VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

NÁVRH BEZPEČNOSTNÍ POLITIKY ICT VE FIRMĚ

DRAFT OF ICT SECURITY POLICY IN COMPANY

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — JIŘÍ ŠPAK
AUTHOR

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

BRNO 2012

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2011/2012
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Špak Jiří

Manažerská informatika (6209R021)

Ředitel ústavu Vám 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 zadává bakalářskou práci s názvem:

Návrh bezpečnostní politiky ICT ve firmě

v anglickém jazyce:

Draft of ICT Security Policy in Company

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Analýza současného stavu
Teoretická východiska řešení
Návrh řešení
Zhodnocení a závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. Computer Press, 2004. ISBN 80-251-0106-1.
HANÁČEK, P., STAUDEK, J. Bezpečnost informačních systémů. 1. vyd. Praha: Úřad pro státní informační systém, 2000. ISBN 80-238-5400-3.
HORÁK, J. Bezpečnost malých počítačových sítí. Praha: Grada Publishing, 2003. ISBN 80-247-0663-6.
NORTHCUTT, S. Bezpečnost počítačových sítí. 2005. ISBN 80-251-0697-7.
PROSISE, CH., MANDIA, K. Počítačový útok - detekce, obrana a okamžitá náprava. Computer Press, 2002. ISBN 80-7226-682-9.

Vedoucí bakalářské práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2011/2012.

L.S.

Ing. Jiří Kříž, Ph.D. Ředitel ústavu	doc. RNDr. Anna Putnová, Ph.D., MBA Děkan fakulty

V Brně, dne 30.05.2012

Abstrakt

Tato bakalářská práce se zabývá problematikou bezpečnosti ICT v reálném prostředí mezinárodní firmy působící v Brně. Součástí práce je analýza současného stavu, teoretická východiska a návrhy ke zlepšení současné bezpečnostní situace firmy, které v případě implementace zajistí požadovaný stupeň bezpečnosti.

Abstract

The presented bachelor's thesis analyses problems of ICT security in the factual environment of international company operating in Brno. It is divided in to three parts. First part contains analysis of current conditions. Second part explains theoretical background. Third part includes propositions how to improve company's security situation.

Klíčová slova

bezpečnost, bezpečnostní politika, bezpečnost dat, řízení bezpečnosti, bezpečnostní směrnice, zálohování dat

Keywords

seucrity, security policy, data security, safety control, security guidelines, data backup

Bibliografická citace

ŠPAK, J. *Návrh bezpečnostní politiky ICT ve firmě*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2012. 50 s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph.D.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne …….

Podpis

Poděkování

Na tomto místě bych rád poděkoval vedoucímu bakalářské práce, panu Ing. Viktoru Ondrákovi, Ph.D. za cenné připomínky a rady poskytnuté při zpracování této bakalářské práce.

OBSAH

Úvod

V dnešní době jsou informace tím nejcennějším aktivem. Téměř každá organizace od těch nejmenších v privátním sektoru až po ty největší ve státní správě zpracovává každý den neustále narůstající množství dat. Tyto data jsou velice soukromého charakteru a v dnešní době, kdy je celá řada systémů připojena ke globální síti Internet, je jejich bezpečnost téma, které určitě není radno brát na lehkou váhu.

Firmy považují informace za svá aktiva a tyto aktiva musí být chráněna proti zneužití neoprávněnou osobou, ať už zvenčí či z vnějšku. Tato ochrana je ve firmách realizována prostřednictvím bezpečnostních politik. Ty jasně popisují, co je předmětem ochrany, jaké jsou nezbytné kroky k zachování této ochrany a také definují zodpovědnosti.

Tyto bezpečnostní politiky představují základ pro zajištění informační bezpečnosti. Pokud jsou dobře zpracovány, riziko neoprávněného přístupu k citlivým informacím je velmi malé a firma si může být jista, že případný útok na data bude rychle odhalen a že způsobené škody budou minimální.

Cíl práce

Cílem této práce je vytvoření návrhu bezpečnostní politiky. Tato politika bude vycházet z analýzy současného stavu a měla by vést ke zlepšení zabezpečení jednotlivých firemních systémů, k vyšší bezpečnosti dat a v neposlední řadě také k stanovení práv a povinností jednotlivých zaměstnanců při práci s IT vybavením.

1 Analýza současného stavu

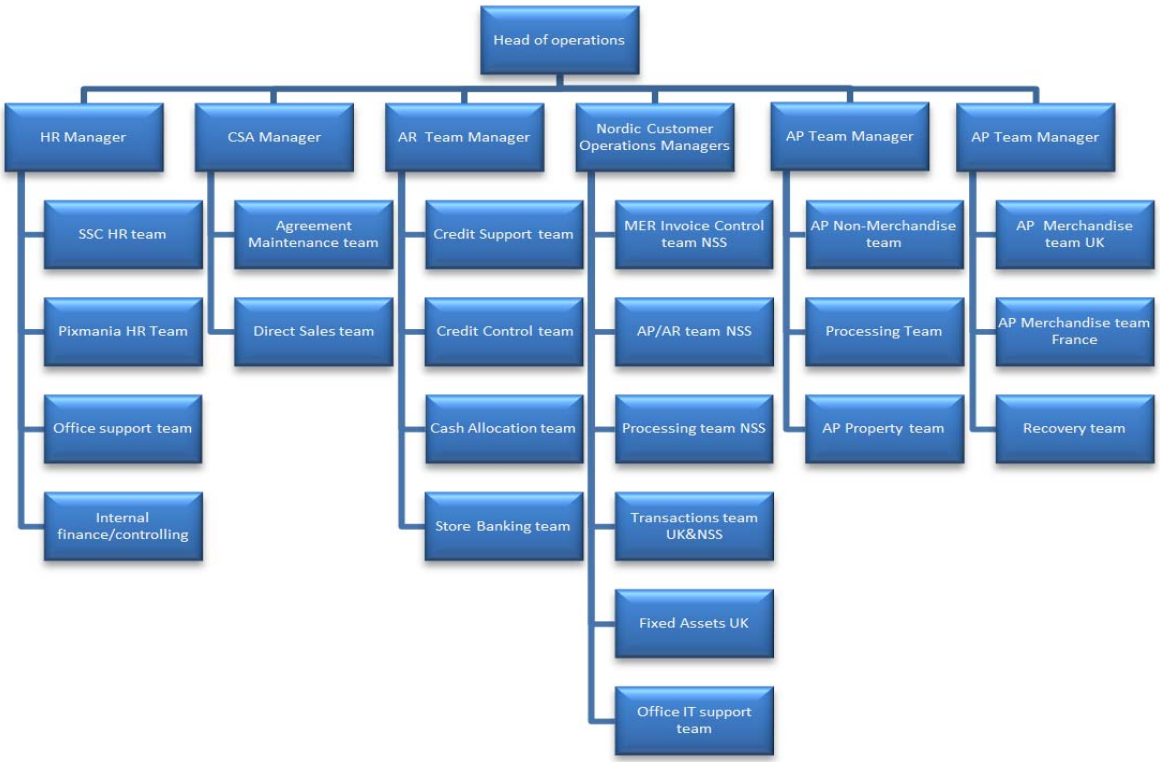
1.1 Informace o firmě

Z důvodů citlivosti údajů bude v bakalářské práci firmu nazývána ABC s.r.o. Tato společnost byla založena v roce 2007 a je součástí mezinárodní skupiny se sídlem ve Velké Británii. Tato skupina se orientuje na maloobchod a služby v oblasti spotřební elektroniky.

V Brně je centrum sdílených služeb, jehož nynější tým tvoří více než 300 pracovníků na pozicích v oblasti služeb zákazníkům, finančního řízení a v oblasti informačních technologií. Před nedávnem proběhlo stěhování do nových prostor, současné prostory již nestačily díky neustále se zvyšujícímu počtu zaměstnanců.

1.2 Organizační struktura firmy

Firma má liniovou organizační strukturu, což znamená, že pozice a vztahy nadřízenosti a podřízenosti jsou uspořádány a orientovány vertikálně. V důsledku má tedy každý nadřízený jasně přidělené podřízené a na druhou stranu každý podřízený má jasně přiděleného nadřízeného (14).



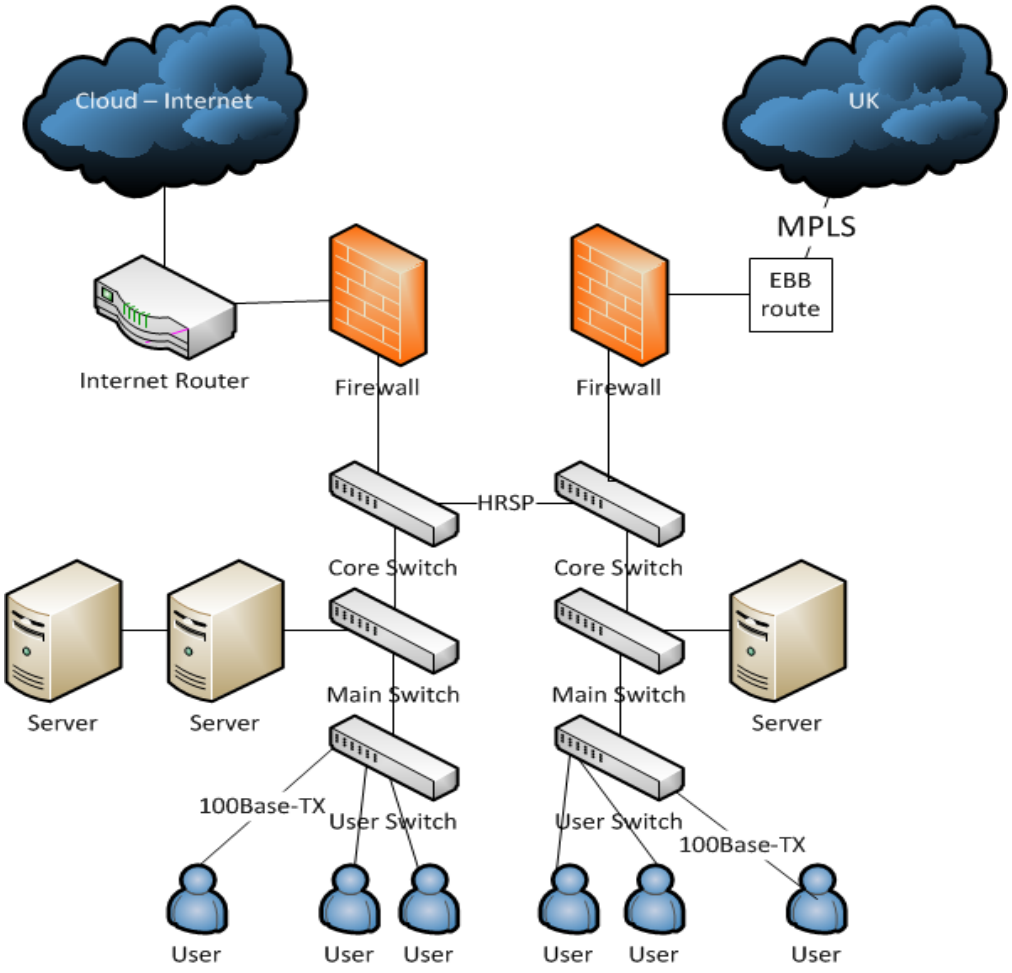
Obrázek 1: Organizační struktura firmy
Zdroj: (vlastní zpracování)

1.3 Počítačová síť

Celá firemní síť je řešena pomocí místní LAN. Do této sítě jsou zapojeny firemní servery a pracovní stanice, IP telefony stejně jako síťové tiskárny. Z bezpečnostních a kapacitních důvodů není ve firmě zavedena síť WLAN. Tato skutečnost se má ovšem v nejbližší budoucnosti změnit, jelikož je v plánu vybudování bezdrátové sítě pro tuzemské i zahraniční návštěvníky.

1.3.1 Struktura PC sítě

Jelikož je firma pobočkou mezinárodní společnosti, potřebuje s centrálou dobrou internetovou konektivitu. Ta je zajištěna jednou vyhrazenou linkou do Velké Británie a druhou záložní pro připojení k internetu. Na obrázku níže je tato struktura vidět.



Obrázek 2: Struktura počítačové sítě

Zdroj: (vlastní zpracování)

1.3.2 Místní síť LAN

Komunikační uzly jsou v rámci sítě LAN spolu propojeny hvězdicovou topologií. Na rozdíl od například kruhové topologie má toto zapojení výhodu, že při náhlém výpadku jedné stanice nebo kabelu mohou ostatní prvky fungovat bez jakéhokoliv omezení. Lokální síť je typu Ethernet, ve verzi Fast Ethernet, tady 100Base-TX s rychlostí 100 Mb/s. Veškeré kabely jsou vedeny pod dvojitou podlahou, která je v budově zařízená od firmy Lindner. Stejnou cestou je vedena i elektrická kabeláž. Vzhledem k dostatku místa jsou kabely vedeny správně a jsou dodržovány poloměry ohybu v rozích. Kabeláž je nestíněná kroucená dvojlinka UTP Cat5e s PVC pláštěm. Datové i silové zásuvky jsou umístěny v podlahových krabicích, kdy jedna tato krabice pokrývá oblast 10 m^2 a umožňuje flexibilitu při přemisťování stanic a zařízení.

1.3.3 Virtuální privátní síť VPN

Jelikož je většina uživatelských aplikací přenášena z data centra v Hemelu a manažeři mají k dispozici notebooky, je potřeba zajistit vzdálený přístup a to prostřednictvím VPN. Z důvodů bezpečnosti se používá dvoufázová autentizace, kromě uživatelského jména a hesla jsou manažeři vybaveni USB tokenem, bez kterého se do sítě není možné přihlásit.

1.3.4 Firewall

Firewall je zajištěn hardwarově a to dvojicí zařízení Nokia Voayger, typ IP390. Tato zdvojená ochrana byla zvolena z důvodu vysoké bezpečnosti a spolehlivosti. Na firewallech jsou správně nastavena natovací a routovací pravidla a kromě výjimek je většina portů zakázána.

1.3.5 VLAN

Vzhledem k bezpečnosti jsou servery, tiskárny, uživatelská PC a celý telefonní systém rozděleny do virtuálních Lan sítí.

1.4 Hardware

Firma spoléhá na ověřené dodavatele hardwaru, jako jsou společnosti DELL, HP, Alcatel a Cisco. Upřednostňuje tedy spíše kvalitu, za kterou je ochotna si připlatit. Stále běžícím procesem je výměna staršího hardwaru za nový. Tato výměna se neděje nárazově, ale probíhá postupně.

1.4.1 Klientské stanice

Ve společnosti jsou použity značkové počítače od výrobce HP. Jedná se o modelovou řadu Compaq. Tyto PC jsou vybaveny procesorem od firmy Intel a pro současný operační systém dostatečnou kapacitou paměti RAM. Všechny stanice dále obsahují optickou mechaniku, přední USB porty a síťovou kartu 10/100Mb Ethernet. Některé stanice jsou vybaveny dvojicí širokoúhlých monitorů, které uživatelům usnadňují práci. Stanice jsou velice tiché, protože jsou zde použity externí zdroje napájení. Dále jsou k některým stanicím připojeny IP telefony, které ovšem fungují samostatně.

1.4.2 Mobilní zařízení a notebooky

Všechny notebooky jsou od společnosti HP, třídy business. S tím je spojena jejich zvýšená odolnost a požadavek na delší práci na baterie. Každý notebook má prodlouženou next business day onsite záruku, což v podstatě znamená, že v případě jakékoliv poruchy přijede technik přímo do firmy a to buď ve stejný den, nebo následující den pracovní. Softwarová výbava podobně jako u stolních PC zahrnuje Windows XP ve verzi SP3 a kancelářský balík Microsoft Office. Při koupi nové řady notebooků se vždy jeden stroj pošle do centrály v Hemelu, kde je nainstalován a nakonfigurován veškerý software a bezpečností politiky a tento stroj je potom spolu s instalačním DVD zaslán zpět. Tato procedura trvá určitý čas a kromě notebooků se týká i stolních PC.

1.4.3 Servery

Servery najdeme ve třech oddělených serverovnách v prvním, třetím a pátém patře. Použitá zařízení jsou od firmy DELL, konkrétně typ Power Edge R210. Jsou to zařízení velikosti 1U a jsou umístěny v racku. Každý server je vybaven čtyř jádrovým procesorem Intel Xeon 3400, dále 8 GB ECC paměti RAM a 250 W zdrojem s 80+ certifikací. Na těchto zařízeních běží operační systém Microsoft Windows Server ve verzi 2003. Servery slouží k hostování několika různých druhů aplikací. Jednou z nich je aplikace docházka, která je vytvořena v programovacím jazyku PHP a data z této aplikace potom slouží jako podklady ke mzdovému vyúčtování se zaměstnanci. Všechny firemní počítače jsou zapojeny do domény, je zde použit software Microsoft Domain Controller verze 2008. Dále servery hostují DHCP/DNS, WebServer, Virtual PC a databázi MS SQL 2003. V případě výpadku proudu jsou servery zálohovány UPS od firmy APC a to konkrétně Smart On-line UPS RT5000. Toto zařízené poskytuje 8 možností připojení serverů až do výkonu 3500 W / 5000 VA. Doba provozu na baterie závisí na množství připojených zařízení a může se pohybovat od 5 minut při 3500 W až po necelých 100 minut při 350 W.

1.4.4 Síťové tiskárny

Tiskárny ve firmě jsou od společnosti Minolta a to typy Bizhub 552, Bizhub C220 a Bizhub 283. Valná většina tiskáren je černobílých, jedna je barevná. Všechny tiskárny jsou se zabudovanými skenery a umožňují standartní operace, jako například skenování dokumentů přímo do emailu či posílání faxu. Každá tiskárna obsahuje zabudovaný server, který posílá veškerou statistiku výrobci a umožňuje její prohlížení managementem. V případě poruchy se tiskárny umí samostatně diagnostikovat a vyslat požadavek na servisní zásah. Ten je servisním centrem garantován do osmi hodin od přijetí. Jelikož firma tiskárny nevlastní, ale jsou v pronájmu, v případě neopravitelné poruchy je tiskárna vyměněna za novou.

1.4.5 IP telefony

Ke komunikaci ve firmě i mimo ni slouží IP telefony a ústředna od výrobce Alcatel. Konkrétně jsou to tři typy telefonu a to IP Touch 4018 a 4038 a starší 4035 Advanced. Všechny telefony využívají technologii PoE (Power over IP), tudíž si vystačí pouze s napájením ze switche. S komunikací souvisí i vybavení zasedacích místností.

Kvůli potřebě videokonferencí s centrálou v Bury je zde nainstalován konferenční Cisco TelePresence systém se dvěma 50" LCD obrazovkami a HD kamerou. Díky tomuto systému je video a audio přenášeno ve vysoké kvalitě.

1.5 Software

1.5.1 Operační systémy

Klientské stanice jsou vybaveny operačními systémy společnosti Microsoft Windows a to ve verzi XP Professional na starších stanicích a ve verzi 7 na stanicích novějších.

1.5.2 Aplikační software

Téměř všechen firemní software včetně emailu je outsourcován v data centru v Hemelu. Pro přístup se používá virtualizační software XeApp od firmy Citrix. Toto řešení ulehčuje správu licencí a velkým plusem je to, že o zálohování se stará obsluha data centra. Mezi základním softwarem nalezneme balík Microsoft Office, pro přístup k poště se používá Outlook nebo Lotus Notes. Dále mají týmy k dispozici nejrůznější softwarové produkty od jednoduchého reportovacího software až po složité ERP systémy, používané napříč všemi společnostmi patřícími do stejné skupiny. Některé stanice jsou vybaveny softwarem Microsoft Office ve verzi 2007. Pro interní správu a účetnictví se používá program Money S3.

1.5.3 Antivirové řešení

Antivirové řešení bylo zvoleno od společnosti McAfee. Řešení se vyznačuje použitím architektury server-klient, kdy se o aktualizace klientských stanic stará přímo firemní server. Není tedy třeba, aby každá stanice stahovala aktualizace zvlášť, server je stáhne jednou a poté je distribuuje dál.

1.6 Zpracovávaná data

Většina dat, se kterými týmy pracují, je zpracovávána a uložena na serverech v data centru. Mezi aplikace vytvářející data, která zůstávají ve společnosti, můžeme zařadit účetní software či různé interní aplikace, většinou využívající databáze MS SQL. Dále jsou to různé dokumenty, ať už se jedná o propagační materiály, smlouvy, analýzy a statistiky, tiskové zprávy apod.

1.7 Archivace a zálohování

Z předchozí kapitoly vyplývá, že se ve firmě nacházejí tři typy dat. Jedná se tedy o databáze, účetní data a uživatelské dokumenty. Co se týče zálohování a archivace dat z uživatelských stanic, situace je zde špatná. Zálohování se neprovádí vůbec a v případě poruchy tak uživatelé přijdou o veškerá data. Lépe se zachází s účetními daty a s databázemi. Záleží, jak často se databáze mění, nicméně záloha probíhá například před začátkem pracovní doby a těsně po jejím skončení. Zálohování je zajištěno přesunutím dat na jinou diskovou jednotku, která je zabezpečena proti selhání zapojením do režimu RAID 1.

1.8 Fyzické zabezpečení

Prostory, ve kterých firma sídlí, jsou lokalizovány v nově postavené kancelářské budově. Všichni zaměstnanci musí projít vrátnicí, aby se dostali na svá pracoviště. Identifikace zaměstnanců je zajištěna čipovými kartami. Z důvodů bezpečnosti je vstup omezen a zaměstnanci tedy nemohou přijít do práce mimo pracovní dobu. Návštěvníkům jsou proti podpisu vydány jednorázové čipové karty. Vrátný má k dispozici kamerový systém, pomocí kterého monitoruje dění v budově a v podzemních garážích. Přístup do serverové místnosti má pouze několik lidí, většinou z IT oddělení. Proti požáru je budova chráněna integrovaným hasícím systémem a na vhodných místech jsou rozmístěny ruční hasicí přístroje. Firma dále pravidelně pořádá protipožární cvičení.

1.9 Současná bezpečnostní politika

V současné době ve firmě neexistuje žádný konkrétní dokument, týkající se bezpečnostní politiky. Všechny pravidla a doporučení jsou nepsaná. Chybí zde jakákoliv směrnice týkající se plánů zálohování, havarijních plánu nebo plánů obnovy po živelné či útokem zaviněné pohromě. Firma postrádá psaná pravidla, definující povinnosti a práva jednotlivých zaměstnanců a správců IT ve vztahu k firemní bezpečnosti. Zaměstnanci jsou sice upozorněni, aby nepoužívali počítače a software pro své soukromé účely, nicméně porušení tohoto zákazu není nijak sankciováno a není ošetřeno v žádné směrnici.

2 Teoretická východiska řešení

Na tomto místě bych chtěl nastínit základní pojmy a principy z oboru počítačové bezpečnosti, kterými se budu řídit při návrhu řešení.

2.1 Bezpečnostní politika IT

„Informační systémy se často stávají obětmi útoků různých druhů lidí, kteří se chtějí například získat neoprávněnou výhodu z průniku do cizího informační systému nebo chtějí mít jenom pocit, že jsou tak dobří, že jsou schopni překonat ochrany, které informační systémy chrání. Protože ale nikdy nevíme a priori o jaký typ narušitele se jedná – jestli o člověka se špatným úmyslem, „sportovcem" nebo jenom o pracovníka, který je nedbalý – musíme se těmto útokům, přesněji řečeno potenciálním hrozbám takových útoků, bránit. Soustavě opatření na ochranu firemních aktiv v oblasti IS/IT říkáme bezpečnost IS/IT (11, s. 65-66)."

Do oblasti bezpečnosti IS/IT spadá několik položek:

- Vymezení bezpečnosti IS/IT
- Koncepce nasazení bezpečnosti IS/IT v konkrétních podmínkách organizace
- Dokumentace bezpečnosti IS/IT a způsoby její správy
- Kontrola a audit bezpečnosti IS/IT

Informační systém můžeme prohlásit za bezpečný v případě, že data v něm uložená splňují následující podmínky:

- Důvěrnost - Atribut dat, díky němuž s nimi mohou pracovat pouze autorizované subjekty a to buď jedinci, technická zařízením či procesy. Data tedy nemohou používat neautorizované osoby či jiné než firemní počítače a mají-li data atribut pouze ke čtení, není možné je zkopírovat či vytisknout (11, s. 66).
- Dostupnost - Neméně důležitý atribut, který má zabezpečit dostupnost a použitelnost informací na vyžádání autorizovaného subjektu (11, s. 66).
- Integritu - Atribut dat zajišťující celistvost dat, což znamená, že data nejsou pozměněna či úplně zničena neautorizovaným způsobem (11, s. 66).

Kromě zabezpečení dat, je pro celkovou bezpečnost informačního systému nutné se věnovat i dalším atributům:

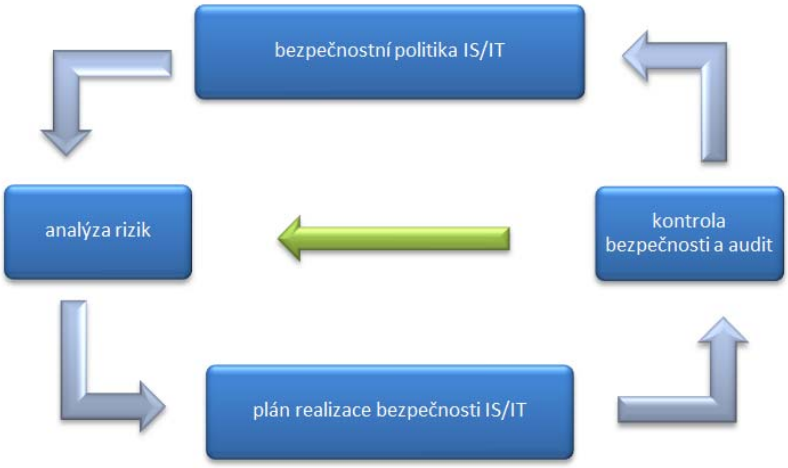
- Prokazatelnost prováděných operací - Tento atribut je spojen s tím, že se jednotlivé akce, prováděné určitou entitou, ať už ve formě datového souboru či technického zařízení, dají zpětně vysledovat. Musí být tedy přesně identifikováno, který subjekt provedl příslušnou operaci (11, s. 66).

- Pravost subjektu - Musí být zajištěno, že subjekt je prokazatelně ten, za kterého se vydává. Tento proces se nazývá autentizace a je prováděn při přihlašování se do informačního systému. Je podmíněn tím, že subjekty vlastní jednoznačný identifikátor, v případě uživatelů se většinou jedná o uživatelské jméno a heslo. Pokud je vyžadována bezpečnější autentizace, je možné použít například čipové karty či z oblasti biometriky snímání oka či otisk prstu (11, s. 66).

- Spolehlivost systému či jeho prvku - Schopnost informačního systému provádět funkce dle specifikovaných požadavků, které můžeme nalézt například v projektové dokumentaci. Spolehlivost IS musí zahrnovat i aspekty spolehlivosti technických zařízení, pravděpodobnost jejich selhání či problém životnosti. Selhání IS či jeho části má za následek velké ekonomické a finanční problémy. Je potřeba uvažovat nad všemi možnostmi zajištění spolehlivosti IS a to například ve formě smluv na náhradní zpracování dat, záložních počítačů a serverů či jiných technických zařízení (11, s. 66).

2.1.1 Výstavba systému bezpečnosti IS/IT

Pro návrh bezpečnostní politiky jsou důležitými body podnikatelská strategie společnosti a také konkrétní požadovaná úroveň zabezpečení. Na základě těchto bodů je možno určit základní firemní bezpečnostní politiku a na ni vypracovat analýzu rizik. Tento proces výstavby je kontinuální a musí být periodicky obnovován, jak je vidět na obrázku níže:



Obrázek 3: Cyklus budování systému bezpečnosti IS/IT

Zdroj: (12, s. 86)

2.1.2 Bezpečnostní politika firmy

Jakmile si firma vyjasní, jakou úroveň bezpečnosti požaduje a která aktiva jsou pro ni nejcennější, může se pustit do zpracování bezpečnostní politiky. Tento dokument je tvořen nejvyšším vedením firmy a obsahuje jak strategické cíle, tak způsoby a nástroje, jak těchto cílů dosáhneme.

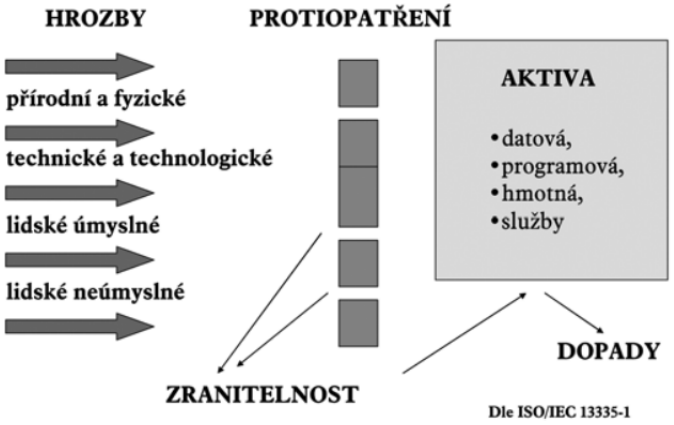
„Vzhledem k tomu, že budování bezpečnosti IS/IT je permanentní proces, je nutné bezpečnostní politiku v pravidelných časových intervalech přehodnocovat a aktualizovat. Za východiska pro změny v bezpečnostní politice jsou obvykle považovány závěry analýzy rizik, výsledky monitorování, vyhodnocování bezpečnostních incidentů a závěry kontrolních a auditorských zpráv (12, s. 87).“

2.1.3 Analýza rizik

Analýzou rizik se v kontextu počítačové bezpečnosti myslí odhad a stanovení ztrát zaviněných hrozbami působícími na IS/IT. Důležitými faktory ovlivňujícími kvalitu a účinnost analýzy jsou zkušenosti expertního týmu a kvalita poskytnutých podkladů. Členové týmu se musí umět vžít do role útočníka a být schopni analyzovat různé druhy hrozeb. Vstupní podklady jsou neméně důležitým faktorem, protože pokud bude analýza provedena na neúplných či málo kvalitních podkladech, tak i výsledný systém bude z hlediska bezpečnosti naprosto nevyhovující. Techniky a postupy analýzy rizik jsou podrobně popsány v normě ČSN ISO/IEC 13335 1-5.

2.2 Základní prvky schématu bezpečnosti

Proces řízení bezpečnosti obsahuje několik základních prvků, o které budou podrobněji rozepsány v dalších podkapitolách. Na obrázku dole je zachycena jejich vzájemná souvislost.



Obrázek 4: Schéma zajištění bezpečnosti IS/IT

Zdroj: (11, s. 66)

2.2.1 Aktiva

Jsou takové součásti IS/IT, které mají pro firmu velkou hodnotu a jejich poškození či ztráta by měly vážné ekonomické následky. Proto si tato aktiva zaslouží adekvátní ochranu dle míry zranitelnosti. Aktiva lze podle jejich podstaty rozdělit na hmotná a nehmotná. Mezi hmotná aktiva počítáme jak technické vybavení, jako například počítače, servery, tiskárny, mobilní telefony, tak i součásti firemní

infrastruktury v podobě rozvodů elektřiny, síťových rozvodů či jiných technických zařízení. V případě nehmotných aktiv uvažujeme veškerá firemní data ať už v podobě databází či firemních dokumentů. Dále sem patří softwarové vybavení a jako poslední prvek zde můžeme zařadit i image firmy či její pověst (11, s. 67).

2.2.2 Hrozby

Pod pojmem hrozby se skrývají různé okolnosti či události, které významným způsobem působí na zranitelné místo aktiva a mohou zapříčinit potenciální škody. Hrozeb existuje několik druhů. Přírodní a fyzické hrozby zahrnují různé živelné pohromy či nehody, způsobené například poruchou dodávky elektrického proudu, požárem nebo povodněmi. Technické a technologické hrozby spočívají v náhlých poruchách počítačů, nosičů dat nebo nesprávnou funkčností programového vybavení. Dále rozlišujeme hrozby způsobené lidmi a to ať už úmyslné, tak neúmyslné. Mezi hrozby neúmyslné řadíme ty, které jsou způsobené neznalostí či zanedbáním povinností. Úmyslné hrozby dále dělíme na vnější, tedy působící na systém zvenku, jako například hackeři, teroristé nebo mezifiremní špionáž. Tyto hrozby tvoří velice malou část a podle některých statistik až 98% hrozeb pochází zevnitř společnosti. Mohou to být například zlomyslní a chamtiví zaměstnanci nebo různí návštěvníci a hosté organizace (11, s. 67).

2.2.3 Zranitelnosti

Slabá místa aktiv se nazývají zranitelnosti. Můžeme je dělit na fyzické zranitelnosti, obsahující budovy a počítačové místnosti, dále na zranitelnosti technických a programovacích prostředku, zranitelnosti nosičů dat, kterým lze předejít například pravidelným zálohováním nebo zranitelnosti komunikačních systému. Tímto se myslí odolnost těchto systémů vůči odposlechu či možnosti přerušení spoje. Jako poslední druh zranitelnosti bych zmínil personální zranitelnost, která spočívá v úmyslných či neúmyslných chybách způsobených lidským faktorem (11, s. 67).

2.2.4 Protiopatření

Snížení síly hrozby nebo jejího úplného zabránění můžeme dosáhnout vhodnými protiopatřeními. Za vhodné protiopatření je považována jakákoliv aktivita, zařízení, technika či postup, působící jako prevence hrozeb, kterým musí informační systém čelit. Tyto protiopatření mívají různý charakter. Administrativní charakter protiopatření zahrnuje různé směrnice pro práci s IS/IT, například směrnice pro použití elektronické

pošty, směrnice pro zajištění zálohování a archivace dat apod. Fyzická protiopatření se zabývají používáním zámku, trezorů pro ukládání kopií dat, čipových karet pro přístup do citlivých prostorů. Technické a technologické protiopatření spočívají v autorizaci a autentizaci přístupů k aktivům IS/IT, například prostřednictvím hesel (11, s. 67).

2.3 Útočníci

Každý počítačový systém se v průběhu času setká s nějakým druhem útoku. Útočníci nemusí být pouze lidé se zlými úmysly. Spousta útoků na systém pramení z neznalosti uživatelů a bohužel tato neznalost často působí rozsáhlé škody. Útočníky můžeme rozdělit na dvě hlavní skupiny a v každé skupině lze nalézt několik typů útočníků.

2.3.1 Vnější útočník

Za vnější útočníky jsou považovány všechny osoby, které nemají fyzický přístup k vnitřní podnikové síti. Pokud se rozhodnou pro útok, musejí se potýkat s veškerými bezpečnostními opatřeními, které jsou v síti zavedeny. Myslí se tím překonávání firewallů či prolomení zabezpečených protokolů, určených ke komunikačním relacím (1, s. 154).

Amatér

Nejméně nebezpečný typ útočníka. Většinou se jedná o studenta střední školy či zástupce laické veřejnosti, kteří mají minimální počítačové znalosti. Motivem útoku u těchto lidí bývá pouhá zvědavost. Snaží se využít například známou bezpečnostní chybu, která je už dlouhý čas popsaná na internetu. Ochrana informačního systému proti amatérským útokům je velice levná a jednoduchá, v podstatě stačí systém udržovat aktualizovaný. V aktualizacích jsou obsaženy záplaty na známé bezpečnostní chyby.

Hacker (Cracker)

Je třeba rozlišovat mezi termíny Hacker a Cracker. Oba dva jsou již vybavení hlubokými znalostmi z oblasti IT. Hacker ovšem své znalosti používá k nalezení bezpečnostních děr. Pokud díru najde, upozorní na to správce serveru a dá mu určitý čas na nápravu. Tito lidé se sdružují do hackerských skupin, které jsou velice dobře organizované. Jde jim o prestiž, nezpůsobují tedy větší hmotné škody. Cracker naproti tomu zneužívá bezpečnostní díry nalezené hackerskou skupinou pro vlastní obohacení

či k jiným kriminálním účelům (botnet apod.). Crackeří také obcházejí zabezpečení programů, vystavují je zdarma na internetu a tím pádem připravují softwarové společnosti o zisk. Motivací k útoku je zase snaha dokázat si své kvality či přirozená zvědavost. Tito útočníci jsou limitováni prostředky a výpočetním výkonem. Většina počítačových systémů je i proti útoku Hackerů a Crackerů dobře chráněna (1, s. 155).

Profesionál

Je člověk, který má hluboké znalosti z oblasti IT. Většinou se dokonce živí jako bezpečnostní expert. Zná téměř všechny slabá místa počítačových systémů a ví, jak je zneužít. Má k dispozici prakticky nelimitované prostředky, ať už výpočetní výkon či jiné. Typicky to může být zaměstnanec vlády provádějící špionáž ať už ve vlastní zemi či mimo ni. Napadený subjekt má velice malou šanci na obranu, ochrana proti takovému druhu útoků je nesmírně drahá. Pravděpodobnost napadení počítačového systému profesionálem je ovšem velice nízká a firmy většinou doufají, že se jim útok vyhne (1, s. 155).

2.3.2 Vnitřní útočník

Tento typ útočníka má přímý přístup k firemní síti. Může se jednat buď o zaměstnance či externistu nebo o osobu, která interního zaměstnance donutila ke spolupráci. Útoky prováděné vnitřním útočníkem mají většinou povahu nechtěných nehod, způsobených nedostatečnou kvalifikací zaměstnanců v oblasti informačních technologii. Může se jedna například o smazání důležitého souboru či zálohy nebo v horším případě záměrný únik cenný dat ke konkurenci. Druhý případ se většinou děje ze msty. Ochrana proti tomuto druhu útočníků spočívá v kvalitním školení zaměstnanců, ve správné konfiguraci celého systému a ve zvyšování loajality zaměstnanců (1, s. 154).

2.4 Organizační struktura bezpečnosti IT

Protože se bezpečnost IS/IT dotýká skoro všech zaměstnanců v podniku a celého informačního systému, je třeba pro zabezpečení efektivního fungování firmy přiřadit jednotlivým uživatelům jejich pravomoci a odpovědnosti. Níže uvedená struktura je univerzální a tudíž až tak nezáleží na velikosti firmy a jejím organizačním schématu. Tyto výkonné a kontrolní role je potřeba pokrýt v každé organizaci.

2.4.1 *Kontrolní role*

- *„Vrcholové vedení organizace*
  - *Deklaruje strategické cíle*
  - *Formuluje bezpečnostní politiku organizace*
  - *Pravidelně vyhodnocuje stav bezpečnosti v organizaci*
- *Auditor bezpečnosti IS/IT*
  - *Provádí pravidelný audit v oblasti IS/IT podle stanovené metodiky*

2.4.2 *Výkonné role*

- *Bezpečnostní manažer organizace*
  - *Provádí aktualizace politiky bezpečnosti IT a bezpečnostních směrnic*
  - *Koordinuje prozkoumávání incidentů*
  - *Metodicky vede bezpečnostního manažera IS/IT*
- *Bezpečnostní manažer IS/IT*
  - *Zodpovídá za zavedení bezpečnosti IS/IT v organizaci*
  - *Řeší bezpečnostní incidenty*
  - *Denně monitoruje implementaci a používání ochranných opatření*
- *Pracovník IT oddělení*
  - *Je odpovědný za provozování bezpečnostních funkcí*
  - *Vyšetřuje a oznamuje bezpečnostní incidenty*
  - *Zodpovídá za nastavení IS/IT (8, s. 12 – 14)“*

2.5 Prostředky zabezpečení

Jsou to nástroje zabraňující v přístupu k citlivým firemním datum a prostředkům neautorizovaným uživatelům a na druhé straně zaručují přístup autorizovaným entitám.

2.5.1 Firewall

Firewall chápeme jako sadu opatření (hardwarových, softwarových či personálních), které mají za cíl propojit dvě či více sítí s různou úrovní důvěryhodnosti tak, že sníží rizika vyplývající pro chráněné sítě z tohoto připojení. Firewally řídí síťový provoz a z hlediska bezpečnosti jsou hlavní bránou mezi bezpečnou vnitřní sítí a (zpravidla) nepřátelským vnějším světem (1, s. 116).

2.5.2 Antivir

Nebezpečný a škodlivý software v podobě virů, trojských koní či spyware je pro společnosti velkou hrozbou. Protiopatřením je právě instalace antivirového software, který se většinou automaticky stará o pravidelné skenování a odstraňování škodlivého softwaru. Pro zajištění plné funkčnosti je potřeba antivirový software pravidelně aktualizovat, jedině potom je schopný zasahovat proti nejnovějším hrozbám.

2.5.3 Proxy server

Může se jedna o určitý druh hardwarového firewallu či softwarového programu, který přebírá požadavky na připojení do sítě internet a předává je dál cílovým internetovým hostitelů, jako by byl jejich původcem sám. Na druhé straně hostitelské počítače potom odpovídají serveru proxy, který jejich odpovědi předává příslušnému klientovi interní sítě. Proxy servery se ve společnostech používají pro omezení přístupů, protokolování požadavků na spojení a v neposlední řadě také ke zrychlení spojení ukládáním často požadovaného veřejného obsahu do paměti cache (3, s. 37).

2.5.4 VPN (Virtual Private Networking)

Je technologie zabezpečeného propojení dvou a více subjektu přes síť Internet. Myslí se tím například propojení různých poboček stejné firmy, které jsou ovšem umístěny v různých geografických lokalitách. Propojení těchto poboček lze vyřešit buď vybudováním přímého fyzického spoje, tedy vlastní síť WAN nebo použitím existující celosvětové sítě Internet. Budování sítě WAN je nesmírně drahé a náročné, proto firmy využívají technologii VPN. Ta pomocí protokolů IPsec nebo PPTP vytvoří zabezpečený

tunel mezi dvěma subjekty, kterým mohou proudit důvěrná firemní data. Využívají se zde pokročilé šifrovací algoritmy a digitální certifikáty identity (3, s. 341-345).

2.6 Řízení přístupu

Řízení přístupu se v kontextu počítačové bezpečnosti myslí soubor technik, které určují oprávnění přístupu uživatelů k systémovým objektům či prostředkům. Většinou se jedná o různé soubory, databáze či sdílené disky. Aby bylo řízení přístupu účinné, používá se přístup tzv. „nejmenších privilegií“. V praxi to znamená, že uživatelé mají implicitně zakázány veškeré přístupy a povoleny jsou pouze ty, které potřebují pro svou práci. Tyto přístupy by měly podléhat časovému omezení a pravidelně se podrobovat revizi.

2.6.1 Active Directory

Pod tímto pojmem se skrývá databáze všech síťových objektů v prostředí Microsoft Windows Server. Active Directory je prostředek k efektivnímu uspořádání síťových prvků do hierarchie, která kopíruje organizační strukturu společnosti. Výhodou je potom centralizovaná správa a možnost úpravy bezpečnostní politiky pro jednotlivé entity. Tato technologie je implementací protokolu LDAP a zároveň využívá autentizační protokol Kerberos (4, s. 103).

2.6.2 Doména

Za doménu je považováno logické seskupení pracovních stanic připojených do sítě, sdílejících stejné síťové a datové zdroje, které poskytuje server. Síťovými údaji mohou být uživatelské účty, informace o zabezpečení či firemní bezpečností politiky. Doména je řízena doménovým řadičem, který uživatelům povoluje či odepírá právo přístupu ke specifickému prostředku či zdroji. Uživatel má tedy po autentizaci k dispozici všechny zdroje serveru, které jsou definovány jeho uživatelským účtem (4, s. 102).

2.6.3 Group Policies (Zásady skupin)

Jsou součástí Active Directory a v zásadě umožňují centralizovanou správu uživatelů a počítačů. Tento nástroj je velice užitečný při výstavbě bezpečnostní politiky, protože umožňuje skupinám či jednotlivým uživatelům nastavení oprávnění přístupu k určitým objektům v doméně i mimo ni. Zabezpečuje implementaci firemní

bezpečnostní politiky například zákazem instalace nových programů na pracovních stanicích bez příslušného oprávnění.

2.7 Ochrana dat

Nejcennějším aktivem ve společnosti jsou bezesporu data. Tyto data jsou typicky uložena na pevných discích v serverech nebo na jiných zálohovacích mediích, ať už to jsou magnetické pásky či optická média. Všechny tyto média mají společnou vlastnost a to je větší či menší nespolehlivost. Naštěstí existují techniky a přístupy k ochraně dat, které budou v této kapitole dále popsány.

2.7.1 Diskové pole

Ať už se jedná o součást serveru či dedikované hardwarové zařízení, kvůli zvýšení výkonu a redukci chyb se disky spojují do tzv. diskových polí. Tyto diskové pole se navenek tváří jako jeden disk a vnitřní uspořádání dat se řídí metodou RAID. Rozlišujeme mnoho typů RAID polí, v praxi se ovšem nejvíc používají tři níže uvedené typy (4, s. 51-52).

- RAID 0 (Striping neboli prokládání)

  V případě RAID 0 se data rozdělují mezi dva a více disků. Výsledkem je podstatné snížení přístupové doby a zvýšení rychlosti čtecích i zapisovacích operací, protože data jsou najednou zapisována či čtena z obou disků. Pokud ovšem jeden z disků selže, přijdeme o všechny data. Z tohoto důvodu se tento typ RAID pole v podnikové praxi moc nepoužívá a slouží pouze v případech, kdy je třeba zapsat či číst velké bloky dat. Například při editaci filmů, fotografií nebo audio nahrávek (4, s. 51-52).

- RAID 1 (Mirroring neboli zrcadlení)

  Pokud jsou disky zapojeny v režimu RAID 1, tak se data automaticky zapisují na oba tyto disky zároveň. Jeden je tedy přesnou kopií toho druhého. Pří poruše jednoho se nic nestane, protože data jsou zálohována na druhém. Při tomto zapojení je nutné používat stejně velké disky, protože pokud by se například obsah menšího disku zrcadlil na disk větší, rozdíl v kapacitách by zůstal na větším disku nevyužit. Nevýhodou je potom poloviční kapacita disků oproti stavu, když by disky v RAID 1 nebyly (4, s. 51-52).

- RAID 5 (Striping s redundancí)

  Zapojení disků do režimu RAID 5 se používá hlavně u dražších serverů. Jedná se o variantu, kdy nadbytečná paritní data jsou rozprostřena na všech discích. Při výpadku jednoho disku je možné jeho obsah dopočítat s pomocí údajů uložených na zbylých discích. Minimální počet disků pro toto zapojení je tři (4, s. 51-52).

2.7.2 Zálohování

Pravidelné zálohování chrání důležitá firemní data proti živelným pohromám v podobě požárů, povodní, výpadku proudu. Dále se zálohováním chrání data proti krádeži či proti zásahu uživatele, který může data nechtěně smazat či jinak znehodnotit.

2.7.3 Plánování zálohování

Aby záloha kvalitně chránila data, je potřeba se detailně věnovat níže uvedeným bodům.

- Co zálohovat

  Zálohovací média mají omezenou kapacitu, a proto je nutné si dopředu rozmyslet, která data zálohovat. Vždy zálohujeme pouze data jednotlivých aplikací, nikoliv aplikace samotné, protože ty se dají vždy lehce obnovit za použití instalačních medií či diskových obrazů (4, s. 131).

- Určení frekvence zálohování

  Frekvence zálohování závisí na povaze dat a hlavně na frekvenci jejich změny. Pokud se data mění denně, je potřeba i zálohy provádět denně. Data, která se mění pouze týdně, je zbytečné zálohovat denně, protože pouze zabírají místo na zálohovacích médiích (4, s. 131).

- Výběr média pro uložení zálohy

  V zásadě jsou dvě možnosti. Buď zálohovat na vyměnitelné médium, jako je například magnetická páska nebo na pevný disk. Z hlediska bezpečnosti dat je výhodnější zálohovat na vyměnitelné médium, protože ho lze umístit odděleně od počítačů a v případě kompromitace serverů živelnou pohromou či krádeží lze tyto data snadněji obnovit (4, s. 131).

- Místní nebo síťové zálohování

  Rozhodnutí mezi místním nebo síťovým zálohováním velice záleží na způsobu práce s daty. Pokud data ukládáme pouze na server, záloha se bude týkat pouze tohoto serveru. Jsou-li ovšem důležitá data uložena na stanicích, je potřeba zálohovat i tyto stanice. Většinou se tyto zálohy soustředí do jednoho bodu, typicky na páskovou jednotku v serveru (4, s. 131).

2.7.4 Typy zálohování

Typů záloh existuje vícero, v praxi se ovšem používají tři a navíc se většinou kombinují dohromady. Každý typ má určité výhody a nevýhody a rozhodnutí, jaký typ zálohování použít, je potřeba důkladně zvážit.

- Normální (úplné)

  Při této záloze se pokaždé zálohují všechna data. Obnova je potom rychlá, nicméně vytvoření zálohy trvá dlouho a samotné jednotlivé zálohy zabírají hodně paměťového prostoru (4, s. 131).

- Přírůstkové

  V případě přírůstkové (inkrementační) zálohy jsou zálohovány pouze soubory, které se změnily od poslední úplné zálohy. Zálohy mají menší objem dat a pro obnovu je nutné mít k dispozici úplnou zálohu a všechny zálohy přírůstkové (4, s. 131).

- Rozdílové

  Stejně jako v případě inkrementační zálohy se zálohují pouze soubory, které se od minulé úplné zálohy změnily. Rozdíl je ovšem v obnově dat, kdy už rozdílové zálohy nám stačí mít úplnou zálohu a pouze jedna rozdílová záloha (4, s. 131).

2.7.5 Obnova dat

Zálohy již vytvořeny jsou, naše data jsou zachráněna. Bohužel pořád ještě není vyhráno. Aby byla ochrana dat dokonalá, je potřeba mít zvládnutý proces obnovy. Je potřeba mít vyzkoušeno, jak se přesně obnova dělá, jak dlouho trvá a také je třeba mít data řádně označena. V případě magnetických pásek je nanejvýš nutné, aby byly správně popsány, co obsahují a kdy byly vytvořeny. Tyto média je potřebné skladovat

v dobrých podmínkách a preventivně je po určitém čase měnit, i když ještě nedošly na konec své životnosti (4, s. 131).

2.8 Normy

2.8.1 ISO 27001:2005

Je hlavní norma pro Systém řízení bezpečnosti informací (ISMS). Byla publikována v roce 2005 a dříve se označovala jako BS7799-2. Tato norma popisuje systém řízení, strukturu a procesy pro řízení bezpečnosti informací podle opatření definovaných v ISO/IEC 27002. Užitím modelu PDCA se snaží zdokonalit efektivnost systému řízení bezpečnosti informací v podniku.

„Mezi hlavní aspekty, kterými se norma zabývá, patří:

- *Harmonizace s normami pro další systémy řízení*
- *Kontinuální zajištění procesu zlepšování řízení bezpečnosti informací*
- *Celopodnikové řízení*
- *Zajištění souladu s právními a regulatorními předpisy*
- *Záruky za bezpečnost informací*
- *Zavedení principů OECD pro oblast bezpečnosti informačních systémů a sítí“ (14)*

2.8.2 ISO 27002:2005

Tato ISO norma je považována za nejlepší sbírku bezpečnostní praktik, které může firma použít pro zabezpečení svých cenných informací. Je rozdělena do jedenácti základních oddílů a v těchto oddílech je stanoveno 39 kontrolních cílů, jejichž splnění vede k vysokému stupni ochrany informačních aktiv proti potenciálnímu útoku. Základní oddíly se zabývají bezpečnostní politikou a organizací bezpečnosti, klasifikací a řízením aktiv, bezpečnosti lidských zdrojů, fyzické bezpečnosti a bezpečnosti prostředí, řízením komunikace a provozu, řízením přístupů, vývojem a údržbou informačních systémů, zvládáním bezpečnostních incidentů, řízením kontinuity činnosti organizace a soulad s požadavky (15).

3 Návrh řešení

Na tomto místě chci navrhnout řešení určitých nedostatků, které se ve firmě nacházejí. Z analýzy vyplývá, že firma si v mnoha ohledech nevede vůbec špatně, co se bezpečnosti týče. Některé detaily si přesto zaslouží pozornost a jejich revizí může dojít ke zlepšení celkové bezpečnostní situace. Ze začátku popíši určitá technická protiopatření, posilující bezpečnost a v druhé části se potom budu věnovat složce organizační. Pokusím se o vytvoření organizační struktury bezpečnosti, vytvořím funkce a přidělím jim odpovědnosti a pravomoci a dále vytvořím návrhy směrnic a předpisů.

3.1 Technické a logické prostředky ochrany dat

3.1.1 Uživatelé

Firemní počítače jsou zapojeny do domény a uživatelské účty jsou součástí systému Active Directory. Problém vzniká při špatném či žádném nastavení tohoto systému. Jako příklad uvedu tvorbu hesel. Systém je nastaven na maximální bezpečnost a pamatuje si posledních 24 hesel. Toto frustrující nastavení vede uživatele k tomu, že si hesla různě lepí na monitory či si je zapisují a případný útočník má tedy svou práci velice ulehčenou. Doporučuji tedy změnit toto nastavení paměti hesel na rozumnou hodnotu 5. Dalším detailem je existence obecných účtů, u kterých se vůbec heslo nemění, a tyto bych z hlediska bezpečnosti rovnou odstranil.

3.1.2 Zálohování a archivace dat

Řešení využívající RAID 1 diskové pole je v pořádku. Problémem je, že toto diskové pole se nachází ve stejné místnosti jako zálohované servery. Navrhuji proto zakoupení páskové zálohovací jednotky a uskladnění pásek mimo budovu. Data jsou pro firmu to nejcennější a tento krok výrazně posiluje jejich bezpečnost. Doporučil bych zakoupení páskové mechaniky od firmy HP a to konkrétně model HP 1/8 G2 LTO 5 3000 FC Autoloader. Toto zařízení kromě vlastní páskové mechaniky obsahuje plně robotickou knihovnu na 8 médií. Podle množství dat určeného k zálohování by zástupci

společnosti vybrali odpovídající velikost pásky. Ty se pohybují ve velikostech od 100 GB do 1,5TB.

3.1.3 Uživatelské stanice

Stanice jsou hlavní pracovní nástroje zaměstnanců, a proto doporučuji častější obměnu hardwaru. Některé jsou zastaralé a práce s nimi je náročná a vyžaduje trpělivost. Dále by se tyto stanice měly aspoň jednou ročně podrobit vyčištění od prachu, které pozitivně působí na zvýšení životnosti.

3.2 Bezpečnostní politika

Jelikož má firma nevýrobní charakter a zabývá se službami, každý zaměstnanec musí při své práci využívat informační technologie. Jak již bylo citováno v teoretické části, většina úmyslných či neúmyslných bezpečnostních hrozeb je realizována samotnými uživateli uvnitř firmy. Bohužel za tyto hrozby nejsou stanoveny žádné sankce. V této kapitole se budu zabývat návrhem bezpečnosti IS/IT, který povede k eliminaci potenciálních hrozeb.

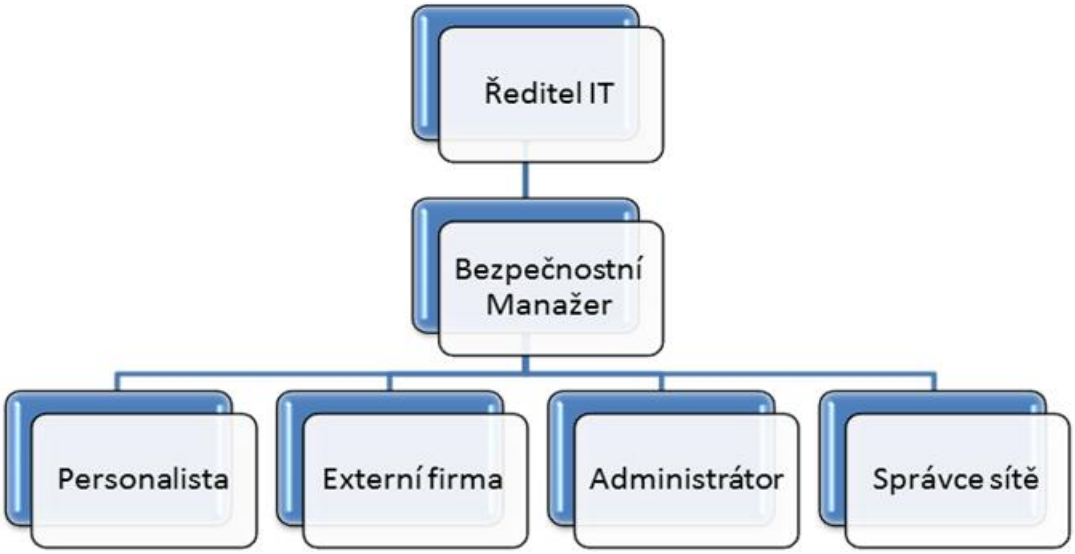
Doporučuji změnit organizační struktury IT oddělení a to vytvořením několika nových rolí. Jednou z nejdůležitějších rolí bude tzv. CISO (Chief Information Security Officer), česky Bezpečnostní Manažer. Bude zodpovídat řediteli IT za zajištění bezpečnosti ve firmě a to zavedením bezpečnostní politiky. Vedení firmy bude mít na starosti výběr adekvátních pracovníků pro nově vytvořené role. Po výběru budou pracovníci obeznámeni s bezpečnostní politikou a budou jim přiděleny práva a povinnosti. CISO bude také zodpovědný za následný audit, který proběhne půl roku po zavedení bezpečnostní politiky a který bude mít za cíl odhalit případné nedostatky. Níže uvádím příklady nových rolí a jejich povinnosti.

3.2.1 Role

V rámci změny v organizační struktuře IT navrhuji následující role:

- **Bezpečnostní Manažer (CISO)**
  - Má na starosti kontrolu dodržování bezpečnostních předpisů
  - Jeho primární zodpovědností je bezpečnost firmy
  - Schvaluje smlouvy s externími firmami
  - Řídí krizové plány
- **Ředitel IT**
  - Určuje bezpečnostní politiku
  - Navrhuje pravidla pro práci s IT vybavením
  - Pravidelně sleduje logy
- **Administrátor**
  - Provádí správu softwarových licencí
  - Má na starosti přidělování a odebírání oprávnění na uživatelských účtech
  - Má zodpovědnost hladký průběh zálohování a následného procesu obnovy dat
  - Provádí aktualizace softwarového vybavení
- **Správce sítě**
  - Nakupuje hardware a periferie, zajišťuje funkčnost, údržbu a servis
  - Má na starosti zabezpečení počítačové sítě včetně nastavení firewallu

- **Personalista**
    - Zodpovídá za organizaci školení o bezpečnosti IS/IT pro zaměstnance
    - Je zprostředkovatelem zpětné vazby od uživatelů k CISO



Obrázek 5: Role v systému řízení bezpečnosti

Zdroj: (vlastní návrh)

3.2.2 Směrnice

Následující řádky popisují jednotlivé směrnice. U každé směrnice je uveden zaměstnanec zodpovědný za její vytvoření. Dále je ve směrnici uvedeno, koho se týká a kdo dohlíží na její dodržování. Za porušení směrnic navrhuji uplatňovat sankce v podobě srážky pohyblivé části mzdy.

- **Směrnice o fyzickém zabezpečení serverové místnosti**

  Navrhne: Bezpečnostní Manažer

  Obsah: Součástí směrnice bude popis opatření, která mají jednak zabránit neautorizovanému vstupu osob do prostorů serverové místnosti a dále potom zajistit její fyzickou bezpečnost. Do návrhu směrnice doporučuji firmě zařadit následující body:

  - Způsob evidence přístupů
  - Popis požárních protiopatření
  - Způsob práce s UPS
  - Nastavení klimatizačního zařízeni
  - Specifikování nároků na vstupní dveře

  Dohlíží: Ředitel IT

  Platí pro: všechny uživatele, kteří mají do serverové místnosti přístup

  Sankce: Za porušení směrnice je zaměstnanci udělena sankce do výše 10 000 Kč sražená z pohyblivé části mzdy.

- **Směrnice o přístupu a pohybu osob ve firemních prostorách**

  Navrhne: Bezpečnostní Manažer, Hlavní personalista

  Obsah: Směrnice se bude detailně zabývat způsoby, jak zabezpečit, aby se ve firemních prostorách pohybovali pouze autorizované osoby. Situace, kdy se do firmy dostanou nepovolané osoby je velice kritická a proto má tato směrnice velkou váhu. Doporučuju v ní popsat tyto body:

  - Povinnosti zaměstnanců při příchodu a odchodu z práce – Zákaz pouštění cizích osob, nutnost použití čipové karty při každém opuštění budovy.
  - Specifikace prostor s omezeným přístupem – Důležité technické zařízení v serverové místnosti či v archivu dat musí zůstat přístupny

pouze několika málo povolaným osobám. Budou zde tedy popsány mechanizmy přidělování příslušných oprávnění.

- Postupy při ztrátě čipových karet – Ověřování totožnosti zaměstnance při ztrátě a metody vydávání dočasných přístupových karet
- Evidence návštěv – Specifikace povinnosti doprovodu.

Dohlíží: Hlavní personalista

Platí pro: všechny zaměstnance a návštěvy

Sankce: Za porušení směrnice je zaměstnanci udělena sankce do výše 5 000 Kč sražená z pohyblivé části mzdy.

- **Směrnice o klasifikaci, ukládání a zálohování dat**

  Navrhne: Administrátor, Bezpečnostní Manažer, vedení společnosti

  Obsah: Jelikož neexistují písemná pravidla pro rozeznání citlivosti dat pro zaměstnance, navrhuji aby, klasifikace dat byla součástí této směrnice. Body, specifikované níže budou tvořit základ této směrnice.

  - Klasifikace dat – V tomto bodě směrnice vedení společnosti ve spolupráci s IT oddělením navrhne klasifikaci dat, určí jejich vlastníky a charakter. Dále také definuje označení důvěrných informací tak, aby bylo pro běžné uživatelé na první pohled jasné, že s nimi pracují.
  - Zálohování dat - Jsou zde popsány způsoby zálohování (kdy, jak často, jaká data, kam) a práce s archivovanými či náhradními kopiemi dat. Dále navrhuji ve směrnici specifikovat zaměstnance, kteří jsou zodpovědní za nastavení zálohovacího softwaru, a určit, kde a za jakých podmínek budou data uložena

  Dohlíží: Ředitel IT

  Platí pro: všechny uživatele

  Sankce: Za porušení směrnice je zaměstnanci udělena sankce do výše 10 000 Kč sražená z pohyblivé části mzdy.

- **Směrnice o konfiguraci firewallu**

  Navrhne: Bezpečnostní Manažer

  Obsah: Jelikož firewall představuje primární ochranou firemní sítě před útoky zvenčí, jakákoliv změna v nastavení musí být v souladu s navrhovanou směrnicí. Doporučuji, aby se v ní objevily tyto důležité body:

  - Povolení či zablokování portů a služeb – Musí být schváleno bezpečnostním manažerem.
  - Audit – Zde budou specifikovány doby kontroly nastavení firewallu, jestli pořád reflektuje aktuální firemní požadavky na bezpečnost příchozích a odchozích informací.
  - Přístup do logů – Specifikace zaměstnance, jehož úkolem bude pravidelná kontrola záznamů a případná akce při nalezení bezpečností hrozby.

  Dohlíží: Ředitel IT

  Platí pro: Správce sítě

  Sankce: Za porušení směrnice je zaměstnanci udělena sankce do výše 5 000 Kč sražená z pohyblivé části mzdy.

- **Směrnice o správě uživatelských účtů**

  Navrhne: Bezpečnostní Manažer, Hlavní personalista

  Obsah: Touto směrnicí se bude řídit zaměstnanec na pozici administrátor. Doporučuji v ní specifikovat následující body:

  - Zavedení uživatelského účtu – Tedy za jak dlouho bude účet vytvořen od nástupu zaměstnance do firmy, v jakém tvaru bude vytvořen uživatelské jméno (kombinace jména a příjmení), jaký tvar a délku bude mít heslo (minimálně 12 alfanumerických znaků, obsahuje alespoň 1 velké písmeno, nesmí začínat číslem).
  - Zařazení uživatelů do skupin – Přidělení uživateli patřičná přístupová práva podle jeho pozice.
  - Běžné vedení účtu – Nutnost změnit heslo jednou za 6 měsíců, udržovat ho v tajnosti.

- Obnova či zrušení účtu – Povinnost administrátora smazat uživatelský účet po ukončení pracovního poměru a v případě resetu zaměstnancova hesla povinný souhlas přímého nadřízeného a osobní účast zaměstnance.

Dohlíží: Ředitel IT

Platí pro: Administrátora

Sankce: Za porušení směrnice je zaměstnanci udělena sankce do výše 2 500 Kč sražená z pohyblivé části mzdy.

- **Směrnice o správě licencí softwarových produktů**

Navrhne: Bezpečnostní Manažer

Obsah: Navrhují, aby se směrnice zabývala následujícími body:

- Kontrola počtu licencí
- Specifikace funkce odpovědné za nákup SW – Stanovení pravidel nákupu.
- Specifikace funkce odpovědné za instalaci a aktualizaci SW
- Stanovení oprávnění uživatelům k instalaci SW – Podle jejich pozice, povolení instalace SW pouze administrátorům.
- Zavedení auditového SW - pro kontrolu nainstalovaných programů na všech stanicí z jednoho místa a pro odhalování pirátského SW.

Dohlíží: Ředitel IT

Platí pro: Administrátora, Uživatele

Sankce: Za porušení směrnice je zaměstnanci udělena sankce do výše 4 000 Kč sražená z pohyblivé části mzdy.

- **Pravidla práce s IT vybavením**

Navrhne: Bezpečnostní Manažer, Administrátor

Obsah: Ve směrnici jsou určena základní pravidla a povinnosti, která musí dodržovat všichni uživatelé při práci s výpočetní technikou.

Navrhuji, aby se směrnice věnovala obsahu následujících bodů:

- Řízení přístupu – Uživatelé se musí přihlašovat pouze pod svými uživatelskými jmény, nesmí do sítě zapojovat vlastní zařízení, nesmí poskytovat informace nepovolaným osobám, přidělené stanice smí využívat pouze k pracovním účelům.

- Použití softwaru – Uživatelé mají zakázáno měnit softwarové vybavení stanic, smějí používat pouze schválený software, nesmí používat nelegální software.
- Použití sítě Internet – Uživatelé mají zakázáno použití Internetu pro soukromé účely.
- Ochrana před škodlivým softwarem – Uživatelé pracují se svými stanicemi tak, aby minimalizovali riziko nakažení škodlivým softwarem.
- Používání elektronické pošty – Je nutno specifikovat dobu, po kterou jsou emaily dostupné, než se přesunou do archívu či jsou smazány. Dále je důležité omezit použití elektronické pošty pouze pro firemní účely a kvůli zatížení poštovních serverů specifikovat maximální velikost příloh. V případě nutnosti velkého přenosu dat je dále vhodné ve směrnici specifikovat jiné možnosti než elektronickou poštu. Může se jednat o přenosná média nebo zabezpečené firemní webové uložiště.

Dohlíží: Ředitel IT

Platí pro: Všechny zaměstnance

Sankce: Za porušení směrnice je zaměstnanci udělena sankce do výše 5 000 Kč nebo částka, odpovídající způsobené škodě.

- **Směrnice používání docházkového systému**

  Navrhne: Správce sítě, Hlavní personalista

  Obsah: Firma používá elektronický docházkový systém. Tento systém je ve formě aplikace, ke které se uživatel dostane až po přihlášení k pracovní stanici. Navrhuji, aby směrnice o jeho používání obsahovala tyto záležitosti:
  - Zákaz předávání uživatelských údajů mezi zaměstnanci – Aby nedocházelo k přihlašování zaměstnanců, kteří ještě nejsou v práci.
  - Nastavení oprávnění – Specifikace možností úpravy údajů v docházkovém systému nadřízeným zaměstnancem.
  - Specifikace termínů – Tzn. do kdy je možno docházku upravovat, než se odešle jako podklad ke zpracování mzdového vyúčtování.

  Dohlíží: Hlavní Personalista

Platí pro: Všechny zaměstnance

Sankce: Za porušení směrnice je zaměstnanci udělena sankce do výše 1 000 Kč sražená z pohyblivé části mzdy.

3.2.3 Krizové plány

Jsou to dokumenty, obsahující opatření a postupy k identifikaci a řešení krizové situace. Krizová situace má za následek použití mimořádných opatření, která se v běžné, provozu firmy nevyskytují.

- **Plán obnovy po havárii**

  Navrhne: Administrátor

  Obsah: Na vytvoření tohoto dokumentu se musí podílet všichni zástupci IT oddělení. Doporučuji tedy v plánu specifikovat postupy, akce a záložní řešení, které budou implementovány v případě následujících havárií a povedou k jejich rychlému odstranění:

  - Výpadek elektrické energie
  - Porucha záložního zdroje
  - Porucha klimatizace v serverové místnosti
  - Porucha serveru
  - Porucha telekomunikace
  - Nedostupnost připojení k internetu
  - Živelná pohroma – Povodeň, požár apod.

  Dohlíží: Bezpečnostní Manažer

  Platí pro: Správce sítě, administrátora

  Sankce: žádné

- **Plán činnosti po napadení IS**

  Navrhne: Administrátor

  Obsah: Navrhuji, aby plán zahrnoval tyto body:

  - Identifikaci hrozby
  - Operativní řešení
  - Analýzu útoku
  - Způsoby zabránění podobnému útoku v budoucnosti

  Dohlíží: Bezpečnostní Manažer

Platí pro: Správce sítě, administrátora

Sankce: žádné

3.2.4 Kontrola bezpečnostních opatření

Jelikož je prostředí firmy velice dynamické, není možné při tvorbě bezpečnostní politika uplatňovat přístup „vytvoř a zapomeň.“ Jak jsem již zmínil dříve, tvorba bezpečnostní politiky je kontinuální proces a aby účinně chránila firmu před hrozbami a riziky, musí se pravidelně revidovat.

- **Průběžná kontrola bezpečnosti**

  Navrhne: Administrátor

  Obsah: Doporučuji tuto průběžnou kontrolu provádět minimálně jednou za půl roku, aby mohla reflektovat aktuální změny a nové požadavky na bezpečnost ve firmě. Na základě výsledků této kontroly potom firma může přijmout nová, specifická protiopatření.

  Dohlíží: Bezpečnostní Manažer

  Platí pro: Správce sítě, administrátora

  Sankce: žádné

- **Školení uživatelů**

  Navrhne: Administrátor, hlavní personalista

  Obsah: Firma může mít sebedokonalejší bezpečnostní politiku, a přesto může dojít ke kompromitaci dat díky uživatelské nedbalosti či úmyslným zaviněním. Proto je důležité pravidelně pořádat školení uživatelů a zvyšovat tak jejich povědomí o bezpečnosti. Navrhuji, aby obsahem školení bylo zejména:

  - Pravidla pro používání internetu
  - Pravidla pro tvorbu silných hesel
  - Bezpečná práce s daty a jejich zálohování
  - Pravidla použití firemní elektronické pošty

  Dohlíží: Bezpečnostní Manažer

  Platí pro: všechny uživatele

  Sankce: žádné

3.3 Ekonomické zhodnocení návrhu

V této kapitole nastíním orientační finanční náročnost mnou navržených změn.

3.3.1 Zálohování

Navržená zálohovací mechanika stojí 195 500 Kč. Jelikož firma neustále nabírá nové zaměstnance a do budoucna plánuje vznik vlastního oddělení vývoje softwaru, stane se potřeba bezpečného uložení a zálohování dat nejvyšší prioritou. Z krátkodobého hlediska se může zdát, že investice je příliš velká, nicméně se zvyšujícím se množstvím dat v budoucnu firma nadbytečné kapacity ocení.

3.3.2 Čištění počítačů

Profylaxe neboli čištění počítačů od prachu je dobrý způsob prevence hardwarových selhání a často vede ke ztišení pracovní stanice a tím pádem k vyššímu uživatelskému komfortu. Toto čištění se provádí pomocí stlačeného vzduchu a cena jedné plechovky se pohybuje kolem 200 Kč. Pro všechny počítače ve firmě tak roční čištění vyjde na přibližně 3000 Kč.

3.3.3 Návrh a zavedení bezpečnostní politiky

Protože je firma součástí mezinárodní skupiny, doporučil bych, aby se na tvorbě bezpečnostní politiky podíleli nejen zaměstnanci, ale i odborníci z mateřské společnosti. Vzhledem k tomu, že mateřská společnost sídlí ve Velké Británii, započítal bych do nákladů na tvorbu bezpečnostní politiky výdaje na cestu a pobyt těchto expertů u nás. Dále bych do výdajů započítal náklady na školení uživatelů, bez kterého je nemožné zajistit účinné fungování bezpečnostní politiky. Celková částka kolem čtvrt milionu korun za zlepšení bezpečnosti se může zdát jako nepřiměřeně vysoká. Pravdou ovšem je, že v případě ztráty dat či útoky se škody šplhají do milionů korun a často působí ztrátu dobrého jméno, která se dá penězi vyčíslit jen těžko.

4 Závěr

Cílem této bakalářské práce bylo vytvoření návrhu bezpečnostní politiky. V první části jsem analyzoval současný stav zabezpečení výpočetní techniky v prostředí reálné mezinárodní firmy. Jelikož se jedná o nevýrobní podnik se zaměřením na služby, selhání technických prostředků či ztráta dat může mít fatální následky. Analýza bezpečnostní situace odhalila určité nedostatky, mající různou míru závažnosti. V teoretické části jsem vycházel z poznatků obsažených v literatuře a z bezpečnostních norem, podle kterých by měla být bezpečnostní politika tvořena. Na základě provedené analýzy a odhalený nedostatků jsem v poslední části nastínil jejich řešení a vytvořil návrhy bezpečnostních směrnice. Tyto směrnice po zavedení výrazně zvýší celkovou bezpečnost podnikových informací a tato bezpečnost potom může představovat důležitou konkurenční výhodu.

Seznam použité literatury

Knihy:

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

[2] HANÁČEK, P. a STAUDEK, J. *Bezpečnost informačních systémů: metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií.* 3., aktualiz. vyd. Praha: Úřad pro státní informační systém, 2000, 127 s. ISBN 80-238-5400-3.

[3] HONTANÓN, R. *Linux praktická bezpečnost*. 2003. ISBN 80-247-0652-0.

[4] HORÁK, J., KERŠLÁGER, M. *Počítačové sítě pro začínající správce*. 3., aktualiz. vyd. Brno: Computer Press, 2006, 211 s. ISBN 80-251-0892-9.

[5] KRČMÁŘ, P. *Linux*: *tipy a triky pro bezpečnost*. Praha: Grada, 2004, 207 s. ISBN 80-247-0812-4

[6] NORTHCUTT, S. *Bezpečnost počítačových sítí*. Brno: Computer Press, 2005, 589 s. ISBN 80-251-0697-7.

[7] PROSISE, C. *Počítačový útok*: *Detekce, obrana a okamžitá náprava*. Brno: Computer Press, 2002, 410 s. ISBN 80-722-6682-9

České technické normy

[8] ČSN 36 9786 – ČSN ISO/IEC 13335 1-4 – *Informační technologie – Směrnice pro řízení bezpečnosti IT.*

[9] ČSN 36 9789 – ČSN ISO/IEC 15408 1-3 – *Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT.*

[10] ČSN 36 9790 – ČSN ISO/IEC 17799 – *Informační technologie – Soubor postupů pro management bezpečnosti informací.*

Časopisy:

[11] DOUCEK, P. Bezpečnost IS/ICT a proces globální integrace. *AT&P Journal*. 2005, č. 1, s. 65 - 68. ISSN 1335-2237.

[12] DOUCEK, P. Budování systému řízení bezpečnosti IS/ICT. *AT&P Journal*. 2005, č. 2, s. 86 - 88. ISSN 1335-2237.

Elektronické zdroje:

[13] Typy organizačních struktur a jejich členění. In: Businessinfo.cz [online]. 2010 [cit. 2012-05-27]. Dostupné z: http://www.businessinfo.cz/cz/clanek/management-msp/typy-organizacnich-struktur-cleneni/1001663/59204/?page=1

[14] ISO/IEC 27001:2005 [online]. [cit. 2012-05-27]. Dostupné z http://www.rac.cz/rac/hompage.nsf/CZ/27001

[15] ISO/IEC 27002:2005 [online]. [cit. 2012-05-27]. Dostupné z http://www.rac.cz/rac/hompage.nsf/CZ/27002

Seznam použitých zkratek

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Systém
ERP	Enterprise Resource Planning
HSRP	Hot Standby Router Protocol
IEC	International Electrotechnical Commission
IPSEC	Internet Protocol Security
ISMS	Information Security Management System
ISO	International Organization for Standardization
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MPLS	Multiprotocol Label Switching
PDCA	Plan-Do-Check-Act
PHP	Hypertext Prepprocessor
PoE	Power over Ethernet
PPTP	Point-to-Point Tunneling Protocol
RAID	Redundant Array of Independent Disks
SQL	Structured Query Language
UPS	Uninterruptible Power Supply
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network

Seznam obrázků