VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

BAKALÁŘSKÁ PRÁCE

2011

MARTIN KOČÍ

VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

Nárožní 2600/9a, 158 00 Praha 5

BAKALÁŘSKÁ PRÁCE

KOMUNIKACE A LIDSKÉ ZDROJE

Vysoká škola ekonomie a managementu

+420 841 133 166 / info@vsem.cz / www.vsem.cz

VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

Nárožní 2600/9a, 158 00 Praha 5

NÁZEV BAKALÁŘSKÉ PRÁCE
Bezpečnost a nakládání s daty a elektronickými dokumenty v podniku

TERMÍN UKONČENÍ STUDIA A OBHAJOBA (MĚSÍC/ROK)
říjen/2011

JMÉNO A PŘÍJMENÍ / STUDIJNÍ SKUPINA
Martin Kočí KLZ2

JMÉNO VEDOUCÍHO BAKALÁŘSKÉ PRÁCE
Ing. Miroslav Lorenc

PROHLÁŠENÍ STUDENTA
Prohlašuji tímto, že jsem zadanou bakalářskou práci na uvedené téma vypracoval samostatně a že jsem ke zpracování této bakalářské práce použil pouze literární prameny v práci uvedené. Datum a místo: 29.08.2011 Praha _____ podpis studenta

PODĚKOVÁNÍ
Rád bych tímto poděkoval vedoucímu bakalářské práce za cenné rady a konzultace, které mi poskytl při zpracování mé bakalářské práce.

VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

Bezpečnost a nakládání s daty a elektronickými dokumenty v podniku

Safety and handling of data and electronics documents in enterprise

Autor: Martin Kočí

Souhrn

Tato práce se zabývá ochranou a bezpečností při nakládání s daty a elektronickými dokumenty v podniku. Data je nutno chránit proti ztrátě, zcizení, nebo zničení v důsledku živelných událostí a poruch hardwaru. Dále je nutno chránit data před neoprávněnou manipulací a zajistit, aby byla dostupná pouze oprávněným osobám. Ochrana dat se skládá ze čtyř základních oblastí, jimiž jsou přenášená data, uložená data, logický přístup k datům a fyzický přístup k datům. Každá z těchto oblastí ochrany dat je zajištěna jinými přístupy či technologiemi. Zatímco uložená data a fyzický přístup k nim jsou chráněna technickými prostředky, přenášená data a logický přístup k nim jsou chráněna softwarovými prostředky. Metody ochrany dat jsou zálohování, firewall, šifrování dat a antivirová ochrana dat. Zálohování dat je v době implementace nejnákladnější součástí ochrany dat, ovšem v případě závažné poruchy hardwaru nebo živelné události může zachránit existenci podniku. Ostatní metody ochrany dat slouží jako ochrana proti zcizení, případně zneužití dat. Podniky také musí dodržovat stanovené povinnosti, a to jak zákonné, tak i smluvní.

Summary

This work deals with the protection and safety in the handling of data and electronic documents in the company. The data must be protected against loss, theft or destruction due to natural disaster and hardware failures. It is necessary to protect data from tampering, and to ensure that accessible only to authorized persons. Data protection is composed of four basic areas, which are transmitted data, stored data, logical access and physical access to data. Each of these areas of data protection is ensured by other approaches or technologies. While the stored data and physical access to them are protected by physical means, the transmitted data and logical access are protected by software resources. Methods of data protection are backup, firewall, data encryption and antivirus protection of data. Data backup at the time of implementation is the costliest part of data protection, but in case of serious hardware failure or natural disaster can save the company´s survival. Other methods of data protection serve as a protection against theft or misuse of data. Companies also must comply with obligations, both statutory, and contractual.

Klíčová slova:

Ochrana dat, zálohování, firewall, šifrování, antivirus.

Keywords:

Data protection, backup, firewall, encryption, antivirus.

JEL Classification:

C800 – Data Collection and Data Estimation Methodology; Computer programs: General

C880 – Data Collection and Data Estimation Methodology; Computer programs: Other Computer Software

Obsah

Seznam zkratek

AES	Šifrovací standard (Advanced Encryption Standard)
CCTV	Uzavřený televizní okruh (Closed-circuit Television)
CD	Kompaktní disk (Compact disc)
DVD	Digitální univerzální disk (Digital Versatile Disc)
EKV	Elektronická kontrola vstupu
EPS	Elektrická požární signalizace
EZS	Elektronická zabezpečovací signalizace
HDD	Pevný disk (Hard Disc Drive)
IT	Informační technologie
NAS	Síťový disk (Network Attached Storage)
RAID	Diskové pole nezávislých disků (Redudant Array of Indipendent Disks)
SHZ	Stabilní hasicí zařízení
UPS	Nepřerušitelný zdroj napájení (Uninterruptible Power Suply)
USB	Univerzální sériová sběrnice (Universal Serial Bus)
VPN	Virtuální privátní síť (Virtual Private Network)

Seznam tabulek

Seznam obrázků

1 Úvod

Bakalářská práce se zabývá problematikou ochrany dat a dokumentů v podniku a nakládání s nimi. Protože jsou data a dokumenty jedním z nejcennějších produktů podniku, je nutné, aby si je každý podnik chránil odpovídajícím způsobem. Vzhledem k rozvoji informačních technologií a jejich použití prakticky v každém podniku je téma bezpečnosti dat velmi diskutované. Bohužel zdaleka ne všechny podniky dodržují alespoň základní bezpečnostní standardy a vystavují se tak, ať už vědomě či nevědomě, možné ztrátě či úniku dat. Dopady těchto ztrát nebo úniků mohou mít pro podnik, vlastníky podniku, nebo zodpovědné zaměstnance fatální následky.

Toto téma jsem si vybral, protože jsem se od roku 1995 profesně zabýval elektronickým zabezpečením objektů a nedílnou součástí této práce je bezpečnost jak přenášených, tak i uložených dat. V současné době působím v oblasti správy budov, kde je bezpečnost a ochrana dat jednou z klíčových součástí mojí práce. Během mojí praxe v oblasti zabezpečení a správy objektů jsem zjistil, že u mnoha subjektů nejsou data dostatečně chráněna proti zničení přírodními živly či poruše hardwaru. Ještě horší situace je však v oblasti zabezpečení dat a dokumentů proti ztrátě, zaviněné neúmyslně, nebo zcizením těchto dat.

Cílem této práce je zhodnotit stav ochrany dat a nakládání s nimi v konkrétním podniku a na základě zjištěných skutečností se pokusit navrhnout vhodná řešení, která by mohla přispět k větší bezpečnosti dat a elektronických dokumentů. Dalším cílem této práce je popsat možnosti a používané metody ochrany dat tak, aby informace mohly být využity pro zlepšení ochrany dat i v dalších podnicích.

Práce se bude snažit najít odpověď na otázky, zda je podnik dostatečně vybaven technologiemi pro ochranu dat, zda dodržuje potřebné standardy a pracovní postupy při ukládání a přenosu dat, a zda je zajištěna důvěryhodnost podniku v oblasti ochrany dat při jejich zajištění proti zničení či ztrátě.

Teoretická část práce se zaměřuje na popis a definici ochrany dat, popisuje metody ochrany dat. Dále popisuje některé metody, které jsou vhodné k ochraně dat. Na závěr

popisuje povinnosti podniku, které jsou stanovené právními předpisy v oblasti ochrany dat.

Praktická část se již zaměřuje na vybranou společnost, kde jsou uvedeny základní informace o podniku, organizační struktura a zaměření podniku. Dále popisuje vybavení podniku v oblasti ochrany dat, použité metody a postupy. Velká pozornost je dále věnována konkrétním návrhům na zlepšení ochrany dat, a to včetně cenové kalkulace navrhovaných řešení.

2 Teoreticko-metodologická část práce

2.1 Vymezení problematiky ochrany dat a nakládání s nimi

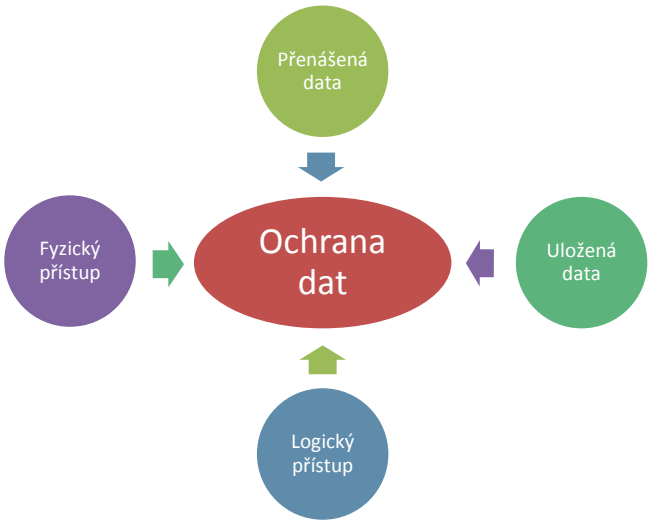
Zpracování informací pomocí informačních technologií lze charakterizovat jako uchovávání, přenos a vyhodnocování informací. V dnešní době se pomocí informačních technologií zpracovává stále větší množství informací. Tyto informace mají často velkou ekonomickou hodnotu, historickou hodnotu, nebo jsou důvěrné.

2.1.1 Ochrana dat

Pojem „ochrana dat“ znamená nejen ochránit data a dokumenty tak, aby byla dostupná pouze oprávněným osobám a zůstala důvěrná, ale také ochránit je proti ztrátě.

„Ne všechna data by měla být přístupná všem lidem, některá data by měla být obzvláště chráněna proti neoprávněné modifikaci, jiná proti zničení. S klidným svědomím tedy můžeme říci, že ke každým datům je z hlediska jejich ochrany nutno přistupovat zcela individuálně.“[1]

Obrázek 1 Ochrana dat



Zdroj: DOSEDĚL, T. (2004). *Počítačová bezpečnost a ochrana dat.* Brno: Computer press, str. 6

[1] DOSEDĚL, T. (2004). *Počítačová bezpečnost a ochrana dat.* Brno: Computer press, str. 47

Z obrázku 1 vyplývá, že se ochrana dat skládá ze čtyř oblastí, které se vzájemně prolínají.

2.1.1.1 Fyzický přístup k datům

Data, uložená na jakémkoli médiu, musejí být fyzicky ochráněna nejen proti neoprávněné manipulaci, ale také proti poškození přírodními vlivy.

Ochrana proti **neoprávněné manipulaci** je zajišťována uložením těchto médií (datové servery, diskové pole, CD/DVD disky, páskové kazety, HDD disky atd.) v prostorech s omezeným přístupem. Tyto prostory jsou chráněny proti neoprávněnému přístupu elektronickou kontrolou vstupu (EKV), elektronickou zabezpečovací signalizací (EZS), kamerovým systémem (CCTV), bezpečnostními dveřmi, bezpečnostními zámky, umístěním v budově a v neposlední řadě i fyzickou ostrahou.

Ochrana dat před poškozením **přírodními vlivy**, zejména požárem, vodou nebo sluncem, je zajištěna kombinací elektrické požární signalizace (EPS), vhodného stabilního hasicího zařízení (SHZ) a umístěním v budově.

V neposlední řadě je také nutno chránit systémy uchovávající data před **ztrátou napájení**, případně také před jeho špatnou kvalitou, a to pomocí záložního napájení (UPS).

Přes veškerou snahu ochránit data před uvedenými možnostmi ztráty či poškození dat je vždy zcela základní ochrana spočívající v **systematickém zálohování dat**. Metody, používané při zálohování, jsou popsány v dalším textu.

2.1.1.2 Logický přístup k datům

Logický přístup k datům je zajišťován operačním systémem. Základní ochrana dat proti **neoprávněnému přístupu** je zajišťována nastavením přístupových práv v operačním systému jednotlivým uživatelům podle jejich oprávnění. Pro zajištění vysoké bezpečnosti se používají hesla o délce alespoň 8 znaků, složená z velkých písmen, malých písmen, čísel a speciálních znaků (+, -, /, ř, atd.). Při použití složení takového hesla je předpokládaná doba jeho prolomení v řádech stovek let. V některých informačních systémech je také nastavena nutnost změny hesla po stanovené době,

výjimkou není ani nemožnost použití stejného hesla v určitém období a uživatelé musí mít během jednoho roku 12 různých hesel.

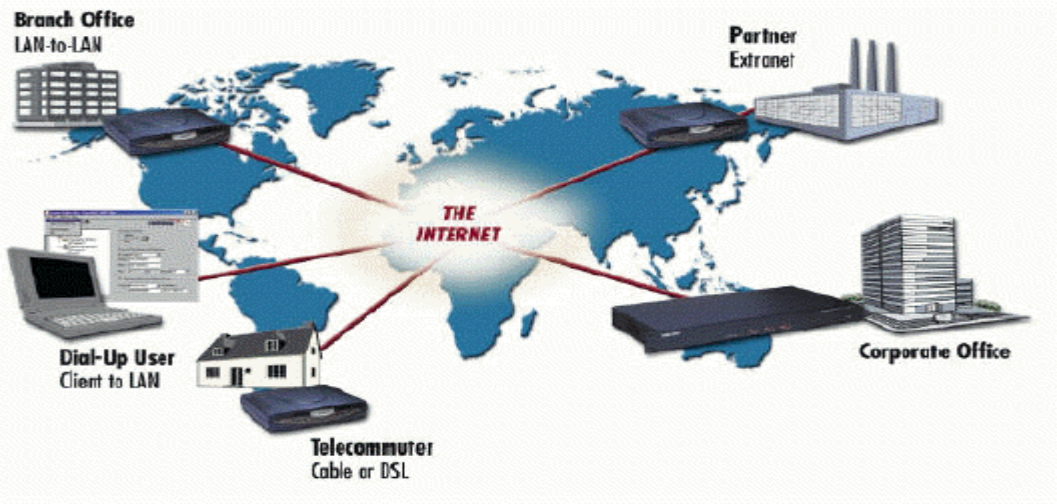
2.1.1.3 Uložená data

Při provozu informačního systému je nutno počítat s tím, že ne všichni uživatelé budou dodržovat všechny stanovené postupy, týkající se hesel a přístupu do operačního systému. Taktéž není doporučeno spoléhat se absolutně na zabezpečení dat proti odcizení datových nosičů. Pro tyto případy se uložená data chrání pomocí šifrovacích prostředků, při jejichž použití se data bez znalosti šifrovacího klíče nedají zobrazit či přečíst.

2.1.1.4 Přenášená data

Podobným způsobem, jako jsou ochráněna uložená data, musejí být ochráněna jak data přenášená v počítačové síti, tak data na přenosných médiích či počítačích. Nejpoužívanější metodou ochrany přenášených dat v síti internet je **virtuální privátní síť** (VPN), která zajišťuje pomocí zabezpečeného tunelu spojení uživatele s firemní počítačovou sítí, a to při přenosu dat přes nedůvěryhodnou síť - veřejný internet, viz obrázek 2.

Obrázek 2 Virtuální privátní síť



Zdroj: VPN Technology [online]. [cit. 2011-07-31]. Dostupné z WWW: http://www.vpn-technology.com/

Podniková síť se proti nepovolenému přístupu z internetu chrání pomocí **firewallu**, který odděluje provoz mezi dvěma sítěmi a propustí dovnitř a ven pouze data, která jsou přesně definovaná. Princip funkce firewallu je popsán dále v textu. Data přenášená na datových médiích, případně na přenosných počítačích, jsou nejčastěji chráněna šifrováním. Taktéž principy šifrování jsou popsány dále v textu.

2.1.1.5 Vytvoření bezpečnostní politiky

Aby bylo možné řešit výše uvedené postupy koncepčně, musí být organizací vytvořena bezpečnostní politika, která definuje, zjednodušeně řečeno, jaká data nebo zařízení ochránit, jakým způsobem se budou chránit a také proti jakým hrozbám je nutno je chránit. V návaznosti na bezpečnostní politiku je nutno definovat zásady zabezpečení. *„Zásady zabezpečení představují komplexní rámec prevence, detekce a reakce na bezpečnostní hrozby. Pokrývají logické a fyzické zabezpečení, ochranu osobních údajů a důvěrných informací a rovněž zákonné nároky kladené na vaši firmu. Určují také úlohy a odpovědnost správců, uživatelů a poskytovatelů služeb.“*[2] Mezi základní kroky pro vytvoření zásad zabezpečení patří:

- inventura veškeré IT techniky včetně softwaru, dat a databází;
- dokumentace a označení všech zařízení, která jsou pro organizaci kritická;
- důkladná analýza těchto zařízení, včetně infrastruktury;
- zvážení zjištěných rizik a potenciálních zranitelných míst;
- stanovení priorit a vytvoření zásad zabezpečení, která budou vycházet z analýzy zjištěných rizik.

Posledním, avšak nejtěžším krokem, je samotná realizace bezpečnostní politiky. Zatímco přínos bezpečnostní politiky je patrný až za relativně dlouhou dobu a pro některé zaměstnance není pozorovatelný nikdy, „otravná“ a „zdržující“ opatření jsou viditelná ihned a proto je úkol nelehký. Management organizace proto musí dobře komunikovat se zaměstnanci nutnost těchto opatření.

---

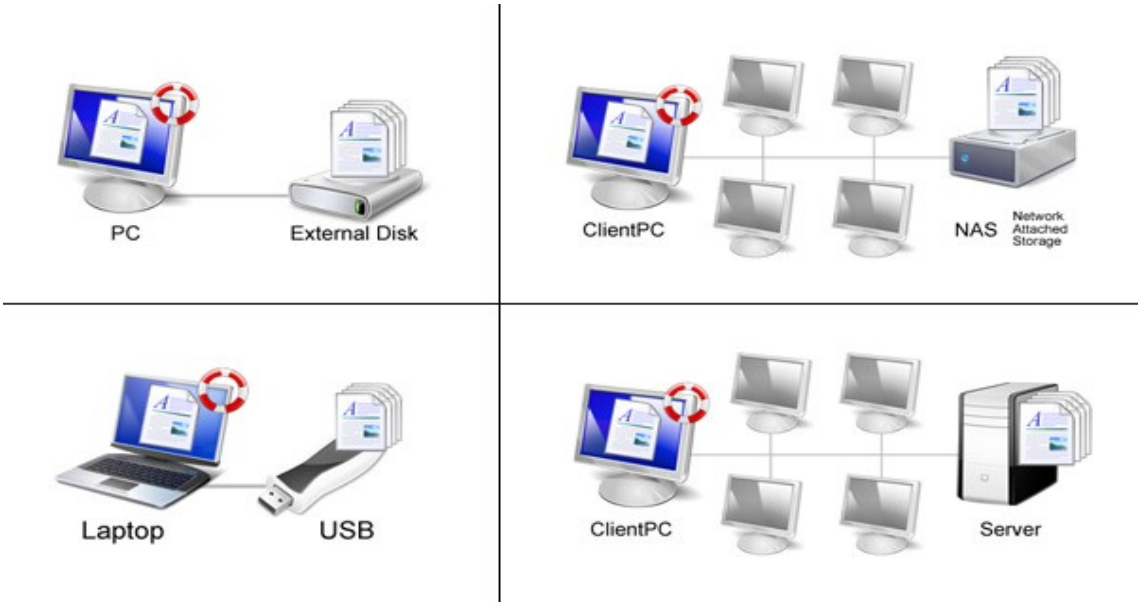
[2]Zdroj: Lustyk, P., Security World [online]. [cit. 2011-07-31]. Dostupné z WWW: http://securityworld.cz/securityworld/zakladna-efektivni-a-ucinne-spravy-zabezpeceni-it-1136

2.2 Metody ochrany dat

2.2.1 Zálohování dat

„Zálohování je mechanismus, při kterém jsou data (nemusí to být tedy všechna) ukládána na jiné médium. V případě zničení původního média jsou data obnovena ze zálohy. Z uvedeného vyplývá, že při jakékoliv obnově vždy část dat ztratíme – minimálně ta, která byla vytvořena od posledního zálohování.[3]

Obrázek 3 Zálohování dat



Zdroj: SuggestSoft [online]. [cit. 2011-07-31]. Dostupné z WWW: http://www.suggestsoft.com/soft/infonautics-gmbh/live-file-backup/

V případě havárie datového serveru nebo pevného disku, zničení dat viry nebo v důsledku živlu, případně ztráta dat zaviněná uživatelskými omyly, přichází na řadu potřeba obnovy dat ze zálohy. Každá zodpovědná organizace či domácí uživatel pravidelně svá data zálohuje, v ideálním případě pravidelně kontroluje funkčnost obnovy dat ze zálohy.

[3] DOSEDĚL, T. (2004). *Počítačová bezpečnost a ochrana dat.* Brno: Computer press, str. 61

Metody zálohy dat jsou:

- **úplná záloha dat**, při které jsou zálohována všechna zvolená data bez ohledu na to, zda již v minulosti byla zálohována. Výhodou tohoto typu zálohy je samostatnost každé zálohy a snazší obnova dat, velkou nevýhodou je však jak časová, tak datová náročnost;
- **rozdílová záloha dat**, při které se provede nejprve úplná záloha dat, a následně se zálohují pouze změny, které proběhly od této úplné zálohy. Výhodou je podstatně menší časová i datová náročnost, která ale s postupem času přibývá;
- **přírůstková záloha dat**, při které se opět nejprve realizuje úplná záloha dat a následně se zálohují pouze změněná data oproti předchozí záloze, a to bez ohledu na to, zda šlo o úplnou či přírůstkovou zálohu. Výhodou přírůstkové zálohy dat je časová i datová nenáročnost, nevýhodou je způsob obnovy, který spočívá v obnovení úplné zálohy i všech přírůstků.

Dále je nutno rozhodnout, na jaká zálohovací média budou zálohy prováděny. Při rozhodování jsou zvažována následující kritéria:

- **rychlost záznamu, vyhledávací doba a přenosová rychlost** – jde o klíčové údaje, na kterých závisí nejen doba strávená zálohováním, ale také čas potřebný k obnovení dat ze zálohy;
- **střední doba mezi poruchami** – jde o průměrnou životnost jak zálohovacího zařízení, tak o životnost médií - jedná se o velmi důležitý údaj;
- **cena médií** – zahrnuje jak cenu pořízení samotného zálohovacího zařízení, tak i cenu za 1 MB zálohovaných dat, případně cenu za správu zálohování.

Po stanovení výše uvedených kritérií přichází na řadu výběr technologie zálohování. V současné době jsou na výběr tyto možnosti:

- **páskové zálohovací systémy** – nejpoužívanější technologie zálohování větších objemů dat. Výhodou je velmi vysoká kapacita, přenosová rychlost a cena za 1 MB, nevýhodou je vyšší přístupová doba a zejména náklady na pořízení;
- **diskové zálohovací systémy** – výhodou je vysoká kapacita, přenosová rychlost, přístupová doba a snadná připojitelnost v případě externích disků. Mezi diskové

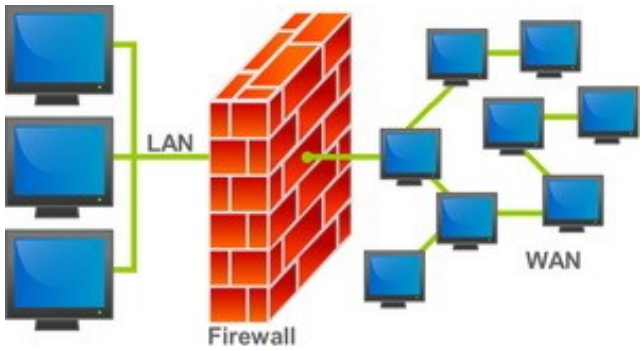
zálohovací systémy řadíme i v poslední době oblíbené a cenově dostupné síťové disky (NAS – Network Attached Storage), které jsou pro funkci zálohování kompletně vybaveny včetně softwaru;

- **optické zálohovací systémy** – jedná se zejména o velmi rozšířené zálohování na disky CD, DVD a v současné době i Blu-Ray disky. Velkou výhodou jsou jak náklady na pořízení zálohovacího zařízení i disků, tak i rozšířené optické mechaniky schopné přehrávání těchto disků. Další výhodou je velmi dobrá použitelnost optických médií pro potřeby archivace. Nevýhodou je však nízká kapacita, přenosová rychlost i přístupová doba;
- **on-line záložní služby** – jde o zálohování na vzdálený diskový prostor, pronajatý od poskytovatele této služby. Výhodou je garantovaná dostupnost dat, dostupnost dat odkudkoli přes internetové připojení a přenesení provozování na poskytovatele. Nevýhodou je nízká kapacita, přenosová rychlost (zejména při zálohování) a nutnost šifrování některých dat;
- **paměťové karty a USB flash disky** – jsou vzhledem ke svojí velikosti, přenositelnosti i relativně nízké kapacitě určeny spíše pro osobní použití, nejčastěji pro zálohu dokumentů.

2.2.2 Firewall

„Firewall je hardwarový a softwarový prostředek s vlastní bezpečnostní politikou, autentizačními mechanismy, aplikační bránou (branami) a filtrem (filtry) paketů, který logicky a fyzicky odděluje bezpečnou síť, resp. důvěryhodnou síť (zpravidla lokální síť organizace) od nezabezpečené, nedůvěryhodné sítě.“[4]

Obrázek 4 Firewall



Zdroj: My Security Software [online]. [cit. 2011-07-31]. Dostupné z WWW: http://www.my-security-software.com/top-five-best-firewall/

Firewall může oddělovat od nedůvěryhodné sítě (internet) celou síť, ať už domácí nebo podnikovou – v tom případě se jedná o **hardwarový firewall**, nebo samostatný počítač – v tomto případě jde o **osobní firewall.**

2.2.2.1 Hardwarový firewall

Hardwarový firewall je samostatné síťové zařízení, které má vlastní softwarové vybavení a jeho úkolem je kontrola komunikace mezi vnitřní a vnější sítí podle pravidel definovaných administrátorem. Může se jednat o samostatný počítač, dnes se nejčastěji používá firewall jako součást routeru. Podle typu kontroly komunikace rozlišujeme tyto firewally:

- **paketový filtr** – nejstarší a nejjednodušší technologie, která je založena na pravidlech, která přesně udávají, ze které IP adresy, protokolu a portu budou

[4] Zdroj: Gála, L., Pour, J., Šedivá, z., (2009) *Podniková informatika 2., přepracované a aktualizované vydání.* Praha: Grada publishing, str. 350

příchozí pakety propuštěny, nebo zamítnuty. V případě zamítnutí je možnost zaslat odesílateli zprávu o zamítnutí. Paketový filtr pracuje na síťové (třetí) vrstvě;

- **stavový paketový filtr** – vylepšený a rozšířený paketový filtr, který si ukládá již povolená spojení, což zrychluje komunikaci a umožňuje snadněji definovat pravidla komunikace. Stavový firewall pracuje na druhé až páté vrstvě;
- **stavový paketový filtr s kontrolou protokolů** – nejmodernější varianta paketového filtru, který kompletně analyzuje obsah komunikace a obsahuje i systém pro detekci útoků. Výhodou těchto firewallů je vysoký stupeň zabezpečení, nevýhodou je však cena i vyšší nároky na znalosti administrátora. Tento typ firewallu pracuje na druhé až sedmé vrstvě ISO/OSI modelu;
- **aplikační brána** – firewall zvaný také jako proxy firewall se dnes používá jen ve specializovaných řešeních, důvodem je náročnost na hardware a relativně velké zpoždění komunikace.

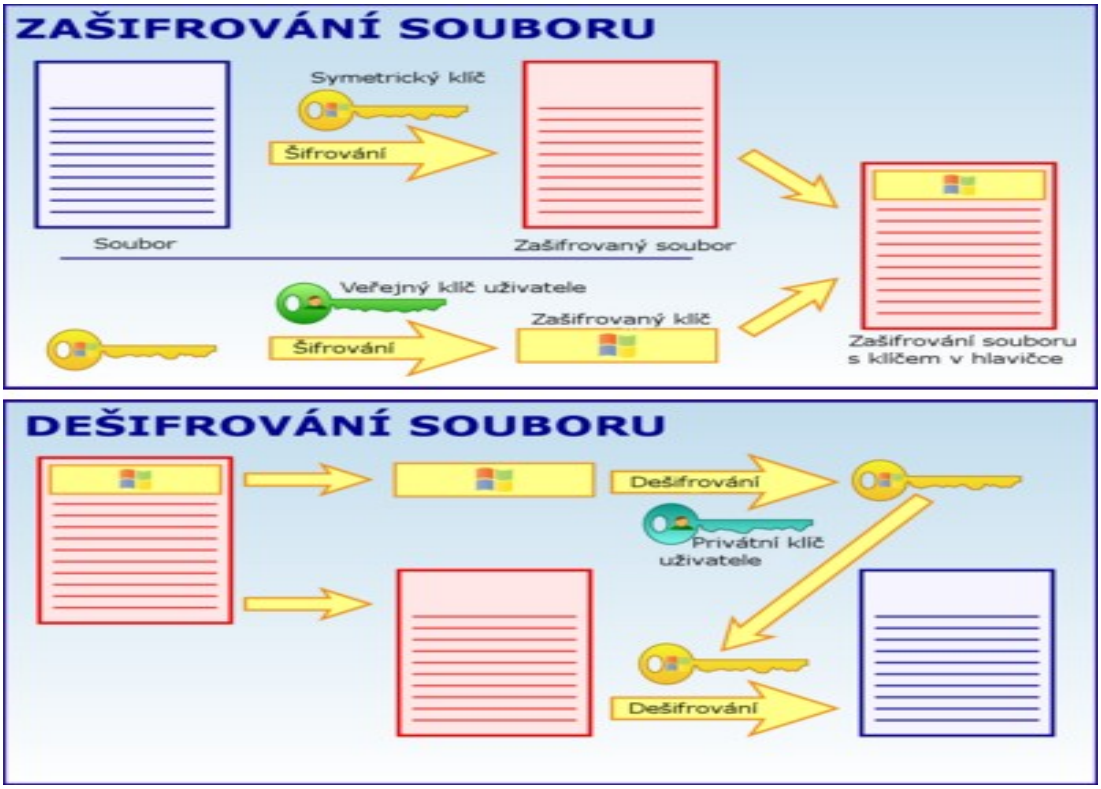
2.2.2.2 Osobní firewall

Osobní firewall, nazývaný také personální firewall, je softwarový firewall určený k ochraně jednoho počítače a je v něm nainstalován. Osobní firewall zaznamenává a řídí kompletní síťový provoz, některé mohou řídit i spuštěné lokální procesy a bránit tím spouštění programů bez vědomí uživatele. Osobní firewall se masově rozšířil díky operačnímu systému Microsoft Windows, jehož součástí je od verze Windows XP. Velkou výhodou je cena, která je nulová u integrovaných firewallů, cenově dostupné pro každého uživatele jsou však i komerční osobní firewally. Jistou nevýhodou je to, že nastavení osobního firewallu provádějí uživatelé bez znalosti síťové komunikace a mohou snadno prakticky vyřadit důležité funkce firewallu.

2.2.3 Šifrování dat

V dnešní době je k dispozici velký výběr softwarových nástrojů na šifrování dat. Podle potřeb uživatele nebo administrátora lze volit mezi symetrickým šifrováním, asymetrickým šifrováním, silnými hesly v archivech RAR nebo skrytím dat. K dispozici jsou jak komerční produkty za poplatek nebo zdarma, tak i šifrování dat jako součást operačního systému.

Obrázek 5 Šifrování dat



Zdroj: Wikipedie [online]. [cit. 2011-07-31]. Dostupné z WWW: http://cs.wikipedia.org/wiki/Encrypting_File_System

2.2.3.1 Šifrování souborů

Tato šifrovací metoda se používá pro šifrování souborů, složek, výměnných médií, částí pevných disků a emailových zpráv. Šifrování souborů je možno realizovat následujícími dvěma způsoby:

- **šifrování vybraných souborů** – šifrovací software zašifruje uživatelem vybrané soubory nebo složky. V tomto případě se jedná o offline šifrování dat a záleží vždy na uživateli, jak často a jaké soubory budou šifrovány;
- **šifrování všech souborů** – šifrovací software, který je nainstalován do operačního systému a je trvale spuštěn, automaticky šifruje všechny soubory, které splňují kritéria nastavená uživatelem. Jedná se o online šifrování dat a vše probíhá automaticky již bez zásahu uživatele.[5]

2.2.3.2 Šifrování disku

Tato metoda se používá pro šifrování pevného disku jako celku, kdy se šifruje celý disk včetně zaváděcího oddílu a odpadá tak volba, které soubory se budou šifrovat. Šifrování dat zajišťuje v operačním systému nainstalovaný ovladač. Nevýhodou je celkové zpomalení výpočetního výkonu, protože šifrování probíhá pro všechna data v reálném čase.[6]

2.2.3.3 Symetrické a asymetrické šifrování

Symetrické šifrování dat je původní metoda, založená na šifrování i dešifrování pomocí sdíleného klíče. Šifrované zprávy se zašifrují i dešifrují pomocí stejného klíče, který si komunikující uživatelé vhodnou cestou smluví. V případě komunikace mezi dvěma uživateli jsou potřeba dva klíče, při větším počtu komunikujících uživatelů však nutný počet klíčů neúměrně roste. Vzhledem k problémům, které s sebou nese správa velkého množství takových klíčů, byla vyvinuta metoda **asymetrického šifrování** dat. Tato metoda je založená na vytvoření veřejného a soukromého klíče pro každého uživatele. Zasílaná zpráva je zašifrována veřejným klíčem uživatele, který je příjemcem zprávy, dešifrovat takovou zprávu je možno pouze soukromým klíčem příjemce.

[5] DOSEDĚL, T. (2004). *Počítačová bezpečnost a ochrana dat.* Brno: Computer press, str. 58

[6] DOSEDĚL, T. (2004). *Počítačová bezpečnost a ochrana dat.* Brno: Computer press, str. 59

V případě asymetrického šifrování dat je počet klíčů dvojnásobkem počtu komunikujících uživatelů.

2.2.4 Antivirová ochrana

Antivirová ochrana počítače je zajišťována antivirovým programem. Antivirový program je software, jehož funkcí je detekce, odstraňování a eliminace škodlivých kódů, označovaných jako **počítačový virus, malware a spyware**. Některé antivirové programy detekují a eliminují jak virus a malware, tak i spyware, k některým je však nutno vybavit počítač samostatným programem na boj proti spywaru, tzv. **anti-spyware.**

Škodlivý kód může útočník do počítače umístit například pomocí přílohy k emailové zprávě, umístěním kódu k různým programům, které se stahují a instalují z nedůvěryhodných zdrojů, případně pomocí spustitelné komponenty na webové stránce. Vzhledem k tomu, že se tyto škodlivé kódy umějí šířit mezi počítači bez vědomí uživatelů, je možné se infikovat i od důvěryhodného zdroje, pokud není používán pravidelně aktualizovaný software.

Antivirový software je možno pořídit ve dvou různých variantách:

- **antivirus zdarma** – antivirový software, jehož používání není zpoplatněno a je volně šiřitelný. Aktualizace programu je nabízena také zdarma. Obvykle je jeho používání omezeno na domácí použití, což uživatel potvrzuje v licenční smlouvě při instalaci programu. Některé tyto antiviry neobsahují ochranu proti spywaru a je nutno ji zajistit jiným programem;
- **antivirus za poplatek** – antivirový software tohoto typu je založen na stejné koncepci jako většina jiných programů a je nutno za něj zaplatit. Obvyklá praxe je taková, že po zakoupení programu jsou aktualizace poskytovány zdarma jeden rok a poté je nutno si zakoupit buď aktualizace na další rok, nebo celý software v nové verzi, předplacený opět na rok.

Antivirový software je možno instalovat jak na přenosné či stolní počítače, tak i na podnikové servery. Při větším počtu instalací antivirového softwaru je možnost

centrální správy všech instalací, což významně usnadňuje nastavování a aktualizování jednotlivých instalací.

2.3 Povinnosti podniku při nakládání s citlivými daty a dokumenty

2.3.1 Zákonné povinnosti

Společnost musí dodržovat především zákonné povinnosti při nakládání jak s vlastními daty a dokumenty, tak i s daty a dokumenty svých zákazníků. Jedná se zejména o tyto právní předpisy:

- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 1. ledna 2011;
- Zákon č. 227/2000 Sb., o elektronickém podpisu;
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, (dále jen „zákon o ochraně utajovaných informací“);
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů.

2.3.2 Smluvní povinnosti

Každá společnost musí v souvislosti se zpracováváním dat dodržovat kromě zákonných povinností také povinnosti vyplývající ze smlouvy se svými obchodními partnery. Jedná se zejména o smlouvy, dodatky, obchodní transakce a další záležitosti, které je možno považovat za obchodní tajemství. V případě podniků, dodávajících provozní a bezpečnostní technologie, musí tyto podniky dodržovat určité bezpečnostní standardy, aby zamezily jakémukoli prozrazení a zneužití souvisejících dat.

3 Praktická část práce

3.1 Popis společnosti

3.1.1 Základní údaje o společnosti

Obrázek 6 Logo společnosti

Zdroj: Alsig [online]. [cit. 2011-07-31]. Dostupné z WWW: http://www.alsig.cz/

Název společnosti: ALSIG, spol. s r.o.

Právní forma společnosti: společnost s ručením omezeným

Sídlo společnosti: Praha 5, Holečkova 31, PSČ 150 00

Provozovny:

hlavní provozovna Praha: Praha 3, Na Jarově 4

provozovna Brno: Brno, Olomoucká 1158/164a, okres Brno-město

Počet zaměstnanců: 40

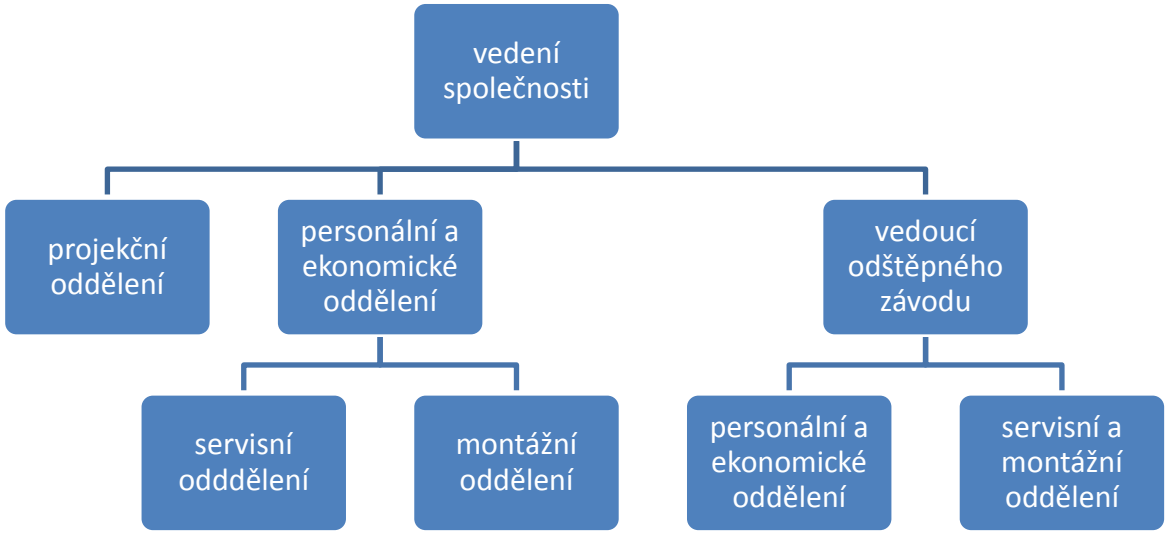
3.1.2 Předmět podnikání

Mezi hlavní činnosti společnosti patří poskytování komplexních služeb v oblasti slaboproudých systémů. Společnost se od založení v roce 1991 specializuje především na elektronickou ochranu budov proti vloupání (systémy EZS), požární signalizaci (EPS), elektronickou kontrolu vstupu (EKV), kamerové systémy (CCTV). Společnost

zajišťuje kompletní služby po celou dobu životnosti instalace systému – od projektové dokumentace, přes dodávku a montáž systému, až po záruční a pozáruční servis ve formě 24/7.

3.1.3 Organizační struktura společnosti

Obrázek 7 Organizační struktura podniku



Zdroj: Vlastní konstrukce na základě údajů a informací společnosti

V dalším textu se práce zabývá pouze technologiemi používanými v hlavní provozovně v Praze.

3.1.4 Zákazníci společnosti

Vzhledem k charakteru nabízených služeb, získaným certifikátům v oblasti zabezpečení a dobrému jménu, se mezi zákazníky řadí:

- **bankovní sektor** – Česká spořitelna, a.s., Česká pojišťovna, a.s., Československá obchodní banka, a.s., Komerční banka, a.s., GE Money bank, a.s., Kooperativa pojišťovna, a.s., Raiffeisenbank, a.s.;

- **dopravní sektor** – Dopravní podnik hl. m. Prahy, a. s., Letiště Praha, a.s. České dráhy, a.s.;
- **státní sektor** – Armáda České republiky, Policie České republiky, Ministerstvo vnitra České republiky, Správa státních hmotných rezerv, 24. základna dopravního letectva Praha – Kbely;
- **kulturní sektor** – Národní technické muzeum v Praze, Náprstkovo muzeum asijských, afrických a amerických kultur, Arcibiskupství pražské.

Mezi další významné zákazníky se řadí VŠE v Praze, Mezinárodní škola Nebušice, řetězce supermarketů Ahold, Interspar a Kaufland.

V neposlední řadě je to mnoho dalších subjektů, včetně soukromých.

3.2 Zjištění současného stavu zabezpečení dat a dokumentů

3.2.1 Zabezpečení uložených dat

3.2.1.1 Přístup k datům

Přístup k datům, uloženým na podnikovém serveru, je omezen pouze pro osoby oprávněné s těmito daty manipulovat. Jsou oddělena provozní podniková data od dat zákaznických a přístup k serveru je povolen pouze autorizovaným zařízením, které přiřadí administrátor. Z důvodu ochrany dat je vzdálený přístup omezen a přistupovat lze pouze z vnitřní sítě, která je výhradně metalická a připojení do sítě je opět povoleno pouze autorizovaným zařízením a pracovníkům.

3.2.1.2 Zálohování dat

Zálohování podnikových dat a dokumentů je zajišťováno automaticky zálohovacím softwarem **Backup & Recovery 10 Advanced Server** od firmy Acronis na centrální datový server, na kterém je pro účely zálohování vyhrazena část diskového pole RAID 5. Vzhledem k relativně malému objemu dat se provádí následná archivace dat na optické disky.

Zálohování zákaznických dat je prováděno výhradně na zašifrovaná média, která jsou uložena v trezoru. V případě nepotřebnosti těchto dat jsou data skartována v souladu se zákonem o ochraně utajovaných informací.

3.2.2 Zabezpečení přenášených dat

Přenášení dat v podniku je realizováno jednak na datových nosičích, jako jsou flash disky, optické CD/DVD disky nebo přenosné pevné disky, tak i ve formě uložených dat v pracovních přenosných počítačích. Zabezpečení dat na jednotlivých nosičích je zajišťováno těmito metodami:

- **flash disky** – pro zálohu a přenos běžných dat a dokumentů jsou používány běžné flash disky bez funkcí šifrování. Naopak pro přenos citlivých dat jsou používány výhradně flash disky se zabudovanou funkcí pro hardwarové šifrování s 256bitovým klíčem, včetně smazání dat po nastaveném počtu vložení nesprávného hesla;
- **optické CD/DVD disky** – přenos dat na těchto nosičích je používán výhradně pro obrazové výstupy a jejich zálohu. Všechna data jsou jak šifrována, tak jsou spustitelná pouze na specializovaném softwaru a jsou tedy pro běžného uživatele zcela nečitelná;
- **přenosné pevné disky** – tyto datové nosiče jsou využívány k zálohám počítačů. Jsou využívány disky s hardwarovým šifrováním 256bit AES, nebo 192bit triple DES;
- **pracovní přenosné počítače** – zabezpečení dat na přenosných počítačích je zajišťováno kombinací silného hesla pro přístup do operačního systému, integrovanou čtečkou otisku prstů a USB hardwarovým klíčem.

Starší přenosné počítače, nevybavené moderními bezpečnostními technologiemi, se postupně přeřazují na domácí či osobní využití.

V případě poruchy jakéhokoliv datového nosiče a nemožnosti obnovy dat vlastními podnikovými prostředky se používá, možná nemoderní, avšak velmi účinná metoda zničení dat – úplné rozebrání a následné fyzické zničení paměťových čipů nebo ploten pevných disků.

3.3 Požadavky na důvěryhodnost zaměstnanců, kteří přicházejí do styku s citlivými daty

3.3.1 Bezúhonnost zaměstnanců

Vzhledem k zaměření podniku na elektronické zabezpečení objektů je po všech zaměstnancích vyžadováno, aby byli trestně bezúhonní. Záznam v trestním rejstříku uchazeče o zaměstnání v podniku je významným hlediskem při rozhodování o přijetí. Předložení výpisu z trestního rejstříku je dále vyžadováno každé 3 roky.

3.3.2 Bezpečnostní prověření zaměstnanců

Některé státní instituce vyžadují po svých dodavatelských firmách, aby tyto firmy disponovaly osvědčením, které jim bude umožňovat přístup k utajovaným informacím podle zákona o ochraně utajovaných informací.

Zaměstnanci, kteří přicházejí do styku s utajovanými informacemi dle uvedeného zákona, jsou pravidelně prověřováni Národním bezpečnostním úřadem. Toto prověření je zárukou důvěryhodnosti jak zaměstnanců, tak podniku.

3.3.3 Spolehlivost zaměstnanců

Nedílnou součástí pracovních povinností je spolehlivost zaměstnanců. Nejedná se pouze o spolehlivost v rámci běžné pracovní kázně, ale především o dodržování bezpečnostních zásad pro používání všech technických prostředků během plnění pracovních úkolů, zejména těmi zaměstnanci, kteří provádějí činnosti mimo provozovnu podniku. Vedoucí zaměstnanci zajišťují pravidelná školení a následnou kontrolu dodržování bezpečnostních zásad.

3.4 Analýza zjištěných skutečností

3.4.1 Zabezpečení uložených dat

3.4.1.1 Nasazení antivirového softwaru

Antivirový software je nainstalován na všech přenosných počítačích, na pracovních stanicích a také na poštovním serveru. Software obsahuje ochranu proti virům, spywaru a mallwaru. Antivirový software nainstalovaný na přenosných počítačích je od společnosti Avast, antivirový software nainstalovaný na pracovních stanicích a na poštovním serveru je od společnosti Symantec.

3.4.1.2 Zálohování dat

Zálohování dat je realizováno zmiňovaným zálohovacím softwarem Acronis Backup & Recovery 10 Advanced Server. Zálohují se pouze data uložená na serveru a to na část diskového pole s technologií RAID 5.

Zálohování dat na pracovních stanicích, stejně jako zálohování dat na přenosných počítačích, není v podniku řešeno. Z těchto počítačů se provádí záloha pouze těch dat, která umístí na server přímo uživatelé.

3.4.1.3 Fyzická ochrana dat

Prostor, kde je umístěn centrální datový server, je chráněn umístěním, což do značné míry snižuje riziko poškození přírodními vlivy, zejména povodní. Prostor je také chráněn elektronickou zabezpečovací signalizací, elektronickou kontrolou vstupu, kamerovým systémem a elektrickou požární signalizací. Prostor je také umístěn v budově s trvalou ostrahou objektu.

Centrální server je chráněn proti výpadku elektrické energie nepřerušitelným zdrojem napájení. Ochrana proti výpadku elektrické energie na pracovních stanicích není v podniku řešena.

Celkový počet pracovních stanic je 12 a přenosných počítačů je 27.

3.4.2 Zabezpečení přenášených dat

Ochrana dat během přenášení je na velmi dobré úrovni, v podniku jsou využívány moderní technologie k zabezpečení datových nosičů. Průběžně je nahrazován starý hardware tak, aby mohly být využívány moderní technologie přístupu k přenosným počítačům. Stejně jsou obměňovány přenosné disky i flash disky, pokud jsou na trhu k dispozici nové technologie šifrování dat.

Vzdálený přístup do centrálního datového úložiště není v podniku používán, a to ani s využitím virtuální privátní sítě.

Ochrana hardwarovým firewallem je zajištěna pro přístup do vnitřní sítě podniku. Pracovní stanice a přenosné počítače jsou vybaveny osobním firewallem, dodávaným s operačním systémem Windows.

3.4.3 Zabezpečení důvěryhodnosti zaměstnanců

Po všech zaměstnancích je požadována trestní bezúhonnost. Zaměstnanci, kteří přicházejí do styku utajovanými informacemi, jsou pravidelně prověřováni Národním bezpečnostním úřadem.

Součástí pravidelných školení v podniku jsou i informace týkající se nových bezpečnostních technologií a nových zákonných úprav v oblasti ochrany utajovaných informací a jejich implementaci.

3.5 Návrh na zlepšení v rizikových oblastech

3.5.1 Zabezpečení uložených dat

3.5.1.1 Nasazení antivirového softwaru

Návrh komplexního řešení

Antivirový software používaný v podniku je od různých výrobců, což znemožňuje komplexní správu. Na základě analýzy používaných informačních technologií ve společnosti doporučuji kompletní řešení od společnosti ESET. Tento výrobce antivirových řešení je dlouhodobě velmi dobře hodnocen, disponuje řadou ocenění a certifikátů. Důležitou vlastností je vysoká úspěšnost v odhalování počítačových virů, rychlost vydávání aktualizací virových databází a v neposlední řadě také cena antivirového softwaru.

Návrh produktů

Vzhledem k nabízeným produktům společnosti ESET navrhuji následující softwarové vybavení:

- **centrální správa antivirového řešení** – ESET Remote Administrator;
- **ochrana emailového serveru** – ESET Mail Security pro Microsoft Exchange Server;
- **ochrana datového serveru** – ESET NOD32 Antivirus pro Windows File Server;
- **ochrana pracovních stanic a přenosných počítačů** – ESET Smart Security Business Edition.

Cena navrhovaného řešení

Tabulka 1 Ceny navrhovaných antivirových produktů

produkt	potřebný počet licencí	pořizovací cena (bez DPH) jedné licence na 1 rok/3 roky	prodloužení jedné licence na 1 rok/3 roky
ESET Remote Administrator	1+1	0,-	0,-
ESET Mail Security	32	7552,- / 15872,-	5280,- / 12832,-
ESET NOD32 Antivirus pro Windows File Server	1	3456,- / 7258,-	2360,- / 5875,-
ESET Smart Security Business Edition	39	29211,- / 61347	20436,- / 49647,-
celková cena		40219,- / 84477,-	28076,- / 68354,-

Zdroj: Vlastní konstrukce, ESET [online]. [cit. 2011-07-31]. Dostupné z WWW: http://www.eset.cz

Z výše uvedené tabulky vyplývá, že cenové zvýhodnění při nákupu jednotlivých produktů s licencí na 3 roky je velmi výrazné oproti licenci na 1 rok a dosahuje téměř ceny jednoroční licence. Podobně, i když ne tak výrazně, je tomu u prodloužení licence.

Centrální správa ESET Remote Administrator je výrobcem dodávána zdarma a je ke stažení z webových stránek výrobce.

Software na ochranu pracovních stanic a přenosných počítačů ESET Smart Security Business Edition obsahuje antivirus, antispyware, osobní firewall a antispam. Použitá integrace bezpečnostního řešení usnadňuje správu softwaru a také méně zatěžuje prostředky počítačů.

Doporučení pro nákup

V prvním kroku je nutné správné načasování nákupu nového antivirového softwaru k datu, kdy bude končit licence stávajícího antivirového softwaru. Všechny licence nejsou prodlužovány ve stejný okamžik, vždy dojde k určitému překrytí licencí starého a nového antivirového softwaru. V žádném případě není možné čekat, až skončí platnost poslední licence a vystavit tak IT techniku velkému riziku napadení.

Jako druhý krok je nutné zvážit, v jakém časovém intervalu budou licence prodlužovány. Vzhledem k výrazné finanční úspoře navrhuji nákup antivirového softwaru s licencí na 3 roky. Po dobu tří let bude administrátor a příslušný zaměstnanec logistiky oproštěn od každoročních povinností se správou a nákupem licencí. Ze stejných důvodů navrhuji též tříleté období prodlužování licencí.

Doporučení pro implementaci

Vzhledem k rozsahu implementace doporučuji provést instalaci antivirového softwaru na všechna zařízení během víkendu, protože služby souborového serveru a mail serveru budou během instalace omezeny. Taktéž bude nutné na určitou dobu „obsadit“ jednotlivé pracovní stanice, což by v pracovní dny omezovalo uživatele a zdržovalo administrátora. V případě přenosných počítačů by byla instalace antivirového softwaru v běžné pracovní době ještě komplikovanější.

Dále doporučuji pravidelné aktualizování všech instalací antivirového softwaru administrátorem, včetně možnosti aktualizace přenosných počítačů mimo vnitřní síť podniku. Součástí implementace antivirového softwaru musí být též zaškolení všech uživatelů, včetně upozornění, kde se nacházejí potenciální zdroje nákazy a jak se jim vyhnout. Toto školení by mělo být realizováno opakovaně po stanovené době, například jeden rok.

3.5.1.2 Zálohování dat

Software

V podniku se používá pro zálohování dat na centrálním serveru zálohovací program od společnosti Acronis. Vzhledem k vyšší ceně již používaného softwaru pro zálohování

serverů, centralizované správy všech instalací, ale také dobrého poměru kvality a ceny softwaru od tohoto výrobce, doporučuji doplnit všechny počítače zálohovacím softwarem od společnosti Acronis. Software pro zálohování je na velmi vysoké úrovni, společnost získává za své zálohovací produkty pravidelná ocenění od předních světových odborných médií.

Návrh produktu

Společnost již používá zálohovací software pro centrální server. Pro zálohování pracovních stanic a přenosných počítačů navrhuji instalovat software Acronis Backup&Recovery 11 Advanced Workstation, který disponuje centralizovanou správou zálohování.

Cena navrhovaného řešení

Tabulka 2 Cena navrhovaného zálohovacího softwaru

produkt	cena za jednu licenci	potřebný počet licencí	celková cena
Backup&Recovery 11 Advanced Workstation	1950,-	39	76050,-

Zdroj: Vlastní konstrukce, Acronis [online]. [cit. 2011-07-31]. Dostupné z WWW: http://www.acronis.cz

Ačkoliv se cena navrhovaného řešení může zdát vysoká, jedná se o komplexní řešení jednoho výrobce. Navrhovaný produkt nabízí centralizovanou správu, lze tedy zálohovat jednotlivé pracovní stanice a přenosné počítače dle stejně nastavených kritérií administrátorem. Společnost Acronis nabízí i výrazně levnější varianty zálohovacího softwaru, avšak ty nejsou vybaveny centralizovanou správou.

Další variantou je využití zálohovacího softwaru jiných výrobců. V tomto případě je však nutno počítat s tím, že centralizovaná správa nebude jednotná pro centrální server a ostatní počítače. V případě volně šiřitelných programů není centralizovaná správa

k dispozici vůbec, možnosti nastavení zálohování nejsou na dostatečné úrovni a problematická je také technická podpora těchto produktů.

Implementace navrhovaného řešení

Instalaci zálohovacího softwaru je možné provést v běžné pracovní době uživatelů. Dobu samotného zálohování je nutno rozložit mezi jednotlivé počítače tak, aby nebyl přetížen centrální server ani datová síť. Proto je vhodné zálohovat počítače v době, kdy jsou co nejméně používány, nejlépe mimo pracovní dobu uživatelů.

Po implementaci zálohovacího řešení je vhodné provést prvotní školení zaměstnanců o tom, které složky v počítačích budou zálohovány a do kterých budou uživatelé svá data ukládat. Toto je nutné stanovit vnitřním předpisem.

Hardware

Společnost používá pro zálohování centrálního serveru část diskového pole a následnou zálohu nebo archivaci na optické disky CD/DVD. Vzhledem k nárůstu zálohovaných dat po implementaci komplexního řešení bude nutno pořídit zálohovací zařízení s výrazně větší kapacitou a přenosovou rychlostí. Vzhledem k nabízené kapacitě, ceně za 1 MB, přenosové rychlosti a trvanlivosti uložených dat nejlépe vyhovuje metoda zálohování dat na datové pásky.

Jako základní variantu zálohovacího zařízení navrhuji páskovou zálohovací mechaniku HP LTO-4 Ultrium 1760 od společnosti Hewlett-Packard, která používá datová média s kapacitou až 1,6TB a je vybavena technologií šifrování dat AES 256bit.

Cena navrhovaného řešení

Tabulka 3 Cena navrhovaného zálohovacího zařízení

produkt	doporučená cena za hardware (bez DPH)	doporučená cena za datové médium (bez DPH)
HP LTO-4 Ultrium 1760	52330,-	666,-

Zdroj: Vlastní konstrukce, Hewlett-Packard [online]. [cit. 2011-07-31]. Dostupné z WWW: http://www8.hp.com/cz/cs/home.html

Implementace navrhovaného řešení

Společnost nyní zálohuje data na zašifrované optické disky, v případě implementace uvedeného řešení lze stále využívat šifrování dat. Pro administrátora bude šifrování dat výrazně snadnější, protože uvedený hardware disponuje zabudovanou technologií šifrování. Ukládání datových médií zůstane zachováno jako doposud, tedy do trezoru mimo prostor serveru.

3.5.1.3 Fyzická ochrana dat

Společnost je v oblasti fyzické ochrany dat vybavena moderními technologiemi ochrany. Bezpečnostní opatření odpovídají jak běžným standardům pro ochranu dat, tak i zákonným požadavkům Národního bezpečnostního úřadu.

Jedinou oblastí, kterou by bylo vhodné zlepšit, je ochrana dat proti výpadku napájení v případě pracovních stanic. Centrální datový server včetně aktivních síťových prvků je vybaven nepřerušitelným zdrojem napájení UPS. Pro přenosné počítače není třeba tuto ochranu řešit, protože jsou vybaveny vlastní baterií.

Návrh řešení

Celkem je v podniku 12 pracovních stanic. Některé pracovní stanice není nutno vybavit záložním zdrojem, protože nejsou stále používány. Záložní napájení je uvažováno pro 7

pracovních stanic. Vzhledem k vlastním zkušenostem podniku se záložními zdroji, přední pozici výrobce na trhu záložních systémů UPS a vysoké úrovni technické podpory navrhuji záložní zdroje od společnosti APC.

Uvažované záložní zdroje budou chránit proti výpadku elektrické energie pracovní stanice, které jsou pro chod podniku důležité. Z tohoto důvodu navrhuji vybavit tato pracoviště záložním zdrojem APC Power-Saving Back-UPS Pro 900, který dokáže dodávat elektrickou energii pro tyto pracovní stanice cca 30-90 minut dle momentálního zatížení.

Cena navrhovaného řešení

Tabulka 4 Cena navrhovaného záložního zdroje

produkt	doporučená cena za 1 ks (bez DPH)	potřebný počet zařízení	celková cena (bez DPH)
APC Power-Saving Back-UPS Pro 900	4379,-	7	30653,-

Zdroj: Vlastní konstrukce, APC [online]. [cit. 2011-07-31]. Dostupné z WWW: http://www.apc.cz/

Implementace

Při implementaci záložních zdrojů elektrické energie není nutné žádné speciální školení uživatelů, nainstalovaný software v případě výpadku napájení ukončí provoz pracovní stanice těsně před vybitím baterií. Administrátor musí dohlédnout pouze na to, aby k záložnímu zdroji byla připojena pouze ta zařízení, která jsou nezbytně nutná k běhu pracovní stanice v případě výpadku elektrické energie.

3.5.2 Zabezpečení přenášených dat

Pro přenos dat jsou využívány moderní technologie i software. Data jsou při přenosu dobře chráněna a i pro případ potenciální ztráty jsou zabezpečena. V této oblasti není potřeba implementovat žádné další technologie.

Jediná bezpečnější metoda je žádná data nepřenášet, což je, vzhledem k zaměření podniku na instalace a servis, vyloučeno.

3.5.3 Zabezpečení důvěryhodnosti zaměstnanců

Všichni zaměstnanci podniku jsou trestně bezúhonní a někteří z nich mohou přicházet do styku s utajovanými informacemi. Vše je dodržováno dle zákonných požadavků a v této oblasti není potřeba přijímat další opatření.

4 Závěr

V úvodu teoretické části této práce jsou popsány základní přístupy k ochraně dat a elektronických dokumentů, které by měl každý podnik chránit proti ztrátě, zcizení či neoprávněné manipulaci. V kapitole 2.2 jsou uvedeny standardně používané metody ochrany dat. Na konci teoretické části jsou shrnuty povinnosti podniku při nakládání s daty.

Praktická část v úvodu popisuje vybranou společnost, její organizační strukturu a klíčové zákazníky. Kapitola 3.2 popisuje v podniku zjištěný stav používaných technologií a postupů, používaných v oblasti bezpečnosti a ochrany dat.

Analýzou jednotlivých oblastí bylo zjištěno, že zejména oblast zálohování dat je řešena pouze částečně. Z jednotlivých pracovních stanic a přenosných počítačů nejsou data zálohována vůbec, případně jen uživatelem vybraná data, navíc pouze na centrální server. Hlavním důvodem je nedostatečné vybavení potřebným hardwarem pro zálohování dat. V případě softwaru je nutná jeho implementace. Další oblastí, kterou by bylo vhodné vylepšit, je ochrana antivirovým softwarem. V podniku je používán různý antivirový software, který neposkytuje všechny potřebné funkce ani centrální správu. Navíc jsou licence zajišťovány samostatně pro každý počítač jednou za rok, což je ekonomicky i časově nevýhodné. V případě použití osobního firewallu na jednotlivých počítačích je využíváno základní řešení, v podobě firewallu dodávaného s operačním systémem. V tomto případě by bylo vhodnější využívat komerční produkt, který poskytuje lepší funkcionalitu a je lépe aktualizován. Poslední oblast ochrany, ochrana proti výpadku napájení, je řešena také jen částečně. Nejdůležitější IT zařízení, kterým je centrální server, je proti výpadku chráněno.

Na základě zjištěných slabých míst v oblasti ochrany dat byly navrženy vhodné metody a technologie, které by slabá místa výrazně posílily. Součástí těchto návrhů jsou i cenové kalkulace a návrhy postupů pro implementaci. V případě zavedení jednotlivých technologií do podniku je potřeba zaškolit všechny pracovníky, odpovědné za bezpečnost a ochranu dat, stejně jako všechny uživatele.

Dále je nutno vytvořit v podniku bezpečnostní politiku, která je zcela opomíjena.

Na závěr lze tedy konstatovat, že vybraný podnik dodržuje bezpečnostní standardy a zákonné povinnosti, zabezpečení dat proti zcizení či zneužití je na velmi dobré úrovni. Slabá místa jsou ovšem v oblasti ochrany uložených dat v případě živelné události, nebo poruchy hardwaru.

Všechny popsané metody a postupy ochrany dat, stejně jako navrhovaná řešení, lze použít i v dalších menších nebo středně velkých podnicích. Základní ochranu dat, jako je zálohování, firewall a antivir, lze použít i pro jednotlivce a to s velmi nízkými náklady, případně zdarma.

Literatura

Primární zdroje

Carl Endorf, Eugene Schultz, Jim Mellander: *Hacking – detekce a prevence počítačového útok*u, nakladatelství Grada Publishing, a.s., 2005. 356 s. ISBN 80-247-1035-8

Jaroslav Horák: *Bezpečnost malých počítačových sítí,* nakladatelství Grada Publishing, a.s., 2003. 200 s. ISBN 80-247-0663-6

Miroslav Ludvík, Bohumír Štědroň: *Teorie bezpečnosti počítačových sítí,* nakladatelství Computer Media s.r.o., 2008. 98 s. ISBN 978-80-86686-35-6

Stuart McClure, Joel Scambray, George Kurtz: *Hacking bez tajemství,* nakladatelství Computer Press, 2003. 632 s. ISBN 80-722-6948-8

DOSEDĚL, T.: *Počítačová bezpečnost a ochrana dat.* Brno: Computer press, 2004. 190 s. ISBN 80-251-0106-1

Gála, L., Pour, J., Šedivá, Z.,: *Podniková informatika - 2., přepracované a aktualizované vydání.* Praha: Grada publishing, 2009. 496 s. ISBN 978-80-247-2615-1

Odborné knihy a časopisy

Schmidt, T., Trousil, P.: *Jak zajistit bezpečí pro data. CHIP, Magazín informačních technologií, ročník 20, číslo 3, str. 56-59.* Praha: Burda Praha, spol. s r. o., 2010. 146 s. ISSN 1210-0684

Hermannsdorfer, M., Kratochvíl, P.: *Vše přes firewall. CHIP, Magazín informačních technologií, ročník 20, číslo 5, str. 56-61.* Praha: Burda Praha, spol. s r. o., 2010. 146 s. ISSN 1210-0684

Internetové zdroje

Acronis [online]. [cit. 2011-07-31]. Dostupné z WWW: http://www.acronis.cz

Alsig [online]. [cit. 2011-07-31]. Dostupné z WWW: http://www.alsig.cz/

APC [online]. [cit. 2011-07-31]. Dostupné z WWW: http://www.apc.cz/

ESET [online]. [cit. 2011-07-31]. Dostupné z WWW: http://www.eset.cz

Hewlett-Packard [online]. [cit. 2011-07-31]. Dostupné z WWW: http://www8.hp.com/cz/cs/home.html

My Security Software [online]. [cit. 2011-07-31]. Dostupné z WWW: http://www.my-security-software.com/top-five-best-firewall/

Security World [online]. [cit. 2011-07-31]. Dostupné z WWW: http://securityworld.cz/

Lustyk, P.: *Security World* [online]. [cit. 2011-07-31]. Dostupné z WWW: http://securityworld.cz/securityworld/zakladna-efektivni-a-ucinne-spravy-zabezpeceni-it-1136

SuggestSoft [online]. [cit. 2011-07-31]. Dostupné z WWW: http://www.suggestsoft.com/soft/infonautics-gmbh/live-file-backup/

VPN Technology [online]. [cit. 2011-07-31]. Dostupné z WWW: http://www.vpn-technology.com/

Wikipedie [online]. [cit. 2011-07-31]. Dostupné z WWW: http://cs.wikipedia.org/wiki/Encrypting_File_System

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 1. ledna 2011, dostupný také na http://business.center.cz/business/pravo/zakony/oou/

Zákon č. 227/2000 Sb., o elektronickém podpisu, dostupný také na http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, dostupný také na http://www.nbu.cz/cs/pravni-predpisy/zakon-c-4122005/uplne-zneni-zakona-c-4122005/

Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, dostupný také na http://www.cesarch.cz/legislat/2004-499.htm