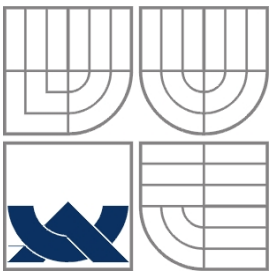
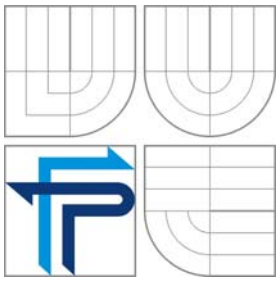


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

BEZPEČNOSTNÍ POLITIKA SPOLEČNOSTI

COMPANY´S SECURITY POLICY

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE — IVANA NOVOTNÁ
AUTHOR

VEDOUCÍ PRÁCE — Ing. VIKTOR ONDRÁK, Ph.D.
SUPERVISOR

BRNO 2007

Vysoká škola: Vysoké učení technické v Brně | Akademický rok: 2006/2007

Fakulta: podnikatelská | Ústav: informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Ivana Novotná

6209R021 - Manažerská informatika

Ředitel ústavu v souladu se zákonem č. 111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů Vám zadává bakalářskou práci s názvem:

Bezpečnostní politika společnosti

Company`s Security Policy

Pokyny pro vypracování:

Úvod
Cíl práce
Analýza současného stavu
Teoretická východiska řešení
Návrh řešení
Zhodnocení a závěr

Rozsah grafických prací:	dle potřeby
Rozsah původní zprávy:	cca 40 stran

Seznam odborné literatury:

Lockhart, A.: Bezpečnost na maximum. Brno: Computer Press a.s., 2005.
Horák, J.: Počítačové sítě pro začínající správce. 3. aktualizované vydání. Brno: Computer Press a.s., 2006.
Northcutt, S.: Bezpečnost počítačových sítí – Kompletní průvodce návrhem, implementací a údržbou zabezpečené sítě. Brno: Computer Press a.s., 2005.
Kretchmar, J. M.: Administrace a diagnostika sítí. Brno: Computer Press a.s., 2005.
Doseděl, T.: Počítačová bezpečnost a ochrana dat. Brno: Computer Press a.s., 2004.
Walter, H.: Jak zabezpečit Exchange Server 2003 a Outlook Web Access. Brno: Computer Press a.s., 2005.

Vedoucí bakalářské práce:	Ing. Viktor Ondrák, Ph.D.
Datum zahájení bakalářské práce:	31. října 2006
Datum odevzdání bakalářské práce:	31. května 2007

Ing. Jiří Kříž. Ph.D.
Ředitel ústavu

Doc. Ing. Miloš Koch, CSc.
Děkan

V Brně dne: 16. února 2007

Abstrakt

Předkládaná bakalářská práce komplexně analyzuje problematiku IT bezpečnosti konkrétního českého podniku střední velikosti, a navrhuje rovněž ucelené řešení této problematiky včetně praktické implementace. Vzhledem k rozsahu problematiky jsem zvolila oblast bezpečnostní politiky společnosti.

Abstract

Presented Bachelor’s thesis comprehensive analyses problems of IT security of concrete Czech company medial size and suggests integrated solution of this sphere including practical implementation at the same time. According to the extent of problems I choose section of company’s security policy.

Klíčová slova

Bezpečnost, bezpečnostní politika, bezpečnostní směrnice, bezpečnost dat, informační systém, zálohování dat

Keywords

Security, security policy, security instructions, data security, information system, data backup

Bibliografická citace

NOVOTNÁ, I. *Bezpečnostní politika společnosti.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2007. 61. s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph.D.

Prohlášení autora o původnosti práce

Prohlašuji, že jsem předloženou bakalářskou práci zpracovala samostatně a pod vedením svého vedoucího bakalářské práce. Prohlašuji, že citace použitých pramenů je úplná a příslušné prameny uvádím v literatuře.

V Brně, dne 22. května 2007 ……

Podpis

Poděkování

Chtěla bych poděkovat vedoucímu bakalářské práce panu Ing. Viktoru Ondrákovi, Ph.D. za odborný dohled, za cenné rady a připomínky při zpracování bakalářské práce.

Obsah

1 Úvod ... 12
1.1 Cíl práce ... 13
2 Analýza současného stavu ... 14
2.1 Informace o firmě ... 14
2.2 Organizační struktura firmy ... 14
2.3 Počítačová síť ... 15
2.4 Informační technologie používané ve firmě ... 16
2.4.1 Hardware ... 16
2.4.1.1 Stolní PC ... 16
2.4.1.2 Servery ... 17
2.4.1.3 Notebooky ... 18
2.4.1.4 Zařízení se vzdáleným přístupem ... 18
2.4.2 Software ... 19
2.4.2.1 Operační software ... 19
2.4.2.2 Aplikační software ... 19
2.5 Archivace dat a zálohování ... 20
2.6 Vzdálený přístup k vnitropodnikovým datům ... 21
2.7 Webové stránky ... 22
2.8 Citlivá data ... 22
2.9 Současná bezpečnostní politika ... 24
2.10 Topologie IT oddělení ... 25
3 Teoretická východiska ... 26
3.1 Co je to bezpečnostní politika ... 26
3.2 Identifikace firemních dat (Analýza rizik) ... 28
3.2.1 Identifikace aktiv ... 28
3.2.2 Identifikace hrozeb ... 28
3.2.3 Vlastní analýza rizik ... 29
3.2.4 Navržení vhodné ochrany ... 29
3.3 Zabezpečení dat proti ztrátě ... 29
3.4 Útočníci a hrozby ... 30
3.5 Zásady zabezpečení (typy) ... 32

3.5.1 Jak vytvořit zásady ... 32
3.5.1.1 Vymezení rizik ... 32
3.5.2 Vytvoření zásad zabezpečení a stanovení podmínek ... 33
3.5.3 Důležité součásti zásad ... 34
3.5.4 Dobré vs. špatné zásady zabezpečení ... 35
3.6 VPN (Virtual Private Network) ... 36
3.6.1 Základní fakta ... 36
3.6.2 Výhody a nevýhody tunelů VPN ... 37
3.7 Archivace a zálohování ... 39
3.7.1 Zálohování ... 39
3.7.1.1 Práce se záložními kopiemi ... 41
3.7.1.2 Obnova dat ... 41
3.7.2 Archivace ... 41
3.8 Zákony a normy ... 42
4 Návrh řešení ... 43
4.1 Organizační struktura správy bezpečnosti ... 44
4.2 Ochrana fyzického přístupu ... 45
4.3 Ochrana logického přístupu ... 47
4.4 Ochrana firemních dat ... 48
4.5 Ochrana přenášených dat ... 52
4.6 Ochrana dat před zničením ... 54
5 Zhodnocení a závěr ... 57
6 Literatura ... 58
7 Přílohy ... 61
7.1 Příloha č. 1 k zákonu č. 499/2004 Sb. ... 61

1 Úvod

Bezpečnost obecně je poměrně mladý a současně důležitý obor, proto je v dnešní době toto téma hodně diskutované. Bezpečnost je velmi rozsáhlá, proto jsem si jako téma své bakalářské práce vybrala užší část, a to bezpečnostní politiku společnosti.

Bezpečnostní politika stanovuje, co se musí provést s ohledem na ochranu informací uložených v počítačích. Dobře napsané zásady musí obsahovat dostatečně jasný popis toho, „co“ udělat a „jak“ jejich vykonávání rozpoznat a změřit nebo posoudit.

V první části mé práce analyzuji současný stav existující české akciové společnosti střední velikosti, která nechce být z důvodu citlivosti dat v práci obsažených jmenována. Z tohoto důvodu ji budu označovat jako společnost XY a.s. Pro tuto společnost je velmi důležité, aby její bezpečnostní politika byla bezchybná, protože její podnikání je ve značné míře založeno na informačních technologiích a informací v digitální podobě, a její informační systém obsahuje rovněž důležitá data, ať už podléhající režimu utajení z obchodních důvodů nebo data, která spadají pod zákon o ochraně osobních údajů.

Druhá část práce obsahuje teoretická východiska, ze kterých jsem ve své práci vycházela. Stav teorie, definic i terminologie v oblasti IT bezpečnosti je dosud z důvodu dynamičnosti poměrně neustálený, proto je tato část poměrně rozsáhlá, aby bylo zřejmé, z jakých teoretických prací jsem vycházela.

Třetí část obsahuje návrh řešení současného stavu. Je proveden rozdělením problematiky na jednotlivé problémy či problematické oblasti, a návrhem opatření spolu s vytvořením, zavedením a kontrolováním příslušných směrnic.

Věřím, že moje práce bude ve sledované společnosti k dispozici a poznatky a návrhy v ní uvedené budou využity v praxi ke zlepšení stávajícího stavu.

1.1 Cíl práce

Cílem mé práce je s využitím detailní analýzy stávajícího stavu a existující bezpečnostní politiky navrhnout takové řešení, které by v dané společnosti zlepšilo bezpečnostní politiku a lépe ochránilo společnost zejména v těchto oblastech: ochrana fyzického a logického přístupu, ochrana firemních dat, ochrana přenášených dat a ochrana dat před zničením.

2 Analýza současného stavu

2.1 Informace o firmě

Firma se kterou jsem spolupracovala na tvorbě bakalářské práce nechce být z důvodu citlivosti dat v ní obsažené zveřejněna, proto ji budu uvádět pod názvem XY.

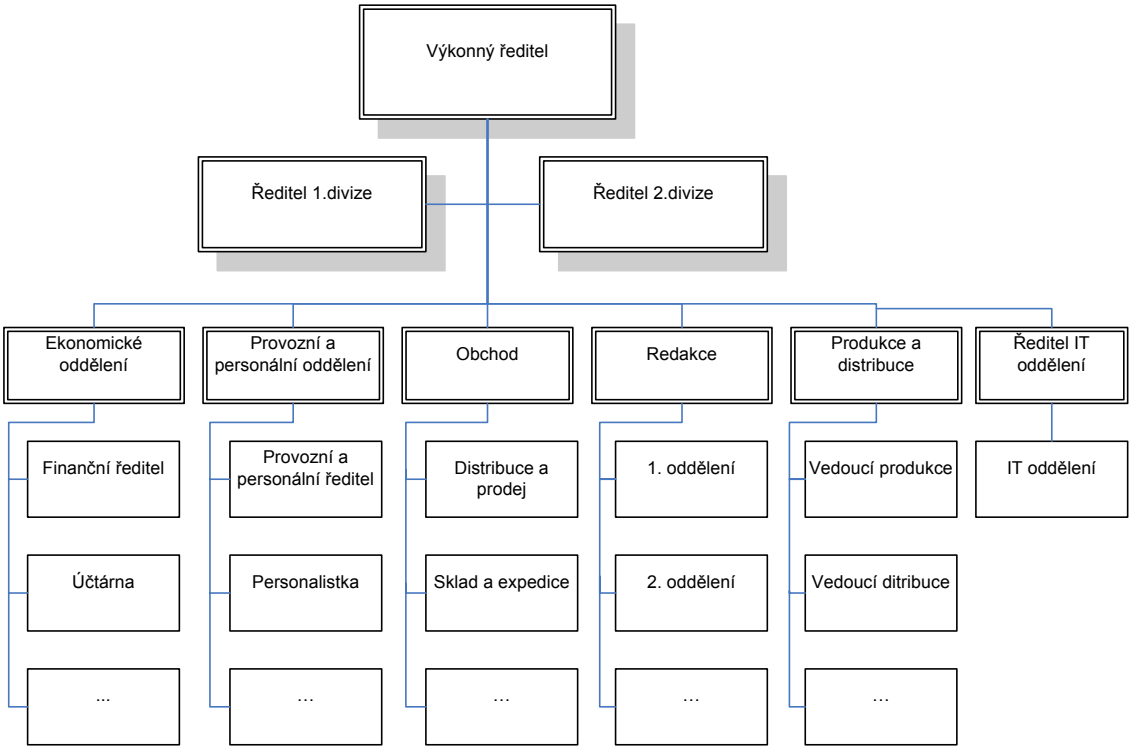
XY je českou akciovou společností s hlavním sídlem v Brně. Dále má pobočky v Praze, Ostravě a Bratislavě. V Brně sídlí ve 3 budovách, dvě z toho jsou samostatně stojící domy a třetí je panelový dům v městské zástavbě.

Společnost se zabývá výrobní a obchodní činností. Na trhu je 13 let a její roční obrat činí okolo 0,5 mld. Kč. Firma rovněž provozuje, spravuje a rozvíjí webové servery pro vlastní účely, což je pro tento typ organizací zvláštností, protože většina podniků si své webové stránky nechává provozovat jinou, specializovanou společností.

XY zaměstnává 250 zaměstnanců, kteří se převážně zabývají duševní činností, proto zhruba 95% z nich má k dispozici stolní počítač. Polovina má přístup k vnitropodnikovým datům rovněž přes domácí nebo přenosné PC, tzn. že jsou propojeni k firemním datům i z bydliště, či případně z přenosného počítače z jakéhokoli jiného místa s internetovou konektivitou.

2.2 Organizační struktura firmy

Organizační struktura firmy je funkcionální. Není popsána kompletně a konkrétně z důvodu toho, že by mohlo vyplynout, o jakou firmu se jedná.

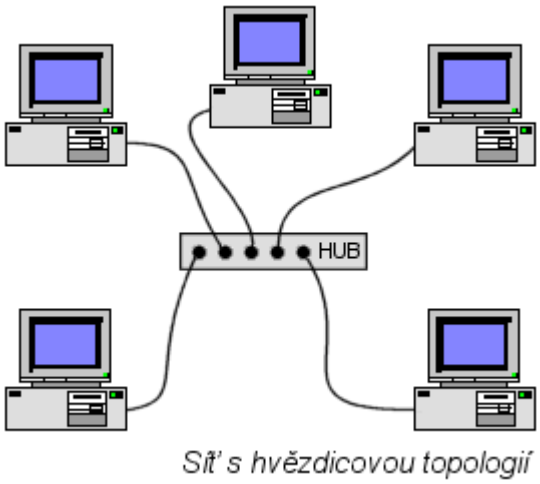


Obrázek 1. Organizační struktura firmy.

2.3 Počítačová síť

Lokace jsou spojeny strukturovanou kabeláží typu Belden & Panduit, kde kabeláž je od firmy Belden a konektory od firmy Panduit. Komunikace mezi pobočkami probíhá pomocí internetu, komunikace je mezi pobočkami šifrována, u vzdáleného přístupu šifrování neprobíhá. Společnost nevyužívá VPN (Virtual Private Network) z důvodu toho, že v době vzniku a rozvoje firmy toto řešení bylo velmi drahé a firma neshledala toto řešení nutným. Firma využívá 100 Mbit/s Ethernet a na 4 portech, které jsou na switchi volitelné, využívá 1 Gbit/s Ethernet. Ve dvou pobočkách v Brně je vybudováno připojení k internetu pomocí wi-fi sítě. Toto řešení bylo zavedeno hlavně kvůli jednáním v jednacích místnostech, na které si zaměstnanci nosí notebooky, aby se kdykoliv mohli připojit do sítě a měli tak přístup k firemním datům. Tato síť je chráněna heslem.

U stolních počítačů se využívá hvězdicová topologie, kde každý počítač (stanice) je připojen vlastním kabelem. Střed sítě tvoří rozbočovač. Předností této topologie je, že když dojde k poruše na jednom kabelu, neovlivní to celou síť, ale jen danou stanici.



Obrázek 2. Hvězdicová topologie. 16)

2.4 Informační technologie používané ve firmě

Firma využívá na počítačích převážně platformu Windows od společnosti Microsoft. Hardware používá od řady výrobců i dodavatelů, nevyužívá služeb systémového integrátora. Stáří hardwaru se pohybuje od 0 do 7 let. Průměrné stáří je 3 roky a vybavení se dle potřeby inovuje.

2.4.1 Hardware

Ve firmě se hardware rozděluje na tyto hlavní části: stolní počítače, servery, notebooky a zařízení se vzdáleným přístupem jako například tiskárny.

2.4.1.1 Stolní PC

Nejčastějším hardwarem v celé firmě jsou stolní počítače. Na pobočkách v Brně je jich zhruba 140. Výrobci počítačů jsou různí, často se jedná o počítače „podomácku“ skládané z komponentů rozličných výrobců. Firma nevyužívá služeb jednoho dodavatele, rovněž své dodavatele často mění zejména podle výhodnosti cenových nabídek. I vybavenost počítačů je různá, liší se podle potřeb oddělení a jejich zaměstnanců. Všechny počítače jsou však, mimo jiné, vybaveny DVD nebo CD zapisovací mechanikou, disketovou mechanikou a USB porty. Stolní počítače se vesměs pronikavě liší ve výkonnosti procesorů, velikosti pevných disků, výkonnosti grafických karet, atd.

2.4.1.2 Servery

Firma používá zhruba 50 serverů, jejich počet se v čase dosti proměňuje. Rovněž servery využívají majoritně platformu Windows, pouze na třech serverech běží operační systém Linux, který slouží pro webové aplikace. Dva z nich jsou webové servery s PHP a třetí je databázový server mySQL. Na všech ostatních serverech běží operační systém od společnosti Microsoft. Stáří serverů se pohybuje v průměru kolem 3 let a jsou vesměs od světových značkových výrobců, jako je Hewlett Packard, Dell, Compaq, SuperMicro či Fujitsu Siemens, některé jsou od českých výrobců (AT Computers atd.).

Všechna aktiva se ukládají na servery. Například do souborových serverů se ukládají všechna data typu souborů; do aplikačních, různé aplikace, které zaměstnanci potřebují k práci; do databázových všechny databáze, jako například databáze zákazníků; do tiskových tiskové úlohy; do poštovních pošta, která přichází i odchází z firmy; do webových obsah webových stránek a informace o jejich provozu; atd.

Data se ukládají na specializované servery, které jsou vybaveny diskovými poli. Velikost diskového datového pole v hlavní budově je 3,5 TB a ve vedlejší budově 800 GB. Jelikož se na disky ukládají všechna data, jediným ochranným prvkem je využití tzv. RAIDu u diskových polí. Firma využívá metodu RAID 5. Kvůli redundanci dat je zapotřebí více disků, konkrétně 14 x 300 GB na jedné pobočce a 4 x 300 GB na druhé pobočce. Servery jsou umístěny ve skříni, tzv. racku. Firma má tři serverové místnosti. Dvě jsou v budovách firmy a třetí, která slouží pro umístění webových serverů, je umístěna na páteřní síti u společnosti Telefonica O2 Czech Republic. Důvod umístění webových serverů na páteři spočívá v silném toku dat, který ve špičce dosahuje 80 Mbps, což je možné realizovat na stávající infrastruktuře pouze na republikové páteřní síti; dalším důvodem je též bezpečnost.

Serverové místnosti jsou umístěny a provozovány podle pravidel daných výrobcem, tzn. v místnosti je dodržována teplota kolísající v povoleném rozpětí, bezprašné a bezvibrační prostředí, atd. Dveře serverové místnosti jsou zabezpečeny zámkem typu FAB, dále čidlem a přístup je povolen jen vyhrazeným osobám z IT oddělení. U větších firem je zvyklostí umístění serverových místností mimo firmu, právě z důvodů bezpečnosti (možná havárie, živelná pohroma, narušení atd.). Mnou popisovaná firma je střední společnost a má serverové místnosti umístěny přímo v budovách sídla.

V hlavním sídle je serverová místnost umístěna v suterénu a v druhé budově je hned za vstupem na více méně veřejně průchozím místě (po otevření dveří recepční).

2.4.1.3 Notebooky

Externí pracovníci, obchodníci a manažeři používají notebooky, jejichž největší výhodou je samozřejmě mobilita, zaměstnanci mohou pracovat i doma a kdekoliv na cestách po celém světě. V brněnských pobočkách je jich zhruba 40. Jsou opět různých značek, nicméně převažují výrobky firem Dell, Hewlett Packard a Acer. Jejich vybavenost se opět liší podle potřeb zaměstnanců. U většiny těchto notebooků je k dispozici zařízení pro wi-fi připojení, ať už z důvodu možnosti připojení na obou pobočkách, ale také z důvodu cestování zaměstnanců a potřeb přístupu k firemním datům.

2.4.1.4 Zařízení se vzdáleným přístupem

Firma využívá multifunkční tiskárny, ty jsou umístěny pro všechna oddělení kromě účetního v centrální části budovy. Důvody umístění v centrální části jsou především následující: může se kontrolovat, co se ve firmě tiskne, zda si někdo netiskne dokumenty pro vlastní potřebu a nebo naopak netiskne dokumenty s citlivými daty. V praxi však tato kontrola příliš neprobíhá. Na pobočkách v Brně je zhruba 25 tiskáren. Většinou jsou laserové, ale firma vlastní také jednu barevnou laserovou tiskárnu a jednu voskovou (xerox) tiskárnu. Nejčastějšími značkami jsou Hewlett-Packard a Canon. Tyto multifunkční tiskárny se dají použít také jako například skener do e-mailů apod. Účetní oddělení má k dispozici svou vlastní tiskárnu z důvodu častého tisku.

V každé budově je jedna ústředna, kde se používají analogové bezdrátové telefony. Jejich výhoda je v tom, že se zaměstnanci mohou během telefonování pohybovat po celé budově bez přerušení signálu.

Ředitelé, manažeři, obchodníci a vedoucí odděleních vlastní služební mobilní telefony různých značek, převládají Nokia, Siemens a Sony Ericsson. Někteří také vlastní tzv. smart phones, což jsou telefony, které v sobě mají nainstalovaný operační systém a umožňují přístup na internet. Na stejném principu pracují též kapesní počítače, které jsou ve firmě rovněž rozšířené.

2.4.2 Software

Ve společnosti se rozděluje software na operační a aplikační software.

2.4.2.1 Operační software

Firma využívá dominantně platformu Microsoft a nainstalovanými operačními systémy na stolních počítačích jsou Microsoft Windows XP Professional Edition. Pro servery se používá operační systém Microsoft Windows Server 2000 (5x) a Microsoft Windows Server 2003 Standard. Pro poštu používá Microsoft Exchange 2003 Standard EN (4x).

Na třech serverech je nainstalován operační systém Linux Fedora 6.4, je to z důvodu již existujících zakoupených webových aplikací vytvořených na této platformě.

2.4.2.2 Aplikační software

Firma používá kancelářský balík Microsoft Office 2003 a 2007, pro poštu poštovního klienta Microsoft Office Outlook 2003, pro databáze SQL Server 2000 Standard EN (2x), SQL 2005 Express (5x) a SQL 2005 Standard (2x). Informační systém, pro vlastní potřeby firmy (např. docházkový systém, správu autoparku, zasedacích místností, atd.), používá svůj vlastní, který vytvořil zaměstnanec IT oddělení. Ekonomický systém je používán Microsoft Navision Financial 4.0. Jako další druh komunikace firma povolila využívání komunikačních programů ICQ a Skype, nicméně příliš nebrání využívání jiných komunikačních programů a služeb.

Věnujme se nyní zmíněnému informačnímu systému. Je to vlastně rozhraní k webové aplikaci ASP. Úvodním článkem tohoto systému je docházkový systém, který je pracovně nazván „Dveřník“. Ihned u vstupu do budovy je umístěn počítač, na kterém běží pouze tato aplikace. Uživatel (zaměstnanec) přijde, zadá svůj autentický kód a po přihlášení do této aplikace si může vybrat zda přišel do práce, odchází, jestli jede na služební cestu, kdy se z ní vrátí, zda-li má dovolenou, do kdy, apod. Tato data se pak přenáší do informačního systému a recepční vidí, kdo je v práci, kdo má dovolenou, kdo má jaké auto půjčené a kdy ho vrátí. Pak může zcela informovaně odpovídat na otázky zákazníků, tak i zaměstnanců. V tomto systému jsou i veškeré informace ohledně zaměstnanců, jsou tam e-mailové adresy, klapky, mobilní čísla, pozice, atd. Jsou zde vystaveny i různé manuály, směrnice a rady, novinky, fotogalerie z různých

společenských akcí a vůbec informace ze života firmy. Vedoucí zde mohou zadávat hodnocení zaměstnanců, psát komentáře k prémiím apod. Tato aplikace je zabezpečena certifikátem SSL.

Přístup do pošty je zabezpečen pomocí hesla, které se ověřuje podle uživatelského účtu. Server kontroluje příchozí i odcházející poštu na viry a na spam. Nejsou zde sledována klíčová slova a potenciálně podezřelé adresy (jako například příjemce je konkurenční firma) nebo zda se odesílají velké přílohy. K poště se dá také přistupovat vzdáleně přes webové rozhraní pomocí tzv. Web Accessu, který podporuje zakoupený rozšířený balíček MS Outlook o tuto funkci.

Firma používá dva druhy antivirů. Na poštovním serveru MS Exchange je Trend Micro Scanmail 6 for Exchange 2000 a 2003 na klientských stanicích je CA eTrust 8.0. Antiviry jsou spuštěny pořád, proto neustále kontrolují veškerou činnost a tak chrání síť před napadením virem, či jiným škodlivým softwarem.

Datově jsou servery chráněny z vnější sítě firewallem Microsoft ISA 2004 Standard Edition. Firewall nastavuje a obsluhuje IT oddělení, ale směrnice k jeho používání vytvořena není. K serverům se vždy přistupuje přes prostředníka, tzn. přes různé aplikace, nikdo bez práv administrátora se nemůže připojit přímo na server. Dále je přístup ošetřen podle práv, kdy nejvyšší práva má administrátor. Řídí se podle hesla, „čím kritičtější data, tím méně lidí k nim má přístup“, proto přístupy řeší tak, že se vše zakáže a pak se postupně povolují přístupy, které daný zaměstnanec potřebuje k práci. Tento princip je však zaveden spíše zvykově, neexistuje přesný popis či směrnice.

2.5 Archivace dat a zálohování

Ve firmě je obrovské množství průběžně se měnících dat a společnost proto neprovozuje jejich kompletní zálohování. Proto se zálohují jen ta data, jejichž ztráta nebo poškození by způsobila velkou hospodářskou či časovou újmu. Ve firmě vznikají autorská díla, která se zálohují ihned po vytvoření tím, že se vypálí na datové médium, v současnosti nejčastěji na DVD. Další data jako pošta, databáze (např. zákazníků), ekonomické informace (např. účetnictví, údaje o prodeji), webové logy (které se musí archivovat ze zákona) se zálohují automaticky pomocí programu Hewlett Packard Open

View Data Protector. Jednou týdně firma provádí úplnou zálohu, ta probíhá o víkendu, a každý den se provádí rozdílová záloha, která probíhá v nočních hodinách, kdy ve firmě není žádný zaměstnanec a uložená data se nemění. Data se zálohují na pásky do páskové knihovny. Firma od tohoto typu zálohování pomalu upouští z důvodu dlouhé doby zálohy, opotřebovanosti pásek, kdy se může stát, že páska už nemusí být čitelná a tím ztratit data uložená na dané pásce. Musí se kupovat nové pásky, což se časem prodraží. Proto stále častěji využívá zálohu na pevné disky. V dnešní době, kdy klesají ceny pevných disků, zvyšuje se jejich kapacita, rychlost zápisu a čtení je mnohem výhodnější koupit pevné disky i o kapacitě celého diskového pole a zálohovat na ně. Záloha je rychlejší, kapacita disků je vyšší a v celkové ceně zálohovacích médií začíná vycházet pevný disk levněji.

Jelikož se nejedná o kriticky tajná data, uchovávají záložní kopie přímo v budově firmy.

Ve firmě se archivují data, která jsou dána zákonem číslo *499/2004 Sb. Zákon o archivnictví a spisovné službě a o změně,* konkrétně v *Příloze 2* tohoto zákona. Zkrácené znění tohoto zákona uvádím v příloze 1. Jsou to zejména zakladatelské dokumenty, stanovy, organizační řády a schémata, dokumenty o změně právní formy, výroční zprávy, zprávy o auditu, finanční dokumenty, účetní záznamy, katalogy s ceníky, různé publikace vydané firmou, kolektivní smlouvy a další. Existuje směrnice, která upravuje, jak má archivace probíhat a jak se mají archivovaná data ukládat.

2.6 Vzdálený přístup k vnitropodnikovým datům

Vzdáleným přístupem se rozumí přístup k vnitropodnikové síti a k podnikovým datům odjinud než z firmy. Do této kategorie spadá přístup například z domova zaměstnance, připojení notebookem přes internetovou síť, ať už v internetové kavárně nebo někde na veřejném místě přes wi-fi síť, v hotelu a na dalších místech, či podobné připojení pomocí kapesního počítače či tzv. smart mobilu. K vnitropodnikové síti se přistupuje pomocí hesel. U vzdáleného přístupu k síti není přístup vázán na určité IP adresy, proto zde hrozí velké riziko, že by mohlo dojít k odposlechu hesla (zejména přes veřejnou wi-fi síť, které nebývají velmi často zabezpečené) a poté přihlášení cizí osoby k firemní síti a tím získání dat, ke kterým má daný zaměstnanec přístup.

K podnikové síti a podnikovým datům rovněž může přistupovat řada domácích PC, které nejsou vlastněny firmou (jsou majetkem jejích zaměstnanců). Firma k těmto počítačům nemá přístup, a proto nemůže být kontrolována bezpečnost nainstalovaného softwaru. Je pravděpodobné, že se na těchto počítačích nalézá nelegálním způsobem pořízený software, že na nich nejsou nainstalovány účinné antivirové programy, firewally a ostatní důležitý software k ochraně PC. Proto domácí počítač může být infikován různým škodlivým softwarem jako jsou viry, červi, keyloggery a jiný software, který může sledovat vše, co se na počítači děje a tyto informace zneužívat.

Vzdálený přístup využívají také zaměstnanci, kteří obchodně cestují po celém světě a potřebují firemní data. Mohou se připojit pomocí notebooků například z hotelů, internetových kaváren nebo z veřejných míst, kde funguje wi-fi připojení k internetu. Tito zaměstnanci ale převážně vlastní firemní notebooky, tudíž firma tyto notebooky může kontrolovat. Je ne nich instalován pouze povolený a legálně zakoupený software a aplikace, které chrání počítač proti škodlivému softwaru.

2.7 Webové stránky

Všechny webové stránky, které firma provozuje jsou založeny na http protokolu. Je použit i u internetového obchodu. Webové stránky se dají rozdělit na dvě části, na tu „zadní“ back-end, kterou uživatel nevidí, tj. správa, a na tu „přední“ front-end, kterou uživatel vidí. Správu webových stránek a serverů zajišťují administrátoři. Ti mají právo mazat, editovat a přidávat cokoliv (materiály) na webové stránky, ke kterým mají přístup. Přístup je řízen systémem přístupových práv. Administrátoři nemají přístup k jiným stránkám než k těm, kterých jsou autoři nebo k těm, ke kterým mají výslovně přiřazen přístup. Správa probíhá pomocí administračního programu, což je rychlejší a přehlednější než úprava zdrojového kódu.

I v tomto případě mají administrátoři přístup ke správě přes vzdálený přístup k firemní síti a opět jen pomocí hesla.

2.8 Citlivá data

Ve sledované firmě vznikají, se distribuují a ukládají (zálohují) data různého významu a různé citlivosti z pohledu bezpečnosti. Firma však v současné době úrovně

citlivosti neurčuje a zachází v podstatě „se všemi daty stejně“. Analýzou jsem zjistila, že společnost pracuje s následujícími typy dat (z pohledu bezpečnosti a citlivosti):

- Databáze zákazníků včetně korespondenčních údajů, zákaznické historie a jednotlivých plateb (jedná se o databázi sledující caa 120 000 unikátních zákazníků)
- Databáze velkoobchodních odběratelů a dodavatelů s korespondenčními údaji a jejich veškerou obchodní historií (řádově několik tisíc záznamů)
- Databáze spolupracovníků společnosti včetně externích autorů, překladatelů, korektorů atd. (řádově několik set záznamů)
- Databázi produktů společnosti a jejich obchodních výsledků včetně dlouhodobé historie (řádově několik tisíc produktů)
- Databáze autorských materiálů (článků) včetně návštěvnosti či čtenosti (týká se materiálů publikovaných na webu)
- Databáze vnitropodnikových údajů personálního a mzdového charakteru včetně historie a hodnocení zaměstnanců
- Databáze firemního účetnictví (faktury, platební deníky, finanční styk se státem atd.)
- E-mailová databáze (vnitřní i vnější e-mailová komunikace) včetně příloh přikládaných k e-mailům
- Autorské materiály, se kterými firma pracuje, včetně licenčních, v různých fázích vývoje (od zdroje přes dočasné a pracovní materiály, meziprodukty až k materiálům určeným k sazbě)
- Různorodé materiály využívané zejména k ekonomickým a analytickým účelům (analýzy ve formě tabulek a písemných rozborů, přehledy trhu apod.), zápisy z porad, informace o konkurenci a další
- Materiály volně šiřitelé, publikované na webu (např. tiskové zprávy) či rozesílané obchodním partnerům

Naprostá většina těchto materiálů existuje pouze v elektronické (digitální) podobě, některé z nich se vytvářejí v tištěné kopii, přičemž se s nimi následně zachází obvykle bez jakékoli kontroly (šíření, povinná skartace atd.)

2.9 Současná bezpečnostní politika

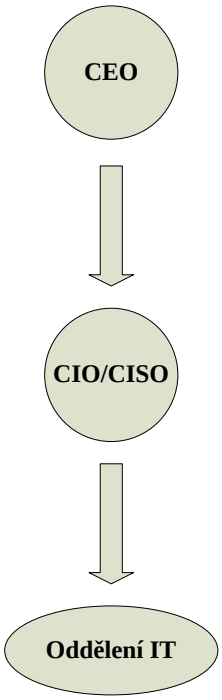
Bezpečnostní politika je ve firmě zažitá z důvodu stálosti zaměstnanců a jsou to spíše nepsaná pravidla. Existuje stručný dokument, který obsahuje zejména následující pravidla:

- Co musí směrnice všechno obsahovat a kde jsou umístěny k nahlédnutí.
- Jak probíhá přijímání pracovníků, jak probíhá zaškolení, jaká přístupová práva dostávají, u koho se mají hlásit, kdo je proškolí o bezpečnosti.
- Jak se tvoří přístupová hesla, že musí být silná, co to znamená, jak často se mají měnit, k jakým přístupům slouží.
- Jak se má používat antivir, jak ho aktualizovat a jak často.
- Zákaz stahování nelegálních programů z internetu.
- Pokud se vyskytne problém, za kým jít a jak ho řešit.
- Co se zálohuje, jak často, na jaká média, kdo za to zodpovídá.
- Používání wi-fi sítě.
- Archivace a skladování archivovaných dat.
- Jak probíhá odchod zaměstnance z firmy, kdo blokuje účet, jak je zajištěno neodnesení citlivých dat z firmy.

Všechny dokumenty vytváří IT oddělení. Co se týče nástupu a výstupu zaměstnanců, spolupracuje IT oddělení s personálním oddělením a také s oddělením, které má na starosti majetek (například, jestli odcházející zaměstnanec vše vrátil, atd.).

2.10 Topologie IT oddělení

Firma se postupně rozrůstala z malé společnosti po středně velkou. Organizační struktura oddělení zůstala stejná. Nejvyšším kontrolorem je tzv. CEO (Chief Executive Officer), firma používá český název generální ředitel. Dalším stupněm je tzv. CIO (Chief Information Officer), tedy ředitel IT oddělení, který však vykonává i funkci tzv. CISO (Chief Information Security Officer), což je ředitel bezpečnosti; ve sledované firmě má označení „manažer IT“. Pod ředitelem IT je samotné IT oddělení, které se skládá z tzv. administrátorů IT. Tito administrátoři však nemají pevně stanovené funkční místa.



Obrázek 3. Organizační struktura IT oddělení.

3 Teoretická východiska

Bezpečnost v IT je dosud mladým odvětvím s ne zcela ustálenou teoretickou základnou. Proto jsem do práce zařadila kapitolu, která stručně definuje hlavní pojmy a principy IT bezpečnosti, které jsem v práci využívala.

Kompletní teoretická východiska není možné ani účelné v této práci publikovat. Odkazuji proto na následující odbornou publikaci o kterou jsem v oblasti teorie bezpečnosti IT opírala:

- NORTHCUTT, Stephen. Bezpečnost počítačových sítí – Kompletní průvodce návrhem, implementací a údržbou zabezpečené sítě. Brno: Computer Press a.s., 2005.

3.1 Co je to bezpečnostní politika

Všude se dozvídáme o tom, jak máme to a ono dělat podle platných zásad bezpečnosti (neboli bezpečnostní politiky), ale nikdo nám nevysvětlí, co to vlastně je a jak se zásady mají používat. Proto jsem do mé práce zařadila tuto kapitolu.

„Zásady zabezpečení neboli bezpečnostní politika stanovuje, co se musí provést s ohledem na ochranu informací uložených v počítačích. Dobře napsané zásady musí obsahovat dostatečně jasný popis toho, „co“ udělat a „jak“ jejich vykonávání rozpoznat a změřit nebo posoudit.“ (8, s. 95)

Bezpečnostní politika je nejdůležitějším dokumentem (v oblasti bezpečnosti) ve firmě. Tento dokument by měl být písemný, protože ústní verze se mohou modifikovat a jsou pak nevynutitelné. „Bezpečnostní politika by měla odpovídat na několik základních otázek:

- Co chceme chránit?
- Proč to chceme chránit?
- Jak to chceme chránit?
- Jak ověříme, že je to opravdu chráněno?
- Co budeme dělat, když se něco pokazí?“ (2, s. 168)

Abychom mohli odpovědět na tyto otázky, potřebujeme si určit data, které ve firmě máme. Jak jsou pro nás cenná a která chceme chránit. Těmto datům se souhrnně říká aktiva (viz kapitola 3.2).

Dokument bezpečnostní politiky ve firmě může vypadat např. takto:

Bezpečnostní politika firmy	
Název dokumentu	Popis
CISO	Definuje personální zajištění bezpečnosti
Analýza rizik	Identifikuje aktiva v systému a jejich cenu
Návrh opatření	Definuje, která aktiva a jakým způsobem budeme chránit
Havarijní plány	Popisuje rozsah činností při bezpečnostních incidentech a přírodních katastrofách
Administrativní část	Stanovuje pravidelné prověřování bezpečnostní politiky apod.

Obrázek 4. Bezpečnostní politika firmy. (2, s.169)

Obrázek 5. Dělení bezpečnostních incidentů. (2, s. 22)

3.2 Identifikace firemních dat (Analýza rizik)

Než začneme vytvářet bezpečnostní politiku firmy, musíme nejprve provést analýzu rizik. Analýza se skládá ze 3 hlavních kroků, a to:

- „identifikace aktiv
- identifikace hrozeb
- vlastní analýzy rizik“ (2, s. 171)

3.2.1 Identifikace aktiv

Obecně lze říci, že aktiva jsou všechna data, programy a vše ostatní, co se ve firmě vyskytuje a na co potencionální útočníci mohou zaútočit.

Úkolem identifikace aktiv je zjistit, jaká aktiva se ve firmě vyskytují a jakou hodnotu pro nás mají. Při této identifikaci by se měla účastnit všechna dotčená oddělení. Nejprve se účastní oddělení IT, které vidí, jaká data se ukládají na disky a ví, na jaká aktiva potencionální útočníci mohou zaútočit. Po zhotovení seznamu aktiv je vhodné tento seznam probrat se všemi odděleními, kterých se aktiva týkají. Tyto oddělení pak vyčíslí hodnoty aktiv, kdyby došlo k jejich zničení. V úvahu pak bereme nejvyšší ohodnocení.

3.2.2 Identifikace hrozeb

Identifikaci hrozeb může provést IT oddělení a nebo si můžeme najmout profesionální firmu, která se těmito problémy zabývá. Při identifikaci bychom měli postupovat následovně:

- Intuitivně přemýšlet, jaká rizika nám hrozí, jaké situace mohou v systému nastat. Co když útočník provede to a to? Co když se vylije řeka z břehů a zatopí přízemí budovy, kde je umístěna serverová místnost? Musíme vymyslet, co nejvíce scénářů, které by mohly nastat.
- Většinou se nám však nepodaří obsáhnout všechna rizika, která nám hrozí, proto je dobré projít seznamy již vytvořených hrozeb. Tyto seznamy bývají vystaveny např. na internetu nebo můžeme využít služeb externí firmy, která má s vytvářením seznamů zkušenosti.

Když máme vytvořené kompletní seznamy hrozeb, můžeme přejít k vlastní analýze rizik.

3.2.3 Vlastní analýza rizik

Pro zahájení analýzy rizik potřebujeme hotové seznamy aktiv i s ohodnocením a seznamy hrozeb. Úkolem je nyní zjistit, jaké hrozby hrozí našim aktivům. Postupně tedy procházíme seznam aktiv a přiřazujeme možné hrozby. Jedno aktivum může postihnout více hrozeb a naopak. Ke každé takto vytvořené dvojici přiřadíme pravděpodobnost, s jakou se tento scénář může naplnit. Informační systém, aktiva i hrozby se v průběhu času mění, proto je vhodné analýzu provádět opakovaně s určitou periodou, podle rychlosti měnících se faktorů.

3.2.4 Navržení vhodné ochrany

Poté co jsme provedli analýzu rizik, nastal čas na závěrečnou fázi, a tou je navržení vhodné ochrany. K námi vytvořeným dvojicím musíme navrhnout ochranu, která bude daný problém řešit. Může se stát, že jeden ochranný prvek zajistí ochranu více dvojicím, proto je vhodné postupovat shora dolů, tzn. od těch širokospektrálních po specifické. Dále vyčíslíme náklady na daný ochranný prvek a zavedeme ty prvky, u kterých náklady jsou nižší než odhadovaná cena aktiv. Pokud je hodnota aktiv nižší než požadovaný ochranný prvek, bude se nám velmi těžko prosazovat u vedení firmy jeho zakoupení.

3.3 Zabezpečení dat proti ztrátě

Firma své data ukládá na disky, proto jedinou možností, jak je zabezpečit, je použití metody RAID.

U diskových polí se využívá metoda RAID (Redundant Array of Inexpensive Disks). V serverech se nepoužívají jednotlivé disky, ale disková pole. Jde o skupinu disků, která se navenek tváří jako jeden disk. Účelem diskových polí je zvýšit bezpečnost dat na nich uložených. Bezpečnost je zajištěna díky tomu, že dochází k redundanci dat, tzn. že se stejná data ukládají na více disků. Když pak dojde k poškození jednoho z nich, data se obnoví z redundantních dat. Vyšší bezpečnost je vykoupena snížením prostoru na discích. Firma využívá metodu RAID 5, jejíž princip popisuji v tabulce č. 1.

Typ	Princip	Výhody	Nevýhody
RAID 5 striping s redundancí	Data jsou rozdělována mezi více disků. „Nadbytečná“ paritní data jsou rozprostřena na všechny disky. Zhavarovaný disk je možné vyměnit. Jeho data jsou pak zrekonstruována pomocí paritních redundantních údajů.	Zvýšení výkonu při čtecích operacích. Redundantní data zaberou jen část kapacity disků (není třeba zdvojnásobovat kapacitu disků). Havarovaný disk je možné vyměnit a pole dopočítá a zrekonstruuje chybějící data.	Potřeba minimálně tří disků, čímž se diskové pole prodražuje.

Tabulka 1. RAID 5. (4, s. 51)

3.4 Útočníci a hrozby

Útočník je člověk se zlými úmysly. Útočníky můžeme dělit podle různých kritérií, například podle toho, odkud se do sítě nabourali (vnitřní, vnější útočník, celý svět) a nebo podle jeho odbornosti (amatér, hacker, profesionál). Nyní tyto typy popíšu:

- Vnitřní útočník – je to osoba, která vniká do sítě zevnitř, jde většinou o zaměstnance, který útočí buď z osobní iniciativy, např. se chce pomstít zaměstnavateli nebo se snaží získat data pro konkurenci a nebo může být někým přinucen. Výhodou je, že tito útočníci většinou nemívají hluboké znalosti ohledně informačních technologií, proto nenapáchají tolik škody. Mohou způsobit škodu i neúmyslně tím, že například smažou nějaký soubor. Tomuto můžeme zamezit řádným zaškolením svých zaměstnanců.
- Vnější útočník – je osoba, která nemá přímý přístup k síti. Při přístupu k síti musí zdolat všechny překážky, které síť chrání, jako např. firewall, šifrování, atd.
- „Celý svět – nejnebezpečnější druh útočníka. Za celým útokem stojí jeden člověk, který ovšem ke své nekalé činnosti zneužívá velké množství počítačů. Jedná se o takzvané Distributed DoS útoky. Jejich hlavní nebezpečí je v tom, že proti nim dosud neexistuje příliš účinná ochrana.“ (2, s. 155)

- Amatér – většinou není tento útočník nějak znalý v informačních technologiích, proto nebývá moc nebezpečný. Může to být například student střední školy. Většinou se inspiruje internetem, kde si najde například nějakou popsanou bezpečnostní díru a návod, jak ji využít. Omezuje se také na dostupnost volně šířeného softwaru, který umožňuje podobné útoky. Motivuje je většinou zvědavost. Proti těmto útočníkům se lze jednoduše chránit. Stačí zakoupit základní ochranný software a pravidelně ho aktualizovat.
- Hacker – tento útočník má už velmi dobré znalosti z informačních technologií, proto může způsobit nepříjemné útoky. Je však ale omezen prostředky nebo výpočetním výkonem. Může to být například studen vysoké školy zaměřené na informační technologie. Motivuje ho hlavně zvědavost, co všechno dokáže. Tato skupina je středně nebezpečná a většina firemních systémů je proti tomuto typu útočníka dobře chráněna.
- Profesionál – profesionál je člověk, který má vynikající znalosti z oblasti výpočetních technologií. Může to být člověk, který dlouhou dobu pracoval v praxi, ví, jak se systémy chrání, jak jsou stavěny, kde můžou být díry, atd. Navíc mají dobré prostředky i vybavení k tomu, aby mohli zaútočit a způsobit tak velkou škodu. Proti těmto útokům je velmi nákladné se chránit, proto většina, hlavně střední firmy, doufají, že se jim tento útočník vyhne.

„Hrozba označuje možnost využít zranitelné místo v informačním systému k útoku a tím způsobit škodu na aktivech.“ (4, s. 14) Máme různé typy hrozeb:

- „Objektivní – jako například přírodní, fyzické (požár, povodeň, výpadek napětí, poruchy, …), fyzikální (elektromagnetické vyzařování), technické nebo logické (porucha paměti, krádež nebo zničení paměťového média, softwarová „zadní vrátka“, špatně zapojené jinak bezpečné komponenty,…)
- Subjektivní, tj. hrozby plynoucí z lidského faktoru – neúmyslné (působení neškoleného uživatele/správce) a úmyslné (představované potenciální existencí vnějších útočníků (špioni, teroristé, konkurence, hackeři,…) i vnitřních útočníků (odhaduje se, že 80% útoků na IT je vedeno zevnitř, útočník pak bývá zaměstnanec, který je třeba chamtivý, rozzuřený, podplacený…).“ 21)

3.5 Zásady zabezpečení

Ve firmách se většinou tyto zásady objevují v nepsané formě, proto zde stručně popíšu, jak by se zásady měly správně vytvářet. Také se zmíním o tom, jak se poznají špatné a dobré zásady ohledně zabezpečení.

Jendou z prvních zásad zabezpečení je použití dobře nastaveného firewallu. Když si nejsme jisti, komu a jaká práva povolit, pak je nejjednodušší způsob vše zakázat a čekat, kdo se ozve, jaká práva potřebuje povolit. Tímto způsobem určitě nezapomenete na nic. Proto jediné a správné pravidlo činnosti firewallu musí být: „Všechno je zakázáno s výjímkou toho, co je výslovně povoleno nebo se nějak samo protlačí.“ (8, s. 103)

Jako ochrana proti využívání pracovní doby k soukromým věcem… existují předplacené služby s definovanou množinou zakázaných URL adres. Do nich je možné stáhnout celé báze serverů, na kterých je například sexuální nebo rasistický obsah. Dále by se měl kontrolovat poštovní klient, měl by být nastavený tak, aby například sám nespouštěl přílohy, odkazy na URL adresy, protože i v nevinném přání od kamaráda k narozeninám se může skrývat škodlivý software.

Například špatným pravidlem zabezpečení jsou tzv. nevynutitelné (neproveditelné) zásady.

3.5.1 Jak vytvořit zásady

Bezpečnostní politiky se dají tvořit různými způsoby. V oboru informační bezpečnosti je asi nejvhodnější postupovat podle rizik. To znamená, že nejprve identifikujeme rizika, zkonzultujeme je se zodpovědným nadřízeným, vytvoříme zásady a stanovíme metody, jakými budeme ověřovat jejich dodržování. V této kapitole se budeme věnovat rizikům, které na nás „číhají“ jen ve firemním prostředí, nebudeme se tudíž zabývat riziky živelných pohrom.

3.5.1.1 Vymezení rizik

Nejdůležitějším prvním krokem je projít si firmu a promluvit si se zaměstnanci. Zjistíme tak, jak se v organizaci využívají počítače a sítě, a to jak za normálního, tak i nouzového provozu. Vždy musíte lidem položit následující dvě otázky:

„S jakými důležitými daty z jiných zdrojů pracujete, tedy která data jsou natolik podstatná, že by jejich nedostupnost znamenala pro organizaci problémy?

Využíváte Internet ještě k něčemu jinému než k zasílání elektronické pošty? (Před položením této otázky si samozřejmě můžete „vyjet“ systémové protokoly a zjistit, jaká je pravda – pokud v organizaci neplatí presumpce soukromí.) Nezapomeňte, že dokud žádné zásady či pravidla neexistují, nemohou lidé dělat nic špatně (tedy něco proti pravidlům). Vysvětlete uživatelům, že se pouze snažíme zjistit současný stavěcí a že nikomu nebudete dělat problémy.“ (8, s. 104)

Odpovědi na tyto otázky nám ukážou rizika, kterým je firma vystavena. Musíme předpokládat také to, že většina zaměstnanců není tak poctivých, aby měla na svém počítači nainstalovaný a zapnutý firewall a ještě k tomu nejaktuálnější verzi antiviru s neustále aktualizovanou virovou databází. Během průzkumu můžeme přijít také na to, že zaměstnanci si například stahují hry z internetu a jiný neověřený software nebo si dokonce posílají soubory a komunikují přes nezabezpečené komunikační programy.

Všechny zjištěné rizika musíme sepsat a předložit nadřízeným (osobám, vedení společnosti) zodpovědným za bezpečnost sítě. Během přednesu takto zjištěných informací, bychom se měli držet obecného tónu, ale pokud možno udávat konkrétní příklady, kde by příslušné chování znamenalo pro organizaci finanční ztráty. Důležitou součástí jsou také možnosti, které by se měly s těmito riziky vypořádat. Musíme navrhnout ty nejlepší opatření, vedení firmy pak uzná za vhodné, co se pořídí a co ne. Naším úkolem je poskytnout jim všechny relevantní informace, na jejichž základě mohou provést toto rozhodnutí dobře.

3.5.2 Vytvoření zásad zabezpečení a stanovení podmínek

Pokud žádná písemná bezpečnostní pravidla neexistují, po řádné analýze je sepište a zajistěte jejich schválení a podepsání vedením společnosti. Jestliže nedokážeme vyhodnotit dodržování nějakých pravidel nebo zásad, pak tyto pravidla jsou nastavena špatně a jsou tzv. nevynutitelná. Pokud námi nastavená pravidla jsou konkrétní a jasně formulovaná, neměl by být s kontrolou dodržování problém. Kontroly by se měli provádět pravidelně (zhruba každé čtvrtletí) a také namátkově. Musíme také kontrolovat, zdali se tyto kontroly opravdu provádějí. Každá kontrola by měla být

zaznamenána a kontrolovat se musí i tyto kontrolní zápisy. Pokud by se kontroly neprováděly, problém by se nikdy nenašel.

Při psaní zásad se nesmí zapomenout na důležitou věc, a to na povahu organizace, ve které se zásady tvoří. Je vhodné položit několik otázek ohledně bezpečnostních postojů ve firmě, jsou to například tyto:

„Jaká platí presumpce soukromí a jak jsou sledovány telefonní hovory a síťový provoz? Mají zaměstnanci rozumné představy o tom, nakolik je jejich komunikace chráněná při ukládání souborů na počítači, při telefonním hovoru a při odesílání po Internetu?

Provádějí se nahodilé fyzické prohlídky, existuje pro ně nějaký aktivní program?

Jsou v konfiguraci obvodu sítě povolena veškerá odchozí spojení,, zahajovaná z vnitřní sítě organizace?

Smí si zaměstnanci doplňovat software nebo upravovat nastavení svého stolního počítače?

Smí administrátoři provádět změny bez formálního schválení úprav konfigurace?“ (8, s. 106)

Tyto odpovědi nám pomůžou v pochopení povahy organizace a pomůžou nám v sestavování bezpečnostních zásad. Během jejich sestavování musíme projít i různé směrnice vydané společností, aby naše zásady nebyly v rozporu s firemní kulturou.

3.5.3 Důležité součásti zásad

Při stanovování bezpečnostních zásad a pravidel musíme zvážit úrovně pravomocí. Tzn., že musíme vědět, pod které zásady bude dokument spadat, který nadřízený ho může odsouhlasit a přijmout. V organizacích bývají často zavedené různé směrnice, zásady a pravidla, proto musíme náš dokument správně zařadit. Pokud navrhované zásady netvoří nejvyšší úroveň, pro koho přesně platí? Úplně pro každého zaměstnance nebo jen v nějakém oddělení či skupině? Proto musíme nadefinovat také působnost zásad.

Působnost stanovuje pro koho a pro co naše zásady platí. Například dokument A platí pro celou organizace, dokument B platí pouze pro oddělení XX. Na působnost je

potřeba dávat dobrý pozor, aby se nestalo, že naše zásady nastavíme špatně, že například pro jedno oddělení budou platit jiné zásady než mají platit. S postupujícím časem se samozřejmě musí kontrolovat a potřebné zásady modifikovat či dokonce rušit.

Některé zásady a pravidla platí pouze po omezenou dobu. Obecná pravidla platí dlouhodobě, pokud jsou dobře nastavená. Zásady obvodového zabezpečení by se měly aktualizovat alespoň jednou ročně. Dobře nastavenými zásadami si usnadníme jejich pravidelnou kontrolu.

3.5.4 Dobré vs. špatné zásady zabezpečení

Obecně lze říci, že dobré zásady by neměly být zbytečně rozsáhlé, neměly by se často používat cizí slova, která nejsou známá, a nesrozumitelných výrazů a zkratek. Naopak musí vystihovat podstaty problémů, přesně je popisovat a uvést jejich řešení. Celkově by se dalo říct, že zásady musí být konkrétní, srozumitelné, stručné, jasné a realistické.

Vynutitelnost zásad dosáhneme tím, že zásady napíšeme srozumitelně, dobře čitelným jazykem a v optimální délce. Je důležité konkrétně vymezit především:

- „Co se má dělat. V dokumentu musí být popsány všechny potřebné informace, ze kterých sestavíme seznam kritérií pro ověření dodržování zásad.
- Proč zásady vůbec jsou definovány a jaký problém mají řešit. Racionálně myslící člověk potřebuje pochopit podstatu problému, aby vzal předložené řešení za své.
- Kdo je zodpovědný za naplňování úkolů vymezených v zásadách. To je důležité zejména v případě, že se podle zásad mají odvozovat konkrétní postupy. Musí být jasné, kdo je za jejich sestavení odpovědný.“ (8, s. 109)

Na konci by si měl zásady přečíst „obyčejný“ zaměstnanec a zhodnotit, zda-li jsou zásady popsány dost srozumitelně, jestli ne, může navrhnout, jak by danou věc popsal vlastními slovy.

Při tvorbě zásad můžeme využít techniku SMART, což znamená, že dotyčná věc by měla být konkrétní, měřitelná, dosažitelná, realistická a časově vymezená. Z této metody vyplývá, že metody musí být realistické, to znamená, aby naše zásady šly splnit,

aby se ve skutečnosti daly udělat. Pokud zásady nebudou realistické, nebudou pak ani vynutitelné. Takto napsané zásady jsou špatné.

3.6 VPN (Virtual Private Network)

V dnešním světě plném elektroniky a komunikačních technologií je zapotřebí přenášet informace z jednoho místa na druhé. Ať už je to v rámci města a nebo po celém světě. Informace, které přenášíme musí být chráněny, protože se jedná o soukromá data. Ale jak tuto bezpečnost přenosu zajistit? Dříve přenos dat probíhal po soukromých linkách, které pronajímali prodejci komunikací. Čím delší spojení bylo, tím dražší byl pronájem linky. Proto se sítě WAN staly přepychem pro většinu firem. Některé firmy si tento způsob transportu nemohly dovolit vůbec, jiné tento „soukromý“ přenos potřebovaly, a proto za něj platili velké částky.

O několik let později, kdy se širokopásmové připojení k Internetu stávalo stále dostupnější pro více firem, začala být síť WAN již nezajímavá. Stále zde ale byla otázka, jak zabezpečit přenos dat. Internet je veřejná síť, do které má přístup každý a tak se muselo najít řešení, jak ochránit soukromá data proti potencionálním útočníkům. Řešením tohoto problému jsou právě virtuální privátní sítě VPN (Virtual Private Network).

3.6.1 Základní fakta

„Síť VPN (někdy nazývaná „tunel“ VPN) je v podstatě připojení, které je pomocí šifrovacích nebo autentizačních technologií zavedeno nad existující veřejnou nebo sdílenou infrastrukturou tak, aby byl zabezpečen užitečný obsah připojení. Tím se vytvoří „virtuální“ segment mezi jakýmikoliv dvěma entitami, které k sobě mají přístup. VPN lze vytvářet přes sdílenou infrastrukturu místní sítě (LAN), přes WAN připojení nebo přes Internet.“ (8, s. 173)

V této kapitole popíši vytvoření VPN přes Internet z důvodu toho, že toto řešení je pro naši firmu nejschůdnější. Navíc tento způsob je levný a efektivní.

Sítě VPN můžeme rozdělit do 3 hlavních typů podle nastavení: hostitel-hostitel, hostitel-vstupní brána (gateway) a vstupní brána-vstupní brána (gateway-gateway). Technologie VPN je postavena na vytváření bezpečnostního komunikačního kanálu

pomocí šifrování. Šifrování může probíhat na různých vrstvách síťového modelu. Jsou to: aplikační, transportní, síťová a datalinková vrstva.

Na aplikační vrstvě může být šifrování zajištěno programově. Většina programů používaných na této vrstvě pracuje z hostitelského počítače na hostitelský počítač, proto nabízejí pouze ochranu obsahu paketů a ne samotného paketu. Zabezpečení přes transportní vrstvu se používá ve většině případů při komunikaci s webovým prohlížečem. I u této vrstvy jsou zabezpečeny pouze obsahy paketů a IP pakety, které tyto informace obsahují může kdokoliv získat. V síťové vrstvě už se nešifruje pouze obsah paketu, ale už i TCP/IP informace. Na datalinkové vrstvě se využívá šifrování paketů pomocí Point-to-Point Protokolu PPP.

„Tunelování je proces zapouzdření jednoho typu paketu do jiného, aby se tak umožnil nějaký výhodný transport.“ (8, s.175) Význam tunelu ukážeme na příkladu: máme 2 sítě propojené pomocí VPN, které je na obou stranách ukončeno firewallem. Firewall šifruje odcházející pakety tak, že k obsahu paketu přidá novou IP hlavičku se svojí adresou, jako adresou zdroje a IP adresou vzdáleného firewallu jako cílovou adresou. Toto zašifrování skryje skutečné IP adresy. Když zašifrovaný paket přijde k cílovému firewallu, ten jej dešifruje a propustí k hostitelskému počítači, ke kterému původně směřoval. „Virtuální segment, který se takto vytvořil mezi dvěma přenosovými bránami, se nazývá tunel.“ (8, s.176) Při tunelování není zajištěna úplná anonymita přenášených dat, i když jsou zašifrovány IP adresy hostitelských počítačů, stále jsou známy IP adresy bran a tak lze vysledovat, které sítě spolu komunikují.

3.6.2 Výhody a nevýhody tunelů VPN

Pokud firma zvažuje připojení k síti pomocí VPN, měla by zvážit několik faktorů, a to zejména tyto:

- „Jaká je úroveň důvěrnosti (utajení) zasílaných dat?
- Jak velký význam je kladen na utajení?
- Jak důležité je znát zdroj dat?“ (8, s. 177)

Pokud je úroveň zabezpečení již dostatečná, řešení pomocí sítě (tunelu) VPN může být zbytečné.

Spojení se vzdálenou sítí může probíhat 3 hlavními způsoby, a to buď přenosem dat po vyhrazené lince, což je sice dobře zabezpečeno a je zde zajištěn vysoký výkon, ale tento způsob je velmi drahý. Další možností je využít Internetového připojení, které má v dnešní době každá firma. Je zde ale problém s bezpečností, protože tento druh spojení využívají miliony lidí na světě a přenos dat je nešifrovaný. Proto nejlepší volbou je využití šifrované komunikace přes Internet pomocí VPN. K této službě mohou být přidány různé úrovně šifrování. Logicky, čím lepší zabezpečení, tím více finančních prostředků musíme vynaložit. Někdy musíme koupit výkonnější hardware a někdy dokoupit další potřebný software. Proto musí každá firma zvážit, jestli VPN opravdu potřebuje a jestli se jí vyplatí.

Hlavní výhodou používání sítě VPN při vzdáleném přístupu je, že přenášíme soukromá data přes „veřejný dopravní prostředek“ a tyto data jsou maximálně v bezpečí. Další výhodou je, že využívá již zavedených infrastruktur a proto ji lze realizovat velmi rychle. Toto řešení je velmi vhodné pro lidi, kteří se potřebují, například ze služební cesty v zahraničí, rychle připojit do firemní sítě, přitom posílat důvěrná data, která musí být zabezpečená a mít jistotu, že data nikdo neodposlechne. Díky všem vlastnostem, které VPN má, jako například různé úrovně bezpečnosti, okamžitá realizace a cenová výhodnost, je VPN excelentním komunikačním řešením.

I přes všechny výhody musí společnost zvážit nevýhody, které toto řešení skýtá. Při šifrování se používají komplikované matematické výpočty, které probíhají pro každý paket. Tyto výpočty zatěžují přenosové brány VPN, ale také šířku pásma. Čím složitější je šifrovací algoritmus, tím potřebuje větší kapacitu spojení a s tím je spojeno větší omezení rychlosti. Je důležité zvážit zatížení hardwaru a kapacity spojení ještě před zřízením VPN. Dalším problémem jsou také pakety, které se při zapouzdřování obalují dalšími daty a tím se zvětšuje jejich velikost, což může ovlivnit kapacitu spojení a v některých prostředích se může tento stav stát problémovým. Můžou nastat i problémy při realizace sítě, kterou budeme chtít vytvořit jako součást již existující infrastruktury.

3.7 Archivace a zálohování

Nejprve vysvětlím rozdíl mezi zálohování a archivací:

Pod pojmem zálohování rozumíme "Vytváření bezpečnostní kopie dat nebo celého operačního systému tak, abychom mohli v případě havárie některé součásti počítače, obnovit stav, který existoval těsně před vznikem poruchy". 17)

Archivace představuje především „shromažďování informací pro případné pozdější použití. Počítáme při tom i s nasazením technologií pro rychlé vyhledávání a třídění výsledků. Pro práci s archivem pak bude nejdůležitější jeho uspořádání, dlouhodobá spolehlivost a vysoká trvanlivost“. 17)

3.7.1 Zálohování

Zálohování slouží k řešení problému, kdy dojde ke zničení dat a my je potřebujeme obnovit. Ke zničení dat může dojít například kvůli smazání nebo poškození dat na svém nosiči nebo přímo ke zničení tohoto nosiče. Proto naše data co nejčastěji a pravidelně zálohujeme, tzn. že vybraná data ukládáme na jiné médium. I přes častou a pravidelnou zálohu nějaká data ztratit můžeme, jsou to ta od poslední zálohy do doby ztráty dat. Existují různé programy, které data zálohují automaticky, stačí nastavit jaká data, jak často, jakým typem zálohy je zálohovat a na jaká média.

Nejdříve si musíme rozmyslet několik důležitých věcí než začneme zálohovat, jsou to tyto:

- Co budeme zálohovat – ve firmě je mnoho dat, ale kapacity zálohovacích médií jsou omezená, proto musíme vybrat, která z nich budeme zálohovat. „Vždy se zálohujeme data jednotlivých aplikací (účetnictví, záznamy o prodeji, zákaznících atd.). Dále je důležité zálohovat soubory registrů a úložiště služby Active Direktory. Naopak je celkem zbytečné zálohovat programy, které můžeme nainstalovat z instalačních médií (např. adresář Program Fines).“ (4, s.131)
- Jak často budeme zálohovat – frekvence zálohování se určuje podle toho, jak často se data mění. Pokud se mění každý den, je dobré zálohovat každý den, pokud se mění týdně, zálohujeme jednou za týden apod.

- Na co budeme zálohovat – existují různé druhy zálohovacích médií. V dnešní době se nejvíce zálohuje na pásky a také na pevné disky. „Obecně je bezpečnější zálohovat na vyjímatelné médium, které pak ukládáme odděleně od počítačů. Je tak možné předejít ztrátě dat způsobené zničením počítačů (krádež, živelná pohroma). Při zálohování na pevné disky jiných PC chráníme data pouze před poruchami počítačů (ale i to je lepší nežli žádná záloha, nehledě na to, že nejvíce problémů vzniká právě poruchami PC).“ (4, s. 131)
- Jaký rozsah bude mít naše záloha – jestli budeme zálohovat pouze ze serveru a nebo i z jednotlivých stanic.

Důležité také je, jaké typy záloh budeme provádět, můžou to být tyto:

- Úplná (normální) – zálohují se všechny soubory a složky, proto je pak obnova dat velmi rychlá. Záporem je dlouhá doba potřebná pro zálohu a také zabírá nejvíce místa na zálohovacím médiu.
- Rozdílová – při zálohování se soubory označí jako zálohované, při rozdílové záloze se pak zálohují jen ty data, která se od úplné zálohy změnily. Označení však zůstává stejné. Proto se při každé rozdílové záloze zálohují data od poslední úplné zálohy, tudíž i ty, které jsme např. předchozí den již zálohovali. Doba u této zálohy je střední a pokud budeme chtít obnovit data z této zálohy, musíme nejdříve obnovit poslední úplnou zálohu a pak poslední rozdílovou.
- Přírůstková – zálohují se soubory od poslední úplné nebo od poslední přírůstkové zálohy. Po záloze se změní označení souboru jako zálohovaný, po změně souboru se označení změní, proto se při další přírůstkové záloze zálohují soubory jen změněné. Tato metoda je nejrychlejší, protože se zálohuje nejméně dat, ale obnova je delší, protože se musí zálohovat z poslední úplné zálohy, pak rozdílové a každá přírůstková. Nevýhodou je, pokud se nějaká přírůstková metoda zničí, nelze pak obnovit další přírůstkové a tím dojde ke ztrátě dat.

Aby bylo zálohování užitečné a účinné, musíme zálohovat pravidelně. Nejlepším způsobem je nastavení zálohování v zálohovacím programu.

3.7.1.1 Práce se záložními kopiemi

Aby se zajistila bezpečnost dat uložených na zálohovacích médiích, je dobré tato média umístit mimo server a úplně nejlépe mimo budovu sídla, například do bankovního sejfu. Zde je zabezpečeno jak příznivé prostředí pro zálohovací médium, tak je zde chráněno i před zloději a případným zničením. Pokud nechceme, aby byla data nějak pozměněna, je dobré zálohu šifrovat.

Důležitou součástí je také řádná evidence záložních kopií. Může se stát, že při záloze více serverů se nám média pomíchají a můžeme je nechtěně přehrát, či špatně zařadit a tím se nám nepodaří obnova námi ztracených dat. Důležité je také vědět, které záložní kopie již nepotřebujeme a můžeme je přemazat novějšími zálohami. Média se starými zálohami by se měla řádně smazat a uložit na místo, kde nemá přístup každý, aby nedošlo k nějaké kompromitaci.

3.7.1.2 Obnova dat

Úspěšná obnova dat je cílem veškerého zálohování. Nutnou součástí zálohování je také občasná kontrola námi zálohovaných dat, jestli jdou data ze záložních kopií obnovit. Může se totiž stát, že média jsou již stará a nefungují dobře, během zálohy se vyskytla nějaká chyba nebo jsme špatně nastavili zálohovací program. Mohli jsme zálohovat jiná data než jsme chtěli nebo jsme je uložili ve špatném formátu nebo dokonce jsou šifrovány klíčem, který už nemáme a nemůžeme je rozšifrovat. Dalším důležitým pravidlem je, řádně evidovat námi zálohované data, nejen kdy jsme je zálohovali, ale také jakým typem zálohy, abychom pak věděli, které záložní kopie použít na obnovu dat.

3.7.2 Archivace

Archivují se především data, která jsou dána ze zákona č. 499/2004 Sb. Jsou to zejména zakladatelské dokumenty, stanovy, organizační řády a schémata, dokumenty o změně právní formy, výroční zprávy, zprávy o auditu, finanční dokumenty, účetní záznamy, katalogy s ceníky, různé publikace vydané firmou, kolektivní smlouvy a další.

3.8 Zákony a normy

Na světě je několik, troufám si říct, i stovek různých norem a zákonů, podle kterých se společnost může řídit v oblasti bezpečnosti. Týkají se všech různých témat v oblasti informačních technologiích. Není zde prostor a ani není cílem práce, abych zde vypsala všechny normy, proto uvádím jen některé, podle kterých by se české společnosti mohly řídit.

- „Norma ISO/IEC 27001 je světově uznávaným standardem, podle kterého se porovnává a certifikuje bezpečnost systému informační bezpečnosti. Tato norma je základním stavebním kamenem, na kterém může organizace založit účinnost řízení veškerých svých informací, údajů a dat.“ 14)
- „Norma ISO 27001 poskytuje model pro zavedení efektivního systému řízení bezpečnosti informací (ISMS) v organizaci a doplňuje tak normu ISO 17799. Obě normy jsou úzce propojeny, každá z nich však plní jinou roli. Zatímco norma ISO 17799 poskytuje podrobný přehled (katalog) bezpečnostních opatření, které mohou být vybrány při budování ISMS, norma ISO 27001 specifikuje požadavky na to jak ISMS v organizaci správně zavést. Případná certifikace ISMS pak probíhá podle ISO 27001.“ 15)
- Ministerstvo financí vydalo metodickou příručku zabezpečování produktů a systémů budovaných na bázi informačních technologií. Byla vydána Úřadem v červenci 2000 pod názvem Bezpečnost informačních systémů.

Mohla bych vyjmenovat mnoho dalších norem, či příruček, ale myslím si, že pro ukázku tyhle 3 stačily. Vnitropodnikové politiky se týkají i další zákony a vyhlášky, jako například:

- Příloha č. 1 k zákonu č. 499/2004 Sb. Dokumenty vzniklé z činnosti podnikatelů zapsaných v obchodním rejstříku, které jsou podnikatelé za podmínek stanovených tímto zákonem povinni uchovávat a umožnit z nich výběr archiválií. Tento dokument přikládám v příloze č. 1.
- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

4 Návrh řešení

Z analýzy vyplývá, že se ve sledované společnosti vyskytují závažné nedostatky v oblasti bezpečnostní politiky. Tato část přináší návrh vytvoření nové bezpečnostní politiky, který by při implementaci nalezená řešení odstranil a systematicky zabránil vznikání dalších bezpečnostních rizik.

Navrhovaná nová bezpečnostní politika sestává z následujících opatření:

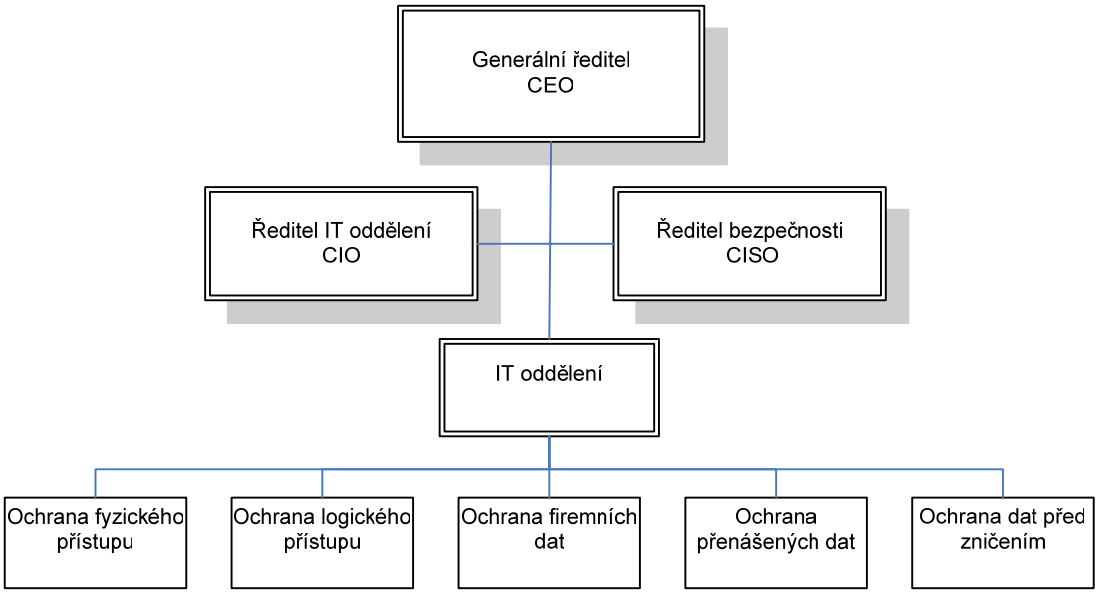
1. Navrhuji pozměnit organizační strukturu společnosti ve smyslu správy bezpečnosti, kde nově definuji odpovědnosti za jednotlivé oblasti bezpečnosti.
2. Navrhuji změnit zabezpečení fyzického přístupu vstupu do firmy, a to jak u zaměstnanců, především pak u návštěvníků společnosti. V tomto smyslu uvedu návrh nových směrnic.
3. Navrhuji nově definovat a zavést ochranu logického přístupu k datům, tzn. přístupy k informačnímu systému. Přístupy rozdělím do dvou kategorií a to na přístupy k síti zevnitř firmy a na vzdálené přístupy k síti odjinud než ze sídla společnosti. Opět doporučím vytvoření několika důležitých směrnic.
4. Navrhuji vytvořit klasifikaci dat podle jejich důležitosti z pohledu bezpečnosti. Součástí návrhu jsou směrnice pro práci s jednotlivými typy dat klasifikovanými z pohledu bezpečnosti.
5. Navrhuji realizovat zásadní změny v oblasti přenosu dat po vnitřní síti i přes Internet, a dále v oblasti využívání programů určených pro komunikaci s využitím Internetu. Součástí návrhu je opět vytvoření řídících směrnic.
6. Navrhuji přepracovat současně používaný způsob ochrany dat před zničením, a způsob práce s datovými zálohami. I tato oblast bude řízena nově vytvořenými směrnicemi.

V každé oblasti, kterou se zabývám, uvádím směrnice, které je nutné vytvořit. Tyto směrnice obsahují popis problému, ke kterému se vztahují, dále pak kdo danou směrnici má vytvořit, kdo ji má kontrolovat a jaké sankce hrozí za jejich porušení. Všechny směrnice, které uvádím, budou vytvářet zaměstnanci IT oddělení, kteří budou mít danou

oblast v popisu práce. Některé směrnice budou vytvořeny s pomocí personálního oddělení. Forma sankcí musí být stanovena ve směrnici o sankcích, kterou vytvoří personální oddělení. Sankce by měly být tvořeny tak, že za porušení směrnice se danému zaměstnanci nepřipíše měsíční pohyblivá složka mzdy. Mnou stanovené sankce jsou pouze orientační a firma si je dále upraví podle svého vlastního uvážení.

4.1 Organizační struktura správy bezpečnosti

Navrhuji následující organizační strukturu:



Obrázek 6. Návrh organizační struktury správy bezpečnosti.

Ve společnosti je zatím jen pozice ředitel IT oddělení (CIO), proto navrhuji vytvoření nových funkcí a to zejména funkci ředitele bezpečnosti (CISO), který se bude zodpovídat generálnímu (výkonnému) řediteli (CEO) za zajištění bezpečnosti ve společnosti. Tento ředitel bude kontrolovat zaměstnance, kteří budou mít v popisu práce zajištění bezpečnosti fyzického přístupu, logického přístupu, ochranu firemních dat, atd. (viz obrázek č. 5). Tito zaměstnanci se budou zodpovídat řediteli bezpečnosti za to, že správně navrhnou směrnice na daný problém v jejich popisu práce a budou zajišťovat jeho zabezpečení a dodržování daných směrnic.

Podotýkám, že navrhuji pouze funkce, proto nemusí každou funkci vykonávat vyčleněný zaměstnanec. Vzhledem k velikosti firmy a tabulkovému omezení počtu personálu v IT oddělení může jeden zaměstnanec například zajišťovat klasickou funkci

IT oddělení a k ní mít přiřazenou bezpečnostní funkci, která se vztahuje k náplni jeho práce (správce serverů bude také zajišťovat fyzický přístup k těmto serverům, atd.). Také mnou navržené funkce jsou jen doplněním stávajících funkcí IT oddělení, které však v popisu neuvádím.

4.2 Ochrana fyzického přístupu

Jedním z nejdůležitějších prvků ochrany dat je omezení fyzického přístupu do firmy a to zejména cizích lidí. V hlavním sídle je tento problém vyřešen dobře, ihned po vstupu do budovy je recepce, přes kterou prochází každý zaměstnanec i návštěva. Pokud recepční není přítomna z nějakého důvodu (například je na toaletě), dveře jsou zavřené a nikdo jiný než zaměstnanci, kteří mají klíče od budovy, se dovnitř nedostane. Ale i přes toto dobré řešení bych doporučila vstup do firmy monitorovat kamerou. U druhé budovy je fyzický přístup vyřešen jinak z důvodu jiného konstrukčního řešení budovy. Vstup je sice monitorován, výstup z kamery vidí recepční a podle toho pouští návštěvy, avšak recepce je umístěna až v prvním patře, tudíž návštěvy přes recepci projít vůbec nemusí (mohou volně odejít do jiných pater budovy, rovněž obsazených sledovanou společností) a v tuto chvíli není zajištěna bezpečnost fyzického přístupu. Navrhuji, aby v této budově byl každý návštěvník osobně po budově doprovázen, a to buď recepční, případně osobou, za kterou návštěvník přichází. V obou případech se tyto návštěvy musí zapsat do knihy návštěv. Dále navrhuji, aby místnosti s citlivými daty byly monitorovány a byly opatřeny čipovým vstupním zařízením. Tímto řešením by odpadly stálé problémy s docházkovým systémem „Dveřník“, který je často poruchový. Pohyb zaměstnanců by byl neustále monitorován a díky tomuto zařízení by se mohly vyřešit také práva přístupů do místností, do kterých má přístup jen omezená skupina lidí.

Dalším velkým problémem je umístění serverových místností v budovách firmy. V hlavním sídle je z pohledu bezpečnosti serverová místnost umístěna vhodně, problém je u druhého sídla, kde se serverová místnost nachází přímo v chodbě za vstupem do budovy. Chodba není monitorována a také díky tomu, že recepce je umístěna v prvním patře, k serverové místnosti má přístup každý. Tato místnost je sice opatřena čidly, ale na dveřích je pouze obyčejný zámek FAB. Navrhuji toto řešení tohoto problému – zvolit lépe zabezpečený zámek u dveří a především přemístit serverovou místnost do míst, kde se návštěvy běžně nepohybují. Pokud by se firma rozhodla využít již výše

navržený přístup pomocí čipových karet, vyřešil by se i tento problém. K této místnosti by měla přístup jen omezená skupina lidí, zejména IT oddělení a nikdo jiný. Díky tomuto zařízení by se bezpečnost serverových místností výrazně zvýšila.

Nyní doporučím vytvoření směrnic týkajících se této oblasti:

- **Směrnice o pohybu zaměstnanců a návštěv po budovách společnosti**

  Vytvoří: zaměstnanec IT oddělení, který bude zajišťovat bezpečnost fyzického přístupu do firmy, s pomocí personálního oddělení

  Popis: Bude zde popsáno, kam daní zaměstnanci mají přístup, povinnost zapisovat návštěvy do knihy návštěv, osobní doprovod atd.

  Kontrolor: osoba na manažerské pozici, pověřená správou dané firemní lokace (budovy)

  Sankce: V případě porušení dané směrnice navrhuji zaměstnanci sankci nepřipsání pohyblivé složky mzdy až do výše 2000,- Kč.

- **Směrnice o přístupu do firmy a docházce zaměstnanců**

  Vytvoří: zaměstnanec IT oddělení, který bude zajišťovat bezpečnost fyzického přístupu do firmy, s pomocí personálního oddělení

  Popis: Zde bude popsáno, jak používat docházkový systém „Dveřník“ a pokud by firma zvolila řešení přístupu pomocí čipových karet, bylo by zde popsáno, jak se čipové karty používají, u kterých oddělení je nutný přístup přes čipovou kartu a stanovení přístupových práv do oddělení s omezeným přístupem.

  Kontrolor: vedoucí personálního oddělení

  Sankce: Výše sankce za porušení této směrnice navrhuji až do výše 10000,- Kč, podle závažnosti pochybení a případné písemné napomenutí.

- **Směrnice o fyzickém zabezpečení serverových místností**

  Vytvoří: zaměstnanec IT oddělení, který bude zajišťovat bezpečnost fyzického přístupu do firmy

Popis: Tato směrnice bude obsahovat, jak serverová místnost musí být zabezpečena, jaké bezpečnostní prvky musí splňovat a kdo do této místnosti má přístup.

Kontrolor: ředitel IT

Sankce: Pokud vlivem nedostatečného zabezpečení místnosti do ní vnikne nepovolaná osoba, navrhuji sankci až do výše 20000,- Kč, při opakovaném porušení možnost rozvázání pracovního poměru.

4.3 Ochrana logického přístupu

Analýzou jsem zjistila, že přístup z vnitřní sítě je dobře zajištěn a existující směrnice tuto situaci vhodně upravují, proto se jí nebudu dále zabývat. Nedostatky jsem však nalezla především ve vzdáleném přístupu do celé podnikové sítě.

Vzdáleným přístupem rozumíme přístup k firemní síti odjinud než z firmy. Zaměstnanci se připojují k síti z domu, případně z cestovních lokací a to včetně zahraničí. K připojení z domu používají své vlastní stolní počítače. Zaměstnanci se připojují pomocí uživatelského hesla a jména. Tato komunikace není šifrována, proto doporučuji řešit vzdálený přístup přes síť VPN, kterou popisuji v kapitole 4.5. Ochrana přenášených dat.

Zejména domácí počítače, pomocí kterých se přistupuje k síti, nejsou kontrolovány, proto doporučuji navrhnout směrnici, která by zajišťovala správnou konfiguraci a zabezpečení přístupových zařízení:

- **Směrnice o konfiguraci zařízení, zejména stolních počítačů a notebooků, pomocí kterých se přistupuje do vnitřní sítě**

  Vytvoří: zaměstnanec IT oddělení, který bude zajišťovat bezpečnost logického přístupu do firmy

  Popis: V této směrnici musí být určeno, jak počítače musí být nakonfigurovány, jaké náležitosti musí splňovat, jaké programy se na tato zařízení mohou instalovat a která ne, a jakým způsobem a jak často se provádí kontrola.

Kontrolor: Nařízení dané směrnice bude kontrolovat příslušný zaměstnanec IT oddělení s pomocí aplikace, která kontroluje, zda-li počítač splňuje určitou úroveň zabezpečení (například ForeFront od společnosti Microsoft Windows) a podle toho zaměstnance spojí s vnitřní sítí nebo ne.

Sankce: Sankce stanovena nebude, pokud zaměstnanec chce plnit svoji práci a musí přistupovat k síti vzdáleně, musí splňovat daná kritéria, jinak se do sítě nepřipojí a nebude plnit svou práci.

Dále doporučuji inovovat operační systémy na serverech a všechny aplikace, jejichž verze je starší než verze z roku 2003, a to z důvodu kvalitnějšího zabezpečení novějších verzí těchto aplikací.

4.4 Ochrana firemních dat

Během analýzy jsem zjistila, že ve firmě neexistuje směrnice, která by data klasifikovala, a proto se může stát, že některá oddělení (či zaměstnanci) se chovají ke všem datům ve firmě stejně, což považuji za zcela špatné. Proto navrhuji vytvořit následující kategorie dat podle jejich citlivosti z hlediska bezpečnosti:

Úroveň 1: *data veřejná či volně zveřejnitelná*: taková data, která jsou buď přímo určena ke zveřejnění (např. tiskové zprávy, informace o nových či chystaných produktech, které se firma rozhodne v rámci marketingu uvolnit).

Úroveň 2: *data důvěrná*: vnitropodniková data, jejichž zveřejnění by s největší pravděpodobností nezpůsobilo společnosti žádnou zjistitelnou škodu, nicméně která současně nepatří k datům aktivně, záměrně zveřejňovaným.

Úroveň 3: *data tajná*: vnitropodniková data, jejichž zveřejnění či únik by s určitou pravděpodobností způsobilo či mohlo způsobit společnosti ekonomickou škodu či újmu na pověsti, nedošlo by však k porušení zákona či uzavřených obchodních smluv.

Úroveň 4: *data přísně tajná*: vnitropodniková data, jejichž zveřejnění či únik by s velkou pravděpodobností způsobil společnosti ekonomickou škodu značného rozsahu nebo citelnou újmu na pověsti, nebo taková data, jejichž zveřejnění či únik by způsobilo porušení zákona či uzavřených obchodních smluv.

V analýze jsem uvedla data, se kterými firma pracuje, nyní je ohodnotím podle výše navržených úrovní:

- (4) databáze zákazníků včetně korespondenčních údajů, zákaznické historie a jednotlivých plateb (jedná se o databázi sledující cca 120 000 unikátních zákazníků)
- (4) databázi velkoobchodních odběratelů a dodavatelů s korespondenčními údaji a jejich veškerou obchodní historií (řádově několik tisíc záznamů)
- (3) databázi spolupracovníků společnosti včetně externích autorů, překladatelů, korektorů atd. (řádově několik set záznamů)
- (4) databázi produktů společnosti a jejich obchodních výsledků včetně dlouhodobé historie (řádově několik tisíc produktů)
- (3) databázi autorských materiálů (článků) včetně návštěvnosti či čtenosti (týká se materiálů publikovaných na webu)
- (4) databázi vnitropodnikových údajů personálního a mzdového charakteru včetně historie a hodnocení zaměstnanců
- (3-4) databáze firemního účetnictví (faktury, platební deníky, finanční styk se státem atd.)
- (4) e-mailová databáze (vnitřní i vnější e-mailová komunikace) včetně příloh přikládaných k e-mailům
- (2) autorské materiály, se kterými firma pracuje, včetně licenčních, v různých fázích vývoje (od zdroje přes dočasné a pracovní materiály, meziprodukty až k materiálům určeným k sazbě)
- (3) různorodé materiály využívané zejména k ekonomickým a analytickým účelům (analýzy ve formě tabulek a písemných rozborů, přehledy trhu apod.), zápisy z porad, informace o konkurenci.
- (1) materiály volně šířené, publikované na webu (např. tiskové zprávy) či rozesílané obchodním partnerům

Pro rozdělení dat podle citlivosti musí být vypracována směrnice, která bude definovat, jak se s danými daty může zacházet a jaké sankce čekají zaměstnance, když směrnici poruší.

- ***Směrnice o klasifikaci firemních dat***

  Vytvoří: Tuto směrnici vypracuje provozní oddělení a bude ji také kontrolovat.

  Popis: tato směrnice klasifikuje data a určuje, jak se s nimi může či musí zacházet. Rozdělení uvádím v tabulce č. 4 níže.

  Kontrolor: vedoucí příslušných oddělení, kterých se data týkají

  Sankce: Navrhuji sankce od výtky až po desetitisíce korun. Přesnější určení viz tabulka č. 4 níže.

Úroveň	**Popis**	**Zabezpečení**	**Sankce za porušení**
1	*Data veřejná či volně zveřejnitelná*	žádné	žádná
2	*Data důvěrná*	Přístup všem zaměstnancům a vybraným externím spolupracovníkům, zabezpečení heslem.	symbolická sankce či domluva
3	*Data tajná*	Přístup pouze vybraným pracovníkům (mohou mezi nimi být i řadoví zaměstnanci). Zakázán jakýkoli vzdálený přístup. Zákaz jakéhokoli šíření mimo prostory firmy (digitální i tištěné kopie), tisk pouze pod dohledem nadřízeného.	sankce v rozsahu 2000 – 10000 Kč, při opakovaném porušování možnost ukončení pracovního poměru
4	*Data přísně tajná*	Přístup omezen na velmi malý počet osob, typicky vrcholovému managementu firmy. Přístup je	sankce až do výše desetitisíců korun, náhrada způsobené

		chráněn šifrováním (klíčem), jakýkoli přístup či pokus o přístup je zaznamenáván. Tištěné kopie jsou evidovány s povinností uložení do archivu (trezoru) společnosti po využití, případně skartovány.	škody a možnost ukončení pracovního poměru, případně i trestněprávní stíhání tam, kde je aplikovatelné

Tabulka 2. Návrh klasifikace firemních dat.

Další směrnicí, kterou bychom mohli zařadit do této oblasti, je směrnice o ukládání a uchovávání dat.

- **Směrnice o ukládání a uchovávání dat**

  Vytvoří: zaměstnanec IT oddělení, který bude zajišťovat bezpečnost firemních dat, může spolupracovat s ekonomickým oddělením

  Popis: Tato směrnice stanovuje, kam se ukládají „živá“ data po ukončení práce zaměstnance (měla by se ukládat vždy na server, aby na klientských stanicích nezůstávala žádná firemní data).

  Kontrolor: pověřený pracovník IT oddělení

  Sankce: Výši sankce navrhuji individuální podle rozsahu pochybení či podle výše způsobené škody.

S tímto uchováváním dat souvisí směrnice, která by měla upravovat zálohování. Tuto směrnici však uvádím až v kapitole 4.6. Ochrana dat před zničením.

Do této oblasti rovněž řadím problém týkající se možnosti odnesení dat z firmy na přenosném médiu. Na všech počítačích ve firmě jsou v současné době k dispozici CD/DVD vypalovací mechaniky a USB porty. Z tohoto důvodu doporučuji demontáž CD/DVD vypalovacích mechanik a zakázaní USB portů přes BIOS u oddělení, které tyto zařízení ke své práci vysloveně nepotřebují. Byly by to zejména následující oddělení – účetní oddělení, ekonomické oddělení, obchodní oddělení, personální oddělení, recepce a správa majetku a budov. Tento zákaz eliminuje možnost odnesení dat většinou z nedbalosti, a poněkud ztížit úmyslné odnesení dat. Úmyslnému vynesení dat z firmy nelze zabránit nijak. V případě, že zaměstnanec z uvedených oddělení

potřebuje určitá data odnést mimo firmu, jeho žádost posoudí a v případě schválení provede pracovník IT oddělení.

- **Směrnice o používání vypalovacích médií a portů k přenosu dat**

  Vytvoří: zaměstnanec IT oddělení, který bude zajišťovat bezpečnost firemních dat

  Popis: Zde bude popsáno, která oddělení mají zakázané používání těchto zařízení a proč a která jejich používání povolené mají. Směrnice dále definuje fyzické či technické odinstalování těchto zařízení u existujících zařízení (počítačů) a rovněž jejich odinstalaci u nově pořízených počítačů.

  Kontrolor: pověřený pracovník IT oddělení

  Sankce: Při porušení této směrnice navrhuji výši sankce až do 2000,- Kč.

4.5 Ochrana přenášených dat

Do této oblasti řadím návrhy na řešení problému s komunikačními programy, přes které ve firmě probíhá komunikace a které nejsou nijak zabezpečeny. Návrh obsahuje vytvoření sítě VPN, která bude obecně řešit problém s nešifrovaným vzdáleným přístupem k firemní síti.

Ve firmě se nyní používají, mimo jiného, komunikační programy ICQ a Skype. Tyto programy, které navíc často procházejí softwarovými aplikacemi, jsou známým bezpečnostním rizikem: nevyhovují vysokým bezpečnostním standardům, jsou v nich velmi často zjišťovány bezpečnostní díry, které nebývají výrobcem obratem odstraněny. Komunikace v nich je nešifrovaná. Tyto programy jsou šířeny zdarma a prakticky zde odpadá jakákoli zodpovědnost či záruky výrobce a neexistuje ani žádná systémová podpora. Z tohoto důvodu navrhuji naprostý zákaz jejich používání. Pokud společnost potřebuje využívat komunikační programy tohoto typu, doporučuji zakoupit ověřený, profesionální komunikační program určený pro firemní sféru, který bude garantovat vysokou úroveň zabezpečení, případně který bude umožňovat šifrovanou komunikaci probíhající přes tento program.

Největší bezpečnostní slabinu ve firmě vidím ve vzdáleném přístupu k podnikové síti. Mezi pobočkami je komunikace šifrována, ale pokud se chce zaměstnanec připojit

k firemním datům například z ciziny přes veřejnou wi-fi síť, nastává bezpečnostní problém. Tato komunikace šifrována není a při zadávání přihlašovacího jména a hesla může být komunikace odposlechnuta a zjištěná data zneužita. Řešení tohoto problému jsou v zásadě dvě. Prvním je povolení přístupu pouze na danou IP adresu, tzn. že by byl vytvořen přesný seznam IP adres, kterým by se přístup povolil. Toto řešení by se dalo realizovat s pomocí zakoupení přenosných modemů, které nabízejí komerční společnosti jako například Telefonica O2 nebo T-Mobile. U těchto zařízení lze dokoupit „službu“, která zajišťuje uživateli stálou IP adresu při každém připojení. Druhou možností řešení problému s přístupem přes veřejnou internetovou síť je využití VPN tunelů. U první možnosti může nastat problém, že v zahraničí tento modem nemusí mít pokrytí, zaměstnanec jej náhodou zapomene doma a pak vzniká opět problém nezabezpečeného připojení k síti, zatímco druhé řešení je pro firmu i zaměstnance výhodnější. Zaměstnanec nemusí myslet na to, zda-li nezapomněl modem, zda-li je v zemi, do které jede, pokrytí a další problémy s tímto řešením spojené. Zaměstnanec odjede ze země a když se bude chtít připojit k firemní síti, jednoduše se připojí, nemusí se o nic starat. Mezi klientem a serverem se vytvoří takzvaný tunel, ve kterém je komunikace šifrována a nikdo tuto komunikaci nemůže odposlechnout. Proto navrhuji řešit tento problém pomocí sítě VPN.

Z důvodu toho, že uživatelé používají výhradně operační systém od společnosti Microsoft Windows a také z toho důvodu, že VPN bude sloužit převážně pro vzdálený přístup zaměstnanců k vnitřní síti, volila bych řešení hostitel-brána u protokolu IPSec a nebo protokol PPTP, který je součástí operačního systému Microsoft Windows.

V této oblasti bych doporučila zavedení následujících směrnic:

- **Směrnice upřesňující firemní komunikaci**

  Vytvoří: zaměstnanec IT oddělení, který bude zajišťovat bezpečnost přenášených dat

  Popis: Tato směrnice popisuje, jak ve firmě probíhá komunikace, jaké dokumenty se mohou posílat jakým typem komunikačního programu. Upřesňuje pravidla používaného poštovního klienta, komunikačního programu, tak i komunikace po telefonu. Definuje prvotní kontrolu a odinstalování nepovolených programů administrátorem.

Kontrolor: pověřený pracovník IT oddělení

Sankce: mohou být uděleny pouze u osob, které mají na svých počítačích povolena práva administrátora (jejich práce vyžaduje časté instalace programů na počítače). Navrhuji výši sankce od 5000 do 10 000 Kč.

- **Směrnice pro používání sítě VPN**

  Vytvoří: zaměstnanec IT oddělení, který bude zajišťovat bezpečnost přenášených dat

  Popis: definuje, co to je, k čemu se využívá a jak v ní komunikace probíhá, co je zapotřebí, aby daný zaměstnanec tuto síť mohl využít atd.

  Kontrolor: zaměstnanec IT oddělení, který bude zajišťovat bezpečnost přenášených dat

  Sankce: jelikož se jedná o technická pravidla provozu a využívání, je bez sankcí

Společnost provozuje řadu webových stránek (webových serverů, webů), všechny jsou založeny na protokolu http. U některých, zejména například u elektronického obchodu a u všech dalších, kde se uživatel registruje a zadává své kontaktní údaje, doporučuji stránky zabezpečit pomocí protokolu SSL, takto zabezpečené stránky se označují jako https.

4.6 Ochrana dat před zničením

V této oblasti se zabývám problematikou umístění serverových místností a také zálohováním dat a prací s těmito zálohami. Otázka archivace dat je pominuta, neboť analýzou jsem zjistila, že je ve společnosti řešena dobře a jsou vypracovány i dodržovány směrnice pro oblast archivace.

Během analýzy jsem zjistila, že serverová místnost v hlavním sídle je umístěna velmi rizikově v suterénu budovy. Budova se totiž nachází v blízkosti (zhruba 15-20 m) řeky. I když je možnost vylití řeky z břehů velmi málo pravděpodobná, určité riziko tu stále existuje (průsak spodní vody atd.). Z tohoto důvodu doporučuji umístění serverové místnosti do vyššího patra budovy, kde by před tímto rizikem byla chráněna.

Dále jsem zjistila, že firma uchovává všechny záložní kopie dat v budovách společnosti. Tento postup je velmi rizikový: pokud by například došlo k nějaké živelné pohromě, například k požáru, tak společnost přijde o všechna data, jak o zálohovaná, tak i o ta uložená na serverech a klientských stanicích, a téměř by nebylo možné provoz společnosti rychle obnovit. Proto doporučuji, aby se jednou za měsíc záložní kopie odvážely do bankovního sejfu, kde jsou v případě živelné katastrofy postihující firmu či při napadení firmy útočníkem v bezpečí.

Z těchto důvodů je vhodné vytvořit tyto bezpečnostní směrnice:

- **Směrnice o uchovávání a kontrole záložních kopií**

  Vytvoří: zaměstnanec IT oddělení, který bude zajišťovat bezpečnost dat před zničením

  Popis: tato směrnice bude popisovat, jak se má správně se záložními kopiemi zacházet, kde mají být umístěny, v jakých podmínkách, atd. V této směrnici musí být také uvedeno, kdo by měl pravidelně záložní kopie kontrolovat, zda-li jsou obnovitelné.

  Kontrolor: pověřený zaměstnanec IT oddělení

  Sankce: V případě porušení této směrnice navrhuji, aby byla uložena sankce do výše několika desetitisíců korun, podle možnosti vzniku škody.

Pokud dojde k nějaké havárii, je nutné co nejrychleji jednat, proto by se měly vypracovat krizové plány, které by měly být uschovány na takovém místě, kde by nedošlo k jejich zničení, ale zároveň aby byly ihned „po ruce“. Na uložení krizových plánů a jejich obsahu navrhuji vypracovat směrnici (viz dále).

- **Směrnice: Krizové plány pro případ živelné pohromy**

  Vytvoří: hlavní jádro krizového plánu je provozní (bezpečnost osob, majetkua td.), který vytvoří provozní oddělení firmy. Za vytvoření části týkající se IT infrastruktury a dat odpovídá zaměstnanec IT oddělení, který bude zajišťovat bezpečnost dat před zničením

  Popis: Tato směrnice by měla obsahovat následující náležitosti: sestavení krizového týmu; prováděcí plány pro záchranu a obnovu informačního systému

jako například návod jak odstranit akutní nebezpečí, postup jak obnovit důležité části systému, postup jak obnovit ztracená data; zavedení protiopatření a jak zanalyzovat proběhlou krizi a vyvodit z ní případné pozměnění postupu při řešení krize. Tato směrnice se týká živelných pohrom.

Kontrolor: ředitel IT (u části týkající se informačních technologií)

Sankce: bez sankcí (jedná se jen o vytvoření předpisu).

5 Zhodnocení a závěr

V mé práci jsem se zabývala existující společností XY a.s., která nechtěla být z důvodu citlivosti dat uváděna pod skutečným jménem. Jedná se o českou společnost střední velikosti s cca 250 zaměstnanci, která se zabývá výrobní a obchodní činností silně postavenou na informačních technologií.

Analyzovala jsem její současný stav v oblasti bezpečnostních politik, kde jsem se zaměřila na analýzu jak používaného hardwaru a softwaru, tak na stav bezpečnostních opatření a k tomu používaných směrnic. V této analýze jsem zjistila řadu nedostatků různé úrovně závažnosti, a usoudila jsem, že společnost je z tohoto důvodu vystavena vážným bezpečnostním hrozbám.

V části věnované teoretickým východiskům jsem uvedla stručný výtah ze zaužívané, akceptované teorie v této oblasti. Vzhledem k velkému rozsahu teorie a její současné značné neustálenosti a dynamice se dále odkazuji na některé zásadní teoretické práce v tomto oboru.

Pro zjištěné a analyzované bezpečnostní problémy společnosti jsem navrhla řešení návrhem nových bezpečnostních politik. Oblast jsem v souladu s teorií rozdělila na pět hlavních okruhů problémů (ochrana fyzického a logického přístupu, ochrana firemních dat, ochrana přenášených dat a ochrana dat před zničením), pro které jsem navrhla a zdůvodnila řešení změn, současně pak též vytvoření směrnic či soustav směrnic vedoucích k implementaci nové bezpečnostní politiky a její dodržování.

Jakkoli si jsem vědoma, že sledovaná společnost může mít různé podnikatelské priority, jejichž vinou byla bezpečnostní politika nemálo zanedbávána, domnívám se, že aplikace navržené bezpečnostní politiky by pro společnost nebyla příliš náročná a současně by přitom pronikavě zvýšila bezpečnost společnosti a ochránila ji před významným podnikatelským rizikem.

6 Literatura

6.1 Knižní publikace

1) BOTT, Ed a SIECHERT, Carl. *Microsoft® Windows® Security Inside Out for Windows XP and Windows 2000*. Microsoft Press, 2002.
2) DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat.* Brno: Computer Press a.s., 2004.
3) DOSEDĚL, Tomáš. *21 základních pravidel počítačové bezpečnosti.* Brno: Computer Press a.s., 2005.
4) HANÁČEK, Petr, STAUDEK, Jan. *Bezpečnost informačních systémů : metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. Praha: Úřad pro státní informační systém, 2000.
5) HORÁK, Jaroslav. *Počítačové sítě pro začínající správce. 3. aktualizované vydání*. Brno: Computer Press a.s., 2006.
6) KRETCHMAR, James, M. *Administrace a diagnostika sítí*. Brno: Computer Press a.s., 2005.
7) LOCKHART, Andrew. *Bezpečnost na maximum*. Brno: Computer Press a.s., 2005.
8) Network Security. Osborne/McGraw-Hill, 2002.
9) NORTHCUTT, Stehen, et al. *Bezpečnost počítačových sítí - Kompletní průvodce návrhem, implementací a údržbou zabezpečené sítě*. Brno: Computer Press a.s., 2005.
10) SOPER, Mark, Edward. *Malé počítačové sítě*. Brno: Grada, 2005.
11) WALTHER, Henrik. *Jak zabezpečit Exchange Server 2003 a Outlook Web Access*. Brno: Computer Press a.s., 2005.
12) WENDELL, Odom. *Počítačové sítě*. Brno: Computer Press a.s., 2005.
13) ZEMÁNEK, Jakub. *Stavba a správa sítě aneb cesta do hlubin internetu*. Brno: Computer Media, 2004.

6.2 Internetové zdroje

14) *Bezpečnost informačních systémů dle BS7799* [online]. 1998 [cit. 2007-05-08]. Dostupný z WWW: <www.versasys.cz/produkty_bis.htm>.

15) *ISMS: normy ISO 17799 a ISO 27001* [online]. 2005 [cit. 2007-05-08]. Dostupný z WWW: <http://www.rac.cz/rac/homepage.nsf/CZ/BS7799>.

16) *Počítačové sítě - Topologie sítí - Hvězdicová topologie (strom)* [online]. [cit. 2007-05-08]. Dostupný z WWW: <http://site.the.cz/index.php?id=17>.

17) *Ukládání dat* [online]. 1995 [cit. 2007-05-09]. Dostupný z WWW: <http://www.k-net.cz/cs2/navigator/6ukladani>.

6.3 Zákony

18) Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů ze dne 30. června 2004.

19) Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů ze dne 4. dubna 2000.

7 Seznam obrázků a tabulek

Obrázek 1. Organizační struktura firmy. 15
Obrázek 2. Hvězdicová topologie. 16) 16
Obrázek 4. Bezpečnostní politika firmy. (2, s.169) 27
Obrázek 5. Dělení bezpečnostních incidentů. (2, s. 22) 27
Obrázek 6. Návrh organizační struktury správy bezpečnosti. 44

Tabulka 1. RAID 5. (4, s. 51) 30
Tabulka 2. Návrh klasifikace firemních dat..... 51

8 Přílohy

8.1 Příloha č. 1 - Příloha č. 2 k zákonu č. 499/2004 Sb.

„Dokumenty vzniklé z činnosti podnikatelů zapsaných v obchodním rejstříku, které jsou podnikatelé za podmínek stanovených tímto zákonem povinni uchovávat a umožnit z nich výběr archiválií.“

1. Statut, dokumenty o vzniku a zániku podnikatelského subjektu

a) zakladatelské dokumenty,

b) organizační řády a řídící akty, stanovy, statuty a jejich změny, jednací řády, organizační řády a schémata,

c) dokumenty o změnách podnikatelských subjektů, rozhodnutí, dekrety, smlouvy a výměry o změně právní formy, sloučení, rozdělení,

d) dokumenty o zrušení, likvidaci a zániku podnikatelského subjektu, rozhodnutí o likvidaci, zprávy o postupu a ukončení likvidace, návrhy na výmaz z obchodního rejstříku.

2. Dokumenty vrcholového řízení podnikatelského subjektu, notářské zápisy z jednání orgánů podnikatelského subjektu, výroční zprávy včetně zprávy o auditu.

3. Dokumenty o majetku podnikatelského subjektu, dokumenty dokládající vlastnictví nemovitého majetku, ochranné známky.

4. Finanční dokumenty, účetní záznamy a statistiky podnikatelského subjektu, zejména knihy podvojného účetnictví, účetní závěrky a roční statistické výkazy.

5. Dokumenty z propagační činnosti podnikatelského subjektu, zejména katalogy zboží s ceníky, publikace vydané podnikatelským subjektem a podnikové kroniky.

6. Výrobní program, jeho změny a uplatnění výrobků na domácím trhu a zahraničních trzích.

7. Zásadní dokumenty o zaměstnaneckých záležitostech, kolektivní smlouvy.