Vysoká škola ekonomická v Praze

Fakulta managementu

Jindřichův Hradec

Katedra managementu informací

Diplomová práce

2007 **Bc. Josef Pinkr**

Vysoká škola ekonomická v Praze

Fakulta managementu

Jindřichův Hradec

Katedra managementu informací

Zacházení s citlivými údaji v organizacích služeb

Vypracoval:

Bc. Josef Pinkr

Vedoucí diplomové práce:

Ing. Tomáš Kincl

Mariánské Lázně, červenec 2007

Prohlášení:

Prohlašuji, že diplomovou práci na téma „Zacházení s citlivými údaji v organizacích služeb“ jsem vypracoval samostatně. Použitou literaturu a podkladové materiály uvádím v přiloženém seznamu literatury.

Mariánské Lázně, červenec 2007

.....

podpis studenta

Anotace

Zacházení s citlivými údaji v organizacích služeb

Práce analyzuje technické, právní a manažerské aspekty zacházení s citlivými klientskými údaji. Na příkladu konkrétní organizace ukazuje, jak jsou tyto požadavky splněny a vytipovává možná zlepšení.

Mariánské Lázně, červenec 2007

Poděkování

Za cenné rady, náměty a inspiraci bych chtěl poděkovat
Ing. Tomáši Kinclovi
z Vysoké školy ekonomické v Praze,
Fakulty managementu v Jindřichově Hradci.

Zvláštní poděkování patří
managementu Parkhotelu Golf Mariánské Lázně, a. s.
za řadu konzultací, podnětů a cenných informací, které mi poskytl,
a umožnil mi tak vypracovat tuto diplomovou práci.

OBSAH

1. ÚVOD 1

1.1 Cíl práce 2
1.2 Metodika 2

2. LEGISLATIVA 4

2.1 Evropská legislativa 4
2.1.1 Aktivity Rady Evropy [8], [26] 6
2.1.2 Směrnice Evropského parlamentu a Rady Evropy 7
2.1.3 Nařízení Evropského parlamentu a Rady č. 45/2001 8

2.2 Legislativa v České republice 8
2.2.1 Zákon č. 2/1993 Sb., listina základních práv a svobod 8
2.2.2 Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech 8
2.2.3 Zákon č. 101/2000 Sb., o ochraně osobních údajů 10
2.2.4 Zákon č. 513/1991 Sb., obchodní zákoník 13
2.2.5 Zákon č. 106/1999 Sb., o svobodném přístupu k informacím 14
2.2.6 Zákon č. 365/2000 Sb., o informačních systémech veřejné správy 15

3. BEZPEČNOSTNÍ POLITIKA 17

3.1 Význam ochrany dat a informací 17
3.2 Bezpečnost systému 18
3.2.1 Fyzická bezpečnost 18
3.2.2 Personální bezpečnost 20
3.2.3 Datová bezpečnost 22
3.2.4 Technická bezpečnost 23
3.2.5 Režimová bezpečnost 23
3.2.6 Komunikační bezpečnost 24

3.3 Kdy a kde informace nejčastěji unikají 26
3.4 Proces řízení bezpečnosti systému [10] 27
3.4.1 Bezpečnostní záměr 27
3.4.2 Analýza rizik [1], [22] 28
3.4.3 Bezpečnostní politika IS 31

3.4.4 Systémové bezpečnostní politiky IS 31
3.4.5 Bezpečnostní opatření 31
3.4.6 Monitoring a audit 31
3.4.7 Akceptování nových potřeb zabezpečení systému 31
3.4.8 Nejčastější nedostatky v řízení bezpečnosti systému 32

3.5 Bezpečnostní politika a ochranné systémy 32
3.5.1 Monitorovací systémy 32
3.5.2 Mechanické zábranné systémy 34
3.5.3 Technické elektrické zabezpečení 34

4. BEZPEČNOSTNÍ AUDIT VE VYBRANÉ ORGANIZACI 36

4.1 Bezpečnost systému 37
4.1.1 Fyzická bezpečnost 37
4.1.2 Personální bezpečnost 46
4.1.3 Datová bezpečnost 49
4.1.4 Technická bezpečnost 51
4.1.5 Režimová bezpečnost 52
4.1.6 Komunikační bezpečnost 57

4.2 Proces řízení bezpečnosti 58
4.3 Ochranné systémy 58
4.3.1 Monitorovací systémy 58
4.3.2 Mechanické zábranné systémy 59
4.3.3 Technické elektrické zabezpečení 60

5. ZÁVĚR 61

SEZNAM POUŽITÉ LITERATURY 66

SEZNAM PŘÍLOH 69

SEZNAM OBRÁZKŮ

Obrázek 1: Pozemek hotelu – parkoviště 38
Obrázek 2: 3. nadzemní patro – místnost se serverem 39
Obrázek 3: Přízemí – recepce 40
Obrázek 4: Přízemí – provozní oddělení 41
Obrázek 5: 1. nadzemní patro – lékař a ordinace 42
Obrázek 6: Přízemí - schodiště č. 3 43
Obrázek 7: 2. nadzemní patro – ekonomické oddělení 44
Obrázek 8: 1. podzemní patro – archiv 45

SEZNAM DIAGRAMŮ

Diagram 1: Připojení jednotlivých oddělení hotelu k serveru 37

1. ÚVOD

Velmi aktuálním tématem v oblasti informatiky je ochrana informací, dat a údajů, a zacházení s citlivými údaji, které v současné praxi zaujímají velmi významné místo. V mnoha vyspělých zemích se tímto problémem zabývají již delší dobu, ale v České republice jsou dosud otázky ochrany informací, dat, informačních systémů a zacházení s citlivými údaji v moderních informačních technologiích dosti podceňovány. V ekonomické a podnikatelské sféře již existuje mnoho případů úniku informací, z nichž většinu lze kvalifikovat jako trestněprávní projev počítačové kriminality.

Důležitým předpokladem prosperity obchodní společnosti je využití znalostí, dat, informací a citlivých údajů svých klientů, které nemá konkurence k dispozici a jsou pro ni jen těžko dosažitelné. Lze konstatovat, že informace jsou nehmotná aktiva, díky nimž může organizace získat konkurenční výhodu. Právě proto se firmy snaží co nejefektivněji využívat dostupné informace. Z tohoto důvodu patří informace zpracovávané v obchodní společnosti mezi její nejcennější aktiva – informace, data a údaje jsou pro společnost nepostradatelné a životně důležité.

Díky rostoucímu významu informací a informačních technologií pro společnost vzniká přirozená potřeba jejich ochrany a zabezpečení. První zmínky o informatice se datují do třicátých let minulého století. V osmdesátých letech minulého století se začíná objevovat pojem bezpečnost zpracování elektronických informací. Tyto informace, data a údaje se začínají zpracovávat pomocí informačních technologií, tím roste objem a význam zpracovávaných informací, jejich následná archivace a objem přenášených informací v elektronické formě. V neposlední řadě začíná docházet k propojování informačních systémů. Současný rozvoj informačních technologií důležitost ochrany informací ještě zdůrazňuje.

Pro úspěšnou realizaci zabezpečení elektronických informací je důležité, aby se všichni zaměstnanci i management společnosti seznámili s danou problematikou alespoň na základní úrovni, uvědomili si tak nezbytnost řízení bezpečnosti a v zájmu prosperity organizace podporovali řešení problematiky bezpečnosti.

V současnosti je v mnoha firmách ochrana elektronických informací a jejich zabezpečení na velmi nízké úrovni. Mnoho manažerů stále postrádá potřebné informace o procesu zabezpečení informací a řešení bezpečnostní problematiky ve firmě se úspěšně

vyhýbá, a to i díky finančním nákladům, které s sebou tento proces přináší. Neuvědomují si však, že zajištění bezpečnosti elektronických informací je jednou z podmínek dosažení ziskovosti a konkurenceschopnosti dané organizace, spolu s vybudováním si dobrého jména společnosti.

Zabezpečením elektronických informací se redukuje možnost znehodnocení nebo poškození jedněch z nejdůležitějších aktiv společnosti, na kterých je mimo jiné závislá její činnost.

Cíl práce

V této diplomové práci se budu zabývat důležitou oblastí, která se týká zacházení s citlivými údaji v organizacích služeb. Cílem práce je popsat a zanalyzovat způsob zabezpečení citlivých údajů ve vybraném podniku a poskytnout celkový pohled na zabezpečení elektronických informací firmy. V závěru zhodnotím, zda organizace vhodně zachází s citlivými údaji na základě evropské a české legislativy.

Metodika

Svou diplomovou práci na téma: „Zacházení s citlivými údaji v organizacích služeb“ jsem rozdělil do pěti základních částí.

Úvod slouží jako krátké seznámení s tématem a s danou problematikou zabývající se zacházením s citlivými údaji a zabezpečením elektronických informací. Je zde také nastíněno několik problémů, na které se budu snažit v průběhu práce najít řešení.

Druhá kapitola se týká vymezení problematiky zabezpečení elektronických informací v návaznosti na platnou legislativu České republiky a na přijatou legislativu v rámci Evropské unie. V první části jsou zmíněny základní evropské směrnice a nařízení Evropského parlamentu a Rady Evropy, ve druhé části české zákony definující práva a povinnosti jednotlivých subjektů při zacházení s citlivými údaji. Při zpracovávání této kapitoly jsem čerpal ze zákonů České republiky, odborné literatury a z textů dostupných na Internetu.

Ve třetí kapitole se podrobněji věnuji problematice bezpečnostní politiky – obzvláště významu ochrany dat a informací. Bezpečnost systému jsem rozdělil do několika

ucelených, logicky strukturovaných podkapitol. Dále jsem se v této kapitole pokusil definovat proces řízení bezpečnosti systému a s tím související nejčastější nedostatky. Kapitola dále pojednává o základních ochranných systémech, které jsou v praxi používány. Jde o monitorovací systémy, mechanické zábranné systémy a technické elektrické zabezpečení, které přispívají k ochraně informací, dat a údajů.

Bezpečnostní audit ve vybrané organizaci je zpracován ve čtvrté kapitole. Věnuji se zde popisu a analýze způsobu zabezpečení citlivých údajů ve vybrané organizaci a snažím se poskytnout celkový pohled na zabezpečení elektronických informací organizace. Při snaze charakterizovat bezpečnostní audit v hotelu Parkhotel Golf Mariánské Lázně, a. s. jsem použil materiály a cenné informace poskytnuté managementem hotelu.

V závěru diplomové práce se snažím o shrnutí popisu současného stavu, zhodnocení, zda byly splněny cíle stanovené v úvodu této práce, a navrhnutí konkrétních nápravných opatření týkajících zabezpečení informací, dat a údajů organizace.

2. LEGISLATIVA

Dnešní společnost by se měla soustředit na oblast zabezpečení jak osobních a citlivých údajů, tak i celých informačních systémů, aby nedocházelo k závažnému porušování právních předpisů. Pokud chceme dodržet tyto předpisy, je nutné nejdříve identifikovat a zdokumentovat požadavky legislativy, které se k zabezpečení vztahují (jako např. zákony, vyhlášky), a požadavky, které vyplývají z uzavřených smluv se spolupracujícími společnostmi.

Zejména je zapotřebí dbát na zajištění souladu v následujících oblastech [10]:

- ochrana osobních údajů,
- dodržování duševních vlastnických práv,
- dodržení podmínek průkazného svědectví,
- užití kryptografických nástrojů v souladu s platnou legislativou,
- při poskytování informací do zahraničí dbát na soulad s tamní legislativou,
- zajištění souladu bezpečnostní politiky s platnou legislativou.

Evropská legislativa

Jednotlivé státy si při vytváření norem začaly uvědomovat, že nelze chránit informace jen na teritoriálním principu. Proto velmi brzy začaly vznikat konvence různých druhů, které byly schopny šetřit práci národním legislativám. Vytvářelo se jednotné mezinárodní prostředí. V tomto prostředí se dodržují stejná pravidla bez ohledu na státní hranice. Došlo k situaci, kdy mnohé vnitrostátní zákony obecně upravující ochranu osobních údajů, byly přijímány později (obzvláště příslušné české zákony) a to již za existence mezinárodních koordinačních norem.

První oficiální orgán, který se začal problémem ochrany informací zabývat z právního hlediska, byla Rada Evropy[1]. Ta v roce 1950 vydala dokument s názvem Konvence o ochraně lidských práv a základních svobod. Konvence obsahovala dva články, které

[1] Evropská rada neboli Evropský summit je hlavním politickým orgánem Evropské Unie, který vznikl na počátku 70. let ze schůzek nejvyšších představitelů členských států. Evropská rada se zabývá většinou záležitostí týkajících se základních oblastí politiky EU (sociální, ekonomická a politická).

popisovaly základní principy, jak zacházet s informacemi. První pokusy o vnitrostátní právní normativy vznikly v roce 1973 ve Švédsku, v roce 1977 ve Spolkové republice Německo a roku 1978 v Rakousku. Dále pak v krátkém časovém období následovalo Dánsko, Francie, Norsko a Lucembursko. Legislativní práce probíhala však i dále na celoevropské úrovni a výsledkem další činnosti Rady Evropy v této oblasti byla Úmluva na ochranu osob se zřetelem na automatizované zpracování osobních údajů, vydaná v roce 1981. [3][1]

První pokus o stanovení opravdu komplexních standardizačních pravidel ve smyslu sjednocení národních pravidel na ochranu osobních dat a zejména pak odstranění bariér pro jejich předávání mezi jednotlivými státy však není spojen s Radou Evropy, ale s Organizací pro hospodářskou spolupráci a rozvoj (OECD). Ta vydala dne 1. října 1980 Doporučení pro ochranu soukromí a toky osobních údajů přes hranice. OECD v něm zejména doporučuje členským státům, aby [8]:

a) do svého vnitrostátního práva zahrnuly principy vztahující se k ochraně soukromí a svobody jednotlivce tak, jak jsou obsaženy v tomto materiálu,

b) odstranily překážky, které v zájmu ochrany osobnosti brání přeshraničnímu toku osobních dat.

Z hlediska právní závaznosti a okruhů působnosti nelze tento dokument počítat k dostatečně významným. Zajímavé jsou na něm však zmiňované principy, které jsou na nadnárodní úrovni použity poprvé. Jedná se o [8]:

1) princip omezení sběru osobních dat (správnost a legálnost),

2) princip kvality osobních dat (adekvátnost účelu, přesnost, úplnost a aktuálnost),

3) princip specifikace účelu sběru osobních dat (stanovení účelu musí předcházet začátku sběru dat),

4) princip omezení užití osobních dat (mohou být zpřístupněna nebo užita jinak pouze se souhlasem subjektu dat nebo na základě zákona),

5) princip záruk bezpečnosti osobních dat (musí být chráněna před ztrátou či neoprávněným přístupem, zničením, užitím, změnou nebo zveřejněním),

6) princip otevřenosti (veřejnost informací o povaze a účelu zpracovávaných osobních dat a o jejich správci),

7) princip účasti subjektu osobních dat (právo na informaci o datech o něm sbíraných, právo na zpřístupnění jeho dat, právo na vymazání, opravu a doplnění),

8) princip odpovědnosti správce osobních dat (odpovídá za dodržování všech výše uvedených principů).

Aktivity Rady Evropy [8], [26]

Dne 28. ledna 1981 schválila Rada Evropy Úmluvu ETS č. 108 o ochraně osob s ohledem na automatizované zpracování osobních dat. Tato úmluva se stala prvním uceleným mezinárodním právním dokumentem v oblasti ochrany osobních údajů, a byla jí dána vysoká důležitost tím, že byla zahrnuta do sféry lidských práv a základních svobod člověka. Jejím účelem je zabezpečit na území každého členského státu pro každého člověka bez ohledu na národnost a místo pobytu respektování jeho práv a základních svobod, zejména práva na soukromí se zvláštním důrazem na automatizované zpracování osobních dat vztahujících se k němu.

Poprvé jsou na této úrovni definovány pojmy: *osobní údaje*, *subjekt osobních údajů*, *automatizovaný soubor dat*, *automatizované zpracování* a *správce osobních údajů*.

Úmluva ETS č. 108 přiznává speciálním typům osobních údajů označení pojmem *citlivé údaje*. Podle článku 6 mohou být *„data prozrazující rasový původ, politické názory, náboženské nebo jiné přesvědčení, jakož i osobní údaje týkající se zdraví nebo sexuálního života automaticky zpracovávána jen tehdy, stanoví-li vnitrostátní právo odpovídající záruky*“. Totéž platí i pro osobní data, která se týkají trestních odsouzení.

Podle článku 12 Úmluva ETS č. 108 předpokládá určení jednoho nebo více úřadů v každé zemi, které budou působit v oblasti ochrany osobních údajů a při spolupráci mezi stranami této úmluvy. V této souvislosti je třeba zmínit, že zejména skutečná existence tohoto úřadu byla jedním z hlavních problémů, které dlouho znemožňovaly podpis a ratifikaci této úmluvy s Českou republikou.

Legislativním základem Evropské unie v této oblasti je již výše zmiňovaná Úmluva o ochraně lidských práv a základních svobod z roku 1950, na kterou se odvolává Zakládací smlouva Evropské unie. K otázkám ochrany osobnosti a osobních údajů se také vyjadřuje velmi podstatný dokument, kterým je Listina základních práv Evropské unie vydána 7. prosince 2000.

Až do roku 1995 nebyla v Evropské unii situace příliš příznivá. Důvodem bylo, že národní zákony o ochraně údajů měly být do jisté míry podobné, avšak existovala mezi nimi celá řada rozdílů. Míra ochrany, zajištěná občanům v členských státech, tak nebyla stejná což v praxi vytvářelo potenciální překážky volnému toku informací.

Směrnice Evropského parlamentu a Rady Evropy

Existuje mnoho směrnic a nařízení Evropského parlamentu a Rady Evropy upravující různé činnosti. Pro potřeby této diplomové práce se zmíním jen o následujících:

Směrnice Evropského parlamentu a Rady č. 95/46/EC

Klíčovou úlohu obecného právního předpisu upravujícího ochranu osobních údajů má v současnosti Směrnice Evropského parlamentu a Rady č. 95/46/EC, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů. Tato směrnice definuje základní pojmy obdobným způsobem jako Úmluva ETS č. 108.

Význam Směrnice č. 95/46/EC pro Českou republiku je mimo jiné dán i tím, že je na seznamu povinných právních předpisů, které musí přijmout kandidátské státy před vstupem do Evropské unie. Česká republika se s požadavky této směrnice vyrovnala přijetím zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

Směrnice Evropského parlamentu a Rady č. 97/66/EC

Směrnici č. 95/46/EC brzy následovala speciální norma – Směrnice 97/66/EC Evropského parlamentu a Rady. Tato směrnice se týká zpracování osobních údajů a ochrany soukromí v sektoru telekomunikací, a její účinnost se datuje k 15. prosinci 1997.

Směrnice Evropského parlamentu a Rady č. 2002/58/EC

Díky rychlému vývoji v oblasti telekomunikací, se v období 5 let musela směrnice č. 97/66/EC nahradit směrnicí novou, a tou byla Směrnice Evropského parlamentu a Rady č. 2002/58/EC. Členské státy jsou díky této směrnici povinny zajistit komunikační důvěrnost prostřednictvím veřejné telekomunikační sítě a veřejně dostupných služeb v oblasti telekomunikací. Mají za úkol vyloučit naslouchání, nahrávání, ukládání, nebo sledování komunikace, bez souhlasu příslušných uživatelů.

Nařízení Evropského parlamentu a Rady č. 45/2001

Další významnou právní normou Evropské unie je Nařízení Evropského Parlamentu a Rady č. 45/2001. Tato směrnice, z 18. prosince 2000, se zabývá jak ochranou jednotlivců s ohledem na zpracování osobních údajů institucemi a orgány, tak volným pohybem takovýchto údajů.

Legislativa v České republice

V České republice je legislativní rámec, který vymezuje zásady práce s citlivými informacemi, zatím neujednocený a koncepčně nevyjasněný. Dosud neexistuje zákon, který by komplexně řešil informační bezpečnost v prostředí elektronického zpracování informací, je však nutné přiznat, že existuje řada zákonů, které porušování ochrany dat definují a postihují. Jedná se o pracovní právo, obchodní zákoník, zákon o ochraně osobních údajů, trestní zákon, zákon na ochranu státního a hospodářského tajemství, zákony o bankách, pojišťovnách, telekomunikacích atd., včetně často podceňovaného zákona autorského.

Zákon č. 2/1993 Sb., listina základních práv a svobod

Základní existující právní normou je Listina základních práv a svobod, která přiznává občanům mimo jiné tyto druhy práv (článek 10) [29]:

1) „*Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno*“.
2) „*Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života*“.
3) „*Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě*“.

Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech

Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech byl první ucelenou obecnou normou České republiky, která upravovala práva a povinnosti provozovatelů při provozování informačních systémů, které nakládají s osobními údaji a

směřující k ochraně těchto informací. Vhodným východiskem byla Úmluva ETS č. 108 o ochraně osob s ohledem na automatizované zpracování osobních dat.

Z aktuálního pohledu jsou snad nejcennější částí tohoto zákona definice jednotlivých pojmů, jsou zde tak definovány nejen pojmy ekvivalentní Úmluvě ETS č. 108 (osobní údaje, subjekt údajů, atd.), ale i další pojmy jako: *informační služba*, *zpracování informace*, *uživatel*, *zprostředkovatel*.

Tento zákon dosahoval nad rámec Úmluvy ETS č. 108, když tento zákon rozšířil o údaje, které vypovídají o osobnosti a soukromí dotčené osoby a její národnosti, o ochranu informací o politických postojích, kterou blíže specifikoval rovněž ve členství v politických stranách, a navíc doplnil i ochranu údajů o majetkových poměrech.

Naproti tomu je zde, poněkud nepochopitelně, stručně pojat princip účasti subjektu osobních údajů. Z požadavků dle Úmluvy ETS č. 108 se zde objevil pouze požadavek na poskytnutí zprávy o informacích o subjektu údajů uchovávaných v informačním systému, a to jedenkrát do roka bezplatně, nebo za přiměřenou úplatu kdykoli, pokud zvláštní zákon nestanoví jinak.

Porovnání zákona č. 256/1992 Sb. s požadavky Směrnice 95/46/EC

Zákon č. 256/1992 Sb. nedostál zcela stoprocentně požadavkům stanoveným v Úmluvě ETS č. 108, a to již z hlediska vlastního textu normy. K tomu se navíc přidružily aplikační problémy, kdy chyběly podzákonné normy a blanketová norma o síle zákona. Určitým znakem nedostatku pozornosti legislativy na tento zákon je i skutečnost, že tento zákon za 8 let své účinnosti nebyl ani jednou novelizován a dočkal se pouze dvou resortních prováděcích pokynů.

V roce 1995 byla přijata již zmiňovaná Směrnice Evropského parlamentu a Rady č. 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů. Ta v porovnání s Úmluvou ETS č. 108 zpřísnila podmínky ochrany osobních údajů, a tím se stala, nejen pro právní řády členských států, ale i pro kompatibilitu právních řádů tzv. kandidátských zemí, rozhodnou.

Zákon č. 256/1992 Sb. byl postaven pouze na aplikaci ochrany osobních údajů při automatizovaném zpracování údajů, a to pouze v rámci systematické činnosti, kterou je provozování informačního systému, přičemž u manuálního zpracování bylo třeba zákon

přiměřeně aplikovat. Mimo působnost zákona tak zůstalo nakládání s osobními údaji vně informačních systémů.

Pojem *osobní údaj* byl vymezen pouze jako informace vztahující se k určité osobě. Směrnice č. 95/46/EC se však vztahuje rovněž na data o *určitelných fyzických osobách*, tzn. těch, které *„nejsou přímo a jednoznačně označeny, ale jejich identitu lze na základě dodatečných údajů nebo dodatečných znalostí zjistit*“. V zákoně č. 256/1992 Sb. chyběla povinnost toho, kdo shromažďuje osobní údaje, informovat občana o jeho právech a o jiných pro něj významných skutečnostech.

Vláda České republiky se na zasedání dne 1. července 1998 usnesla, že ochrana občanů vzhledem k nakládání s osobními daty (jak ve veřejné, tak i soukromé sféře) je nezbytná. Tato ochrana je dána vnitřními potřebami České republiky a jejími mezinárodními závazky. Vláda současně rozhodla o nutnosti připravit zcela novou právní normu, která bude vycházet především z výše uvedených mezinárodních smluv a dokumentů. V rámci těchto smluv bude vláda usilovat o založení úřadu na ochranu osobních údajů, což bude nezávislý kontrolní orgán, který bude dohlížet na dodržování zásad ochrany osobních údajů při jejich shromažďování a dalším nakládání s nimi.

Zákon č. 101/2000 Sb., o ochraně osobních údajů

Dne 1. června 2000 nabyl účinnosti zákon č. 101/2000 Sb. o ochraně osobních údajů a změně některých zákonů, který nahradil zákon 256/1992 Sb. o ochraně osobních údajů v informačních systémech. Cílem této právní úpravy je snaha harmonizovat vnitrostátní úpravu s právem EU, kde jak již bylo zmíněno, je ochrana osobních údajů řešena převážně Úmluvou Rady Evropy č. 108/1981 o ochraně osob s ohledem na automatizované zpracovávání osobních údajů a Směrnicí Evropského parlamentu a Rady č. 95/46/ES o ochraně osob se zřetelem na zpracování osobních dat a o volném pohybu takových dat.

Zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů se uplatňuje prakticky ve všech obchodních společnostech. Zákon se týká podmínek zpracování osobních údajů automatizovaně v informačních systémech nebo v systémech nevyužívajících výpočetní techniku.

Zákon se vztahuje na údaje zpracovávané v § 3 [31]:

- „*státními orgány*,
- *orgány územní samosprávy*,
- *orgány veřejné moci*,
- *fyzickými a právnickými osobami*“.

Zákon se nevztahuje na zpracování osobních údajů, které fyzická osoba zpracovává výlučně pro svoji osobní potřebu – příkladem může být osobní seznam telefonních čísel.

Základní pojmy uvedené v tomto zákonu jsou vymezeny v § 4 [31]:

- „*osobní údaj*,
- *citlivý údaj*,
- *subjekt údajů*,
- *správce osobních údajů*,
- *zpracovatel osobních údajů*“.

Jelikož tato práce z velké části vychází právě ze zmiňovaného zákona č. 101/2000 Sb., o ochraně osobních údajů, rozhodl jsme se tento zákon popsat podrobněji a vyzdvihnout důležité části tohoto zákona.

Vymezení pojmů

V tomto zákoně jsou vymezeny důležité pojmy, které jsou předmětem zájmu této diplomové práce. Mezi ně patří tyto pojmy vymezené v § 4 zákona č. 101/200 Sb. [31]:

Osobní údaj – jakýkoliv „*údaj týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze na základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu*“.

Citlivý osobní údaj – je definován jako „*osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v politických stranách či hnutích, náboženství a filozofickém přesvědčení, trestné činnosti, zdravotním stavu a sexuálním životě subjektu údajů*“.

Subjekt údajů – rozumí se jím „*fyzická osoba, k níž se osobní údaje vztahují*“.

Správce osobních údajů – je chápán jako každý „*subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a zodpovídá za ně*“.

Zpracovatel osobních údajů – každý subjekt, který „*na základě zvláštního zákona nebo z pověření správcem zpracovává osobní údaje*“.

Práva a povinnosti

Práva a povinnosti při zpracování osobních údajů jsou vymezeny a popsány v § 5 a § 9. Z nich plyne, že „*správce je povinen stanovit účel, k němuž mají být osobní údaje zpracovány, stanovit prostředky a způsob zpracování osobních údajů, zpracovávat pouze pravdivé a správné údaje, shromažďovat pouze osobní údaje v nezbytném rozsahu pro naplnění stanoveného cíle, uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování*“. Správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů, pokud není stanoveno jinak (např. zvláštním zákonem).

Předání osobních údajů do jiných států

Tento zákon se také zabývá úpravou podmínek předávání osobních údajů jak do členských států Evropské unie, tak do třetích zemí.

Zejména s otevíráním trhu práce roste význam předávání údajů do zahraničí, přičemž se v daném případě může jednat o datovou komunikaci nejrůznějšího typu mezi zaměstnavateli a zaměstnanci, sídly zaměstnavatelských organizací a jejich pobočkami, předávání dat o zaměstnancích veřejnoprávním orgánům jiných států i nejrůznější další způsoby.

Obecně platí, že z České republiky do jiných států mohou být osobní údaje předány pouze tehdy, když právní úprava cílového státu, kde mají být zpracovány, odpovídá požadavkům stanoveným v českém zákoně č. 101/2000 Sb. Prakticky ovšem nepůjde o individuální posuzování dílčích ustanovení jednotlivých zahraničních právních norem. V zásadě jde o kompatibilitu právního prostředí uvedených států s Úmluvou ETS č. 108 a Směrnicí č. 95/46/EC, kterou z úřední povinnosti na základě svých kontaktů a vazeb posoudí Úřad pro ochranu osobních údajů a výsledek pro jednotlivé státy oznamuje patřičným způsobem. Toto pravidlo je stanoveno ve vztahu ke zcela obecnému adresátovi a týká se tedy jak správců či zpracovatelů osobních údajů, tak subjektů osobních údajů

samotných. A zatímco subjekt údajů nelze za nezákonné zacházení se svými údaji účinně postihnout, svědčí uvedené pravidlo zejména správcům osobních údajů. [8]

Postavení a působnost Úřadu na ochranu osobních údajů

Úřad je nezávislý orgán, do jehož činnosti lze zasahovat jen na základě zákona, a který provádí dozor nad dodržováním povinností stanovených tímto zákonem. Tyto povinnosti jsou popsány v § 29.

Úvodní ustanovení zákona vymezuje existenci Úřadu pro ochranu osobních údajů, který má zaručené právo na ochranu občana před neoprávněným zasahováním do jeho soukromého a osobního života neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů. V současné společnosti je vlivem rozvoje informačních technologií toto právo stále více narušováno. [27]

Na složení zaměstnanců Úřadu a jejich činnost dohlíží předseda Úřadu, jímž je v současné době RNDr. Igor Němec.

Zákon č. 513/1991 Sb., obchodní zákoník

Pro obchodní společnosti je významným nehmotným aktivem *obchodní tajemství*. Právní otázky spojené s obchodním tajemstvím jsou řešeny v obchodním zákoníku (zákon č. 513/1991 Sb.).

V ustanovení obchodního zákoníku, konkrétně v § 17, se uvádí, že „*Obchodní tajemství tvoří veškeré skutečnosti obchodní, výrobní čí technické povahy související s podnikem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu, nejsou v příslušných obchodních kruzích běžně dostupné, mají být podle vůle podnikatele utajeny a podnikatel odpovídajícím způsobem jejich utajení zajišťuje*“.

Uvedené vymezení pojmu obchodního tajemství je značně široké, nicméně lze je zhruba rozdělit na dvě části. První část bývá označována jako „know-how“ společnosti, druhou část lze nazvat skutečnostmi obchodní povahy (například seznamy odběratelů a dodavatelů, adresy obchodních zástupců a dealerů, obchodní strategie a plány).

Při porušení práva na obchodní tajemství náleží podnikajícímu subjektu právní ochrana. Obchodní zákoník však již vůbec neřeší, co se rozumí utajením obchodního tajemství. Z obchodního zákoníku tudíž nevyplývají podmínky pro zabezpečení obchodního tajemství. [10].

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím

Zákon o svobodném přístupu k informacím, který nabyl účinnosti 1. ledna 2000, upravuje podmínky práva svobodného přístupu k informacím a stanoví základní podmínky, za nichž jsou informace poskytovány.

V tomto zákoně jsou stanoveny *subjekty*, které mají podle tohoto zákona povinnost poskytovat informace vztahující se k jejich působnosti. Těmito subjekty jsou podle § 2 tohoto zákona [33] tyto:

- „*státní orgány,*
- *orgány územní samosprávy,*
- *subjekty, kterým zákon svěřil rozhodování o právech, právem chráněných zájmech nebo povinnostech fyzických nebo právnických osob v oblasti veřejné správy*“.

Základní pojmy

Zde jsou uvedeny základní pojmy vymezené v § 3 zákona o svobodném přístupu k informacím [33], se kterými se můžeme v běžné praxi setkat:

Žadatel – každá „*fyzická i právnická osoba, která žádá o informaci*“.

Zveřejněná informace – je to taková „*informace, která může být vždy znovu vyhledána a získána, zejména vydaná tiskem nebo na jiném nosiči dat umožňujícím zápis a uchování informace, vystavená na úřední desce, s možností dálkového přístupu nebo umístěná ve veřejné knihovně*“.

Doprovodná informace – jedná se o takovou informaci, která „*úzce souvisí s požadovanou informací (například údaj o její existenci, původu, počtu, důvodu odepření, době, po kterou důvod odepření trvá a kdy bude znovu přezkoumán, a dalších důležitých rysech)*“.

Ochrana osobnosti a soukromí

V § 8 je definována ochrana osobnosti a soukromí, která nám říká, že „*informace, které vypovídají o osobnosti a soukromí fyzické osoby, zejména o jejím rasovém původu, národnosti, politických postojích a členství v politických stranách a hnutích, vztahu k náboženství, o její trestné činnosti, zdraví, sexuálním životě a majetkových poměrech,*

povinný subjekt poskytne pouze tehdy, stanoví-li tak zvláštní zákon[2]*, nebo s předchozím písemným souhlasem žijící dotčené osoby*“.

„*Písemnosti osobní povahy, podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy poskytne povinný subjekt jen za podmínek stanovených zvláštním zákonem*“.

Žádost o poskytnutí informace

Žádost o poskytnutí informace se podává ústně nebo písemně, a to i prostřednictvím telekomunikačního zařízení.

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy

V tomto zákoně jsou stanovena určitá práva a povinnosti osob, která souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy.

Základní pojmy

Přehled základních pojmů, tak jak je vymezuje § 2 zákona o informačních systémech veřejné správy [34]:

Informační činnost –taková činnost, ve které jde o „*získávání a poskytování informací, reprezentace informací daty, shromažďování, vyhodnocování a ukládání dat na hmotné nosiče a uchovávání, vyhledávání, úprava nebo pozměňování dat, jejich předávání, šíření, zpřístupňování, výměna, třídění nebo kombinování, blokování a likvidace dat ukládaných na hmotných nosičích*“. Informační činnost je prováděna správci, provozovateli a uživateli informačních systémů prostřednictvím technických a programových prostředků.

Informační systém – definuje „*funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost*“.

Správce – rozumí se jím „*subjekt, který podle zákona určuje účel a prostředky zpracování informací a za informační systém odpovídá*“.

Provozovatel – je definován jako „*subjekt, který provádí alespoň některé informační činnosti související s informačním systémem*“.

---

[2] Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech

Informační systémy veřejné správy jsou souborem informačních systémů, které slouží pro výkon veřejné správy. Jsou jimi i informační systémy zajišťující činnosti podle zvláštních zákonů[3].

Správci informačních systémů veřejné správy jsou *„ministerstva, jiné správní úřady, orgány územní samosprávy a další státní orgány*“.

Podle § 3 se zákon [34] nevztahuje na informační systémy veřejné správy vedené:

- *„zpravodajskými službami,*
- *Policií České republiky při prevenci a odhalování trestné činnosti,*
- *Ministerstvem financí v rámci finančně-analytické činnosti,*
- *Národním bezpečnostním úřadem,*
- *Ministerstvem obrany*“.

Úřad pro veřejné informační systémy

Tímto zákonem se také zřizuje se Úřad pro veřejné informační systémy, který je ústředním správním úřadem pro vytváření a rozvoj informačních systémů veřejné správy.

Hlavní činností úřadu je kontrola dodržování povinností stanovených tímto zákonem u orgánů veřejné správy, vyhodnocování projektů mající meziresortní dopady na informační systémy veřejné správy. Dále vyhlašuje standardy, vydává a odnímá pověření právnickým nebo fyzickým osobám k výkonu atestací v rámci informačních systémů veřejné správy, stanovuje pravidla pro sdílení dat a služeb mezi jednotlivými informačními systémy veřejné správy. V neposlední řadě ukládá sankce za porušení povinností stanovených tímto zákonem, ukládá opatření směřující k nápravě nedostatků, a vyjadřuje se k projektům informačních systémů veřejné správy a jejich finančním nárokům.

[3] Zákon č. 89/1995 Sb., o státní statistické službě, ve znění zákona č. 356/1999 Sb., zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, zákon č. 48/1997 Sb., o veřejném zdravotním pojištění, ve znění pozdějších předpisů, zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů, zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů.

3. BEZPEČNOSTNÍ POLITIKA

Bezpečnostní politika je základním pilířem pro řízení bezpečnosti informačního systému organizace. Vyjadřuje bezpečnostní cíle, definuje zásady procesu ochrany, všechny principy, omezení, požadavky, pravidla a postupy, které určují způsob správy, ochrany a distribuce citlivých informací a hodnot informačního systému. Pravidla bezpečnostní politiky jsou nejvyšší úrovní ochranných mechanismů informačního systému. Cílem bezpečnostní politiky je minimalizovat vliv působících rizik. Podle oblasti působení, a tím i různých požadavků na ochranu informací, se bezpečnostní politika může velmi lišit (např. armáda, výzkumné ústavy, finanční sektor, atd.).

Bezpečnostní politika se však nesmí chápat jako pojistka proti úniku informací nebo vzniku škody, je to prostředek, který redukuje rizika výskytu nebezpečí a určuje všeobecná pravidla a postupy pro různé systémy [3][1].

Význam ochrany dat a informací

V dnešním světě mají data a informace klíčovou roli. Obzvláště v tržním světě představují významnou výhodu (popř. nevýhodu) pro soutěžící subjekty. Cenu informací ještě umocňuje počítačová technologie, která je spjata se současným životním stylem velice úzce.

Pod pojmem informace je třeba si představit texty, číselné údaje, e-mailové zprávy, počítačové soubory apod. Hodnotu těchto dat a informací většinou oceníme, až když je ztratíme. Zatímco získávání a sběru, evidování, zpracovávání či archivování dat a informací se věnuje značná pozornost, ochraně před zneužitím se dosud tolik pozornosti nevěnuje. Výjimkou jsou většinou jen specializovaná odvětví (armáda, policie, vrcholové státní instituce, výzkumné ústavy apod.), i když i u nich se lze setkat s krádeží, či odcizením důležitých dat a informací.

Pojem ochrana informací představuje zajištění důvěrnosti, integrity a dostupnosti informace. Tyto pojmy jsou definovány takto [10]:

- *důvěrnost* – prevence proti neoprávněnému užití informace,
- *integrita* – prevence proti neautorizované modifikaci informace,
- *dostupnost* – prevence proti znemožnění oprávněného informaci použit.

Ochrana informací se stává významným faktorem dlouhodobého úspěchu či naopak neúspěchu podniku. Složité společenské a ekonomické podmínky vedou nejen k ochraně jednotlivých informací, ale především k ochraně informačních systémů jako celku. V těchto informačních systémech se totiž v současné době soustřeďují informace tak, aby je bylo možné efektivně využívat. Ztráty, které vznikají poškozením, zneužitím nebo zničením, ať už části, nebo celého takového informačního systému bývají katastrofální a někdy i nenahraditelné. To si začínají mnohé organizace a instituce uvědomovat, zejména po rozšíření možnosti výpočetní techniku využívat.

Bezpečnost systému

Celková bezpečnost informačního systému je dána bezpečností jeho jednotlivých částí, zejména jeho nejslabší částí.

Bezpečnostní informační politikou v rámci řízení organizace budeme rozumět souhrn organizačních a řídících opatření, norem, standardů a pravidel, jejichž východiskem je ohodnocení informací jako jednoho z aktiv organizace, zhodnocení jejich ohrožení, stanovení rizik a návrh jejich ochrany v rámci technických, technologických, organizačních, personálních a dalších opatření jako nedílné součásti systému řízení organizace a koncepce jejího rozvoje. Předmětem nebo objektem ochrany je tedy informace a informační systém.

Fyzická bezpečnost

Fyzická bezpečnost se zabývá zabezpečením budov, ve kterých je informační systém umístěn, ochranou před přírodními vlivy a opatřeními proti neoprávněnému vniknutí osob do objektů. Do fyzické bezpečnosti také spadá zabezpečení uložení datových nosičů s informacemi (diskety, výměnné disky, magnetické pásky) a tiskových výstupů, způsoby ničení již nepotřebných informací a médií, ochrana proti požáru a vodě. Nesmíme také opomenout na technologické vybavení budov, především zajištění nepřetržité dodávky elektrické energie, které také s touto problematikou souvisejí. Cílem fyzické ochrany je eliminace případné hrozby ještě dříve, než přijde do přímého kontaktu s vlastním výpočetním systémem [3][1].

Přírodní katastrofy

Pro přírodní katastrofy je charakteristické to, že je nelze předvídat, nelze jim předcházet a zabránit jejich vzniku. Můžeme se tedy pouze soustředit na snížení a omezení jejich možného dopadu na informační systém a na rychlé odstranění případných nepříznivých následků.

Povětrnostní vlivy, zemětřesení, záplavy, atd. jsou sice málo pravděpodobnými hrozbami, protože jejich výskyt je v naší oblasti přece jen vzácnější, ale nesou s sebou vysoké náklady na odstranění způsobených škod. Je skoro nemožné plánovat je dopředu.

Požáry

Oheň je nebezpečný nejen pro informační technologie, ale také pro obsluhující personál. Při požáru vzniká tzv. druhotné nebezpečí – jednak je zde možnost zničení technologie vodou použitou pro hašení požáru a za druhé hrozí nebezpečí pro obsluhující personál v podobě jedovatých zplodin, kterých se mohou z kouře nadýchat.

Základním opatřením proti požáru je systém zabývající se monitorováním výskytu ohně a kouře, instalace automatických hasicích systémů nebo přenosných hasicích přístrojů. Tuto protipožární bezpečnost lze zvýšit řadou doplňkových technických a režimových opatření.

Technické opatření se zabývá konstrukcí objektů a místností, které by neměly obsahovat snadno hořlavé materiály, popřípadě je chránit instalací protipožárních stěn, přepážek, atd.

Režimová protipožární opatření se týkají především definování zásad práce s hořlavými materiály a způsobů jejich skladování, omezení kouření jen na vymezené prostory a protipožárního školení personálu spolu s definováním postupů pro únik osob z objektu a záchranu majetku.

Výpadky a kolísání elektrické energie

Výpadky elektrického napájení a napěťové špičky jsou dalším možným zdrojem škod. Základním protiopatřením je instalace systémů nepřetržitého napájení a záložních generátorů.

Personální bezpečnost

Zaměstnanec představuje vždy určitou potenciální hrozbu. Jak ukazuje praxe, celá řada majitelů informačních systémů věnuje velké výdaje na zajištění technického a programového zabezpečení, ale často opomíjí vliv lidského faktoru (svých zaměstnanců). U lidí, jako jedné ze součástí informačního systému, narozdíl od ostatních technických subjektů, nelze předem změřit jejich očekávané chování (nelze určit, co udělají).

Personální problematice je nutné věnovat minimálně stejně významnou pozornost jako ostatním oblastem bezpečnosti. Není náhodou, že každá firma považuje kvalitní personál za jeden z nejhodnotnějších majetků podniku.

Ochranu informačního systému před nežádoucím vlivem lidského faktoru zajišťuje personální bezpečnost a ta také definuje jednotlivé druhy personálních hrozeb[3]:

- neoprávněná úprava vlastních přístupových práv ke zdrojům informačního systému,
- záměrné nebo nechtěné poškození dat (jejich vymazání, změna hodnot, přidání nových údajů),
- úprava konfigurace (nastavení některé části nebo celého informačního systému),
- nedodržování stanovených bezpečnostních předpisů, a to jak záměrné, tak i z nedbalosti či neznalosti,
- nelegální instalace vlastních programů a jejich využívání.

S personální bezpečností úzce souvisí i životní cyklus personálu, který je možno obecně rozdělit do čtyř etap [3]:

Výběr nových zaměstnanců

Kvalitní výběr nových pracovníků je jedním ze základních předpokladů zvyšování kvality personálu.V praxi se lze občas setkat s chybou, že se výběrové řízení nových kandidátů zaměřuje pouze na odborné a jazykové znalosti, organizační a řídící schopnosti uchazeče, namísto toho, aby pohled zahrnoval i další významná kritéria výběru jakými jsou morální, osobní a pracovní vlastnosti (pracovní spolehlivost, poctivost, psychická odolnost, dobré rodinné zázemí apod.).

Nejpřísnější kritéria musí mít především výběr zaměstnanců, u nichž se předpokládá přístup k citlivým informacím. Od uchazečů je vhodné požadovat úřední výpis z rejstříku trestů, popřípadě je podrobit testům na požívání alkoholu nebo drog.

Základní příprava a zaškolení nových zaměstnanců

Přijatý zaměstnanec se po seznámení s náplní své práce seznamuje s bezpečnostními předpisy a směrnicemi organizace (mezi které patří: zásady práce s důvěrnými informacemi, pravidelná změna hesla, odhlášení se od systému při opuštění pracoviště, atd.). Absolvování tohoto bezpečnostního školení se zpravidla stvrzuje pracovníkovým podpisem, což vylučuje pozdější námitky a výmluvy pracovníků.

Neméně významné je zapracování nového zaměstnance do konkrétní funkce formou odborného školení nebo samostatného studia. Nově přijatý pracovník by měl mít velmi omezený přístup k citlivým informacím, a až časem, získá-li důvěru zaměstnavatele, by se jeho oprávnění k citlivým údajům a informacím mělo postupně zvyšovat.

Průběžné zvyšování kvalifikace personálu

Bezpečnostní kvality se dosahuje trénováním, kontrolou dodržování bezpečnostních požadavků a směrnic a průběžným bezpečnostním školením. Na rozdíl od toho, odborné kvality se dosahuje především soustavným tréninkem prováděným na cvičných aplikacích a průběžným školením.

Kvalitní, zaškolený a důvěryhodný personál je nutné si udržet. Je to i otázka ochrany vložených investic do personálu. Je důležité vytvářet pocit sounáležitosti s organizací a pocit důležitosti, nabízet hmotný stimul, pracovní perspektivu, sociální programy a umožnit další odborný růst.

Ukončení pracovního poměru

Odcházející zaměstnanec si s sebou odnáší všechny vědomosti a informace (i důvěrné), které na svém pracovišti získal. Při rozvázání pracovního poměru musí být odcházející pracovník poučen o svých povinnostech vůči bývalému zaměstnavateli, popř. se kladou požadavky na mlčenlivost po určitou dobu po jeho odchodu ze zaměstnání.

Zaměstnanci

Vlastní pracovníci představují nejrizikovější faktor ohrožení informací. Podle odhadů způsobují zhruba 80 % [5] případů porušení ochrany informací. Musíme přitom vzít v úvahu takové vlivy, jako je neodborné zacházení a chyby operátorů, lidské selhání nebo omyl, nespokojenost, zloba a pomstychtivost. Zaměstnanci jsou potenciální hrozbou už

proto, že mají největší znalosti o daném informačním systému, znají jeho funkčnost, způsob zabezpečení a jeho slabé stránky.

Externí a dočasní pracovníci

Jedná se zpravidla o lidi, kteří jsou zaměřeni na krátkodobé nebo úzce specializované práce, mají možnost seznámit se s řadou informací ohledně činnosti informačního systému, a navíc jejich nábor zpravidla neprobíhá podle tak přísných kritérií, jako je tomu u stálých zaměstnanců.

Hackeři

Pod tímto názvem rozumíme někoho, kdo se snaží neoprávněně vniknout do cizího počítače a provést v něm neoprávněnou činnost. Může se jednat o mladé nadšence, studenty, ale také o profesionály, kteří cíleně kradou počítačové informace pro průmyslovou nebo politickou špionáž, nebo jiným způsobem vědomě škodí.

Zloději

Zloději se převážně orientují na odcizení výpočetní techniky, a tím získání důvěrných dat. Jedná se o stálou hrozbu informačních systémů. Rovněž krádež záložních kopií, které zpravidla obsahují důležité informace a data informačního systému, představuje pro organizaci velikou hrozbu. Základním pravidlem řešení je důkladné fyzické zabezpečení organizace jako celku.

Datová bezpečnost

Data jsou v informačním systému středem celého dění, systém se buduje a provozuje právě kvůli nim a kvůli jejich citlivosti se chrání a zabezpečuje. Datová bezpečnost je tedy jedním z nejdůležitějších aspektů výstavby a provozu systému. Při posuzování hodnoty, kterou data svému majiteli přinášejí, je nutné rozlišovat morální a finanční cenu informací. Dále je třeba si uvědomit rostoucí důvěrnost informací spojenou s jejich seskupováním.

Ochrana informací, které jsou uloženy v databázích, v mnoha pohledech připomíná ochranu poskytovanou operačními systémy. Řízení přístupu subjektů k jednotlivým objektům (elementům) databáze má mnoho společných rysů, zdroje operačního systému (především programy a soubory) jsou chráněny jako celek. Operační systém pracuje

s fyzickou úrovní objektů, kdežto systém řízení báze dat (SŘBD) pracuje s logickými entitami.

Technická bezpečnost

Doposud žádné technické prostředky nedokáží pracovat bez chyb a výpadků. Technická bezpečnost řeší ochranu dat použitím odpovídajícího technického vybavení. Sem spadá kvalitní výběr vybavení, zajištění potřebné spolehlivosti, servisní služby dodavatelů technologií během provozu systému atd. Jedná se tedy o ochranu dat související s využitím vhodného technického vybavení. Pod tímto pojmem však v technické bezpečnosti chápeme především zajištění dostupnosti a integrity.

Základní problém ve vztahu technického vybavení s uchováváním dat představují paměťová zařízení, disky a pásky, které jako jediná část výpočetní techniky obsahují mechanické součástky. Tato zařízení jsou ve srovnání s ostatními elektronickými součástkami v počítači více poruchové, jelikož vykonávají určité mechanické pohyby.

Technická bezpečnost řeší problém nosičů dat tak, že navrhuje systémy s vysokou redundancí, tj. s vysokou odolností proti chybám. Technické úniky jsou způsobeny poruchami výpočetní techniky a technickou nedokonalostí jednotlivých zařízení.

Paměťové nosiče

Nejen zálohovací pásky a diskety, ale také samotné tiskové výstupy představují další potenciální cestu úniku informací. Vytištěné informace jsou přístupné bez pomoci dalších technických prostředků, zálohovací média obsahují stejné informace, nebo jejich část, jako vlastní informační systém. Z praxe je známo, že zacházení s nimi často neodpovídá ani minimálním bezpečnostním zásadám, ukládají se např. hned vedle počítačů.

Režimová bezpečnost

Tuto bezpečnost tvoří soubor administrativních opatření, nařízení a systému kontrol, který zajišťuje bezpečnost informačního systému. Tyto nástroje pomáhají k respektování právních norem a zákonů (jak mezinárodních, tak národních) a bezpečnostních standardů v provozu informačního systému. Režimová bezpečnost definuje způsoby, postupy a procedury, které je nutné dodržovat pro zajištění bezpečnosti daného systému. Respektování administrativně legislativních metod ochrany je významné z hlediska

trestně-právních následků při narušení bezpečnosti informačního systému. Považuje se za rozhodující kritérium při posuzování charakteru vzniklých škod a určování viníků a míry jejich zavinění.

Základní procedury

Mezi základní procedury režimové bezpečnosti patří ty, které definují režim vstupu do objektů a místností, s tím související způsoby kontroly a vedení přehledu o přítomnosti osob v objektech a vyhrazených prostorech. Součástí těchto procedur je i metodika výběru a prověřování osob pro výkon činností na úsecích zpracovávajících citlivé údaje. Dále se definují povolené a zakázané činnosti uživatelům informačního systému, kontroluje se přístup k jednotlivým zařízením a rozsah oprávnění pro manipulaci s nimi. Používají se kryptografické ochranné prvky, mezi které patří aplikace šifrovacích klíčů, jejich distribuce, uložení a likvidace.

Důležitou procedurou je označování (evidence) médií a postup při jejich likvidaci, způsob bezpečného zálohování dat a uložení záložních a archivních médií. Řeší se zde i postup připojení nového počítače do systému, přidání nového uživatelského účtu, rušení uživatelského účtu, nastavení přístupových práv, postup přihlášení/odhlášení se k/ze systému.

Základní postup a pravidla řešení bezpečnostního incidentu [3]:

- podezření na napadení informačního systému je nutné ihned hlásit,
- všechny diskriminované účty musejí okamžitě změnit heslo,
- kontrola všech účtů, jsou li oprávněné, a zda není nějaký navíc, tzv. černá duše,
- kontrola nastavení přístupových práv a systémové politiky,
- kontrola bezpečnostních vztahů mezi doménami,
- přejmenování účtů s právy administrace.

Komunikační bezpečnost

Ještě v nedávné minulosti sloužily pro výměnu dat pouze diskety nebo jiné výměnné nosiče informace. Pak ale přišlo období spojování počítačů do lokálních (nejen firemních) sítí, a v současnosti nastává doba globální celosvětové komunikace na heterogenních sítích. Komunikační cesty informačních systémů dnes představují jedno z nejdůležitějších

a zároveň nejvíce zranitelných míst, a to z důvodu obtížně sledovatelných toků informací, které probíhají v rozsáhlých veřejných komunikačních systémech.

Počítačovou sítí rozumíme soustavu počítačů, která je vzájemně propojena pomocí spojovacích prostředků do určité komunikační architektury. Při řešení komunikační bezpečnosti se vychází z faktu, že každý samostatný počítač je již zabezpečen, považuje se za důvěryhodný a řeší se pouze ochrana komunikačních cest a přenášených informací.

Počítačové sítě lze nejčastěji rozdělit na sítě lokální (LAN) a sítě rozlehlé (WAN). Někdy lze příslušnost určité sítě do jedné z těchto kategorií určit zcela jednoznačně, zatímco jindy to může být dosti nejasné. Lokální počítačové sítě vznikají především z potřeby sdílet technické a programové prostředky. Naproti tomu rozlehlé sítě vznikají především z potřeby komunikovat a provádět určité činnosti na dálku (elektronická pošta, přenos souborů, videokonference, internetová telefonie atd.).

Základním prostředkem výměny dat je komunikační protokol. Protokolem rozumíme řadu pravidel, která výměnu informace mezi jednotlivými příslušnými stanicemi realizují. Některé přenosové protokoly síťové vrstvy dokáží pracovat jak v lokálních, tak i v rozlehlých sítích (příkladem může být protokol TCP/IP), jiné, např. protokol IPX/SPX, jsou v rozlehlých sítích velmi neefektivní. V dnešní době se navíc stále více ztrácí rozdíl mezi lokálními a rozlehlými počítačovými sítěmi. Síťové operační systémy, určené dříve pouze pro lokální počítačové sítě, mají dnes charakteristické rysy sítí rozlehlých.

Lokální počítačové sítě

Lokální počítačové sítě mají z hlediska bezpečnosti svá specifika. Aktivní i pasivní prvky lokální sítě jsou umístěny v omezeném prostoru jedné nebo několika budov. Na její komponenty je tedy možné uplatnit různé metody fyzické ochrany. Lokální počítačová síť bývá zpravidla vybudována pomocí jednotné technologie. Správa lokální sítě je řízena jednoznačně definovaným síťovým administrátorem, který je podřízen vedení informačního oddělení firmy, a který si může efektivně vynucovat dodržování stanovené bezpečnostní politiky ve všech komunikačních uzlech. Uživatelé lokální sítě jsou zpravidla zaměstnanci jedné organizace, kteří často pracují ve společném oboru a mají k sobě tedy patřičnou důvěru [3][1].

Komunikační cesty

Tyto cesty často představují nejzranitelnější místo informačního systému. Interní sítě LAN lze zabezpečit i fyzickou ochranou, např. bezpečným umístěním kabelového vedení (stíněné trubky, vodiče pod omítkou), avšak u externích sítí WAN známe jen svůj vstupní bod do této sítě (popř. i výstupní) a bezpečnostní kvalita celé přenosové trasy není pod naší kontrolou. V tomto případě lze použít pouze logické principy ochrany dat, mezi které patří např. kryptování přenosu.

Kdy a kde informace nejčastěji unikají

Při hodnocení jakýchkoli úniků nebo zneužití informací se ukazuje, že nejslabším článkem v celém systému ochrany je lidský faktor. Statistiky, které vyplývají ze známých narušení bezpečnosti informačních systémů, jednoznačně ukazují, že zhruba v 80 % [5] případů se jednalo o vlastní zaměstnance, kteří buď záměrně (krádež, pomsta, zlomyslnost), nebo neúmyslně (nezkušenost, neznalost) způsobili škodu. Nebezpečím jsou i externí pracovníci, kteří někdy mají možnost seznamovat se s řadou skutečností, protože jsou za určitých okolností bráni jako vlastní lidé organizace.

Všech těchto skutečností lze využít k narušení bezpečnosti informačního systému. Například nespokojený zaměstnanec, který má zlost na svého zaměstnavatele, může udělat podniku hodně škody tím, že se stává velmi sdílným, nebo dokonce vstupuje do služeb konkurence. V některých případech může dokonce vzniknout zárodek budoucí špionáže díky náhodnému úniku informací, kterého se pracovník neúmyslně dopustil.

Nepochybně nejjednodušší způsobem ztráty dat je přímá krádež tajemství, zejména v tom případě, kdy je velice snadné vloupat se v nočních hodinách do kanceláře, laboratoře či dílny, když jsou tyto místnosti prázdné. Ovšem je to možné také ve dne, před očima zaměstnanců. Souběžně s tím přispívá k velkým úspěchům průmyslové špionáže rozsáhlá škála speciálních metod a technických prostředků (odposlouchávacích, fotografických, snímacích).

Identifikace hrozeb

Identifikují se především ty hrozby, které mohou ohrožovat informace (databáze, data, dokumenty), hardware (servery, pracovní stanice, směrovače, tiskárny, kabely apod.) nebo

software (operační systém, programy, atd.). Při identifikaci hrozeb lze vycházet ze seznamu hrozeb příslušných pro daný typ aktiva, ve kterých jsou jednotlivým skupinám přiřazeny konkrétní hrozby.

Přehled nejčastěji uvažovaných hrozeb [10]:

- pronikání neoprávněné osoby do systému, nepovolené užití aplikace,
- porucha počítače (serveru, pracovní stanice), hardwarového zařízení,
- porucha síťových služeb,
- porucha softwaru,
- chyba uživatele systému,
- nedostatek pracovníků,
- výpadek dodávky elektřiny,
- poškození vodou,
- poškození požárem,
- krádež,
- přírodní katastrofa (zemětřesení, záplavy),
- teroristická akce.

Proces řízení bezpečnosti systému [10]

Proces řízení bezpečnosti systému lze chronologicky rozdělit na následující části:

Bezpečnostní záměr

Aby mohlo být ve společnosti postupně realizováno zabezpečení systému, musí být tímto úkolem pověřen určitý útvar. Nezbytným předpokladem úspěšného budování bezpečnostního systému je podpora nejvyššího vedení. Pověřený útvar zpracuje a předloží nejvyššímu vedení společnosti ke schválení dokument nazvaný bezpečnostní záměr. Tento dokument může být velmi stručný, a mělo by v něm být uvedeno, jakým způsobem bude informační bezpečnost řešena, jaký je cílový stav a jakým způsobem bude tohoto stavu dosaženo. Hlavním cílem každé společnosti je zamezení zneužití, neoprávněné modifikace, poškození, nedostupnosti a zničení informací za účelem minimalizace negativních dopadů.

Analýza rizik [1], [22]

Na základě schválených cílů a postupů k dosažení bezpečného systému je potřeba, aby společnost zmapovala skutečný stávající stav v oblasti bezpečnosti informačního systému. Z tohoto důvodu je potřeba provést analýzu rizik systému z pohledu bezpečnosti. Analýzu rizik je nutno provádět prostřednictvím odborníků, například velké firmy řeší provedení analýzy rizik formou projektu, jehož řešitelský tým je složen z pracovníků externí specializované firmy v dané oblasti a z vlastních pracovníků společnosti.

Výstupními materiály analýzy rizik je zpráva, která popisuje daný stav bezpečnosti systému, obsahuje popis existujících bezpečnostních rizik a obvykle i návrh bezpečnostních opatření k eliminaci rizik na přijatelnou úroveň. V praxi je vhodné výstupní zprávu analýzy rizik rozdělit na dvě části. Část podrobně popisující existující rizika v informačním systému a navrhovaná bezpečnostní opatření určená pro odborné pracovníky firmy z obchodních útvarů, z oblasti IT, organizačního a personálního útvaru, atd.

Provedení analýzy rizik systému je nutný krok ke zjištění skutečného stavu bezpečnosti daného systému. Pokud se analýza neprovede, nejsou známa existující rizika a tudíž není realizace vybraných bezpečnostních opatření efektivní.

Podle podrobnosti jednotlivých analýz lze rozlišit jejich druhy:

Základní přístup

Základní přístup spočívá v zavedení určitých bezpečnostních opatření bez podrobnější analýzy rizik, např. opatření a doporučení některých bezpečnostních norem. Tento přístup lze poměrně rychle realizovat. Problémem může být nezmapování některých závažných rizik. Další nevýhodou je neznalost míry rizik a tudíž možná nevhodnost navržených bezpečnostních opatření. Tím pádem pak budou navržená bezpečnostní opatření neefektivní.

Neformální přístup

Tento přístup vychází ze zkušeností pracovníků a znalosti prostředí informačního systému. Přístup využívá účelových interview s pracovníky společnosti, a úroveň míry rizik je zpravidla určována na základě kvalifikovaného odhadu specialisty v oblasti analýzy rizik. Uvedený přístup provedení analýzy rizik podporuje například metodika

IPAK, která byla vyvinuta v USA. V poslední době se také při provádění analýzy rizik v obchodních společnostech rozšířilo použití metodiky FRAP.

IPAK [2]

Analýza rizik IPAK se realizuje na základě interview pracovníka provádějícího analýzu rizik se specialisty společnosti. Jednotliví specialisté odpovídají při rozhovoru na kladené dotazy. Jde o několik tématických okruhů, kdy každý okruh obsahuje kolem 20 dotazů. Na každý dotaz lze vybrat odpověď z 10 možných úrovní, podle toho, zda je realizováno bezpečnostní opatření či nikoliv.

FRAP [7]

FRAP je metoda vhodná pro vlastní analýzu rizik, ve které se identifikují a popisují bezpečnostní rizika, která jsou specifická pro dané prostředí. Metoda se opírá o řízené workshopy mezi odbornými garanty, uživateli informačního systému či aplikace a pracovníky informatiky odpovědnými za vývoj a provoz systému.

Hlavní výhodou metody FRAP je snaha o otevřenou komunikaci mezi oběma stranami, která přispívá ke sdílení představ a zlepšení vzájemné výměny informací. Často vede k odhalení doposud skrytých bezpečnostních rizik.

Podrobná metoda analýzy rizik

Tato metoda je založena na matematickém výpočtu míry rizik. Metoda umožňuje podrobně zmapovat existující rizika v oblasti bezpečnosti a aplikovat přiměřená bezpečnostní opatření vzhledem k ohodnocení chráněných aktiv. Metoda zahrnuje kroky od stanovení hranice analýzy rizik, identifikace hrozeb a jejich následného ohodnocení až k analýze hrozeb a zranitelností systému a stanovení míry rizik. Nevýhodou uvedené metody je její pracnost a také časová náročnost.

K analýze rizik tohoto přístupu lze využít metodiku softwarového nástroje CRAMM a COBRA. Obě uvedené metodiky byly vyvinuty ve Velké Británii.

CRAMM [19]

Jedná se o metodiku pro zavádění a podporu systému řízení bezpečnosti informací, pro provádění analýzy rizik informačních systémů a sítí, k návrhu bezpečnostních

protiopatření, určování havarijních požadavků na informační systém a k návrhům na řešení havarijních situací.

S použitím metodiky a souboru nástrojů CRAMM je možné provést analýzu rizik informačního systému během jednoho dne, detailně určit hodnotu dat zpracovávaných v informačním systému, stanovit nejrizikovější části informačního systému, navrhnout protiopatření snižující zjištěná rizika, vytvořit a neustále aktualizovat kompletní bezpečnostní dokumentaci, analyzovat všechny druhy informačních systémů, ve všech fázích jejich životního cyklu, atd.

Tato metoda dokáže rychle odpovědět na otázky typu: Jaký vliv může mít nedostupnost, prozrazení nebo modifikace dat na podnikatelské cíle? Jaké hrozby ohrožují systém, jaké slabiny systém má? Jakou úroveň bezpečnosti zvolit, aby byla efektivní a levná? Jak vyhodnotit, které kryptografické služby jsou zapotřebí? Je fyzická bezpečnost Vašeho výpočetního centra dostatečná? A mnoho dalších otázek zabývajících se důsledky analýzy rizik.

COBRA [20]

Tento nástroj umožňuje, aby si společnost sama prováděla kontrolu bezpečnosti systému. COBRA ohodnotí důležitost všech hrozeb a zranitelností vyskytujících se v daném podniku a vytvoří konkrétní návrhy řešení na nápravu současného stavu. V tomto nástroji lze využít automatického spojování rozpoznaných rizik do skupin, tyto skupiny pak automaticky přiřazuje k potenciálním důsledkům, které z existence těchto rizik plynou. Modifikací tohoto nástroje je možnost zkoumat konkrétní problém samostatně, aniž by byly sledovány celkové dopady na společnost.

Při provádění podrobné analýzy rizik externími specialisty za využití specializovaných softwarových nástrojů může někdy dojít k nedocenění názorů a pohledů interních pracovníků společnosti na danou problematiku. Použitá metodika navíc může být pro interní pracovníky společnosti nesrozumitelná tím, že ji externí specialisté drženi v tajnosti

Kombinovaný přístup

Tento přístup spočívá ve vzájemné kombinaci zmíněných metod, čili v kombinaci podrobných metodik analýzy rizik se základním a neformálním přístupem.

Bezpečnostní politika IS

V souladu se závěry analýzy rizik je vypracována bezpečnostní politika informačního systému. Tento dokument definuje východiska pro všechny další aktivity společnosti v oblasti informační bezpečnosti. Po schválení nejvyšším vedením společnosti je tato politika závazná pro všechny zaměstnance společnosti i pro externí pracovníky, kteří informační systém dané společnosti využívají.

Systémové bezpečnostní politiky IS

Základní bezpečnostní principy a zásady obsažené v dokumentu bezpečnostní politiky informačního systému je zapotřebí rozpracovat podrobněji do systémových bezpečnostních politik a do ostatních bezpečnostních předpisů.

Bezpečnostní opatření

Bezpečnostní opatření se týká zajištění postupné realizace těch doporučených opatření, která vyplývají ze závěrů rizikové analýzy, a která jsou v souladu se zásadami platné bezpečnostní politiky. Některá opatření nejsou finančně ani personálně náročná, ta která už náročná jsou, bývají často řešena formou projektů.

Monitoring a audit

Po zavedení bezpečnostních opatření je zapotřebí provádět kontrolu a audit stavu zabezpečení a dle potřeby odstraňovat zjištěné nedostatky.

Akceptování nových potřeb zabezpečení systému

Informační systém každé společnosti se průběžně mění především v důsledku změn obchodních aktivit společností a změn způsobených v důsledku rychlého vývoje informačních technologií. Je zapotřebí, aby společnost prováděla analýzu rizik periodicky, aktualizovala a realizovala potřebná bezpečnostní opatření.

Nejčastější nedostatky v řízení bezpečnosti systému

Mezi nejčastější nedostatky v organizaci a řízení bezpečnosti systému patří [10]:

- informační bezpečnost není managementem podporována nebo je podporována pouze formálně,
- nekomplexnost řízení,
- neexistence některých bezpečnostních rolí nezbytných k vybudování zabezpečeného informačního systému,
- nejasné vymezení pravomocí a povinností pracovníků v oblasti bezpečnosti,
- neexistence klasifikace informací ve společnosti a stanovení pravidel, jak s informacemi jednotlivých tříd nakládat,
- analýza rizik není prováděna periodicky,
- bezpečnostní politika a bezpečnostní předpisy nepokrývají komplexně bezpečnostní problematiku, není prováděna její aktualizace,
- nedostatečně prováděný audit vztahující se na dodržování platných bezpečnostních předpisů,
- nevyvozování postihu vůči zaměstnancům při porušování předpisů,
- nízké povědomí zaměstnanců o bezpečnosti,
- nedostatečné prověření uchazečů na pozici vyžadující vyšší úroveň důvěryhodnosti.

Bezpečnostní politika a ochranné systémy

Bezpečnostní politika úzce souvisí s ochrannými systémy, které lze k zabezpečení informací, dat a údajů použít. Mezi nejzákladnější patří:

Monitorovací systémy

Elektrické zařízení řízeného vstupu a pohybu

Základním úkolem tohoto systému je automatická kontrola vstupu oprávněných osob do objektu, s tím související i jejich pohyb v prostorách tohoto objektu. Systém řízeného vstupu a pohybu je nadstavbou ke zkvalitnění strážní služby daného objektu. Existuje mnoho různých systémů, které se od sebe liší [9].

Fyzikální princip činnosti [9]:

- magnetický proužek,
- čárový kód,
- laserová či čipová karta,
- rezonanční, bezkontaktní vstupník.

Množství poskytnutých informací o nositeli karty [9]:

- oprávnění vstupu do určené zóny,
- osobní údaje apod.

Podle toho, co se od vstupního systému požaduje, lze vybrat vhodný systém pro řízení vstupu a pohybu.

Pro návrh takového systému je důležité specifikovat počet kontrolovaných zón, hierarchii přístupu do těchto zón, množství vyhodnocovaných informací, princip snímání (kontaktní či bezkontaktní), rozlehlost kontrolovaného objektu, a v neposlední řadě důležitý prvek, kterým je požadavek vazby na jiné informační systémy.

Systémy průmyslové televize

Dalším monitorovacím systémem je využití videotechniky, která slouží nejen k zabezpečení objektů. Tyto systémy jsou mimo jiné vhodné také jako podpora klasické elektrické zabezpečovací signalizace. Některé speciální systémy elektronického kamerového střežení mohou část úloh elektrické zabezpečovací signalizace přímo převzít. Příkladem může být uplatnění videotechniky především v oblasti venkovní ochrany ve spojení s mikrovlnnými či infračervenými bariérami.

Video-systém lze využít v kombinaci se systémy kontroly a řízení vstupu, pro určování oprávněnosti vstupu na základě porovnání reálného portrétu osoby s portrétem uchovaným v paměti, atd.

Uplatnění zmíněných monitorovacích systémů pomocí zabezpečovací techniky lze shrnout do následujících úloh monitorování [9]:

- vjezdů a vstupů do objektů a na pozemky,
- parkovišť,
- provozu letišť a přistávacích ploch,

- exponátů např. v muzeích, galeriích apod.,
- bankovního provozu a provozu v obchodních střediscích,
- při kontrole oprávněnosti dokladů, atd.

Mechanické zábranné systémy

Mezi hlavní typy mechanických zábranných systémů patří bariéry a překážky. Jejich úkolem je při napadení objektu vytvořit určitou časovou prodlevu mezi okamžikem napadení objektu a časem jeho dokončení. Tuto časovou prodlevu lze považovat za určité kriterium bezpečnostní úrovně mechanického zábranného systému.

Z hlediska záměru ochrany se jedná o to, jak odpovídajícím způsobem zabránit násilnému proniknutí osob do chráněného prostoru a následnému znehodnocení, narušení či poškození technického zařízení chráněného prostoru. Tím by měl systém bránit krádeži informací, dat a předmětů.

Stupně bezpečnosti mechanických zábranných systému se navzájem odlišují množstvím vynaložené energie, lhůtou potřebnou k jejich překonání a agresivitou použitého nářadí a použitých nástrojů.

Podle tohoto kriteria a celkové koncepce působení v bezpečnostním systému můžeme mechanické zábranné systémy rozdělit na [9]:

- části vnějšího uzavření objektu (ploty, vrata, závory, zdi),
- stavební prvky budov (stěny, podlaha, strop, střecha),
- otvorové výplně budov (dveře, okna, mříže, armované stěny),
- úschovné objekty (schránky, trezory, trezorové místnosti, pokladny, kovové skříně).

Technické elektrické zabezpečení

Technické elektrické ochranné systémy rozdělujeme na dva druhy signalizace:

Elektrická požární signalizace (EPS)

Jde o soubor zařízení sloužící k preventivní ochraně objektů před požárem. Z tohoto hlediska je třeba elektrické požární signalizační zařízení chápat jako pomocné zařízení, které slouží ke zkrácení doby od okamžiku zjištění ohniska požáru k příslušnému požárnímu zákroku. Uživatel se instalací elektrické požární signalizace nezbavuje

odpovědnosti za veškerá jiná protipožární opatření, a tudíž není možné zanedbávat ostatní protipožární opatření, která slouží k celkové ochraně objektu před požárem.

Bezpečnostní systém elektrické požární signalizace musí být trvale v provozu. Signál o zjištěném požáru je přenášen do ohlašovny požáru po chráněné komunikační cestě. Touto cestou může být zajištěno okamžité spuštění funkce hasícího zařízení.

Elektrická zabezpečovací signalizace (EZS)

Tato signalizace plní funkci ochrany majetku a osob. Je ze všech možností zabezpečení tou nejrozšířenější a v praxi nejčastěji uplatňovanou. Detektory slouží k identifikaci narušení objektu. Pracují na různých principech, jakými jsou sledování infračerveného vyzařování pohybujícího se objektu a detekování změny v odrazu mikrovlnného vlnění.

Vlastní návrh a realizace elektrické zabezpečovací signalizace vychází z analýzy bezpečnosti, která je v daném podniku zpracována. Posouzení projektu elektrické zabezpečovací signalizace vychází z kvalitní analýzy následujících faktorů [9]:

- okolí objektu (střešní přístupy, vikýře, sklepní průchody, dvorky, apod.),
- přístupy z veřejně přístupných míst,
- rozvody elektrické energie a jejich přístup v rámci objektu,
- rozvody elektrické energie a jiné rozvody, které jsou ve správě jiné organizace a musí pro ně být přístupné zvenčí,
- vjezdy do garáží ústící ven z objektu,
- podzemní garáže, zejména veřejnosti přístupné, s vchody a výtahy ústícími do chráněného objektu,
- provedení stavby (jako např. velké zasklené plochy, skleněné dveře. vstupy klimatizací, podhledy).

Důležitou vlastností navrženého systému elektrické zabezpečovací signalizace je také způsob přenosu provozní, poruchové a poplachové informace, od čidel směrem k ústředně.

SEZNAM POUŽITÉ LITERATURY

[1] BRECHLEROVÁ, D. *Řešení informační bezpečnosti* [online]. duben 2005, [cit. 2007-08-10]. < http://www.systemonline.cz/clanky/reseni-informacni-bezpecnosti-1-cast.htm>

[2] CSI: Computer Security Institute. *Information Protection Assessment Kit (IPAK)*. 22. 11. 1999, [cit. 2007-08-10]. < http://www.gocsi.com/press/prelea991122.jhtml>

[3] DOBDA, L. *Ochrana dat v informačních systémech*. Praha: Grada Publishing, 1998, ISBN 80-7169-479-7

[4] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, a. s., 2004. ISBN 80-2510106-1

[5] HANÁČEK, P. – STAUDEK, J. *Bezpečnost informačních systémů* [online]. Datum aktualizace není uveden, [cit. 2007-08-09]. s. 14. <http://www.micr.cz/files/479/uvis-Bezpecnost-20000701.pdf>

[6] INTERVAL.CZ. *Většina útoků na informační systém má svůj původ uvnitř firem* [online]. 19. 4. 2002, [cit. 2007-08-09]. <http://interval.cz/tiskove-zpravy/vetsina-utoku-na-informacni-system-ma-svuj-puvod-uvnitr-firem/>

[7] ISSS: Konference Internet ve státní správě a samosprávě. *Proč a jak řídit informační rizika ve veřejné správě* [online]. Datum aktualizace není uveden, [cit. 2007-07-30]. <http://www.isss.cz/archiv/2006/download/isss2006.pdf>

[8] KARDOŠ, D. *Řízení informačních systémů veřejné správy* [online]. 18. 11. 2004, [cit. 2007-01-04]. <http://objekty.pef.czu.cz/2004/sbornik/30_Kardos.pdf>

[9] LÁTAL, I. a kol., *Ochrana informací, dat a počítačových systémů*. Praha: Eurounion s. r. o., 1996, ISBN 80-85858-32-0

[10] MLÝNEK, J. *Zabezpečení obchodních informací*. Brno: Computer Press, a. s., 2007. ISBN 978-80-251-1511-4

[11] Nařízení Evropského parlamentu a Rady č. 45/2001

[12] Parkhotel Golf Mariánské Lázně, a. s. – etický kodex

[13] Parkhotel Golf Mariánské Lázně, a. s. – normy ISO 9001:2000

[14] Parkhotel Golf Mariánské Lázně, a. s. – požární řád

[15] Parkhotel Golf Mariánské Lázně, a. s. – pravidla provozování výpočetní techniky a programového vybavení

[16] Parkhotel Golf Mariánské Lázně, a. s. – vnitřní směrnice a pokyny

[17] Parkhotel Golf Mariánské Lázně, a. s. – zásady bezpečnosti a ochrany zdraví při práci

[18] PŘIBYL, J. – KODL, J.: *Ochrana dat v informatice*. Praha: Monografie ČVUT, 1997.

[19] Risk Analysis Consultants. *CRAMM: Information Security Toolset* [online]. Datum aktualizace není uveden, [cit. 2007-07-30]. <http://www.rac.cz/rac/homepage.nsf/CZ/CRAMM>

[20] Security Risk Analysis & Assessment. *COBRA* [online]. Datum aktualizace není uveden, [cit. 2007-08-10]. < http://www.riskworld.net/>

[21] SMEJKAL, V. – RAIS, K. *Řízení rizik*. Praha: Grada Publishing, 2003. ISBN 80-247-0198-7

[22] SMEJKAL, V. – RAIS, K. *Řízení rizik ve firmách a jiných organizacích*. 2. aktualizované a rozšířené vydání. Praha: Grada Publishing, 2006. ISBN 80-247-1667-4

[23] Směrnice Evropského parlamentu a Rady č. 95/46/EC

[24] Směrnice Evropského parlamentu a Rady č. 97/66/EC

[25] Směrnice Evropského parlamentu a Rady č. 2002/58/EC

[26] ŠMÍD, V. *Ochrana osobních údajů v pracovněprávních vztazích* [online]. 2003, [cit. 2006-11-04]. <http://www.fi.muni.cz/~smid/oouppv.html>

[27] Úřad pro ochranu osobních údajů. *Úřad* [online]. Datum aktualizace není uveden, [cit. 2007-07-28]. <http://www.uoou.cz/index.php?l=cz&m=top&mid=01&u1=&u2=&t=>.

[28] Úmluvu ETS č. 108, o ochraně osob s ohledem na automatizované zpracování osobních dat

[29] Zákon č. 2/1993 Sb., listina základních práv a svobod

[30] Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech

[31] Zákon č. 101/2000 Sb., o ochraně osobních údajů

[32] Zákon č. 513/1991 Sb., obchodní zákoník

[33] Zákon č. 106/1999 Sb., o svobodném přístupu k informacím

[34] Zákon č. 365/2000 Sb., o informačních systémech veřejné správy

[35] ČSN 73 0875 Seznam technických norem. Třída 73 - *Navrhování a provádění staveb*: Požární bezpečnost staveb. Navrhování elektrické požární signalizace.

[36] ČSN 34 2710 Seznam technických norem. Třída 34 – *Elektrotechnika*: Předpisy pro zařízení elektrické požární signalizace.

SEZNAM PŘÍLOH

Příloha č. 1: Půdorys 3. nadzemního patra 70

Příloha č. 2: Půdorys 2. nadzemního patra 71

Příloha č. 3: Půdorys 1. nadzemního patra 72

Příloha č. 4: Půdorys přízemního patra..... 73

Příloha č. 5: Půdorys 1. podzemního patra 74

Příloha č. 6: Půdorys pozemku hotelu 75