UNIVERZITA PARDUBICE

FAKULTA EKONOMICKO-SPRÁVNÍ

BAKALÁŘSKÁ PRÁCE

2009 **Josef Švejcar**

Univerzita Pardubice

Fakulta ekonomicko-správní

Služby ochrany majetku a osob při zajišťování informační bezpečnosti

Josef Švejcar

Bakalářská práce

2009

SOUHRN

Sluťby ochrany majetku a osob jsou jedním z nejefektivnějších způsobů zajištění informační bezpečnosti. Společnosti často využívají alespoň určité prvky z této formy zabezpečení. Nejprve se zabývám informační bezpečností jako takovou, kterou následně realizuji v auditu zjištění informační bezpečnosti ve společnosti Hospital Systems s.r.o. (jedná se o firmu fiktivní vytvořenou na základě podkladů reálné firmy), a následně se zaobírám výhradně sluťbami ochrany majetku a osob. Cílem je zjistit, zda informační zabezpečení ve společnosti Hospital Systems s.r.o. je dostačující a případně navrhnout patřičná opatření.

KLÍČOVÁ SLOVA

Informační bezpečnost, informace, audit, Hospital Systmes s.r.o., sluťby ochrany majetku a osob

TITLE

Services protection of property and persons at locking informative safeness and audit determination informative safeness in select company.

ABSTRACT

Protection services of property and persons are by one of most effective ways security informative safeness. Companies often make use of at least specific component unit from those security forms. At first I deal with informative safeness in itself, which after realize in audit detecting informative safeness in company Hospital Systems Ltd (use fictive created company on the basis source materials realistic company) and subsequently behind pick wholly protection services of property and persons. The aim is find, if informative security in company Hospital Systems Ltd is sufficient and eventually project due arrangements.

KEYWORDS

Information safeness, information, audit, Hospital Systmes with.r.o., services protection of property and persons,

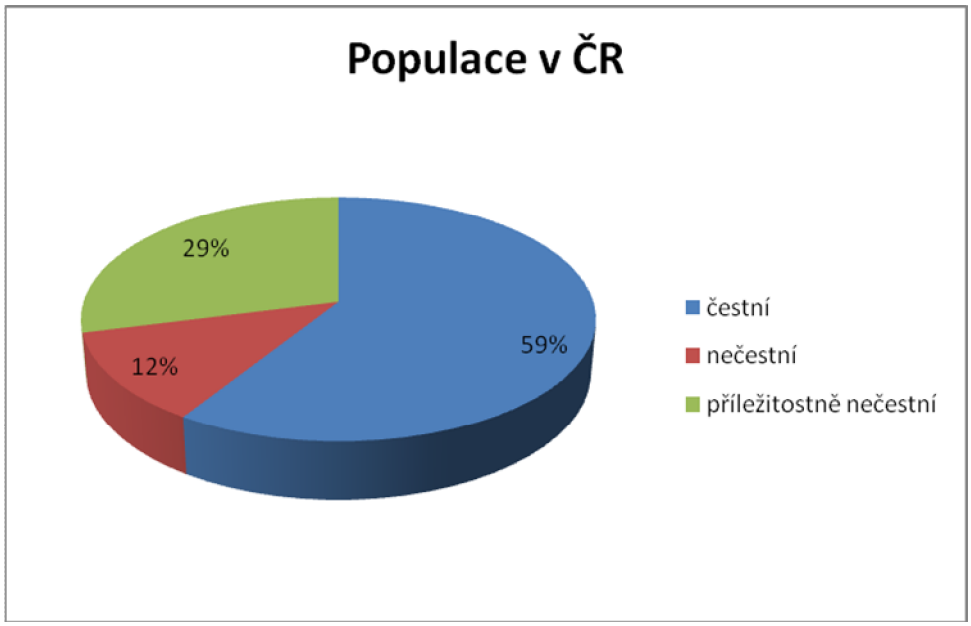
Obsah

1. Informační bezpečnost[1]

Informační bezpečnost je žádoucím stavem každé organizace. V prostředí konkurenčního boje význam informací a práce s nimi stále vzrůstá. Jestliže se firmě podaří pracovat s informacemi efektivněji a účinněji než těm ostatním, získá tak významnou konkurenční výhodu. Pokud jsou informace navíc obohaceny o přidanou hodnotu analytických závěrů, stávají se zbožím s vysokou tržní hodnotou.

Pro organizování, ukládání a využívání informací, stejně jako pro ostatní životně důležitá aktiva, platí, že se musí stát objektem bezpečnosti. Nelze však informace a informační systémy zužovat pouze na informace, k jejichž zpracování, využívání a uchovávání se používají počítačové systémy. Z okruhu informací, které je třeba zabezpečit, nelze vyloučit ty, které jsou uchovávány a přenášeny na přenosných mediích, ani ty v přímo čitelné formě na papíře. Skloubení obou systémů je součástí komplexnosti přístupu k řešení bezpečnosti.

Pokud hovoříme o informacích, nemůžeme pominout ani jejich uživatele. Lidský faktor představuje nerizikovější složku v oblasti informačních systémů a jejich bezpečnosti, jakož ostatně u všech systémů.



Obrázek 1 - statistika čestnosti populace ČR[2]

[1] Rodrýnová, D., Staňa, P. *Bezpečnost informací jako podmínka prosperity firmy*, Grada Publishing, spol. s.r.o., 2000
[2] Ministerstvo spravedlnosti, *http://www.ms.cz/*

Statistika ministerstva spravedlnosti vykazuje každoroční přírůstek trestných činů a tím tedy i zvýšení počtu lidí, kteří jsou nečestní. Kromě zvýšení počtu nečestných lidí dochází i ke zvýšení části populace, která je příležitostně nečestná. Jedná se o lidi, kteří se navenek jeví jako čestní, ale pod tlakem okolností mohou sáhnout k nečestným praktikám. A konečně třetí skupina lidí, přibližně tedy necelé dvě třetiny, jsou lidé čestní. Je tedy důležité zabývat se bezpečností informací a informačních systémů nejen s přihlédnutím k první skupině obyvatel, ale je třeba brát v úvahu i druhou skupinu potenciálně nečestných.

Bezpečnost informací nelze chápat jinak než jako proces, který zahrnuje celou činnost organizace a její aktiva. Nejedná se o produkt, který lze jednoduše zakoupit a nainstalovat. Chybou by také bylo domnívat se, že již jednou vytvořená bezpečnost je řešením jednou provždy. Podmínky, v nichž se informace zpracovávají a uchovávají, se neustále mění a na tyto změny je potřeba neustále reagovat.

1.1 Identifikace aktiv a ohodnocení aktiv[3]

Identifikace aktiv a jejich ohodnocení je součástí analýzy rizik, která je důležitou složkou v tvorbě bezpečnosti. Každá organizace si musí nechat provést analýzu rizik, na základě které se pak bude firma rozhodovat, které informace je nutné chránit a naopak. Informace představuje aktivum společnosti a jako každé aktivum má i informace svojí hodnotu (ohodnocení aktiv). Ocenění informací je velmi složitý a specifický krok pro každou organizaci. Manažeři se často dopouštějí podstatných chyb v ohodnocení informací, a to zvláště proto, že vyjadřují informační hodnotu na základě její finanční hodnoty, ale neuvědomují, že ztráta může být mnohonásobně vyšší (ukradne-li zloděj firemní počítač, vznikne škoda kolem 20 000,- Kč, kterou umí firma zlikvidovat účetně z pojištění. Ztracený počítač poté koupí v nejbližším obchodě, ale po informacích, které byly uloženy v počítači, se už vesele prohání konkurent. Tímto pak vznikají milionové škody).

Je důležité, aby si všichni, kdo s touto informací přijdou do styku, uvědomovali, že manipulují s něčím, co má nemalou hodnotu. Skutečnou hodnotu informací dokáže vyčíslit pouze jedna osoba, a tou je vlastník dat. Ostatní zúčastnění v procesu, což jsou uživatelé informace, musí tuto skutečnost přijmout a chápat svou zodpovědnost za ni v tom okamžiku, kdy je jim informace dána jejím vlastníkem k dispozici. Ohodnocení informace je práce nelehká a nikdo jiný než majitel (vlastník) informací je udělat nemůže. Odborníci

[3] Mlýnek, J. *Zabezpečení obchodních informací,* Computer Press, a.s., 2007

např. na rizikovou analýzu mohou pomoci radou, postupem nebo příkladem, ale pouze majitel je tím, kdo určí konečnou sumu.

Realizace bezpečnosti není nikterak levnou záležitostí a bývá z hlediska organizace investicí s velmi malou prioritou. Za co vynaložit tyto peníze není vždy každému na první pohled jasné. Výhoda vynaložených peněz na zabezpečení informací však není měřitelná jen okamžitým ziskem a návratností investic v nejbližší době. Možná, že se nikdo nepokusí informace zcizit, snad se nikdo nepokusí o to, nabourat se do počítačové sítě a změnit naši prezentaci v neprospěch firmy. Ale čím je atraktivnější výrobní program firmy a čím je silnější konkurence v daném odvětví, tím je to pravděpodobnější. Navíc přírodní živly mohou jakoukoliv organizaci ohrozit kdykoliv a při každé činnosti.

1.2 Ochrana informací v organizaci

Ochrana informací je jedním z primárních úkolů každého subjektu (občana, fyzické či právnické osoby, organizace, instituce apod.). Bez toho nelze docílit informační, a tím i konkurenční výhody.

Základními pojmy v ochraně informací jsou řízení přístupu, přístup k informacím, subjekt a objekt. Řízení přístupu je metoda zabývající se vztahem mezi subjekty a objekty pro zajištění ochrany informací. Jedná se o stěžejní metodu ochrany informací. Přístup je chápán jako přenos informací z objektu do subjektu. Subjekt představuje aktivní entitu, která prostřednictvím přístupu vyhledává informace z objektu nebo o objektu (uživatel, program, proces počítače apod.). Naproti tomu objekt představuje pasivní entita, která obsahuje informace (soubor, databáze, záznamové médium apod.).

Mezi základní funkce řízení přístupu patří preventivní funkce (snaha zabránit nechtěným a neautorizovaným aktivitám), odrazující funkce (snaha odradit od porušení bezpečnostní politiky), detektivní funkce (snaha odhalit nechtěnou, nebo neautorizovanou aktivitu), nápravná funkce (snaha obnovení systému do normálního stavu po výskytu nechtěné, nebo neautorizované aktivity), apod.

Řízení přístupu je nezbytné pro zajištění trojice CIA (Confidentiality, Integrity, Availability), která představuje důvěrnost, integritu a dostupnost. Důvěrnost je princip, že objekty nejsou vyzrazeny neautorizovaným subjektům. Integrita je princip, že si objekty ponechají důvěryhodnost a mohou být úmyslně pozměněny pouze autorizovaným subjektem.

Dostupnost je princip, že autorizovanému subjektu je garantován včasný přístup k objektům, aby mohl provádět požadovanou interakci.

Rozdělení řízení kontroly podle implementace:

- **administrativní implementace** – jsou politiky a procedury definované v bezpečnostní politice organizace (politiky, procedury, praktiky výběru nových zaměstnanců, školení zaměstnanců apod.)
- **logická/technická implementace** – jsou hardwarové softwarové mechanizmy (použití hesel, čipových karet, biometrik, firewallů, routek, apod.)
- **fyzická implementace** – je vytvoření fyzických bariér (ochranka, ploty, detektory pohybu, zámky, světla, psi, alarmy, apod.)

V řízení přístupu se zpravidla nepoužívá pouze jeden mechanizmus, ale tyto mechanizmy se kombinují. Vrstvený způsob řízení přístupu je rozumnější než pevnostní způsob řízení přístupu. Ve vrstveném způsobu řízení přístupu se využívá implementace všech tří typů implementace (administrativní, logická/technická a fyzická).

Obrázek 2 - vrstvený způsob řízení přístupu, zdroj: vlastní

1.2.1 Chráněné informace právním řádem ČR

Je třeba si položit otázku: Které informace je třeba v organizaci chránit? Právní řád České republiky chrání určité informace příslušnými zákony. Jedná se především o „obchodní tajemství“, „zvláštní skutečnosti“, „osobní a citlivé osobní údaje“ a také o „utajované informace“.

1.2.1.1 Obchodního tajemství (provozních a obchodních informací)

Informace o provozech a provozních činnostech, technologiích know-how, obchodních aktivitách apod. jsou ze strany konkurence velice žádané. Jsou cenným zbožím, neboť mají vysokou užitnou, a tím i směnnou hodnotu. Zájmem každé organizace by mělo být tyto informace chránit jako významný majetek, protože jejich zcizení či zneužití může mít za následek obrovské ztráty. Právní řád České republiky umožňuje chránit hmotný a nehmotný majetek před škodlivými útoky, které mohou mít formu rozkrádání, poškození, zkreslení, zneužití, ztráty nebo zničení. Ochranu upravuje jednak Obchodní zákoník, Zákoník práce i Trestní zákon (např. nekalá soutěž, zneužití informací v obchodním styku apod.)

Je nutné, aby obchodní tajemství bylo upraveno v interních normách organizace, aby bylo definováno a zajištěno jeho utajení (přijetím organizačních, režimových a technických opatření k zajišťovací ochrany) a také aby bylo sankciováno porušení těchto interních norem podle pracovněprávních předpisů, zajištěn závazek mlčenlivosti a odpovědnosti za škodu podle pracovněprávních předpisů a upozornění na možnost trestního stíhání případných pachatelů.

1.2.1.2 Zvláštních skutečností[4, 5]

Institut zvláštních skutečností zavedl do právního systému České republiky zákon č.240/2000 Sb. o krizovém řízení a změně některých zákonů (tzv. krizový zákon), a to v ustanovení § 27 zákona. K provádění činností v souvislosti s ochranou zvláštních skutečností zejména v oblasti personální a administrativní bezpečnosti vydala vláda ČR Nařízení vlády č.462/2000 Sb. k provedení ustanovení § 27 odst. 8 a § 28 odst. 5 krizového zákona.

Zákon stanoví působnost a pravomoc státních orgánů a orgánů územních samosprávních celků a práva povinnosti právnických a fyzických osob při přípravě na krizové situace (mimořádné události). Z krizového zákona vyplývá, že organizace, u které se vyskytují písemnosti obsahující „zvláštní skutečnosti“ v oblasti krizového řízení musí být stanoveným způsobem označeny a musí být dodržován zákonem požadovaný režim manipulace s nimi. Zvláštní skutečnosti jsou informace z oblasti krizového řízení, které by v případě zneužití mohly vést k ohrožení života, zdraví, majetku, životního prostředí nebo

[4] zákon č.240/2000 Sb., o krizovém řízení

[5] nařízení vlády č.462/2000 Sb. k provedení ustanovení § 27 odst. 8 a § 28 odst. 5 krizového zákona

podnikatelských zájmů právnických osob nebo fyzických osob vykonávajících podnikatelskou činnost podle zvláštních právních předpisů (viz § 2 krizového zákona). Pracovníci organizace, kteří jsou oprávněni se seznamovat se zvláštními skutečnostmi, musí být zapsáni ve zvláštním seznamu, který schvaluje zaměstnanec orgánu krizového řízení. Povinnost mlčenlivosti je stanovena všem, kteří jsou oprávněni se seznamovat se zvláštními skutečnostmi, a všem osobám, které se s nimi seznámily při plnění úkolů krizového řízení.

V případě ochrany zvláštních skutečností je organizace povinna provést opatření požadovaná zákonem č.240/2000 Sb. o krizovém řízení, a dalšími normami, které zákon rozpracovávají, zejména pak Nařízením vlády č.462/2000 Sb., a to vždy po projednání s příslušným orgánem krizového řízení.

1.2.1.3 Osobních a citlivých osobních údajů[6]

Výchozím dokumentem upravujícím oblasti ochrany informací, obsahující osobní údaje, je zákon č.23/1991 Sb. ze dne 9. ledna 1991, kterým se uvozuje Listina základních práv a svobod. Do nedávné doby poskytoval ochranu osobních údajů zákon č.256/1992 Sb. o ochraně osobních údajů v informačních systémech, který byl zrušen a nahrazen zákonem č.101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů ze dne 4. dubna 2000 (od 1. června je zákon účinný). Ochrana osobních údajů je součástí evropské úmluvy o lidských právech a základních svobodách. Smyslem zákona je dosáhnout toho, aby se s osobními údaji občanů nakládalo jen podle stanovených pravidel, která odpovídají standardům Evropské unie. Zákon je v souladu s direktivou EU a úmluvou Rady Evropy.

Tento okruh chráněných informací se tedy opírá o zákon č.101/2000 Sb. o ochraně osobních údajů. Ochrana osobních údajů je běžnou součástí života moderní demokratické společnosti. Ten, kdo má být chráněn, je jednotlivec, tj. fyzická osoba, o níž osobní údaje vypovídají. Tím, kdo má osobní údaje chránit je každý, kdo osobní údaje zjišťuje, zpracovává, případně uchovává a sděluje jiným subjektům.

Ochrana osobních údajů a citlivých osobních údajů v organizacích nemá význam pouze pro občana (zaměstnance), kterého se týkají, ale má obrovský význam i z hlediska celkové a informační bezpečnosti organizace. Je třeba si uvědomit, že z hlediska celkové bezpečnosti, a informační bezpečnosti zvláště, je nejrizikovějším faktorem právě lidský faktor. Zajištění personální bezpečnosti se bezprostředně dotýká zajištění i ostatních

[6] zákon č.101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů ze dne 4. dubna 2000

bezpeļnostních okruhŢ. Únik osobních údajŢ, a zvlášŧtě pak citlivých osobních údajŢ, mŢže poslouţit konkurenci k zneuţití formou vydírání, korupce apod.

1.2.1.4 Utajované informace[7]

Utajované informace upravuje zákon ļ.412/2005 Sb. o ochraně utajovaných informací a bezpeļnostní způsobilosti.

Vzhledem k charakteru ļinností prováděných organizací a v souvislosti s rozvojem podnikatelských aktivit mŢže vzniknout potřeba poţádat NBÚ (Národní bezpeļnostní úřad) o prověrku, a tím i nutnost zahájit budování ochranných procedur a opatření ve smyslu poţadavkŢ zákona, který utajované informace upravuje. Zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další poţadavky na jejich ochranu, zásady pro stanovení citlivých ļinností a podmínky pro jejich výkon, a s tím spojený výkon státní správy.

Zákon vymezuje zejména informace, které je nutno v zájmu Ļeské republiky utajovat, a s tím související způsob ochrany těchto skuteļností či informací, působnost a pravomoc orgánŢ státu při výkonu státní správy v oblasti ochrany utajovaných informací. Zákon také staanovuje povinnosti orgánŢ státu, práva a povinnosti fyzických a právnických osob, odpovědnosti za poruţení povinností stanovených zákonem. Dále upravuje postavení Národního bezpeļnostního úřadu, vytváří předpoklady pro vzájemné poskytování utajovaných informací v rámci aliance. Pojetí zákona zabezpeļuje přesnou klasifikaci utajovaných informací, jejich ochranu a dispozici s nimi, určuje, kdo a za jakých podmínek se s utajovanými informacemi mŢže seznamovat, a stanovuje takové ochranné mechanizmy, které zajišťují na vysoké úrovni jejich bezpeļnost.

1.2.2 Politika informaļní bezpeļnosti

Bezpeļnostní politika informaļních systémŢ je integrálním prvkem informaļních systémŢ, která zahrnuje technické, fyzické, administrativní, personální, etické, ekologické, právní a sankļní opatření pro přístup a pouţití dat v informaļních systémech. Představuje soubor norem, pravidel a praktik definujících formát informací, jejich ochranu, distribuci citlivých informací, ale také i jiných aktiv spoleļnosti, v níţ je bezpeļnostní politika aplikována. Bezpeļnostní politika je nástrojem pro sníţení pravděpodobnosti výskytu zneuţití

[7] zákon ļ.412/2005 Sb. o ochraně utajovaných informací a bezpeļnostní způsobilosti

informaţního systému, který zahrnuje pravidla, normy a postupy, které je třeba dodržovat, aby byla zajištěna důvěrnost, ale také odpovídající dostupnost dat. Bezpečnostní politika lze také charakterizovat jako principy zajišťující důvěrnosti a neporušitelnosti informaţního systému a dostupnosti všech služeb poskytovaných informaţním systémem. Systém, který splňuje bezpečnostní politiku, nazýváme důvěryhodný systém.

Bezpečnostní politika má charakter závazného dokumentu, který musí být v organizaci přijat jako vnitřní organizaţní norma. Musí být veřejně přístupný a je žádoucí, aby tento dokument byl struţný, srozumitelný, přehledný a úplný a řešil všechny moţné otázky a konfliktní situace v rámci bezpečnosti informaţního systému.

Bezpečnostní politika organizace zahrnuje nejširší a nejvyšší politiky organizace směřující k ochraně jejich pracovníků a aktiv. Bezpečnostní politikou týkající se informaţního systému organizace se obvykle nazývá politika informaţní bezpečnosti, resp. Bezpečnostní politika informací, kterou dělíme na celkovou bezpečnostní politiku a na systémovou bezpečnostní politiku.

Celková bezpečnostní politika prezentuje globální popis cílů organizace, jejího informaţního systému a jeho zabezpečení. Jedná se o nadţasový dokument vypracovaný pro ţasový limit 5 ï 10 let. Systémová bezpečnostní politika prezentuje popis jak chránit, organizovat a distribuovat aktiva informaţního systému, vţetně popisu konkrétních cílů, popisu konkrétních ohroţení (zjištění analýzou rizik) a popisu konkrétních bezpečnostních opatření. Systémová bezpečnostní politika spoleţnosti urţuje aspekty bezpečnosti a zahrnuje poţadavky na ochranu a nakládání s citlivými informacemi v souladu s platnými zákony a vyhláškami. Systémová politika zahrnuje fyzickou, technickou, personální a komunikaţní bezpečnostní politiku, specifikaci funkcí prosazujících bezpečnost, specifikaci síly bezpečnostních mechanizmů a ohodnocení úrovně bezpečnosti (bezpečnostní audit)

1.3 Standardy ISMS[8]

V roce 1995 vznikl britský standard BS7799:1995 Code of Practice for Information Security Management. Tento standard byl ve své podstatě souborem nejlepších praktik pro management bezpečnosti informací.

[8] NBÚ, Národní bezpečnostní úřad, *http://www.nbu.cz/cs/*

Ve výše zmíněném standardu ale chyběl návod, jak jednotné tento standard implementovat do organizace. To se povedlo až v roce 1999, kdy došlo k novelizaci původního standardu (BS7799-1:1999). Tvůrci aplikovali postupy standardů řízení kvality ISO 9000, které se začaly implementovat do organizací. BS7799:1999 byl doplněn o další část, která již poskytovala pravidla pro implementaci (BS7799-2:1999).

Na základě problematiky, kterou tyto standardy řeší, se pro ně vžil název „standardy ISMS“ (Information Security Management System). Standardy BS7799-1:1999 a BS7799 2:1999 byly v průběhu let novelizovány a v roce 2006 byly doplněny standardem BS7799 3:2006 ISMS Guidelines for Information Security Risk Management, který poskytuje návody, jak řešit řízení rizik ISMS. Oba standardy byly poté přijaty jako mezinárodní normy ISO. Standard BS7799-1:1999 byl v roce 2000 přijat jako mezinárodní norma pod označením ISO/IEC 17799:2000 a standard BS7799-2:1999 byl v roce 2005 přijat jako mezinárodní norma pod označením ISO/IEC 27001:2005.

Standardy ISMS byly přijaty i jako české normy, jejichž posledními vydáními jsou:

- ČSN ISO/IEC 17799:2006 Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací
- ČSN ISO/IEC 27001:2006 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky
- ČSN ISO/IEC 27006:2008 Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

1.4 Role managementu organizace v systému řízení bezpečnosti informací

Zavedení ISMS do organizace vyžaduje vynaložení nemalých nákladů. Z tohoto důvodu si nejprve musí organizace ujasnit svou motivaci a potřebu zavedení takového systému. Tato úloha je úkolem managementu organizace, který odpovídá za hospodárné vynakládání prostředků. Management musí mít neustále na paměti, že bezpečnost se musí organizaci vyplatit. Pro organizaci s téměř nulovým rizikem útoku je zavedení ISMS bezpředmětné.

Management organizace vedou k řízení bezpečnosti svých informací motivy. Existují tři základní motivy, jejichž vzájemná kombinace obvykle vyjadřuje postoj managementu. Těmito motivy je odpovědnost (management organizace si je vědom závislosti na vlastních informacích a snaží se jim poskytnout náležitou ochranu), alibi (management organizace si je vědom své odpovědnosti vůči zajištění dostatečné ochrany informací své organizace a chce jednoznačně prokázat, že učinil veškerá opatření k zajištění jejich bezpečnosti) a obchodní výhoda (management organizace chce řídit a následně deklarovat spolehlivost organizace v oblasti bezpečnosti informací vůči svým partnerům, a upevnit tím své postavení na trhu)

Management organizace je obvykle plně vytížen řízením a snahou o dosahování strategických cílů organizace. Bezpečnost vnímá jen jako druhořadou službu, která sekundárně podporuje činnost organizace. Zde se otevírá pole pro bezpečnostní manažery organizací, kteří by měli působit na vedení svých organizací tak, aby změnila postoj k bezpečnosti a chápali ji jako organickou součást systému organizace, která předchází vzniku ztrát v důsledku bezpečnostních incidentů.

Management organizace zajišťuje tvorbu, implementaci a vynucování bezpečnostní politiky v rámci plánování řízení bezpečnosti. Nejefektivnější přístup tohoto plánování je metodou „shora dolů“ (od top managementu až po koncové uživatele).

Top management je zodpovědný za vedení a definování politiky organizace. Jednotlivé bezpečnostní politiky definují nařízení pro nižší úrovně hierarchie organizace. Střední management doplňuje standardy, normy, směrnice a postupy. Řídící pracovníci nejnižší úrovně nebo bezpečnostní specialisté potom implementují předepsané konfigurace. Koncový uživatelé musí plnit všechny bezpečnostní politiky organizace

Plánování řízení bezpečnosti zahrnuje zavedení bezpečnostních rolí pro implementaci ISMS. Jedná se o role, které osoby hrají v celkovém schématu implementace bezpečnosti a administrativy uvnitř organizace. Bezpečnostní role nemusí být nezbytně předepsány pro danou pracovní pozici, ačkoli nejsou zřejmé a statické. Znalost těchto rolí usnadní stanovení komunikace a podpoří strukturu uvnitř organizace. Mezi bezpečnostní role patří senior manažer, který představuje osobu plně zodpovědnou za bezpečnost v organizaci, dále bezpečnostní specialista, vlastník dat, správce dat, koncový uživatel a auditor, což je osoba zodpovědná za testování a ověřování, že bezpečnostní politika je řádně implementována a

bezpeţnostní Ńeġení jsou adekvátní. Tato role mŢġe být pŚidŊlena bezpeţnostnímu specialistovi nebo ġkolenému uġivateli.

2. Informaţní systémy[9, 10]

Základními ţástmi informaţních systémŢ jsou výpoţetní systémy, coġ jsou systémy, kde jsou zpracovávána a uchovávána data, která jsou nositeli informací. Výpoţetní systém zahrnuje hardware, software a vlastní data. Tyto komponenty výpoţetního systému pŚedstavují systémové ţásti informaţního systému a charakterizována jako aktiva informaţního systému.

2.1 Bezpeţnost informaţních systémŢ

V dneġní dobŊ je velice rozsáhlá distribuce výpoţetní techniky v podnikové sféŚe, ale i pro osobní vyuġití. Zaţaly se hromadit pŚípady zneuġití dat (informací) v digitální formŊ a proto je velice dŢleġité zajiġtŊní bezpeţnosti informaţních systémŢ, jako pŚedbŊġné opatŚení proti útokŢm na informaţní systémy. Bezesporu dalġím velmi dŢleġitým komponentem v oblasti bezpeţnosti informaţních systému je personál spoleţnosti.

V rámci zabezpeţení je podstatné rozliġit, co je objekt a subjekt informaţního systému (viz. kapitola 1.2. Ochrana informací v organizaci). Subjekt je povinen se identifikovat (tvrzení subjektu, ġe je to subjekt oprávnŊný k pŚístupu k objektu), na coġ následnŊ odpovídá autorizace (ovŊŚení, ġe subjekt, který se identifikoval, je opravdu tím subjektem). Autorizovaný subjekt je povaġován za dŢvŊryhodný pro vykonávání jistých ţinností. DŢvŊryhodný subjekt ţi objekt pŚedstavuje takovou entitu, která je implementována v souladu s bezpeţnostní politikou.

Zranitelné místo informaţního systému je takové místo, které je moġné vyuġít pro zpŢsobení ġkody na informaţním systému, nebo ke zpŢsobení ztrát informací. Vyuġití slabého místa systému se nazývá útokem na informaţní systém. Podstata zranitelného místa mŢġe být rŢzná. (fyzická, pŚírodní, informaţní nebo fyzikální).

Bezpeţnost systémŢ se rozdŊluje do více oblastí, které jsou tvoŚeny poţítaţovou bezpeţností, která spoţívá v ochranŊ dat uloġených v poţítaţích, dále komunikaţní bezpeţností, která spoţívá v ochranŊ dat pŚi jejich pŚenosu (napŚ. zaslání emailové zprávy),

[9] PŚibyl, J. *Informaţní bezpeţnost a utajování zpráv*, ŢVUT, Praha, 2004
[10] Ţandík, M. *Základy informaţní bezpeţnosti*, Univerzita Tomáġe Bati ve ZlínŊ, 2004

dále fyzickou bezpečností, která spočívá v ochraně proti přírodním hrozbám, a v neposlední řadě také personální bezpečností, která spočívá v ochraně proti vnitřním útočníkům.

V oblasti bezpečnosti dat informačních systémů jsou specifikovány čtyři hrozby, které jsou směrovány proti informačním systémům. Jedná se hrozbu přerušení, odposlechu, modifikace a vytvořením falsifikátu. Všechny zmíněné hrozby jsou cíleny jako útoky na trojici CIA (Confidentiality, Integrity, Availability), kdy dochází k narušení důvěrnosti, dostupnosti a integrity informací.

2.2 Útoky na informační systémy a ochrana

Většina škod způsobená na programovém vybavení počítačů a na datech, která v nich jsou uložená, je způsobená právě počítačovými viry. *„Počítačový vir je malý programový modul, který se připojí k původnímu programu. Po zavedení napadeného programu do paměti (při jeho spuštění) provádí virus činnosti, které uživatel neočekává. Virus může být aktivován bezprostředně po jeho zavlečení do operační paměti počítače nebo až za určitých okolností, například v určený den nebo hodinu.*[11]"

V počítačové terminologii se rozlišují útoky, na informační systémy, do tří skupin, kterými jsou počítačové viry, počítačové červy a trojské koně. Útoky na informační systémy se zpravidla vyznačují jako útoky na důvěrnost, integritu a dostupnost. Z tohoto důvodu se útoky na informační systémy klasifikují na pasivní a aktivní. Pasivní útok je realizovaný odposlechem informačního toku dat v informačním systému a aktivní útok je realizovaný přerušením informačního toku dat v informačním systému, modifikací dat apod.

Podobně jako útoky na informační systémy rozlišujeme také samotné útočníky, kteří se dělí rovněž do tří skupin. Útočník slabé síly je spíše amatérským útočníkem, který disponuje omezenými znalostmi a také prostředky k realizaci útoků. Útočník střední síly bývá někdy označován jako hacker. Jedná se útočníky, kteří disponují velkými znalostmi, ale jejich prostředky jsou omezené. Zpravidla se jedná o SŠ/VŠ studenti. Profesionální útočníci, kteří většinou pracují na zakázku, bývají označováni, jako útočníci veliké síly. Tito útočníci mají dostatečné znalosti, ale také prostředky k realizaci útoku.

[11] Čandík, M. *Základy informační bezpečnosti*, Univerzita Tomáše Bati ve Zlíně, 2004

2.2.1 Spamming v informaţních systémech

Spamming je činnost spočívající v rozesílání nežádoucích emailů, tzv. spamů. Jedná se o jednu z novějších forem zneužití elektronické komunikace, kterou nabízí internetovská technologie. Podstatou činnosti spammingu je zaplavovat internet velkým množstvím stejných zpráv ve snaze vnutit ji lidem, kteří by za běžných okolností takovouto zprávu přijmout vůbec nechtěli. Většinou je spam nějaká obchodně zaměřená nabídka, kdy se velmi často jedná o nabídky pochybných produktů.

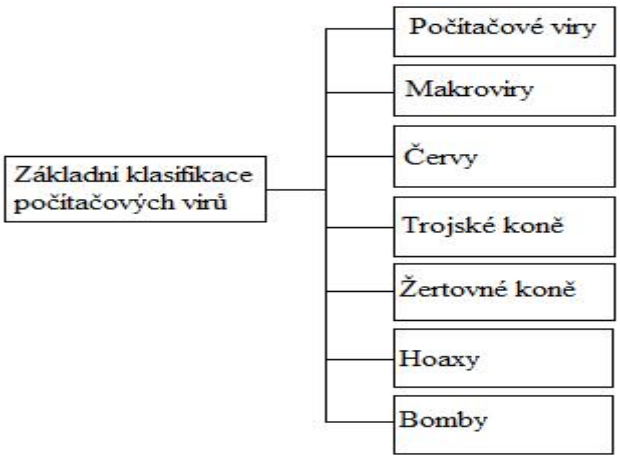
Spamming je škodlivý a nebezpečný z mnoha různých důvodů. Uživatel musí věnovat část svého času, aby spam rozpoznal a přijatelně na něj zareagoval (běžně smazáním). Spam omezuje funkčnost komunikačních systémů, která spočívá v zahlcení přenosových cest zbytečnostmi, které brání včasnému a rychlému přenesení některých jiných důležitých dokumentů. K zahlcení dochází v důsledku potřeby určité části kapacity přenosového média k přenesení velkého množství spamů. Další a nejvážnější nebezpečí, které spam představuje, spočívá ve zneužívání osobních údajů rozesíláním nevyžádaných emailů (zásilek). Jedná se o zneužití elektronických adres v případě, že si vlastník elektronické adresy email (zásilku) nevyžádal.

Proti spammingu již existuje velké množství způsobů, jak proti němu bojovat, jedná se zejména o legislativní opatření a technická opatření. Z hlediska legislativních opatření se jedná především o zákon o ochraně osobních údajů[12]. Ochrana osobních údajů je součástí evropské úmluvy o lidských právech a základních svobodách. Smyslem zákona je dosáhnout toho, aby se s osobními údaji občanů nakládalo jen podle stanovených pravidel, která odpovídají standardům Evropské unie. Zákon je v souladu s direktivou EU a úmluvou Rady Evropy.

2.2.2 Počítačové viry a ochrana před nimi

Počítačové viry jsou bezesporu nejznámějším rizikem pro počítačové sítě a zejména počítače. Důležitou složkou řízení informační bezpečnosti je eliminace počítačových virů z počítačových systémů.

[12] zákon č.101/2000 Sb., o ochraně osobních údajů



Obrázek 3 - klasifikace počítačových virů[13]

Počítačový virus je program, který bez vědomí uživatele počítače dokáže připojovat, přepisovat nebo jiným způsobem modifikovat ostatní programy nebo systémové oblasti pevného disku a disket s cílem vlastní reprodukce apod. K aktivaci počítačového viru dochází při spuštění infikovaného programu. Cílem počítačového viru je ve většině případů způsobit druhému škodu nebo obtíže při užívání počítače uživatelem.

Makroviry jsou viry, které souvisí především s užíváním kancelářského balíku Microsoft Office, které se vyskytují například v dokumentech MS Word, sešitech MS Excel či prezentacích MS PowerPoint). Makroviry jsou tvořeny Makry a z tohoto hlediska je velmi důležitá šablona NORMAL.DOT. K spuštění této šablony dochází při spuštění Wordu a pokud je šablona napadena makrovirem, tak má na Wordem kontrolu v podstatě hned po startu.

Červ je samostatný program, který se nepřipojuje k žádnému dalšímu programu, na rozdíl od počítačového viru, ale šíří se obdobně. Červ ke svému šíření využívá komunikační připojení s dalšími počítači a vkládá se do samostatných souborů. Samotné spuštění těchto souborů je obvykle zajištěno již při startu počítače. Využívá slabé stránky v zabezpečení sítě, snadno vyluštitelná hesla uživatelů a chyb v operačním systému PC.

Trojský kůň je zvláštním typem viru, protože jde o program, který se na venek jeví jako užitečný, o kterém uživatel ví, že jej spouští. Trojský kůň tedy funguje jako užitečný program, ale zároveň provádí další činnosti, o kterých uživatel nemá tušení. Trojský kůň je virem, který se nedokáže sám šířit, uživatelé si jej musejí nevědomky sami předávat.

[13] Čandík, M. *Základy informační bezpečnosti*, Univerzita Tomáše Bati ve Zlíně, 2004

Červotné programy jsou nebezkodným program, který simuluje chybové stavy operaèního systému nebo libovolný druh destrukèní èinnosti.

Hoax je e-mailová zpráva, která obsahuje falešné upozornění na možné ohrožení nějakým virem apod. Z tohoto hlediska může být zpráva hromadně přeposílána více uživatelům. Tím pádem dochází k zbytečnému zahlcování sítě přeposíláním dezinformace.

Bomby jsou programy, které způsobují destrukční akci a následné úplné zamrznutí všech funkcí počítače.

2.2.3 Způsoby ochrany před počítačovými viry[14]

Počítačové viry svojí přítomností v systémových prostředcích způsobují vážné problémy, proto je nutné přijmout různá opatření, aby se zabránilo vniknutí těchto virů do informačního systému anebo aby se úspěšně podařilo eliminovat účinky virů. Z tohoto hlediska je velmi významným prvkem bezpečnosti informací ochrana před počítačovými viry, které se realizuje různými způsoby.

Softwarová ochrana je realizována antivirovými programy, jejichž služby lze rozdělit do tří skupin. Konkrétní antivirové techniky jsou takové, které vyhledávají pouze známé viry podle virové databáze, kterou je nutné neustále aktualizovat. S informacemi, které o viru vím nebo s informacemi o programu či souboru, které popisují, jak vypadal dříve, dokáže virus vždy takto nalezených odstranit. Obrovskou výhodou této metody je její rychlost a používá se pro pravidelné kontrolování disku. Obecné antivirové techniky jsou takové, které se snaží vyhledat a pokud je to možné i odstranit virus. Obecné antivirové techniky ke své činnosti využívají srovnávací testy, heurestickou analýzu, plnou heurestickou analýzu a testy prostředí na souborové viry. Preventivní techniky jsou techniky, které se snaží najít a odstranit neznámé viry ještě před jeho nakopírováním do počítače

Antivirové systémy jsou v současné době nejfrekventovanějším antivirovým programem. Antivirové systémy jsou systémy, které plní v první řadě funkci preventivní, aby nedošlo k nakažení počítače virem. Mezi další funkce antivirového systému patří identifikace viru a jeho následné odstranění. Antivirové programy sledují všechna podstatná vstupní místa, kterými by mohl virus proniknout do počítače (např. elektronická pošta, www stránky, média

[14] Čandík, M., Ivanka, J. *Bezpečnost v informačních technologiích*, Praha, 2003

apod.). Antivirové systémy mají také schopnost aktualizovat se prostřednictvím internetu. Antivirovými programy jsou např. AVG, Norton AntiVirus, NOD32 apod.

2.3 Bezpečnost datových sítí

Datové sítě zabezpečují přenosy dat ze zdrojových systémů do systémů cílových. Z tohoto hlediska je nejdůležitější zajištění bezpečnosti přenosu informací, aby nedošlo např. k pozměnění původní zprávy, k odposlechu informací a následnému jejich zneužití apod.

Šifrování patří mezi kryptografické bezpečnostní mechanizmy. Princip šifrování spočívá v zašifrování zprávy na straně odesílatele pomocí nějakého klíče a následné dešifrace zprávy na straně příjemce opět pomocí nějakého klíče. Šifrování je používáno jako ochrana proti ztrátě důvěrnosti informace, ale zároveň jej lze použít i pro zajištění autenticity informace. Rozlišujeme šifrování na symetrické šifrování a asymetrické šifrování.

Symetrické šifrování je šifrování, kdy obě komunikující strany používají stejný klíč, tzv. tajný klíč. Tento klíč je nutné udržet v tajnosti, aby nedošlo k ohrožení důvěrnosti informací. Oproti asymetrické šifrování je šifrování, kdy obě komunikující strany používají dva klíče. V případě odesílatele jde o tzv. soukromý klíč a v případě příjemce o tzv. veřejný klíč. Přenášená data nemají chráněnou důvěrnost, protože veřejný klíč může použít kdokoliv, ale autenticita i těchto dat zajištěna je, protože šifru vygeneroval pouze vlastník příslušného soukromého klíče.

Elektronický podpis je způsobem pro zajištění autenticity, integrity a nepopiratelnosti zprávy. Elektronický podpis lze uplatnit v elektronickém dokumentu. Elektronický podpis je vygenerován jako výtažek z původního dokumentu pomocí algoritmu a je připojen k tomuto dokumentu. Elektronický podpis se před přenosem zašifruje a je přidán původnímu dokumentu. Na straně příjemce je dešifrován a opět je vytvořen elektronický podpis z původního textu. Oba vygenerované elektronické podpisy se poté porovnají, zda jsou stejné či nedošlo k modifikaci textu při přenosu.

Řízené uživatelské přístupy je v podstatě zadání uživatelova jména a hesla, které si ve většině případů volí uživatelé sami. Jde o nejrozšířenější způsob ochrany autentizace. Je důležité, aby heslo bylo složeno z dostatečného počtu znaků a kombinací různých znaků na klávesnici (číslice, interpunkční znaménka, písmena apod.). Také heslo je pak označováno za silné.

Firewall je program, který spolu se směrovačem řídí přístup do chráněné sítě. Firewally můžeme rozdělit do dvou skupin. Jsou to paketové filtry a aplikační brány. Paketové filtry pracují na principu kontroly některých polí v hlavičkách paketů a tato pole porovnává s pravidly uloženými v paměti a provádí akce, které jsou v pravidle definovány. Paketové filtry jsou poměrně levnou záležitostí, ale také účinným způsobem zabezpečení vnitřní sítě. Aplikační brána bývá uložena mezi lokální a rozsáhlou sítí. Uživatelský program komunikuje s aplikační bránou místo toho, aby komunikoval se skutečným serverem. Aplikační brána musí rozumět protokolu, kterým klient se serverem komunikují. To jí umožňuje vyhodnocovat požadavky obou stran a zabraňovat tak nepovolaným operacím.

Existují čtyři základní typy složitějších firewallů, které získáme konstrukcí paketových filtrů a aplikačních bran. Jedná se o jednoduchý filtrující směrovač, jednoduchá aplikační brána, směrovač a aplikační brána a směrovač s demilitarizovanou zónou, který představuje typ firewallu, který přidává mezi rozsáhlou síť a lokální síť jeětě jednu malou síť, označovanou jako demilitarizovaná zóna. *„Vnitřní filtrující směrovač poskytuje ochranu vnitřní sítě jak proti vnější síti, tak i proti demilitarizované zóně v případě, že byla narušena. Vnitřní směrovač může blokovat spojení tak, aby bylo umožněno spojení pouze mezi demilitarizovanou zónou a vnitřní sítí.“*[15]

3. Audit zajištění informační bezpečnosti s využitím Paretova diagramu[16]

Cílem auditu je v obecné rovině poskytnout managementu informace, které zmírní případné negativní důsledky vyskytující se při dosahování obecných cílů organizace. Cílem bezpečnostního auditu je poskytnout managementu informace o stavu bezpečnosti organizace, které umožní managementu, aby při dosahování základních cílů organizace mohl přijmout opatření, která eliminují nebo alespoň minimalizují zjištěná bezpečnostní rizika (a z toho plynoucí možnost vzniku újmy pro organizaci).

Hlavním cílem auditu je ověřit účinnost bezpečnostní politiky, kterou společnost přijala, a také vyhodnocení současného stavu zabezpečení aktiv společnosti se zaměřením na zabezpečovací prvky spojené se službami ochrany majetku a osob.

---

[15] Řandík, M. *Základy informační bezpečnosti*, Univerzita Tomáše Bati ve Zlíně, 2004

[16] Kameník, J., Brabec, F. a kol. *Komerční bezpečnost. Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*.1. vyd. Praha: ASPI, a.s., 2007

Předmětem auditu je společnost Hospital Systems s.r.o., která zajišťuje vývoj, dodávky, implementaci a konzultační služby informačních systémů pro zpoplatnění zdravotnictví, dodávky patřičných nástrojů potřebných pro zpoplatnění služeb ve zdravotnictví a ovládání o platbách.

Tato firma vznikla v roce 2005 za účelem vývoje informačního systému pro plánované zpoplatňování služeb ve zdravotnictví. Hospital Systems s.r.o. je společnost založená ještě z této činnosti. Jejím předmětem podnikání není jen vývoj tohoto informačního systému, ale i jeho dodávka, implementace a následná správa.

Informační systém byl z počátku instalován pouze do krajských nemocnic, ale v dnešní době je postupně instalován i do zbývajících nemocnic v jednotlivých krajích. Hospital Systems s.r.o. z tohoto důvodu provádí školení pracovníků nemocnic související s obsluhou informačního systému pro zpoplatňování služeb zdravotnictví. Samostatnou údržbu systému spravuje Hospital Systems s.r.o.

Název společnosti	Hospital Systems s.r.o.
Právní forma	S.R.O.
Rok založení	2005
Sídlo společnosti	Pardubice
Adresa společnosti	U kostelíčka 1432
Počet zaměstnanců	80
Výše základního kapitálu	1 000 000 Kč
Předmět činnosti	- vývoj informačního systému pro zpoplatnění zdravotnictví - dodávky a implementace systému a nástrojů potřebných pro zavedení tohoto systému - konzultační služby - provádění školení nemocničních pracovníků

Tabulka 1 - základní údaje o společnosti Hospital Systems s.r.o., zdroj: vlastní

Hospital Systems s.r.o. má pobočky ve čtyřech krajských městech (Hradec Králové, Brno, Plzeň a Ostrava), ale hlavní sídlo této společnosti je v Pardubicích. Předmět činnosti jednotlivých poboček je zásadní měrou závislý na zpracování dat a informací. Na pobočkách se vyskytují údaje o realizovaných obchodních případech a vzhledem k tomu, že se tam

mohou vyskytovat i faktury za miliony korun a více (což tvoří významnou položku v cash flow firmy), vyskytují se zde i citlivé informace, jejichž bezpečnost je pro firmu prvořadá. Tyto informace jsou uchovávány na serverech jednotlivých poboček, odkud jsou zálohovány na společný server v sídle společnosti, kde jsou dále zpracovávána z hlediska jejich významu a aktuálnosti.

Společnost přijala pro řízení bezpečnosti informací bezpečnostní politiku. Bezpečnostní politika[17] představuje základ pro zajištění informační bezpečnosti. Společnost Hospital Systems s.r.o. na základě výsledků z rizikové analýzy přijala bezpečnostní politiku, která řeší strategické principy, jež se týkají organizace jako celku nebo informačního sytému jako celku. Společnost se tímto zavazuje uplatňovat principy důvěrnosti, dostupnosti a úplnosti informací, vytvářet podmínky pro zajišťování zdrojů potřebných k zavedení, udržování a neustálému zlepšování systému managementu bezpečnosti informací. Hospital Systems s.r.o. je povinna pravidelně hodnotit plnění cílů a cílových hodnot vycházejících z analýzy rizik a této politiky, zajišťovat vysokou ochranu informací, které představují předmět jejich činností a u kterých hrozí bezpečnostní incident ze strany vnějšího pachatele. Rovněž je povinna zajišťovat vysokou ochranu citlivých dat a informací na všech pracovištích, racionálním uplatňováním zásad informační bezpečnosti vůči smluvním partnerům a třetím stranám, a pravidelným vzděláváním všech zaměstnanců a zvyšováním jejich povědomí o ochraně aktiv zvyšovat informační bezpečnost. Tato politika je závazná pro všechny zaměstnance společnosti. Vedení společnosti se zavazuje pravidelně přezkoumávat tuto politiku, rozpracovávat ji do měřitelných cílů, k plnění cílů poskytovat potřebné zdroje a osobní příklad.

Krok	Termín	Odpovědná osoba	Výstup
schválení plánu auditu	7.3.2009	ředitel pro správu	plán auditu - schválený
provedení auditu	10.-13.3.2009	auditoři, vedoucí auditovaných útvarů	dílčí protokoly o auditu pracovišť
zpracování sumárního protokolu	16.3.2009	vedoucí auditor	protokol o interním auditu - návrh
schválení protokolu	17.3.2009	generální ředitel	protokol o interním auditu - schválený
odstranění neshod a slabých míst	19.-25.3.2009	vedoucí auditovaných prvků	odstraněné neshody

Tabulka 2 - harmonogram auditu, zdroj: vlastní

[17] Hospital Systems s.r.o., *Bezpečnostní politika*, Pardubice, 2005

V termínu od 19. do 25. bŚezna 2009 probĎhne odstranĎní neshod a slabých míst za coŕ jiŕ odpovídají vedoucí auditovaných prvkŢ. OdstranĎní neshod probĎhne ale pouze v pŚípadĎ, ŕe ve výsledné zprávĎ z interního auditu se objeví slabá místa ļi nĎjaké nesrovnatelnosti.

3.1 Situaļní analýza

Hlavní sídlo spoleļnosti, na kterém je provádĎn audit informaļního zabezpeļení, je tvoŚen jednou výŕkovou budovou. Do budovy vede jeden vchod do vstupní haly, v níŕ je pult recepce, která je tvoŚena osobami bezpeļnostní agentury. Vchod budovy je opatŚen kamerovým systémem od spoleļnosti Alarmtec.

Místnosti spoleļnosti Hospital Systems s.r.o. jsou chránĎny ve vĎtšinĎ pŚípadŢ pouze bĎŕnými zámky a evidencí klíļŢ, za kterou je zodpovĎdný ļlen ostrahy na recepci.

V rámci celé spoleļnosti se pouŕívají poļítaļe znaļky DELL, se kterou má spoleļnost uzavŚenou smlouvu garantující výraznĎjší slevu poļítaļŢ. Spoleļnost se tím firmĎ DELL zavázala smluvním kontraktem v ļasové lhŢtĎ 10 let uŕívání poļítaļŢ této znaļky. Tyto poļítaļe jsou vybaveny operaļními systémy Windows Vista Home Basic a balíļkem Microsoft Office (verze 2007) od spoleļnosti Microsoft. Poļítaļe jsou opatŚeny antivirovým programem ESET NOD32, verze databáze 3880. Uŕivatelskéŕ poļítaļe nejsou opatŚeny ŕádným modemem, vŕechny mají pouze standardní síŠový adaptér. Systémy nepodléhají ŕádnému omezení z pohledu manipulace s daty ļi datovými nosiļi v ļetnĎ USB flashdiskŢ.

ESET NOD32 - Antivirový systém ESET NOD32 od spoleļnosti ESET je uznávaným Śeŕením v boji se ŕkodlivými kódy. Škodlivý kód (malware) dokáŕe nejen detekovat, ale nabízí i moŕnost jeho odstranĎní. ESET NOD32 drŕí krok s posledními trendy v oblasti malware a tak jiŕ nelze o ESET NOD32 mluvit jako o Ăļistokrevném antivirovém systému, ale i o anti-spyware Śeŕení, které bojuje s nejmladŕím malwarem, který je oznaļován jako spyware, adware, riskware. V neposlední ŚadĎ je Śeŕení ESET NOD32 jedno z prvních, které nabízí detekci rootkitŢ, tedy produktŢ, které se snaŕí maskovat v systému, popŚípadĎ maskovat i ŕkodlivý kód jiného typu.

Ve spoleţnosti Hospital Systems s.r.o. není v souţasné dobţ zavedený ţádný informaţní systém. Spoleţnost využívá sluţeb aplikace Microsoft Outlook a Exchange Server 2003. PŘechod na vnitrofiremní informaţní systém je plánován na rok 2008. Byl zvolen modulární informaţní systém QIod firmy DCConcept. O veţkerou infrastrukturu informaţních technologií ve spoleţnosti se z technického i administraţního hlediska stará jediný administrátor. Na technicky nároţnţjší projekty, jako je napŘíklad instalace kabeláţí v budovţ, se najímají externí dodavatelé.

Podniková síŠ je Řízena dvţma doménovými Řadiţi na platformţ Windows Server 2003. Hlavní server zajišŠuje provoz Microsoft Exchange Serveru 2003, slouţí jako DNS (Domain Name Server) server, DHCP (Domanic Host Configuration Protocol) server a faxový server. Vedlejší server slouţí jako datové úloţiš pro informace ze vţech poboţek spoleţnosti. Tato data jsou zámţrnţ umístţna na vedlejším serveru kvţli vysoké diskové zátţži. Oba dva servery mají vlastní UPS (Uninterruptible Power Supply) zaŘízení umožňující zhruba dvacetiminutový chod serveru v pŘípadţ výpadku dodávky elektrické energie. Servery jsou nakonfigurovány, aby se v pŘípadţ pŘechodu na záloţní zdroj automaticky pŘivedli k bezpeţnému ukonţení provozu.

Pro zabezpeţení sluţeb firewallu byla ve firmţ použita hardwarová brána Ovislink AirLive RS-1200. Tato brána byla zvolena kvţli podpoŘe duálního pŘipojení WAN pro umožnţní správy rozdţlování zátţže a zvýšení redundance v pŘípadţ výpadku pŘipojení. ProstŘednictvím DMZ (Demilitarized Zone) portu je možné zpŘístupnit vnţjším uživatelům pŘístup k serverům, aniž by došlo k vystavení sítţ možnosti útoku. Brána RS-1200 dále poskytuje funkci VPN serveru a klienta. K dispozici jsou protokoly IPsec i PPTP.

3.1.1 Systém Řízení bezpeţnosti informací

Systém zajišŠuje ochranu významných informaţních aktiv firmy pŘed ztrátou, poškozením nebo zneužitím.

Standard: ISO 27001:2006 - Norma Řeší osvţdţený způsobem bezpeţnost informací s cílem Řídit rizika s touto problematikou související, aŠ už se jedná o technologie nebo prostory. Cílem je poskytnout doporuţení, jak správnţ aplikovat ISO/EIC 17999 (v budoucnu 27002). Interpretace a implementace se může lišit v návaznosti na rozsahu systému, druhu a způsobu zpracování dat, jejich hodnotţ atd. Pokud je systém Řízení bezpeţnosti informací zaveden pouze v urţité ţásti organizace, vydaný certifikát je platný právţ pro tuto ţást nikoli pro celou

organizaci. Norma prosazuje procesní pŕístup a je plnŏ kompatibilní s ostatními systémy, lze ji proto certifikovat nejen samostatnŏ, ale i integrovanŏ.

Systém managementu dle poğadavkŧ normy ISO 27001 je urļen vğem organizacím, které chtŏjí získat nejen konkurenļní výhodu, ale které chtŏjí chránit svá informaļní aktiva s vysokou hodnotou a tím minimalizovat ztráty zpŧsobené jejich únikem. Ti, kdo nakládají s citlivými informacemi nebo osobními údaji mohou touto cestou pŕedejít finanļním postihŧm a trestŧm, vyplývajících ze zákona, pŕi úniku informací nebo neoprávnŏným nakládáním s osobními údaji.

ISO 17799:2006 ï mezinárodní norma upravující Ŕízení bezpeļnosti informací

PŧsobnostÍ tŏchto norem Ŕízení bezpeļnosti platí pro vğechna pracovišŧ spoleļnosti Hospital Systems s.r.o.

3.2 Hodnotová analýza[18]

Hodnotová analýza zahrnuje ohodnocení veğkerých aktiv, kterými spoleļnost Hospital Systems s.r.o. disponuje. Hodnotová analýza je vyjádŕení penŏğní hodnoty aktiv v pŕípadŏ obnovy daného aktiva. Hodnotová analýza je prvotní dokument, na základŏ kterého se organizace rozhoduje, jaká aktiva je nutné chránit a naopak (založeno právŏ na hodnotŏ obnovy aktiva).

Následující tabulka vyjadŕuje registr aktiv spoleļnosti Hospital Systems s.r.o. Registr aktiv je sestaven na základŏ ceny obnovy aktiv spoleļnosti, ale v cenŏ není zahrnuta újma zpŧsobená zcizením informací, které jsou uloğená v nŏkterých aktivech z tohoto registru, jako napŕ. v serverovnŏ 1, kam se na vedlejğí server ukládají informace z poboļek spoleļnosti. Registr aktiv je sestaven tak, ğe aktiva, v nŏm obsağená, jsou zabezpeļena pomocí sluğeb ochrany majetku a osob.

Registr aktiv obsahuje i vyļíslenou délku obnovy v hodinách pro jednotlivá aktiva. Dobu trvání obnovy aktiv si vyļíslila spoleļnost sama, ale v této dobŏ je poļítáno pouze s tím, ğe penŏğní prostŕedky má firma vğdy k rychlému vynaloğení na obnovu aktiv, a to i v pŕípadŏ, ğe na tuto záleğitost nemá vyhrazen rezervní fond. Registr aktiv rovnŏğ obsahuje veğkeré bezpeļnostní mechanismy, které jsou vyuğívány právŏ k zabezpeļení tŏchto aktiv spoleļnosti.

[18] Rodryļová, D., Staša, P. *Bezpeļnost informací jako podmínka prosperity firmy*, Grada Publishing, spol. s.r.o., 2000

Název položky	Vlastník	Doba obnovy (hod.)	Cena obnovy (tisíce	A	B	C	D	E	F	G	H	I	J
Prostory se zvláštním režimem													
Servrovna 1	Správce IS	8	230	X			X	P	X	P	P		X
Servrovna 2	Správce IS	6	70	X			P	X	X	P			X
Rozvaděč	Správce IS	6	30	X	X		P	P	X				X
Archiv smluv	Asist. Šéd.	4	50	X				X	X		X		P
Přír. archiv ÚD	Fin. ředitel	4	50	X					X		X		P
Kancelář Šéd.	Gen. Šéd.	4	150	X				X	X	P	X		P
Míst. Uklízeček	Ved. prov.	48	12	X									X
Prostory s omezeným přístupem													
Kancelář ÚFř	Prov. Šéd.	6	200	X					X	P	X		P
Kancelář	Prov. Šéd.	2	50	X				X	X		X		X
Sklad	Ved. nák.	24	80	X			X		X		X		X
Úklolící místnost	Prov. Šéd.	120	80	X					X	P	X		X
Prostory obecně přístupné vždem zaměstnancům													
Chodby	Prov. Šéd.	120	20	X					X				
Kuchyňky a SZ	Prov. Šéd.	120	50	X					X				
Zasedací míst.	Prov. Šéd.	120	80	X					X		X		
Prostory veřejně přístupné v pracovní době													
Recepce		120	150	X				X	X				X

Tabulka 3 - registr aktiv[19]

[19] Hospital Systems s.r.o., *Registr aktiv*, Pardubice, 2005

Legenda:

A ï bĐžné zámky, evidence klíļŢ (klíļový reģim)

B ï bezpeļnostní dveŚe se zvýģenou odolností proti zniļení nebo mŚížemi

C ï okenní mŚížge nebo bezpeļnostní fólie

D ï bezpeļnostní zámky, zdvojené zámky nebo závory

E ï monitoring vlhkosti, teploty a klimatizace

F ï poģární detektory

G ï elektronický zabezpeļovací systém

H ï monitorování prostor ï kamerový systém

I ï náhradní prostory (urļení náhradních prostor jako plánŢ kontinuity)

J ï zabezpeļení napájení (UPS, náhradní zdroje)

X ï aplikováno

P ï plánováno

3.2.1 Využití Paretova diagramu[20, 21, 22]

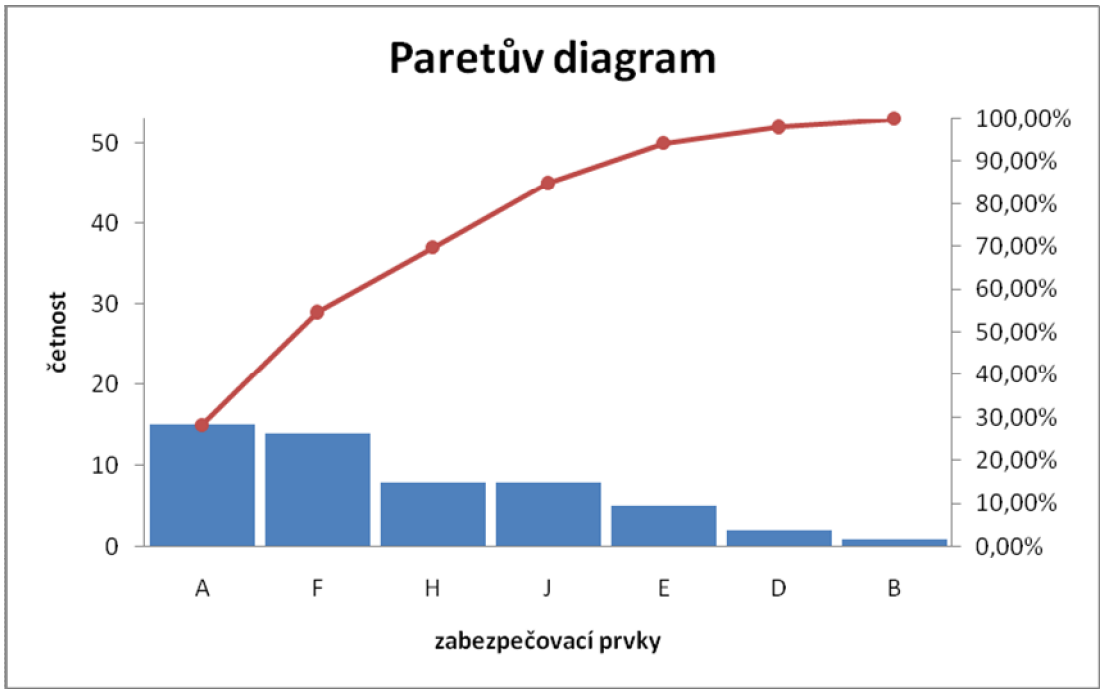
Aktiva spoleļnosti Hospital Systems s.r.o. mají jiģ urļitou úroveŔ zabezpeļení, která by mĐla být z pohledu spoleļnosti dostaļující pro zajiģtĐní informaļní bezpeļnosti. V rámci auditu zajiģtĐní informaļní bezpeļnosti využiji Paretova diagramu, a to z dŢvodu, ģe ParetŢv diagram mi poskytne pomocí grafického vyjádŚení/tabulky matematický popis, zda úroveŔ zabezpeļení aktiv spoleļnosti je dostaļující ļi nikoliv.

ParetŢv diagram je jedním ze sedmi základních nástrojŢ Śízení jakosti. Diagram je dŢleģitým nástrojem manaģerského rozhodování, který umoģŔuje stanovit priority pŚi Śeģení problémŢ s Śízením jakosti. Napomáhá oddĐlit podstatné faktory Śeģeného problému od tĐch ménĐpodstatných, coģ je principem Paretova diagramu.

[20] ParetŢv diagram, *http://lorenc.info/3MA112/paretova-analyza.htm*
[21] ParetŢv digram, *www.businessinfo.cz/files/2005/061019_nastroje-rizeni-jakosti-1.pdf*
[22] Zuzák, R., *Krizové Śízení podniku*, Professional Publishing, Praha, 2004

Druh zabezpeļení	Ļetnost	Ļetnost v %	Kumulativní ļetnost
A	15	28,3 %	28,3 %
B	1	1,8 %	30,1 %
C	0	0 %	30,1 %
D	2	3,8 %	33,9 %
E	5	9,5 %	43,4 %
F	14	26,4 %	69,8 %
G	0	0 %	69,8 %
H	8	15,1 %	84,9 %
I	0	0 %	84,9 %
J	8	15,1 %	100 %
Celkem:	53	100 %	

Tabulka 4 - ļetnosti výskytu zabezpeļovacích prvkŢ, zdroj: vlastní[23]



Obrázek 4 - ParetŢv diagram (souļasný stav), zdroj: vlastní

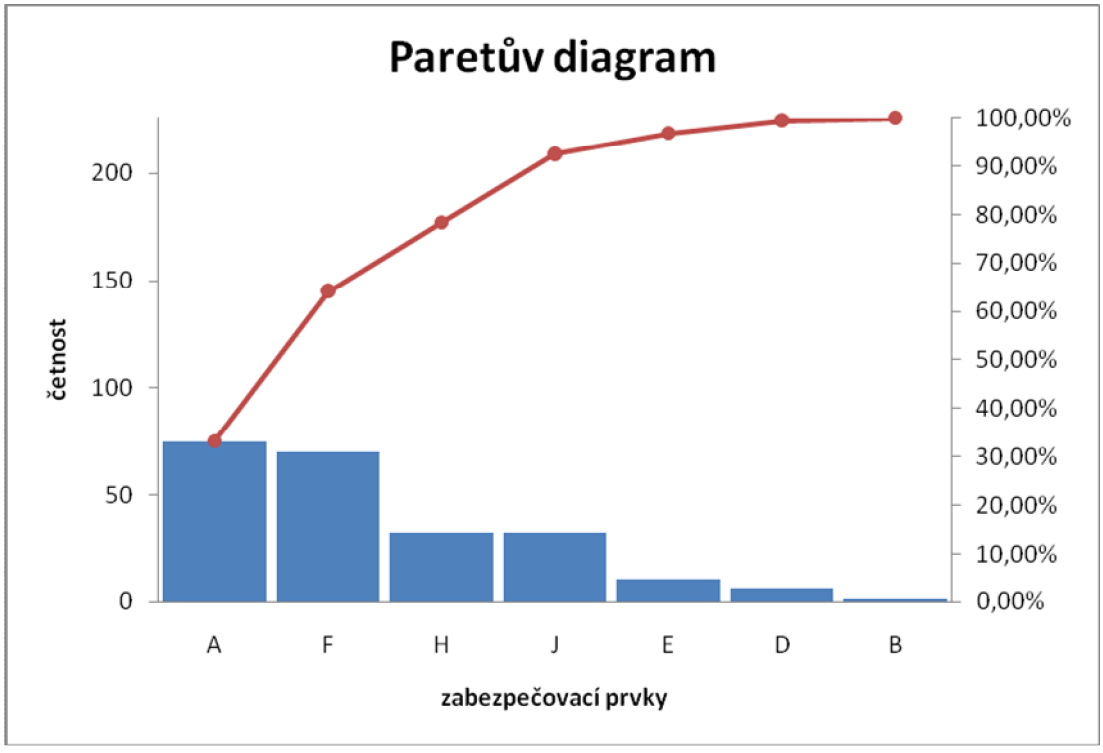
Jednotlivé sloupce v ParetovĎ diagramu pŚedstavují ļetnost jednotlivých bezpeļnostních mechanizmŢ a ļervená trendová kŚivka pŚedstavuje souļet kumulativních ļetností. Tato kŚivka mi vyjadŚuje mnoģství procent z celkového zabezpeļení aktiv spoleļnosti, kterou tvoŚí urļitá ļást zabezpeļovacích mechanizmŢ. Z diagramu je zŚejmé, ģe pro dosaģení zabezpeļení aktiv spoleļnosti staļí z více jak 50% zabezpeļení bĎģnými zámky ï evidencí klíļŢ a poģárními detektory. Z tohoto vyplývá, ģe se firma se v zabezpeļení svých aktiv spoléhá výhradnĎna dva zabezpeļovací prvky.

[23] Hospital Systems s.r.o., *Registr aktiv*, Pardubice, 2005

Vzhledem k tomu, ůe jednotlivé zabezpeļovací prvky mají pro optimalizaci zabezpeļení aktiv spoleļnosti rŢznou dŢleůitost, byla jednotlivým zabezpeļovacím prvkŢm pŚiŚazena jejich váha.

Zabezpeļení	Ļetnost	Váha (1-5)	Ļetnost*váha	Ļetnost v %	Kumul. ļetnost
A	15	5	75	33,2 %	33,2 %
B	1	1	1	0,4 %	33,6 %
C	0	1	0	0 %	33,6 %
D	2	3	6	2,7 %	36,3 %
E	5	2	10	4,4 %	40,7 %
F	14	5	70	30,9 %	71,6 %
G	0	5	0	0 %	71,6 %
H	8	4	32	14,2 %	85,8 %
I	0	1	0	0 %	85,8 %
J	8	4	32	14,2 %	100 %
Celkem:	53		226	100 %	

Tabulka 5 - zohlednŊní rŢzné dŢleůitosti zabezpeļovacích prvkŢ, zdroj:vlastní



Obrázek 5 - ParetŢv diagram (souļasný stav s pŚidŊlenými váhami), zdroj:vlastní

Zabezpeļením aktiv spoleļnosti zabezpeļovacími prvky (bŊůnými zámky ï evidencí klíļŢ a poůárními detektory) spoleļnost dosahuje aů 65% z celkové úrovnŊ zabezpeļení. Tato informace je pro firmu stŊůejní, protoůe vzhledem k nárŢstu kriminality a bezpeļnostnímu vývoji je zabezpeļení informací ve firmŊ zaostalé a bez nároku na obstání proti útokŢm

v dnešní době, které také pokrouţily s využitím informaţních technologií. Z tohoto dŧvodu jsem managementu spoleţnosti navrhnul zavedení ménţ rozhodujících zabezpeţovacích prvkŧ k urţitým aktivŧm. Zavedení tţchto prvkŧ by mţlo výraznţ zvýšit úroveŕ zabezpeţení, a to pŕedevšším z hlediska prognózy vývoje útokŧ a bezpeţnostních mechanizmŧ. Velkou výhodou pŕijetí mnou navrhovaných opatŕení je, že se bezpeţnostní hrozba rozloší na více zabezpeţovacích prvkŧ, coš bude hrozbu minimalizovat. Prvky, navrţené k zlepšení úrovnţ zabezpeţení, jsou v Ătabulka 3 ï registr aktivñ oznaţené jako P, coš znamená prvky plánované ke zlepšení zabezpeţení aktiv spoleţnosti.

3.3 Bezpeţnostní riziková analýza

Podstatnou souţástí bezpeţnostní rizikové analýzy je ŕízení rizik, které pŕedstavuje dokument stanovující postup ŕízení právţ pŕi bezpeţnostní rizikové analýze. Dokument obsahuje úţel a vymezení, pojmy a zkratky, ţetnost provádţní, postupy identifikace hrozeb, evidenci podnţtŧ ke zjišťování rizik, identifikace a ohodnocení rizik, návrh na opatŕení a plán zvládnutí rizika, schválení a realizace opatŕení, hodnocení úţinnosti opatŕení a zbytkových rizik a výstupní dokumenty.

3.3.1 Identifikace slabých míst spoleţnosti a mošná opatŕení

Serverovna 1 ï místnost, kde je soustŕedţn zálošní server pro hlavní sídlo spoleţnosti, ale i jednotlivé pobouţky. Mošných hrozeb tohoto aktiv je více a úroveŕ hrozeb je rŧznorodá. První identifikovaným slabým místem je neoprávnţní pŕístup s vysokou úrovní hrozby pro pŕípadný útok pachatele. Mošným bezpeţnostním mechanizmem odstraňujícím tuto hrozbu je elektronický bezpeţnostní systém. Další identifikovaným slabým místem je neoprávnţní pŕístup rovnţš s vysokou úrovní hrozby pro pŕípadný útok. Mošným bezpeţnostním mechanizmem je kamerový systém. Existuje zde i slabé místo v podobţ poškození dat vlivem klimatických podmínek. Úroveŕ hrozby pro pŕípadný útok je stŕední a bezpeţnostním mechanizmem pro odstranţní této hrozby je monitorování vlhkosti, teploty a klimatizace.

Serverovna 2 ï místnost, kde je soustŕedţn hlavní server pro hlavní sídlo spoleţnosti sloužící pro uchovávání dat. Jedná se opţt o aktivum, které nabízí více slabých míst a tudíš více mošností pro pŕípadného pachatele. Identifikovaným slabým místem je neoprávnţný pŕístup s vysokou úrovní hrozby pro pŕípadný útok pachatele. Mošným bezpeţnostním

mechanizmem odstraňujícím tuto hrozbu je bezpečnostní zámek a případně i elektronický bezpečnostní systém.

Rozvaděče - zařízení sloužící pro rozvody sítí v celé budově společnosti. Mezi slabá místa tohoto aktiva patří neoprávněný přístup se střední úrovní hrozby. Možným bezpečnostním mechanizmem pro odstranění tohoto slabého místa jsou bezpečnostní zámky, zdvojené zámky nebo závory. Dalším slabé místo představuje poškození zařízení vlivem klimatických podmínek. V tomto případě se ale jedná o nízkou úroveň hrozby. Možným bezpečnostním mechanizmem je monitoring vlhkosti, teploty, klimatizace.

Archiv smluv - místnost sloužící pro ukládání smluv uzavřených s klienty. U tohoto aktiva byla identifikována nemožnost napájení energií jako slabé místo představující střední úroveň hrozby. Bezpečnostním mechanizmem je navrhováno zajištění napájení.

Příruční archiv účetních dokladů - místnost sloužící pro ukládání účetních dokladů, které firma vykazuje. Také v tomto případě byla identifikována nemožnost napájení energií jako slabé místo se střední úrovní hrozby. Možným bezpečnostním mechanizmem je zajištění napájení.

Kancelář ředitele - místnost určená pouze generálnímu řediteli, jakožto nejvýše postavené osoby v managementu firmy. Nemožnost napájení energií je slabým místem se střední úrovní hrozby a možným bezpečnostním mechanizmem je zajištění napájení. Dalším slabým místem je neoprávněný přístup, který představuje vysokou úroveň hrozby útoky pachatelem. Možným bezpečnostním mechanizmem je elektronický bezpečnostní systém.

Kancelář ÚFř - je kancelářské pracoviště, kde se přechodně vyskytují cenné informace. Slabá místa představuje nemožnost napájení energií se střední úrovní hrozby a pro zajištění bezpečnosti je navrhován bezpečnostní mechanizmus zajištění napájení. Další slabé místo představuje neoprávněný přístup, který přináší vysokou úroveň hrozby útoku možného pachatele. Bezpečnostním mechanizmem pro odstranění této hrozby je elektronický bezpečnostní systém.

Školící místnost - místnost určená k internímu školení zaměstnanců společnosti. Slabým místem toho aktiva je neoprávněný přístup s vysokou úrovní hrozby útoku. Elektronický bezpečnostní systém představuje bezpečnostní mechanizmus pro odstranění této hrozby.

3.4 Prognóza bezpeľnostního vývoje

Bezpeľnostní mechanizmy se stále mŋní a zdokonalují, je potŚeba vzít v potaz bezpeľnostní vývoj v pŚípadŋ zmŋn firemních bezpeľnostních mechanizmŢ. Vývoj bezpeľnostních mechanizmŢ reaguje na stále rostoucí vývoj hrozeb pŢsobících na aktiva spoleľnosti. PŚi takových zmŋnách ï na lidské ľinnosti nezávislých i zmŋnách vyvolaných zámŋrnŋ vždy dochází k urľitému ohrožení stability a jistot, a rovnŋž k omezování.

Vývoj pŚípadných útokŢ na aktiva spoleľnosti ľi informaľní systémy se za posledních nŋkolik málo let posunul mílovými kroky dopŚedu. Vŋtšina útokŢ je realizována prostŚednictvím elektroniky a poľítaľového pokroku. Ale poŚád platí, že nejvŋtší hrozbou pro jakoukoliv spoleľnost je lidský faktor v podobŋ zamŋstnancŢ firmy. Ale hrozba lidského faktoru se zvŋtšuje se stále rostoucím bezpeľnostním vývojem.

3.5 Navrhovaná opatŚení

Hlavním cílem této kapitoly je zdokonalit zabezpeľení aktiv spoleľnosti a odstranŋní identifikovaných slabých míst. V rámci navrhovaných zmŋn v zabezpeľení aktiv spoleľnosti bezpeľnostními prvky bylo zohlednŋno i to, jakým smŋrem se ubírá bezpeľnostní vývoj. Z tohoto dŢvodu byl kladen dŢraz spíše na zabezpeľovací prvky s pokrokem elektroniky, kterými firma doposud v podstatŋ nedisponovala. Firma se doposud spoléhala spíše na zabezpeľovací prvky, jako je bžžná evidence klíľŢ.

Veškerá mnou navrhovaná opatŚení jsou uvedená v registru aktiv (v kapitole 3.2.), jako P, které pŚedstavuje plánovaná opatŚení pro odstranŋní slabých míst aktiv.

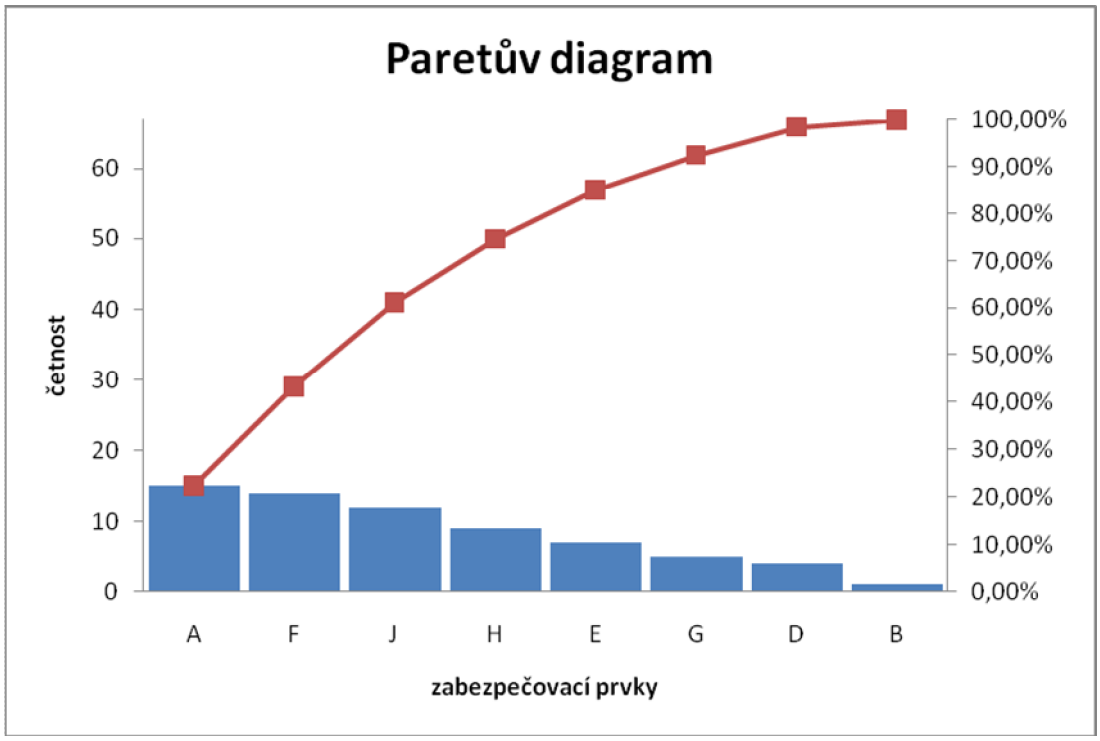
3.5.1 Využití Paretova diagramu[24, 25, 26]

ParetŢv diagram byl již využit v kapitole Hodnotová analýza pro zjištŋní souľasného stavu zabezpeľení aktiv spoleľnosti Hospital Systems s.r.o. Z diagramu v kapitole Hodnotová analýza bylo zŚejmé, že pro dosažení zabezpeľení aktiv spoleľnosti staľí z více jak 50% zabezpeľení bžžnými zámky ï evidencí klíľŢ a požárními detektory. Jinými slovy Śeľeno, že spoleľnost doposud v podstatŋ nepŚikládala žádnou váhu vývoji bezpeľnostních mechanizmŢ a využívání technického pokroku k využití slabého místa útoľníkem.

[24] ParetŢv diagram, *http://lorenc.info/3MA112/paretova-analyza.htm*
[25] ParetŢv digram, *www.businessinfo.cz/files/2005/061019_nastroje-rizeni-jakosti-1.pdf*
[26] Zuzák, R., *Krizové Śízení podniku*, Professional Publishing, Praha, 2004

Druh zabezpeļení	Ļetnost	Ļetnost v %	Kumulativní ļetnost
A	15	22,4 %	22,4 %
B	1	1,5 %	23,9 %
C	0	0 %	23,9 %
D	4	5,9 %	29,8 %
E	7	10,4 %	40,2 %
F	14	20,9 %	61,1 %
G	5	7,5 %	68,6 %
H	9	13,4 %	82 %
I	0	0 %	82 %
J	12	18 %	100 %
Celkem:	67	100 %	

Tabulka 5 - ļetnosti zabezpeļovacích prvkŢ, zdroj:vlastní



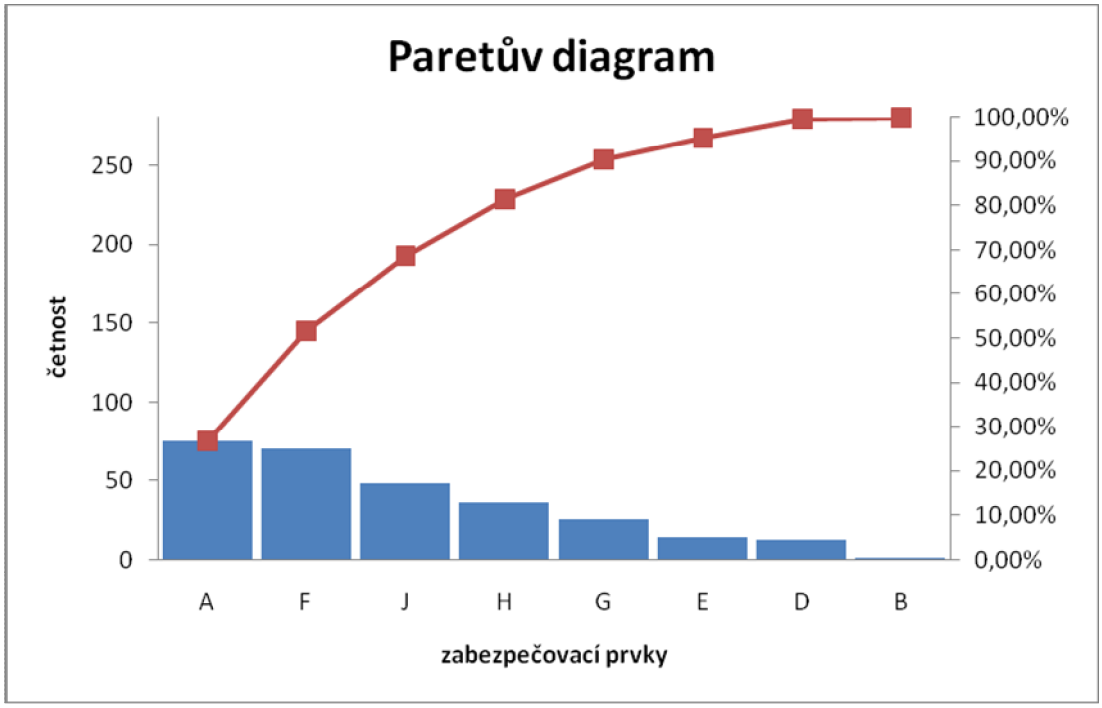
Obrázek 6 - ParetŢv diagram (navrhovaná opatŚení), zdroj: vlastní

Z diagramu je zŚejmé, ģe bĎģné zámky ï evidence klíļŢ a poģární detektory jiģ netvoŚí tak velkou ļást v zabezpeļení aktiv, jako doposud. Výraznou mĎrou bylo rozģíŚeno zajiģtĎní napájení v místnostech, ve kterých je to nezbytnĎ nutné a ve kterých tento zabezpeļovací prvek doposud chybĎl.

Vzhledem k tomu, ģe jednotlivé zabezpeļovací prvky mají pro optimalizaci zabezpeļení aktiv spoleļnosti rŢznou dŢleģitost, byla jednotlivým zabezpeļovacím prvkŢm pŚiŚazena jejich váha.

Zabezpeļení	Ļetnost	Váha (1-5)	Ļetnost*váha	Ļetnost v %	Kumul. ļetnost
A	15	5	75	26,7 %	26,7 %
B	1	1	1	0,4 %	27,1 %
C	0	1	0	0 %	0 %
D	4	3	12	4,3 %	31,4 %
E	7	2	14	5 %	36,4 %
F	14	5	70	24,8 %	61,2 %
G	5	5	25	8,9 %	70,1 %
H	9	4	36	12,8 %	82,9 %
I	0	1	0	0 %	82,9 %
J	12	4	48	17,1 %	100 %
Celkem:	67		281	100 %	

Tabulka 6 - zohlednĎní rŢzné dŢleğitosti zabezpeļovacích prvkŢ, zdroj: vlastní



Obrázek 7 - ParetŢv diagram (navrhovaná opatŚení s pŚidĎlenými váhami), zdroj: vlastní

Navrhované zmĎny vedly pŚedevğím k tomu, ğe aktiva spoleļnosti jiğ nebudou takovou mĎrou závislé na jednou ļi dvou zabezpeļovacích prvcích, ale odstranĎní hrozby ļi slabého místa bude rozloğené na více zabezpeļovacích prvcích. Tímto rozloğením na více zabezpeļovacích prvkŢ se dosáhne kompaktnĎjğího a efektivnĎjğího zabezpeļení aktiv spoleļnosti.

3.6 Shrnutí auditu zajiątění informaąní bezpeąnosti

Ve vąech provĚšovaných oblastech bylo doloąeno, ąe SŘ BI je implementovaný v souladu s poąadavky normy, dostateąnĚ dokumentován v rámci integrovaného systému Ízení. Systém je efektivní, SŘ BI využívá zkuąeností z manaąerských systémĚ ï ISMS, QMS a EMS, se kterými je ve velké míše integrován.

Trvalé zlepąování na základĚ politiky SŘ BI aktualizováno k 20.1.2009. SdĚlování a pochopení politiky je na velmi dobré úrovni. SdĚlování politiky vąem zainteresovaným stranám je v souladu s poąadavky. Celofiremní cíle za rok 2008 v oblasti SŘ BI jsou pševážnĚ splnĚny. Cíle pro rok 2009 jsou ambiciózní se zámĚrem dalšího zlepąování bezpeąnosti informací. PŘezkoumání vedením ï viz záznam ŽZpráva o pŘezkoumání SŘ BIñ ï provedeno na poradĚ vedení 20.2.2009. Dalším zdrojem pro zlepąování jsou interní audity. Záznamy z realizaąních procesĚ jsou dostupné. Řízení dokumentĚ interních a externích záznamĚ odpovídá poąadavkĚm.

Právní a jiné poąadavky ï poąadavky zahrnuté v pŘehledném registru. Registr právních a jiných poąadavkĚ zahrnuje pŘedpisy vztahující se k SŘ BI. Revize provedena k 5.1.2009. Nebyly zjiątĚny nedostatky v této oblasti.

Organizace prohlaąuje, ąe není ve správním Ízení v oblasti bezpeąnosti informací.

RovnĚž byla pŘezkoumána úroveŇ zabezpeąení aktiv spoleąnosti s prognózou vývoje hrozeb a bezpeąnostních mechanizmĚ. Zde byly zjiątĚny asi nejvĚtší nedostatky v celém systému Ízení bezpeąnosti informací, protoąe bezpeąnostní mechanizmy pouąité pro zajiątĚní aktiv spoleąnosti jsou již zastaralé a neschopné takové úrovnĚ zabezpeąení jako dŘíve. Z tohoto dĚvodu byly spoleąnosti navrąeny patŘiąné zmĚny v zabezpeąovacích mechanizmech pro dosaąení vyąší úrovnĚ zabezpeąení.

Silná místa:

- evidentní zájem vedení systematického zabezpeąení informací a dodrąování pŘíslušné legislativy
- celková úroveŇ implementace SŘ BI, jako prĚŘezového poąadavku vąech procesĚ ve spoleąnosti

- kvalifikovaný pracovní tým
- systematický přístup k řešení problémů, incidentů a rizik
- efektivní komunikace s využitím Share Point Services a dokumentace řešení požadavků prostřednictvím Help Desk

Slabá místa:

- nejsou stanovena pravidla pro archivaci dokumentů a záznamů v elektronické podobě. To souvisí nejen s odpovědností za chování příslušného SW a HW po dobu uložení dat, zajištění nemožnosti obsahu (např. ukládáním ve formátu pdf.), ale též vyřešení verzování dokumentů na Portálu tak, aby byly rozlišeny automaticky vzniklé verze od skutečných revizí.
- záznamy o pravidelném testování UPS v serverovně mají být zapisovány v administrátorském deníku. Tam zatím záznamy nejsou vedeny.
- doložení vyhodnocení trvalého souladu s právními požadavky ve zprávě o přezkoumání SŘ BI za rok bezpečnosti informací je stručné i pouze konstatování, že daný předpis je splněn.
- nejsou stanovena pravidla a periody pro pravidelné testování záložních médií, aby se potvrdilo, že jsou v požadovaném čase použitelná k obnovení provozu
- zastaralé bezpečnostní mechanizmy v zabezpečení aktiv společnosti

4. Služby ochrany majetku a osob[27]

Služby ochrany majetku a osob (SOMO) jsou službami poskytujícími fyzickými nebo právnickými osobami na komerčním základě. Jedná se o zákonem upravené služby, konstituované na základě rozhodnutí živnostenského úřadu (orgánu státní správy). Z tohoto vyplývá, že jde o výkon soukromé bezpečnostní činnosti realizované v souladu s koncesní listinou.

Mezi obecné úkoly služeb ochrany majetku a osob při ostraze objektu představují kontrolní propustkovou službu, které slouží k zamezení neoprávněného vstupu a kontroly

[27] Kameník, J., Brabec, F. a kol. *Komerční bezpečnost. Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*.1. vyd. Praha: ASPI, a.s., 2007

osob a dopravních prostředků s cílem zjištění neoprávněného vnášení a vynášení nebo přepravy věcí. Dále se jedná o kontrolní činnost, která by měla zabránit rozkrádání, ztrátám a poškozování majetku. Tato činnost spočívá obvykle v kontrole uzamčenosti dveří, oken, těsnosti nádob apod. Ostraha či střežení objektu, jejichž cílem je nedovolit vstup nepovolaných osob do objektu a odchod z objektu a zabránění vzniku mimořádných událostí nebo zmenšení jejich následků v objektu. Dále je to realizace zásahů či bezpečnostních opatření při mimořádných událostech (např. použití hasicího přístroje bezpečnostním pracovníkem, spolupráce s policií ČR při napadení objektu apod.). Realizace zásahu při signálu EZS představuje reakci SOMO na signály o narušení objektu nepovolanou osobou. A nakonec vyrozumění institucí poskytujících pomoc, jako jsou např. havarijní služby apod.

4.1 Kontrolní propustková služba[28]

Kontrolní propustková služba je nejčastěji se vyskytující činnost služeb ochrany majetku a osob, jejíž cílem je zabezpečení vstupů a výstupů v objektu, jako je např. zabránit vstupu nepovolaným osobám do objektu či vjezdu a výjezdu vozidel do a z chráněných objektů apod. Tato forma služeb ochrany majetku a osob je členěna do několika činností. Těmito činnostmi je kontrola přicházejících a odcházejících osob, kontrola vozidel, smíšená kontrola a kontrola stavu.

Kontrola přicházejících a odcházejících osob spočívá v práci na pevných stanovištích, zpravidla vrátnicích. Pro tuto činnost je nezbytné znát informace, které nám říkají, jaké osoby se v chráněném objektu či prostoru nacházejí, za jakým účelem, jaká mají poslání a oprávnění apod. Tyto informace napomáhají pracovníkům SOMO rozpoznat nežádoucí osobu a zabránit tak jejímu vstupu do objektu či výstupu z objektu. Součástí této činnosti je také kontrolovat osoby zda z objektu něco nevynášejí či do něj nevnášejí.

Kontrola vozidel spočívá v kontrole vozidel vjíždějících do objektu či prostoru, který je chráněn, a vozidel, která z chráněného objektu či prostoru vyjíždějí. Obsah a rozsah kontroly musí být definovaný ve směrnicích pro ochranu objektu či vozidel. Cílem této činnosti není pouze ověřovat oprávnění vjezdu do objektu či výjezdu z objektu, ale také kontrolovat zda nejsou přiváženy do chráněného objektu nedovolené věci nebo zda z něj nejsou vyváženy.

[28] Srov. Brabec, F. a kol. *Hlídací služby*, Praha: Eurounion, 1995

Smíšená kontrola je kombinací kontroly přicházejících a odcházejících osob a kontroly vozidel. Při této činnosti kontrolní propustkové služby je důležité zohlednit pohyb pracovníků na smíšených pracovištích, tak aby nedošlo k zanedbání povinností pracovníků SOMO.

Kontrola stavu souvisí zpravidla s opatřeními k ochraně životního prostředí, ochraně bezpečnosti a zdraví při práci, ochraně protipožární bezpečnosti, protipovodňovou ochranou apod. Tato kontrola se většinou provádí pomocí elektronických monitorovacích systémů. Pro tuto činnost jsou rovněž vyčleněna kontrolní stanoviště, na kterých je kontrola prováděna, ale zpravidla se jedná o záležitost dálkového bezpečnostního dozoru.

4.2 Strážní služba[29, 30]

Strážní služba představuje další z forem služeb ochrany majetku a osob, kterou ale můžeme rozlišovat na službu vykonávanou na pevných stanovištích nebo na pochůzkových strážních stanovištích, kdy hovoříme o tzv. hlídkové službě. Jinými slovy řečeno se jedná o činnost prováděnou na vymezeném pevném strážním stanovišti nebo je prováděna na trase pohybu strážného.

Hlavním cílem této formy služeb ochrany majetku a osob je nenarušenost vnějšího obvodu střeženého objektu či prostoru. Jedná se tedy o doplňkovou formu kontrolní propustkové činnosti, která je prováděna mimo stanoviště kontrolní propustkové služby, s cílem zamezit narušení objektu mimo tato stanoviště. Tato forma jednou z nejrozšířenějších a nejfrekventovanějších forem služeb ochrany majetku a osob.

4.3 Bezpečnostní dohled[31]

Tato forma služeb ochrany majetku a osob obsahuje kontrolu oprávněnosti činnosti a pohybu, dodržování stanoveného vnitřního režimu. Dále také provádí doprovod určených osob a dozor nad pracemi prováděnými externími pracovníky. Rovněž také provádí kontrolu pečetí určených prostor a plní další specifické uložené úkoly. Bezpečnostní dohled probíhá v místech, kam mají přístup i další osoby, jako jsou zákazníci objektu nebo návštěvníci. Když hovoříme o bezpečnostním dohledu, jde především o práci ochranky v supermarketu či kasinech apod.

[29] Srov. Brabec, F. a kol. *Hlídací služby*, Praha: Eurounion, 1995
[30] Nejezchleba, M. a kol. *Vybrané problémy profesní přípravy*, Praha 1993
[31] Nejezchleba, M. a kol. *Vybrané problémy profesní přípravy*, Praha 1993

„Bezpečnostní dohled je významným prvkem systému bezpečnostní prevence, kterou je třeba zařadit do celkového rámce – systému prevence boje se zločinností (kriminalitou) a jinými negativními jevy. Je ji možno chápat jako subsystém tohoto boje a v širším pojetí jako boj s protiprávními jednáními a skutečnostmi. Soukromou bezpečnostní prevenci, prevenci SOMO, lze členit na Obecnou soukromou bezpečnostní prevenci – prevenci SOMO a Speciální soukromou bezpečnostní prevenci."[32]

„Obecná soukromá bezpečnostní prevence se projevuje v tom, že služby ochrany majetku a osob existují a provozují svou činnost na ochranu pořádku, bezpečnosti majetku, osob a jiných bezpečnostních zájmů. Právě tato ochrana v širším rámci se stává do jisté míry zábranou páchání protiprávních jednání (zločinnosti, kriminality), a stávají se tak součástí systému prevence boje se zločinností."[33]

„Speciální soukromá bezpečnostní prevence- speciální prevence SOMO – spočívá ve specifických opatřeních preventivní činnosti realizovaných SOMO za využití stanovených metod činností SOMO, a to především v rámci bezpečnostního dohledu SOMO, jakožto formy činnosti SOMO."[34]

4.3.1 Dálkový dohled zabezpečení objektů

Jedná se o speciální formu bezpečnostního dohledu, kdy zabezpečení je zajištěno na poplachovém signálu vyslaném zabezpečovacím zařízením a následné odpovídající reakci. Signál je vyslaný do přijímacího střediska, pro který se vžil termín pult centralizované ochrany (PCO). Při napojení objektu k PCO se nám naskýtají dvě možnosti, můžeme volit mezi tichým poplachem a poplachem doplněným akustickými a optickými signalizacemi. Tichý poplach bývá upřednostňován v případě, že je pravděpodobný útok profesionálním útočníkem. V tomto případě se zvyšuje pravděpodobnost jeho dopadení. Poplach s akustickými a optickými signály se využívá, když předpokládáme málo zkušeného pachatele, který se akustických a optických signálů zalekne a objekt opustí.

Systém dálkového dohledu je tvořen zabezpečovacím zařízením na objektu, přenosovou trasou, telefonní linkou, radiovým přenosem apod. Zabezpečovací zařízení by

[32] Kameník, J., Brabec, F. a kol. *Komerční bezpečnost. Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*.1. vyd. Praha: ASPI, a.s., 2007

[33] Kameník, J., Brabec, F. a kol. *Komerční bezpečnost. Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*.1. vyd. Praha: ASPI, a.s., 2007

[34] Kameník, J., Brabec, F. a kol. *Komerční bezpečnost. Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*.1. vyd. Praha: ASPI, a.s., 2007

mělo splňovat několik potřebných a důležitých parametrů. V první řadě by mělo být spolehlivé, dále také odolné proti planým poplachům apod. Telefonní linka je považována za spolehlivý prostředek pro přenos signálu (poplachových), což ale v České republice neplatí. Kvalita telefonní sítě dříve nebyla dobrá, postupem docházelo k modernizaci celé sítě, ale na kabelových trasách jsou volně přístupné rozvodné skříně. Proto je použití telefonních linek pro přenos poplachových signálů v ČR velice problematické.

„Telefonní linka ISDN v sobě obsluhuje tři přenosové kanály – dva B-kanály a jeden D-kanál. B-kanál slouží pro přenos hovorového signálu a lze je využít také pro přenos poplachové informace za použití modemu pro analogovou síť. Největší předností linky ISDN je možnost využít pro přenos poplachových informací D-kanál. Ten prioritně přenáší signalizace, lze jej ale využít pro digitální přenos. Výhodou přenosu po D-kanálu je možnost trvalého monitorování přenosové cesty, dobře zkonstruované ISDN komunikátory pak umožňují nejen kontrolu linky NT na obou stranách přenosové cesty, protože přenosová cesta je kontrolována od vstupu komunikátoru na straně objektu až po výstup přijímacího zařízení na straně PCO.“[35] Pak-li, že hovoříme o vstupu a výstupu, tak předpokládáme, že objekt je zdrojem poplachového informace a PCO příjemce. Samotná data je však možno přenášet oboustranně (obousměrně). Rozdíl mezi běžnou telefonní linkou a ISDN spočívá v tom, že u ISDN je možnost neustálého monitorování přenosové cesty.

Pro komunikaci s pultem centralizované ochrany se používají na straně odesílatele (objektu) zařízení označovaná jako komunikátory nebo v případě radiového přenosu tzv. vysílače. V ČR jsou radiové sítě většinou jednosměrné, kdy na straně objektu je vysílač a na straně přijímače PCO. U méně sofistikovanějších systémů se pro přenos signálu užívá nebo přímo kanálů, které mají pouze dva stavy. Je tedy možné přenášet pouze kusou informaci o poplachu. Pro lepší přenos signálu se využívají sofistikovanější systémy, které umožňují přenést stavy jednotlivých komponent systému, což znamená, že se na obrazovce v OS PCO může objevit schéma objektu s vyznačenými detektory, které vysílají signál. Velkou výhodou je, že je možné posoudit, zda jde o skutečný poplach či falešný.

„Nejjednodušší, ale také nejméně výhodnou variantou, jak realizovat přijímací zařízení v dispečinku, je telefonní karta a obslužný software v běžném stolním počítači. Bohužel takovéto řešení nebylo zejména v počátečním období zavádění dálkového dohledu výjimkou

[35] Kameník, J., Brabec, F. a kol. *Komerční bezpečnost. Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*.1. vyd. Praha: ASPI, a.s., 2007

a pravděpodobnému místě, kde přetrvává dodnes."[36] Největší problém tohoto řešení spočívá v malé spolehlivosti vlastního počítače. Proto jediným správným řešením je použití odborného přijímače. Tento přijímač je schopen na displeji zobrazovat a sledovat přicházející zprávy a následně je tisknou a dokumentují. Tímto způsobem by ale nebylo možné realizovat dálkový dohled nad velkým množstvím objektů. Z tohoto důvodu jsou přijímací jednotky připojeny k pracovní stanici nebo počítačové síti operačního střediska. Tento software vykonává řadu funkcí, jakými jsou např. informovat v případě příjmu poplachové zprávy operátora o napadaném objektu, zobrazit příčinu poplachu, sledovat stav zařízení, vyhodnocovat stav přenosové trasy apod.

4.3.2 Obsluha a pracovní postupy

Personální zajištění obsluhy operačního střediska je nezbytné z několika důvodů. Jedná se sice dálkový dohled, ale na operačním středisku musí být zajištěn nepřetržitý dohled. Nepřetržitý dohled musí být zajištěn vždy nejméně dvěma osobami. Každý pracovník operačního střediska musí být prověřen, a to minimálně pro období 10 let před nástupem do této pracovní pozice. Tato prověrka zaměstnanců je důležitá z důvodu, že na operačním středisku pultu centralizované ochrany nesmí být zaměstnáni jednotlivci s pochybnou minulostí, která naznačuje, že dotyčná osoba nemusí být schopná odolat příležitosti k získání nezákonného osobního prospěchu. Operátoři musí nejprve projít základním výcvikem, než jim bude umožněna samostatná činnost bez dohledu. Výcvik je prováděn z důvodu získání základních schopností plnit specifické povinnosti.

Pro zajištění bezpečného a nepřetržitého dálkového dohledu musí být testována funkčnost součástí operačního střediska a výsledky dokumentovány. Testováno je ve dvou časových intervalech, a to v intervalu nepřekračujícím 24 hodin, kdy je testováno vnější spojení na zásahový subjekt nebo jiné složky a vnitřní hodiny veškerého vybavení z hlediska přesného záznamu data a času všech událostí, a v intervalech nepřekračujících 7 dní, kdy jsou testovány hlavní a záložní zdroje, automatické přepínací zařízení, nouzové osvětlení a systém EZS OS PCO a všechny přenosové trasy sloužící k příjmu poplachových signálů včetně vstupních i výstupních komunikačních linek.

Audit operačního střediska pultu centralizované ochrany musí být proveden každých 6 měsíců a musí být plně dokumentovaný.

[36] Kameník, J., Brabec, F. a kol. *Komerční bezpečnost. Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*.1. vyd. Praha: ASPI, a.s., 2007

4.4 Bezpečnostní zásah[37, 38]

Bezpečnostní zásah (bezpečnostní výjezd) je další formou služeb ochrany majetku a osob, která je uskutečňována v návaznosti na dálkový dohled. Tato forma provádění zásahovými skupinami v případě vyhlášení signálu o narušení objektu. V podstatě se jedná o zabránění prohlubování odchylky a následně navrátit stav skutečný do žádoucího stavu.

Bezpečnostní zásah a osoby provádějící bezpečnostní zásah v souladu s ustanovením § 76 odstavce 2 trestního zákona zadržet a předvést pachatele a následně tuto osobu předat orgánům Policie ČR nebo strážníkům obecních či městských policií. Dále zabránit dalšímu napadení majetku, osoby či dalších bezpečnostních zájmů. Zajištění místa činu, ale tak aby nenarušili kriminalistické stopy pro ohledání místa činu Policií ČR, a případné zajištění svědků bezpečnostního incidentu a zjištění jejich totožnosti (tento krok je ale problematický).

[37] Kameník, J., Brabec, F. a kol. *Komerční bezpečnost. Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur.*1. vyd. Praha: ASPI, a.s., 2007

[38] Srov. Brabec, F. a kol. *Hlídací služby*, Praha: Eurounion, 1995

Seznam použité literatury

1. Zákon č.240/2000 Sb., o krizovém řízení. Sbírka zákonů ČR, 2008
2. Nařízení vlády č.462/2000 Sb. k provedení ustanovení § 27 odst. 8 a § 28 odst. 5 krizového zákona
3. Zákon č.101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů ze dne 4. dubna 2000. Sbírka zákonů ČR, 2008
4. Zákon č.412/2005 Sb. o ochraně utajovaných informací a bezpečnostní způsobilosti. Sbírka zákonů ČR, 2008
5. Zákon č.101/2000 Sb., o ochraně osobních údajů. Sbírka zákonů ČR, 2008
6. Hospital Systems s.r.o., Bezpečnostní politika, Pardubice, 2005
7. Hospital Systems s.r.o., Registr aktiv, Pardubice, 2005
8. Rodryľová, D., Staňa, P. Bezpečnost informací jako podmínka prosperity firmy, Grada Publishing, spol. s.r.o., 2000
9. Mlýnek, J. Zabezpečení obchodních informací, Computer Press, a.s., 2007
10. Přibyl, J. Informační bezpečnost a utajování zpráv, ČVUT, Praha, 2004
11. Ľandík, M. Základy informační bezpečnosti, Univerzita Tomáše Bati ve Zlíně, 2004
12. Ľandík, M., Ivanka, J. Bezpečnost v informačních technologiích, Praha, 2003
13. Kameník, J., Brabec, F. a kol. Komerční bezpečnost. Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur.1. vyd. Praha: ASPI, a.s., 2007
14. Zuzák, R., Krizové řízení podniku, Professional Publishing, Praha, 2004
15. Srov. Brabec, F. a kol. Hlídací služby, Praha: Eurounion, 1995
16. Nejezchleba, M. a kol. Vybrané problémy profesní přípravy, Praha 1993
17. Ministerstvo spravedlnosti ČR. Dostupný z WWW: http://www.ms.cz/
18. NBÚ, Národní bezpečnostní úřad. Dostupný z WWW: http://www.nbu.cz/cs/
19. Paretův diagram. Dostupný z WWW: http://lorenc.info/3MA112/paretova-analyza.htm
20. Paretův digram. Dostupný z WWW: http://www.businessinfo.cz/files/2005/061019_nastroje-rizeni-jakosti-1.pdf

Seznam tabulek a obrázkŢ

Seznam pŚíloh

PŚílohy

Příloha 1: Prohlášení vedení společnosti ve vztahu k bezpečnosti informací

Vedení společnosti považuje systém řízení bezpečnosti informací za klíčový pro zajištění všech aktivit společnosti. Základní smysl systému informační bezpečnosti spatřuje v těchto strategických cílech:

- ochrana majetku společnosti,
- ochrana dobrého jména společnosti,
- ochrana dat zákazníků,
- ochrana dat zaměstnanců,
- zajištění shody s platnou legislativou.

Z toho důvodu vedení společnosti:

- stanovuje role a jejich pravomoci a odpovědností v oblasti bezpečnosti informací,
- propaguje význam plnění strategických cílů bezpečnosti informací v rámci organizace, odpovědnosti vyplývající ze zákona a potřebu soustavného zlepšování,
- zajišťuje dostatečné zdroje pro provoz a zlepšování systému informační bezpečnosti,
- eliminuje rizika a stanovuje kritéria pro akceptaci rizik a akceptovatelnou úroveň rizika,
- provádí pravidelné přezkoumání přiměřenosti a účinnosti systému informační bezpečnosti včetně této politiky

Hlavní požadavky na ochranu informací

- jsou zabezpečeny požadavky vyplývající ze smluvních závazků, obecně závazných právních předpisů a stanovena odpovědnost za jejich plnění,
- je stanovena doba kritické dostupnosti informací v souladu s jejich významem pro obchodní aktivity a tato dostupnost musí být zajištěna,
- jsou stanovena opatření k zamezení nežádoucí (neoprávněné) modifikace, ztráty nebo zneužití informací v datových agendách společnosti,
- je vytvořen plán pro zajištění aktivit společnosti v případě bezpečnostních incidentů na úrovni havárie.

Principy naplnění požadavků na ochranu informací

- adresné pravomocí a zodpovědností,
- co není povoleno, je zakázáno,
- síla a cena bezpečnostních opatření je úměrná rizikům,
- osoby zúčastněné v procesech systém informační bezpečnosti mají odpovídající znalosti příslušných pravidel chování v rámci systém informační bezpečnosti včetně znalosti této bezpečnostní politiky.

Porušení

- Porušování těchto ustanovení zaměstnanci společnosti je chápáno jako bezpečnostní incident, který má vliv na bezpečnost informací a v těchto intencích musí být řešen.
- Příčiny porušení musí vedení analyzovat a přijímat účinná opatření s cílem učení se z těchto událostí.

Za naplňování těchto ustanovení odpovídají všichni zaměstnanci v rozsahu svých kompetencí.

Příloha 2: Systém řízení bezpečnosti informací

Předpisy pro správu:

Příručka systému řízení bezpečnosti informací (SŘBI) – vymezuje rozsah systému bezpečnosti informací a stanovuje postupy zajištění bezpečnosti nebo se na ně odkazuje

Analýza aktiv – inventarizace a ohodnocení informačních aktiv

řízení rizik - identifikace a vypořádání rizik

Postupy pro správce – postupy zálohování a nastavení přístupu pro správce

Všeobecné předpisy:

Informační řád – základní pravidla pro práci s informacemi určená všem zaměstnancům

Dokumentační řád – stanovuje klasifikaci dokumentů dle obsažených informací a pravidla pro nakládání

Provozní řád – stanovuje klasifikaci prostor a pravidla přístupu

řízení přístupu k IS – pravidla přístupu zaměstnanců k informačním prostředkům

Zálohování lokálních dat – pravidla pro zálohování a archivaci lokálních dat zaměstnanců

řešení incidentů vnitřního IS - co mám udělat, když se stane

Vzdálená správa – řešení přístupu k IS zákazníka vzdálenou správou

Externí subjekty – pravidla pro nastavení vztahů a spolupráci s externími subjekty

Návody – podrobné návody a pomoc k jednotlivým úlohám informační bezpečnosti

Plány a záznamy:

Politika bezpečnosti informací – stanovuje základní strategii společnosti v oblasti ochrany a bezpečnosti informací a je dále rozvíjena Bezpečnostní politikou

Prohlášení vedení k SŘBI – detailně rozpracovává strategii bezpečnosti informací

Registr aktiv – seznam informačních aktiv s přidělením odpovědnosti za jejich řízení a ohodnocením významu

Registr rizik – evidence podnětů a analýza rizik pro jejich hodnocení a vypořádání. Dostupné pouze manažerovi ŘBI a bezpečnostnímu správci

Registr externích subjektů – přehled externích subjektů s přístupem k interním informacím a odpovědnost za jejich řízení

Plán monitoring – plán monitorování správného fungování systému bezpečnosti informací

Prohlášení o aplikovatelnosti – přehled aplikovaných opatření dle normy ISO 17799

Dokumentace auditů – plány a zprávy z externích a interních auditů

Zprávy o přezkoumání – zprávy o přezkoumání systému vedením

Registr cizích zařízení – registr zařízení, která nejsou v majetku společnosti a ze kterých se přistupuje k síti nebo k informačním aktivům

Registr sdílených a privilegovaných účtů – seznam sdílených účtů (používaných více uživateli) a privilegovaných účtů (účtů s vyššími právy)