Zajištění informační bezpečnosti organizace

Ensuring information security of company

Andrea Bézová

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Andrea BÉZOVÁ**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Zajištění informační bezpečnosti organizace**

Zásady pro vypracování:

1. **Uveďte používané způsoby zabezpečení dat z hlediska software a hardware.**
2. **Popište způsoby zajištění bezpečného provozu organizace z pohledu administrátora a uživatele.**
3. **Porovnejte nároky na bezpečnost organizací z hlediska požadovaného stupně ochrany dat.**
4. **Uveďte normy vztahující se k problematice informační bezpečnosti organizace.**
5. **Na základě získaných poznatků navrhněte pokročilé způsoby pro zajištění informační bezpečnosti střední organizace.**

Rozsah práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **LUDVÍK, Miroslav. Teorie bezpečnosti počítačových sítí. Praha: Computer media, 2008. 98 s. ISBN 978-80-86-686-35-6.**
2. **STAUDEK, J. Standardizace bezpečnosti IT, Fakulta informatiky Masarykovy Univerzity Brno, 2002.**
3. **EDWARDS, L. Law and the Internet, Framework for the Electronice Commerce, Hart Publishing, Oxford 2000, ISBN 1-84113-141-5.**
4. **ŠTĚDROŇ, B. Elektronická kontrola zaměstnanců a právo, Convergence 10/2004, CNG, ISSN 1214-5785.**
5. **BARKEN, L. Bezpečnost bezdrátové komunikace. Computer Press, 2005.**

Vedoucí bakalářské práce: **Ing. Ivo Motýl**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **19. února 2010**

Termín odevzdání bakalářské práce: **19. května 2010**

Ve Zlíně dne 19. února 2010

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Tato práce se zabývá problematikou ochrany interních dat v organizacích. Teoretická část pojednává o členění organizací a možných způsobech obrany před napadením útočníkem i interních rizik z hlediska uživatelů a techniky. Nesdílnou součástí ochrany dat je i prevence před jejich ztrátou. V praktické části budu rozebírat úroveň informační bezpečnosti a rizik konkrétní organizace. Na základě výsledku budou navrhnuty možné efektivnější inovace systému. Jedním z cílů mé práce bude uvedení některých z moderních způsobů zabezpečení dat v organizaci.

Klíčová slova: organizace, informační bezpečnost, riziko

ABSTRACT

This work deals with the protection of internal data in organizations. The theoretical part discusses the organization and layout of possible defenses against attacks by the assailant and internal risks in terms of users and technology. Retiring part of data protection is prevention before a loss. The practical part will discuss the level of information security and risk management of a particular organization. Based on the outcome will be designed to be more effective innovation system. One of the goals of my work will be putting some of the modern methods of data security in an organization.

Keywords: organization, information security, risk

Chtěla bych poděkovat vedoucímu mé bakalářské práce Ing. Ivu Motýlovi, za čas, který mi věnoval, účelné rady a optimistický, přitom věcný, přístup. Dále nejmenované organizaci, která mi dovolila pracovat s jejími daty a za konzultace s informačními techniky. V neposlední řadě patří dík mé rodině, která mě při práci plně podporovala a věřila v mé schopnosti.

Motto mé práce je ze životních zkušeností a zní: „Když se má něco pokazit, tak pořádně“

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Žijeme v době, ve které je práce s počítačem téměř pro každého samozřejmostí a s tím souvisí zároveň i práce s internetem. Ve světě organizací to platí dvojnásob. Existují organizace živící se a fungující pouze na internetu. Neocenitelnou výhodou informačních systémů pro svět byznysu je možnost komunikovat se svými partnery, zákazníky či interně mezi sebou na velké vzdálenosti za pár sekund.

Stejně tak jako organizace živící se legálně na internetu existují jednotlivci i skupiny útočníků, kteří se živí na internetu nelegálně. Tito útočníci používají mnoho způsobů jak napadnout počítač či celou jejich síť. Proti těmto útokům má naši stanici ochránit antivirový program a firewall. Velké společnosti zabývající se vytvářením ochranných programů svádějí neustálý boj s těmito útočníky, ale útočníkům se daří vytvářet nové, stále lepší infikované programy či soubory, které napadají počítače a kriticky ohrožují jejich funkčnost či data uložená na počítači.

Dnes se stává u organizací ochrana před těmito útoky důležitou složkou pro její bezpečný a hladký chod. Infikování systému popř. zničení či zneužití dat může mít pro organizaci drtivý dopad a někdy může být až likvidační. V potaz se musí vzít také fakt, že mnohdy může mít ty samé destruktivní účinky i interní špatné nastavení systému, nedbalost zaměstnance či nehoda přírodního typu. Proto je třeba nastavit v organizaci podmínky takové, aby její informační chod byl pokud možno kontrolovaný a chráněn před maximálním počtem rizik.

Tato práce by měla čtenáři poskytnout informace o možnostech ochrany počítače i celé sítě počítačů a uvést příklad informačních inovací na konkrétní organizaci jako příkladu. Téma jsem si vybrala, protože mě zajímá svět informatiky, jeho možnosti a moderní technika v boji proti útočním hrozbám, které můžou potkat jak běžného uživatele, tak i organizaci.

I. TEORETICKÁ ČÁST

1 POUŽÍVANÉ ZPŮSOBY ZABEZPEČENÍ DAT Z HLEDISKA SORTWARE

Jeden z hlavních způsobů zabezpečení dat i celého počítače z hlediska software patří antivirové programy a firewally. Měli by chránit náš počítač od nebezpečných virů, spamů, malware a mnoha dalších nežádoucích hostů. Aby tento software byl opravdu účinný je zapotřebí provádět pravidelné aktualizace. Typicky se jedná o programové celky se sadou zabezpečení. V praxi jsou tyto programové celky používány jako komplexní řečení od jednoho výrobce nebo komplexní řešení od různých výrobců. Je nutností, aby všechen použitý software byl legální a měl by být instalován profesionálem, aby byla zaručena jejich správná konfigurace.

- **Komplexní řešení od jednoho výrobce** – jedná se o nasazení softwaru na všech úrovních. Zpravidla má tento způsob řešení centrální správu. Výhodou je, že z jedné stanice můžeme spravovat všechny komponenty tohoto řešení. Centrální správa se ve většině případů projevuje jako nejvhodnější, protože ušetří velké množství času, který by strávil administrátor nad instalováním softwaru na každou stanici zvlášť. Problémem uvedeného řešení je závislost na jednom výrobci, protože všechny části používají stejnou virovou bázi.

- **Komplexní řešení od různých výrobců** – centrální správu všech komponent lze provozovat i v případě, kdy je řešení od různých výrobců. Jako u předchozího řešení i zde se jedná o nasazení antivirového softwaru na věch úrovních. Řešení od různých výrobců má výhodu v tom, že využívají virové databáze všech uvedených výrobců, což zvyšuje úroveň zabezpečení dané organizace. Ovšem ani toto řešení nám nezajistí 100% zabezpečení organizace, protože aktualizace virových databází probíhá až po výskytu nového viru.

1.1 Pojem antivirový program

Antivirový program je počítačový software, sloužící k vyhledání, identifikaci, eliminaci či odstraňování počítačových virů, škodlivých kódů a jiného softwaru, který by mohl narušit poklidný chod našeho PC. Sleduje všechny nepodstatnější vstupní a výstupní místa, kterými by mohly tyto viry do počítačového systému vniknout. Běží nepozorovaně na pozadí při naši práci se systémem, tuto činnost většinou nezaregistrujeme, pokud je systém dostatečně rychlý a samozřejmě pokud nejsou soubory napadené virem. V praxi jsou požívány dvě metody detekce virů:

- Prohlížení souborů na lokálním disku (harddisku), které má za cíl nalézt sekvenci odpovídající definici některého počítačového viru v databázi.
- Detekcí podezřelé aktivity některého z počítačových programů, která může značit infekci, tato technika zahrnuje analýzu zachytávaných dat, sledování aktivit na jednotlivých portech či jiné techniky.

1.1.1 Druhy antivirových programů

- **On – demand skenery** - přestože On – demand skenery jsou součástí antivirových systémů, je nabízen některými antivirovými společnostmi zdarma. Spouštějí se přes rozhraní OS DOS ovládané přes příkazový řádek. Jsou využívány v případech, kdy systém není schopen, z jakéhokoliv důvodu poškození, nastartovat se obvyklým způsobem.

- **Jednoúčelové antiviry** - jde o programy vytvořené za účelem detekce a popřípadě i odstranění jednoho konkrétního viru, popřípadě malé skupiny virů. Jedná se o tzv. „krabičku poslední záchrany“, nelze je tedy považovat za plnohodnotnou antivirovou ochranu. Jednoúčelové antiviry jsou využívány v případě, kdy vypukne epidemie určitého viru. Některé antivirové společnosti v době této epidemie zveřejní antivir, který má odhalit daný konkrétní vir. Tyto antiviry jsou obvykle k dispozici zdarma na internetu a slouží k odstranění viru, který je v dané době rozšířený.

- **Antivirové systémy** - jde o komplexní, v dnešní době nejfrekventovanější antivirové řešení, jejímž úkolem je sledovat všechna nejpodstatnější vstupní i výstupní místa, kterými by mohla nastat infiltrace počítačového systému virem. Mezi tato sledovaná místa může patřit například elektronická pošta (červi, spam), www stránky (škodlivými skripty), media (Cd, flash disky). Některé antivirové systémy mají také jako svou součást firewall a další specializované nástroje.

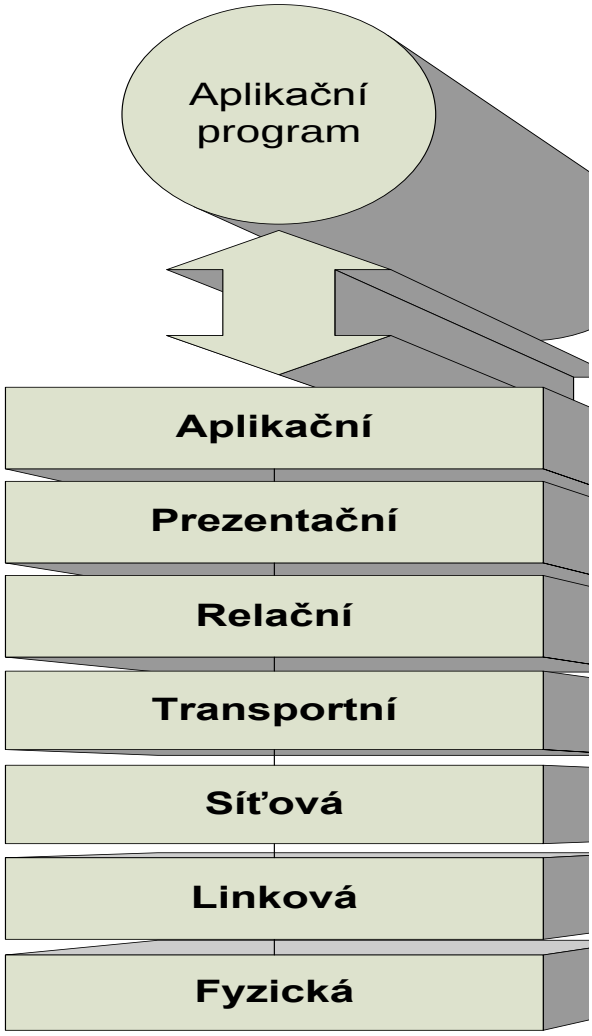
1.2 Pojem firewall

Jedná se o síťové zařízení, sloužící k řízení a zabezpečování síťového provozu mezi sítěmi různých důvěryhodností. Zjednodušeně se dá říci, že se jedná o kontrolní bod, který definuje pravidla pro komunikaci mezi různými sítěmi. Nastavení firewallu se řídí podle pravidel, která jsou definována administrátorem. Dříve firewall používal identifikaci zdrojové a cílové IP adresy, což je pro dnešní potřeby zabezpečení nedostačující. Modernější firewally využívají možnosti kontroly informace o stavu připojení, kontroly protokolů a také prvků IDS (Intrussion Detection Systém).

Firewall by nám měl, poskytnou ochranu proti neoprávněnému vzdálenému přístupu. Je vhodný jak pro klasické počítačové stanice či servery, tak slouží i pro ochranu hardwaru, protože existují verze hardwarových a softwarových firewallů.

1.2.1 Druhy firewallů

- **Paketové filtry** – jedná se o nejstarší a nejjednodušší formu firewallu, spočívá v tom, že jsou pevně dána pravidla z jaké adresy, na jakou adresu může být doručen paket. Na základě těchto pravidel firewall vyhodnotí všechny příchozí pakety a buď je propustí, nebo zamítne. Tato kontrola je prováděna na třetí a čtvrté vrstvě modelu síťové komunikace OSI. V dnešní době se tento druh firewallu v podstatě nepoužívá. Paketové filtry je vhodné spíše volit do míst, která nejsou náročná na přesnost nebo nevyžadují dokonalejší analyzování dat, které sítí prochází. Důvodem je nízká úroveň kontroly procházejících spojení.



Obr. 1. Síťová komunikace ISO OSI

- **Aplikační brány** – vznikly pouze chvíli po jednoduchých paketových filtrech. Rozdíl mezi nimi je však značný. Dokážou naprosto oddělit sítě mezi, které tyto aplikační brány byly postaveny. Někdy se aplikačním branám říká také proxy firewally. Výhodou použití aplikačních bran, je že dokážou velmi spolehlivě chránit známé protokoly. Naopak nevýhodou aplikačních bran je jejich velká náročnost na hardwarové řešení. Každý protokol vyžaduje napsání specializované proxy. Proto většina aplikačních bran umí kontrolovat pouze okolo deseti protokolů. Po zavedení stavových paketových filtrů se vývoj a inovace aplikačních bran zastavila a díky jejich náročnosti se dnes využívají pouze ve specializovaných nasazeních.

- **Stavové paketové filtry** – provádějí kontrolu protokolů stejně jako jednoduché paketové filtry, ale funkcí navíc, je paměť již povolených spojení, což značně urychluje jejich použití. Tuto funkci lze využít při rozhodování, zda procházející pakety patří do povoleného spojení, nebo zda musejí procházet novým rozhodujícím procesem. Z toho plyne urychlení zpracování paketů a také lze v pravidlech pro firewall uvádět směr navázání spojení, což zapříčiní, že firewall dokáže příště sám rozhodovat i o povolení odpovídajících paketů u známých protokolů. Díky vysoké rychlosti a slušné úrovni zabezpečení jsou stavové paketové filtry jednou z nejpoužívanějších forem firewallů. Výhodou jejich nasazení do systému je také několikanásobněji snazší konfigurovatelnost oproti jednoduchým paketovým filtrům a aplikačním branám, tím se značně sníží možnost chybného nastavení pravidel obsluhou. Nevýhodou tohoto nasazení je všeobecně nižší bezpečnost, kterou nám mohou poskytnout aplikační brány.

- **Stavové paketové filtry s kontrolou protokolů a IDS** – tyto filtry dnes dokáží nejen kontrolovat informace o stavu spojení a mají schopnost dynamicky otevírat porty, ale implementují technologie sloužící pro identifikaci i autentikaci protokolů a aplikací využívajících IP protokol. Tuto technologii nazýváme Deep Inspection nebo Application Inteligence. Jednoduše lze říci, že filtry dokáží kontrolovat spojení až do úrovně korektnosti procházejících dat. Což umožní zakázání průchodu http spojení, ve kterých jsou znaky nebezpečného protokolu. Nejnověji se do firewallů integrují tzv. IDS (Instrusion Detection Systems), jedná se o systém detekující narušení neboli potenciální útok.

1.3 Ochrana dat pomocí zálohování

Zálohování je velmi důležitý prvek k uchování dat s možností jejich opětovné obnovy. Metod zálohování je velké množství, volba správného řešení záleží na objemu zálohovaných dat, na rychlosti, s jakou je požadována jejich obnova i na riziku, které při ztrátě dat hrozí. Data by měla být uložena v šifrované podobě. Zálohy jsou prováděny dle administrátorem definovaných četností. Jsou situace, ve kterých stačí jednoduché zálohování a v jiné, na první pohled velmi podobné situaci, je zapotřebí rozsáhlý zálohovací systém.

Další otázkou je úschova záložních medií. Data, která jsou ukládána, se zapisují na pásku, medium či externí harddisk. Je možné provádět zálohování i na více prvků. Pro jistotu, že se uložená data neztratí, je vhodné vytvářet kopie těchto záloh a ukládat je na bezpečném místě, nejlépe mimo budovu např. v bankovním sejfu. Pokud by zálohovaná data byla uložena v místnosti budovy organizace, v případě požáru by mohlo dojít k jejich zničení, tím pádem by se stala pro obnovení nepoužitelná.

Zálohování dat je prevence před jejich zničením, které může nastat vnitřní závadou hardwaru běžného datového úložiště, zničení běžného datového úložiště zevnějšku např. požár, živelná katastrofa apod., poničení softwaru a závažnou chybou obsluhy.

1.3.1 Způsoby zálohování dat

- **Cyklické zálohování** – jedná se o způsob ukládání dat v pravidelných intervalech. Nevýhodou použití této metody je, že v následujícím cyklu nelze obnovit data z cyklu minulého. Tuto nevýhodu vyvažuje fakt, že objem dat oproti trvalé archivaci je znatelně menší a bývá konstantní.

- **Úplná záloha dat** – využívá zálohování kompletní množiny dat. Touto metodou lze vrátit uložená data i několik záloh nazpět. Nevýhoda je velké množství ukládaných dat.

- **Inkrementální záloha** – zálohují se pouze data, která se pouze změnila od poslední plné zálohy dat.

- **Rozdílová záloha** – zálohovány jsou pouze všechny data, která se změnila od poslední zálohy bez ohledu na to, jestli se jedná o zálohu úplnou, inkrementální nebo rozdílovou.

1.4 Využití aktualizací systému

Stejně důležité jako nasazení antivirového programu, firewallu, zálohování dat je i aktualizace systémů (Servis pack). Pro udržení bezpečného počítače je zapotřebí aktualizovat jak operační systém, tak i internetový prohlížeč. Aktualizace se dá chápat jako skupina záplat, která záplatuje místa systému, která by se mohla stát snadno napadnutelná. Pravidelná aktualizace zabraňuje stárnutí systému. Abychom mohli aktualizace provádět, je nutné vlastnit legální software. Společnost Microsoft celkem pravidelně vydává balíček aktualizací každé druhé úterý v měsíci. Možnosti aktualizace by měl využívat každý uživatel, bez ohledu na to zda se jedná o fyzickou osobu s jednou stanicí nebo organizaci.

2 ZABEZPEČENÍ ORGANIZACE Z HLEDISKA UŽIVATELŮ

V dnešní době využíváme dva typy sítí, jsou jimi peer to peer a režim domény. Peer to peer řeší spojení počítačů bez použití serveru. Toto řešení je nevýhodné a vzniká při něm vysoká náročnost režie na údržbu. Data uživatelů musí být definovaná na všech stanicích zvlášť. Mnohem výhodnější řešení pro správu uživatelů přináší režim domény. V režimu domény je nasazen doménový řadič (Domain Controller, DC), který nám umožní centrální správu a vytvoření databáze uživatelů. Dokážeme na něm vytvořit bezpečnostní skupiny (security group´s, SG) a umožní to jednodušší správu přístupu na objekty v síti. Doménový řadič je kritický bezpečnostní prvek, přes který se distribuují bezpečnostní politiky na jednotlivé uživatele a počítače. Má v sobě databázi dat, jmen, hesel a organizačního členění. Mezi jeho funkce patří také omezování přístupu k prostředkům na síti jako např. server, počítač nebo tiskárna. Tento síťový prvek musí být maximálně chráněn, přistup k datům a nastavení doménového řadiče může mít pouze administrátor nebo správce sítě.

2.1 Druhy uživatelů

- **Admin** – uživatel, který vykonává správu sítí a počítačů. Může měnit kritické nastavení systému, má plnou kontrolu nad systémem.

- **Power user** – nemá takové oprávnění jako administrátor. Dokáže měnit nebo mazat systémové soubory.

- **User** – nejnižší stupeň oprávnění, nemůže měnit systémové soubory, nedokáže měnit kritické nastavení systému.

Zásada je, aby uživatel na stanici byl typ user, pokud nevyžaduje povaha aplikací jinak. Je to opatření, které vede ke zvýšení bezpečnosti hlavně z hlediska neúmyslného nebo úmyslného zneužití dat zaměstnancem. Pokud by měl běžný uživatel přístup ke všem datům, mohlo by se stát, že neproškolený a nezkušený zaměstnanec nevědomě smaže důležitý soubor či nastavení a tím vznikne kritická situace v organizaci. Odstranění takovéto závady může trvat i několik hodin, což může majiteli způsobit nemalé finanční újmy. Musíme také brát v potaz, že ne každý zaměstnanec je loajální zaměstnanec. Pokud by měl kterýkoliv ze zaměstnanců nekalé úmysly a měl přístup ke všem souborům, snadno by je mohl odcizit a zneužít pro svůj prospěch. Z toho vyplývá, že přístup k důvěrným datům by měl mít pouze omezený počet lidí, nejlépe jen majitel organizace a administrátor.

2.2 Způsob zajištění informační bezpečnosti

Pro vytvoření nebo ověření bezpečnostní politiky musí pověřený IT technik provést analýzu nastavené bezpečnostní politiky. Základem je prověření zda organizace již má nastavenu bezpečnostní politiku či nikoliv. Pokud se jedná o organizaci, která je nově vytvořena a nemá aplikovánu bezpečnostní politiku, je na IT technikovi, aby vytvořil řádný projekt pro bezpečný provoz sítě v organizaci. Musí znát, jaký informační systém bude bezpečnostní politiku aplikovat a přesně si určit bezpečnostní záměr, kterého chceme dosáhnout. Přitom by měl využívat vlastních zkušeností, zavedených postupů a řídit se příslušnými normami a legislativou. Předložený návrh musí odsouhlasit majitel organizace či pověřená osoba. Pokud se jedná o organizaci, která má již informační historii, prací technika je prověřit, jaký antivirový a firewallový software je používán, zda jsou prováděny aktualizace (Servis pack), jestli jsou prováděny zálohy dat a v neposlední řadě by měl také ověřit, zda probíhá řízení uživatelských účtů.

Při vytváření informačního zabezpečení organizace je důležité provést analýzu a hodnocení rizik, která mohu organizaci hrozit. Vytvoření analýzy a hodnocení rizik dokáže lépe odhalit slabá místa a tím pádem lze přijmout efektivnější opatření. Za další velkou výhodu se považuje fakt, že dokáže organizaci lépe připravit na hrozící rizika a tak značně snížit možnou újmu, kterou by dané riziko mohlo způsobit.

2.2.1 Teorie analýzy rizik

Analýza rizik je určena pouze do rukou vrcholového vedení organizace a slouží k ochraně investic vynaložených do informačních systémů. Je možné si ji nechat vypracovat odbornou nezávislou externí organizací nebo tento úkol lze svěřit informačnímu specialistovi přímo uvnitř organizace. Existuje mnoho způsobů, jak lze analýzu rizik vytvořit a ustanovení co vše by měla obsahovat.

Různé způsoby realizace analýzy rizik celkem podrobně popisuje mezinárodní norma ISO/IEC TR 13335. Definuje čtyři základní typy provádění analýzy rizik.

- **Základní přístup** – organizace nemusí mít analýzu rizik vypracovánu vůbec nebo jsou rizika brána v potaz pouze jako skutečnosti, které se mohou stát, ale nejsou proti nim vytvořena příslušná opatření. Jedná se o řešení, které využívají hlavně malé firmy s malým finančním rozpočtem.

- **Neformální přístup** – jedná se o metodu, kdy jsou rizika posuzována dle subjektivních znalostí a zkušeností člověka, který dobře zná informační systém dané organizace, často se jedná o informačního technika zaměstnaného přímo v organizaci. Tento způsob analýzy může postačit, ale nedokáže dokonale nahradit podrobnou a odbornou analýzu rizik, proto se doporučuje pouze jako počáteční krok.

- **Podrobná analýza rizik** – jedná se o nejdelší a finančně nejnáročnější metodou analýzy rizik avšak je zaručeno téměř přesné hodnocení rizik a kvalitní návrh řešení. Klasický postup podrobné analýzy spočívá v identifikaci zaměření a aktivity organizace, dle daných údajů stanovit hodnocení rizik a přijmout odpovídající opatření.

- **Kombinovaný přístup** – jedná se o kombinaci předešlých druhů analýzy rizik.

Rizika, která organizaci hrozí, můžeme rozdělit do tří druhů. Všechna tato rizika by měla být brána v potaz a posouzena podle procenta možné újmy a výše pravděpodobnosti zasažení daného rizika v organizaci. V níže uvedené tabulce jsou příklady některých možných rizik, která se mohou vyskytnout.

Tab. 1. Příklady možných druhů ohrožení

Příklad možných druhů ohrožení		
Úmyslné	**Náhodné**	**Přírodního rázu**
odhalení/odposlech	**chyby a opomenutí**	**zemětřesení**
podvod/narušení integrity	**vymazání souboru**	**požár**
narušení dostupnosti	**nesprávné směrování**	**blesk**
přisvojení/krádež	**fyzické nehody**	**povodeň**
		elektrický výboj

2.3 Povinnosti a náplň práce administrátora

Administrátor je člověk, který se stará a udržuje celkový chod a bezpečnost sítě. Stanovuje bezpečnostní politiky informačních systémů v organizaci. Provádí novou registraci uživatelů, stanovuje uživatelská práva a stará se o údržbu uživatelských účtů. Konzultuje s uživateli otázky provozu sítě. Prověřuje všechny náznaky nedovoleného nebo podezřelého jednání. Stará se o instalaci všech systémů, o aktualizace a zálohování těchto systémů. Sleduje nové trendy informační problematiky. Pokud se jedná o malé či střední organizace postačí jeden administrátor, ale měl by mýt za sebe zástupce ve chvíli, kdy nebude z jakéhokoliv důvodu svou práci schopen vykonávat. Nadnárodní i veliké společnosti se stovkami zaměstnanců mají týmy informačních techniků, kteří se starají o bezpečný a hladký provoz.

2.4 Povinnosti běžného uživatele pro udržení bezpečnosti

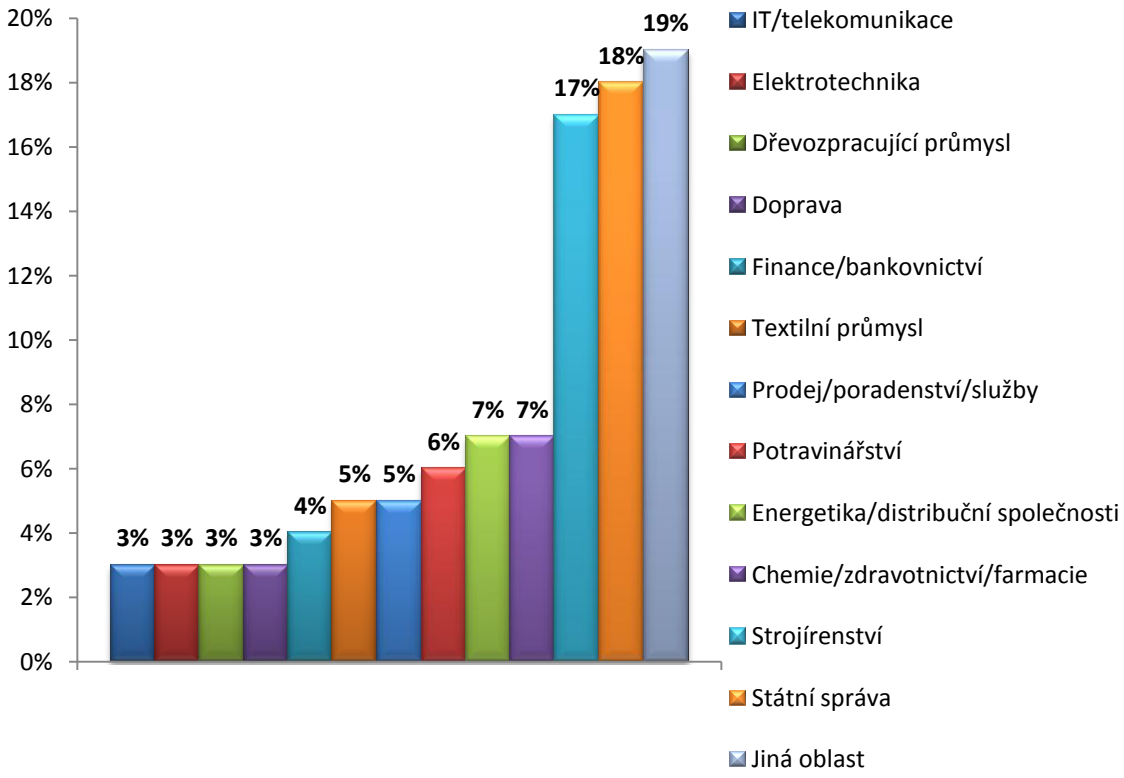
I běžný uživatel musí dodržovat určitá pravidla pro udržení bezpečnosti stanic i sítě. Základem je správné užívání hesla do systému. Žádná stanice nesmí být bez hesla, uživatel by měl používat silná hesla. Silné heslo má minimálně 8 znaků, musí obsahovat malá i velká písmena, číslici a speciální znak. Zásadně si nesmí uživatel hesla psát na papírky nebo v horším případě lepit ty papírky na monitor. Heslo by se mělo pravidelně měnit, obvykle po 90. dnech. Uživatel by do své stanice měl vkládat pouze prověřená media, flash disky apod. Neměl by prohlížet nebezpečné stránky na internetu, stahovat nelegální či podezřelý obsah a otvírat nebezpečnou poštu. Povinností uživatele by měla být pravidelná aktualizace systému.

3 KLASIFIKACE ORAGANIZACÍ

Můžeme si vybrat z několika druhů klasifikace organizací, pro svou práci jsem zvolila 2 druhy. Uvedeno je dělení dle zaměření organizace a dle potřeby ochrany osobních dat či možné újmy na zisku při vyřazení informačního systému z provozu. Chtěla bych také podotknout, že bez ohledu na počet zaměstnanců, zaměření i možné újmy na zisku, každá organizace potažmo i obyčejný uživatel, by měli využívat a dodržovat alespoň základní bezpečnostní pravidla a chránit počítač před možným napadením nebo ztráty dat. Mnohokrát žijeme v domnění, že mě se to stát nemůže, ale opak je tomu pravdou. Největšímu nebezpečí svůj počítač vystavujeme např. v kavárnách či prostranstvích, kde je možné volné připojení k wi-fi síti.

3.1 Dělení dle zaměření organizace

Dělení dle zaměření je bráno dle procentuálního pokrytí daného zaměření organizace na českém trhu.



Obr. 2. Dělení dle zaměření organizace [1]

Výše uvedený graf znázorňuje pokrytí zaměnění organizací na českém trhu v roce 2003. Výhodou je, že dělení dle zaměření má celkem dobře vyřešenou problematiku požadovaného zabezpečení pro daný typ organizace a je pokryto mnohem větší množství různých řešení dle požadovaného stupně zabezpečení. Přestože dané řešení se zdá být plně postačující, je zapotřebí vždy brát v úvahu i počet zaměstnanců, kteří jsou v organizaci. Čím je počet zaměstnanců vyšší, tím stoupá riziko úmyslného i neúmyslného poškození možného zničení nebo zneužití dat. Někdy se stává, že organizace mohou spadat pod dva nebo více typů zamření, což může činit značné problémy, při vytváření bezpečnostní politiky jelikož každý druh zaměření organizace má své specifické směrnice či požadavky na bezpečnost. Jsou organizace, které přijímají řešení bezpečnostní politiky dle počtu zaměstnanců. Výhodou tohoto řešení je jeho jednoduchost, snadné zařazení organizace a lehčí implementace do systému, ovšem i organizace s deseti zaměstnanci můžou pracovat s citlivými daty např. právní kancelář a proto budou vyžadovat maximální zabezpečení systému

3.2 Dělení dle nároků ochrany dat a možné újmy pro organizaci

Toto dělení je zaměřeno na důležitost uchovávaných dat, možnou újmu při ztrátě nebo odcizení těchto dat a také následky, které mohou vyplynout z ochromění systému. Jedná se o komplexní řešení zahrnující jak počet zaměstnanců tak i zaměření organizace.

3.2.1 Banky, velké peněžní ústavy a telekomunikační operátoři

Většinou se jedná o velké někdy i nadnárodní společnosti se stovkami až tisíci zaměstnanců. Tyto společnosti musí zajišťovat, aby dostupnost jejich služeb fungovala nepřetržitě a naprosto bezpečně. Proto vydají do výpočetní techniky desítky milionů korun ročně, z toho na bezpečnost obvykle jde 30 procent z celkové částky. Bezpečnostní politika musí být dokonale propracována a zabezpečení uchovávaných dat maximální. Jakákoliv kompromitace společnosti zapříčiní nedůvěru a odliv klientů, tím vystanou velké finanční ztráty.

3.2.2 Celosvětové komerční firmy, působící ve velkém množství států

Typicky se jedná o nadnárodní společnosti, s velkým polem působnosti, jejichž zisk se pohybuje ve stovkách milionů USD ročně. Oproti tomu musí na výpočetní techniku vydat až přes několik desítek milionů USD ročně a stejně jako u bank a operátorů 30 procent z celkové částky jde na bezpečnost. Zvláštností je, že využívají dvou až tří podpůrných center a z těch jsou centrálně spravovány všechny pobočky. Jejich kompromitace může mít likvidační účinky, ale ochromení systému nemá za následek velké finanční ztráty, samozřejmě že toto ochromení nesmí trvat dlouhou dobu. Z hlediska bezpečnosti by měla být chráněna hlavně interní data a know – how před konkurencí.

3.2.3 Komerční firmy působící převážně v ČR, které mají přes 200 zaměstnanců

Tyto firmy mají dostatečné množství finančních prostředků a jejich zisk se pohybuje ve stovkách milionů. Do výpočetní techniky jsou investovány desítky milionů. Jejich dostupnost dat musí být stálá, vyřazením systému mohou nastat prostoje a s tím i velké finanční ztráty. Kompromitací této společnosti může nastat odliv klientů, ale ve většině případů nemá likvidační účinky.

3.2.4 Komerční firmy působící převážně v ČR, které mají 21 – 199 zaměstnanců

Jedná se již o firmy obvykle se dvěma administrátory a záleží na majiteli či zodpovědné osobě kolik financí vydá na výpočetní techniku, ale většinou se jedná o částku pohybující se okolo stovek tisíc korun. U těchto firem již je plně na administrátorovi jakou nasadí bezpečnostní politiku a dokáže si ji obhajovat. Své data musí firmy chránit hlavně před zneužitím konkurencí. Kompromitace pro ně znamená odliv klientů a velké finanční ztráty, ale většinou nemá likvidační účinky.

3.2.5 Komerční firmy působící převážně v ČR, které mají méně než 20 zaměstnanců

Tyto společnosti zpravidla nevydávají velké finanční prostředky na výpočetní techniku, ve velké míře případů je oblast bezpečnosti velmi podceňována a kolikrát není řešena vůbec. Většinou se jedná o společnosti „rodinného typu“, proto je zde velmi vysoká míra důvěry mezi zaměstnanci a tím i vysoká solidárnost vůči zaměstnavateli. Na dobré jméno musí dbát pouze u svých zákazníků, z toho plyne, že vyřazení jejich systému nemá kritické účinky a vznikají pouze malé finanční ztráty.

3.2.6 Státní instituce, které pracují s osobními údaji

Nevýhodou těchto institucí je, že mají finanční prostředky účelově rozdělovány, proto i když dostávají dostatečné prostředky na výpočetní techniku, je s nimi plýtváno nebo jsou využity k méně nepodstatným účelům. Tyto instituce si nemohou častokrát dovolit skutečné odborníky v oblasti IT, jelikož jsou jejich platy stanovovány podle platových tříd a není možné je dostatečně ohodnotit. Přitom tyto instituce schraňují citlivá data, jejichž odcizení či ztráta mohou mít neblahé důsledky na mnoho lidí a dokáží značně snížit důvěryhodnost těchto institucí u široké veřejnosti. Častokrát se tato situace řeší nasazením odborníka z externí firmy, který vyřeší daný úkol, ale nemá danou instituci stále pod dohledem, tím pádem jeho nasazení nemá 100 procentní účinek. Výjimkou jsou vysoké školy a Česká akademie věd, které mají skutečné odborníky. Tuto kategorii nelze brát jako celek, jelikož jednotlivé podskupiny se liší (povahou, velikostí apod.).

4 NORMY SOUVISEJÍCÍ S INFORMAČNÍ BEZPEČNOSTÍ

Normu lze chápat jako určitý standard a souhrn zkušeností, přijatých širokou odbornou komunitou pro tu kterou oblast lidské činnosti. Co se týká norem používaných pro bezpečnost informací, jsou zaměřeny hlavně na systémy řízení bezpečnosti informací, v hojné míře označované jako ISMS (Information Safety Management System).

Zavádění norem pomáhá organizaci nejen sjednotit pracovní postupy, vytvoření kvalitního produktu, dodržování bezpečnostních pravidel, ale dokáže zvýšit prestiž a důvěryhodnost. Způsobem zavádění určitých standardů ne nazývá certifikace.

Nejpodstatnější pro použití kteréhokoli standardu pro informační bezpečnost jsou normy zajištění jakosti ISO 9000. Avšak u norem pro zabezpečení informační bezpečnosti se jako základní a první norma, která se zabývala touto problematikou, považuje BS 7799 z roku 1995. Navázat lze sérií ISO 27000, jež je v současnosti bezesporu hlavním proudem v normativním zabezpečení informační bezpečnosti.

Série ISO 27000 vešla do praxe 15. října 2005 vydáním ISO/IEC 27001:2005, prakticky se jedná o změnu normy s označením BS 7799-2:2004. Do budoucna by tato norma měla obsahovat sedm níže uvedených dokumentů.

ISO/IEC 27000, principy a slovník;

ISO/IEC 27001, požadavky na ISMS (resp. BS 7799-2:2004);

ISO/IEC 27002, návody pro zavádění;

ISO/IEC 27003, analýzy rizik (souvisí s ISO 13335-3);

ISO/IEC 27004, metriky a měření;

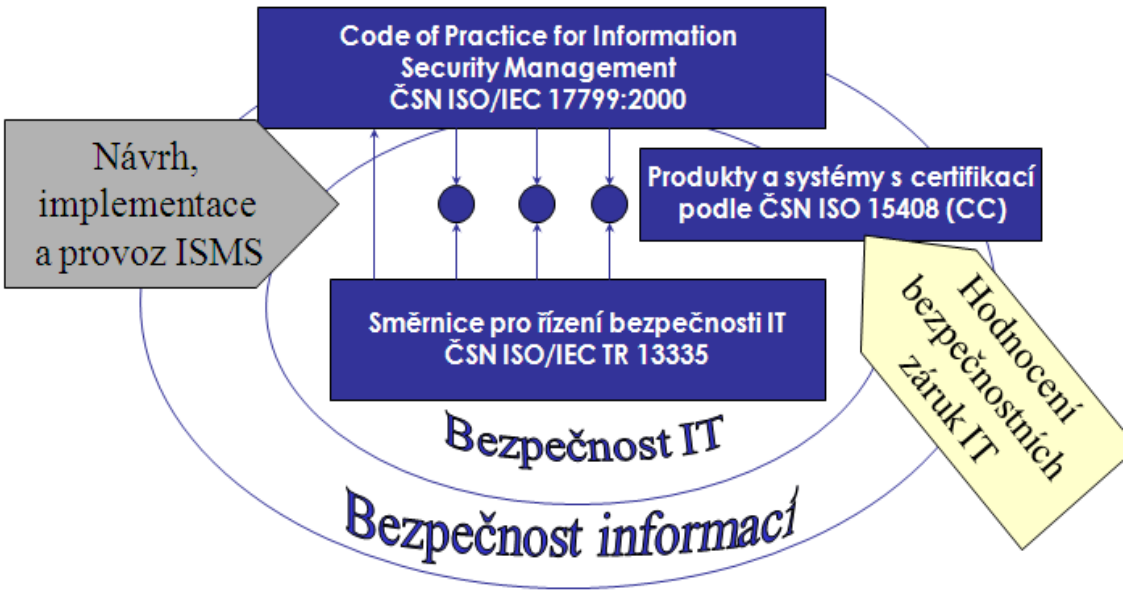
ISO/IEC 27005, řízení rizik;

ISO/IEC 27006, kontinuita podnikání a obnova po havárii.

ISO/IEC 27001:2005 je vhodná pro všechny typy organizací, komerční firmy, státní organizace, nevýdělečné společnosti a další. Popisuje požadavky pro celý životní cyklus systému řízení informační bezpečnosti a pro všechny okruhy souvisejících aktivit. Norma chápe organizaci ve vazbách na její okolí a je použitelná pro řadu účelů, například pro vnitřní hodnocení a řízení rizika, zajištění požadavků zákonů a předpisů, nalezení a definici bezpečnostních procesů, zjištění a hodnocení souladu s firemními politikami a regulemi, jako kritérium pro interní i externí auditovaní, prokazování bezpečnostních vlivů na zákazníky, pro přípravu a certifikaci třetími stranami a v neposlední řadě také pro řízení efektivnosti nákladů na zajištění bezpečnosti informací.[2]

V dnešní době nejmodernější užívanou směrnicí je ISO/IEC 27007 - doporučení pro auditování ISMS.

Lze doporučit také normu ISO 15408, známou svým termínem „Common Criteria“, označovanými jako CC. Jedná se o metodu hodnocení bezpečnostních vlastností produktů a systémů IT, i když je nutno počítat s poměrně úzkým zaměřením na počítačová zařízení a software.



Obr. 3. Hodnocení informační bezpečnosti

Tab. 2. Historický vývoj norem informačních systémů [3]

Rok vydání	Slovník ISMS	Požadavky ISMS	Soubor postupů	Implementace ISMS	Měření účinnosti	Řízení rizik	Certifikační schéma	Audit ISMS
1995			BS 7799					
1996	ISO/IEC TR 13335-1							
1997	ISO/IEC TR 13335-2							
1998						ISO/IEC TR 13335-3	c:cure	
1999		BS 7799-2	BS 7799-1				EA7/03	
2000			ISO/IEC 17799			ISO/IEC TR 13335-4		
2001						ISO/IEC TR 13335-5		
2002		BS 7799-2 v2						
2003								
2004	ISO/IEC 3335-1							
2005		ISO/IEC 27001	ISO/IEC 17799 v2			ISO/IEC 13335-2 převedeno na ISO/IEC 27005		
2006						BS 7799-3		
2007			ISO/IEC 27002				ISO/IEC 27006	
2008						ISO/IEC 27005		
2009	ISO/IEC 27000			ISO/IEC 27003	ISO/IEC 27004			
2010								ISO/IEC 27007

II. PRAKTICKÁ ČÁST

5 UVEDENÍ PROBLEMATIKY PRAKTICKÉ ČÁSTI

Cílem praktické části bakalářské práce bude vytvoření bezpečného prostředí z hlediska správy informací pro reálnou střední organizaci, která si nepřeje být jmenována. Provedena bude analýza současného stavu informační bezpečnosti, proběhne zhodnocení rizik, které za současného stavu v organizaci hrozí a navrhnu nové řešení zabezpečení informací sítě a dat. Práce bude obsahovat také inovace, které lze v budoucnu v organizaci uplatnit.

5.1 Popis reálné organizace

Pro bakalářskou práci byla zvolena organizace střední velikosti zabývající se vytvářením a propagací reklamy. Organizace je rozdělena do dvou budov z důvodu nenalezení vhodných prostor. V jedné z budov je sídlo technického týmu, který se stará o samotnou vizuální či verbální tvorbu a realizaci reklam a v druhé budově pracuje marketingový, finanční a personální tým s vrcholovým vedením organizace. Pro organizaci je důležité zejména udržení důvěryhodnosti před svými zákazníky, udržení svého know – how, bezpečnou správu dat a interních postupů a v neposlední řadě ochrana informací o aktuální finanční situaci organizace. Na stanicích jsou shromažďovány veškerá data o provedených a připravujících se kampaních, data týkající se kompletního portfolia partnerů a zákazníků a samozřejmě data o zaměstnancích a finanční situaci organizace.

5.2 Analýza stavu organizace

Momentálně je v organizaci zaměstnáno 80 lidí i s vedením, každý z těchto zaměstnanců vlastní pevnou nebo přenosnou počítačovou stanici. Jelikož jsou zaměstnanecké týmy v různých budovách, jejich spolupráce funguje z 80% v emailové formě nebo pomocí sociálních sítí. Organizace si je vědoma rizik, která ji hrozí a bere v potaz, že současné řešení informační bezpečnosti naprosto nevyhovuje dnešním požadavkům. Částka vyhrazená na vytvoření informační bezpečnosti v organizaci byla stanovena přibližně půl milionu korun. Proto bude navrhnuto řešení zabezpečení tak, abychom se do tohoto rozpočtu vlezli a až posléze bude navrhnuto řešení, které by organizaci ochránilo velmi kvalitně téměř před každou hrozbou.

5.3 Postup řešení zabezpečení informačního systému

Jelikož existuje určitý finanční limit, který je ochotna organizace investovat do zajištění informační bezpečnosti, není možné docílit naprosto dokonalého řešení. Také je třeba vzít v potaz, že organizace zvoleného typu nevyžaduje takový stupeň bezpečnosti jako třeba armáda české republiky. Proto jedním z cílů této práce bude dokázat, že kvalitní zabezpečení dat a sítě organizace se dá vytvořit i s finančním limitem.

Zvolený postup:

- Audit informačního systému.
- Vyhodnocení hrozících rizik.
- Implementace samotného řešení.
- Řešení a možné inovace bez omezení finančního rozpočtu.

6 AUDIT STAVU INFORMAČNÍHO SYSTÉMU ORGANIZACE

Audit je systematický, nezávislý a dokumentovaný proces získání důkazů z auditu a jejich hodnocení s cílem stanovit rozsah splnění kriterií auditu [4].

6.1 Rozbor systému, sítě a počítačového vybavení

Při rozboru současného stavu informační sítě konkrétní organizace byly zjištěny tyto skutečnosti:

Tab. 3. Základní údaje o organizaci

Pevné počítačové stanice:	**70**
Přenosné počítačové stanice (notebooky):	**10**
Počet tiskáren:	**20**
Operační systém:	**Microsoft Windows XP Professional**
Použitý typ sítě:	**Peer to peer**
Připojení k internetu:	**bezdrátový spoj, 4MBit příchozí i odchozí**
Používaný typ internetového prohlížeče:	**Internet Explorer verze 5 a 6**
Typ poštovního klienta:	**Microsoft Office Outlook Expres**

6.2 Stav antivirového a firewallového softwaru

Používaný antivirový software je AVG.

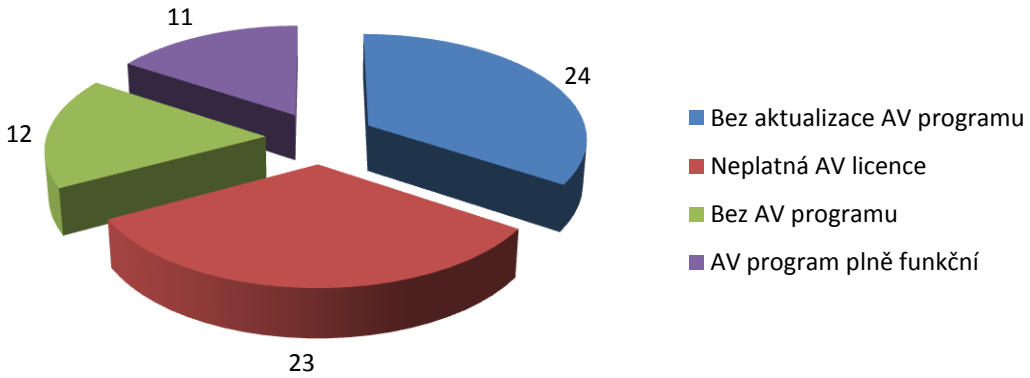
Používaný firewallový software: starý hraniční firewall na principu Linuxu bez paketových filtrů a kontroly IDS.

6.2.1 Antivirový program používaný v organizaci

I přes použití antivirového programu AVG, tak jeho nasazení na stanicích bylo v drtivé většině neefektivní nebo byl v nefunkčním stavu. Vysoký počet stanic byl bez platných licencí a našli se i stanice bez antivirového programu. I když tento program na stanici byl v provozu, neprobíhala jeho pravidelná aktualizace, protože bylo na každém z uživatelů, zda aktualizace provede. Tento volný způsob aktualizace vedl k tomu, že antivirové programy nebyly aktualizovány vůbec. Aktuálně lze stav antivirového programu procentuelně vyjádřit dle níže uvedeného grafu.

Tab. 4. Stav antivirového programu pevných stanic

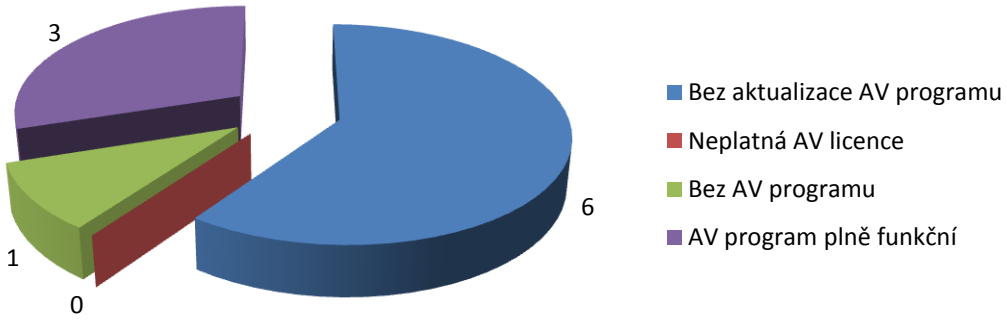
70	Bez aktualizace AV programu	Neplatná AV licence	Bez AV programu	AV program plně funkční
Pevné stanice	**24**	**23**	**12**	**11**



Obr. 4. Stav antivirového programu pevných stanic

Tab. 5. Stav antivirového programu přenosných stanic

10	Bez aktualizace AV programu	Neplatná AV licence	Bez AV programu	AV program plně funkční
Přenosné stanice	**6**	**0**	**1**	**3**



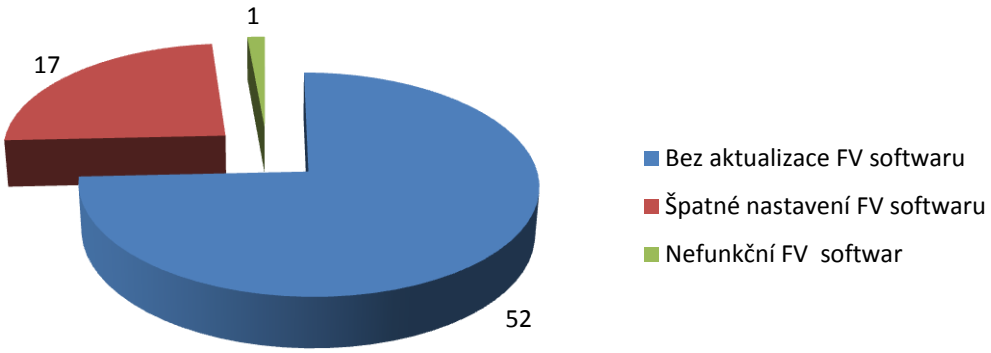
Obr. 5. Aktuální stav antivirového programu přenosných stanic

6.2.2 Firewallový software používaný v organizaci

S analýzou antivirového programu probíhala současně i kontrola stavu firewallového softwaru. Jako původní hraniční firewall sloužil u všech stanic obyčejný neznačkový typ firewallu na principu Linux 2.4 bez stavových paketových filtrů, bez kontroly protokolů IDS a na mnoha stanicích byl firewall špatně nastaven.

Tab. 6. Stav firewallového softwaru na pevných stanicích

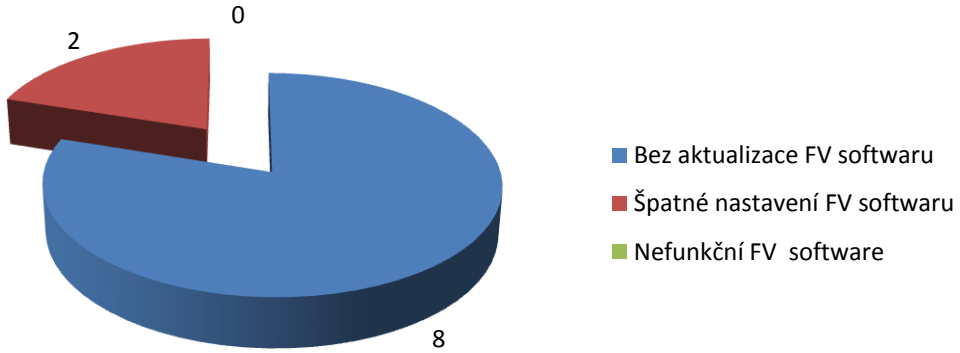
70	Bez aktualizace FV softwaru	Špatné nastavení FV softwaru	Nefunkční FV software
Pevné stanice	**52**	**17**	**1**



Obr. 6. Stav firewallového softwaru na pevných stanicích

Tab. 7. Stav firewallového softwaru na přenosných stanicích

10	Bez aktualizace FV softwaru	Špatné nastavení FV softwaru	Nefunkční FV software
Přenosné stanice	**8**	**2**	**0**



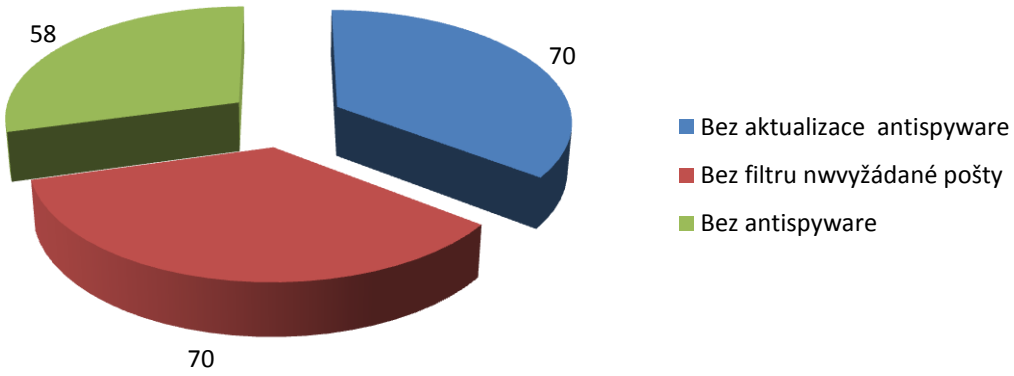
Obr. 7. Stav firewallového softwaru na přenosných stanicích

6.3 Poštovní kurýr, antispyware

Organizace jako poštovního kurýra využívala program Microsoft Outlook Expres bez filtru nevyžádané pošty. I když email patří mezi téměř stále využívané programy ani na jedné ze stanic neprobíhala jeho aktualizace. Není vytvořeno centrální úložiště pošty, ale je ukládána pouze v dané stanici. Antispyware využívala pouze malá část stanic.

Tab. 8. Stav poštovního kurýra a antispyware na pevných stanicích

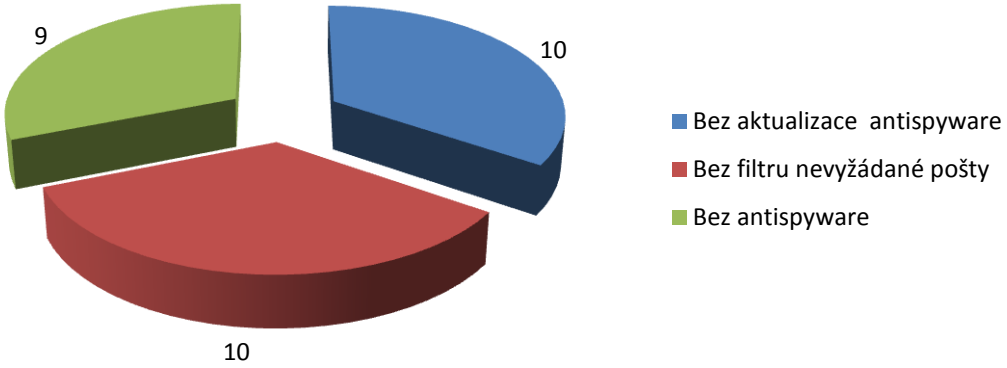
70	Bez aktualizace antispyware	Bez filtru nevyžádané pošty	Bez antispyware
Počet pevných stanic	**70**	**70**	**58**



Obr. 8. Stav poštovního kurýra a antispyware na pevných stanicích

Tab. 9. Stav poštovního kurýra a antispyware na přenosných stanicích

10	Bez aktualizace antispyware	Bez filtru nevyžádané pošty	Bez antispyware
Počet přenosných stanic	10	10	9



Obr. 9. Stav poštovního kurýra a antispyware na přenosných stanicích

6.4 Zálohování dat, použití hesel, tiskárny

Bylo zjištěno, že většina dat, se kterými se pracuje, není zálohována a jsou ukládána pouze na interních harddiscích stanic. Pokud zálohy probíhaly, tak na CD nebo externí harddisky. Všechny uživatelské účty byly chráněny heslem. Jednalo se ovšem o hesla jednoduchá bez speciálních prvků a neprobíhalo časové nastavení obměny hesla. Polovina z přenosných stanic byla vybavena biometrikou otisku prstu, ale této služby využívali pouze dva z uživatelů. Jedenáct tiskáren bylo nastavených jako sdílené a zbylých osm bylo připojeno přímo k síti.

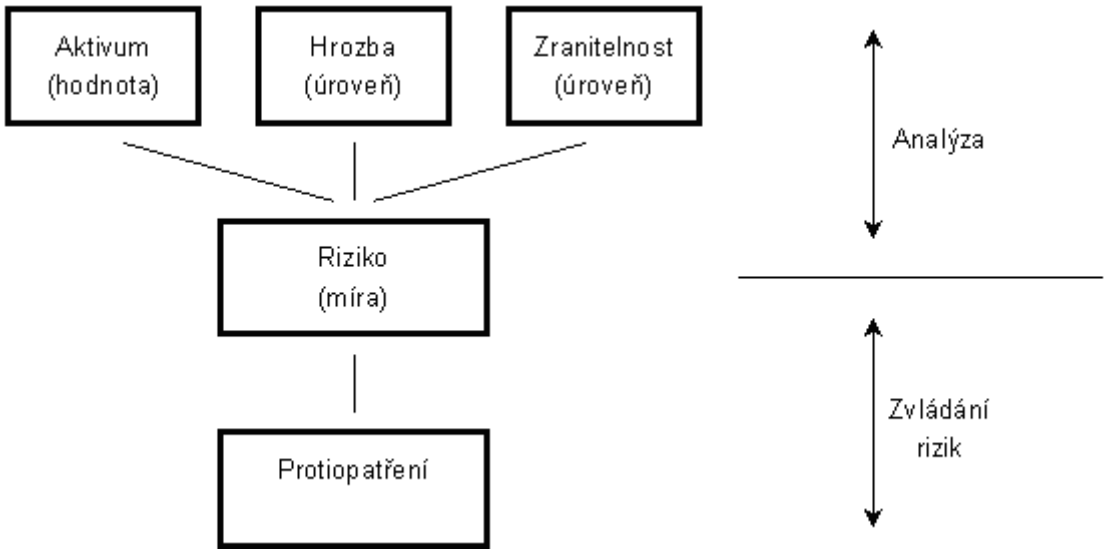
6.5 Komplexní vyhodnocení auditu

Po vyhodnocení všech posuzovaných kritérií bylo zjištěno, že používané řešení informační bezpečnosti je naprosto nevyhovující a dalo by se srovnat s průměrným zabezpečením běžného domácího uživatele. Za největší nedostatek byl určen typ sítě peer to peer. Naprosto neexistuje řízení oprávnění, kontrola uživatelských účtů, což má za následek, že veškeré programy a nastavení musí být instalovány na každé stanici zvlášť. Velkým problémem je také špatné používání a nastavení antivirových programů a firewallého softwaru. Chybí jakákoliv aktualizace software i hardware, tím pádem je používaný systém zastaralý a neefektivní. Organizace nemá vedenu žádnou evidenci majetku a postrádá jakoukoliv dokumentaci. Není počítáno s možnou neúmyslnou nebo úmyslnou ztrátou dat.

7 ANALÝZA RIZIK KONKRÉTNÍ ORGANIZACE

Organizace si je vědoma, že existují určitá rizika, která jí hrozí, a není proti nim dostatečně chráněna. Nikdy nebyla provedena analýza rizik. Chybí jakákoliv dokumentace, která by určovala směrnice a opatření proti možným rizikům.

Ať je zvolen kterýkoliv ze způsobů vytváření analýzy rizik, měla by být vždy podle postupu uvedeného na schématu obrázku 3.



Obr. 10. Schéma analýzy rizik [5]

7.1 Aktiva organizace

Za aktiva dané konkrétní organizace jsou považovány hlavně informace, se kterými se pracuje, data, která shromažďuje a majetek.

Jako hlavní aktiva organizace byly zvoleny tyto prvky:

- Know – how.
- Veškeré připravované i hotové projekty.
- Smlouvy a data svých klientů.
- Informace ohledně finanční situace.
- Informace personálního charakteru.
- Emailová databáze.

Se všemi těmito aktivy by mělo být zacházeno s maximální opatrností, přístup k nim by měl mít pouze majitel organizace nebo zodpovědný zaměstnanec a měla by být chráněna proti jakémukoliv zneužití, odcizení či nehodě.

7.2 Rizika hrozící organizaci

Organizací hrozí vysoká škála rizik, některá z nich jsou vzhledem k výsledku auditu velmi nebezpečná a aktuální a jiná jsou nebezpečná méně. Bylo vyhodnoceno, že organizaci hrozí spíše rizika interního typu nežli napadení zvenčí.

7.2.1 Rizika úmyslná

- Interní krádež nebo zneužití informací a dat.
- Konkurenční špionáž.
- Útoky a možné vyřazení systému z provozu.
- Úmyslné pošpinění dobrého jména organizace.

7.2.2 Rizika neúmyslná

- Nechtěné smazání důležitých dat.
- Selhání či opotřebení techniky.
- Chyby a opomenutí zaměstnanců.
- Špatná konfigurace systému.

7.2.3 Rizika přírodního rázu

- Požár.
- Zemětřesení.
- Elektrický výboj.

7.3 Hodnocení uvedených rizik a ochrana proti jejich účinkům

- **Interní krádež nebo zneužití informací a dat** - jedná se krádež informací či dat, kterou provedl přímo zaměstnanec organizace. Všichni zaměstnanci mají v pracovní smlouvě uvedeno, že nesmí zneužívat interní data a také předávat know – how organizace třetím stranám. Data mohou mít různý charakter, ale je téměř zaručeno, že mohou organizaci způsobit obrovské újmy. Jedná se o vysoké riziko s vysokou prioritou.
- **Konkurenční špionáž** – v organizaci probíhají často schůzky s klienty, není zaručeno, že by se mohlo jednat o fiktivního klienta, který chce pouze zjistit cenovou nabídku pro srovnávací účely. V horším případě je možné, aby odcizil citlivá data přímo z některé ze stanic, protože v organizaci není zaveden kamerový systém a používané hesla do stanic jsou špatně nastavena a není těžké je prolomit. Jedná se o středně vysoké riziko se středně vysokou prioritou.
- **Útoky a možné vyřazení systému z provozu** – organizace je připojena k internetu, tím pádem jí hrozí základní rizika jako napadení viry, pokusy o nakažení pošty, přesměrování IP adresy a mnoho dalších. Jedná se o vysoké riziko s vysokou prioritou.
- **Úmyslné pošpinění dobrého jména organizace** – jelikož má organizace ve městě svého sídla dva téměř rovnocenné konkurenty, existuje mezi nimi určitá rivalita. Zatím situace, že by se někdo pokusil jméno organizace pošpinit, nenastala, ale musí se s ní počítat. Jedná se nízké riziko s nízkou prioritou.
- **Nechtěné smazání důležitých dat** – vzhledem k faktu, že organizace nevyužívá centrálního řízení bezpečnostních politik na uživatele je velmi pravděpodobné, že daná situace může nastat. Dokonce bylo zjištěno, že nehody podobného rázu se již několikrát staly. Toto riziko může mít za důsledek dočasné ochromení systému. Jedná se o střední riziko se střední prioritou.
- **Selhání či opotřebení techniky** – protože organizace téměř vůbec nezálohuje data a používaná technika není neopotřebitelná a nerozbitná je toto riziko pro ni velmi aktuální. Jedná se o vysoké riziko s vysokou prioritou.

- **Chyby a opomenutí zaměstnanců** – zaměstnanci nejsou bezchybní a ani neomylní. Vzhledem k tomu, že velká většina zaměstnanců není proškolena nebo poučena, jak udržet informační bezpečnost existuje riziko nedbalosti, kterou si zaměstnanec nemusí uvědomovat. Jedná se o střední riziko se střední prioritou.
- **Špatná konfigurace systému** – opět se vyskytuje problém se zavedenou sítí peer to peer, je pouze na rozhodnutí uživatele zda bude aktualizovat systém nebo ne. Ti na aktualizace nedbají a tím je riziko úspěšného napadení mnohem vyšší. Jedná se o vysoké riziko s vysokou prioritou
- **Požár** – pokud by vypukl požár v jedné z budov organizace, některá data by mohla být zničena nadobro, jelikož neexistují zálohy dat, některá data by mohla být obnovena, jelikož se s nimi pracuje i ve druhé z budov. Jedná se o střední riziko se střední prioritou.
- **Zemětřesení** – organizace se nenachází v místech seismologické aktivity, avšak vystává stejný problém jako u požáru, může se stát, že budou mechanicky zničena data. Jedná se o nízké riziko s nízkou prioritou.
- **Elektrický výboj** – toto riziko je vzhledem k jeho charakteru pro organizaci aktuální a z rizik přírodního rázu nejvíce pravděpodobné. Dokáže zničit jak data, tak i techniku. Může přijít nečekaně, umí napáchat vysoké škody, ale je možné se před tímto rizikem plnohodnotně bránit. Jedná se o vysoké riziko s vysokou prioritou.

7.4 Možná protiopatření

O možných konkrétních protiopatřeních z hlediska hardware a software bude pojednávat další kapitola zaměřená na inovace informačního systému. V této části bych chtěla rozebrat možná protiopatření z hlediska zaměstnanců a pohybu osob v budovách.

Pro minimalizaci interních a neúmyslných hrozeb je důležité seznámit zaměstnance o možných hrozbách a informovat je, jak se mají chovat, aby tyto hrozby eliminovali nebo v případě, kdy dané riziko nastane co dělat, aby následky byly minimální.

Tato protiopatření by měla být prováděna:

- Formou školení zaměstnanců.
- Formou team buildingu – zvýšení loajality zaměstnanců.
- Seznámení zaměstnanců s možnými následky rizik a co to pro ně znamená.

Aby se co nejefektivněji zamezilo možnému napadení zvenčí, jsou organizaci doporučena tato opatření:

- Kvalitnější hardwarové a softwarové řešení systému
- Umístění kamer před vchod organizace, aby byl monitorován pohyb lidí.
- Uložení nejdůležitějších dokumentů a smluv na bezpečném místě mimo organizaci.

Celá analýza aktiv a rizik v organizaci, hodnocení těchto rizik i protiopatření proti nim by mělo být řádně zdokumentováno. Tato dokumentace by měla být považována za přísně tajnou a přístupná by měla být pouze vedení organizace a odpovědným zaměstnancům.

8 NÁVRH BEZPEČNOSTNÍCH INOVACÍ INFORMAČNÍHO SYSTÉMU

Po prověření aktuálního stavu a funkčnosti informačních prvků používaných a zhodnocení možných rizik v organizaci, se tato kapitola práce bude zabývat možnými inovacemi, které dokáží pomoci eliminovat nedostatky a dostatečně chránit data před zneužitím či napadením. Inovace budou rozděleny do tří skupin podle jejich charakteru. Cílem bude navrhnutí co nejefektivnějšího řešení a pokusit se splnit finanční limit.

Je nutno podotknout, že se jedná pouze o návrh inovací a záleží pouze na vedení organizace, zda přijme některá z těchto opatření za svá.

8.1 Návrh vnitřních bezpečnostních inovací

Při zpracování analýzy rizik bylo zjištěno, že v organizaci je mnohem vyšší riziko vnitřního charakteru. Proto musí být navrhnuta opatření, která organizaci ochrání před zneužitím a ztrátou interních dat.

8.1.1 Využití doménového řadiče a jeho funkce

Nyní využívaný typ sítě peer to peer byl hodnocen jako značně nepraktický a proto je vhodné jej vyměnit za řešení s využitím doménového řadiče. Jedná se o software, který obsahuje mnoho funkcí. Největší výhodou tohoto řešení je mnohem jednodušší instalace aplikací na stanice podle skupin uživatelů. Všechny aplikace mohou být instalovány a řízeny z jedné stanice. Obsluha doménového řadiče by měla být řádně proškolena a seznámena s jeho funkcemi a řízením. Přístup k němu by měl mít pouze administrátor sítě.

Funkce doménové řadiče vhodné pro organizaci:

- Nastavení uživatelských skupin a aplikace bezpečnostní politiky na tyto skupiny.
- Vzdálená kontrola uživatelů a jejich činnosti na stanicích.
- Omezení přístupu na určité webové stránky.
- Nastavení nutnosti užívání silných hesel s obměnou po devadesáti dnech, přičemž hesla se nesmějí opakovat.

8.1.2 Ochrana před ztrátou dat

Pokud vznikne situace, při které by mohla být zničena data, jak díky nedbalostí zaměstnance nebo technickou závadou, měly by existovat zálohy těchto dat, aby mohla proběhnout jejich celková nebo alespoň částečná obnova. Této organizaci je doporučeno využít inkrementální zálohování, protože nezabere tolik místa jako třeba úplné zálohování. Je vhodné zvolit každodenní ukládání rozdílných dat.

Dalším způsobem jak ochránit data je vytvoření centrálního úložiště pošty na serveru a využití poštovního klienta. Toto řešení je nejvíce oceněno v případě, kdy dojde k nechtěnému smazání důležitého emailu nebo ztracení dat z důvodu technické závady. Pro organizaci bylo vybráno síťové úložiště s označením NAS (Network Attached Storage). Aby mohlo síťové úložiště v pořádku pracovat a stanice byly chráněny před nevyžádanou poštou je doporučeno nainstalovat plnohodnotný program Microsoft Office Outlook s využíváním bezpečnostních záplat.

Velmi důležité nebo tajné dokumenty a zálohované data je vhodné uložit do bankovního trezoru, tam budou chráněna před krádeží nebo rizikem přírodního rázu jako požár, povodeň apod.

8.2 Návrh vnějších bezpečnostních inovací

Navrhnutá opatření by měla organizaci chránit před útoky „Hackerů“, nechtěné špionáže konkurence, nemožnost zneužití dat při ztrátě přenosné stanice. Bylo zjištěno, že organizaci hrozí spíše rizika vnitřního typu, ale i vnějším rizikům je potřeba věnovat vysokou pozornost, jelikož napadení zvenčí může mít pro organizaci drtivé účinky, možná až likvidační.

8.2.1 Antivirové a firewallové řešení

Jelikož současný stav nastavení antivirových programů a firewallu je téměř nefunkční je potřeba provést nově kompletní instalaci a konfiguraci těchto systémů. Mnoho počítačů nemělo platnou licenci antivirového programu, proto je potřeba chybějící licence dokoupit, aby mohl program v pořádku pracovat. Současný antivirový program AVG je pro účely organizace plně dostačující a není důvod zavádět tento program od jiného výrobce.

Je žádoucí výměna stávajícího základního hraničního firewallu za kvalitní integrovaný firewall s paketovými filtry, kontrolou protokolů a IDS. Integrovaný firewall lze využít i u přenosných stanic.

8.2.2 Způsob aktualizace systému

Pro kvalitnější a mnohem jednodušší práci s aktualizacemi celého systému organizace je vhodné zvolit řešení s využitím centrální správy aktualizací. Využívá možnosti řízeného způsobu aktualizace bez možnosti uživatele rozhodovat, zda bude či nebude chtít aktualizaci provádět na stanici v daný čas. Jedná se o velmi dobrý způsob jak centrálně zabezpečit zvyšování slábnutí a tím i stárnutí systému.

8.2.3 Ochrana před krádeží dat

U přenosných stanic je vhodné využívat ověření uživatele na základě otisku prstu a hesla. Aby byla data na přenosných stanicích opravdu dobře chráněna, je vhodné nainstalování software na šifrování harddisku.

Pevné i přenosné stanice by měli mít k dispozici software na šifrování pošty, pro případy kdy dojde k nechtěnému zaslání pošty jinému příjemci nebo v případě krádeže pošty útočníkem.

Dalším z prvků, které organizaci mohou chránit před únikem dat je nainstalování kamerového systému na klíčových místech vstupů do budovy a u vstupu do místnosti se serverem.

8.3 Technické řešení navrhnutých inovací

Organizace nyní využívá svůj server, který nestačí na zvládnutí všech navrhovaných inovací, proto bude třeba zakoupit server nový a výkonnější. Protože by byla škoda původní server nevyužít, může být použit pro správu doménového řadiče, aktualizací, antiviru a jako centrální úložiště pošty. Nový server by měl mít čistě zálohovací funkci. Oba servery by měli být umístěny v samostatné uzamykatelné místnosti s klimatizací a hasicím přístrojem. Klíč k ní by měl mít z důvodu bezpečnosti pouze omezený počet lidí.

Nutností je zakoupení všech potřebných licencí, aby mohl systém fungovat naprosto plnohodnotně a legálně. Je známo, že právě koupě těchto licencí je finančně nejnáročnější prvek inovací a finance do nich vkládané nejsou pouze jednorázového typu. Většinou bývají licence kupovány s platností jednoho roku.

Aby dané inovace byly efektivní a byla přesně dána pravidla jejich využívání, je třeba provést kompletní dokumentaci informačních systémů a stanovit směrnice, které budou závazné pro všechny zaměstnance a přesně vymezí pravidla používání firemních prostředků. Pro okamžitý přehled o majetku v organizaci je vhodné zavést jeho evidenci.

Jelikož v organizaci není informační technik takových znalostí, aby dokázal tyto inovace plnohodnotně zavést, a postarat se jejich bezchybnou implementaci v organizaci je třeba vytvořit poptávku na realizaci těchto inovací a posléze si vybrat správnou organizaci s kvalitními informačními techniky zabývajícími se touto problematikou pro realizaci těchto inovací.

9 MODERNÍ PRVKY KE ZVÝŠENÍ INFORMAČNÍ BEZPEČNOSTI

V této části práce budou uvedeny efektivní inovace, které mohou být použity u jakékoliv organizace bez ohledu na jejich charakter, ale jsou značně finančně náročné, proto mohou být využívány hlavně u organizací vyžadující maximální informační zabezpečení.

9.1 HoneyPots

Mezi moderní techniky jak eliminovat nebezpečí, které hrozí ze strany hackerů je nasazení HoneyPots. Jedná se o systém, který přitahuje potencionální útočníky. K tomuto účelu jsou používány například pro útočníka atraktivní DNS názvy. Funkcí tohoto systému je vytvořit imaginární produkční systém či dokonce celou produkční síť, na který se naláká útočník. Cílem je poučit se od nepřítele a podle jeho kroků inovovat zabezpečení systému. Tento software má samozřejmě i své nevýhody a to, že nemusí nalákat opravdové útočníky.

Tento program by měla obsluhovat plně zaškolená a provozu schopná osoba, pokud by tomu tak nebylo, nemusel by program mít takové účinky.

Existují dva druhy programů pracující na principu HoneyPots, jsou jimi:

- **Low-Interactive** – jde o HoneyPots, který je realizován pomocí softwaru. Výhodou je velmi snadno čitelný výstup, zpravidla v textovém souboru. Naopak nevýhodou může být oproti High-Interactive menší zisk informací o útočníkovi, protože je simulována pouze jistá služba, není mu umožněno ovládnutí celého systému a tak po sobě nezanechá příliš velké množství stop.

- **High-Interactive** – i když se jedná o velice časově i odborně náročnou činnost, pomocí simulace celé sítě na virtuálním stroji nebo přímo na funkční nezabezpečené síti můžeme zjistit motivaci, cíl útočníka nebo způsob jakým za sebou „zametá stopy“. Útočník zanechá mnohem více pozorovatelných stop. Po získání důležitých informací od útočníka je nutné provést hloubkovou analýzu napadeného systému.

9.2 Scannery bezpečnostních chyb

Scannery bezpečnostních chyb jsou velmi užitečnou pomůckou každého kvalifikovaného administrátora. Jedná se o systém, který automaticky vyhledává a reaguje na zranitelná místa v systému, které mohl administrátor přehlédnout a díky dostupným databázím okamžitě vyhledá záplatu na toto zranitelné místo. Je třeba si však uvědomit, že se jedná o velmi silný nástroj a v nekvalifikovaných rukách může způsobit více problémů než pomoci. Jako nevýhoda scannerů bezpečnostních chyb může být považováno automatické a bezhlavé záplatování systému, protože některá místa v síti mohou být ponechána bez ochrany schválně a to tyto scannery nedokážou předvídat.

9.3 Čipové karty a tokeny

Využiti čipových karet nebo tokenů napomůže odbourat problémy se zadáváním hesel, zapamatováním hesel či psaní hesel na papírky, které si zaměstnanci nechávají přilepené na monitorech či pod klávesnicí jejich stanice. Tuto techniku lze také využít u docházkových systémů či povolení a kontrole pohybu zaměstnanců v místnostech budovy. Funkčním ochranným prvkem těchto karet a tokenů je přístup do systému pomocí PINu a v některých případech mají i tzv. PUK. Nezanedbatelným prvkem jejich ochrany je šifrování pomocí algoritmů, jako například AES (Advanced Encryption Standard). U kvalitních čipových karet a tokenů výrobce garantuje, že tajný klíč nikdy neopustí token. Některé tokeny mají dokonce certifikaci „na obal“. Tato certifikace zajišťuje při pokusu útočníka rozebrat token, že veškerá data budou automaticky zničena a jeho obal se roztříští na malé kousky.

V dnešní době se již s využíváním čipových karet můžeme setkat běžně, ale obecně se do budoucna počítá s mnohem větším rozšířením tokenů, z důvodu jejich malé velikosti, přenosnosti bez čtečky a možnosti „připoutání tokenu k tělu“.

9.4 Kvalitní biometrika

Skutečně kvalitní biometrika je nejspíše nejbezpečnější způsob jak rozeznat uživatele na stanici. Nejbezpečnější, protože nezkoumá znalost hesla nebo vlastnictví čipu, ale nezaměnitelnou vlastnost uživatele. Ověřování zaměstnanců pomocí biometriky je dnes již hodně využívaným a rozšířeným prvkem v organizacích. U počítačových stanic je hojně využíváno rozpoznávání uživatele pomocí otisku prstu. Avšak za kvalitní biometriku se

snímání otisku prstu nepovažuje. Mezi kvalitní biometrické prvky lze zařadit třeba čtečku na snímání oční sítnice. Ovšem je nezbytné, aby taková čtečka nesnímala pouze sítnici, ale také lesk oka, aby se zamezilo jejímu možnému zfalšování. Je nutné dodat, že se jedná hlavně o vnitřní zabezpečení, které chrání organizaci před interní krádeží či zneužití dat.

9.5 Prověřování znalostí zaměstnanců

Ověřování zaměstnanců by měl mít na starosti administrátor sítě. Protože útočníci jsou vždy jeden rok dopředu oproti odborníkům a databázím, které proti nim bojují, je možné ověřovat znalosti zaměstnanců. Jedná se o občasné prověřování znalostí a loajality zaměstnanců vůči organizaci. Je mnoho způsobů, jak ověřit zkušenosti a reakce zaměstnanců na určitou hrozbu. Mezi ně se řadí:

- Administrátor vyšle falešné nakažené poštovní zprávy a kontroluje, jak budou zaměstnanci s tímto spamem nakládat.
- Jedním ze způsobů kontroly zaměstnanců může být infikace stanic virem a čekání, za jak dlouhou dobu, a zda vůbec si zaměstnanci této skutečnosti všimnou. Kontrola rychlosti reakce zaměstnanců na nestandardní chování stanice.
- Lze využít ověřování pomocí dotazníků, ve kterém bude několik modelových situací, a zaměstnanci mají popsat způsob, jak by se při takové mimořádné situaci zachovali nebo jak takové situaci mají předcházet.

Po ukončení prověřování zaměstnanců je na administrátorovi, aby provedl vyhodnocení testu, sdělil zaměstnancům výsledky a uvedl, kteří zaměstnanci a způsob jakým budou proškoleni, aby se do budoucna jejich chyby neopakovaly. Pokud se chyby vyskytnou, je žádoucí, aby byl o této skutečnosti administrátor okamžitě informován a byla přijata konkrétní opatření.

9.6 Pokročilá ochrana notebooku před zloději

Na českém trhu se letos objevil software, který dokáže kvalitně ochránit notebook před zloději a nechtěným zneužitím dat. Notebook je napojen a kontrolován techniky v monitorovacím centru společnosti poskytující tyto služby. Ve chvíli odcizení se dá okamžitě zablokovat a popřípadě i zničit data na něm uložená. Tato služba je cenově dostupná téměř pro každého člověka, lze si ji předplatit vždy na určité časové období dopředu, jako pojistka. Proto se očekává její budoucí masivní rozšíření. Pomocí SIM karty, která bude v notebooku vložena, lze lokalizovat jeho aktuální polohu na mapě a tak i určit, kde se zloděj s ním právě nachází.

Funkce softwaru:

- **Časovač** – notebook je evidován v monitorovacím centru. Časovač sleduje, zda se NB připojuje v nastavených intervalech. Pokud se v daném intervalu nepřihlásí je automaticky zablokován. Tuto funkci lze využít v případě zapomenutí počítače v zaměstnání apod.
- **Vzdálená blokace** – notebook může být na dálku zablokován. K odblokování je třeba zadat heslo, které zná jen uživatel.
- **Notebook „vyřazen z činnosti“** – na žádost klienta je možno počítač vyřadit z provozu. Ten se stává nepoužitelným. Operační systém nebootuje.
- **Zadání hesla** – celý software funguje na heslo. Heslo si může uživatel zvolit sám (musí se jednat o silné heslo) nebo v případě zablokování monitorujícími pracovníky pro jeho opětovné odblokování bude automaticky vygenerováno heslo nové.
- **Lokalizace notebooku** – lze jej lokalizovat na mapě a tak i sledovat, kde se notebook právě nachází.

ZÁVĚR

Cílem této práce bylo uvedení možných způsobů ochrany informační bezpečnosti organizace. Zaměřila jsem se na řešení z hlediska software a hardware, druhu uživatele na stanici a charakteru organizace. Proběhlo seznámení s normami používanými v informatice.

Pro vytvoření efektivního informačního zabezpečení je potřeba zhodnotit stav stávajícího systému a uvést rizika, která mohou organizaci hrozit. Na základě výsledku tohoto rozboru může organizace přijmout odpovídající opatření. Jelikož bývá vysoké riziko interních hrozeb, je zapotřebí důkladné proškolení a seznámená zaměstnanců s danou problematikou.

Jak jsem se sama mohla přesvědčit u své pokusné organizace, tvorba takového projektu na vytvoření informační bezpečnosti není lehká záležitost a neměl by jej člověk dělat sám. Provedla jsem analýzy systému a navrhla možný způsob, jak docílit kvalitního zabezpečení, ale většina takovýchto zásahů do systému by měla být prováděna skutečnými odborníky, aby mohla opatření fungovat správně a efektivně.

Ověřila jsem si, že mnoho organizací ještě dnes značně podceňuje problematiku informačního zabezpečení a spoléhá na rčení: „Mě se to stát nemůže“. Opak je tomu pravdou. Hrozby jsou stále silnější a mají vyšší následky někdy i pro organizaci likvidační. Chránit svůj počítač před hrozbami by měl každý uživatel bez ohledu, zda se jedná o domácí stanici či firemní síť stanic.

Čím vyšší požadujeme procento bezpečnosti a ochrany, tím úměrně roste i cena za tyto služby. Opravdu kvalitní zabezpečení s eliminací téměř každého rizika si mohou dovolit pouze movité organizace a ty, které musí svá data chránit, protože spravují data klientů a ty podléhají zákonu o ochraně osobních údajů. Tato opatření mohou organizaci stát i miliony korun ročně. Ovšem kvalitního zabezpečení se dá dosáhnout i z nižšího rozpočtu, důležitá je správní instalace a konfigurace systémů.

ZÁVĚR V ANGLIČTINĚ

The aim of this study was the possible ways of protecting information security organizations. I focused on addressing aspects of software and hardware, the type of user station and the nature of the organization. Conducted familiarization with the standard in science.

To create an effective information security is becoming a need to assess the system and noted the risks that may threaten the organization. Based on the results of this analysis, organizations can take appropriate action. Since is a high risk of internal threats, an in-depth training and familiarization of staff with the topic.

How I could convince myself with my trial organization, creating a project to develop information security is no easy matter and it should not make one yourself. I performed the analysis of the system and propose possible ways to achieve quality security, but most such interventions into the system should be implemented by real professionals that can measures work properly and efficiently.

I checked out that many organizations today still greatly underestimate the information security issues and relies on saying: "I could not have happened." The opposite is the truth. Threats are becoming stronger and have greater consequences for the organization and then liquidation. Protect your computer from threats should any user regardless of whether the home station or the corporate network stations.

The higher the percentage of demand and safety, thereby proportionately increasing the price for these services. Really good security with the elimination of nearly every risk you can afford only the affluent and those organizations that must protect their data, because customers manage data and are subject to privacy. These measures may also be the organization millions of crowns annually. But quality security can be achieved from a lower budget, the importance of the installation and configuration management systems.

SEZNAM POUŽITÉ LITERATURY

[1] LUDVÍK, M., Teorie bezpečnosti počítačových sítí. Praha: Computer media, 2008. 98 s. ISBN 978-80-86-686-35-6

[2] KOSTIHA, F., Bezpečnost informací. *Ikaros* [online]. 2006, 5, [cit. 2010-05-07]. Dostupný z WWW: <http://www.ikaros.cz/node/3332>. ISSN 1212-5075

[3] DOUČEK, P., Řízení bezpečnosti informací. 1. vyd. Praha: Edition, 2008. 239 s. ISBN: 978-80-86946-88-7

[4] ISO 19011: 2003 – Guidelines for quality and/or enviromental management systém auditing

[5] Analýza rizik. IT security [online]. 2009, 1, [cit. 2010-05-09]. Dostupný z WWW: <http://www.it-security.cz/sluzby/analyza-rizik.html>.

[6] BRUCKNER, T., VOŘÍŠEK, J., Outsourcing informačních systémů. 1. vyd. Praha: Ekopress, 1998. 119 s. ISBN: 80-86119-07-6

[7] JAŠEK, R., Informacní a datová bezpecnost. 1. vyd. Academia centrum UTB, 2006. 140 s. ISBN 8073184567

[8] STAUDEK, J., Standardizace bezpečnosti IT. 1 vyd. Fakulta informatiky Masarykovy Univerzity Brno. 2002.

[9] KOLÁČEK, M. Ochrana Vašich dat. Svět hardware [online]. 2009, 1. Dostupný z WWW:<http://www.svethardware.cz/art_doc066ACD02A35E15A1C1257552003C4C06.html>.

[10] Bezpečnostní audit (v čem spočívá, pro koho je určen) Www.westcom.cz : Bezpečnostní audit - Informačních systému a sítí [online]. 1998-2008. Dostupný z WWW: <http://westcom.cz/bezpecnostni_audit.php>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AV Antivir

AES Advanced Encryption Standard

CC Common Criteria

ČR Česká Republika

DC Domain Controller

DNS Domain Name Systém

FW Firewall

IDS Instrusion Detection Systems

IEC Mezinárodní Norma Pro Elektrotechniku

ISO Mezinárodní Norma

IP Připojovací Adresa

IT Informační Technika

OS Operační Systém

PC Počítač

USD Americký dolar

SEZNAM OBRÁZKŮ

SEZNAM TABULEK