s příslušným odborným personálním obsazením v podobě informačního managementu a bezpečnostního informačního managementu. Přístup k této problematice je v každé organizaci specifický. Jsou však jistá základní pravidla a postupy, které by měly být pro zajištění bezpečnosti naplněny. [1, str. 51]

1.3.3 Analýzy bezpečnosti informačního systému

Při analýze bezpečnosti informačního systému je naším cílem prověřit aktuální stav bezpečnosti, odhalit slabá místa a najít nejvhodnější opatření k jeho odstranění. Výsledkem analýzy je podrobná dokumentace o bezpečnostní situaci IS společnosti. Ochrana a bezpečnost informací ovšem nezahrnuje jen počítačovou část. Zahrnuje také veškeré činnosti a subjekty, které s informacemi přicházejí do styku a to jak s informacemi v elektronické, tak i papírové i jiné podobě. Z tohoto důvodu je třeba při analýze neopomenout a významně se zabývat sociální oblastí, tedy lidským faktorem, neboť opomenutí něčeho v této oblasti se stává místem informačního úniku. Tohoto pak samozřejmě mohou využít jak neloajální zaměstnanci, tak i další pracovníci, kteří vůbec nemusí být nutně specialisté v oblasti informatiky. Může jít například o ostrahu objektů, opraváře, obslužný personál kanceláří, externí průnikáře a to jak počítačové, tak využívající metod sociálního inženýrství - tzv. sociotechnika. [1, str. 51]

1.3.4 Efekty bezpečnostní analýzy

- **Zvýšení důvěryhodnosti společnosti** – podobně jako certifikáty řady ISO 9000, lze jasnou bezpečnostní politiku prezentovat jako konkurenční výhodu.
- **Zabránění poškození dobrého jména společnosti medializací úniku dat** – bezpečnostní politika jasně říká, jaký bude postup v případě úniku dat.
- **Ochrana stability organizace** – minimalizuje nebezpečí úniku dat z informačního systému vnějším narušitelem. Způsobů jak proniknou je mnoho. Je třeba mít na vědomí, že protokol TCP/IP je zcela otevřený a proto není problém sledovat obsah jakékoliv otevřené, nešifrované komunikace firmy prostřednictvím internetu.

- **Chrání investice do výzkumu a vývoje před zneužitím** – vývoj a výzkum je nesmírně drahou záležitostí a jakýkoliv únik těchto dat by mohl na straně konkurenta vést k urychlené výrobě a uvedení na trh za zcela jiných podmínek nežli my.
- **Chrání společnost před útokem hackerů či virů** – společnost je chráněna před hackery, tedy před osobami, které ať už pro zábavu nebo s jiným cílem (vydírání, krádeže) pronikají do cizích systémů. Nebo je chráněna před viry, které rovněž působí destruktivním charakterem.
- **Chrání práci zaměstnanců před zneužitím** – chrání ji před zneužitím konkurencí, ale také před zneužitím jinými zaměstnanci.
- **Chrání informace obchodního charakteru** – zde jde převážně o databáze klientů, předměty smluv, apod.
- **Omezuje absolutní moc uživatelů nad informačním systémem** – jsou dána přesná pravidla platná pro všechny zaměstnance a jejich pozice ve společnosti. Pravidla jsou jasná a srozumitelná.
- **Schopnost analyzovat podezřelé situace** – jakýkoliv pokus o průnik je rozpoznán a umožňuje připravit adekvátní reakci.
- **Společnost je připravena na technické selhání** – v případech selhání technických zařízení společnosti nastupují předem určené náhradní prostředky. [1, str. 51]

1.3.5 Kdy je vhodné provádět analýzu bezpečnosti IS

- V případě restrukturalizace podniku
- Pro uspokojování požadavků auditorských firem
- Před zavedením bezpečnostních opatření
- Jako součást pro vstup zahraničního kapitálu
- Pokud společnost usiluje o získání některého z certifikátů jakosti
- V případě pochybení o bezpečnosti informací
- Jsme-li donuceni legislativou, například zákony č. 101/2000 Sb., o ochraně osobních údajů a zákonem č. 148/1998 Sb., o utajovaných skutečnostech. [1, str. 52]

1.3.6 Doporučené schéma řešení bezpečnosti IS dle normy ISO 13335

Schéma řešení informační bezpečnosti



Obr. 3: Schéma řešení informační bezpečnosti [1, str. 54]

Následující schéma vychází z předpokladu, že se společnost nachází v situaci, kdy pro bezpečnost dosud nic nepodnikla a rozhodla se jí řešit. Jde tedy víceméně o teoretický bod nula. I když je možné najít řadu různých schémat, tak níže uvedené vycházející z mezinárodního bezpečnostního standardu ISO 13335 je obecně platné a na body v něm uvedené panuje všeobecná shoda.

1.3.7 Cíle a strategie řešení bezpečnosti IS

Prvním krokem procesu řešení bezpečnosti je rozhodnutí o tom, co přesně bude hlavním cílem a jaká cesta k tomuto cíli povede. I když obecně platí, že je třeba chránit všechny informace, které společnost má, mohou existovat oprávněné důvody, proč bude zvolené řešení omezené pouze na

některé z nich. Je například potřeba urychleně řešit nejaktuálnější problémy, investiční omezení, atd....

Základním cílem je tedy eliminovat případné přímé a nepřímé ztráty způsobené zneužitím, poškozením, zničením nebo nedostupností informací, vytvořením uceleného, nákladově optimalizovaného a efektivně fungujícího systému řízení bezpečnosti informací.

Dílčími cíly potom jsou:

- Zhodnocení současné úrovně informační bezpečnosti
- Definování principu řízení
- Navržení postupu k dosažení požadované úrovně bezpečnosti
- Příprava prostředí pro udržování a zvyšování úrovně bezpečnosti

Je také nutno **přesně vymezit hranice, ve kterých se budeme pohybovat**. Ty jsou vymezeny minimálně v těchto dimenzích:

- Typy informací a dat zahrnutých do bezpečnostního řešení
- Části informačního systému zahrnutých do bezpečnostního řešení
- Organizační složky společnosti
- Části významného okolí společnosti (dceřinné společnosti, dodavatelé, partneři)

[1, str. 55]

1.3.8 Analýza rizik IS

Analýza rizik IS je klíčovou aktivitou v procesu řešení bezpečnosti, která musí poskytnout odpověď na následující tři základní otázky:

- Co se stane, když nebudou informace chráněny?
- Jak může být porušena bezpečnost informací?
- S jakou pravděpodobností se to stane?

Typickým výstupem tohoto kroku je dokument obsahující popis systému a výsledky analýzy, tedy úroveň hrozeb, zjištěné zranitelnosti, úroveň ochranných opatření a distribuci výsledných rizik. [1, str. 56]

1.3.9 Bezpečnostní politika IS

V tomto kroku vznikne základní dokument pro řešení informační bezpečnosti – bezpečnostní politika IS. Jde o dokument, který je po přijetí managementem závazný pro celou společnost a který definuje východiska pro všechny další aktivity společnosti v oblasti informační bezpečnosti. Hlavními cíly bezpečnostní politiky je:

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

Pokud má společnost přijatu bezpečnostní politiku, potom se jedná o rozpracování obecných zásad v oblasti informační bezpečnosti.[1, str. 56]

1.3.10 Bezpečnostní standardy IS

Hlavní oblasti a principy informační bezpečnosti, definované v bezpečnostní politice IS, se dále rozpracovávají do detailní podoby. To se děje formou bezpečnostních standardů – závazných interních dokumentů společnosti. Důležité je, že z bezpečnostní politiky nejen vycházejí, ale jsou s ní ve shodě. Zatímco bezpečnostní politika IS je relativně neměnným dokumentem, u bezpečnostních standardů se předpokládá častější frekvence úprav. [1, str. 56]

1.3.11 Implementace bezpečnosti IS

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. Z tohoto pohledu je vhodné doporučit přípravu dokumentu, který formou projektů popisuje proces

implementace. Podklady pro jeho vytvoření jsou k dispozici již při tvorbě bezpečnostní politiky IS, kdy je také nejvhodnější okamžik pro jeho vznik. [1, str. 56]

1.3.12 Monitoring a audit

Provedením analýzy rizik, přijetím bezpečnostní politiky IS, 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 je alespoň do určité míry připraveno, nastává čas pro důležité rutinní činnosti. Jde o průběžné sledování (monitoring) a průběžnou kontrolu (audit).

Podle schématu řešení informační bezpečnosti se z monitoringu a auditu můžeme vracet k implementaci bezpečnosti, bezpečnostní politice IS, analýze rizik a dokonce na samotný začátek – k otázkám strategickým. V tomto všem tkívá právě význam kontroly a sledování funkčnosti zavedené bezpečnostní politiky IS. [1, str. 57]

1.3.13 Možnosti spolupráce s externími firmami

Externí firmy specializované na řešení informační bezpečnosti nastupují do firmy poté, co si vedení společnosti uvědomí, že ne vše a ne vždy je vše řešitelné vlastními silami. Jsou ovšem oblasti, na které plně postačují možnosti dané společnosti, a nebo jsou pro řešení externí firmou zcela nevhodné. Spolupráce s externí firmou na poli informační bezpečnosti znamená vždy pro firmu jisté otevření se směrem ven a tím i jisté potenciální riziko zranitelnosti. Z těchto důvodů je třeba se při výběru externího řešitele zajímat o:

- Reference z předmětné činnosti
- Profesní certifikáty řešitelského týmu
- Konkrétní složení řešitelského týmu
- Používané metodiky pro řešení bezpečnosti a řízení projektů
- Aktivitu členů řešitelského týmu v oblasti publikační, či odborné účasti na konferencích
- Smluvně zakotvenou ochranu informací
- Celkovou velikost a stabilitu řešitele [1, str. 58]

1.4 Možnosti ochrany dat před hrozbami

Informační systémy, jejich aktivita, mohou být za určitých okolností cílem působení různých nebezpečí. Mohou to být lidé (vlastní zaměstnanci), události způsobené přírodními jevy (oheň, voda, zásah blesku, atd....), poruchy techniky (výpadky napájení, porucha zařízení). Lidské hrozby představují agenti rozvědky, průmysloví agenti, teroristé, organizovaní nebo jednotliví zločinci, zlomyslní nebo pomstychtiví lidé, dobrodruzi, počítačová nadšenci, avšak také vlastní zaměstnanci či přátelé. Od útočníka musíme očekávat, že použije libovolný způsob průniku. Nemusí jít vždy o nejzřejmější metodu a také o útok na nejsilnější místo ochrany. Fyzická poškození způsobená přírodními katastrofami a závadami techniky obvykle zjistíme okamžitě. Informační systém přestane být jednoduše funkční a způsobené škody lze celkem přesně definovat. Horší situace však nastává při nelegálním úniku informací. Zde nelze téměř nic dokázat, pokud získané informace nejsou někde zjevně použity (dokazuje se tedy až důsledek průniku). Provozovatel informačního systému většinou nemá zájem na negativní publicitě a tak dochází k představě, že se vlastně nic nestalo a že ochrana informačního systému je vlastně zbytečná. Většina útoků právě z uvedeného důvodu zůstává neodhalena a ty odhalené neproniknou na veřejnost i z toho důvodu, aby narušitel neměl potvrzen rozsah svého úspěchu a uživatel informačního systému neztratil svou pověst. Informační systém se před působením hrozeb brání řadou protipatření. Ta pak mohou mít různé podoby:

- administrativní (zákaz přístupu, či manipulace s daty)
- logická (nastavení přístupových práv)
- fyzická (zabránění přístupu nepovolaných osob, ochrana objektů)
- technická (disková pole, šifrovací a kryptografické systémy) [1, str. 15]

1.5 Některé prvky ochrany dat v podnikovém IS

Ochrana dat ve vnitropodnikových informačních systémech samozřejmě probíhá za silné podpory určitých prvků bezpečnosti. Není to pouze lidský faktor, který se na této činnosti podílí. Existují prvky aktivní i pasivní bezpečnosti, které za účasti člověka data zejména v počítačových sítích chrání. Mezi ty nejpoužívanější patří:

1.5.1 Antivirové programy

Jedná se o programy, jejichž hlavní činností je soubory napadené virem identifikovat, popř. je i vyléčit. Úspěšnost takovéto akce závisí na použitém antivirovém programu a jeho nastavení, jeho použité verzi a aktualizované databázi virů. Rozeznáváme různé druhy antivirových testů. Mezi ně patří antivirový test, heuristická analýza, srovnávací analýza, rezidentní antivirová kontrola, kontrola elektronické pošty, apod. Mezi nejpoužívanější antivirové programy patří: AVG, AVAST!, F-Prot, Norton AntiVirus. [2, str. 135]

1.5.2 Firewally

Firewall je součást sítě, která zajišťuje bezpečnostní bariéru mezi sítěmi nebo jejich segmenty. Firewally jsou obvykle určeny k tomu, aby chránily určitou síť nebo její součásti od útoku nebo neautorizovaného proniknutí vnějších vetřelců. Firewall však může být nastaven i tak, aby chránil životně důležitá data společnosti nebo jejich prostředky před interními útoky nebo nekompetencí. Veškerý provoz do nebo z chráněné sítě musí projít firewallem a tento je navržen tak, aby povolil pouze autorizovaný provoz. Firewall musí být schopen také chránit sám sebe před proniknutím. Proto jsou firewally většinou jednoúčelové počítače. To znamená, že firewall nezajišťuje jiné služby než pouze nutné ověření uživatele a rozhodnutí, zda povolit průchod či nikoliv. [2, str. 149]

1.5.3 Hesla

Pokud někdo chce proniknout do počítače, musí nejprve prolomit heslo (pokud je v systému nastaveno). Tím lze chránit počítač před neoprávněným přístupem. Takto chráněný počítač buď nelze spustit, anebo spustit lze, ale je zabráněno přístupu k datům. Existuje však několik pravidel pro používání hesel. To první a nejdůležitější říká, že **jen nesmyslná hesla dávají smysl**. Tzv. „social hacking“ je nejpravděpodobnější způsob, jak zaútočit na cizí počítače. Útočník hledá heslo v sociálním okolí oběti. Mezi další pravidla patří:

- Heslo by nemělo mít méně než 8 znaků a mělo by se skládat jak z písmen, tak i z číslic a jiných znaků

- Nepoužívat jako heslo existující pojem, žádná jména, data narození či řady čísel, jako např. „123“
- Pro různé přístupy používat různá hesla. Pokud heslo někdo objeví, jsou způsobené škody omezené
- Hesla co nejčastěji měnit [5, str. 121]

1.6 Některé prostředky nutné pro přenos dat mezi podnikem a okolím

Pokud chce podnik mít kvalitní informační systém, musí mít i kvalitní informační technologie. Ty jsou dnes převážně tvořeny výpočetní technikou, propojením počítačů do sítí a jejich připojení do internetu. Aby toto vše fungovalo na dobré úrovni, je třeba v této oblasti neustálé inovace a progresivního vývoje ze strany společností, tak jak se vyvíjí i hrozby zneužití těchto prostředků a hlavně následného zneužití informací a dat, jejichž nosičem informační technologie jsou. V této souvislosti mluvíme o základních prostředcích nutných pro efektivní přenos dat a komunikaci. Do této kategorie zahrnujeme například počítače a jejich softwarové vybavení, počítačové a telekomunikační sítě, personál a zaměstnance zahrnuté v informačním systému, obecně tedy všechny subjekty, účastníci se informačního a datového procesu bez nichž by se informační a datová výměna nedala uskutečnit.

1.6.1 Operační systémy

Operační systém je základní program, který se spouští automaticky po zapnutí počítače a který řídí činnost jeho technických prostředků podle požadavků uživatele. Dnešní počítače se obvykle mohou ovládat pouze pokud na nich běží operační systém. Bez spuštěného operačního systému jsou pro uživatele nepřístupné. Mezi nepoužívanější operační systémy je vhodné zařadit následující:

MS-DOS - Microsoft Disk Operating System – tak zní jeho originální název. V dnešní době se již nepoužívá. Jedná se o jednoúlohový, jednouživatelský operační systém s textovým a nabídkovým uživatelským rozhraním. Jednouživatelský znamená, že ho v jednom okamžiku používá pouze jeden uživatel. Jednoúlohový – umožňuje spuštění pouze jedné aplikace, před spuštěním druhé se ta původní musí ukončit. O nějakém kvalitním zabezpečení zde ještě nemohla být vůbec řeč. Přelomem

bylo potom uvedení nadstavby MS-DOSu, operačního systému MS Windows verze 3.1x., který určil budoucí vývoj operačních systému řady Windows:

Microsoft Windows 3.1x – Dnes již nepoužívaný, tento systém umožňoval v pěkně zpracovaném grafickém prostředí (GUI) provádět operace známé z MS-DOSu bez nutnosti znát příkazy (příkazy pro kopírování souboru, vytváření adresářů, mazání, přejmenování, atd....) Během krátké chvíle se objevilo množství programů určených pouze pro operační systém MS Windows a nekompatibilních s MS-DOS. Jedním z takovýchto byl zcela jistě další produkt firmy Microsoft – Word a Excel. Word v té době nabízel v podstatě podobné věci jako známe dnes z jeho nejnovějších verzí – psaní textu, editace, množství stylů, vkládání grafických objektů, tvorbu tabulek, kontrolu pravopisu a to vše na mnohem vyšší úrovni, nežli to nabízel např. textový procesor t602. Tabulkový procesor Microsoft Excel dále rozšiřoval možnosti využití počítačů ve firmách. Tato aplikace zpracovávala číselná data sestavená do tabulek a umožňovala práci s nimi (matematické operace, tvorbu grafů a tabulek). Všechny tyto produkty měly jedno společné – naprosto nenáročnou obsluhu, jednoduché ovládání přístupné i začátečníkům a společné propojení a kompatibilitu. Zde už můžeme hovořit o jistém zabezpečení, jelikož vytvořené soubory se daly opatřit ochranou před otevřením, či editací a rovněž operační systém Windows 3.11 jistě možnosti nabízel.

Další zcela novou koncepcí byl **Microsoft Windows 95**. Byl to opět diskový operační systém. Je charakteristický grafickým uživatelským rozhraním (GUI) podobně jako jeho předchůdce Windows 3.11, ale na rozdíl od něj již nepotřeboval předinstalovaný MS-DOS, fungoval sám. A co nabízel nového:

- dlouhé názvy souborů a složek (až 255 znaků)
- průzkumník (společná správa souborů a složek)
- zdokonalené GUI, funkce Drag and Drop (manipulace se soubory či adresáři tažením na pracovní ploše)
- tlačítko START, hlavní panel
- funkce Plug and play – nový hardware okamžitě k použití
- rozšířená a zlepšená práce s multimédií (zvuk a video)
- 32-bitové zpracování dat
- multitasking – spouštění několika programů najednou
- Integrovaný MS Internet Explorer – WWW prohlížeč integrovaný zdarma přímo v programu, podpora internetových služeb

Zde, právě díky podpoře internetových aplikací a internetu vůbec, zřejmě nastal průlom co se týče zabezpečení systému. Uživatel si již v internetovém prohlížeči mohl volit z několika úrovní zabezpečení systému proti hrozbám číhajícím na internetu. Díky dalšímu softwaru, který se začal objevovat závratnou řadou, bylo možné ochránit systém před neoprávněným spuštěním či modifikací.

Microsoft Windows NT 4.0 je robustní NOS vhodný pro správu podnikových sítí client-server. Existuje ve verzi **Server** (se všemi nástroji podnikového serveru) a **Workstation** (určené pro pracovní stanice). Vyznačuje se stejným GUI jako Windows 98, čímž se (oproti předchozí verzi Windows NT) významně zlepšila konzistence používání Windows NT a Windows 98. Kromě tradičních uživatelských požadavků na NOS, jako jsou adresářové služby, souborové služby, bezpečnost, integrované předávání zpráv, správa sítě atd..., které Windows NT zajišťují beze zbytku, zde byla silným faktorem podpora firmy Microsoft v upgrade systému na nové podmínky vývoje informačních technologií a nových hrozeb za použití tzv. Service Packů, které byly pravidelně vydávány a distribuovány přes Internet. Dnes je tento systém na ústupu a je nahrazován svým nástupcem MS Windows 2000 či MS Windows XP Professional vhodným pro menší podnikové sítě.

Microsoft Windows 98 byl dalším počinem firmy Microsoft v oblasti operačních systémů. Pokrok byl zřetelný již při instalaci systému na počítač, kdy o postupu srozumitelně informuje příslušný průvodce. Důležitou inovací zde byl fakt, že systémová databáze obsahovala ovladače nejpoužívanějších hardwarových zařízení a operační systém si je korektně nainstaloval sám. Jednalo se zejména o grafické či zvukové karty, CD-ROM jednotky či ostatní mechaniky. Správa systému byla lehce přístupná ze složky ovládací panely. Jedním ze základních bodů „filosofie“ Windows 98 je hodnotný přístup k informacím, ať už se nacházejí na lokálním disku počítače, na serveru lokální sítě či na intranetu nebo internetu. Systém Windows 98 se lišil i vylepšenou pasivní bezpečností. Byl totiž robustnější, stabilnější a odolnější vůči zhroucení nežli jeho předchůdce, a to ať už vlivem nekorektního chování programů nebo dokonce hardwarových závad. Když už k závadě, a třeba i k poškození některých systémových souborů Windows dojde, nastoupí prvky aktivní bezpečnosti, zajišťující diagnostiku, popřípadě i nápravu. I přes všechno zmíněné Windows 98 nedosahují kvalit systému postavených na bázi NT či operačních systémů jiných firem (IBM OS2 Warp). Obecně tento systém lze považovat za meziskok mezi Microsoft Windows 95 a Windows NT, které se měly sloučit v jeden robustní silný operační systém schopný chránit data a aplikace a vhodný zejména do podnikových sítí.

Dalším operačním systémem firmy Microsoft , který měl nastolit nový standart v této oblasti byl **Windows 2000**. Tato platforma představuje operační systém pro novou generaci práce s počítači. Od přenosných počítačů přes stolní PC až po vysoce výkonné servery. Tento NOS je založený na technologii NT a je plnohodnotným a výkonným nástupcem verze NT 4.0. Hlavní význam systému Windows 2000 spočívá ve stanovení nového standardu integrace operačního systému se sítí WWW, aplikacemi a službami pro práci v síti, komunikaci a infrastrukturu a pochopitelně ochrany dat. Prodává se v těchto verzích:

- **MS Windows 2000 Server** – Zásadní výhodou je možnost zavádět systém postupně, tempem vyhovující konkrétní společnosti. Tento systém mohou postupně využít společnosti všech velikostí. Jako příklad může posloužit síť WWW. Tam, kde se u jiných dodavatelů nacházejí technologie určené pro síť WWW spouštěné pod operačním systémem, pracují c rámci systému Windows 2000 Server technologie WWW, které zjednodušují použití a zlepšují zabezpečení i funkčnost. K dalším zlepšením oproti Windows NT 4.0 patří neobyčejně široká podpora nejnovějšího hardware, integrace služby Terminal Services, integrovaná podpora sítí VPN (Virtual Private Network) a mnohé další funkce
- **MS Windows 2000 Advanced Server** – poskytuje veškeré funkce a výhody systému Windows 2000 Server. Kromě toho také zahrnuje další funkce zlepšující dostupnost a škálovatelnost elektronického obchodování a obchodních aplikací.
- **MS Windows 2000 Datacenter Server** – je nejvýkonnější a funkčně nejrozsáhlejší serverový operační systém společnosti Microsoft. Je určen pro firmy, které potřebují velmi výkonný a vysoce spolehlivý hardware a software pro síť se silným provozem. Nabízí dále rozsáhlé a důležité aplikace: zpracování transakcí online, databáze, poskytovatelé aplikačních služeb a služeb sítě Internet.
- **MS Windows 2000 Professional** – díky dobré podpoře ze strany výrobce, ale i ze strany dodavatelů hardware a softwarových aplikací a samozřejmě vzhledem k jeho cenným vlastnostem, je až nad očekávání uplatňován při upgradu starších verzí Windows. Protože netrpí podobnými neduhy jako předešlé operační systémy, ale naopak vykazuje perfektní stabilitu a je schopen plnohodnotného preemptivního multitaskingu, nahrazuje i starší verze diskových operačních systémů na domácích i přenosných PC. Jinak je ovšem přednostně

určen pro podnikovou sféru, jako klientský systém pro síť ovládanou MS Windows 2000 Server. Pro správu robustních a náročných podnikových aplikací přináší tolik potřebnou spolehlivost, jednoduchost (ovládáním velmi podobný předchozím verzím), nenáročnost na údržbu a zabezpečení moderními prvky.

Microsoft Windows Millennium je jakýmsi mezistupněm mezi Windows 98 a Windows 2000 či XP. Je určen přednostně pro domácí využití a to zejména díky široké podpoře multimédií, ale na druhou stranu ne tak stabilním prostředím, jaká nabízí Windows 2000 či XP (na bázi NT). Mezi hlavní obměny oproti systému Microsoft Windows 98 patří:

- **Digitální multimédia** – široká podpora periférií pro digitální fotografie, vylepšené nástroje pro audio či videozáznam, vylepšená podpora dynamického třírozměrného zvuku, úpravy, katalogizace a odesílání domácího videa elektronickou poštou, apod.
- **Sítě peer-to-peer** – pro propojení všech domácích PC, sdílení jediného připojení k síti Internet, použití technologie více sítí a sdílení systémových prostředků, použití zařízení typu Universal Plug and Play, atd. [Rosman, Sodomka, Juřenčák, Benda 2001, s. 90]

Zatím posledním operačním systémem z dílny Microsoft, prodáváním i u nás je **Microsoft Windows XP** (eXPerience – zkušenost). Je to systém který slučuje obrovskou stabilitu a bezpečnost systému Windows 2000 a k tomu nabízí obrovskou podporu multimédií a nejnovějšího hardware. Je konstruován tak, aby bylo možno využít veškerého potenciálu dnešních osobních počítačů a obsahuje proto celou řadu nových zajímavých nástrojů. Možnost tzv. Active Windows Update za použití internetu. Obsahuje podporu ověření bezpečného přístupu za použití karet Smart Card, atd. Je dodáván ve 2 základních verzích:

- **MS Windows XP Professional** – určený zejména pro firmy a pro náročné uživatele. Windows XP Professional je založen na prověřeném kódovém základu systémů Windows NT a Windows 2000, který zahrnuje 32-bitovou programovací architekturu a plně chráněný model paměti. Odstraňuje většinu případů, při kterých musí koncoví uživatelé systémů Windows NT 4.0 a Windows 95/98/ME restartovat počítač. Tato výhoda se týká i mnoha instalací softwaru. Klíčové datové struktury jádra jsou určeny pouze pro čtení, takže je ovladače a aplikace nemohou poškodit. Veškerý kód ovladačů zařízení je jen pro čtení a je

zabezpečen. Umožňuje použití nejnovějších zabezpečovacích standardů a obsahuje vylepšené možnosti správy a monitoringu počítačové sítě. Obsahuje pochopitelně všechny prvky obsažené v systému Windows XP Home Edition.

- **MS Windows XP Home Edition** – je určený zejména pro domácí použití, k přednostem patří zejména:
 - snadnější vytváření, editování a sdílení digitálních fotografií
 - pohodlnější manipulace s digitálními sklady nejvyšší kvality
 - vysoká úroveň zázemí pro zážitek z počítačových her a DVD titulů
 - instant messaging, komunikace za použití audio/video přenosu
 - efektivnější sdílení počítačů a periférií v domácnosti [7]

Všechny výše zmíněné operační systémy či serverové operační systémy pocházejí z dílen firmy Microsoft. Ostatní operační systémy (např IBM OS/2) nejsou v podnicích využívány v takovém měřítku jako produkty firmy Microsoft a představují pouze malá procenta podílu.

Operační systém **Linux** nachází největší uplatnění na internetových, síťových a jiných serverech. Dle statistik používá polovina internetových serverů Linux a jeho Apache (www server). Je to dáno zejména jeho stabilitou a cenou. Linux je totiž zdarma šířen dle licence GNU. Autorem této licence je Free Software Foundation a ta jej dává k dispozici každému uživateli, podmínky licence chrání autora před zcizením autorských práv, zároveň zaručuje, že kdokoliv může program měnit a distribuovat dále (i za peníze). Tvůrcem projektu je Linus Torvald, který společně s mnoha programátory z celého světa vyvinul plně funkční a stabilní operační systém, použitelný na platformě IBM, PC, Apple MacIntosh, servery Alpha, Sun a některé další. Byl napsán jako kompletní přepis UNIXu. Jde o plně 32-bitový, případně 64-bitový OS (závisí na platformě). Jeho jedinou podstatnou nevýhodou bránící jeho rozvoji do domácích i podnikových sfér je vysoká obtížnost ovládání a konfigurace systému pro neznalého uživatele a nízká kompatibilita s aplikacemi MS Office. [2, str. 96]

Linux je kromě vlastního linuxového jádra a jednotlivých aplikací k dispozici i ve formě ucelených souborů jádra doplněného o „balíčky“ jednotlivých linuxových aplikací, označovány jako distribuce. Těchto distribucí existují stovky. Jsou k dostání v základních verzích prostřednictvím internetu,

některé se prodávají za cenu nosičů, jiné za cenu zahrnující podporu a přidanou hodnotu výrobce či distributora. Mezi ty nejznámější distribuce patří Debian/GNU Linux, Linux Mandrake, RedHat Linux, SuSE Linux. Mezi ty nejpoužívanější u nás patří právě SuSE Linux, Mandrake a RedHat, hlavně díky převodu do lokální jazykové verze. Všechny tyto systémy se vyznačují vysokou stabilitou a ochranou dat avšak také množstvím freewarových aplikací k nim dodávaných (např. OpenOffice – ekvivalent Microsoft Office, ovšem zdarma) a rovněž i rozsáhlými návody.

[6, str. 124]

1.6.2 Internet

Počátkem 60. let se v USA zrodila myšlenka vytvořit síť, která by propojovala nejdůležitější vojenské, vládní a akademické počítače. Tato síť měla být schopna provozu i v případě výpadku některého z uzlů. V srpnu 1969 byla hotova první síť se čtyřmi uzly a postupně se k této síti začaly připojovat i další instituce, především univerzity a v dalších letech se tato síť začala prudce rozvíjet i na evropský kontinent. V této době byl tento zárodek internetu čistě nekomerční. V roce 1989 byl na půdě ústavu částicové fyziky CERN vyvinut tzv. hypertextový dokument, ve kterém označená slova mohou odkazovat na další dokumenty nacházející se třeba na jiném kontinentu. CERN pro svoji potřebu vytvořil programový komplet, který nazval web (pavučina). Web se díky svým schopnostem rychle rozšířil po celé síti a dnes je v podobě World Wide Web (www, celosvětová pavučina) nedílnou součástí internetu. V roce 1992 se objevily první grafické prohlížeče, které začaly umožňovat zobrazování obrázků připojených k textu. Právě existence www spolu s rozšířením osobních počítačů přilákala na internet milióny nových uživatelů.

Slovo "Internet" je dnes skloňováno ve všech pádech. Snad všichni si již uvědomili význam tohoto pro někoho nového a pro někoho starého informačního a komunikačního média. Pomocí Internetu může každý oslovit doslova celou planetu. Zasednete k počítači, připojíte se a během několika málo minut jste na druhé straně Zeměkoule. Práce s Internetem bude jistě již zanedlouho patřit k základním dovednostem člověka 21. století. V roce 1994 slavil Internet 25. výročí vzniku. Roku 1995 se služba WWW dostává na první místo v počtu přenesených dat. Objevuje se první oficiální špionáž, namířená proti nelegálním výrobcům mobilních telefonů a dalšího elektronického zařízení, vedená americkou tajnou službou prostřednictvím Internetu. Rok 1996 přináší první veletrh Internetové technologie. V současné době se Internet u nás stává stále více součástí běžného života.

Rovněž nelze opomenout jeho důležitost pro podnik jako komunikační prostředek a musíme jej také chápat jako jeden z obrovských možných zdrojů úniku či zničení dat.

V listopadu 1991 se u nás v ČR do evropského internetu připojily první univerzity prostřednictvím sítě CESNET a tím prakticky začala historie internetu v České republice. CESNET v dalších letech začal poskytovat nevyužitou přenosovou kapacitu zájemcům i mimo okruh akademických sítí, čímž byly vytvořeny předpoklady pro zahájení činnosti prvních komerčních poskytovatelů připojení. Rozvoj služeb internetu pro širokou veřejnost začal v ČR po roce 1995. Po roce 1999 prodělal veřejný internet v České republice další velký rozvoj, zejména díky dokončení digitalizace telefonní sítě, stanovení levnějšího tarifu pro připojování k internetu, díky poklesu cen osobních počítačů a především vzhledem následnému nástupu volných poskytovatelů připojení.[8], [9]

1.6.3 Počítačové sítě a důvody jejich zavádění

Počítačové sítě v podstatě znamenají propojení několika (mnoha) počítačových pracovních stanic do jednoho celku. Tyto systémy přinášejí oproti práci na samostatných počítačích několik zásadních výhod. Mezi nejvýznamnější patří:

- **sdílení dat** – jedná se o to, že potřebné datové soubory mohou zpracovávat uživatelé na více počítačích současně. Je to umožněno tím, že datové soubory lze umístit na servery a ostatní počítače k nim pak mají prostřednictvím sítě přístup
- **sdílení prostředků** – stanice mohou využívat prostředky, které jsou nabízeny serverem. Nejčastěji se jedná o diskový prostor a tiskárny. To znamená, že když např. nemá stanice přímo připojenou tiskárnu, může pro tisk využít sdílenou tiskárnu připojenou k serveru
- **zvýšení spolehlivosti systému** – tím, že existuje možnost sdílet prostředky, je snadno realizovatelný i systém jejich zálohování. Např. při poruše pracovní stanice uživatele může být použita jiná stanice, protože data uživatele jsou uložena na serveru. [2, str. 141]

1.7 Bezpečnost dat a informací a legislativa

Zákonů a vyhlášek, které se nějakým způsobem dotýkají problematiky ochrany znalostí a dat v české republice je několik set. Liší se oblastí své působnosti, svými cíli, aspekty bezpečnosti beroucí do úvahy a liší se také v tom, jak podrobně a zda vůbec se zabývají otázkami řešení. S těmito zákony a vyhláškami včetně jejich komentářů je dobré se seznámit. Mezi jinými existují 3 nejvýznamnější:

- Obchodní zákoník – zákon č. 513/1991 Sb. v posledním platném znění definuje v §17 pojem obchodní tajemství: Předmětem práv náležejících k podniku je i obchodní tajemství. To tvoří veškeré skutečnosti obchodní, výrobní či technické povahy související s podnikem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu, nejsou v příslušných obchodních kruzích běžně dostupné, mají být podle vůle podnikatele utajeny a podnikatel odpovídajícím způsobem jejich utajení zjišťuje. [Obchodní zákoník §17 zákon č. 513/1991 Sb. 2001]
- Zákon o ochraně utajovaných skutečností – Na bezpečnosti některých informací má zájem stát, protože jsou důležité pro jeho fungování, obranu, apod. Tím se zabývá zákon č. 148/1998 Sb. o ochraně utajovaných skutečností a o změně některých zákonů (od roku 1998 byl šestkrát novelizován). Tento zákon byl přijat jako jedna z podmínek pro vstup České republiky do NATO. [Národní bezpečnostní úřad 2002]
- Zákon o ochraně osobních údajů – V polovině roku 2000 byl přijat zákon č. 101/2000 Sb. o ochraně osobních údajů a změně některých zákonů. Zákon platí od 1.6.2000. Zákon je poměrně nový a jeho důsledky pro jednotlivce i organizace jsou značné. Týká se osobních údajů zpracovávaných automatizovaně v informačních systémech nebo bez využití výpočetní techniky (kartotéky), státní správy stejně jako soukromých firem. [11]

1.8 Vybrané ISO normy bezpečnostních mechanismů

Jen pro ilustraci trendů zde zmíním některé normy zabývající se a řešící problematiku informační bezpečnosti. Všechny zmíněné normy jsou produktem ISO/IEC JTC1/SC27, a to především WG2 z SC27.

- ISO/IEC 9979: Registr šifrovacích algoritmů

- ISO/IEC 10116: Režimy činnosti šifrovačů
- ISO/IEC 9797: Autentizační kódy zpráv (Message Authentication Codes - MACs)
- ISO/IEC 10118: Hašovací funkce
- ISO/IEC 9796: Digitální podpisy s obnovou zprávy
- ISO/IEC 14888: Digitální podpisy v dodatku zprávy
- ISO/IEC 13888: Mechanismy nepopiratelnosti
- ISO/IEC 15946: Kryptografie na bázi eliptických křivek
- ISO/IEC 9798: Norma autentizačního protokolu
- ISO/IEC 11770: Norma správy klíčů. [13, str. 100]

1.9 Workshop při řešení informační bezpečnosti

Nadřazené cíle mohou být dosaženy tehdy, pokud jsou na jedné straně důsledně sledovány a dosahovány cíle orientované na lidské chování a na druhé straně, zda se struktury a chování přizpůsobily změněným podmínkám. Proto je nutné uvést úkoly, projekty a procesy do souladu, v žádném případě si nesmí konkurovat. Platformou pro zlepšování je tzv. workshop (tvůrčí dílna), který se zaměřuje na hloubkovou analýzu procesu vybraného managementem a na kterém se schází tým zainteresovaných pracovníků. Takovýto tým je schopen efektivně řešit problémy spojené s danou oblastí. [14, str. 39]

Od participace zaměstnanců na workshopu, jehož cílem je řešit problémy zabezpečení IS je možné očekávat pozdější větší zainteresovanost zaměstnanců a důslednější dodržování navržených opatření. Jelikož je workshop týmovou akcí, na výsledcích by měla panovat všeobecná shoda a měl by být identifikován vysoký stupeň ztotožnění.

1.10 Zhodnocení teoretických zdrojů

Při průzkumu literárních zdrojů jsem narazil na velké množství knih a publikací, které se ožehavou problematikou ochrany znalostí a dat zabývají. Stejně je tomu tak na internetu a v odborných časopisech. Zájemce, který by se chtěl s touto rozsáhlou problematikou seznámit má tedy široké spektrum možností. V poslední době na rozdíl od předchozích let se objevují některé nové tituly, které přináší zájemci velké množství důležitých a zejména potom aktuálních informací. Situace na internetových informačních serverech je velice dobrá. Renomovaní autoři a odborníci zde přispívají zajímavými články, které jsou nejen zajímavé, ale rovněž i aktuální. Celkově lze tak hodnotit situaci za velmi dobrou. Odborníci i široká veřejnost najdou množství publikací a titulů, které se této problematice věnují.

1.11 Teoretická východiska pro analytickou část

V závěru teoretické části bych rád shrnul vše, o čem jsem se doposud zmínil a zformuloval si tím tak předpoklady pro analytickou část ve firmě LIMIRE, s r. o. Prostějov.

Na základě teoretických poznatků definuji a analyzuji možné zdroje ztráty či úniku dat v tomto podniku. Dále zhodnotím současnou situaci v oblasti informační technologie v podniku a zjistím jaká data tvoří informační systém firmy. Dále se pokusím zhodnotit silné a rovněž i slabé stránky ochrany dat v místech, které označím za možné zdroje úniku. Pokud identifikuji některá slabá místa informačního systému, navrhnou opatření vedoucí ke zlepšení situace.

2 ANALYTICKÁ ČÁST

2.1 Představení společnosti

Firma Limire, s. r. o. vznikla v roce 2002. Jejím cílem je vybudovat obchodní a částečně výrobní společnost se zaměřením na export zahradní techniky do západoevropských zemí se současným importem podobné techniky do ČR. Neoddiskutovatelnou výhodou od samého začátku byla vlastní vývojová konstrukce, díky které se mohly výrobky plynule inovovat a přizpůsobovat konkrétním potřebám zákazníků. Tak mohly vzniknout další obchodní oblasti a aktivity.

Z důvodu rozpadu velkých firem vyrábějících zemědělskou a zahradní techniku, např. podnik Agrozet, vzniklo množství menších firem. Ty jsou specializovány na konkrétní výrobu, službu či prodej určitého zboží, výrobku, apod. Hlavním úkolem společnosti je tedy uplatnění se na současném trhu, kde je velmi silná konkurence.

Převážná část obrátu firmy LIMIRE je tvořena exportem orientovaným na západní Evropu cca 70% a zbylých 30% tvoří aktivity na tuzemském trhu. Tato situace vznikla důsledkem pozdějšího vstupu LIMIRE na trh se zahradní a zemědělskou technikou. Firma si musí získat kvalitními výrobky své zákazníky a s tím souvisejícími službami. Příkladem může být prodej náhradních dílů, servisní opravy a pozitivní přístup řešit problémy zákazníků.

Firma Limire na současném trhu prodává zahradní techniku, která je jejím hlavním artiklem. Dále se zabývá výrobou a prodejem chmelové techniky a techniky pro chov koní. Svým potenciálním i současným zákazníkům nabízí konstrukční a poradenské služby, neboť chce uspokojit jejich přání a požadavky. Současně nabízí zakázkovou výrobu strojírenského charakteru.

Firma se rozhodla pro rozšíření sortimentu své výroby a prodeje, aby tak zajistila plynulou vytíženou práci po celý rok. Většina jejich výrobků má sezónní charakter a díky širšímu sortimentu dochází k eliminaci výrobních výkyvů. Nebrání se poskytování nových druhů zboží, výrobků či služeb, které by uspokojily přání zákazníků.

Hlavním předmětem činnosti firmy Limire je:

a) Výrobní činnost

- výroba zahradní techniky
- výroba chmelové techniky
- výroba techniky pro chov a ustájení koní
- ostatní strojírenská výroba

b) Prodejní činnost

- prodej zahradní techniky vlastní výroby v ČR a v zahraničí
- prodej importované zahradní techniky
- prodej chmelové techniky
- prodej techniky pro chov koní
- prodej strojírenských dílů dle požadavků zákazníka

c) Servisní činnost

- firma prodává náhradní díly na celý sortiment zboží a poskytuje servisní opravy, které provádí do 24 hodin od nahlášení poruchy zákazníkem.

d) Konstrukční činnost

- pro zpracování podkladů k výrobě
- pro vývoj nových výrobků
- pro inovaci starých výrobků

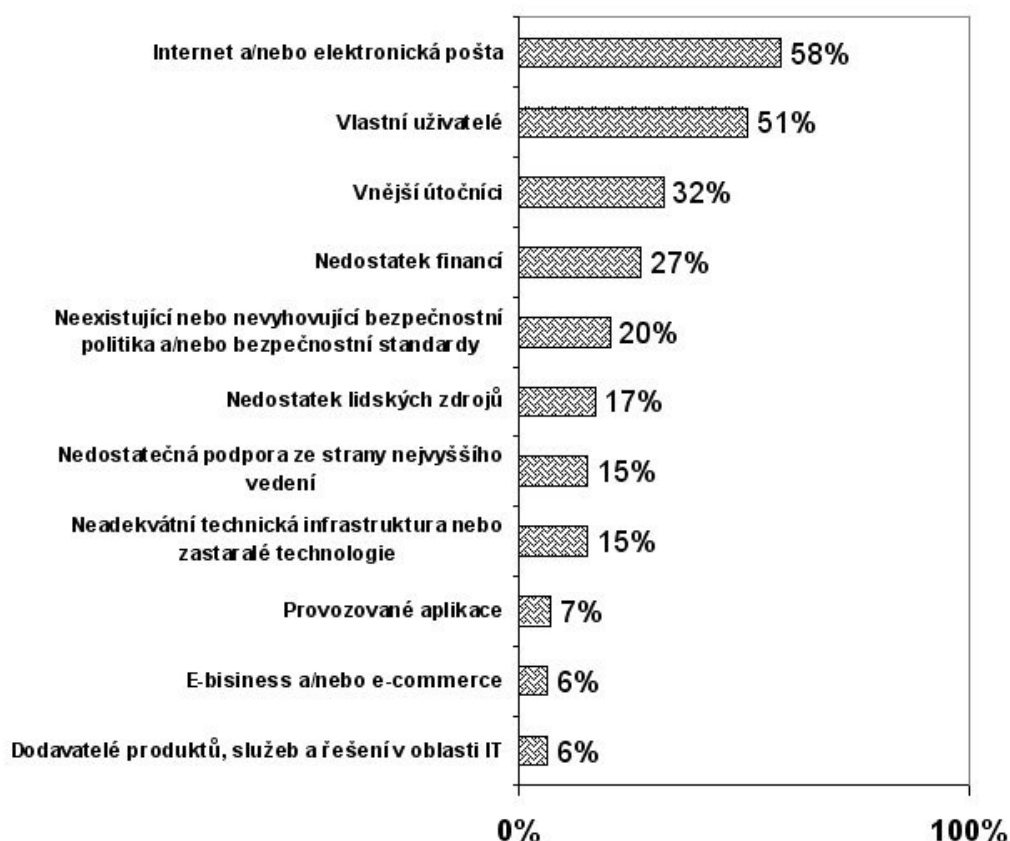
2.2 Stav informační bezpečnosti v ČR v roce 2003

V České republice byl v roce 2003 již potřetí (dříve v letech 1999 a 2001) proveden průzkum stavu informační bezpečnosti. Průzkum prováděly následující organizace: Ernst and Young, časopis DSM - data security management a Národní bezpečnostní úřad. Tento průzkum probíhal od března do června 2003. Bylo osloveno celkem 1100 společností, z nichž 380 dotazník vrátilo, 362 z nich bylo zpracováno. Jednalo se o střední a velké společnosti, s počtem pracovníků větším než 100, 60 % z nich bylo do 500 pracovníků.

Průzkum byl prováděn anonymně, bylo položeno celkem 56 otázek. Část průzkumu se týkala bezpečnostních incidentů, se kterými se organizace setkala. Nejčastějším bezpečnostním incidentem je výpadek proudu (89 %), počítačový virus (79 %) a porucha HW (77 %). Naopak mezi velmi řídké incidenty - pod 10 % - organizace počítají zneužití zařízení, nepovolený přístup k datům zvenku a nepovolený přístup k datům zevnitř. To ovšem vůbec neznamená, že je podobné incidenty nepotkaly, možná je prostě jen nezaznamenaly. Dále 20 % organizací udává v minulých dvou letech přírodní katastrofu, což znamená vzrůst.

Celkem 95 % organizací uvedlo, že pro ně má informační bezpečnost význam nebo velký význam. Největší význam uvádějí organizace z oblasti bankovníctví a financí, kde velký význam má pro 93 % organizací. Mezi těmito organizacemi nejsou žádné, pro které by informační bezpečnost měla malý význam. Oddělení odpovědné za informační bezpečnost v podniku je v České republice v drtivé většině oddělení IS /IT, navíc tento podíl dokonce roste. Celkem to je 78 % organizací. Pouze zcela výjimečně se jedná o útvar bezpečnosti, pouze ve 3 %. To je zcela nevyhovující situace, neboť bezpečnost by měla být od IS /IT oddělena a rozhodně by pracovník či pracovníci zodpovědní za bezpečnost neměli podléhat vedené IS/IT. Pokud má budování informační bezpečnosti mít nějaký význam, je nutno neustále zvyšovat bezpečnostní vědomí zaměstnanců. To činí organizace různými způsoby. Nejčastěji (72 %) se jedná o interně publikované směrnice a kontrolní činnost (37 %). Dále jsou zaměstnanci školeni, mají přílohu k pracovní smlouvě nebo je vydána zaměstnanecká příručka. Vzhledem k tomu, že vlastní uživatelé představují jednu z nejvýznamnějších hrozeb pro počítačovou bezpečnost, zdá se, že organizace tuto oblast značně podceňují.

Co je největší hrozbou z hlediska informační bezpečnosti? Pro 58 % organizací je to internet a/nebo elektronická pošta. Ovšem již pro 51 % jsou to vlastní uživatelé!!! Celkový přehled ukazuje následující obrázek. [12]



Obr. 4: Největší hrozby z hlediska informační bezpečnosti [12]

Další zjišťovanou otázkou je, kdo v organizaci bezpečnost řeší. Nabízí se možnost vlastními silami, nebo zcela externí firmou, nebo nějaký kompromis. Zatímco v roce 2001 byl poměr řešení vlastními silami a spolupráce s externí firmou vyrovnaný, loni již zcela převažovalo řešení ve spolupráci s externí firmou/firmami (57%). Pouze 2 % organizací řeší bezpečnost výhradně dodavatelsky. [12]

2.3 Vývoj IT ve firmě

Není tomu tak dávno co se v kancelářích podniků dopisy psaly na psacích strojích a nabídky či poptávky se posílaly poštou. Teprve před deseti až patnácti lety se u nás začaly masověji rozvíjet

systémy, které tyto zastaralé metody nahrazovaly, tedy počítače a informační systémy vůbec. Počítače se staly dostupnějšími zejména pro firmy. Pro domácnosti tehdy nový počítač představoval obrovskou finanční investici, v podstatě využitelnou jen pro zábavu. V období 1990 - dnešek je tedy zaznamenáván rozmach výpočetní techniky a rovněž dochází ke snižování cen veškeré elektroniky a tedy i výpočetní techniky. Rozvoj nastává nejprve pochopitelně v podnikové oblasti. Tam byly počítače využívány ke zpracování databází a provádění složitějších výpočtů, kde razantně snižovaly dobu nutnou pro řešení úloh (byly to tzv. sálové počítače). Později s obrovským rozvojem softwarových aplikací a platformy PC (Personal Computer, osobní počítač), se počítače začaly využívat i pro administrativní a podnikatelskou činnost. Tento pojem dostal zcela nový rozměr po připojení ČR oficiálně do sítě internet. Současný rozmach výpočetní techniky a informačních technologií je v dnešní době způsobený zejména těmito faktory:

- obrovské množství výrobců, velká konkurence
- snaha o digitalizaci
- snaha o simplifikaci
- pokles cen z důvodu přesunu veškeré výroby do Číny, kde se měsíční mzda dělníka v průmyslových zónách pohybuje okolo 10 USD za měsíc
- pokles cen z důvodu posilování koruny vůči USD

Již od roku 2002 - tedy od svého vzniku se firma snaží držet krok s vývojem IT. Již na počátku vzniku byly pořízeny osobní počítače a samozřejmě nezbytné další softwarové a jiné hardwarové zařízení a vybavení. Mezi ně patřily PC, tiskárny i kopírky. Vzhledem k tomu, že v dnešní době se téměř veškerá komunikace odehrává právě v elektronické podobě byl tento krok absolutně nezbytný. Stejně tak bylo nezbytné připojení k internetu. Nejprve bylo toto připojení řešeno pomocí telefonní linky a modemu. Ovšem z hlediska produktivity práce a z hlediska potřeb firmy absolutně nevyhovovalo. Proto se firma minulý rok rozhodla pro pořízení bezdrátového internetového připojení standartu WI-FI 802.11b tak, aby mohla využívat internet neomezeně a pochopitelně i rychleji. S rostoucími požadavky na kvalitu spojení i stabilitu komplexního informačního systému se na základě vzniklých požadavků informační systém firmy LIMIRE neustále rozrůstá a to jak hardwarově, tak zejména z hlediska programového vybavení - tedy softwarově. A to jak komunikačního, tak i z hlediska zabezpečení. Tento trend je nevyhnutelný vzhledem k pokroku v oblasti informačních

technologií a zejména v oblasti kompatibility na úrovni mezipodnikové komunikace. Velkou roli zde hraje i podpora výrobců softwaru pro své produkty. Takto nepřímě nutí své zákazníky k upgradu a k zakoupení nových produktů. Ty poté mají neustále vyšší hardwarové nároky což dále nutí firmy i k upgradu hardwarové platformy.

Tento trend je patrný zejména v posledních letech. Morální zastarávání výpočetní techniky i jejího softwarového vybavení můžeme pozorovat okamžitě po zakoupení. V podstatě už po jednom roce používání jsou systémy morálně znehodnoceny. Obvyklá doba pro obměnu informačních technologií jsou potom 2 - 4 roky. Problémem firem tedy zůstává nutnost shánění finančních prostředků nutných pro nákup, udržování či upgrade svého informačního systému.

Na pracovišti, na kterém jsem svou práci zpracovával byly k dispozici tři počítače PC. Dva z nich vybaveny operačním systémem Windows XP, jeden vybaven operačním systémem Windows Millenium Edition. Jeden z počítačů funguje jako serverová pracovní stanice. Je připojena do sítě internet a ostatní PC jsou k ní připojeny. Veškerá síťová komunikace včetně internetového připojení tedy prochází tímto jedním počítačem a ostatní systémy toto připojení sdílí.

Je také obecnou a známou pravdou, že firmy v České republice, zejména ty menší, problematice ochrany znalostí a dat prostřednictvím nákupu nejmodernějších technologií nevěnují velkou pozornost. Z jedné strany je to dáno jistým pocitem „bezpečí“. Na straně druhé však stojí finanční namáhavost daných projektů. Mnoho firem není ochotno a ani nemůže dané finanční prostředky poskytnout. Cílem mé práce bude zjistit právě stav informační bezpečnosti ve firmě LIMIRE.

2.4 Postup auditu bezpečnosti ve firmě

1. Budou určeny typy dat využívaných ve firmě.
2. Budou identifikovány možné zdroje úniku dat a informací ve firmě.
3. Na základě vyplnění dotazníku „Test bezpečnosti“ odpovědnou osobou bude vyhodnocen aktuální stav a současná situace týkající se ochrany znalostí a dat na úrovni lidských zdrojů.

4. Za použití kritériální tabulky bude určeno pořadí priorit zabezpečení podle stupně ohrožení dat
5. Na základě identifikovaných možných zdrojů úniků v bodě 2 bude provedena analýza současného stavu úrovně zabezpečení se zhodnocením silných i slabých stránek v současné situaci. Bude využit nástroj Microsoft Baseline Security Analyser (MBSA) jež kontroluje samostatný počítačový systém a hledá v něm chybné konfigurace a chybějící aktualizace zabezpečení. Jeho výsledek poskytne přehled o úrovni zabezpečení počítačových dat. Rovněž budou provedeny penetrační testy k ověření napadnutelnosti počítačové sítě prostřednictvím sítě Internet.
6. Budou navržena opatření pro zlepšení současné situace zabezpečení informací, znalostí a dat.

2.5 Cíl tvorby zásad zabezpečení

Tvorba tohoto projektu informační bezpečnosti je první ve firmě. Mým úmyslem a úkolem bude vytvořit pohled na rizika zabezpečení, kterým společnost čelí a co nejrychleji vytvořit a podniknout kroky, které zranitelnost firmy omezí na minimum. Při tomto postupu budu omezen zejména finančními prostředky. Úspory a přínos v této oblasti bude velice těžko vyčíslitelný neboť stejně tak těžce vyčíslitelná je i hodnota dat a velmi těžko se dá predikovat možnost výskytu hrozby zničení či ztráty dat v daném časovém horizontu. Při tvorbě plánu pečlivě zvážím všechny možnosti tak, abych našel vyvážený poměr mezi praktičností, náklady, pohodlím a účinností v oblasti zabezpečení.

2.6 Typ dat využívaných v podniku

Firma používá pro svůj stabilní chod a fungování množství počítačových a jinak tvořených dat a informací, jež jí zabezpečují spojení se svými zákazníky, dodavateli či jinými subjekty svých pracovních i vnitropodnikových vztahů. I když se jedná o malou firmu, množství přenesených dat je

obrovské. Velké množství z nich je důvěryhodné povahy a je nezbytné zajistit jejich plnou nedotknutelnost. Z hlediska využití a typu dat v podniku je můžeme rozdělit takto.:

Databázově řízená data - veškeré podnikové databáze, ve kterých se shromažďují velice cenné údaje nutné pro provoz firmy. Jsou shromažďována postupem času a odráží se v nich veškerá podniková činnost. Mezi ty nejhlavnější patří zejména databáze tvořené účetním programem Pohoda a její nutné zálohy. Ty jsou pro firmu nepostradatelné z hlediska účetnictví a pozdějšího vykazování. Jejich ztráta by měla obrovské následky.

Data osobního charakteru - další z velice důležitých složek podnikového informačního systému. Sem patří elektronická pošta zaměstnanců určená pro komunikaci, její veškeré přílohy, dokumenty, smlouvy, nabídky, zakázky. Patří sem v podstatě veškerý textový materiál putující mezi pracovníky jak pouze ve firmě, tak i na mezipodnikové, mezikontinentální úrovni. Patří sem zejména komunikace mezi zákazníky a dodavateli.

Data vizuálního charakteru - jelikož se jedná firmu, zaměřenou spíše technickým směrem, je jasné, že podstatnou část dat tvoří výkresy a veškerá technická dokumentace pro výrobky. Tato dokumentace je zpracovávána ve speciálních grafických aplikacích na bázi CAD systémů. Množství výkresů je dále uloženo i v papírové podobě, jak kreslené, tak i tištěné. Firma se pravidelně účastní veletrhů a tak je dále vlastníkem různých grafických prezentací. Dále jsou provozovány i firemní webové stránky a jejich grafický i textový obsah patří rovněž do firemního informačního systému.

Systémová a konfigurační data - Tyto data jsou nosiči veškerých nastavení pro aplikace související k ochraně dat, k provozu aplikací tvořící jádro informačního systému a dále pro fungování počítačů samotných. Jejich ztráta znamená zdlouhavý proces obnovování.

Ztráta jakékoliv části výše jmenovaných dat by znamenala pro jakoukoliv firmu značnou a citlivou ztrátu. Zničení či zcizení pracně tvořených databází či smluv nebo nabídek znamená jisté finanční ztráty, a to z důvodu pracné obnovy či znovuvytvoření těchto dokumentů jejichž obnova je značně časově i finančně nákladná. Dále se dá hovořit i o ztrátě výhodné tržní pozice pro firmu, která je jediným držitelem těchto dat a informací v tomto podnikatelském prostředí. Zničení konfiguračních

dat znamená zbytečné plýtvání časem pracovníků, jejichž úkolem bude systémy znova obnovit a nastavit. Ztráta výkresové dokumentace by znamenala další pohromu. Jejich opětovné vytvoření by znamenalo obrovské finanční náklady i zbytečné zatěžování dalších pracovníků. Je tedy nutné říci, že firma disponuje důležitými daty, které je nutné chránit, neboť jejich ztráta by mohla vést k mnoha problémům. Náklady na obnovu dat či náklady spojené se znovuoobením výhodné konkurenční pozice by pravděpodobně byly větší než náklady na zabezpečení těchto dat.

2.7 Možné zdroje úniku či ztráty informací a dat v podniku

Možných zdrojů úniku informací a dat z podniku existují desítky. Záleží na mnoha faktorech. Mezi ty nejvýznamnější patří velikost podniku, obor podnikání a obor působnosti. Z těchto atributů se nadále determinují objem a typ dat, které se v podniku vyskytují. Těmto je přidělen určitý stupeň důležitosti. Důležitá data je potom nutné chránit neboť může dojít k jejich ztrátě či zničení. Ty nejdůležitější a nejvýznamnější možné zdroje úniku mají obecnější charakter a můžeme je rozdělit následovně:

Rizika rozdělujeme do čtyř hlavních kategorií:

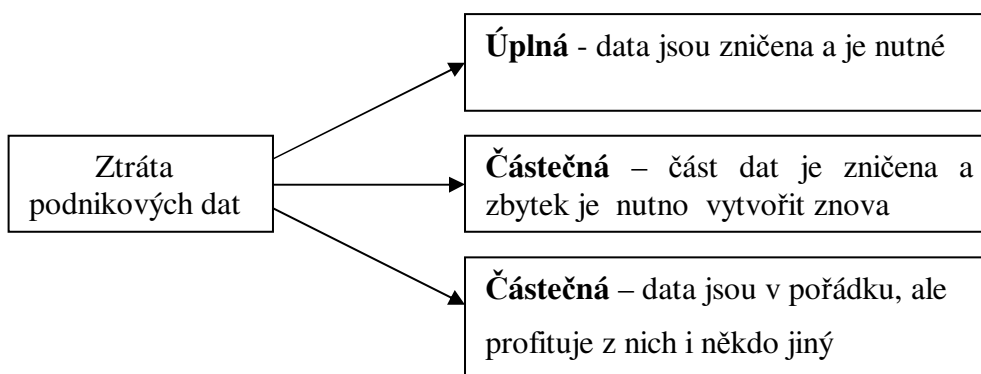
1. **Útočníci** (viry, wormy, zneužití prostředků počítačů nebo připojení k internetu a náhodné škodlivé použití). Jedná se o rizika, jimž čelí všichni jejichž počítače jsou připojeny k Internetu. Vysoké riziko. Vysoká priorita.
2. **Ohrožení zvenku** (konkurence, nespokojení bývalí zaměstnanci, zloději). Tito uživatelé používají pravděpodobně stejné nástroje jako útočníci, ale při svém náhodném útoku mohou přesvědčit zaměstnance k předání důvěrných informací nebo jiných materiálů, které mohou později použít k vydírání nebo k našemu poškození. Naše prostředky potřebujeme chránit fyzickou i elektronickou formou zabezpečení. Vysoké riziko, vysoká priorita.
3. **Interní ohrožení.** Ať už úmyslně nebo nikoliv mohou zaměstnanci chybně použít svých oprávnění k vyrazení či zničení důvěrných informací. Sem patří i instalace takzvaných

pirátských kopií programů a softwarového vybavení vůbec. Patří sem i náhodný výmaz dat. Nízké riziko, nízká priorita.

4. **Nehody a katastrofy.** Požár, záplavy, porucha hardwaru a havárie počítače. Nízké riziko, středně velká priorita.

Dále je třeba zamyslet se nad rozsahy možných destruktivních činností páchaných na podnikových datech. Narušitelé mohou informace či data poškodit, či je nechat nedotčená a pouze z nich profitovat. Pochopitelně zde nemluvím pouze o narušitelích jako fyzických osobách. Patří sem i škody na datech napáchaných jiným způsobem (požár, záplavy, přepětí v síti). Vždy, jak už jsem však uvedl v teoretické části je nutné okamžitě analyzovat situaci a zjistit rozsah škod na datech napáchaný.

Jako nejzákladnější rozdělení se mi jeví následující:



Obr. 5: Druhy ztrát podnikových dat [vlastní zpracování]

2.8 Test bezpečnosti

Tento test [viz příloha, str. 85] představuje diagnostický a vzdělávací nástroj, který může pomoci začít na zabezpečení pohlížet jako na nezbytnou součást provozu malé firmy. Správné odpovědi a

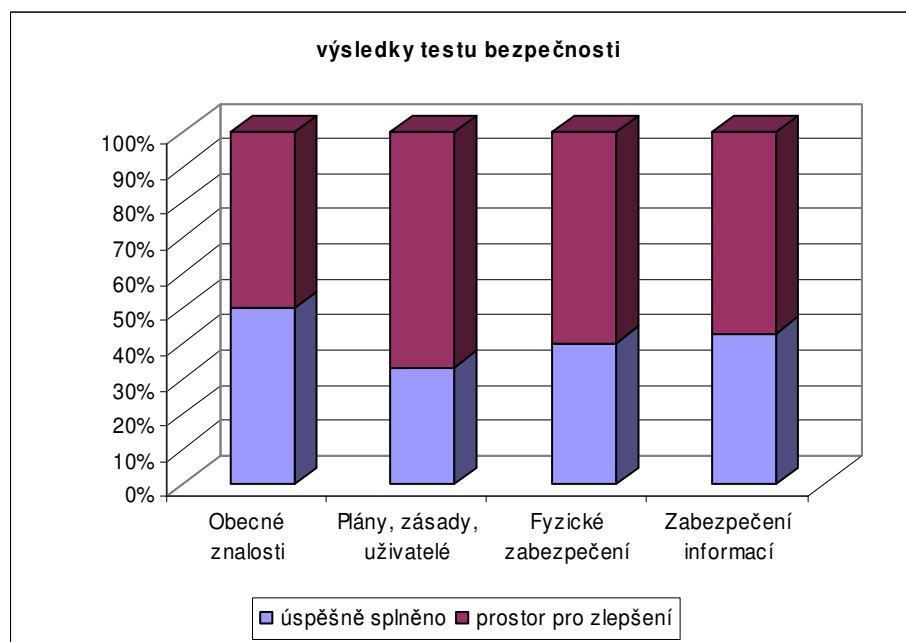
počet bodů jsou uvedeny v závorkách za každou volbou. Test je rozdělen do několika sekcí, které se týkají vždy určité oblasti zabezpečení podnikových dat a informací. O vyplnění testu jsem požádal osoby, které jsou bezprostředně v kontaktu s důležitými daty kolujícími ve firemním informačním systému. Výsledek testu v podstatě potvrdil předchozí domněnky o stavu komplexního přístupu k problematice ochrany znalostí a dat ve firmě. A to jak v oblasti samotné ochrany, tak i v oblasti chápání problematiky ochrany informačního systému a dat v něm uložených.

Výsledky testu podle úspěšnosti v jednotlivých sekcích ochrany dat:

Sekce	Maximum bodů	Získaných bodů	% úspěšnost
Obecné znalosti	8	4	50
Plány, zásady, uživatelé	12	4	33
Fyzické zabezpečení	10	4	40
Zabezpečení informací	14	6	43
Celkem	44	18	41

Tab. 1: Výsledky dotazníku testu bezpečnosti

Procentuelní úspěšnost firmy v testu se pohybuje okolo hranice 40%. Což je podle výsledků dlouhodobých analýz průměrná hodnota, jež dosahuje většina českých firem. Bohužel to však není zdaleka hodnota optimální. Ta by se měla pohybovat někde nad hranicí 60 %. Dotazník testu bezpečnosti je uveden v příloze.[viz příloha, str. 85]



Obr. 6: Grafické zobrazení výsledků dotazníku testu bezpečnosti

Výsledek dále říká, že firma je na tom podobně jako ostatní firmy. Má tedy dobré záměry, provedla určité kroky, avšak ze všeho nejvíce doufá, že k žádnému bezpečnostnímu incidentu nedojde. Existují ovšem kroky, které téměř okamžitě dokážou současný stav posunout výrazně k lepšímu. To by mělo být rovněž cílem mé práce.

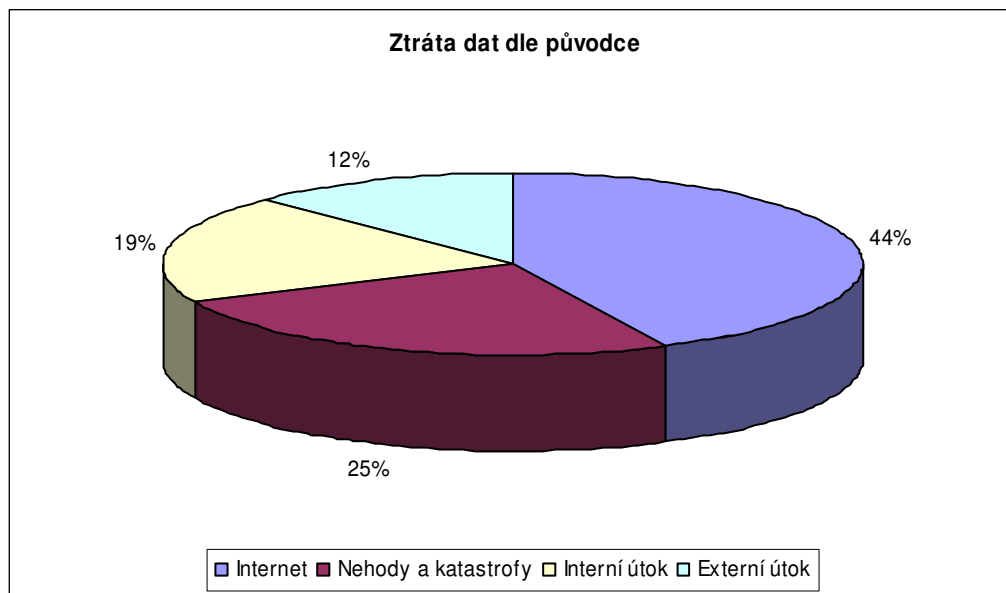
2.9 Ztráta dat dle původce ohrožení

Na základě identifikovaných možných zdrojů úniku či ztráty dat, které jsem prezentoval v kapitole uvedené výše jsem dále určil pořadí priorit zabezpečení. K tomu jsem využil hodnotící tabulku (matici) v níž byla uvedena jednak pravděpodobnost výskytu daného jevu (ohrožení), tak i stupeň tohoto ohrožení dat v případě, že daný jev nastane. Vzájemným vynásobením těchto dvou hodnot vzniklo pořadí priorit zabezpečení, kde nejvyšší číslo představuje největší možnou hrozbu pro firmu. Proto je nutné se takovéto položce věnovat přednostně tak, aby nebyla pozornost zbytečně zaměřována na irelevantní oblasti zabezpečení podnikového informačního systému.

Pořadí	Druh ohrožení	Pravděpodobnost výskytu (x)	Stupeň ohrožení (y)	Dopad (x.y)
1	Viry, wormy	7	6	42
2	Havárie počítače	3	9	27
3	Spyware	7	3	21
4	Neznalost uživatelů	5	4	20
5	Hacker	2	8	16
6	Nelegální software	2	8	16
7	Požár	1,5	10	15
8	Zloděj	1,5	10	15
9	Konkurence	2	4	8
10	Záplava	0,5	10	5

Tab. 2: Výpočet stupně dopadu jednotlivých druhů ohrožení

Tabulka byla sestavena na základě konzultací s odpovědným pracovníkem firmy. Takto jsme byli schopni určit pravděpodobnost, se kterou daný jev může nastat, stejně tak i rozsah možného poškození, který by z daného incidentu resultoval.



Obr. 7: Graf ztráty dat dle specifikovaného původce

Jednotlivé identifikované druhy ohrožení prezentované v tabulce uvedené výše je poté možno rozdělit systematicky do oblastí, které byly již prezentovány v předchozích kapitolách. Jedná se tedy o hrozby přicházející z Internetu, o nehody a katastrofy, o interní (zaměstnanecké) incidenty a rovněž o

externí útoky (zloděj, konkurence). Z grafu je jasně patrné, že firma se nejvíce obává ztráty dat způsobené útokem z vnější sítě. Podstatné pro nás bude rovněž zaměření se na předcházení nehodám a katastrofám respektive na minimalizaci ztrát v případě, že takovýto incident nastane. Nezanedbatelnou složkou budou rovněž samotní uživatelé informačního systému firmy, kteří sami o sobě mohou představovat hrozbu. Externí útoky (konkurence, zloději) v dané chvíli nepředstavují pro firmu bezprostřední ohrožení. To ovšem neznamená, že se jim ve své analýze vyhnu.

2.10 Diagnostický nástroj MBSA

Microsoft Baseline Security Analyser (MBSA) je bezplatný nástroj poskytovaný společností Microsoft. Tento program je možné bezplatně stáhnout z webových stránek společnosti Microsoft. Dále ho lze užívat bez nutnosti zakoupení licence. Je určen zejména pro malé podniky a je vytvořen a nakonfigurován tak, aby jej bylo možno velmi jednoduše obsluhovat bez nutnosti detailní znalosti problematiky. Tento nástroj slouží k provedení diagnózy současného stavu zabezpečení v počítačových systémech. Tento program po spuštění kontroluje přítomnost, konfiguraci a tím i účinnost aktuálních zabezpečovacích prvků v počítači. Zejména sem tedy patří přítomnost a činnost antivirového programu, firewallu a stavu uživatelských účtů. Dále program analyzuje aktualizovanost systému, stav hesel a oprávnění pro daný počítač. Představuje tedy komplexní nástroj pro zjištění aktuálního stavu zabezpečení s možností okamžitého zjednání nápravy v případě negativního výsledku.

Tento nástroj byl nainstalován a posléze i spuštěn na všech počítačích na oddělení tak, abych získal ucelené informace o aktuálním stavu zabezpečení jednotlivých pracovních stanic. Výsledky, které byly potom tímto programem prezentovány jsem zanalyzoval a budou dále v práci uvedeny vždy v kapitole, ke které se obsahově vážou. Mezi některé poznatky o stavu zabezpečení informačního systému zjištěné nástrojem MBSA patří:

- Není použit software pro filtrování nevyžádané pošty
- Brána firewall je zavedena a je funkční

- Všechny systémy vybaveny operačním systémem Microsoft Windows XP jsou aktualizovány, je na nich povolena automatická aktualizace. Jeden z počítačů je vybaven operačním systémem Microsoft Windows Millenium Edition a není aktualizován vůbec.
- Některé uživatelské účty nejsou chráněny heslem

2.11 Penetrační test

Penetrační testy jsou testy určené pro zjišťování napadnutelnosti vnitřní sítě prostřednictvím útoku vedeného z vnějšku (Internet, externí síť). V současné době je jich množství poskytováno důvěryhodnou třetí stranou zcela zdarma.

2 Vyhodnocení

GRATULUJEME!

Bylo otestováno celkem 19 služeb a ani jedna nebyla vyhodnocena jako napadnutelná.

Neusnete však na vavřínech. To že náš základní test nenašel prvotní napadnutelné místo, neznamená, že není způsob jak vaši síť napadnout.

Vysvětlivky výsledku testu:

Otevřeno
služba je veřejně dostupná v celé síti Internet. Pokud běží bez vašeho vědomí je to napadnutelné místo vašeho počítače a známka špatného zabezpečení. Zde pomůže [Firewall](#).

Odmítnuto
služba je zřejmě používána, ale odmítá přijmout požadavek z našeho serveru, nebo neběží a server ji aktivně odmítá (nevhodné řešení). Odmítnutí je sice postačující proti napadení, ale stále umožňuje hackerům provést zahlácení dotazy. Zde pomůže [Firewall](#).

Zabezpečeno nebo vypnuto
služby vyhodnocené jako nedostupné, zakázány. Pravděpodobně na vašem počítači neběží, nebo je FIREWALL blokuje. Jediné opravdu bezpečné řešení..

Port	Služba	Bezpečnostní význam	Stav
21	FTP	Veřejný FTP server. Slouží ke kopírování dat. Hackeři je často používají ke vtažování dat a zakodovaných databází hesel.	Zabezpečeno nebo vypnuto
23	Telnet	Nekódované terminálové spojení - dá se odposlouchávat. Máte pravděpodobně FIREWALL. Váš správce nechal velkou bezpečnostní díru do systému. Přes terminál se může někdo pokusit připojit k serveru...	Zabezpečeno nebo vypnuto

Obr. 8: Výsledek penetračního testu

Test spočívá v otevření požadované webové stránky. Dále následuje testování počítače, které není nikterak viditelné. Na závěr jsou potom zobrazeny výsledky testu i s hodnocením. Tento typ útoku je často používán hackery i počítačovými viry. Testy byly provedeny od třech rozdílných poskytovatelů (www.test.bezpecnosti.cz, www.auditmypc.com, www.qualys.com) a ani jeden z nich neshledal v systému napadnutelná místa. To svědčí o dobrém zabezpečení sítě firewallem a rovněž i o tom, že zcizení či zničení dat potencionálním útočníkem přes vnější síť by bylo dosti náročné. K dobrému

výsledku zcela jistě přispěl i fakt, že síť je chráněna na straně poskytovatele internetu, který garantuje určitou míru nenapadnutelnosti počítačů přes něj připojených do vnější sítě (internetu). Výsledky tohoto testu budu opět prezentovat a zmiňovat v kapitolách, ke kterým obsahově patří. Existuje rovněž velké množství komerčních (placených) externích testů, které nabízí širší spektrum možností nastavení a mnohem přehlednější prezentaci výsledků. K odhalení potencionálních slabých míst pro potřebu firmy však bohatě stačily verze nekomerční.

2.12 Silné a slabé stránky současného zabezpečení dat

Pro vypracování pozdějšího projektu pro mne bylo velice důležité provést analýzu současného stavu zabezpečení informací a dat procházejících informačním systémem společnosti. K tomu mi nejprve posloužily analýzy, které jsem detailněji popsal v předchozích kapitolách. Tyto byly východiskem pro určení počátečního stavu a k určení směru a prioritních cílů při řešení projektu informační bezpečnosti ve firmě LIMIRE. Bylo tedy nutné abych se nejprve zaměřil na otázky informační bezpečnosti, které firmu v současné době trápí nejvíce. U těchto se pokusil zanalyzovat současnou situaci a to tak, že určím silné a posléze i slabé stránky současného stavu. Toto posléze bude východiskem pro tvorbu kvalitní projektové části. Při rozboru silných a slabých stránek bude třeba dodržovat již předem stanovené rozdělení jednotlivých druhů ohrožení do skupin tak, aby komplexně řešená analytická část byla uspořádána přehledně a aby se z ní daly později velmi srozumitelně vyčíst podstatné informace. V neposlední řadě bude tato analýza sloužit jako východisko pro projektovou část a tvorbu plánu řešení informační bezpečnosti z čehož rovněž vyplývá nutnost exaktního a přehledného zpracování všech relevantních informací v analytické části.

2.12.1 Útočníci

Do této skupiny ohrožení dat můžeme zařadit veškeré hrozby, které přicházejí z venkovního prostředí a to zejména prostřednictvím sítě internet. Tato činnost může být záměrná. To znamená, že se někdo pokusí odcizit nebo zničit podniková data záměrně tím, že se zkouší nabourat do vnitřní firemní počítačové sítě (hacker). Další hrozbou, která patří do této kategorie jsou počítačové viry a spyware. Tyto se mohou do počítačové informační sítě dostat například prostřednictvím e-mailu či tím, že

uživatel prochází webové stránky s nebezpečným obsahem. Jejich hrozba a zákeřnost spočívá v tom, že nemusí páchat žádnou viditelnou destruktivní činnost, avšak naprosto skrytě odesílají data na server útočníka. V mnoha případech jsou však naprogramovány k tomu, aby prováděli předem danou, záměrně škodlivou činnost.

Počítačové viry

Jakožto jediná ochrana před počítačovými viry se jeví antivirový program. Všechny počítače na pracovištích byly vybaveny legálně zakoupeným a aktualizovaným antivirovým programem AVG ve verzi 7.0. Ten představuje ucelenou ochranu a nabízí řadu nadstandardních prvků jako rezidentní ochranu či email scanner. Všechny počítače kromě jednoho byly rovněž vybaveny operačním systémem Microsoft Windows XP Professional s platnými licencemi a s nejnovější aktualizací SP2. Na všech byl rovněž povolen režim automatické aktualizace dat, takže systém byl z tohoto hlediska maximálně zabezpečen což rovněž potvrdil i diagnostický nástroj MBSA. Provedl jsem rovněž kontrolní testy antivirovým programem a všechny výsledky byly negativní. Analýza potvrdila obecně známé pravidlo, že v českých firmách se o problematice virů ví, a antivirové programy jsou jedním z mála ochranných prvků, u nás častěji používaných.

Spyware

Spyware je program, který se stará o posílání důvěrných informací o počítači a jeho uživateli na vzdálené servery a to samozřejmě bez vědomí uživatele. Bývají součástí různých freewarových (zdarma) programů. Riziko jejich přenesení na počítač v jakékoliv firmě je tedy značné. Při provádění auditu v této oblasti jsem ani na jednom z počítačů nenalezl odpovídající a aktualizovaný nástroj pro odstranění tohoto druhu zákeřného softwaru. Proto byla nasazena zkušební verze programu pro odstranění spyware. Po instalaci na všechny počítače a nutné aktualizaci jsem provedl kontrolní testy. Ty prokázaly přítomnost obrovského množství těchto programů na všech počítačích což byl výsledek zanedbávaného zabezpečení dat v této oblasti. Program již stihl zasáhnout všechny podstatné aplikace v počítačích a mnohdy absolutně znemožňoval jejich korektní funkci. Naprosto evidentně snižoval produktivitu a výkonnost práce na všech napadených počítačích. Za pomoci nainstalovaného nástroje byl veškerý spyware z počítačů odstraněn, stejně jako i samotný program, jelikož se jednalo pouze o zkušební verzi.



Obr. 9: Výsledek testu na přítomnost spyware

Hacker

Stoprocentně účinná ochrana před externí sítíovou infiltrací hackerem neexistuje. Existují ovšem prostředky, které dokáží takovéto útoky velmi účinně blokovat a přinejmenším dokážou hackera od další činnosti odradit svou neprůchodností. Mezi takové nástroje patří zejména firewall. Ten monitoruje příchozí a odchozí spojení mezi počítačem a vnější sítí a v případě podezření dokáže spojení blokovat. Je to nejúčinnější nástroj. Jak už jsem v předchozích kapitolách popsal, provedl jsem penetrační testy, které simulují útok hackera. Všechny provedené testy byly negativní a nebylo objeveno slabé místo zabezpečení. Bylo to způsobeno zejména tím, že poskytovatel Internetu firmě LIMIRE je vybaven zařízeními, která takovéto útoky blokují a de facto tak své uživatele chrání. Další podstatnou věcí je to, že počítače s operačními systémy Windows XP jsou maximálně aktualizovány a jsou vybaveny standardním softwarovým firewallem a posledními bezpečnostními záplatami, které potenciální nebezpečí infiltrace minimalizují.

Silné stránky zabezpečení v této oblasti:

- Kromě jediného jsou počítače vybaveny operačním systémem Microsoft Windows XP, který je aktualizován a je na něm povolena funkce auto update, která garantuje automatické instalace bezpečnostních záplat.
- Počítače jsou vybaveny aktualizovaným antivirovým programem.
- Síť je chráněna firewallem.
- Poskytovatel Internetu používá aktivní prvky ochrany

Slabé stránky v této oblasti:

- Jeden z počítačů používá zastaralý operační systém bez kvalitního zabezpečení.
- Počítače nejsou vybaveny softwarem pro odstranění spyware.
- Některé počítače nebyly chráněny hesly či silnými hesly.
- Nebyl aktivován nástroj pro filtraci nevyžádané pošty (antispam).
- Neexistují zásady pro bezpečný pohyb po internetu a stahování dat.

2.12.2 Nehody a katastrofy

Do této kategorie ohrožení podnikových dat a informací můžeme v podstatě zahrnout naprosto neočekávatelné a nikým nezaviněné bezpečnostní incidenty. V první řadě sem patří nehody typu požár či záplava. Zde jsou kromě počítačových dat ohroženy i data na papírových nosičích a data v archivech. Nemůžu však opomenout ani další podstatné složky. A to zejména neočekávané havárie počítačů, jejich komponent i dalších nutných prostředků pro přenos podnikových dat a informací. Stejně tak jako externí útoky, ani nehody či katastrofy nelze nikterak předvídat. Ovšem při dodržování zásad jim lze velmi dobře předcházet a minimalizovat tak riziko. Rovněž je možné nasadit některé účinné prvky aktivní či pasivní ochrany.

Havárie počítače

Tato dosti obsáhlá kapitola v sobě zahrnuje několik přímých druhů ohrožení podnikových dat. Mezi tu nejčastější patří zničení některé z počítačových komponent. Nejčastěji tedy bohužel pevného disku, na kterém jsou uložena veškerá data. Takovéto havárie může předcházet například přepětí v elektrické síti které má za následek přetížení komponent uvnitř počítače a jejich funkční destrukci. Jedinou možnou ochranou před tímto druhem ohrožení je pravidelné zálohování dat a použití záložních zdrojů spolu s přepět'ovými ochranami. Do této kategorie bychom dále mohli zařadit i ztrátu dat způsobenou nenadálým výpadkem elektrické energie. Zde je opět vhodné použití záložních zdrojů, které jsou schopny v případě výpadku elektřiny udržet počítače v chodu několik desítek minut tak, aby mohla být provedena efektivní záloha dat. Při podrobnější analýze jsem bohužel zjistil, že v objektu, ve kterém se kanceláře nachází ke kolísání napětí dochází poměrně často a již došlo k zasažení a poškození některých komponent, které poté musely být nákladně měněny. Stejně tak se velice negativně jeví fakt, že ve firmě nejsou použity zásady pro zálohování dat, tudíž data se nezalohují. V případě jejich ztráty by bylo nutné je vytvořit nákladně znova. Rovněž není použito ani přepět'ových ani záložních zdrojů, což značně zvyšuje riziko ztráty či poškození podnikových dat ve spojení s nebezpečím přepětí či naopak nedostatku elektrické energie.

Živelná pohroma

Do této kategorie, jak už jsem výše zmínil jsem zařadil požár či záplavy. V otázce ochrany znalostí a dat před tímto druhem ohrožení vidím možnosti zejména v důsledné prevenci před jejich vznikem. V případě, že k požáru dojde za nepřítomnosti pracovníků je totiž vysoce pravděpodobné, že škody na aktivech budou značné. Zaměstnanci jsou pochopitelně v této oblasti poučeni tak, aby riziko vzniku požáru bylo co nejmenší. Jediným účinným prvkem ochrany je zde důsledné zálohování dat a jejich uchování na jiném místě tak, aby v případě požáru nebyly zničeny i případné zálohy. Riziko poškození dat vodním živlem bych téměř vyloučil z důvodu umístění kanceláří v prvním patře budovy. Mimoto se v okolí sídla nevyskytuje žádný vodní zdroj, který by byl schopen takovou škodu způsobit. Bohužel i zde tedy vidím velký nedostatek v tom, že firma neprovádí pravidelné zálohování alespoň těch nejdůležitějších dat. V ostatních oblastech vidím přístup adekvátní možnosti vzniku rizika.

Silné stránky zabezpečení v této oblasti:

- Zaměstnanci poučení o zásadách minimalizace rizika vzniku požáru

Slabé stránky zabezpečení v této oblasti:

- Neexistují zásady pro zálohování dat
- Neprovádí se záloha dat
- Počítače nejsou chráněny přepět'ovými ochranami
- Komunikační prostředky nejsou chráněny přepět'ovými ochranami
- Nejsou nasazeny záložní zdroje

2.12.3 Interní ohrožení

Do této kategorie můžeme zařadit veškeré nebezpečí ztráty informací a dat plynoucí z neznalosti vlastních zaměstnanců (uživatelů) či z důvodu jejich korupce. Zaměstnanci tedy at' už úmyslně či zcela náhodně způsobí ztrátu či zničení dat. Tento způsob vynášení dat může být velice zákeřný a jen stěží odhalitelný. Spočívá totiž v odvolatelnosti – tedy schopnosti uživatele nepravdivě popřít akci, kterou nemohou ostatní strany dokázat. Ačkoliv se to může zdát divné, do této kategorie patří i takzvané instalace pirátských kopií softwarových produktů na počítače. V takovémto případě se firma dostává do rozporu s licenčním zákonem a může dojít k vymáhání tohoto práva. Obvykle by to tedy znamenalo pro firmu obrovskou finanční pokutu.

Neznalost uživatelů

Neznalost uživatelů je velkým problémem českých firem. Informační systémy jsou věcí poměrně novou a množství uživatelů zejména staršího věku má občas problémy nové technologie vstřebat. Z tohoto právě pramení hrozba ztráty dat díky neuváženému chování uživatele. Ten může zcela

náhodně smazat některá data aniž by si to uvědomil. Stačí pouze když se pohybuje v prostředí aplikace, kterou ovšem moc dobře nezná. Dalším problémem může být korupce. Někdo prostě podplatí zaměstnance a ten citlivá data vynese aniž by si toho někdo všimnul. Ve všech těchto případech platí, že na vině je vždy zaměstnanec a dále platí, že takovýmto incidentům lze předcházet. Při analýze tohoto problému ve firmě jsem nabyl přesvědčení, že zaměstnanci ke své práci používají pouze ty programy, které potřebují a s těmi umějí pracovat. Co se týče problému korupce a vynášení informací i zde se zdá být situace v pořádku. K loajálnosti vede zaměstnance zejména fakt, že firma vůči nim nemá žádné závazky a své povinnosti plní řádně. Z toho plyne, že ani sami zaměstnanci nemají potřebu zaměstnavatele okrádat o data. Problémem tedy pouze zůstává nedokonalé proškolení zaměstnanců o bezpečné práci v prostředí Windows a dále o bezpečném pohybu po Internetu a stahování dat.

Nelegální software

Ačkoliv by se mohlo zdát, že tento problém nemá s bezpečnostní politikou firmy co dělat, je tomu právě naopak. Jak už jsem popsal výše, software podléhá licenčním ujednáním a jakožto něčí majetek je nutné za jeho používání platit. To platí dvojnásob právě u využívání těchto produktů ve firmách. Existují speciální policejní složky, které se bojem proti softwarovému pirátství zabývají. Postihem viníka u kterého je nelegálně držený software zjištěn je potom většinou vysoká finanční pokuta. Při analýze jsem prošel počítače na oddělení s cílem zjistit zda-li není přítomen software, za který je nutné platit a který je užíván v rozporu s licenčním ujednáním. Veškeré operační systémy, stejně jako kancelářské balíky byly však v pořádku, řádně zakoupeny a s platnými licencemi. Dále kromě programů, které jsou svými výrobci poskytovány zdarma nebyly žádné jiné nelegálně instalované programy objeveny.

Silné stránky zabezpečení v této oblasti:

- Minimum používaných programů
- Pracovníci umí daný software a programy ke své práci využívat
- Firma nemá závazky vůči svým zaměstnancům

Slabé stránky zabezpečení v této oblasti:

- Proškolení v oblasti využívání Internetu a bezpečného stahování dat

2.12.4 Ohrožení zvenku

Sem můžeme zařadit jakékoliv pokusy o získání našich dat jinou cestou nežli útokem přes Internet. Patří sem tedy „návštěva“ zloděje či pokusy o tzv. „social engineering“ – tedy pokusy o přesvědčení našich zaměstnanců k poskytnutí informací, které by za normálních okolností nikdy neposkytli. Například předstíráním jiné identity. V pozadí mohou stát naši konkurenti či bývalí nespokojení zaměstnanci. Rizika ztráty dat mohou být obrovská ovšem záleží na velikosti a povaze firmy. Samotní mistři sociálního inženýrství neboli sociotechniky jsou experty na bezpečnost a jejich metoda získávání informací je založena na naprosto přesných a spolehlivých technikách přesvědčování a ovlivňování tak, že se jim většinou potřebnou informací podaří bez problémů či s menšími obtížemi získat.

Zloděj

Slovo vzbuzující respekt ve všech oblastech. V dnešní době platí, že pokud chceme být před zloději v bezpečí musíme vynaložit nemalé finanční prostředky na zabezpečení toho, co chceme chránit. Zloděj dat ale i běžný zloděj jde většinou na jisto a ví přesně co hledá. Opět je zde důležitá prevence. Ta spočívá v poskytnutí co nejmenšího množství dat k odcizení. A dále rovněž v kvalitním zabezpečení objektu. To znamená nejen v přítomnosti mříží a alarmu, ale třeba rovněž v tom, že nedáme cizím lidem možnost nahlédnout do kanceláře ať už jako návštěva nebo nepozorovaně skrze okno. V tomto případě při mém auditu byl objekt kvalitně zabezpečen nejen mřížemi a alarmem, ale i dalšími prvky, které ovšem firma nechtěla zveřejňovat. Kladem je rovněž fakt, že okna kanceláře jsou v prvním patře a je téměř nemožné dovnitř vidět nebo se dostat jako návštěva. Rovněž i obrazovky počítačových monitorů jsou otočeny mimo okno tak, aby do nich nepadalo přímé světlo a zároveň de facto tak, aby do nich nebylo zvenčí vidět. V tomto ohledu bylo zabezpečení ve firmě na velmi dobré úrovni.

Konkurence

Mít výsadní postavení na trhu neznamená pouze užívat si. Znamená to hlavně každodenní boj o udržení pozice. Konkurence ze všech stran tlačí a nebojí se použít různých metod tak, aby naši pozici oslabila či se dostala ke zdrojům, které máme pouze my. Mezi tyto metody pochopitelně patří i odcizení důvěryhodných a důležitých dat které může vést přinejmenším k finančním ztrátám. Zde opět platí to, co jsem již napsal v předchozí kapitole. Objekt firmy je velmi dobře zabezpečen po stránce fyzické i elektronické. Zaměstnanci ovšem nebyli nikterak školeni v oblasti sociálního inženýrství, tedy získávání dat jejich prostřednictvím díky předstírání identity někoho jiného. Zde bych viděl jediný nedostatek v této oblasti. Je jisté, že zaměstnanci by neposkytli důvěrné informace někomu jinému, avšak profesionálové v oblasti získávání dat mají účinné metody jak si data opatřit. To jsem ovšem popsal již v předchozí kapitole.

Silné stránky zabezpečení v této oblasti:

- Kvalitní fyzické zabezpečení
- Kvalitní elektronické zabezpečení
- Do objektu se nedostane nikdo cizí
- Není vidět dovnitř kanceláří

Slabé stránky zabezpečení v této oblasti:

- Chybí proškolení v oblasti sociálního inženýrství

2.12.5 Výsledky analýzy aktuálního stavu zabezpečení

Silné stránky zabezpečení dat	Slabé stránky zabezpečení dat
Operační systém Windows XP, aktualizovaný	Jeden z počítačů používá zastaralý operační systém
Antivirový program, aktualizovaný	Není nainstalován nástroj pro odstranění spyware
Firewall, aktualizovaný	Filtrace nevyžádané pošty není povolena
Poskytovatel internetu používá další bezpečnostní prvky	Některé počítače nejsou chráněny hesly
Fyzické zabezpečení objektu	Neexistují zásady pro bezpečný pohyb po internetu a stahování dat
Elektronické zabezpečení objektu	Neprovádí se záloha dat
	Nejsou používány záložní zdroje
	Nejsou použity přepět'ové ochrany
	Chybí proškolení zaměstnanců v oblasti sociotechniky

Tab. 3: Výsledky analýzy aktuálního stavu zabezpečení

V předcházející tabulce je uveden výčet nejpodstatnějších identifikovaných silných a slabých stránek zabezpečení informací a dat v podniku. Tyto jsem vytvořil na základě předchozího auditu a analýzy současného stavu a dále na základě priorit, které jsem vytvořil na základě kritériální tabulky. Data mi poslouží při tvorbě plánu a projektu informační bezpečnosti, kterým se budu zabývat samostatně v projektové části mé práce.

2.13 Hrozby nedostatečně zabezpečeného informačního systému

Hrozeb, které plynou z toho, že firma neřeší svoji informační bezpečnost dostatečným způsobem je množství. Jako první se nabízí krádež našich dat, které někdo zneužije pro svůj prospěch. Naše firma jakožto jediný vlastník této informace přijde o výhodu plynoucí z toho, že jsme jediní, kteří ji máme a známe dobře její cenu. Cesta k získání unikátních informací a dat pro firmu je složitá a těžko vyčíslitelná. Jedná se zejména o její nákladné vytvoření přímo ve firmě (nákresy, specifikace, patenty) anebo její odkoupení od někoho jiného. Tak jako tak, krádež takového druhu informací pro

nás bude znamenat jisté finanční ztráty. Do ceny informace se započítává její hodnota na trhu, okamžitý přínos, náklady na její pořízení, a mnoho dalších složek. Proto ztrátu plynoucí z jejich odcizení či kompletního zničení můžeme jen velmi těžko finančně vyjádřit. Důležitým poznatkem při studiu problematiky informační bezpečnosti je fakt, že takovéto investice nejsou na první pohled vůbec nikde vidět. Jde o to, že pokud k bezpečnostnímu incidentu nedojde lze investici do zabezpečení považovat za ztrátovou. Ovšem co by se stalo, kdyby k incidentu došlo a firma zabezpečena nebyla. Zcela jistě by to znamenalo finanční ztrátu, a dále bez nadsázky oslabení pozice na trhu. Vždyť ztratí-li se data společnosti, která je považována za důležitou, znamená to pokles důvěry vůči této firmě. Dále se dá mluvit o profitu cizích osob a firem na našich pracně vytvořených datech. Taková firma se potom může dostat na naši úroveň aniž by musela vynakládat alespoň ekvivalentní finanční prostředky jako my. Proto musíme celý proces řešení informační bezpečnosti ve firmě chápat více jako pojištění nežli investici.

2.14 Syntéza analytické části a vytvoření závěrů pro projektové řešení

Z předchozí analýzy vyplývá, že některé prvky informační bezpečnosti ve firmě jsou zavedeny a jsou plně funkční. Některé z prvků jsou naopak v neaktivním stavu či nejsou bohužel přítomny vůbec.

- Počítače jsou kromě jediného vybaveny operačním systémem Microsoft Windows XP, který je aktualizovaný a jsou na něm přítomny veškeré podstatné bezpečnostní záplaty vydávané výrobcem tohoto softwaru.
- Počítače jsou vybaveny legálním a aktualizovaným nástrojem pro odstranění možné virové nákazy.
- Na počítačích je přítomná softwarová brána firewall, a stejně tak i poskytovatel internetového připojení je na své straně vybaven určitými bezpečnostními prvky chránícími síť před možným napadením.
- Objekt, ve kterém tato divize firmy sídlí je fyzicky zabezpečen proti vniknutí neoprávněných osob. Dále je rovněž chráněn i elektronicky což opět snižuje koeficient rizika.

- Jeden z počítačů je vybaven starším operačním systémem, jehož napadnutelnost je vyšší nežli je tomu u novějších verzí.
- Na počítačích není nainstalován účinný nástroj pro bezpečné odstranění spyware z počítačů. Ten potom může provádět destruktivní činnost, aniž by o tom uživatelé věděli.
- Není povolena filtrace nevyžádané pošty. To vede ke zbytečné časové ztrátě při vynuceném manuálním třídění pošty.
- Chybí psané zásady a proškolení uživatelů v oblasti bezpečného pohybu po internetu, stahování dat a v oblasti sociotechniky.
- Nejsou vytvořeny zásady pro zálohování důležitých dat. Tím pádem se rovněž neprovádí ani samotné zálohování a v případě havárie systému hrozí ztráta veškerých podnikových dat.
- Nejsou používány záložní zdroje což vede ke zbytečným časovým a finančním ztrátám způsobeným nedostatkem či naopak přebytkem elektrické energie v síti (podpětím nebo přepětím).

3 PROJEKTOVÁ ČÁST

V této části své diplomové práce se budu snažit vzniklé úkoly vyřešit a navrhnout opatření, která povedou ke zlepšení situace týkající se informační bezpečnosti ve firmě. Při řešení budu vycházet ze závěrů z analytické části, zejména tedy z výsledků analýzy silných a slabých stránek současného stavu zabezpečení informací a dat ve firmě, prezentovaných v závěru analytické části.

Prioritním problémem bude řešení internetové bezpečnosti, tedy snaha o zajištění a zabezpečení elektronických dat před jejich zneužitím prostřednictvím sítě internet. Zde se budu zabývat návrhy projektu pro zabezpečení samotných počítačů, které v sobě zahrnují pořízení nových součástí programového vybavení a optimální konfigurace současných programů. Další v pořadí se budu věnovat oblasti možných nehod a katastrof z čehož by mohla resultovat ztráta jak dat v elektronické podobě, tak i v podobě tištěné. To bude obnášet návrh účinných řešení pro oblast zálohování dat, ochrany počítačů před nestabilní elektrickou sítí a v poslední řadě i tvorbu konceptu pro sestavení zásad bezpečného pohybu po internetu a stahování dat. V závěru potom přijdou na řadu interní a externí prostředí a s ní i sociotechnika.

Z dotazníku, týkajícího se ochrany znalostí a dat jasně vyplynulo, že firma má snahu problematiku řešit, avšak prozatím v této oblasti nepodnikla podstatné kroky. Podobná situace je bohužel ve většině českých firem. Velkým kladem však je, že management firmy už sám o sobě má snahu se touto problematikou zabývat a je ochotný v této oblasti spolupracovat, vzniklé problémy řešit a pokračovat v tom i do budoucna.

3.1 Cíle projektového řešení

Hlavním cílem projektu řešení informační bezpečnosti ve firmě bude vytvoření koncepčně správných a fungujících opatření, které budou v první řadě vycházet ze současného stavu informační bezpečnosti ve firmě a které povedou ke snížení rizika zničení, ztráty či zneužití podnikových dat kolujících interním prostředím firmy jak v elektronické tak i v papírové podobě. Z povahy informací a jejich uchování není možno zaručit jejich 100% ochranu. Lze však pomocí nejrůznějších metod a

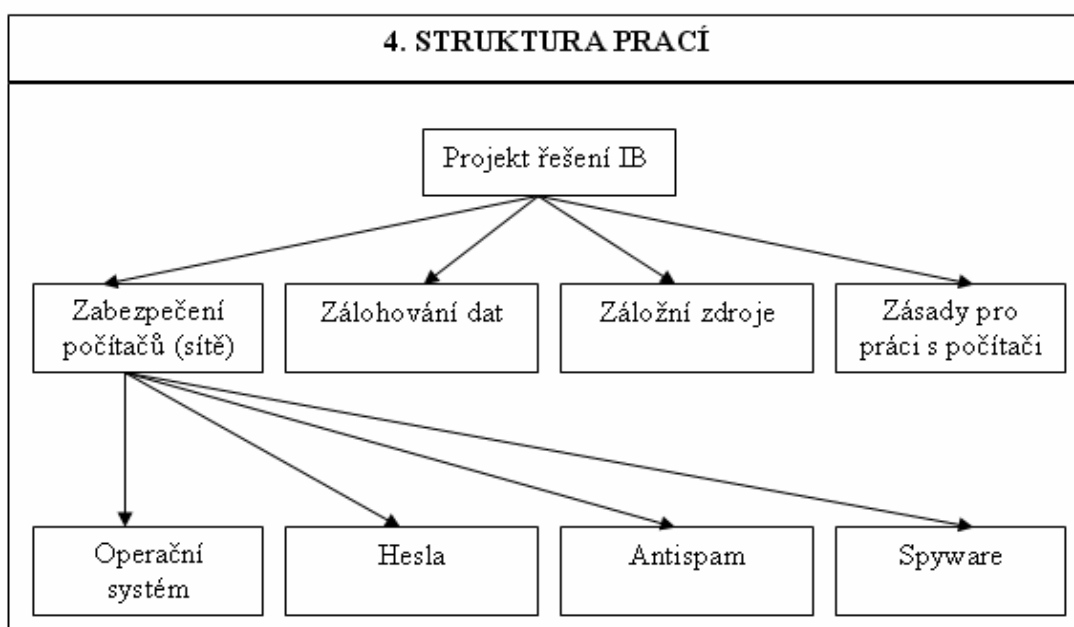
nástrojů koeficient rizika snižovat na přijatelnou úroveň. Budu se snažit nalézt vždy řešení takové, které při daných finančních nákladech zajistí snížení tohoto koeficientu. Dá se tedy hovořit o kontinuálním hledání možností s dobrým poměrem cena/výkon.

3.2 Plánování projektu

1. PROJEKT ŘEŠENÍ INFORMAČNÍ BEZPEČNOSTI	
Historie projektu	• Snaha o řešení informační bezpečnosti • Zkvalitnění ochrany informací a dat • Vytvoření opatření pro zlepšení celkové bezpečnostní situace
Požadavky managementu	• Analyzovat současný stav a situaci týkající se ochrany znalostí a dat ve firmě • Navrhnout a aplikovat vhodné prvky ochrany • Vytvořit zásady a doporučení pro řešení informační bezpečnosti
Co se již udělalo	• Byla provedena důkladná analýza současného stavu informační bezpečnosti ve firmě

2. CÍLE PROJEKTU	
Hlavní cíl projektu	• Fungující a zlepšený systém ochrany znalostí, dat a informací ve firmě • Vytvořený na míru přímo pro danou společnost
Kritéria úspěchu	• Projekt bude úspěšný podaří-li se zanalyzovat současnou situaci a na základě ní vytvořit fungující systém, který bude chráněn před bezpečnostními incidenty
Co není součástí projektu	• Součástí projektu není kompletní inovace informačních systémů a technologií • Součástí není spoluúčast dalších externích osob ani firem

3. OMEZENÍ PROJEKTU	
Omezení projektu	- Není možné libovolně využívat zaměstnanců - Projekt musí být hotov a zaveden do 30.4.2005 - Není možné libovolně využívat dostupnou výpočetní techniku
Rozpočet projektu	Investice do celkového zlepšení situace nesmí přesáhnout 50.000,- CZK
Podmínky projektu	Nebude možnost verifikace dodržování veškerých navržených projektových opatření



5. ČASOVÝ PLÁN												
červenec	srpen	září	říjen	listopad	12/2004	leden	únor	březen	duben	květen	červen	červenec
● Zadání projektu								● Zavádění projektu				
			● Analýza současného stavu						Zhodnocení výsledků		●	
						● Vypracování návrhu na projekt						

6. ORGANIZACE PROJEKTU	
Řídící tým	• Ing. Vladimír Dragoun
Sponzor projektu	• Bez sponzoringu
Vedoucí projektu	• Ing. Vladimír Dragoun
Projektový tým	• Tým zaměstnanců na oddělení firmy Limire • Bc. Martin Diviš – navrhovatel řešení

3.3 Projekt vylepšení úrovně zabezpečení sítě (Internetu)

Penetrační a další testy prezentované v analytické části neodhalily kritické chyby v zabezpečení dat v této oblasti, ale díky vyplnění dotazníku zabezpečení dat vyšlo najevo, že firma v této oblasti spatřuje hrozbu a je třeba se na tuto zónu opětovně zaměřit. Následný podrobnější průzkum tuto tezi potvrdil a ukázal na některé nedostatky, které je potřeba odstranit tak, aby se celková úroveň zabezpečení v tomto prostředí zvedla.

Mezi problém patří fakt, že všechny počítače jsou vybaveny novým operačním systémem Microsoft Windows XP, kromě jediného počítače. Na něm běží již zastaralý operační systém Microsoft Windows Millenium Edition, pro nějž brzy jeho výrobce ukončí veškerou technickou podporu. V tu chvíli se stane tento počítač neaktualizovaný a tím pádem i nezabezpečený a sám o sobě nebezpečný. Jako takový může být terčem napadení a zdrojem šíření potenciálně nebezpečného obsahu po vnitřní síti firmy. V důsledku tak tento jediný systém musíme chápat jako možnou hrozbu pro kompletní podnikový informační systém a v rámci zlepšení informační bezpečnosti ve firmě je potřeba navrhnout a provést určitá opatření.

Na základě analýzy zabezpečení a snížení rizika ohrožení dát je potřebné tento jediný systém nahradit novým operačním systémem Microsoft Windows XP Professional tak, aby bylo možné síť maximálně chránit a snižovat koeficient možného rizika. Tento operační systém jsem navrhl ze dvou důvodů:

1. Ve firmě se již úspěšně používá
2. Jedná se o nejkompatibilnější platformu pro malé a střední podnikání

Vzhledem k výše uvedenému je tedy jasné, že náklady spojené z nákupem, instalací, konfigurací a zaškolením uživatelů na tento operační systém budou nejnižší právě u této varianty. Vzhledem k množství ochranných prvků integrovaných v tomto systému, maximální podpoře ze strany výrobce a systému automatické aktualizace bude tímto řešením částečně sníženo riziko možné zničení či ztráty dat. Ovšem je nutné navrhnout a přijmout v této oblasti ještě další kroky.

Dalším návrhem pro zlepšení situace ochrany znalostí a dat, týkající se zabezpečení počítačové sítě je pořízení programu pro zachytávání a odstraňování spyware. Jak už bylo popsáno výše, na základě provedených testů a samostatné analýzy bezpečnosti, bylo zjištěno, že v síti se vyskytuje škodlivý software tohoto typu. Provedl jsem sice jeho odstranění, avšak k zajištění kontinuálního a udržitelného dalšího bezpečného stavu je nutné pořídit produkt, který dokáže podobné jevy zachytit a nadále blokovat. Proto jsem navrhl pořízení produktu LavaSoft Ad-Aware SE Plus Edition, která potřebné požadavky splňuje a která bude zakoupena s originální licencí tak, aby nedošlo k rozporu se zákonem. I tento krok přispěje ke snížení rizika ztráty dat a bude tvořit ucelený systém zabezpečení společně s dalšími navrhovanými řešeními.

Při analýze jsem dále zjistil, že pracovníci, kteří se starají o emailovou korespondenci nepoužívají žádný účinný nástroj pro automatickou filtraci příchozí elektronické pošty. Díky tomuto stráví denně zbytečně mnoho času tříděním nepotřebné pošty, která do firmy chodí v hojném počtu, zatímco by bylo možné se věnovat jiné, hodnotu přidávající činnosti. Zjistil jsem, že součástí softwaru pro práci s elektronickou poštou, který firma používá – Microsoft Outlook je i účinný antispamový filtr, který jeho výrobce poskytuje zcela zdarma právě pro účely ochrany před nevyžádanou poštou. Tento nástroj však nebyl aktivní a rovněž ani nebyla nastavena pravidla pro filtraci příchozí elektronické pošty. Dalším navrhovaným řešením je tedy povolení funkce filtrace pošty v tomto programu a vytvoření pravidel pro třídění této pošty. To povede k celkové úspoře času pro zaměstnance, který už dále nebude muset zprávy ručně mazat.

Posledním návrhem v oblasti zabezpečení podnikové informační bezpečnosti v oblasti počítačové sítě a možného zneužití dat je důkladné používání hesel všude tam, kde je to nezbytně nutné. Při analýze i díky nástroji MBSA bylo zjištěno, že u některých počítačů a přístupů k uživatelským účtům nejsou

vyžadována hesla. To může potenciálnímu útočníkovi usnadnit přístup k důležitým datům. Proto navrhuji, aby byly veškeré uživatelské účty chráněny hesly a pokud možno silnými (dlouhými) hesly. Provedu tedy novou revizi a označím účty, které nejsou dostatečně hesly chráněny. Ve spolupráci s odpovídajícím pracovníkem potom dohlédnu na to, aby byla politika hesel důsledně dodržována. Přístup k datům je tak alespoň částečně chráněn a dá se hovořit o tom, že tato navrhnutá opatření zvýší úroveň zabezpečení dat a informací v této oblasti možného úniku.

3.4 Návrh opatření pro účinné zálohování dat

Rozsahem i povahou nejdůležitější forma ochrany veškerých podnikových informací a dat kolujících v informačním systému zejména elektronickou formou. Řešení a zejména návrh účinných opatření v této oblasti by měl významně zvýšit úroveň zabezpečení dat ve firmě. Při kvalitním zálohování zůstávají nejdůležitější data neustále k dispozici i v případě jakékoliv havárie systému. Bohužel se této problematice ještě stále nevěnuje dostatečná pozornost a tato oblast je bohužel pokládána neprávem za nepodstatnou.

V mém návrhu vycházím ze současné situace ve firmě, kdy i na základě analýz vyšlo najevo, že se ve firmě data téměř nezalohují. Ke zlepšení celkové situace a pro účinné řešení informační bezpečnosti je potřeba zajistit, aby se záloha dat prováděla pravidelně. Samotnou zálohu bude zajišťovat odpovědný pracovník a to za použití nástroje, který je přímo součástí operačního systému a je pro zálohování přímo určen. Tento nástroj je poskytován zcela zdarma a jeho používání tedy není v rozporu s licenčními ujednáními. Zálohovat se budou předdefinované adresáře do kterých si zaměstnanci ukládají data. Dále budou vybrány adresáře, obsahující důležité databázové soubory nutné k obnově při havárii. Bude rovněž provedena záloha systémového nastavení tak, že při případném selhání se dá nastavení systému rekonfigurovat během několika minut. První záloha bude provedena jako kompletní nová. Ostatní pravidelné zálohy budou prováděny jako přírůstkové, což znamená, že se budou zálohovat pouze nové či změněné struktury v adresářích a nastaveních. Záloha bude prováděna na prepisovatelná média tak, aby bylo umožněno jejich opětovné využívání. Jelikož je velikost zálohovaných souborů interní báze velká a přesahuje velikost 3GB, bude nutné pořídit dvouvrstvou DVD vypalovací mechaniku, na které se bude záloha provádět. Záloha bude odzkoušena tak, aby bylo zaručeno, že případné obnovení souborů proběhne bez problémů. Zálohování bude probíhat posléze pravidelně minimálně každý měsíc, tak aby byla zaručeno, že v případě zničení bude většina dat obnovena. Záložní média, které budou obsahovat zálohu musí být

uchovány mimo budovu zvlášť tak, aby v případě, že v místě firmy dojde například k požáru nebyla zničena i samotná záložní média. Ačkoliv se zdá být tento postup složitý, ve skutečnosti v sobě obnáší pouze pár rutinních záležitostí. Rovněž i ovládání záložního programu je velice jednoduché a intuitivní. Proškolení v oblasti zálohování provedu sám osobně spolu s proškolením i v jiných oblastech o kterých se ještě zmíním.

POKYNY K ZÁLOHOVÁNÍ DAT				
Číslo	Druh dat	Četnost	Typ zálohy	Druh média
1	Smlouvy, dokumenty interní i externí komunikace a mezifirmní komunikace	1x týdně	Přirůstková	CD-RW DVD-RW
2	Zálohy elektronické pošty	1x týdně	Přirůstková	CD-RW DVD-RW
3	Zálohy databázových programů	1x týdně	Přirůstková	CD-RW DVD-RW
4	V případě signalizace výpadku proudu a provozu pouze z baterie okamžitě ukončí činnost, proved' uložení práce a bezpečně vypni počítač.			
5	Média se zálohami uchovávej mimo firmu			
Firma: LIMIRE, s r. o., Západní 75, Prostějov		Vytvořil: Bc. Martin Diviš Dne: 12.4.2005	Schválil: Ing. Vladimír Dragoun Dne: 12.4.2005	

Tab. 4: Pokyny k zálohování dat

Na základě konzultací a provedeného workshopu byly vytvořeny pokyny k zálohování dat, které obsahují nejpodstatnější informace o samotném zálohování. Budou vyvěšeny v blízkosti pracovních stanic a měli by přispět k důslednějšímu dodržování zálohování dat.

3.5 Návrh řešení ochrany dat a práce prostřednictvím záložních zdrojů

V průběhu analýzy zabezpečení vyšlo najevo, že ve firmě nejsou použity záložní napájecí zdroje ani přepětové ochrany. V případě výpadku elektrické energie jsou veškerá neuložená data odsouzena

k zániku a náhlé ukončení práce rovněž nepřispívá k bezproblémovému chodu a udržení životnosti hardwarových součástí počítačů. Navíc v případě přepětí v elektrické síti, což jak se ukázalo není výjimečná věc, může dojít k trvalému poškození některých součástí, s čímž už se ve firmě rovněž setkali. Oprava či koupě nové součásti včetně obnovy dat je potom poněkud nákladnou činností.

Navrhuji tedy pořízení záložních zdrojů, které budou zároveň vybaveny i přepět'ovými ochranami tak, aby dokázaly korigovat nadbytek elektrické energie v síti a nedošlo ke zničení komponent. Zároveň však budou vybaveny rovněž i baterií a budou schopny v případě výpadku elektrické energie ještě po několik minut udržet počítače v chodu tak, aby bylo možno provést bezpečné zálohování rozdělané práce a bezpečné vypnutí systému. Tento krok zvýší opět úroveň zabezpečení dat a rovněž i produktivitu práce. Jelikož však v tomto případě existuje větší množství ekvivalentních řešení, je nutné, abych provedl výběr pouze některého z možných zařízení. Proto provedu hodnocení odpovídajících zařízení a na základě tabulky multikriteriálního hodnocení technické úrovně zařízení potom vyberu řešení, které bude dle zadaných parametrů pro provoz v našem případě nejvýhodnější. Na trhu existuje velké množství podobných zařízení. Pro prvotní výběr vzorků do testu budu vycházet z jejich možného okamžitého nasazení. Ne všechny záložní zdroje jsou totiž vhodné k našim účelům a rovněž i pořizovací cena některých zařízení v prvopočátku vysoko přesahuje hodnoty, které je firma v tomto případě ochotna zaplatit. Vybrané zařízení bude odpovídat zadaným a preferovaným parametrům a bude možné je poté okamžitě nasadit do provozu.

Volbu budu provádět mezi těmito zařízeními :

- APC Back UPS CS 350EI
- APC Back UPS CS 650EI
- APC CyberFort UPS 350 USB
- APC CyberFort UPS 500 USB
- Power Kinetics ZZ BlackOutBuster 800VA

Všechny tyto výše uvedené záložní zdroje splňují svými parametry požadované vlastnosti a jsou schopny okamžitého nasazení a provozu do firemní sítě. Všechny jsou vybaveny záložní baterií i přepět'ovou ochranou. Poskytnou tak ucelené řešení při záloze a ochraně dat. Při výpočtu váhy parametru jsem vycházel z následujícího vzorce:

$$k(\%) = \frac{d}{\sum d} \times 100$$

Hodnocené parametry		1	2	3	4	5	Důležitost kritéria (d)	k (%)
1	Možnost SW řízení zdroje		0	0	0	1	2	13,3
2	Výbava	0		1	1	1	4	26,6
3	Výdrž zdroje	0	1		1	0	3	20
4	Cena	1	1	1		1	5	33,3
5	Uživatelský komfort	0	0	0	0		1	6,6
Součet bodů.... $\sum d$							15	100

Tab. 5: Hodnotící matice

Výše uvedená tabulka nám poskytla hodnoty vah u jednotlivých hodnocených parametrů a z těchto hodnot budeme dále vycházet u sestavování samostatné multikriteriální tabulky, která je uvedena níže.

$$\text{Součet bodů dle důležitosti} = \sum h \times k(\%)$$

Hodnocené parametry	1 (h)	CS350	2 (h)	CS 650	3 (h)	Cyber 350
SW Řízení zdroje	7	93,1	7	93,1	6	79,8
Výbava	7	186,2	7	186,2	6	159,6
Výdrž	5	100	7	140	5	100
Cena	7	233,1	7	233,1	7	233,1
Komfort	7	46,2	7	46,2	9	59,4
Součet bodů	33		35		33	
Součet bodů dle důležitosti		658		698		632

Tab. 6: Multikriteriální hodnocení technické úrovně záložních zdrojů

Hodnocené parametry	4 (h)	Cyber 500	5 (h)	Power Kinetics
SW Řízení zdroje	6	79,8	7	93,1
Výbava	6	159,9	8	121,8
Výdrž	7	140	7	140
Cena	8	266,4	6	199,8
Komfort	9	59,4	7	46,2
Součet bodů	36		35	
Součet bodů dle důležitosti		705,3		691,3

Tab. 7: Multikriteriální hodnocení technické úrovně záložních zdrojů –
dokončení

Na základě výše uvedené tabulky jsem zjistil, který z nabízených záložních zdrojů nejlépe splní předem definované požadavky, které jsme sestavili již předtím a ve kterých se odráží potřeby a nároky, které budou na tyto zdroje kladeny v průběhu jejich nasazení a v průběhu jejich životnosti, po kterou budou ve firmě sloužit. Výsledky a pořadí jednotlivých zdrojů jsou uvedeny v tabulce níže. Na základě těchto výsledků tedy navrhuji zakoupení zdroje, který se umístil na prvním místě.

Typ záložního zdroje	Počet bodů	Pořadí
APC CyberFort UPS 500 USB	705,3	1.
APC Back UPS CS 650EI	698	2.
Power Kinetics ZZ BlackOutBuster 800VA	691,3	3.
APC Back UPS CS 350EI	658	4.
APC CyberFort UPS 350 USB	632	5.

Tab. 8: Výsledky multikriteriálního hodnocení technické úrovně záložních zdrojů

Z hlediska všech sledovaných parametrů se nejlépe umístil zdroj APC CyberFort 500, který mimo jiné nabízí řadu výhod oproti ostatním zdrojům. Zejména tedy fakt, že je osazen klasickými typy zásuvek, do kterých je možno připojit i klasické kancelářské zařízení. Navrhuji tedy koupi a nasazení právě tohoto záložního zdroje vybaveného zároveň i přepětovou ochranou i ochranou telefonní linky. Samotnou instalaci a konfiguraci zařízení provedu opět osobně. Další udržování a správa již později nebude nutná z hlediska plné automatizace tohoto zařízení.

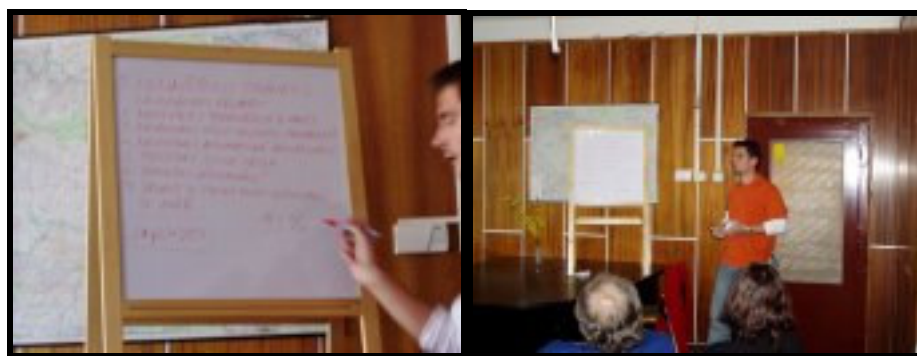
Pro testovací účely byl jeden ze záložních zdrojů zapůjčen a byla ověřena jeho kompatibilita a možnosti využití. Zařízení se ukázalo být podle předpokladů velice účinné a užitečné. Proto budou tato zařízení ve firmě na základě projektu nasazena.



Obr. 10: Nasazení záložního zdroje APC

3.6 Vytvoření zásad pro bezpečný pohyb na internetu a ochranu dat

Náplní analytické části byla rovněž analýza prostředí a znalostí problematiky informační bezpečnosti ze strany zaměstnanců vyplývající z rizik pohybu po internetu a počítačové síti vůbec. Na základě zjištění, že zaměstnanci nejsou poučení o některých hrozbách při pobytu na internetu a stejně tak i o hrozbách sociotechniky jsem navrhl uspořádání workshopu na toto téma, jehož cílem bylo zvýšení povědomí o těchto hrozbách a tím i zvýšení koeficientu bezpečnosti, který se později zcela jistě odrazí ve zvýšení celkové úrovně informační bezpečnosti ve firmě. Rovněž jsem navrhl vytvoření určitých zásad bezpečného pohybu po internetu a stahování dat, které by se měli dodržovat ze strany zaměstnanců firmy tak, aby riziko napadení a ztráty podnikových dat či informací bylo absolutně minimalizováno. Některé body budou zároveň vycházet z již výše uvedených pokynů k zálohování dat a dále tyto zásady vyplývají z informací, které byly prezentovány v průběhu workshopu tak, aby byly později srozumitelné.



Obr. 11: Workshop a přednáška na téma informační bezpečnosti

Hlavním cílem workshopu tedy bylo zvýšení úrovně informační bezpečnosti ve firmě Limire prostřednictvím získávání nových informací o možných hrozbách. Účastnili se jej zaměstnanci na oddělení, kteří mají přístup k firemním datům, počítačům a s nimi i přicházejí do styku. Důraz byl kladen na osvětlení problematiky a společnými silami byly vytvořeny zásady pro bezpečný pohyb po síti a pro zvýšení ochrany dat.

Tyto informace byly potom přehledně zobrazeny v tabulce a prezentovány. Participací zaměstnanců na tomto workshopu si slibují větší zájem o problematiku a pozdější důslednější dodržování společně vytvořených zásad.

ZÁSADY BEZPEČNÉHO VYUŽÍVÁNÍ POČÍTAČŮ		
• Při odchodu od počítače se nezapomeň odhlásit • Důsledně dodržuj pokyny k zálohování dat • Nikdy neotvírej nevyžádané podezřelé e-maily či jejich přílohy • Nikdy nevypínej automatické aktualizace systému ani je nepřerušuj • Nikdy nenavštěvuj webové stránky s nelegálním obsahem • Neignoruj výzvy bezpečnostních programů v počítači • Žádost o poskytnutí informací a dat si vždy ověř		
Firma: Limire, s r. o., Západní 75, Prostějov	Vytvořil: Tým ZIB Dne 16.4.2005	Schválil: Ing. Vladimír Dragoun Dne 18.4.2005

Tab. 9: Zásady bezpečného využívání počítačů

Na základě provedeného workshopu byly společně s týmem identifikovány nejpodstatnější záležitosti týkající se ochrany dat, které by se měli důsledně dodržovat tak, aby se zabránilo možnému narušení bezpečnosti. Participací zaměstnanců na projektu by se mělo dosáhnout důslednějšího dodržování sestavených pravidel.

3.7 Katalog opatření projektové části

Z předchozích bodů prezentovaných projektových řešení jsem vytvořil katalog opatření, které je nutné pro splnění cíle zadání diplomové práce provést. U většiny opatření není uveden termín plnění z důvodu individuálního přístupu firmy a stávající finanční situaci, kdy není jistá přesná doba, kdy bude možné navrhovaná opatření provést. Z hlediska přibližného časového horizontu lze mluvit přibližně o několika týdnech, maximálně měsících.

KATALOG OPATŘENÍ navrhovaných projektových řešení					
Číslo	Název opatření	Zodpovídá	Termín plnění	Realizace	Náklady (Kč)
1	Nákup jedné instalace operačního systému Microsoft Windows XP Professional	Dragoun	Neurčen		3300,-
2	Nákup třech instalací programu Ad-Aware SE Plus Edition	Dragoun	Neurčen		2300,-
3	Aktivace antispamového filtru	Diviš	Neurčen		0,-
4	Zajištění silných hesel pro přístup k uživatelským účtům	Dragoun	Neurčen		0,-
5	Nákup dual layer vypalovací mechaniky	Dragoun	Neurčen		1500,-
6	Nákup dvou kusů dvouvrstevných záznamových médií		Neurčen		300,-
7	Tvorba pokynů pro zálohování	Diviš	28.4.2005	ANO	0,-
8	Nákup dvou záložních zdrojů, jejich instalace a konfigurace	Dragoun	Neurčen		4600,-
9	Vytvoření zásad pro bezpečný pohyb na internetu a ochranu dat	Diviš	28.4.2005	ANO	0,-
10	Workshop a přednáška na téma informační bezpečnost	Diviš	28.4.2005	ANO	0,-
	Náklady celkem				12.000,-

Tab. 10: Katalog opatření navrhovaných projektových řešení

Pouze u úkolů, jejich zadavatelem a zároveň i osobou zodpovědnou za plnění jsem byl já osobně již realizace úspěšně proběhla. Všechny požadované úkoly jsem zvládl úspěšně v předem daném časovém termínu. Jejich očekávaný přínos se potvrdil.

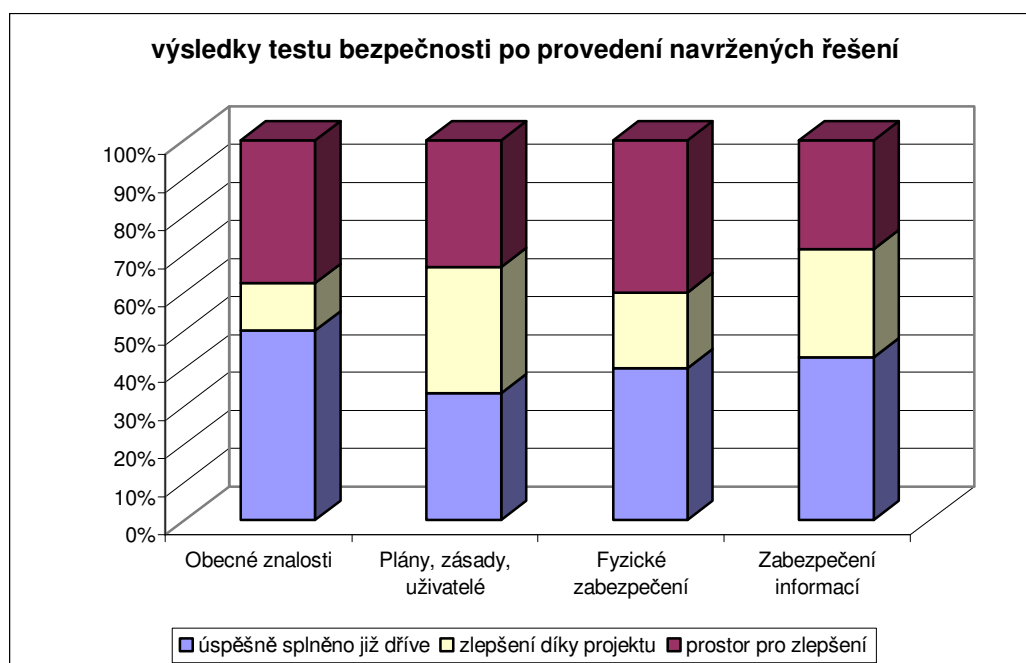
4 ANALÝZA EFEKTŮ A RIZIK PROJEKTOVÉHO ŘEŠENÍ

V této části diplomové práce shrnu jednotlivé poznatky z návrhů jednotlivých projektových řešení v podniku LIMIRE, s r. o., a budu se zabývat jejich reálných hodnocením, efektivitou a celkovým přínosem pro samotný podnik.

Navrhovaná opatření pro celkové zlepšení informační bezpečnosti ve firmě.

4.1 Přínos navrhovaných projektových řešení

Jak již bylo výše popsáno, efektivita projektů, které se vztahují k informační bezpečnosti se dá finančně jen velice těžko vyjádřit. Je to z důvodu nepředvídatelnosti bezpečnostních incidentů a těžkého vyjadřování hodnoty dat. Existují však způsoby nepřímého vyjádření efektivnosti. Jedním z nich je i opětovné vyplnění dotazníku testu bezpečnosti.



Obr. 12: Výsledky testu bezpečnosti po provedení navržených řešení

Nové bodové hodnoty vyjadřují přírůstek efektivity a lze si tak udělat komplexní přehled o přínosu navrhovaných projektových řešení. Tento přínos je v grafu vyjádřen světlou barvou a dosahuje rozmezí 10 – 30 %. S úspěchem však lze tvrdit, že ve všech sledovaných oblastech se firma dostala nad 60 % úspěšnost což představuje standart v této oblasti. V případě dalších analýz a dalších kroků učiněných v oblasti bezpečnosti lze očekávat ještě další vzestup. Obecně však lze považovat tento stav za dobrý. Vzhledem k povaze problému informační bezpečnosti však doporučuji v bezpečnostní politice nadále pokračovat a rozvíjet ji.

4.2 Vylepšení úrovně zabezpečení sítě

- S přihlédnutím k finančním možnostem byla vylepšena celková situace zabezpečení výpočetní techniky. Celkově uspokojivá situace, která byla zjištěna během analýzy naznačovala, že nebude nutné vynakládat přílišné finanční prostředky pro další vylepšení v této oblasti.
- Navrhovaná řešení v podobě nákupu nového operačního systému a programu pro odstranění programů typu spyware znamenají pouze minimální finanční náklady v porovnání s efektem, který přinesou. Další kroky v podobě vytvoření bezpečných hesel u uživatelských účtů a povolení antispamového filtru nebudou znamenat již další finanční náklady. Jejich další přínos bude pochopitelně ve zvýšení úrovně zabezpečení počítačů a dále ve zvýšení produktivity práce.
- Vzhledem k povaze problému informační bezpečnosti je třeba náklady vynaložené na zabezpečení chápat jako formu pojištění. Proto nelze finančně spočítat celkový efekt, který zvýšení úrovně zabezpečení dat v podniku přinese. V případě, že by k bezpečnostnímu incidentu došlo, celkový efekt řešení informační bezpečnosti a náklady spojené s jeho zavedením by se firmě několikanásobně zúročily. Ovšem nikdy nelze předem určit, zda-li by k bezpečnostnímu incidentu v následujícím období došlo či nikoliv.
- Možná rizika spojená s tímto problémem byla rozebrána na podnikovém workshopu na toto téma a zaměstnanci byli s možnými problémy seznámeni. Na základě toho později vznikly i zásady bezpečného využívání počítačů.

4.3 Návrh opatření pro účinné zálohování dat

- Tento krok znamená pro firmu konečné řešení problému zálohování svých dat. Neexistence koncepce pro vytváření záloh znamenala každodenní riziko jejich ztráty.
- Projekt bude vyžadovat dodatečné finanční náklady spojené s pořizováním zvláštního vybavení pro účinné zálohování dat.
- Vypracováním pokynů pro vytváření záloh ve spolupráci se zaměstnanci by se mělo dosáhnout jejich dodržování.
- To bude znamenat pravidelné zálohování dle rozpisu a tím pádem i existence bezpečně uchovávaných záloh pro případ havárie systému. Následná obnova by sice byla časově náročnější, avšak bude možné dosáhnout stavu systému před zničením dat.
- Rizika vyplývající z předání kompetencí v této oblasti na zaměstnance jsou jednoznačná: po určité době by se zálohy přestaly důsledně tvořit. I proto byly vytvořeny výše zmíněné zásady, které umístěné v blízkosti počítačů budou připomínat nutnost se tímto problémem zabývat.
- Dále by bylo ještě možné rozpracovat možnou vynutitelnost těchto zásad.

4.4 Návrh řešení ochrany dat a práce prostřednictvím záložních zdrojů

- V důsledku možného ohrožení díky neočekávaným výpadkům elektrické energie bylo potřeba se tímto problémem zabývat.
- Navrhované řešení vzešlo z několika možností jež byly eliminovány prostřednictvím multikriteriálního hodnocení technické úrovně výrobků.
- Od zavedení tohoto řešení očekávám zvýšení stupně ochrany dat a zvýšení efektivity a produktivity práce. V případě výpadku elektrické energie bude možné ještě po několik minut bezpečně pracovat. To umožní uložit data a bezpečně ukončit aplikace a systém vypnout, aniž by se uživatel musel obávat ztráty dat z rozpracované činnosti.

- Dalším přínosem v této oblasti bude zároveň i ochrana před možnými přepětovými rázy v elektrické síti. Nasazením tohoto řešení by se mělo zamezit možnému poškození některým částí počítačů a následné finančně nákladné opravě.
- Finanční náklady spojené se zavedením této části navrhovaného projektu představují největší část. Ovšem zároveň i škody na výpočetní technice spojené s tímto druhem ohrožení představují největší možné položky. S výpočtem možného přínosu daného řešení je situace podobná jako v prvním případě. Podobné jevy nelze předikovat. Lze pouze předpokládat, že nastanou.

4.5 Vytvoření zásad pro bezpečný pohyb na internetu a ochranu dat

- Obecně platí, že sám uživatel je jedním z nejnebezpečnějších článků samotného informačního systému.
- Návrhem zásad pro bezpečné používání výpočetní techniky by se mělo předcházet možnému ohrožení dat ze strany samotných uživatelů.
- K vytvoření těchto zásad a osvětlení problematiky jsem využil workshopu. Participací zaměstnanců by měl být efekt zavedení a dodržování těchto zásad mnohem vyšší. Zároveň jsem v průběhu workshopu formou přednášky objasnil některé problémy spojené z informační bezpečností čímž se rozšířilo povědomí zaměstnanců o dané problematice.
- Tímto krokem bude možné zajistit trvalé dodržování bezpečnostních pokynů a nadále by již nemělo docházet k ignoraci bezpečnostních výstrah a obcházení základních pravidel pro bezpečný pohyb po počítačové síti.
- Pravidla budou vytištěna a umístěna v blízkosti počítače tak, aby bylo možné eliminovat riziko jejich pozdějších opětovných nedodržování.

ZÁVĚR

Tato diplomová práce byla zaměřena na zhodnocení a následnou tvorbu prvků bezpečnostní politiky firmy. Vycházela z aktuálního stavu zabezpečení a jejím úkolem bylo pomoci firmě při řešení situace informační bezpečnosti. Ta, jak již bohužel bývá u firem zvykem nebyla ani v tomto případě dostatečně řešena. Rovněž i povědomí pracovníků o možných nebezpečných situacích a rizicích spjatých s daty nebylo vysoké. Mým cílem tak bylo se na tyto oblasti zaměřit a pomyslný koeficient zabezpečení dat ve firmě zvýšit.

V teoretické části jsem se snažil vysvětlit ty nejpoužívanější pojmy a formule, které se v oblasti bezpečnosti dat a informací vyskytují. K tomu jsem využil několika zdrojů a publikací, které se této či podobné problematice věnují. K osvětlení některých výrazů jsem však využil i internetové zdroje či některá periodika. Tímto způsobem bylo možné teoreticky a obecně popsat celý proces tvorby bezpečnostní politiky a jejich standardů.

V analytické části jsem využil právě teoretická východiska pro to, abych byl schopen provést revizi současného stavu ve firmě. Byl tak vytvořen postup bezpečnostního auditu a byly identifikovány hlavní subjekty účastnící se a podílející se na informační výměně. Popsal jsem dále hlavní hrozby a možné zdroje úniku, ztráty či zničení dat. Na základě těchto identifikovaných činitelů bylo možné provést analýzu jejich silných a slabých stránek čímž byl vytvořen seznam oblastí, které jsou zabezpečeny důsledně, dostatečně či nedostatečně. Za pomoci dotazníku pak byl vytvořen závěrečný přehled současného stavu zabezpečení s vytyčením priorit dle požadavků managementu. V závěru analytické části jsem potom provedl její syntézu a vytvořil jsem tak závěry a podklady pro následné projektové řešení, které z výsledků analytické části čerpá.

Projektové řešení této práce mělo za úkol navrhnout účinná opatření, která jednak povedou ke zlepšení současné situace informační bezpečnosti ve firmě a jednak budou respektovat konkrétní potřeby firmy tak, jak byly tyto identifikovány v analytické části této práce. Konkrétní návrhy projektových řešení se vztahují k jednotlivým oblastem možných zdrojů úniků informací a dat v podnikovém informačním systému. Navrhovaná opatření dále respektují jistá omezení ze strany firmy a jsou navržena tak, aby po zavedení poskytovala maximální efekt užítku při zachování

principu minimalizace nákladů potřebných pro realizaci konkrétního navrhovaného opatření. Obecně je toto pravidlo nazýváno hledáním řešení, respektující poměr cena/výkon, se kterým je možné se setkat ve více oblastech.

Vzhledem ke stanoveným cílům této práce mohu prohlásit, že jak zpracování, tak i samotná navrhovaná řešení splnila očekávání zadavatele a již jejich částečnou implementací byla prokázána jejich funkčnost a schopnost plnit požadované úkoly v rámci bezpečnostní politiky firmy. Bezpečnostní politika je stále ještě v mnoha nejen českých firmách chápána jako nepodstatný článek zařazený v podnikovém řetězci činností. Do jisté míry je to způsobeno i faktem, že investice do bezpečnosti nejsou nikde vidět. Jejich přínos není nijak měřitelný a nemůže být finančně vyjádřen tak, jako například investice do výrobního zařízení. Problém nastane v případě, že k bezpečnostnímu incidentu opravdu dojde. Finanční ztráty způsobené na nezabezpečeném systému jsou posléze obrovské. Naopak zabezpečený informační systém, kde se bezpečnostní politika důsledně dodržuje vykazuje naopak většinou pouze minimální finanční ujmu. Investice do zabezpečení informačních systémů a investice do bezpečnostní politiky je tak potřeba chápat spíše jako formu pojištění nežli finanční výdaje ve kterých potom management hledá možné finanční výnosy.

SUMMARY

The main target of this diploma work was aimed at evaluation and following creation of the security policy elements. This work was based on current information security conditions and the primary goal was to help company with the information security problems solving. The situation with information security was in this company unfortunately not properly solved as it becomes a kind of tradition. The same situation was recognized at the area of employees and their knowledge about the possible threats joined with data loss. So my target was to aim at these areas and to raise the imaginary security coefficient.

The whole work is basically divided into three separate parts. The theoretical part describes and explains most of the terminology and definitions that later appears in this work. I used the suitable literature as well as some of the internet sources. The magazines and journals were found as a suitable source as well. In the analytical part of this work, I used the elements of the theoretical part to be able to describe the current situation with information security in the company. Moreover I described the strength and weak parts of the current information security and policy. At the end of analytical part, based on the results of the analysis I created the final conclusions for the following project part of the work that is based on the results of the analytical part. The main goal of the project part of this work was to suggest an efficient disposal that would lead to the improving of the current situation concerning the information security.

According to the main targets of this work, I can declare that all of them were met. The suggested parts of the project proved to be able to work and met all the requirements of the management of the company. A lot of managers consider the security policy as an unimportant part of the company's processes. It might be caused by the fact that investments to the information security cannot be measured and cannot be verified unlike for example the investment to the production device. The problem appears in the moment when the security incident reveals. The possible financial loss is much more higher with an unsecured information system. That is why it is necessary to take the investments to the information more as a kind of insurance than the financial expenditure.

SEZNAM POUŽITÉ LITERATURY

- [1] JAŠEK, R. *Ochrana znalostí a dat v podnikových informačních systémech*. 1. vyd. Zlín: Univerzita Tomáše Bati, 2002. 115 s. ISBN 80-7318-095-2
- [2] ROSMAN, P., SODOMKA, P., JUŘENČÁK, B., BENDA, R. *Základy informatiky*. 1. vyd. Zlín: Univerzita Tomáše Bati, 2001. 250 s. ISBN 80-7318-034-0
- [3] DOBDA, L. *Ochrana dat v informačních systémech*. 1. vyd. Praha: Grada, 1998. 286 s. ISBN 80-7169-479-7
- [4] *Obchodní zákoník*. Ostrava: Sagit, 2001. ISBN 80-7208-263-9
- [5] CHIP: magazín informačních technologií. č.1 (leden 2003). Praha: Vogel, 2002. Vychází měsíčně. ISSN 1210-0684
- [6] CHIP: magazín informačních technologií. č.4 (duben 2003). Praha: Vogel, 2003. Vychází měsíčně. ISSN 1210-0684
- [7] MICROSOFT ČESKÁ REPUBLIKA. *Popis produktu Windows XP* [online]. c2005, poslední revize 25.4.2005 [cit. 2005-04-18] Dostupné z WWW: <<http://www.microsoft.com/cze/windows/xp/pro/evaluation/features.asp>>
- [8] INTERNETOVÉ VYDAVATELSTVÍ GALANCE. *Historie internetu ve světě* [online]. c2005, poslední revize 1.1.2003 [cit. 2005-05-11] Dostupné z WWW: <<http://www.galance.cz/HOME/internet.htm>>
- [9] PUBLIKAČNÍ SYSTÉM MĚSTA BEROUNA. *Historie internetu v ČR* [online]. c2001, poslední revize 19.2.2003 [cit. 2005-04-29] Dostupné z WWW: <<http://www.beroun.cz/tema/internet-historie/>>
- [10] NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. *Zákon o ochraně utajovaných skutečností* [online]. c2005, poslední revize 18.2.2005 [cit. 2005-04-17] Dostupné z WWW: <<http://www.nbu.cz/legislative/zakon.php>>
- [11] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Zákon o ochraně osobních údajů* [online]. c2001, poslední revize 19.4.2005 [cit. 2005-04-17] Dostupné z WWW: <http://www.uoou.cz/101_2000.php3>
- [12] BRECHLEROVÁ, Dagmar. *Výsledky průzkumu stavu informační bezpečnosti v České republice* [online]. 1.8.2004. Systemonline, 2005, 1.8.2004 [cit. 2005-05-16]. Dostupné z WWW: <http://www.systemonline.cz/site/doc-management/04_08brechl.htm>

- [13] HANÁČEK, Petr, STAUDEK, Jan. *Bezpečnost informačních systémů*. 1. vyd. Praha : [s.n.], 2000. 127 s. ISBN 80-238-5400-3.
- [14] VYTLAČIL, Milan, MAŠÍN, Ivan. *Dynamické zlepšování procesů*. 1. vyd. Liberec : Institut průmyslového inženýrství, 1999. 193 s. ISBN 80-902235-3-2.

SEZNAM OBRÁZKŮ

Obr. 1: Informační systém podniku [1, str. 62]	10
Obr. 2: Objekty zabezpečení a ochrany [vlastní zpracování]	11
Obr. 3: Schéma řešení informační bezpečnosti [1, str. 54]	15
Obr. 4: Největší hrozby z hlediska informační bezpečnosti [12]	35
Obr. 5: Druhy ztrát podnikových dat [vlastní zpracování]	41
Obr. 6: Grafické zobrazení výsledků dotazníku testu bezpečnosti	43
Obr. 7: Graf ztráty dat dle specifikovaného původce	44
Obr. 8: Výsledek penetračního testu	46
Obr. 9: Výsledek testu na přítomnost spyware	49
Obr. 10: Nasazení záložního zdroje APC	69
Obr. 11: Workshop a přednáška na téma informační bezpečnosti	70
Obr. 12: Výsledky testu bezpečnosti po provedení navržených řešení	73

SEZNAM TABULEK

Tab. 1: Výsledky dotazníku testu bezpečnosti.....	42
Tab. 2: Výpočet stupně dopadu jednotlivých druhů ohrožení.....	44
Tab. 3: Výsledky analýzy aktuálního stavu zabezpečení.....	56
Tab. 4: Pokyny k zálohování dat.....	65
Tab. 5: Hodnotící matice	67
Tab. 6: Multikriteriální hodnocení technické úrovně záložních zdrojů	67
Tab. 7: Multikriteriální hodnocení technické úrovně záložních zdrojů –	68
Tab. 8: Výsledky multikriteriálního hodnocení technické úrovně záložních zdrojů.....	68
Tab. 9: Zásady bezpečného využívání počítačů	71
Tab. 10: Katalog opatření navrhovaných projektových řešení	72

SEZNAM PŘÍLOH

P I Dotazník testu zabezpečení dat a informací ve firmě.

PŘÍLOHA P I: DOTAZNÍK TESTU ZABEZPEČENÍ DAT A INFORMACÍ VE FIRMĚ.

Tento test představuje diagnostický a vzdělávací nástroj, který může pomoci začít na zabezpečení pohlížet jako na nezbytnou součást provozu malé firmy. Správné odpovědi a počet bodů jsou uvedeny v závorkách za každou volbou.

Obecné znalosti

1. Co je brána firewall?
 - a. Způsob ochrany počítačové sítě proti neoprávněnému přístupu z Internetu (1 bod)
 - b. Souvislá protipožární stěna kolem místnosti se servery

2. Proč vydávají výrobci softwaru aktualizace pro vlastní software?
 - a. Jsou rádi v kontaktu se zákazníky.
 - b. Tisíce útočníků se stále snaží najít dříve neznámé chyby zabezpečení a softwarové společnosti proti nim chtějí uživatele chránit. (1 bod)

3. Které z následujících možností patří mezi nebezpečné útoky?
 - a. Zcizení identity
 - b. Neoprávněné změny
 - c. Odvolatelnost
 - d. Zveřejnění informací
 - e. Odepření služby (Denial of Service, DoS)
 - f. Zvýšení oprávnění
 - g. Všechny uvedené (1 bod)

4. Došlo ve vaší firmě k některým z následujících potíží? (1 bod za každou odpověď)
 - a. Odcizení počítače
 - b. Neoprávněné zveřejnění informací zaměstnanci nebo externími uživateli
 - c. Ztráta kritických dat, která nebyla zálohována
 - d. Nákaza virem
 - e. Jakýkoli druh útoku nebo narušení zabezpečení

Plány, zásady a uživatelé

5. Dohlíží někdo z vašich zaměstnanců na potíže se zabezpečením?
 - a. Ano (1 bod)
 - b. Ne

6. Kdy jste naposledy prováděli revizi zásad zabezpečení?
 - a. V uplynulých třech měsících (2 body)
 - b. Během uplynulého roku (1 bod)
 - c. Co jsou to zásady zabezpečení?

7. Existuje osoba odpovědná za trvalé vynucení zásad zabezpečení?
 - a. Ano (1 bod)
 - b. Ne

8. Provádíte pravidelné audity inventáře počítačů a softwaru?
 - a. Ano (1 bod)
 - b. Ne

9. Má vaše firma aktuální zásady zahrnující následující? (1 bod za každou odpověď)
 - a. Zásady přijatelného používání
 - b. Zásady vzdáleného přístupu
 - c. Zásady ochrany informací
 - d. Zásady ochrany proti virům
 - e. Zásady hesel
 - f. Zásady zabezpečení hranice sítě

10. Vědí vaši zaměstnanci, co jsou to smyšlené e-maily a jak s nimi naložit?
 - a. Ano (1 bod)
 - b. Ne

Fyzické zabezpečení

11. Pomocí jakých fyzických opatření chráníte klientské počítače? (1 bod za každou odpověď)
- a. Zámky, poplašná zařízení a fyzické zábrany
 - b. Správa přístupu návštěvníků
 - c. Počítače bezpečně upevněné ke stolům
 - d. Zaznamenaná výrobní čísla součástí
 - e. Neviditelnost počítačů z ulice
 - f. Poloha monitorů jinak, než proti oknům, ve všech patrech
12. Pomocí jakých fyzických opatření chráníte své servery? (1 bod za každou odpověď)
- a. Umístění v bezpečné místnosti
 - b. Omezení přístupu pouze na oprávněné osoby
 - c. Přiměřená protipožární ochrana
 - d. Zaznamenaná výrobní čísla součástí
 - e. Záložní zdroj napájení
 - f. Uzamčení ve skříních RACK s přístupem pouze vyjmenovaných osob ke konkrétním systémům v konkrétní skříně
13. Pomocí jakých fyzických opatření chráníte přenosné počítače? (1 bod za každou odpověď)
- a. Počítače jsou přenášeny v anonymních brašnách
 - b. V případě nepřítomnosti jsou zabezpečeny kabelovým zámkem
 - c. Součásti jsou bezpečnostně označeny
 - d. Data v počítači jsou šifrována
14. Pomocí jakých fyzických opatření chráníte software a zálohy? (1 bod za každou odpověď)
- a. Média a licenční dokumenty jsou uloženy na bezpečném místě
 - b. Zálohy jsou uloženy v protipožárním trezoru či mimo prostory organizace
15. Máte sjednání smlouvy na údržbu počítačového vybavení?
- a. Ano (1 bod)
 - b. Ne

16. Zjišťujete při pohovorech s konzultanty pro oblast zabezpečení jejich zkušenosti a kvalifikaci?

- a. Ano (1 bod)
- b. Ne

Zabezpečení informací

17. Otevřeli jste někdy přílohu e-mailu od neznámého odesílatele jen proto, že vypadala zajímavě?

- a. Ano
- b. Ne (1 bod)

18. Které z následujících mechanismů máte nasazeny v provozní síti? (1 bod za každou odpověď)

- a. Aktualizace softwaru se instalují ihned po vydání
- b. Pravidelně se aktualizují definice virů
- c. Je nainstalována a správně nakonfigurována brána firewall
- d. Centrálně jsou vynuceny zásady silných hesel
- e. Procházení webu a používání e-mailu odpovídá zásadám
- f. Zabezpečené připojení vzdálených uživatelů
- g. Zabezpečená bezdrátová síť
- h. Pravidelné zálohování

19. Zálohujete pravidelně svá data?

- a. Ne
- b. Ano (1 bod)
- a. Bod navíc: Pravidelně testujete obnovení dat

20. Testujete pravidelně své zálohy obnovením a následnou kontrolou?

- a. Ne
- b. Ano (1 bod)

21. Používáte nejnovější verze aplikací Microsoft Internet Explorer a Microsoft Outlook?

- a. Ne
- b. Ano (1 bod)

22. Používáte v bezdrátové síti šifrování?

- a. Ne
- b. Ano (1 bod)

Výsledky testu:

Méně než 10 bodů: Vážně se zamyslete nad studiem problémů zabezpečení a vytvořte plán zabezpečení (nebo si jej nechte vytvořit).

11 až 20: Víte, že zabezpečení je nutné, ale nemáte dostatečné znalosti, čas ani přesvědčení s tím něco udělat. Riziko je velké a k ochraně firmy je třeba provést některé kroky.

21 až 30: Jste na tom podobně jako ostatní. Vaše záměry jsou dobré, provedli jste některé kroky, ale nejvíce ze všeho doufáte, že se vám nic špatného nepříhodu. Existují kroky, jejichž okamžité provedení změní stav zabezpečení z „téměř dostatečné“ na „dostatečně dobré“.

31 až 40: Vaše situace je poměrně dobrá. Projděte si znova jednotlivé kroky zabezpečení a pokuste se najít, co vám ještě chybí. Možná jste něco přehlédli, možná jste nevážili všechna rizika.

41 až 50: Vedete si výborně. Přesto si ale projděte jednotlivé kroky zabezpečení a zjistěte, zda jste něco nepřehlédli. Nezapomeňte na nutnost provádět revize zabezpečení a aktualizovat svůj plán.

Více než 50 bodů: Není co dodat.