UNIVERZITA PARDUBICE
FAKULTA EKONOMICKO-SPRÁVNÍ

BAKALÁŘSKÁ PRÁCE

2007 **Jitka HAVELKOVÁ**

UNIVERZITA PARDUBICE
FAKULTA EKONOMICKO-SPRÁVNÍ
ÚSTAV SYSTÉMOVÉHO INŽENÝRSTVÍ A INFORMATIKY

BEZPEČNOSTNÍ POLITIKA FIRMY

BAKALÁŘSKÁ PRÁCE

AUTOR PRÁCE: Jitka Havelková
VEDOUCÍ PRÁCE: ing. Renáta Bílková

2007

UNIVERSITY OF PARDUBICE
FACULTY OF ECONOMIC ADMINISTRATIVE
DEPARTMENT OF SYSTEMS ENGINEERING AND INFORMATICS

SECURITY POLICY OF FIRM

THESIS

AUTHOR: Jitka Havelková
SUPERVISOR: Ing. Renáta Bílková

2007

Prohlašuji:

Tuto práci jsem vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně Univerzity Pardubice.

V Pardubicích dne 21. 05. 2007

Jitka Havelková

Abstrakt:

Bakalářská práce je zaměřena na bezpečnostní politiku firmy a na informační bezpečnost. Bezpečnostní politika byla vytvářena pro firmu Magnet Blance Porte, pozornost je zaměřena především na oblast IT bezpečnosti, kde je riziko nebezpečí nejvyšší. Byl sestaven dokument bezpečnostní politiky a tým, který zajistí její realizaci. Dokument obsahuje zásady, principy a standardy pro dodržování bezpečnosti a dále stanovuje odpovědnost za jejich dodržování a postup při vzniku nebezpečí. Bezpečnostní politika je dokumentem důvěrným, proto je přístupná jenom stanovenému okruhu lidí. Tuto skupinu tvoří především generální ředitel, správce a oddělení IT. Ostatní zaměstnanci budou o bezpečnostních zásadách informování a proškoleni. Informační bezpečnost je provázána na související legislativní dokumenty v podobě právních předpisů, norem, či plánů EU.

Obsah:

1. Úvod

Současnou společnost lze označit jako společnost informační, firmy v současnosti intenzivně využívají prostředky výpočetní techniky. Na tyto prostředky lidé spoléhají prakticky ve všech činnostech, které provádí: pomocí počítačů uzavírají dohody, komunikují, uchovávají v nich důležité kontakty, podklady pro vedení účetnictví, pro rozhodování či plánování. Firma tedy pracuje efektivněji, s nižšími náklady na čas i finance, ale jen do doby, než nastane nějaký bezpečnostní incident. Ten může být představován útokem hackera stejně jako přírodní katastrofou. Výsledek je v obou případech stejný - nastává problém informačního systému firmy, či dat v něm, ztráta dobrého jména či ztráta finanční.

Jedním z hlavních faktorů pro definování bezpečnostní politiky firmy je poznání bezpečnostního prostředí. Ve všech úrovních tohoto prostředí se mohou odehrávat události různého charakteru, které ovlivňují úroveň bezpečnosti firmy. Proto je analýza bezpečnostního prostředí mimořádně důležitá a čím dál více aktuální.

Informace obsahující utajované skutečnosti, přičemž nakládání s těmito informacemi a přístup k nim určuje legislativa příslušného státu. Obvyklým způsobem ochrany utajovaných informací je jejich klasifikace a následné umožnění přístupu pouze těm osobám, jež byly prověřeny pro příslušný stupeň utajení. Např. v českém právním řádu jsou jako utajované vymezeny ty informace, u nichž by neoprávněné zacházení s nimi mohlo způsobit újmu (poškození nebo ohrožení) zájmu České republiky. Podle stupně utajení a ochrany jsou členěny na informace vyhrazené, důvěrné, tajné a přísně tajné.

Cílem této práce je zmapování vztahu bezpečnostní politiky firmy k jednotlivým oddělením firmy, vymezení základních standardů, zákonů a plánů EU, které se vztahují k informační bezpečnosti a dále sestavení bezpečnostní politiky pro firmu Magnet Blance Porte (dále jen Magnet). V práci bude sestaven tým pro realizaci bezpečnostní politiky firmy Magnet a také bude definována informační bezpečnost a významné dokumenty, které s informační bezpečností souvisí. Práce byla konzultována s IT oddělením firmy Magnet, která poskytla řadu informací ohledně své bezpečnostní politiky, ovšem některé informace poskytnout nemohla, neboť se jednalo o informace neveřejné.

2. Bezpečnostní politika firmy

Základním dokumentem každé společnosti je takzvaná bezpečnostní politika. V každém případě by se mělo jednat o dokument písemný, ústní verze mají nepříjemný sklon k modifikaci, ať chtěné či nechtěné. Bezpečnostní politika by měla odpovídat na několik základních otázek:

- **co** chce firma chránit,
- **proč** to chce chránit,
- **jak** to chce chránit,
- **jak** ověří, že je to opravdu chráněno,
- **co** bude dělat, když se něco pokazí.

Pod pojmem „ochrana informací“ se nachází informační bezpečnost, klasifikace informací a ochrana osobních údajů. Informace může být veřejně přístupná i neveřejná. Neveřejná informace, která má být na základě příslušných zákonů stanoveným způsobem chráněna, může být takto klasifikována:

- důvěrné informace,
- obchodní tajemství[1],
- osobní údaje[2],
- citlivé osobní údaje.

Za klasifikaci neveřejných informací odpovídá odpovědná osoba (správce), a to v souladu se zákonem a vnitřní směrnicí firmy. Písemnosti, datové soubory, nosná média a jiné materiálny obsahující neveřejnou informaci jsou chráněný dokumentem. Cílem zabezpečení neveřejných informací je ochrana soukromí zaměstnanců firmy a ochrana práv společnosti. Taková ochrana je zajišťována s ohledem na technické a finanční možnosti firmy.

Důvěrnou informací se rozumí informace, která nemá charakter žádné z ostatních neveřejných informací, ale je důležité ji (alespoň dočasně) chránit, je určena úzkému okruhu

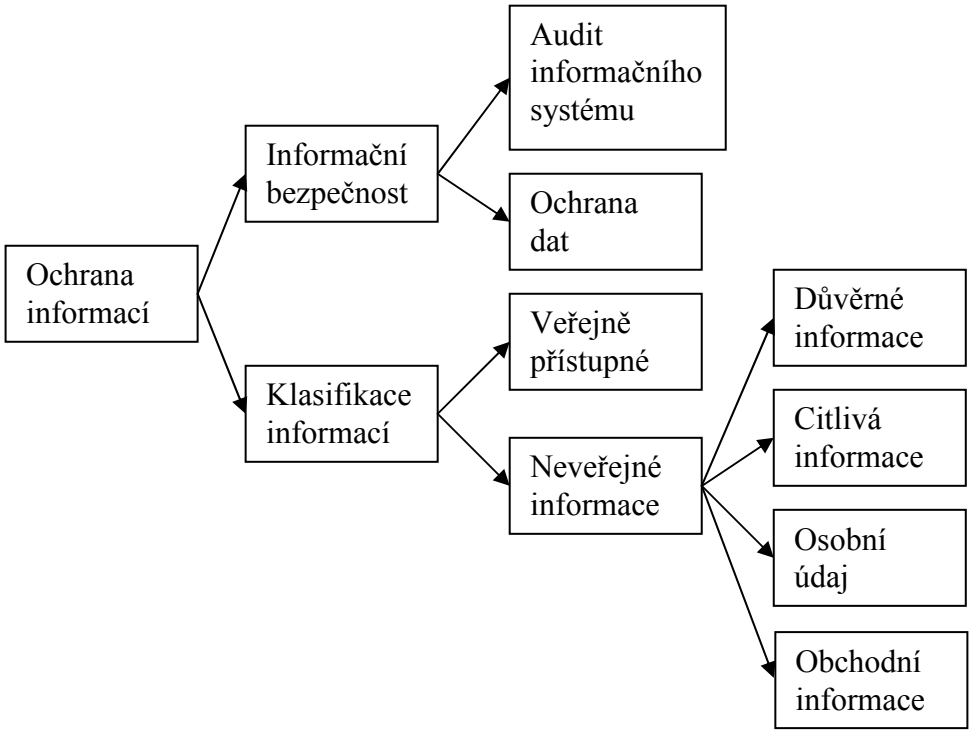
[1] Viz. zákon č.513/1991 Sb.,obchodní zákoník
[2] Viz. Zákon č. 101/2000 Sb.,o ochraně osobních údajů a o změně některých dalších zákonů

osob. Obchodním tajemstvím jsou veškeré skutečnosti obchodní, výrobní či technické, které mají hodnotu (materiální i nemateriální), nejsou běžně dostupné a mají být utajeny. Osobní údaje jsou jakékoliv informace , které se týkají určeného subjektu údajů (lze ho identifikovat). Subjektem údajů je fyzická osoba, ke které se osobní údaje vztahují. Citlivé osobní údaje vypovídají o národnostním, rasovém nebo etnickém původu, politických postojích, náboženství, zdravotním stavu.

Zabezpečení neveřejných informací se provádí několika způsoby. Může to být personální opatření, jehož cílem je minimalizovat počet osob, které se s neveřejnou informací seznamují, protože s ní se může seznamovat jen oprávněná osoba. Dalším je administrativní opatření, kdy je chráněný dokument zpracován a manipulace s ním je prováděna podle obecných zásad stanovených pro archivaci, skartaci a evidenci. Neveřejné informace se zabezpečují také prostřednictvím opatření fyzické bezpečnosti, organizačním, kontrolním a jiným opatřením.

Pro zpracování neveřejných informací dále platí zvláštní podmínky. U obchodního tajemství se vychází ze zákona č. 513/1991 Sb., u osobních (citlivých) údajů se vychází ze zákona č. 101/200 Sb. [9]

Na obrázku č. 1 jsou zobrazeny jednotlivé okruhy ochrany informací.



Obrázek 1: Ochrana informací[6]

2.1 Definice základních pojmů

Bezpečnostní politikou se rozumí souhrn bezpečnostních zásad a předpisů, které definují způsob zabezpečení organizace jako celku (od fyzické ostrahy, přes ochranu soukromí až po ochranu lidských práva). [2]

Jako informační systém se označuje skupina počítačů, serverů, disků a jiných záznamových médií, propojovacích a síťových kabelů, instalovaných programů a používaných dat. Je to zkrátka všechno, co běžní uživatelé většinou chápou pod pojmem „počítač“. [1]

Součástí každého informačního systému jsou aktiva. Aktiva jsou právě tím, na co se útočí, patří mezi ně data, programy. Všechna aktiva je možno přesně finančně ohodnotit, toto ohodnocování se často řídí heslem:„ Jaké finanční škody by firmě způsobilo zničení tohoto aktiva, takovou bude mít aktivum hodnotu.“ Jedná se jednak o škody na ušlém zisku, jednak o škody na poškození dobrého jména firmy.

Informační systém není nikdy naprosto izolovaný, je totiž umístěn v nějakém prostředí. To tvoří jednak uživatelé systému, okolní počítače, sítě počítačů, fyzické prostředí (vlhkost, prašnost,..), ale i společenská a ekonomická situace. Je samozřejmé, že okolní prostředí ovlivňuje v určité míře informační systém, nepochybně i z bezpečnostního hlediska.

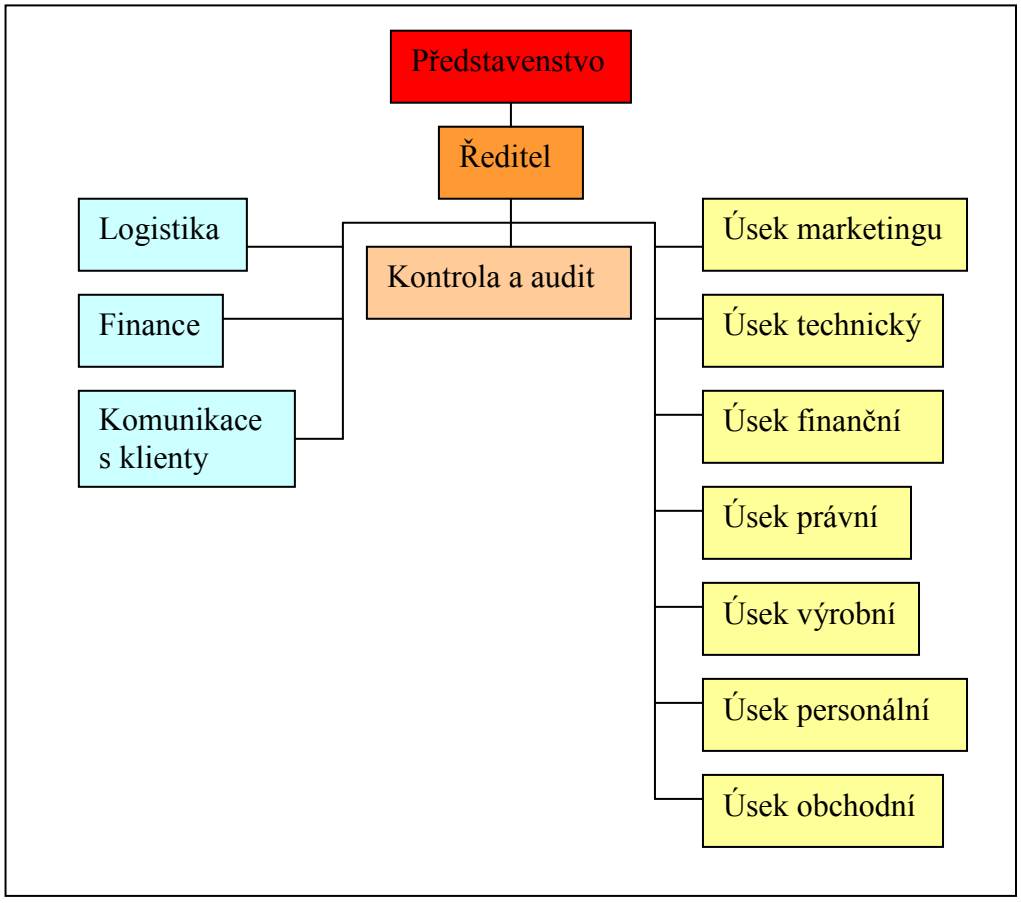
Lze tedy říct, že v prostředí existují jisté **hrozby**. Zatím nikde není řečeno, že hrozby mohou být naplněny. Jejich konkrétní složení závisí přímo na daném prostředí, informační systém jim nabízí svá zranitelná místa. Jiné hrozby budou hrozit systému, který je nasazen v prostředí počítačové laboratoře studentů informatiky, jiné hrozby budou hrozit stejnému systému, pokud ho bude používat negramotný domorodý kmen. Jiné hrozby budou systému hrozit, bude- li pracovat v zemi, kde náklady na prolomení ochran převýší finanční zisky z toho plynoucí, jiné zase ve státě, kdy se jeho obyvatelům útok vyplatí. [1]

Dokud zůstane hrozba hrozbou, je vše v pořádku. Vždy se však musí počítat s tím, že hrozba bude naplněna. V tomto případě se už jedná o útok, tím, kdy ho provádí, je útočník.

Vzhledem ke globální počítačové síti Internet už není otázka prostředí tak jasná, jako před několika lety. Systém umístěný v nejpřívětivějším možném prostředí je totiž také propojen s potenciálními útočníky z prostředí, ve kterém je motivace k útoku podstatně vyšší, než ve kterém se tento systém nachází. Tomuto zjištění musí být pochopitelně přizpůsobena i ochrana.

2.2 Magnet Blanche Porte

Zásilkový firma MAGNET Blanche Porte má na českém trhu již dlouholetou tradici. Od roku 1994 je součástí nadnárodní společnosti 3Suisses INTERNATIONAL sídlící ve Francii. vydávající více než 20 zásilkových katalogů různého zaměření po celé Evropě. Firma Magnet, se sídlem v Pardubicích- Černá Za Bory, patří mezi nejvýznamnější zásilkové obchody v České republice s více než 350 tisíci stálých zákazníků.

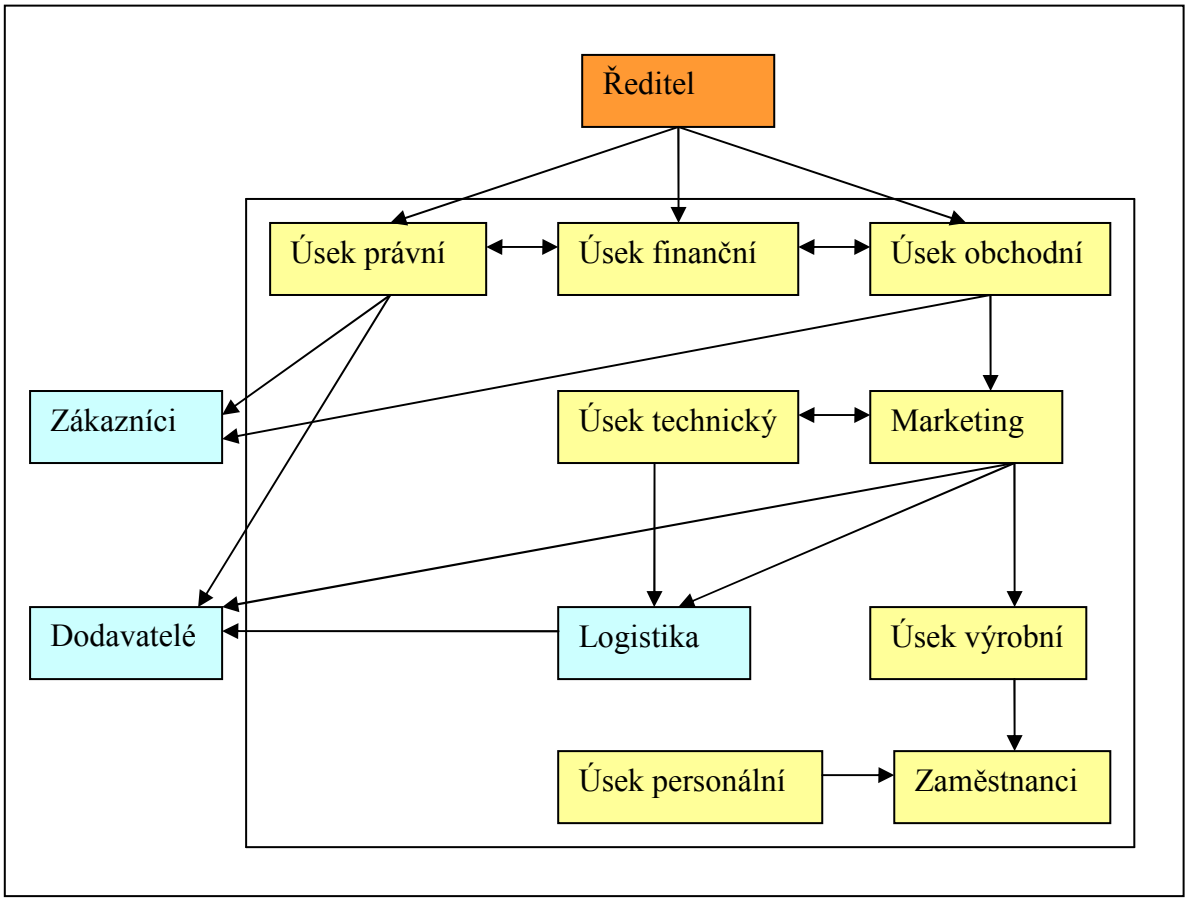


Obrázek 2: Organizační schéma firmy[8]

Firma Magnet má vlastní rozsáhlý informační systém a heterogenní HW prostředí. Základ systému tvoří IBM i Series a databáze DB/2. Pracovní stanice představují klasické PC a „vetstations“, což jsou vlastně procesory se síťovou kartou, které slouží pro přihlášení do systému. Firma Magnet využívá Windows servery i Linux servery, má vlastní www stránky, které zatím slouží hlavně pro e-shop. [8]

Magnet aplikuje různé aspekty IT bezpečnostní politiky. Pro přihlášení do sítě se používá doménový systém, kdy přihlašování probíhá prostřednictvím jména uživatelského účtu a hesla. Uživatelský účet a heslo dále slouží pro přihlášení přes vetstations tak, aby se

uživatel dostal do konkrétní databáze oddělení firmy. Mezi další bezpečnostní opatření lze zařadit firewall, router, zabezpečení bezdrátové sítě a systém sledování a ochrany citlivých dokumentů. Mezi nejcennější aktiva[3] firmy v IT oblasti patří databáze zákazníků. [8]



Obrázek 3: Schéma informačních toků

2.3 Sestavování bezpečnostní politiky

Pozornost byla zaměřena především na IT oblast, protože se jedná o zásilkovou firmu, která je v kontaktu se zákazníky především prostřednictvím elektronické cesty. Nabízí elektronické katalogy a odesílá více než milion balíčků. Také musí být v kontaktu s dceřinou firmou, která sídlí ve Francii a řídit distribuci ze skladů ke svým zákazníkům. V této oblasti je proto riziko nebezpečí nejvyšší.

Možnými riziky se stalo ohrožení:

- integrity dat: přenášená data mohou být v průběhu přenosu změněna, je důležité zajistit průkaznost, že tato data odesílala správná osoba a že přišla ve správném pořadí,
- autentičnosti[4]: osoba, která data odesílá, musí být jednoznačně identifikována,

[3] Aktiva= souhrnné označení pro všechno cenné, co se v informačním systému nachází.

- důvěrnosti: k datům musí mít přístup pouze oprávněné osoby,
- právní jistoty: veškeré použité metody přenosu dat musí být v souladu se zákonem,
- „platnosti“bezpečnostní politiky: hrozby se stále vyvíjí, proto musí být i bezpečnostní politika v pravidelných intervalech aktualizována.

2.4 Obsah bezpečnostní politiky firmy

Bezpečnostní politika byla definována jako souhrn norem, pravidel a činností, které regulují způsob zpracování, ochrany a distribuce citlivých informací. Dokument bezpečnostní politiky informačního systému organizace obsahuje následující body:

- **definici bezpečnosti** informací, její cíle, rozsah a důležitost,
- **prohlášení vedení** firmy o záměru podporovat cíle a principy bezpečnosti informací,
- **stručný výklad** bezpečnostních zásad, principů, standardů a požadavky zvláštní důležitosti pro organizaci, např. dodržování legislativních a smluvních požadavků, požadavky na vzdělávání v oblasti bezpečnosti, zásady prevence, zásady plánování kontinuity informačních činností firmy nebo důsledky porušení bezpečnostních zásad,
- **stanovení** obecných a specifických **odpovědností** pro oblast řízení bezpečnosti informací, včetně hlášení bezpečnostních incidentů,
- **odkazy** na dokumentaci, která podporuje bezpečnostní politiku, např. detailnější bezpečnostní politiky a postupy zaměřené na specifické informační systémy nebo bezpečnostní pravidla, která by měli uživatelé dodržovat.

2.5 Tým bezpečnostní politiky

Aplikace bezpečnostní politiky musí probíhat v rámci celé firmy, čili musí se jí řídit veškerý personál. Dokument bezpečnostní politiky vypracovává **oddělení bezpečnosti** ve spolupráci se **správcem**, což je odpovědná osoba, která provádí klasifikaci dat/informací a rozděluje je na veřejně přístupná a neveřejná, tj.dat, která se musí chránit. Finální podobu

[4] Autentický= původní, pravý, hodnověrný

bezpečnostní politiky firmy dále schválí **ředitel**, to po konzultaci s **personálním oddělením**, které data zpracovává. Oddělení bezpečnosti následně zajišťuje dodržování bezpečnostní politiky a případně řeší její porušení. **Řadoví zaměstnanci** musí být předem proškoleni tak, aby znali své povinnosti pro dodržování jednotlivých zásad, aby znali i své odpovědnosti při porušení těchto zásad a aby věděli, jak postupovat v případě havárie. Realizaci bezpečnostní politiky zajišťují **vedoucí zaměstnanci**, to v mezích své pravomoci. Jejich povinností je okamžité řešení problému.

a. Vedoucí zaměstnanci

Jsou povinni zabezpečit realizaci bezpečnostní politiky firmy v podobě stanovených společných i zvláštních opatření (pro jednotlivý úsek) k zabezpečení neveřejných informací, pokud jejich působnosti ke zpracování těchto informací je dostatečná. Jsou povinni jmenovat **oprávněnou osobu**. Při zjištění ohrožení bezpečnosti neveřejných informací musí bezodkladně přijmout opatření k jeho eliminaci. Při zjištění porušení bezpečnosti neveřejných informací musí bezodkladně přijmout opatření, aby tento stav byl odstraněn a škodlivý následek minimalizován.

b. Zaměstnanci

Zaměstnanci firmy jsou povinni plnit stanovená opatření k zabezpečení neveřejných informací. Jsou povinni zachovávat mlčenlivost o skutečnostech obsažených v neveřejné informaci, s níž byli seznámeni a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo účel ochrany neveřejných informací. Při zjištění ohrožení nebo porušení bezpečnosti neveřejné informace jsou povinni ihned oznámit tuto skutečnost vedoucímu zaměstnanci a podle možnosti přiměřeným způsobem ohrožení nebo porušení odvrátit.

c. Personální oddělení

Personální oddělení zpracovává, za součinnosti příslušných **správců- odpovědných osob,** osobních údajů všech zaměstnanců, to po předchozím ověření identity. Personální oddělení dále:

- zajišťuje komunikaci s ÚOOÚ[5], policií ČR a dalšími orgány státní správy nebo samosprávy, ve věci ochrany neveřejných informací,
- plní na základě rozhodnutí generálního ředitele oznamovací povinnosti vůči ÚOOÚ,

[5] ÚOOÚ= Úřad pro ochranu osobních údajů

- žádá u ÚOOÚ o povolení předání osobních údajů do třetích zemí (mimo EU).

Personální zajišťuje centrální evidenci všech zaměstnanců firmy ke zpracování jejich údajů za jednotlivými účely.

d. Správce- odpovědná osoba

Správce provádí klasifikaci informací, které následně rozděluje na informace veřejně přístupné a neveřejné, to jsou informace, které se musí chránit. Správce dále právní delikty, přestupky, náhradu škody, či majetkové újmy v souvislosti s porušením ochrany neveřejných informací v jeho působnosti.

- **Oddělení bezpečnosti**

Prostřednictvím pověřeného zaměstnance plní tyto povinnosti:

- zajišťuje pravidelnou aktualizaci bezpečnostní politiky,
- provádí ve firmě vnitřní koordinaci úkolů k naplňování povinností, vyplývajících z bezpečnostní politiky,
- předkládá řediteli firmy návrhy a podklady pro nezbytná rozhodnutí,
- informuje ředitele o zvlášť závažných případech porušení povinností stanovené zákonem nebo firemní bezpečnostní politikou,
- ověřuje míru závažnosti rizika, vyplývajícího z porušení ochrany neveřejných informací,
- zajišťuje konzultace ve věcech ochrany neveřejných informací.

2.6 Realizace bezpečnostní politiky

Prvním krokem byla **identifikace**, jaká data, či jaké prostředky se ve firmě nacházejí. Ne všechna tato aktiva je třeba chránit stejně. Toho se tedy týká druhý a třetí krok: **proč a jak** chce firma konkrétní aktivum chránit, aby bylo odpovídající jeho hodnotě pro firmu.

Samotné zavedení bezpečnosti je jen částí celého procesu. Předně je nutno správnost zavedení nějak zkontrolovat, aby byly vyloučeny úmyslné či neúmyslné lidské chyby. **Kontrola** by měla být prováděna periodicky, čímž se zajistí, že ochrana nebyla omylem nebo záměrně odstraněna, případně neztratila svou účinnost.

Součástí bezpečnostní politiky jsou také takzvané **havarijní plány**. Pro konkrétní druhy havárií by jsou stanoveny konkrétní kroky, které je třeba podniknout. Funkčnost havarijních plánů je třeba v pravidelných intervalech také prověřit.

Samotná bezpečnostní politika by neměla zůstat neměnným dokumentem. Prostředí, ve kterém je informační systém umístěn, se v průběhu času mění. Je třeba čelit jiný hrozbám, chránit jiná aktiva apod. Sebelepší bezpečnostní politika proto bude **aktualizována**.

Aby bylo prosazování bezpečnostních opatření snazší, bude celá politika vysvětlena kompletnímu vedení společnosti. S bezpečnostní politikou se musí všichni dokonale ztotožnit a pochopit, proč se konkrétní věci provádějí konkrétním způsobem. Názvy jednotlivých dokumentů společně s jejich popisem jsou uvedeny v tabulce č. 1.

2.6.1 Analýza rizik

Při sestavování bezpečnostní politiky bude nejprve provedena **analýza rizik**. Je tedy potřeba zjistit, co a proti čemu (tedy jaká aktiva proti jakým hrozbám) se musí chránit. Analýza rizik se skládá z několika kroků:

- **Identifikace rizik**: prvním krokem je zjištění, jaká aktiva se v systému vyskytují a jednotlivá aktiva jsou oceněna.
- **Identifikace hrozeb**: v závislosti na prostředí, ve kterém bude systém nasazen, se identifikují hrozby, které systému hrozí.
- **Vlastní analýza rizik**: v posledním kroku dojde k přiřazení konkrétních hrozeb konkrétním aktivům. Po provedení tohoto kroku by mělo být jasné, kterým aktivům hrozí zanedbatelné hrozby a která je třeba naopak chránit.

Jednotlivé kroky jsou nyní probrány postupně, navíc s procesem návrhu bezpečnostních opatření.

2.6.1.1 Identifikace aktiv

Tento krok má jediný úkol- zjistit, jaká aktiva se ve firmě vyskytují a jakou pro ni mají hodnotu. Seznam aktiv bude konzultován s oddělením IT. Jeho pracovníci totiž vědí, jaká data ukládají uživatelé na disky.

Vzhledem k tomu, že toto oddělení má na starost firemní informační systém, dokáže zaměstnanec IT oddělení jasně stanovit, jaká data jsou v systému uložena. Dokáže navíc jejich označení převést do podoby srozumitelné běžnému člověku. Místo označení „tabulka TAB_123“ tak může tento člověk používat „seznam telefonních čísel zákazníků uložený v tabulce TAB_123“, což zní běžným uživatelům mnohem lépe.

Toto převádění do obecné řeči je důležité pro úzkou spolupráci se zákazníky firmy. Po vytvoření seznamu všech aktiv je zapotřebí vyčíslit jejich hodnotu pro firmu.

Tento úkol se již tolik nevztahuje na IT oddělení. Jeho vedení může vyčíslit dobu, která je potřebná na obnovu útokem poškozeného systému, snadno odhadne škody vzniklé například fyzickým poškozením kabeláže. Hodnotu dat ale musí stanovit někdo jiný, v závislosti na tom, kdo je vlastníkem ohodnocovaných dat. Jinou hodnotu bude mít databáze zákazníků pro obchodní úsek, jinou pro úsek finanční, jinou pro personální úsek apod.

2.6.1.2 Identifikace rizik

Mnohem složitější bude identifikace hrozeb, které firemním aktivům hrozí. Seznam hrozeb se navíc poměrně dynamicky vyvíjí, je tedy velmi důležitou součástí pravidelná aktualizace identifikace rizik. K této lze přistupovat několika způsoby, pro firmu Magnet se použije způsob první- **intuitivní vyhledávání rizik**.

Jeho základem je důkladné přemýšlení nad všemi situacemi, které mohou v informačním systému nastat. „Co když útočník provede takový to útok? Co se stane v případě přírodní katastrofy?“ Ovšem jen samotné přemýšlení nad krizovými situacemi nestačí, proto dochází k aktualizování seznamu hrozeb.

Druhým způsobem je inspirace **jinými seznamy hrozeb**. Pokud se zvolí seznam, který byl vytvořen pro podobné prostředí a podobnou situaci, může být úspěšnost poměrně vysoká. I zde ovšem hrozí jisté riziko v případě neindividualizování seznamu podle vlastního systému- každý systém i každé prostředí je lehce odlišné!

Třetím způsobem je využití **dotazníků**. Pro různé části prostředí jsou vytvořeny vysoce podrobné dotazníky. Při identifikaci rizik pak bezpečnostní expert prochází otázku po otázce a zjišťuje, jak je na tom tento systém v tomto prostředí. Výhodou tohoto přístupu je jeho vysoká kvalita- při dobře navrženém dotazníku je nízká pravděpodobnost, že bude

nějaká situace opomenuta. Nevýhodou je poměrně vysoká časová náročnost a hlavně nedostupnost dotazníků.

2.6.1.3 Vlastní analýza rizik

K dispozici jsou dva seznamy- seznam aktiv, která se ve firmě vyskytují včetně jejich finančního ohodnocení, a seznam hrozeb, které firmě v daném prostředí hrozí. Úkolem analýzy rizik je proto zjistit, jaká nebezpečí konkrétním aktivům hrozí.

Dochází tedy k postupnému procházení jednotlivých aktiv a dále k rozhodnutí, které hrozby se na konkrétní aktivum vztahují. Například na zmiňovanou databázi telefonních čísel zákazníků se nevztahuje hrozba zničení požárem. Tato hrozba se naopak vztahuje na nosič dat (disk), na kterém je databáze fyzicky uložena. Na nosič dat se zase nevztahuje hrozba nechtěného smazání uživatelem.

Výsledkem analýzy rizik je seznam oceněných aktiv, kterým jsou přiřazeny jednotlivé hrozby. Každé konkrétní dvojici **aktivum- hrozba** lze přiřadit pravděpodobnost, s jakou dojde ke konkrétní hrozbě pro dané aktivum. Tímto jsou firemní informace kvalifikovaně chráněny.

Problém je, že ani analýza rizik není záležitostí statickou. Prostředí, ve kterém se informační systém nachází, se průběžně mění. Mění se aktiva, mění se jejich finanční hodnota a mění se i hrozby, to vše v závislosti na výskytu hrozeb.Proto bude prováděna podobná analýza opakovaně s určitou periodou.

2.6.1.4 Navržení vhodné ochrany

V předchozích krocích byla identifikována aktiva s tím, jakou hodnotu pro firmu mají. Stanovila se také pravděpodobnost výskytu hrozeb, proti kterým je zapotřebí se chránit.

Posledním krokem je navržení jednotlivých ochran. Ochrana bude navržena pro každou dvojici aktivum- hrozba, často ale nastane situace, kdy jeden použitý bezpečnostní prostředek zajistí ochranu více takových dvojic. Proto se u každé dvojice navrhne odpovídající ochrana a vyčíslí se náklady na její zavedení a udržování.

S vyčíslováním nákladů opět pomáhá oddělení IT, které dokáže odhadnout personální i materiální hodnoty. Poté se projde celý seznam a tím se zjistí, které dvojice tato ochrana také chrání. Celý postup bude opakován až do chvíle, kdy jsou všechny dvojice obsazeny svými ochranami.

2.6.2 Havarijní plány

V běžném chodu firmy mohou nastat nejrůznější nebezpečí, problémem ale je, že tato nebezpeční neodhalí vždy analýza rizik a může dojít k selhání bezpečnostních opatření. Proto bude připraven havarijní plán. V případě **havárie (krizového stavu systému)**, je prioritou, aby byla co nejdříve obnovena činnost důležitých částí informačního systému, co nejrychleji musí být obnovena poškozená data. Celý proces obnovy systému lze shrnout do následujících kroků:

- odstranění aktuálního nebezpečí,
- obnovení důležitých částí systému,
- obnovení důležitých dat,
- vypracování příslušných protiopatření

Součásti havarijního plánu lze tedy definovat následovně:

- **Vyhlášení a zrušení havarijního stavu**: tato část odpovídá na otázky, co je to havarijní stav, kdo a za jakých podmínek ho vyhlašuje a jakým způsobem ho vyhlašuje. Definuje také, kdy krizový stav pomine a kdo má právo ho zrušit.
- **Personální zajištění**: toto určuje další postup, stanovuje kdo má právo řídit činnosti při havarijním stavu. Tato část bude propojena na procesy personálního oddělení, které v případě příchodu nebo odchodu zaměstnance zašle informace na všechna potřebná místa. Tato část dále stanoví, jakým způsobem bude o havarijním stavu informovat vedení společnosti a jakým způsobem zaměstnance, příp. zákazníka.
- **Postup pro konkrétní havarijní stavy**: jedná se o konkrétní postup pro odstraňování následků jednotlivých typů havárií.
- **Administrativní záležitosti**: tato poslední část se týká přímo havarijního plánu jako dokumentu. Musí se stanovit, kdo bude s havarijním plánem seznámen v rámci školení, dále kde bude havarijní plán uložen tak, aby nebyl při havárii zničen, aby zůstal dostatečně dostupný apod.

Nesmí se zapomenout ani na pravidelnou kontrolu a aktualizaci havarijního plánu, pravidelné ověřování jeho funkčnosti apod. Součástí havarijního plánu proto budou konkrétní termíny konkrétních činností, které je třeba provést, včetně zodpovědných osob. [1]

tabulka 1: Bezpečnostní politika firmy [7]

Název dokumentu	Popis
Analýza rizik	Identifikuje aktiva v systému a jejich cenu
Návrh opatření	Definuje, která aktiva a jakým způsobem budeme chránit
Havarijní plány	Popisuje rozsah činností při bezpečnostních incidentech a přírodních katastrofách
Administrativní část	Stanovuje pravidelné prověřování bezpečnostní politiky

2.7 Uložení bezpečnostní politiky

Havarijní plán bude součástí bezpečnostní politiky firmy, ale také minimálně jedna jeho kopie bude uložena odděleně od bezpečnostní politiky, čili v dostatečně bezpečném a dostupném prostředí.

Havarijní plán musí být uložen na bezpečném místě, aby ho nezničil zdroj havárie (např.požár či povodeň). Jednou z možností uložení havarijního plánu je také jeho uložení na různých místech, ale otázkou zůstává, jestli je účelné havarijní plán dělit. Ve zmatku, který zákonitě při havárii nastane, bude mít je těžko kdokoliv čas a myšlenky na to, kde je konkrétní část havarijního plánu uložena. Jako první pravidlo uložení havarijního plánu lze tedy uvést: **ukládat havarijní plán** na co nejmenší množství míst, která jsou chráněna proti všem odpovídajícím katastrofám.

Druhým problémem se stává snadná **dostupnost havarijního plánu**. Dokument uložený v sejfu je zbytečný, když se k němu dostane jen generální ředitel společnosti. Samozřejmě pokud by v sejfu byla uložená kopie tohoto dokumentu, nebude to na škodu, vždy však bude minimálně jedna kopie uložena na místě, které je snadno dostupné všem osobám, kterým by měl být havarijní plán k dispozici.

Celá bezpečnostní politika je dokumentem důvěrným. I sebelépe vypracovaná bezpečnostní politika, pokud je prozrazena potenciálnímu útočníkovi, je pro něj silným

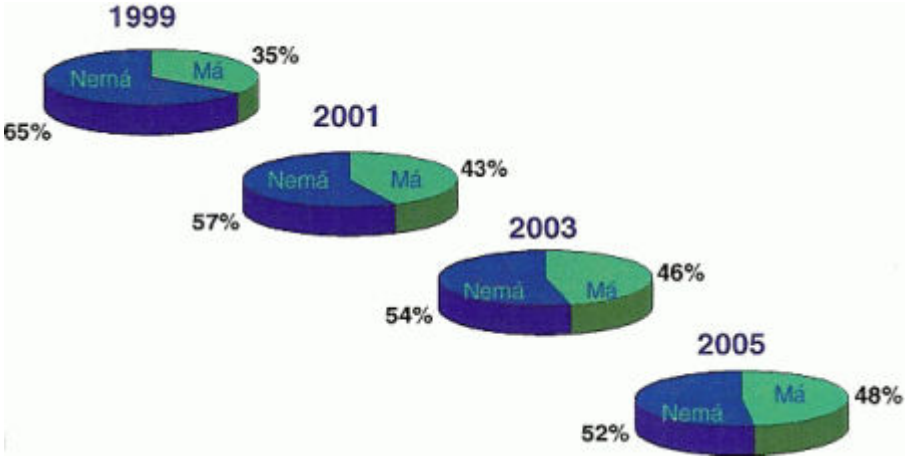
ulehčením. Tento útočník se totiž může dopodrobna seznámit se všemi opatřeními, které firma má pro případ napadení. Snadno zjistí, jaká nebezpečí firma očekává a jaká nechává naopak beze všeho povšimnutí.

Dalším pravidlem je tedy **zajištění důvěryhodnosti zaměstnanců**, kteří mají možnost se s bezpečnostní politikou firmy seznámit, to i v případě, že firmu opustí.

2.8 Aktualizace bezpečnostní politiky

Bezpečnostní politika bude mít **garanta,** který bude odpovědný za její údržbu a aktualizaci v souladu s pevně definovaným revizním procesem. Tento proces zajistí, že údržba i aktualizace proběhnou jako relace na jakékoliv změny, které ovlivní původní hodnocení rizik- např. významné bezpečnostní incidenty, nové hrozby nebo změny v organizační či technické infrastruktuře. Takovýmto garantem bude **bezpečnostní manažer** organizace nebo specialista- bezpečnostní manažer informačního systému organizace.

Počet firem využívajících bezpečnostní politiku rok od roku stoupá, jak je vidět z grafu č.1.



Graf 1: Počet společností disponujících bezpečnostní politikou[12]

3. Druhy bezpečnostní politiky

3.1 Bezpečnostní politiky podle ITSEC

Podle metodologie ITSEC[6] by měly být zpracovány až tři úrovně bezpečnostních politik:

- **celková** bezpečnostní politika,
- **systémová** bezpečnostní politika,
- **technická** bezpečnostní politika.

Tyto úrovně popisují jednotlivá bezpečnostní opatření, vyplývající ze systémové bezpečnostní politiky. Obsahem **celkové bezpečnostní politiky** je zejména stanovení cílů a popis způsobu zajištění celkové bezpečnosti informačního systému ve vztahu k bezpečnosti organizace. Je to výběr bezpečnostních zásad a předpisů splňující bezpečnostní politiku organizace a všeobecně definujících bezpečné používání informačních systémů v rámci organizace. [2]

Obsahem **systémové bezpečnostní politiky** je zejména stanovení cílů a popis způsobu zajištění bezpečnosti informačního systému organizace, a to zejména:

- způsob uplatnění celkové bezpečnostní politiky ve vztahu k informačnímu systému organizace,
- popis vnitřních a vnějších vazeb informačního systému organizace,
- způsob ochrany aktiv informačního systému,
- popis bezpečnostních opatření informačního systému,
- vyhodnocení analýzy rizik informačního sytému.

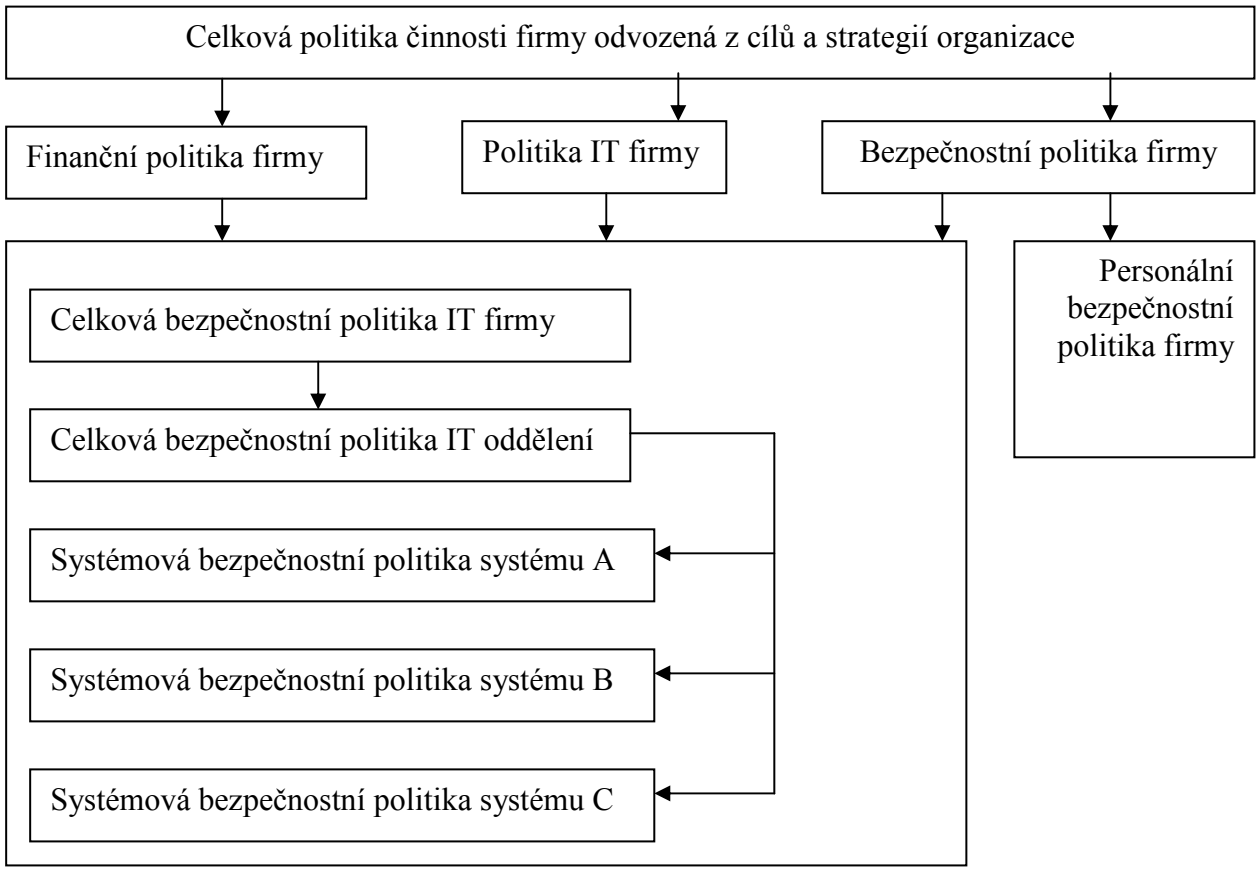
Jedná se tedy o detailní normy, pravidla, praktiky, předpisy konkrétně definující způsob správy, ochrany, distribuce citlivé informace a jiných IT zdrojů v rámci organizace, specifikace bezpečnostních protiopatření a způsobu jejich implementace-určení způsobu jejich použití, který zaručuje přiměřenou bezpečnost splňující bezpečnostní politiku.

[6] ITSEC (Information Technology Security Evaluation Kriteria)= standard pro hodnocení bezpečnosti IS

Technická bezpečnostní politika popisuje jednotlivá opatření pro zajištění bezpečnosti při využívání zdrojů a zpracování informací v organizaci.

Dokumenty celkové bezpečnostní politiky by měly být předloženy všem zaměstnancům organizace správce, resp. provozovatele, včetně uživatelů IS, a to ve formě, která je relevantní, přístupná a pochopitelná všem potenciálním příjemcům.

Systémová a případná technická bezpečnostní politika by měla být k dispozici pouze pověřený zaměstnancům správce, resp. provozovatele. Jednotlivé druhy politik organizace jsou uvedeny v obrázku č.2.



Obrázek 4: Politiky organizace[7]

3.2 Bezpečnostní politiky podle předpisu pro utajované skutečnosti

Podle vyhlášky Národního bezpečnostního úřadu č. 523/2005 Sb., o bezpečnosti informačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor, tvoří bezpečnostní dokumentaci informačního systému[10]:

Projektová bezpečnostní dokumentace informačního systému, která obsahuje:

- bezpečnostní politiku informačního systému a výsledky analýzy rizik,
- návrh bezpečnosti informačního systému zajišťující splnění bezpečnostní politiky informačního systému, přičemž podrobnost jejího popisu musí umožnit přímou realizaci navrhovaných opatření,
- dokumentaci k testům bezpečnosti informačního systému.

Provozní bezpečnostní dokumentace informačního systému, která obsahuje:

- bezpečnostní směrnice informačního systému, které předepisují činnost bezpečnostních správců informačního systému v jednotlivých rolích zavedených v informačním systému pro zajištění bezpečnostní správy informačního systému,
- bezpečnostní směrnice informačního systému, které předepisují činnost správců informačního systému v jednotlivých rolích zavedených v informačním systému pro správu informačního systému, pokud se týká zajištění bezpečnosti informačního systému,
- bezpečnostní směrnice informačního systému, které předepisují činnost uživatelů informačního systému, pokud se týká zajištění bezpečnosti informačního systému.

4. Bezpečnost IT

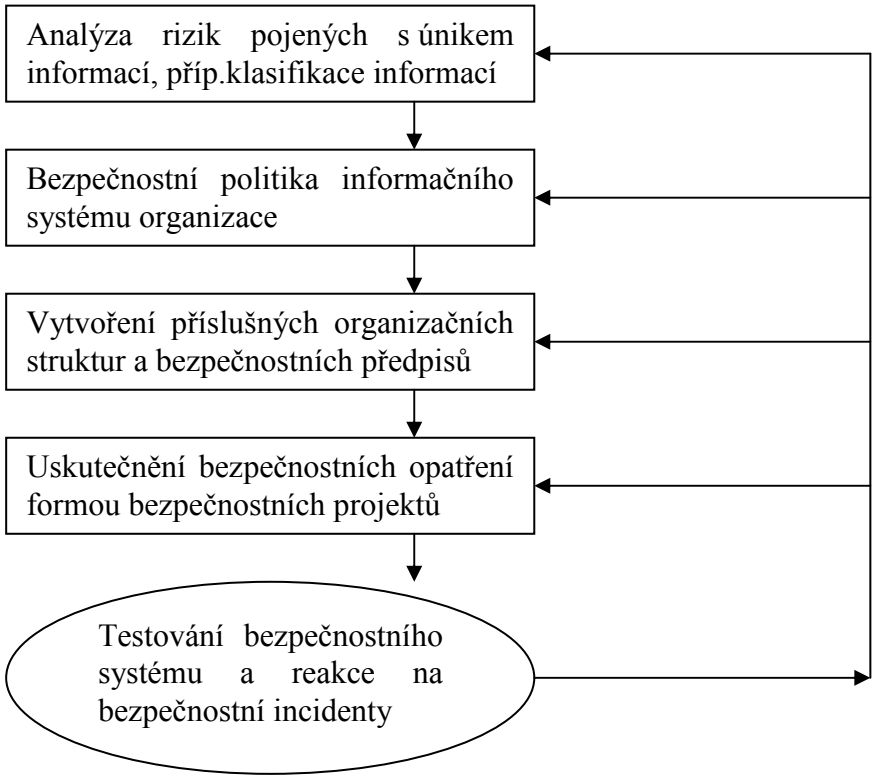
Pod pojmem bezpečnost IT se obvykle rozumí ochrana odpovídajících informačních systémů a informací, které jsou v nich uchovávány, zpracovávány a přenášeny. Součástí takto obecně chápané bezpečnosti IT je i komunikační bezpečnost, tj. ochrana informace přenášené mezi počítači, fyzická bezpečnost, tj. ochrana před přírodními hrozbami a fyzickými útočníky a personální bezpečnost, tj. ochrana před vnitřními útočníky.

Mezinárodní normalizační organizace ISO ve svých normách definuje bezpečnost jako „*zajištěnost proti nebezpečím, minimalizaci rizik a jako komplex administrativních, logických, technických a fyzických opatření pro prevenci, detekci a opravu nesprávného použití informačního systému"*.

Informační systém je bezpečný, je- li zajištěn fyzicky, administrativně, logicky i technicky. Informační systém je třeba zabezpečovat, protože se jedná o ochranu investic, neboť informace je zboží, nutí k tomu právní nebo morální pravidla, činnost konkurence a zákonné úpravy pro ochranu dat. V soudobém chápání bezpečnosti IT je bezpečnost dána zajištěním:

- **důvěrnosti**: k aktivům mají přístup pouze autorizované subjekty,
- **integrity a autenticity**: aktiva smí měnit jen autorizované subjekty a původ informací je ověřitelný,
- **dostupnosti:** aktiva jsou autorizovaným subjektům do určité doby dostupná, nedojde tedy k odmítnutí služby, kdy subjekt nedostane to na co má právo.

Budování informační společnosti má několik fází, které jsou zobrazeny na obrázku č. 3.



Obrázek 5: Budování informační bezpečnosti[zdroj: vlastní]

4.1 Základní principy bezpečnosti při použití IT

Informační technologie zpracovávají stále více a více informací s velkou hodnotou, které jsou zpracovávány, uchovávány, přenášeny, vyhodnocovány i prezentovány. Mezi takovéto informace patří například: zdravotní záznamy, daňová přiznání, bankovní účty, elektronické platební nástroje, výsledky vývoje nebo výzkumu, obchodní záměry apod.

Je proto důležitá ochrana, která by zabezpečovala, aby k těmto informacím měly přístup pouze oprávněné osoby, aby se zpracovávala nefalšovaná informace, aby se dalo zjistit, kdo konkrétní informaci vytvořil, změnil, odstranil, aby informace nebyly nekontrolovaným způsobem vyzrazeny a aby byly dostupné tehdy, když jsou potřebné. [3]

Charakteristickým rysem soudobých firem je, že svoje poslání plní pomocí propojení informačních a komunikačních systémů budovaných na bázi IT, a to jak uvnitř organizace (intra…, lze připomenout pojem „intranet“, vnitřní síť), tak i s ostatními organizacemi (extra… /inter…, např. „extranet“ / Internet). Tím se ale činnosti firmy stávají silně závislé na

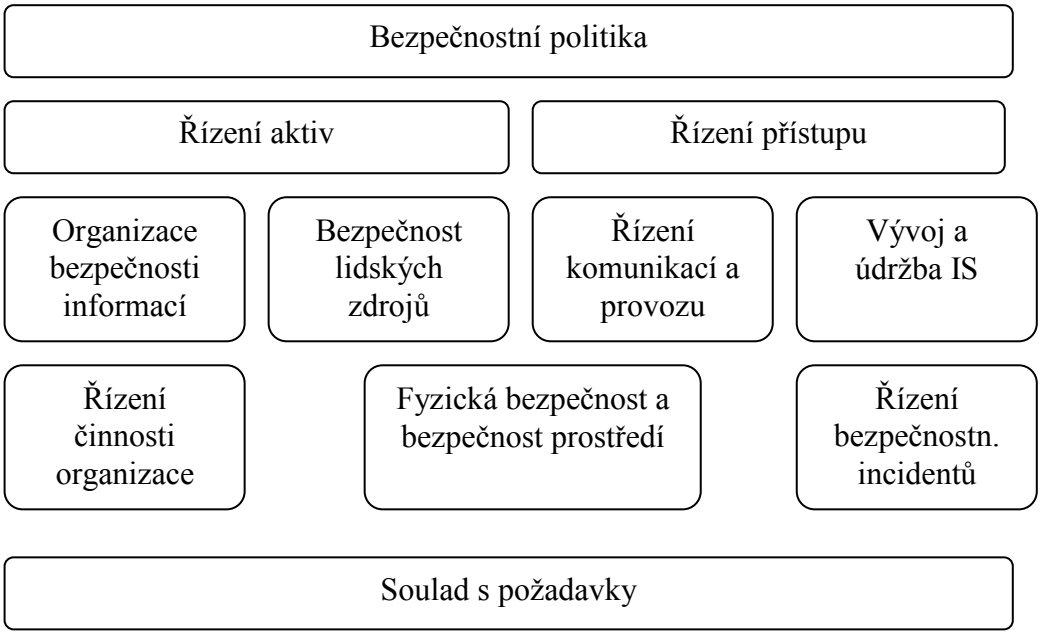
informacích a službách IT. Důsledkem je, že ztráta důvěrnosti, integrity, dostupnosti, prokazatelnosti odpovědnosti, autenticity a spolehlivosti informací a služeb IT má na chod organizace nepříznivý dopad. Řešením je uplatnění zásad bezpečnosti IT.

Firma musí své informační systémy zabezpečovat stejně jako jiné investice do své činnosti. Hardwarové komponenty IT lze zničit (teroristy nebo i nespokojenými zákazníky či zaměstnanci) nebo ukrást (a levně prodat nebo používat pro vlastní potřebu). „Ukrást“ lze i software, který mnohdy představuje enormní a přitom špatně vyčíslitelné hodnoty. Konkurent tak může ušetřit náklady na vývoj nebo na pořízení softwaru. Neoprávněné užívání softwaru zaměstnanci pro osobní potřebu nebo pro jejich druhé zaměstnání je zdrojem jejich nelegálních zisků. Provozovateli kradeného softwaru mohou vzniknout škody plynoucí z trestní odpovědnosti za porušení licence.

Informační systém lze používat neautorizovaně, a tím způsobit např. zničení systému nebo porušení soukromí jiných osob („krádeží“ přístupového hesla, překonáním mechanismu řídicího přístup k IS) nebo ho lze využívat autorizovanými zaměstnanci k nepracovní činnosti, ať již osobní, nebo výdělečné.

Informace jsou v podstatě zboží, pro organizaci představují mnohdy cenná aktiva. Data uložená v bázích dat lze ukrást neoprávněným okopírováním, lze ukrást i výstupy generované IS pro potřebu organizace. Data, která jsou pro organizaci citlivá, je potřeba chránit před konkurencí. [4]

V současnosti existuje celá řada právních, morálních či etických pravidel pro používání informací, existují zákonné úpravy pro ochranu dat, a ty je žádoucí, resp. nutné, dodržovat. Bezpečnost informací má několik oblastí, jak vyplývá z následujícího obrázku č.4.



Obrázek 6: Oblasti bezpečnosti informací [4]

4.2 Aktivity managamentu IT bezpečnosti

- vývoj bezpečnostní politiky,
- identifikace rolí a odpovědnosti (určení kdo za co je v organizaci odpovědný),
- správa rizik (identifikace, zvládnutí, odstranění nebo minimalizace nepředvídatelných událostí, které mají nežádoucí vliv na aktiva organizace),
- identifikace a ohodnocení (chránění aktiv: citlivá data a jejich klasifikace, zranitelných míst a s nimi souvisejících hrozeb vč. určení forem útoků a typu útočníků),
- pravděpodobnosti s jakými se útočí, jakým rizikům je IS vystaven,
- výběr bezpečnostních opatření a jejich implementace (bezpečnostní mechanismy),
- správa konfigurace,
- správa změnového řízení,
- vypracování havarijního plánu,

- školící aktivity v oblasti bezpečnosti,
- provozní činnost (údržba, bezpečnostní audit, monitorování, oponentury, reakce na incidenty).

4.3 Motivace

Mezi nejčastější motivace pro zabezpečení IT oblasti patří zabránění:

- narušení citlivých či utajených informací,
- vydávání se za jinou oprávněnou osobu a zneužívání jejích privilegií,
- distancování se od odpovědnosti nebo od závazků plynoucích z manipulace s informacemi,
- tvrzení, že se nějaká informace někam poslala a toto se nikdy nestalo,
- tvrzení, že se informace získala od nějakého podvodníka,
- neoprávněného zvýšení svých privilegií přístupu k informacím,
- modifikace privilegií ostatních osob,
- výskytu důvěrné informace v jiných informacích,
- zjištění, kdo a kdy si zpřístupňuje které informace,
- zařazení se jako skrytý mezičlánek v konverzaci jiných subjektů,
- porušení funkcionality softwaru doplněním skrytých funkcí,
- narušení protokolu činností jiných subjektů zavedením nesprávných, nekorektních informací,
- podkopání důvěryhodnosti protokolu způsobeným zjevným, byť možná jen zdánlivými,
- poruch,
- bránění jiným uživatelům legitimně komunikovat.

5. Definování důležitých pojmů z oblasti bezpečnosti IT

5.1 Použitý model

Základní pojmy, které vymezují oblast bezpečnosti IT, lze vysvětlit na modelu, ve kterém se použité informační systémy skládají ze tří následujících typů komponent:

- hardware: procesor, telekomunikace, paměti, terminály apod.
- software: aplikační programy, operační systém apod.
- data: data uložená v databázi, vstupní data, výsledky, výstupní sestavy apod.

Je samozřejmé, že přirozenou čtvrtou komponentou informačního systému jsou lidé: uživatelé, personál. První tři z uvedených komponent představují pro firmu, která provozuje informační systém, jisté hodnoty, označené jako již zmiňovaná aktiva.

Pokud dochází k analýze informačního systému z hlediska potřeb na jeho zabezpečení, rozeznává se:

- **objekt informačního systému:** pasivní entita, která obsahuje/přijímá informace a je přístupná autorizovaným subjektům IS
- **subjekt informačního systému***:* lze ho nazvat aktivní entitou (osoba, zařízení nebo proces subjektu, objekt, tj. uživatel, proces, systém, informační struktura apod.), tato entita je autorizovatelná pro získání informace z objektu, pro změnu stavu objektu, pro vydávání příkazů ovlivňujících udělení práv přístupu k objektu, apod.

Pojmem **autorizace**[7] subjektu pro jistou činnost se rozumí určení, že se daný subjekt z hlediska této činnosti dá označit za důvěryhodný. Udělení autorizace subjektu umožňuje práci s autentickými subjekty. **Autentizací** se označuje proces, při kterém dochází k ověřování pravosti identity entity.

Důvěryhodným informačním systémem se označuje taková entita, o které se věří (je o tom podán důkaz), že je implementovaná takovým způsobem, že splňuje svoji úlohu při

[7] Autorizace= oprávněnost, autorizovat znamená povolit schválit, zmocnit, oprávnit subjekt používat služby IS

používání konkrétní bezpečnostní politiky. Na důvěryhodnou entitu se lze spolehnout v případě, že se chová tak, jak se od ní očekává, že se bude chovat.

5.2 Zranitelné místo

Zranitelným místem se rozumí slabinu informačního systému, kterou lze využít k útoku na informační systém a následnému způsobení škod nebo ztrát. Existence zranitelných míst je důsledkem chyb, selhání v analýze, v návrhu případně v implementaci informačního systému, důsledek vysoké hustoty uložených informací, složitosti softwaru, existence **skrytých kanálů** pro přenos informace jinou než zamýšlenou cestou apod.[1]

Podstata zranitelného místa může být:

- **fyzická**: např. umístěním informačního systému v místě, které je snadno dostupné pro případný lidský útok i pro např.výpadek proudu,
- **přírodní:** jedná se o přírodní pohromy typu požár, zemětřesení, záplava, blesk,
- **fyzikální**: vyzařování,
- **lidský faktor**: ten způsobuje největší zranitelnost.

Zranitelná místa vznikají jako důsledek selhání (opomenutí, zanedbání) buď již **v návrhu** nebo **ve specifikaci požadavků**. Informační systém může plnit všechny své funkce a vykazovat všechny bezpečnostní rysy, které se po něm vyžadují, a přesto ještě obsahuje zranitelná místa, díky kterým se stává z hlediska bezpečnosti nevhodným nebo neúčinným.

Dalším způsobem vzniku zranitelných míst může být **řešení** nebo **konstrukce.** Informační systém nesplňuje svoje specifikace nebo do něj byly zavlečeny zranitelná místa v důsledku špatných konstrukčních standardů nebo nesprávných rozhodnutí při jeho návrhu či implementaci.

Zranitelné místo může nastat i **v provozu.** Informační systém byl sice správně zkonstruován podle správných specifikací, ale zranitelná místa do něj byla zavlečena prostřednictvím použití nevhodných provozních řídicích nástrojů.

Zranitelným místem se tedy rozumí slabina informačního systému, kterou lze využít ke způsobení škod případně ztrát útokem. Takovýto útok může nastat:

- v organizačních schématech,
- v administrativních opatřeních,
- ve fyzickém uspořádání,
- v personální politice,
- ve vlastní správě (managementu) organizace,
- v logických a technických opatřeních (hardware, software, data).

Mezi příčiny vzniku zranitelných míst se řadí: chyby v analýze, složitost software, existence skrytých kanálů, chyby v návrhu nebo implementaci, vysoká hustota informací, apod.

Příkladem zranitelného místa je:

- **identifikace a autentizace:** podvrženým login programem lze ukrást cizí heslo,
- **nedokonalá implementace** bezpečnostního mechanismu pro řízení přístupu,
- chybný předpoklad **důvěryhodnosti:** předpokládá se, že správný program je jiným, než ten, u kterého by bylo vhodné otestovat správnost parametrů, které tento program dodává,
- **skryté sdílení**: znamená, že systém může ukládat kritické informace do adresových prostorů procesů, aniž by to bylo definováno v manuálu,
- **komunikace mezi procesy:** zde se jedná o testování možností zasíláním a čtením zpráv až do získání kladné odpovědi,
- nekontrolované **počty opakování** pokusů.

5.3 Hrozba a riziko

Zranitelná místa jsou vlastnostmi (součástmi) informačního systému, jejichž existence způsobuje, že některé vlivy prostředí, ve kterém se informační systém provozuje, představují pro něj hrozby. Pojmem **hrozba** označujeme možnost využitkovat zranitelné místo

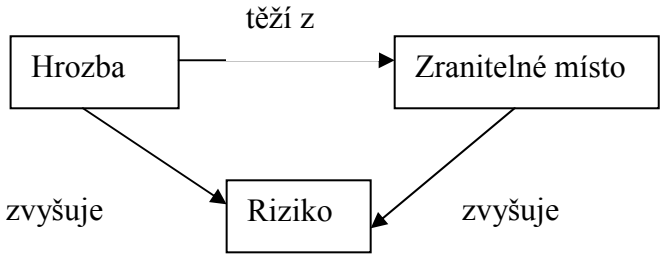
informačního systému k útoku na něj– ke způsobení škody na aktivech. Hrozby lze kategorizovat na objektivní a subjektivní. [1]

Charakteristikou hrozby je její zdroj (např. vnější nebo vnitřní), potenciální útočník má také jistou motivaci (finanční zisk, získání konkurenční převahy), mezi charakteristiky lze zařadit i frekvenci a kritičnost uplatnění hrozby. K neautorizovanému zpřístupnění informací může útočník využít např. nebezpečný software.

Hrozbou mohou být agregace citlivých informací z méně citlivých dílčích informací, dedukce ze znalosti, která říká, že jistá informace je uložena v databázi, nebo dedukce z informací neoprávněně dostupných na veřejných zdrojích, lze hrozbou označit také odposlech pomocí zařízení pro práci se zvukem, instalovaných na mnoha počítačích.

Dalším typem hrozeb je neautorizované používání informačních systémů a služeb jimi poskytovaných, neautorizované použití zdrojů, znepřístupnění služeb[8].

Mezi hrozbou, zranitelným místem a rizikem existují vazby, ty jsou zobrazeny na obrázku č. 5.



Obrázek 7: Vazby mezi hrozbou, zranitelným místem a rizikem[zdroj: vlastní]

5.4 Útok

Útokem lze označit bezpečnostní incident,při kterém dojde k úmyslnému využitkování zranitelného místa, tj. využití zranitelného místa ke způsobení škod/ztrát na aktivech informačního systému, nebo neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech. Při analýze možných forem útoků na IT je třeba typicky řešit problémy typu: jak se projevuje počítačová kriminalita, jaké jsou možné formy útoků, kdo útočí, kdo může páchat počítačový zločin, jaká rizika souvisí s používáním informačních technologií, jak se chránit před útoky apod. Následně řešenými problémy jsou pak rozhodnutí typu: jak

[8] Služby= akce a události, které brání autorizovaným subjektům využívat systém IT na dohodnuté úrovni poskytovaných služeb, popírání odpovědnosti za akce citlivé z hlediska bezpečnosti, např. popírání aktu zaslání nebo přijetí zprávy, popírání autorství dané zprávy.

detekovat útok, jak zjistit bezpečnostní incident, jak reagovat na útok, co dělat, když dojde k bezpečnostnímu incidentu. [1]

5.4.1 Kategorizace útoků

Útok na hardware lze provést:

- přerušením: přírodní havárie, útoky způsobené údery, krádeží, kouřením, destrukcí, apod.
- odposlechem,
- přidáním hodnoty: změnou režimu činnosti informačního systému,

Útok na software lze provést:

- přerušením: úmyslné vymazání programu, vymazání softwaru způsobené špatným konfiguračním systémem nebo archivačním systémem, použití neotestovaných programů, chyby operátora,
- odposlechem: provedení neoprávněné kopie programu,
- přidáním hodnoty: trojský kůň, vir, červ, apod.

Útok na data je mnohem nebezpečnější, protože data umí číst a interpretovat de facto kterýkoliv člověk. Tento útok lze provést:

- přerušením: vymazání, sabotáž,
- odposlechem: porušení důvěrnosti,
- změnou: porušení integrity, apod.

5.4.2 Kdo může útočit?

Útok na informační systém lze provést z vnějšku i z vnitřku. Mezi typy útočníků (tedy vnějším a vnitřním) a typy cílů útoků není velká souvislost. Jako příklad lze uvést tajnou vojenskou operaci, o jejíž informace má zájem jak špion, tak i hacker.

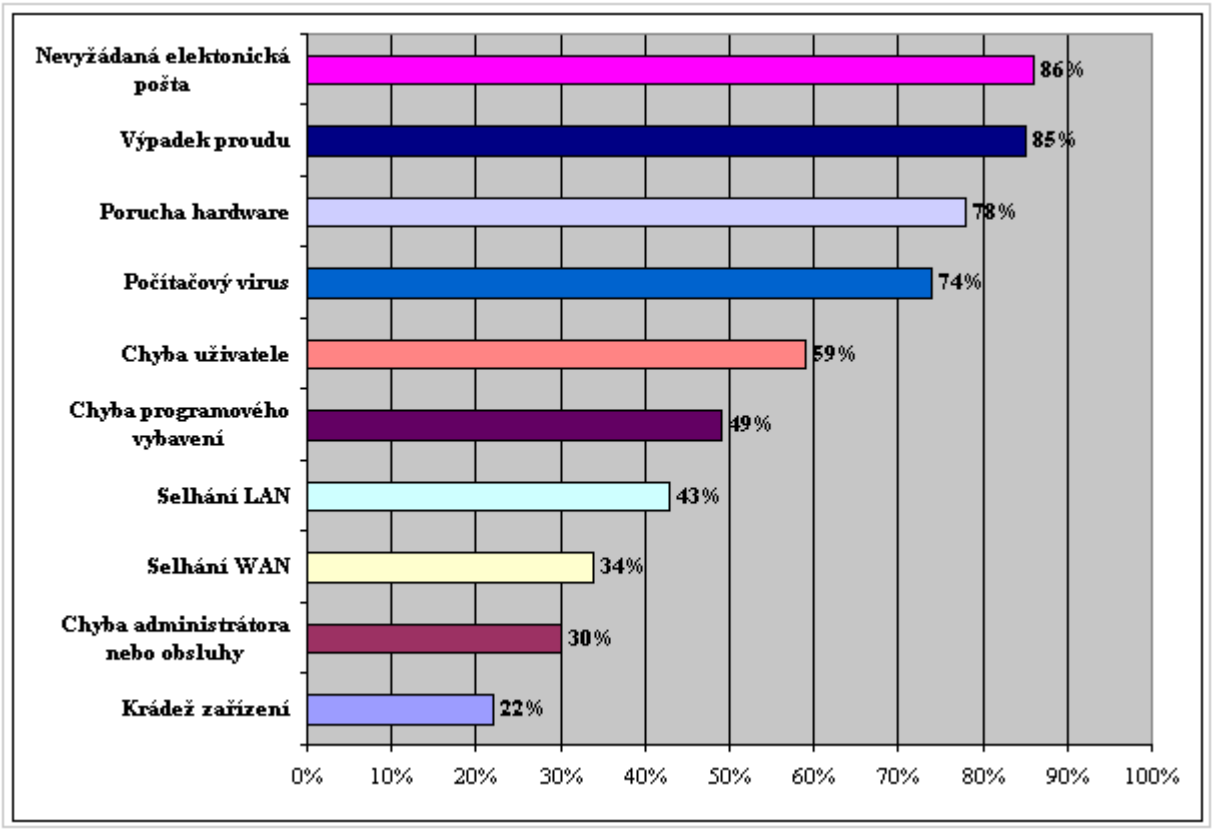
Útočit může:

- **amatér, náhodný útočník**: tito objeví jen náhodně zranitelná místa, to při své běžné práci, lze je definovat omezenými znalostmi o informačním systému, další omezenost spočívá ve financích či časové náročnosti, jejich útoky jsou náhodné a činí se proti nim jen slabá protiopatření,

- **hacker:** pro tuto skupinu útočníků jsou typické noční útoky, využívají různé časové zóny,

- **vandal:** obvykle ho nemotivuje žádná intelektuální, finanční či politická situace, jeho jedinou motivací je jen nenávist a zloba, jejich cílem je zničení, škoda logická i fyzická.

Mezi nejčastější bezpečnostní incidenty lze zařadit spam, který si prvenství „zasluhuje“ díky 86 procentům, překvapující je těsný závěs výpadku elektrického proudu s 85 procenty, další nebezpečí představuje porucha hardwaru ze 78 procent, nákaza počítačovým virem (74 procenta) a chyby uživatelů (59 procent), atd. tyto incidenty jsou zobrazeny na grafu č.2, kde osa x znázorňuje procenta a osa y druhy bezpečnostních incidentů.



Graf 2: Nejčastější bezpečnostní incidenty[9]

Doporučením ke zlepšení ochrany dat v oblasti prevence může být [5]:

- zajistit bezpečnost fyzického přístupu pouze pro autorizované osoby,
- řízení provozního prostředí(klimatizace, vytápění) pod kontrolou,
- ochrana proti výpadkům a kolísání napětí,
- antivirový software,
- řízení uživatelských přístupů: přidělování přístupových práv, změny přístupových práv při změnách pracovního zařazení, rušení uživatelských přístupů u odcházejících zaměstnanců,
- pravidla pro přístupová hesla ke kritickým datům: počet a kombinace znaků, periody pro změny hesel.

Následující tabulka č.2 obsahuje stručný seznam nejpoužívanějších antivirových software.

tabulka 2: Antivirový software[zdroj: vlastní]

Název	**www adresa**
Kaspersky Anti-Virus	http://www.kaspersky.com
Norton Anti Virus	http://www.symantec.com
Panda	http://www.panda-software-online.com
PC Tools AntiVirus	http://www.pctools.com
AVG Grisoft	http://www.grisoft.com

6. Bezpečnostní politika v oblasti IT

Bezpečnostní politika v oblasti IT je nedílnou součástí všeobecné **bezpečnostní politiky organizace**, která představuje souhrn bezpečnostních zásad a předpisů definujících způsob zabezpečení organizace od fyzické ostrahy, přes ochranu profesních zájmů až po ochranu soukromí a lidských práv.

Bezpečnostní politika IT organizace (také **celková bezpečnostní politika IT**) se v tomto kontextu zabývá výběrem bezpečnostních zásad a předpisů splňujících bezpečnostní politiku organizace a obecně definujících bezpečné používání informačních zdrojů v rámci organizace nezávisle na konkrétně použitých informačních technologiích (určuje, která data jsou pro organizaci citlivá, kdo je za ně odpovědný, předpisuje infrastrukturu zabývající se v rámci organizační struktury organizace bezpečností, vymezuje základní omezení, která se musí respektovat apod.). [2]

Náplní **systémové bezpečnostní politiky IT** je určení detailních konkrétních norem, pravidel, praktik, předpisů konkrétně definujících způsob správy, ochrany, distribuce citlivých informací a jiných konkrétních informačních zdrojů v rámci organizace, specifikace bezpečnostních opatření a způsobu jejich implementace, určení způsobu jejich použití, který zaručuje přiměřenou bezpečnost odpovídající požadavkům bezpečnostní politiky IT organizace. Provozní prosazování systémové bezpečnostní politiky se často označuje pojmem **bezpečnostní program**.

Důležité je si uvědomit, že zkušenosti útočníků v čase rostou, cíle jejich útoků se postupně upřesňují, informační technologie se vyvíjejí a zdokonalují, mění se případně i cíle profilu organizace. Proto se i cíle, strategie a politiky bezpečnosti musí periodicky korigovat. Vhodné jsou proto periodické aktualizace bezpečnostních politik, které mohou vyvolat požadavek opakovaného provedení analýzy rizik, periodicky je potřebné provádět i bezpečnostní audit.

6.1 Zásady výstavby bezpečnostní politiky IT

Bezpečnostní politika IT organizace obecně vymezuje:

- tím, co vyžaduje ochranu,
- proti jakým hrozbám je ochrana budovaná,

- jak je potřeba chránit to, co vyžaduje ochranu.

Dosažení požadované úrovně bezpečnosti informačního systému podporuje řádné provádění **správy konfigurace.** Jedná se o systematické vedení evidence změn konfigurace použitých IT. Každá změna v konfiguraci se vždy musí posoudit z hlediska dopadu na jeho bezpečnost. Systematičnost zaručí promítnutí změn i do všech relevantních dokumentů, např. do havarijního plánu, do přijatých administrativních opatření atd. Kriticky rozsáhlá změna může vyvolat přepracování systémové bezpečnostní politiky. Smyslem správy konfigurace je přitom mít vědomost o tom, co se změnilo a ne zabránit změnám.

Druhou podporu bezpečnosti informačního systému přestavuje **správa změnového řízení.** Zde se jedná se o pomocný řídicí nástroj pro identifikaci nových požadavků na bezpečnost po změně vlastností IS. Změny mohou představovat zařazení nových provozních procedur, inovaci softwaru, revize hardwaru, zařazení nových uživatelů, nových skupin uživatelů, nová síťová spojení. Každá změna se opět musí posoudit z hlediska dopadu na bezpečnost. Výsledek projednání dopadu změn a případné manažerské rozhodnutí se musí dokumentovat.

6.2 Cíle bezpečnostní politiky IT

V reálném prostředí se nelze vyhnout tlaku na zajištění potřebné úrovně důvěrnosti, autentizace, integrity dat a prevence před viry a jinými škodlivými programy, nepopiratelnosti odpovědnosti a potřebné velikosti výpočetního a paměťového výkonu. [2]

V distribuovaném prostředí, jakým síť Internet je, se k uvedeným cílům přidává požadavek **bezpečnosti** transakcí, např. mezi webovskými klienty a servery. Na webovských serverech se uchovávají jak veřejně dostupné soubory, tak soubory citlivé a důvěrné, a ty je třeba ochránit. Je třeba přijmout opatření proti virové nákaze, prohlížeč by neměl spouštět žádné nedůvěryhodné aplikace. Nabízí se otázka:„ Které požadavky na bezpečnost zpracování komerčních a legislativně citlivých informací můžeme považovat za přirozené?“ Určitě je takovým bezpečnostním požadavkem poskytnutí důvěrnosti.

Důvěrnost má zásadní význam z hlediska ochrany soukromých dat, a to jak z hlediska zachování soukromí, tak i z hlediska možnosti zneužití informačních služeb. Důvěrnost informačního systému lze zabezpečit pomocí šifrování, řízením přístupu k souborům, např. na WWW serverech.

Přirozeným požadavkem na **šifrovací systém** je dostupnost opačné operace dešifrování. K šifrování a dešifrování je třeba znát jistá tajemství. Prokázání totožnosti pomocí znalosti těchto tajemství se často využívá v souvislosti s bezpečnostní funkcí autentizace a nepopiratelnosti. Šifrování se může provádět na různých úrovních distribuovaného systému podle požadované úrovně náročnosti na výkon procesoru a na prostor paměti.

Dalším možným bezpečnostním způsobem, jak zabezpečit informační systém může být uplatnění **řízení přístupu.** Může být žádoucí, aby byla neviditelná pouze část nějaké transakce, zatímco její zbytek může být veřejně dostupný. Takové výběrové řízení přístupu k transakcím, umožní zákazníkovi (např. při elektronickém obchodování) „zabalit“ svoje identifikační informace o platební kartě do elektronické obálky, kterou může otevřít pouze banka tohoto zákazníka, kartu pak může tato banka přiložit k objednávce a zaslat obchodníkovi. Obchodník obálku předá bance, která obchodníkovi potvrdí solventnost zákazníka, a tento může pokračovat v prodeji, aniž by mu zákazník svoje soukromá data zpřístupňoval.

Dalším přirozeným požadavkem je požadavek zajištění **integrity**. Integrita musí zajišťovat, aby aktiva, dostupná autorizovaným uživatelům, byla úplná a věrná, tj. odpovídající své specifikaci. Data při přenosu nemohou být neautorizovaně měněna. Data nelze modifikovat ani v místě jejich dlouhodobého uložení v nějaké paměti. Pro zajištění integrity dat lze použít např. elektronického podpisu. Pro zajištění integrity softwaru je přirozeně nutné používat také adekvátní aktuální antivirové nástroje.

Zajištění **autentičnosti** je dalším požadavkem bezpečnosti IT. Komunikující strany by měly důvěřovat tomu, že komunikují s tím partnerem, se kterým komunikovat chtěly. K silné autentizaci je zapotřebí obvykle použít mechanismů již zmiňovaného elektronického podpisu a certifikátů. Dostatečně důvěryhodné prokázání identity lze (podle výsledků analýzy rizik) také dosáhnout např. jednoduchým používáním hesel.

Je-li dalším požadavkem zajištění **nepopiratelnosti**, pak je podmínkou, aby žádná ze spolupracujících stran neměla možnost svoji účast v transakci popřít, a to i po jejím ukončení. Aby bylo možné použít nějaký mechanismus pro implementaci funkce nepopiratelnosti, je zapotřebí, aby tento mechanismus měl i tu vlastnost, která by prokazovala autorství. Takovým mechanismem je např. certifikovaný elektronický podpis.

Nedílnou součástí bezpečnostní politiky on-line provozovaných informačních systémů musí být mechanismus, který by zajišťoval trvalou **dostupnost** jeho informatických služeb, tj. který by zamezil neoprávněnému vyčerpání zdrojů vnějším útočníkem nebo nedokonale vyškoleným vlastním zaměstnancem firmy. Tyto mechanismy se realizují např. definováním mezí dostupného paměťového prostoru, omezením délek elektronicky vyměňovaných zpráv nebo velikostí dostupného procesorového výkonu.

Možností přístupů k zabezpečení IT je více, některé jsou zajímavější nákladově, jiné dosaženou transparentností, další pak odolností proti útoku výjimečné síly. Doporučená varianta bezpečnostní politiky IS by měla vždy vzejít z oponované a závazně přijaté bezpečnostní politiky firmy a bezpečnostní politiky IT firmy (při respektování výsledků analýzy rizik informačního systému).

Podle požadované úrovně zabezpečení lze rozeznat bezpečnostní politiky těchto obecných typů [7], [2]:

a. Promiskuitní bezpečnostní politika

Jedná se o bezpečnostní politiku, která nikoho neomezuje, která každému v zásadě povoluje dělat vše, tedy i to, co by dělat neměl. Informační systémy s promiskuitní bezpečnostní politikou jsou obvykle provozně nenákladné, častokrát ani nenutí povinně používat pro autentizaci alespoň hesla a zaručují pouze minimální nebo vůbec žádnou bezpečnost. Důvodem používání informačního systému s promiskuitní bezpečnostní politikou může být ekonomičnost řešení, potřebná úroveň bezpečnosti může být zajišťována prostředky mimo IT.

b. Liberální bezpečnostní politika

Jedná se o bezpečnostní politiku, která každému povoluje dělat vše, až na věci explicitně zakázané. Liberální bezpečnostní politika zaručuje větší bezpečí než promiskuitní bezpečnostní politika. Liberální bezpečnostní politika je často uplatňována v prostředích, ve kterých se hrozby považují za málo až průměrně závažné a nepominutelným požadavkem je nízká ekonomická náročnost řešení bezpečnosti. Je pro ni typické, že se opírá o zásadu volitelného řízení přístupu založeného na identitě subjektů.

c. Paranoidní bezpečnostní politika

Zde se jedná o bezpečnostní politiku, která zakazuje dělat vše potenciálně nebezpečné, tedy i to, co by nemuselo být explicitně zakazováno. Zaručuje nejvyšší stupeň bezpečnosti.

Např. zakáže používat jakékoliv internetovské služby, s odůvodněním, že by se daly zneužít, resp. předepíše používat informační systém bez možnosti on-line napojení pro komunikaci. Vede pak k maximální izolaci systému. Paranoidní bezpečnostní politika může být pro mnoho organizací stále ještě užitečná. Databázový systém, který bude ve firmě zpracovávat vysoce důvěrné informace, lze fyzicky a technicky izolovat na systém s konečným počtem snadno kontrolovatelných vstupů a výstupů. Charakter paranoidní bezpečnostní politiky umožní implementovat aplikace v prostředí s vyšší výkonností při zachování nižší úrovně nákladů.

6.3 Principy určující charakter bezpečnostní politiky

Následující výčet popisuje principy, kterými se firma musí při vypracovávání bezpečnostní politiky řídit. Všechny principy musí být specifikovány přesně a konkrétně[2], [6]:

a. Princip znalosti

Tento požaduje, aby všechny subjekty, vztahující se na informační systém, znaly cíle bezpečnostní politiky a použitá opatření a uměly je také aplikovat. Rozumět a být informován o principech zabezpečení je hlavním zájmem takových subjektů. Je samozřejmé, že se nejedná o otevírání informačních systémů útokům, nejedná se ani o učení, jak využít jednotlivé nástroje, které by případný útok na informační systém firmy usnadnily. Jestliže provozovatel nějaké sítě umožní další organizaci tuto síť používat pro poskytování služeb třetím stranám, může si tento provozovatel do smlouvy napsat požadavek, že musí být jako provozovatel sítě seznámen s bezpečností takového informačního systému. To platí i naopak, provozovatel takového informačního systému může po provozovateli sítě požadovat seznámení s aplikovanými bezpečnostními opatřeními a jejich váhou. Zákazník banky má právo být informován o existenci a implementaci bezpečnostních politik své banky.

b. Princip adresné odpovědnosti

Tento princip požaduje, aby byly stanoveny konkrétní odpovědnosti vlastníka, správce, uživatele informačního systému a všech ostatních, kteří mají možnost dostat se do styku s daným informačním systémem, a aby jejich činnost byla na potřebné úrovni detailizace bezpečně protokolována. Takovými to lidmi je třeba rozumět management organizace, operátory, programátory, pracovníky údržby a pracovníky provozních složek organizace, externí a interní auditory, správce sítě apod.

c. Princip multidisciplinárnosti

Tento požaduje, aby byla všechna relevantní provozní, komerční, technická, administrativní, výchovná či legislativní hlediska bezpečnosti informačního systému firmy akceptována. Bezpečnostní politika firmy musí být budována s respektováním zájmů a povinností managementu firmy, jejího právního oddělení, oddělení technické podpory apod. Jiná bezpečnostní politika je pochopitelně vhodná pro zdravotnickou organizaci, jiná pro městský úřad, jiná pro obchodní firmu a jiná pro školu.

d. Princip integrity

Ten požaduje, aby byla dosažena integrita cílů a funkcí bezpečnostní politiky firmy. A to s cíli, praktikami, strukturami a zvyklostmi běžně zavedenými v této firmě. Bezpečnostní politika musí zajistit celý cyklus života informací, jejich získávání, vytváření, zpracovávání, uchovávání, přenášení, rušení. Záruka za celkovou bezpečnost informačního systému takovéto firmy je dána úrovní bezpečnosti jeho nejslabšího článku.

e. Princip aktuálnosti

Takovýto princip vyžaduje spolupráci všech partnerů při vyskytnutí aktuální hrozby a způsobům jejich projevu.

f. Princip periodického hodnocení

Tento princip je dán tím, že informační systém je obvykle dynamickou jednotkou a požadavky na jeho bezpečnost a efektivnost se v průběhu času mění, je proto důležité uvědomit si i nutnost aktualizace.

g. Princip úměrnosti

Jeho cílem je, aby síla bezpečnostních funkcí byla úměrná jak možným hrozbám a jejich rizikům, tak i možným škodám. Dosažení maximálně možné bezpečnosti za každou cenu by nemuselo být pro firmu vždy ekonomické. Proto je třeba nejprve provést ocenění aktiv, pak analýzu rizik a teprve poté určovat potřebnou bezpečnostní ochranu a sílu použitých bezpečnostních mechanismů pro její implementaci. Možným bezpečnostním opatřením může být i pojištění.

7. Závěr

Díky tomu, že bezpečnostní politika firmy Magnet je dokumentem důvěrným, nemohla firma poskytnout veškeré informace, neboť se jednalo i informace neveřejné. Ze zmapování vztahu bezpečnostní politiky k jednotlivým oddělením firmy vyšlo najevo, že je tento dokument důležitý především pro oddělení IT, které provádí dohled nad dodržováním zásad bezpečnostní politiky a dále pro personální oddělení, které zpracovává osobní údaje všech zaměstnanců. Je tedy potřeba, aby se tímto dokumentem řídili všichni zaměstnanci firmy a znali svá práva i povinnosti při dodržování bezpečnosti.

Pro sestavení bezpečnostní politiky byl nejprve stanoven její obsah. Obsah tvoří analýza rizik, která určí, co a proti čemu se musí chránit, dále byla navrhnuta vhodná ochrana všech aktiv firmy a stanoveny havarijní plány tak, aby každý věděl, co má v případě havárie dělat. Byly stanoveny i zásady, kde má být tento dokument uložen a jak má být aktualizován. Dála byl sestaven tým pro realizaci bezpečnostní politiky tvoří oddělení bezpečnosti, které tento dokument vypracuje společně se správcem, schválí ho ředitel, to po konzultaci s personálním oddělením a řídit se jím musí všichni zaměstnanci.

Mezi nejdůležitější právní předpisy České Republiky, které se týkají informační bezpečnosti byl zařazen zákon č. 513/1991 Sb., který upravuje obchodního tajemství a zákon č. 101/200 Sb., který upravuje ochranu osobních údajů. Pro Evropskou Unii je jednou z takovýchto předpisů Směrnice 1995/46/ES o ochraně osobních dat a informační bezpečnost je také zakotvena v normách ČSN ISO/IEC.

8. Použitá literatura

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

[5] Kunderová, L. *Obnova podnikových procesů po havárii informačního systému*, Zlín: Univerzita Tomáše Bati ve Zlíně, 2005, ISBN 80-7318-269-6

[6] Požár, J. *Informační bezpečnost*. Praha: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

[3] Smejkal, V., Rais, K., *Řízení rizik ve firmách a jiných organizacích*, 2. vydání, Grada Publishing, 2006, ISBN 80-247-1667-4

[2] Souček, Z., *Firma 21. století*, 1. vydání, Professional publishing, ISBN 80-86419-88-6

[7] Staudek, J., Hanáček, P. *Bezpečnostní politika IS a Internet*. Praha: Lancom, 1997. ISSN 1210-2997.

[4] Veber, J. a kol. *Management kvality, enviromentu a bezpečnosti práce*, Praha: Management Press, 2006, ISBN 80-7261-146-1

[8] Směrnice firmy Magnet Blance Porte

[9] URL: <http: // www.isdn.cz >

[11] URL: <http://www.isvs.cz>

[12] URL: <http: // www.lupa.cz >

[10] URL: <http://www.micr.cz>

9. Seznamy

Obrázky:

Tabulky:

Grafy:

Zkratky:

apod.= a podobně
č.= číslo
ČSN= Česká numismatická společnost
DB= Databáze
EDI= Electronic Data Interchange
EHS= Evropské Hospodářské Společenství
ES= Evropská Společenství
EU= Evropská Unie
HW= Hardware
IBM= International Business Machines
IDA= Interchange of Data between Administrations
IS= informační systém
ISO= International Organization for Standardizartion
IT= Informační Technologie
ITSEC= Information Technology Security Evaluation Kriteria)
např.= například
NBÚ= Národní Bezpečnostní Úřad
odst.= odstavec
PC= počítač
příp.= případně
resp.= respektive
Sb.= Sbírka
tj.= to je
ÚOOÚ= Úřad pro ochranu osobních údajů
viz. (od latinského slova "videlicet")= patrně, zřejmě, zjevně, totiž, jistěže, jmenovitě
www= world wide web

10. Rejstřík

Příloha 1: Právní předpisy ČR

Mezi nejdůležitější právní předpisy České republiky se vztahem na informační bezpečnost patří:

Ústavní zákon č. 23/1991 Sb., kterým se uvozuje Listina základních práv a svobod,

Zákon č. 101/2000Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů,

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů,

Zákon č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů,

Zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů,

Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů,

Zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů,

Zákon č. 551/1991 Sb., o Všeobecné zdravotní pojišťovně České republiky, ve znění pozdějších předpisů,

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějšího předpisu,

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích),

Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů,

Zákon č. 480/2004 Sb., o některých službách informační společnosti,

Usnesení vlády ČR č.624 ze dne 20. června 2001, o pravidlech, zásadách a způsobu zabezpečování kontroly užívání počítačových programů,

Ústavní zákon č. 110/1998 Sb., o bezpečnosti ČR, ve znění pozdějšího předpisu,

Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně dalších zákonů, ve znění pozdějších předpisů,

Vyhláška NBÚ č. 56/1999 Sb., o zajištění bezpečnosti informačních systémů nakládajících s utajovanými skutečnostmi, provádění jejich certifikace a náležitostech certifikátu,

Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění zákona 320/2002 Sb.,

Nařízení vlády 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon),

Zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů, ve znění pozdějších předpis,

Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon),
Zákon č. 89/1995 Sb., o státní statistické službě, ve znění pozdějších předpisů,
Zákon ČNR č. 552/1991 Sb., o státní kontrole, ve znění kontrolního předpisu,
Zákon č. 166/1993 Sb., o Nevyšším kontrolním úřadu, ve znění pozdějších předpisů.

Příloha 2: Legislativní předpisy a programy Evropské unie

Nejdůležitějšími legislativní předpisy a plány Evropské unie pro oblast informační bezpečnosti jsou:

Směrnice 1997/66/ES o ochraně dat v telekomunikacích,

Směrnice 1995/46/ES o ochraně osobních dat,

Směrnice 2002/58/ES o soukromí v elektronické komunikaci,

Směrnice 1999/93/ES o zásadách Společenství pro elektronické podpisy,

Směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí,

Nařízení 2001/45/ES o ochraně fyzických osob při zpracování osobních údajů orgány a institucemi,

Směrnice rady 1991/250/EHS o právní ochraně počítačových programů,

Směrnice rady 2001/264/ES o ochraně utajovaných informacích,

IDA: elektronická výměna dat mezi administrativami členských zemí,

eEurope 2005: informační společnost pro všechny, víceletý program podpory k prosazování informační společnosti v Evropě.

Příloha 3: Normy, které se týkají informační bezpečnosti

V rámci řízení informační bezpečnosti jsou nejvýznamnější tyto normy:

ČSN ISO/IEC 17799:2001

Informační technologie – Soubor postupů pro řízení informační bezpečnosti

ČSN BS 7799-2:2004

Systém managementu bezpečnosti informací - Specifikace s návodem pro použití

ČSN ISO/IEC 13335-1:1999

Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 1: Pojetí a modely bezpečnosti IT

ČSN ISO/IEC 13335-2:2000

Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 2: Řízení a plánování bezpečnosti IT

ČSN ISO/IEC 13335-3:2000

Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 3: Techniky pro řízení bezpečnosti IT

ČSN ISO/IEC 13335-4:2002

Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 4: Výběr ochranných opatření

ČSN ISO/IEC 13335-5 (zatím nevydáno)

Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 5: Ochranná opatření pro externí spojení

ČSN ISO/IEC 15408-1:2001

Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT

ČSN ISO/IEC 15408-2:2002

Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT – Část 2: Bezpečnostní funkční požadavky

ČSN ISO/IEC 15408-3:2002

Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT – Část 3: Požadavky na záruky bezpečnosti

ČSN ISO/IEC 15816:2003

Informační technologie - Bezpečnostní techniky - Bezpečnostní informační objekty pro řízení přístupu

ÚDAJE PRO KNIHOVNICKOU DATABÁZI

Název práce	Bezpečnostní politika firmy
Autor práce	Jitka Havelková
Obor	Systémové inženýrství a informatika
Rok obhajoby	2007
Vedoucí práce	Ing. Renáta Bílková
Anotace	
Klíčová slova	Bezpečnostní politika, informační bezpečnost a ochrana, bezpečnost IT, informace, útok, riziko.