Návrh řešení bezpečnostní politiky firmy ISDIM s.r.o.

The proposal of solving the security policy in the company ISDIM s.r.o.

Kateřina SULOVSKÁ

Bakalářská práce
2007

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2006/2007

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Kateřina SULOVSKÁ**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Návrh řešení bezpečnostní politiky firmy ISDIM s.r.o.**

Zásady pro vypracování:

1. Vyhledejte vhodné informační zdroje řešící problematiku bezpečnostních politik organizací.
2. Analyzujte současný stav úrovně bezpečnostní politiky ve vybrané organizaci.
3. Navrhněte vhodné řešení bezpečnostní politiky na úrovni současných poznatků.
4. Vyhodnoťte úspěšnost návrhu řešení a definujte jeho silná a slabá místa.

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] Látal, I., Štantejský, M.: Bezpečnostní zásady ochrany podniku: prevence a řešení krizových situací, 4. vydání, PROSPEKTUM, Praha 2001, 120 str., ISBN 80-7175-091-3
[2] Brabec, F. a kol.: Bezpečnost pro firmu, úřad, občana, 1. vydání, Public History, Praha 2001, 400 str., ISBN 80-86455-04-06
[3] Brabec, F.: Ochrana bezpečnosti podniku, 1. vydání, EUROUNION, Praha 1996, 204 str., ISBN 80-85858-29-0
[4] Rodryčová, D., Staša, P.: Bezpečnost informací jako podmínka prosperity firmy, 1. vydání, Grada Publishing, Praha 200, 144 str., ISBN 80-7169-144-5
[5] Laucký, V.: Technologie komerční bezpečnosti II, 1. vydání, Univerzita Tomáše Bati ve Zlíně, Zlín 2004, 123 str., ISBN 80-7318-231-9
[6] Doseděl, T.: Počítačová bezpečnost a ochrana dat, 1. vydání, Computer Press, Brno 2004, ISBN 80-7226-632-2

Vedoucí bakalářské práce: **Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a statistiky

Datum zadání bakalářské práce: **13. února 2007**

Termín odevzdání bakalářské práce: **29. května 2007**

Ve Zlíně dne 13. února 2007

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cílem této práce je na základě získaných informací kvalifikovaně zhodnotit stávající bezpečnostní politiku reálné firmy a navrhnout její zlepšení. Byla provedena analýza rizik s vyhodnocením silných a slabých stránek bezpečnostních opatření firmy a byla navržena řešení k jejich eliminaci. Výstupem je komplexní řešení problematiky bezpečnostní politiky reálné firmy jako podklad pro další využití touto firmou. V práci jsou podrobně teoreticky rozebrány i jednotlivé části bezpečnostní politiky s ohledem na okolní i vnitřní činitele.

Klíčová slova: Bezpečnostní politika, bezpečnostní expertíza, ochrana znalostí a datová bezpečnost, objektová bezpečnost, konkurence

ABSTRACT

The aim of this work is to evaluate expertly the current security policy of an existing company and propose measures for its improvement on the basis of the gained information. The risk analysis was made, strong and weak points of safety precautions in the company were assessed, and solutions leading to their elimination were suggested. The output of this work is a complex solution of the security policy in a real company with consecutive utilization in this company. The individual components of the security policy are theoretically analyzed with reference to inner as well as outer factors.

Keywords: Security policy, security expertise, knowledge protection and data security, object security, competition

PODĚKOVÁNÍ

Na tomto místě bych ráda poděkovala svému vedoucímu bakalářské práce Doc. Mgr. Romanu Jaškovi, Ph.D. za odborné konzultace, poskytnuté odborné znalosti, vědomosti a poznatky, jejich přínos, ale také čas k úpravě, připomínkám a návrhům formy zpracování bakalářské práce.

Ráda bych také poděkovala Ing. Michalu Hrabákovi a zaměstnancům jeho společnosti ISDIM s.r.o. za zpřístupnění informací potřebných k tvorbě návrhu řešení bezpečnostní politiky a vzájemnou spolupráci po celou dobu tvorby této práce.

Současně chci poděkovat JUDr. Vladimíru Lauckému za odborné rady, vedení a podnětné připomínky, které mi poskytl nejen k problematice související s tématem této práce.

V neposlední řadě bych chtěla poděkovat své rodině za cenné připomínky při tvorbě bakalářské práce a podporu po celou dobu studia, čehož si nesmírně vážím.

Prohlašuji, že jsem na bakalářské práci pracovala samostatně a použitou literaturu jsem citovala. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uvedena jako spoluautor.

Ve Zlíně 29.05.2007

…….....

Kateřina SULOVSKÁ

OBSAH

ÚVOD

V dnešní době je pro každou konkurenceschopnou firmu důležité, aby si dokázala různými prostředky ochránit svoje firemní know-how, výrobní postupy a znalosti, investice, kompetentnost svých zaměstnanců a jejich pravomoci především vzhledem k informacím a datům. Moderní doba umožňuje moderní věci. S neustálým zaváděním nových technologií tak vzniká problém především jak ochránit tolik ceněné informace. Jednou z možností jak snížit riziko různých krádeží informací, ale i majetku, je vytvoření kvalitní bezpečnostní politiky s návazností na krizové nebo havarijní plány. S kvalitní bezpečnostní politikou potom může firma směle čelit většině útoků, aniž by utrpěla citelnou ztrátu, která by její činnost ukončila.

Téma své bakalářské práce jsem si zvolila především pro jeho nespornou praktičnost, díky níž si na vlastní kůži mohu vyzkoušet, někdy i velmi nesnadnou, úlohu navržení funkčního systému, který bude kromě svých bezpečnostních funkcí plnit i funkce, jež požaduje klient a na něž musí být nahlíženo i z hlediska ekonomické situace subjektu. S těmito otázkami se poté v praxi setkávají dennodenně projektanti a poradci v oblasti bezpečnosti.

Bezpečnostní politiku jako takovou zpravidla řeší pro danou organizaci tým specialistů, který minimálně půl roku sleduje veškerý chod v organizaci, poté navrhne vlastní řešení bezpečnostní politiky, který je následně implementován a opět pozorován minimálně pět měsíců po dokončení implementace. Samotné úspěšné zavedení bezpečnostní politiky je tedy otázkou minimálně jednoho roku, kdy je pečlivě sledován a v případě dlouhodobějších potíží ihned program politiky regenerován.

Ve své práci se proto pokusím co nejlépe nahradit tým specialistů a potřebné časové intervaly zkrátit na nezbytné minimum pro základní poznání chodu firmy a navrhnout takové řešení bezpečnostní politiky na základě informací o společnosti, které mi byly poskytnuty, které bude v souladu s přáním a požadavky majitele.

I. TEORETICKÁ ČÁST

1. BEZPEČNOSTNÍ POLITIKA

Bezpečnostní problematika provází člověka již od počátků jeho existence. Důvody a metody zabezpečení se samozřejmě v průběhu historie měnily, avšak předmětem zabezpečení a ochrany byly vždy tři hlavní skupiny, které spolu úzce souvisí a často se i prolínají, zejména v případě ochrany nehmotných statků a informací a znalostí na informacích založených. Jsou to:

1) zdraví a život – to jest vše, co je spojeno s fyzickou existencí jedinců
2) majetek – tzn. vše, co je spojeno s vlastnickými a obdobnými vztahy k věcem a předmětům i k nehmotným statkům
3) informace a znalosti na těchto informacích založené – tzn. to, co je spojeno s prosazováním a ochranou zájmů jednotlivých osob a skupin osob v rámci jejich existence ve společenství.

Zvláštní skupinou jsou poznatky a znalosti získané na základě informací. Jde zejména o takové znalosti a informace, které nejsou běžně dostupné nebo jejich zpracování je náročné a méně dostupné většímu okruhu subjektů. Nejsou to tedy veškeré informace, ale jen takové, které mají určitou, často velmi významnou, hodnotu pro jejich nositele a pro určitý okruh subjektů v případě, že by takovou informaci, popř. znalost, získaly. Současně jde ale i o informaci s omezenou dostupností. Jsou to tedy informace a znalosti, které svému nositeli umožňují získat určitou výhodu před ostatními subjekty a jejich ztráta (např. prozrazení apod.) by mu mohla způsobit újmu. Nejde pouze o výhodu v konkurenčním hospodářském prostředí, ale může jít i o výhodu v oblasti politiky apod. [2]

Řešení bezpečnostní problematiky vyžaduje u konkrétních subjektů posouzení individuálních podmínek a zájmů dotčených subjektů. V zásadě si každý subjekt musí odpovědět na několik otázek, a to především:

1) zda a co má být chráněno
2) před čím má být předmět ochrany chráněn
3) jakým způsobem a jakými prostředky má být ochrana prováděna

Odpovědi na uvedené otázky jsou závislé na řadě okolností, které z hlediska subjektu ochrany můžeme rozlišit na vnější a vnitřní. Vnější vlivy jsou vlivy okolí organizace, tedy

okolnosti stojící mimo organizaci. Okolí organizace představují celkové politické, ekonomické, sociální, technologické a bezpečnostní rámce, ve kterých se organizace pohybuje. Jsou to faktory, které organizace svým jednáním nemůže ovlivnit, popř. je může ovlivnit pouze částečně. Jde např. o legislativní činnost státu, existence závazkových vztahů ovlivňujících organizaci (mezinárodní vztahy, smlouvy mezi podnikatelskými subjekty), dále pak demografické faktory, významné technologické inovace, konkurenční prostředí. Tyto vnější vlivy představují vnější bariéry bezpečnostní politiky organizace. Východiskem pro stanovení zásad a cílů bezpečnostní politiky jsou vnitřní vlivy – vnitřní bariéry, které pramení z možností organizace samotné a které jsou ovlivnitelné organizací. Jsou to především ekonomické možnosti organizace, její organizační uspořádání, úroveň řízení, úroveň personálního vybavení organizace, technická úroveň, úroveň vnitřní komunikace, atd. Mezi vnitřní okolnosti patří např. ekonomické možnosti subjektu realizovat nutná protiopatření. Mezi vnější okolnosti náleží zejména existence hrozeb a míra rizika, s jakou se hrozby mohou uskutečnit. [2]

Jak vnější, tak vnitřní vlivy se podílejí i na formulaci obecné politiky organizace (jedná se o poznání těchto vlivů, nalezení jejich vzájemných souvislostí a pochopení jejich významu pro fungování organizace). V rámci formulace bezpečnostní politiky budou vlivy vnější i vnitřní podrobeny opětné analýze z hlediska dalších kritérií, které pro formulaci obecné politiky nejsou použity. Kritériem pro jejich zkoumání a určování jejich vlivu na bezpečnost organizace budou bezpečnostní hlediska. Se zkoumáním vnějších a vnitřních vlivů a jejich podrobení cílenému procesu poznání (analýza, syntéza a prognóza) se opět setkáváme při hledání odpovědi na konkrétní otázky v rámci řešení konkrétních bezpečnostních problémů, tedy úkolů organizace.

Jeden z prostředků, který umožňuje organizacím dosahovat jejich obecné cíle, je i přesně formulovaná a následně realizovaná bezpečnostní politika organizace. Jde o obecnou bezpečnostní politiku organizace, která se především zabývá všemi hlavními aspekty bezpečnosti v organizaci a definuje, jaké bezpečnostní prostředí je pro organizaci optimální, s ohledem na hlavní cíle organizace, a jakými prostředky bude toto bezpečnostní prostředí dosaženo. Obecná bezpečnostní politika je také výsledkem konfrontace vnějších bezpečnostních podmínek a požadavků s vnitřními bezpečnostními podmínkami a možnostmi organizace. [2]

Bezpečnostní politika organizace zahrnuje všechny stránky bezpečnosti organizace a je jedním z nejdůležitějších dokumentů podniku, který se stává bezpečnostní normou organizace. Zároveň podporuje ostatní politiky podniku (výrobní, obchodní, atd.) současně se základními principy (etiky, obchodu, marketingu), kterými se bude řídit vrcholový management. Dokument obsahuje přesně vymezené požadované minimální standardy s ohledem na rizika, které vedení podniku přijme. Správně zvolená a jasně specifikovaná bezpečnostní politika vytváří image zdravého a stabilního podniku a umožňuje okolí nahlédnout do cílů v oblasti bezpečnosti i samotného podnikání.

Bezpečnostní politika je souhrn organizačních a řídících opatření, právních norem, standardů a jiných pravidel v rámci řízení podniku, jejichž úkolem je ohodnotit informace o veškerých podnikatelských aktivitách a ostatní fakta. Jde o zhodnocení informací o ohrožení podniku, stanovení rizik a návrhy na ochranu podniku v rámci technických, technologických, organizačních, personálních a dalších opatření jako nedílné součásti systému řízení organizace. Taktéž sem spadá koncepce rozvoje ochrany podniku, postupy a prostředky k dosažení cílů vytyčených strategií podniku. [1]

Bezpečnostní politiku organizace zpravidla definujeme jako soubor norem, opatření a pravidel, které ve svém souhrnu odpovídají především na tři základní otázky:

1) co má organizace ochraňovat, z jakého důvodu a jaké bezpečnostní cíle hodlá dosáhnout
2) před jakými hrozbami má být ochrana prováděna
3) jaké prostředky a metody ochrany budou použity

Kromě výše uvedených otázek musí být v dokumentu bezpečnostní politiky organizace zodpovězena řada dalších otázek, např.:

- kdo nese odpovědnost za naplnění závěrů bezpečnostní politiky
- kterých oblastí činnosti organizace se bezpečnostní politika dotýká
- jaký je časový horizont pro naplnění cílů bezpečnostní politiky
- způsob uvádění bezpečnostní politiky do praxe
- jaké jsou na bezpečnostní politiku kladeny požadavky z hlediska efektivity a nákladů

- jak bude dodržování bezpečnostní politiky vynucováno nebo sankcionováno při porušování
- zásady koordinace informační, majetkové a osobní bezpečnosti podniku

Jak jsem již výše zmínila, problematika bezpečnosti organizace se zaměřuje na tři základní oblasti – fyzické osoby (ochrana zdraví a života), majetek a informace společně se zájmy. Problematika bezpečnostní politiky organizace je tedy poměrně velmi široká a stejně jako ona bude muset řešit i obecná bezpečnostní politika organizace problematiku uvedených tří základních oblastí. Z toho důvodu se povětšinou pro každou oblast těchto bezpečnostních zájmů organizace formuluje samostatná dílčí bezpečnostní politika:

- politika personální bezpečnosti
- politika administrativní bezpečnosti
- v oblasti ochrany majetku:
    - politika objektové bezpečnosti – ochrana nemovitého majetku
    - politika ochrany majetku – ochrana movitého majetku
    - politika ochrany nehmotného majetku – ochrana know-how a obchodního tajemství
- politika technické bezpečnosti
- politika bezpečnosti informačních systémů
- politika ochrany utajovaných informací
- politika kryptografické ochrany

Ačkoli existuje vnitřní členění dokumentu bezpečnostní politiky podle těchto dílčích kritérii, zůstávají formule opatření a zásad v obecné rovině a k jejich podrobnému rozpracování dojde až v rámci jednotlivých projektů.

Úkolem bezpečnostní politiky je především prosadit důvěryhodný informační systém. Předpokladem pro určení cílů bezpečnostní politiky je schopnost podniku dosáhnout vytyčených cílů zvolenými a koordinovanými postupy s důrazem na efektivní realizaci záměrů. Nezbytným předpokladem a podmínkou pro přijetí a fungování bezpečnostní politiky je seznámení zaměstnanců na všech stupních řízení diferencovaně s jejími cíli a obsahem. Úspěšnost realizace závisí na schopnosti všech zaměstnanců dostát všem závazkům, jenž mají vůči podniku. Souběžně by měl probíhat i bezpečnostní průzkum v daném podniku,

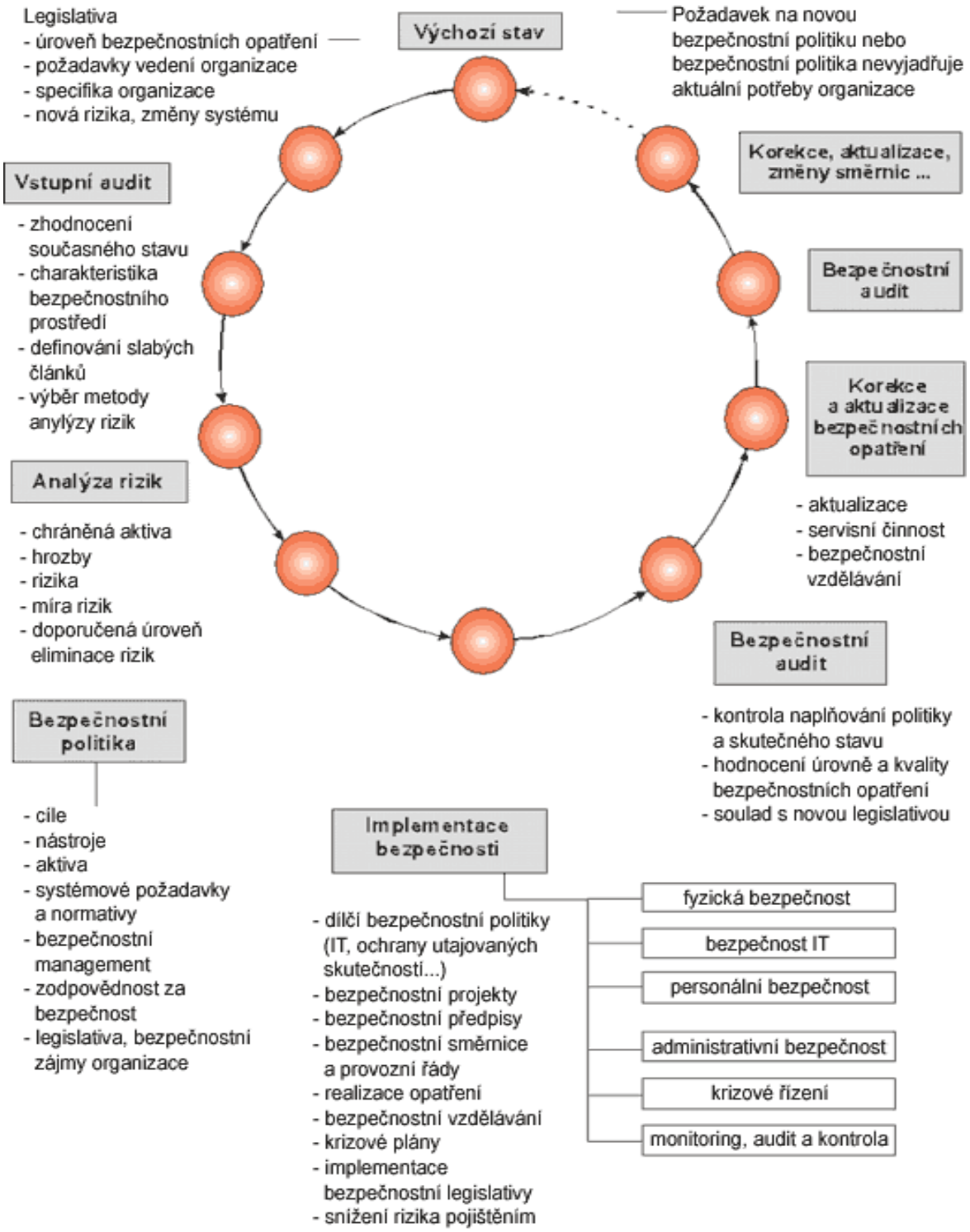
neboť formulování bezpečnostní politiky musí vycházet z konkrétní situace, odhadu budoucího vývoje a dalších podmínek. [1]

Dokument zvaný bezpečnostní politika má charakter všeobecného plánu pro oblast bezpečnosti organizace a má poměrně obecný charakter. Z hierarchie celkových zájmů a cílů organizace vyplývá, že bezpečnostní politika musí brát zřetel na závěry obecné politiky organizace, tedy na obecný strategický plán organizace, poněvadž bezpečnost je pouze jedna část činnosti organizace. Veškeré formulace v prohlášení v dokumentu bezpečnostní politiky jsou obecné a zabírají celou šíři dané problematiky uvnitř organizace a jako takové nemohou být bez dalšího rozpracování použity k přímé realizaci, avšak rozhodujícím způsobem určují směr a způsob dalšího konání organizace v dané oblasti. Bezpečnostní politiku, stejně jako obecnou politiku organizace, tedy celkovou strategii, nelze zaměňovat s vizí organizace, která hovoří o základních důvodech existence organizace. V případě konfliktu mezi cíli bezpečnostní politiky a obecné politiky, by měly být upřednostněny cíle obecné strategie organizace. Lze však připustit, že za mimořádných okolností cíle bezpečnostní politiky budou muset být naplněny i proti vůli organizace včetně překročení rámce daného obecnou politikou a tedy budou působit zpětně na formulace zásad obecné politiky organizace, která pak následně bude muset být korigována. [2]

Základním východiskem pro formulování bezpečnostní politiky organizace je obecná politika organizace, která deklaruje základní i dlouhodobé záměry organizace a způsoby a prostředky k jejich dosažení. Cíle jsou především zaměřeny na pozici firmy v daném odvětví (resp. oboru podnikání) na stanovení dlouhodobých podnikatelských cílů, očekávaných výnosů a způsobu jejich využití, na vztah organizace ke společnosti a vztah k zaměstnancům organizace.

Cílem bezpečnostní politiky je zpravidla dosažení určitého stavu a úrovně bezpečnosti organizace v určitém čase. Zájmem organizace současně je, aby se jednalo o stav a úroveň, která bude trvat i do budoucnosti a bude trvalou součástí obecné strategie organizace. Z tohoto důvodu lze bezpečnostní politiku chápat jako nepřetržitý proces, jehož obsahem je trvalé definování bezpečnostních zásad, opatření a potřeb organizace při naplňování celkové politiky organizace. Tvorba bezpečnostní politiky a bezpečnostního projektu organizací není mechanickou prací, spočívající v dosazování jednotlivých prvků do předem dané

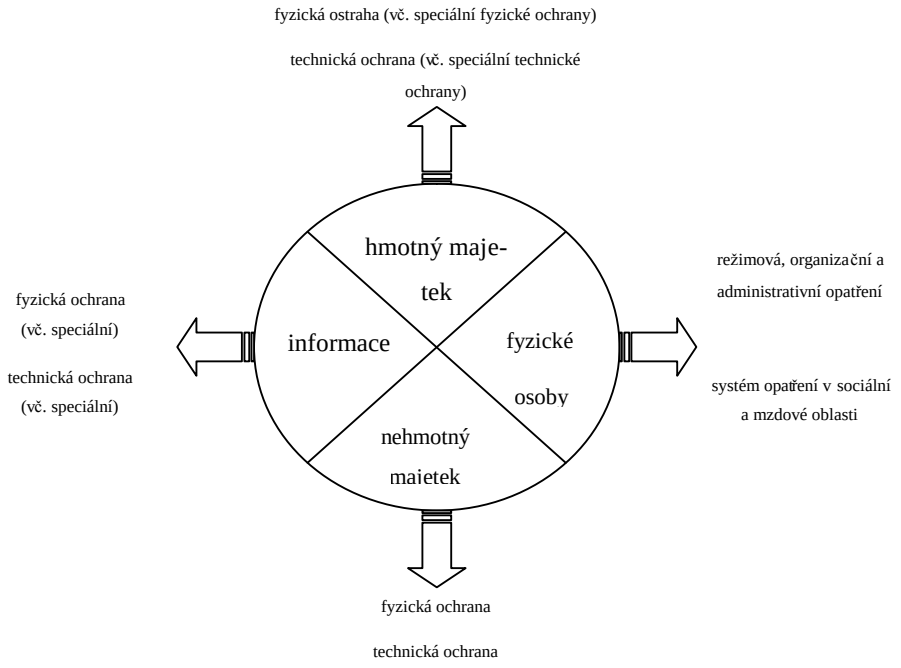
šablony, ale jedná se o tvůrčí přístup k řešení daného problému specifických podmínek konkrétní organizace. [2]



Obrázek 1. Schéma tvorby bezpečnostní politiky a její implementace (bezpečnostní plánování)

2. BEZPEČNOSTNÍ EXPERTÍZA

Bezpečnost organizace jako celku považujeme za komplexní problém a bezpečnost jejich jednotlivých součástí za problémy dílčí. Jestliže mluvíme o bezpečnostní expertíze organizace, máme na mysli komplexní bezpečnostní expertízu celé organizace. Rozdíly mezi komplexní a dílčí expertízou můžeme najít jen v šíři zkoumaných skutečností, v míře pracnosti a v počtu a složitosti zkoumaných vzájemných vazeb a souvislostí. Rozdíly mohou být v nákladech nejen na expertízu, ale i na realizaci opatření a v šíři dopadu opatření na organizaci a její jednotlivé složky. Nicméně základní přístup k řešení problému, tedy k úplnému posouzení a řešení problému všech hledisek, je společný. [3]



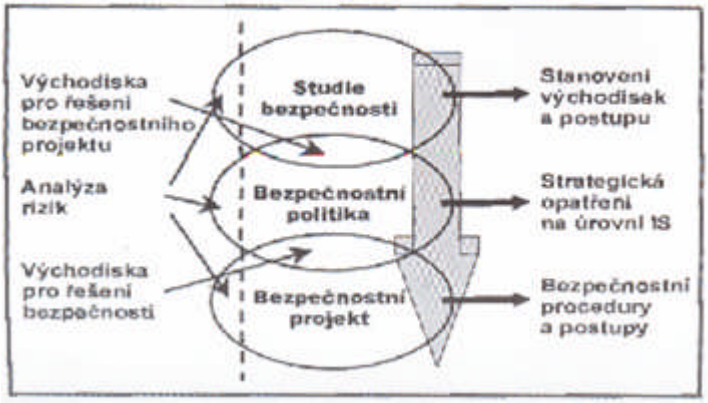
Obrázek 2. Bezpečnost organizace – komplexní pojetí

Komplexní bezpečnostní expertíza organizace zkoumá způsob, rozsah a úroveň zabezpečení jednotlivých objektů ochrany v organizaci. V zásadě lze objekty, jenž jsou nezbytné v organizaci chránit, rozdělit do tří skupin a to majetek, fyzické osoby (jejich život a zdraví) a v neposlední řadě jsou to informace. Organizace nechrání jen objekty, které jsou součástí jí samotné, ale také objekty, které jsou mimo ni. Tato skutečnost vyplývá z obecně platných právních předpisů a norem, ze smluvních závazků a z obecně nebo profesně uznávaných nepsaných pravidel a zvyklostí. K dosažení potřebného stupně zabezpečení se pak používají tyto čtyři základní skupiny bezpečnostních opatření a prostředků:

- fyzická ochrana
- technická ochrana
- administrativně organizační a režimová opatření
- kombinace předchozích prostředků a opatření

Bezpečnostní expertíza se skládá z:

- bezpečnostní analýzy
- bezpečnostní prognózy
- bezpečnostního plánu a bezpečnostního projektu



Obrázek 3. Bezpečnostní mechanismy

2.1. Bezpečnostní analýza

Bezpečnostní analýza je nezbytným východiskem pro proces syntézy získaných poznatků a vypracování bezpečnostního projektu, jehož úkolem je stanovit naprosto konkrétní opatření, kterými bude dosaženo cíle definovaného bezpečnostní politikou. Pro provádění bezpečnostní analýzy obecně nebyly vypracovány žádné speciální techniky a standardy a každá poradenská firma kombinuje běžně používané techniky s vlastními postupy. Je třeba si uvědomit, že v oblasti zabezpečení organizací nedostává analytik všechny informace v podobě, která by se dala přesně kvantifikovat.

Základním krokem před započetím analýzy je správná formulace problému. Tato informace je určující pro provedení činnosti, která bezprostředně analýze předchází. Touto činností je sběr a třídění informací. Tyto informace musí být relevantní formulovanému problému a

vytyčenému cíli. Ostatní informace mohou přispět k chybným závěrům, avšak některé informace se jako relevantní mohou začít jevit v průběhu práce. Správné posouzení použitelnosti informací tedy záleží na zkušenostech pracovníka provádějícího analýzu.

Informace relevantní pro bezpečnostní analýzu jsou obsaženy především uvnitř organizace, jsou to informace, které vypovídají přesně o konkrétních jevech v organizaci a jsou proto nejvýznamnějším zdrojem pro bezpečnostní expertízu a analýzu. Jsou to především informace obsažené uvnitř organizace:

- v základních ustavujících dokumentech organizace
- v předmětu činnosti organizace
- v organizačních a interních předpisech organizace, včetně organizační struktury
- v postavení organizace v rámci většího organizačního upořádání (např. holding, atd.)
- v technickém a technologickém vybavení organizace
- v architektonickém a stavebním řešení objektů, ve kterých organizace svou činnost vyvíjí (nejen činnost, která je předmětem podnikání)
- ve vztazích (definovaných i nedefinovaných) nadřízenosti a podřízenosti mezi jednotlivými pracovníky včetně určení osobní odpovědnosti v rámci jejich působení v organizaci
- v personálním složení organizace a zásadách personální politiky
- v rozsahu a struktuře dodavatelsko-odběratelských vztahů
- v obchodní politice organizace a v jejích vytyčených cílech
- ve vnitřní situaci organizace a jejím trendu

Další informace můžeme získat i vně organizace, a to zejména:

- v mezinárodních smlouvách a závazcích
- v mezinárodních standardech a doporučeních
- v tuzemských obecných právních předpisech a normách
- v tuzemských standardech a doporučeních
- v interních resortních předpisech
- v interních předpisech nadřízených organizačních jednotek nebo celků, ve kterých je organizace zařazena
- v celospolečenské situaci a jejím trendu

- v interní situaci resortu a jejím trendu

Zdrojem informací jsou také řídící a ostatní pracovníci organizace, ve které se analýza provádí, ale mohou to být i zaměstnanci dodavatelských firem. Ti mohou situaci zprůhlednit ze svého hlediska, ze svých praktických zkušeností, které v žádném dokumentu nejsou exaktně zaznamenány.

Výše uvedené informace mají zpravidla ustálenou formalizovanou podobu, a to:

- originální písemnosti a dokumenty
- články a studie z odborných publikací, tisku, periodik a dalších tiskovin
- statistické výkazy a roční zprávy státních orgánů a institucí
- ústní i písemná vyjádření a komentáře fyzických osob k analyzovanému problému
- dotazníkový průzkum u vybraných pracovníků
- vlastní pozorování pracovníků, kteří sběr informací provádějí
- informace získané ze sítě Internet, apod.

Vliv na kritéria výběru informací má i metodický přístup k provádění bezpečnostní expertízy, dále pak formulovaný problém a vytyčený cíl bezpečnostní expertízy. Informace třídíme v dalších etapách podle míry jejich abstraktnosti nebo konkrétnosti ve vztahu k řešenému problému a podle časového významu informace (zda je významná jen pro posouzení stávajícího stavu, nebo je významná i pro budoucnost). Podle významu můžeme informace roztřídit na informace mající rozhodující vliv na výsledky analýzy a řešení problému a informace, které mají jen omezený vliv na řešení. Dalším kritériem je dostupnost informací, podle něhož dělíme informace na veřejné, určené pro určitý okruh osob, a utajované. Podle věrohodnosti pak informace dělíme na věrohodné a nevěrohodné. Posledním hlediskem, který zde uvedu, je třídění podle oblastí, kterých se informace dotýkají a jenž souvisí s bezpečností organizace, tedy informace personální, technické, administrativní a organizační. Hledisek a kritérií, podle kterých je možné informace třídit, je ovšem mnohem více a záleží pouze na pracovníkovi, tvořícím analýzu, které využije.

Kromě sběru informací a jejich třídění je prováděno také slučování získaných informací do celků, což nám může pomoci např. v kompletaci neúplných informací nebo při zvýšení kvality informace jejím upřesněním apod. Konečné analýze pak podrobíme takto zkompletovanou novou informaci.

Analýzu můžeme charakterizovat jako metodu poznání, jejíž podstatou je postupné rozčlenění celku na jednotlivé části a studium těchto částí a jejich vzájemných vztahů. Zjednodušeně můžeme říci, že se jedná o metodu, ve které postupujeme od obecného ke konkrétnímu. Aby analýza splnila svůj cíl a měla smysl, je nutné odhalit vzájemné vztahy mezi jednotlivými částmi , mechanismy a zákonitostmi jejich vzájemného fungování. Toto umožňuje syntéza, což je proces, ve kterém jsou jednotlivé části skládány zpět do celku, avšak za účelem pochopení vzájemných vazeb mezi jednotlivými částmi navzájem a mezi jednotlivými částmi a celkem. Obě metody, analýza i syntéza, jsou navzájem úzce spjaty a jsou velmi často spojovány v jednu metodu. [3]

Bezpečnostní analýza podrobuje zkoumání předměty, jevy, informace a skutečnosti dotýkající se přímo či nepřímo bezpečností organizace, jejího bezpečnostního systému s cílem přispět k nalezení přiměřených bezpečnostních prostředků a opatření, která jsou vhodná k účinnému a adekvátnímu řešení bezpečnostního problému organizace. Pro bezpečnostní analýzu nebyly zpracovány žádné obecně platné postupy, techniky nebo mezinárodní standardy, jak jsem již zmínila. Přesto lze k provádění analýzy využít řady metod a technik z jiných oblastí, např. z oblastí ekonomiky a financí.

Mezi techniky a metody použitelné při provádění bezpečnostní analýzy organizace můžeme zařadit např.:

a) analýzu SWOT
b) analýzu PEST
c) Paretovu analýzu
d) modifikovanou analýzu stupně ohrožení
e) Išikavův diagram

2.1.1. Analýza SWOT

Tato analýzy se užívá při formulování strategického plánu organizace. Je odvozena z prvních písmen anglických slov strenghts (přednosti, silné stránky), weaknesses (slabé stránky, nedostatky), opportunities (příležitosti) a threats (hrozby), které obsahují informaci o tom, co je analyzováno. Tato metoda vychází z předpokladu, že cesta k dosažení strategického úspěchu organizace je závislá na maximalizaci jejích předností a příležitostí a na

minimalizaci jejích nedostatků a hrozeb. Pro účely bezpečnostní expertízy je nezbytné tuto metodu modifikovat, takže předmětem analýzy nebude celá organizace a její postavení na trhu, ale pouze stav její bezpečnosti jako celku.

Z pohledu této analytické metody jsou za přednosti požadovány takové vnitřní podmínky v organizaci, které představuje např. dobře propracovaná organizační struktura organizace, přesné rozdělení kompetencí a pravomocí mezi jednotlivé řídící pracovníky, odborná kvalifikace pracovníků působících v oblasti bezpečnosti organizace nebo mají na její fungování bezprostřední vliv, dobré finanční zdroje, atd.

Za nedostatky můžeme v organizace považovat nepříznivé vnitřní podmínky v organizaci, jenž nebezpečně ovlivňují stav bezpečnosti organizace. Nedostatkem může být nedostatečně rozvinutá a definovaná organizační struktura, špatná ekonomická a finanční situace, absence kvalifikovaných pracovníků v oblasti zabezpečení nebo jejich významný nedostatek, nekvalitní nebo vůbec žádná zabezpečovací technika atd.

Příležitostmi jsou vnější podmínky, které příznivě ovlivňují organizaci v jejím postavení na trhu jak v současnosti, tak i v budoucnu. Jestliže tyto příležitosti nyní nebo v budoucnu mohou nepříznivě zasahovat a ovlivňovat organizaci i stav jejího bezpečnostního systému, jsou při využití této metody pro nás použitelné a hodné zřetele. Budou to především příležitosti, které v prvé řadě ovlivňují příznivě organizaci jako celek a teprve zprostředkovaně i její bezpečnostní systém. Mezi příležitosti s ohledem na zabezpečení organizace je možné zahrnout i dlouhodobé snížení cen bezpečnostních zařízení a služeb v důsledku příznivého vývoje vnějších ekonomických vztahů apod.

Hrozby představují stávající i budoucí negativní podmínky ve vnějším prostředí, které mají nepříznivý dopad na stav zabezpečení organizace. Mohou to být hrozby, které zasahují nebo mohou zasáhnout organizaci jako celek a jejich negativní dopad na zabezpečení organizace je až druhotný, ale může se jednat i o hrozby, které zasáhnou stav bezpečnostních opatření v organizaci přímo. Obecnou hrozbou s důsledky na chod a existenci celé organizace je např. ztráta jedné nebo více významných zakázek a snížení ekonomických výsledků a pokles finančních zdrojů. Mezi nepříznivé podmínky vnějšího prostředí z hlediska stavu

bezpečnosti organizace může být počítán i kvalitativní a kvantitativní nárůst bezpečnostních opatření u konkurence a možnost zaostávání za ní.

Je zřejmé, že mezi přednostmi, nedostatky, příležitostmi a hrozbami můžeme nalézt podmínky, které ovlivňují stav a úroveň zabezpečení v organizaci buď bezprostředně, nebo zprostředkovaně. Některé podmínky vytvářejí tlak na rychlou a zásadní změnu bezpečnostních opatření v organizaci, jiné mají účinnost spíše výhledovou a potřebu změn signalizují do budoucnosti.

SWOT analýza se skládá ze čtyř částí, které jsou zaznamenané na obrázku níže. Kvadrant I. představuje oblast uplatňující soulad externích příležitostí a interních předností, II. kvadrant ukazuje, kde nelze využít externí příležitosti z důvodů interních nedostatků, III. kvadrant znázorňuje situaci, kdy externí hrozba ohrožuje existenci organizace z důvodu jejích interních nedostatků a poslední IV. kvadrant hovoří o situaci, kdy může být poškozena vnitřní organizační přednost v důsledku vnější hrozby. [3]

Výhodou této analýzy je schopnost hodnocení současného i budoucího stavu, což zjednodušuje a zpřesňuje volbu nejvhodnějších účinných opatření. Přispívá ke zlepšení funkce bezpečnosti organizace v případě správné identifikace a pochopení významu vnitřních nedostatků a vnějších hrozeb odpovědnými pracovníky.

2.1.2. Analýza PEST

Zkoumání v této analýze je zaměřeno do čtyř oblastí, které jsou taktéž odvozeny z názvu samotné analýzy, tedy jde o politiku, ekonomiku, sociální oblast a technologii. Analýza událostí a trendů v těchto oblastech přináší vedení organizace informace o okolním prostředí v širším záběru včetně pravděpodobných budoucích trendů a při aplikaci na bezpečnost organizace musíme zúžit zkoumání pouze na ty události, které mají nebo mohou mít význam pro systém zabezpečení organizace. Analýza PEST svým zaměřením na faktory, které v budoucnu mohou ovlivnit postavení organizace, umožňuje vedení organizace připravit se na budoucí události a změny včas a tak eliminovat negativní dopady budoucích hrozeb. [3]

V oblasti politiky nás zejména zajímá , zda v důsledku mezinárodních smluv a dohod nedojde ke změnám vnitřních právních předpisů a norem, které upravují oblast bezpečnosti organizací. Zabýváme se především obsahem a vývojem diskuse o připravovaném zákonu o soukromých bezpečnostních službách a zda v oblasti pojišťovnictví jednotlivé pojišťovny připravují změny požadavků na zabezpečení organizace při uzavírání příslušných pojistek a jejich podmínky obecně.

Oblast ekonomiky nelze při této analýze pominout, neboť organizace jsou subjekty ekonomiky, působí na hospodářském trhu a mírou jejich úspěšnosti je jimi dosažená úroveň ekonomických výsledků. Vše, co může potenciálně negativně ovlivnit jejich hospodářské postavení, dříve či později ovlivní i jejich systém zabezpečení. Zabýváme se však i událostmi a trendy neovlivňující bezprostředně hospodářské postavení organizace samotné, ale mohou se problematiky zabezpečení dotknout nepřímo.

Sociální oblast je charakterizována dominantním lidským prvkem. Události a trendy v této oblasti mohou mít velmi významný vliv na organizaci jako celek i na jednotlivé oblasti její činnosti včetně systému jejího zabezpečení. Negativní pohyby v sociální oblasti jsou provázeny i negativními pohyby v oblasti obecné kriminality. Ne vždy ovšem negativní vývoj v sociální oblasti musí znamenat pro organizaci a její systém zabezpečení negativní přínos. Změny právních předpisů v sociální (ale i jiné) oblasti mohou být na první pohled méně významné, avšak ve svých důsledcích mohou organizaci zasáhnout velmi silně.

V technologické oblasti dochází k událostem a trendům, které mohou ovlivnit bezpečnostní systém organizace zásadním způsobem, a to především vznikem a vývojem nových technologií v oblasti zabezpečovací techniky. V oblasti výpočetní techniky má vznik a vývoj nového hardwaru a softwaru zásadní význam pro bezpečnost provozu počítačů a počítačových sítí v organizaci, ale i pro získávání a analýzu potřebných informací z různých oborů. Zde je důležité uvést, že sebelepší a dokonalejší technika zastarává morálně i fyzicky, což nutí organizace k zaměření se na nejnovější produkty hardwaru a softwaru z důvodu zajištění bezpečnosti informací v informačních systémech.

2.1.3. Paretova analýza

Paretova analýza je nejznámější kvantitativní technikou, kterou management používá při analyzování příčin. Jde o nepříliš komplikovanou, ale také ne naprosto přesnou techniku, která se nedá použít na všechny problémy současně, ale jednotlivé problémy se musí analyzovat odděleně. Hlavní přínos je v ukázání směru kam zaměřit svou pozornost.

Princip této metody je založen na poznatku W. Pareta, který postřehl, že 80% majetku bylo vlastněno pouze 20% obyvatelstva, později se zjistilo, že toto pravidlo je platné i v jiných oblastech života – v ekonomické sféře lze toto pravidlo vyjádřit slovy, že 20% úsilí produkuje 80% efektu. Pro analýzu příčin pak platí, že za 80% následků stojí 20% příčin.

Abychom mohli sestrojit tzv. Paretův diagram je nutné sebrané údaje kvantifikovat a seřadit v sestupném pořadí podle určitých kritérií, která si stanovíme (může jít o četnost výskytu, velikost rozsahu následné škody, apod.). Na svislou osu grafu vyneseme např. kumulativní relativní četnost příčin a na vodorovnou osu jejich kumulativní podíl na celkovém množství důsledků – vše v procentech. [3]

2.1.4. Modifikovaná analýza stupně ohrožení

Jde o metodu používanou v oblasti krizového managementu. Cílem analýzy stupně ohrožení je zjistit, jaká je pravděpodobnost, že nastane určitá krize nebo konflikt a jaké budou její účinky (následky), když skutečně nastane. Úspěšnost použití této metody závisí na přesném určení pracovních kroků. Prvním krokem je možné krize popsat a pojmenovat. Druhým krokem je správně vymezit posuzované období, protože s přibývající délkou posuzovaného období se zvyšuje pravděpodobnost, že krize nastane. Nejtěžším krokem je třetí krok, který představuje stanovení stupně pravděpodobnosti. Maximální pravděpodobnost je vyjádřena hodnotou 1,0 = jistota, že krize nastane v předpovězeném období. Čtvrtým krokem je stanovit účinky krize, protože mohou zasáhnout mnoho dalších oblastí činnosti organizace (bude nás zajímat především oblast zabezpečení organizace). Posledním pátým krokem je zapsání hodnocení do připraveného formuláře a přenesení do matice, která představuje graficky ohraničenou plochu v podobě obdélníku rozděleného podélně a svisle na celkem devět polí. [3]

Po umístění jednotlivých ohnisek krize do krizové matice, musíme provést také jejich hodnocení. Matice nám přehledně zobrazuje celkové ohrožení organizace. Podle umístění jednotlivých krizí v matici můžeme usoudit, jak závažné krize hrozí organizaci a jaká by měla být zvolena strategie, aby se organizace s krizí vyrovnala. Čím více ohnisek krize je v pravém horním obdélníku, tím větší problémy bude muset organizace řešit.

Metoda analýzy stupně ohrožení je použitelná jak při zpracování komplexní bezpečnostní analýzy organizace, tak i při zpracování dílčí bezpečnostní analýzy dílčího bezpečnostního problému. Je možné zabývat se dopadem a účinky jednotlivých krizí na celou organizaci nebo jen na bezpečnostní systém organizace či jen jeho část. Řešení krizových situací je nezbytným předpokladem pro bezkonfliktní rozvoj organizace i v budoucnu. V určitých případech je krizové plánování a příprava na řešení budoucích krizí či mimořádných situací povinností, kterou organizaci ukládá přímo zákon.

2.1.5. Iškavův diagram 17

Iškavův diagram je též známý pod názvem diagram příčin a důsledků nebo také rybí kost. Tento diagram nám umožňuje velmi jednoduše znázornit konkrétní analyzovaný problém z hlediska jeho příčin. Jednoduchost spočívá pouze v jeho grafickém vyjádření a v žádném případě ne v jeho správném sestavení. Přesný formát závisí především na specifice konkrétního řešeného problému. To nám určí i počet hlavních a vedlejších větví. Diagram by měl znázornit všechny příčiny, které se k danému problému vztahují. [3]

Základní kategorie příčin lze rozdělit do pěti kategorií: lidská pracovní síla, stroje,metody, materiály a měření (nebo informace). Tyto kategorie příčin jsou typické především pro výrobní organizace ve vztahu k problémům spojeným s jakostí výrobků. Pro oblast služeb bývá struktura problémů proměnlivější, avšak jednotlivé problémové oblasti úzce souvisí s problémem, který má být analyzován, a jejich struktura se od něj odvíjí.

Pro oblast komplexní bezpečnosti organizace je důležité určit kategorie příčin, které skutečně s problémem souvisí. Tyto základní kategorie také budou hlavními větvemi diagramu, přičemž je třeba příčiny zkonkretizovat, tzn. vytyčit i vedlejší větve. Ty mohou být vytyčeny takto:

1) kategorie zaměstnanci

- systém výběru zaměstnanců
- úroveň kvalifikace zaměstnanců
- kvalita a úroveň komunikace mezi zaměstnanci – řízení zaměstnanců – sociální program a tvorba motivace

2) kategorie zabezpečovací technika

- funkčnost
- morální a fyzická opotřebovanost
- kvalifikovanost obsluhy
- úroveň servisu

3) kategorie ostatní fyzické osoby

- kontrola pohybu cizích osob po areálu organizace

4) kategorie dodavatelé technologií a služeb souvisejících s bezpečností organizace

- počet dodavatelů
- bezpečnostní úroveň dodavatelských organizací
- ekonomická stabilita dodavatelských organizací
- míra závislosti na dodavatelích bezpečnostních služeb a techniky
- bezpečnostní prověrka zaměstnanců dodavatele

5) kategorie metody

- úroveň kontrolních mechanismů v oblasti bezpečnosti
- existence zpětné vazby
- existence a kvalita signalizace hrozeb
- řídící úroveň vedoucích pracovníků

6) kategorie informace

- existence informačního systému v organizaci
- úroveň bezpečnosti ochrany informačního systému organizace
- existence kategorizace citlivých informací uvnitř organizace
- existence politiky informační bezpečnosti
- pohyb písemností uvnitř organizace (administrativní bezpečnost)

7) kategorie systémy

- vhodnost použitých systémů zabezpečení
- existence systému řízení jakosti v organizaci

- systém průmyslové bezpečnosti podle zákona o ochraně utajovaných skutečností, příp. analogický systém – systém objektový

8) kategorie vnějšího prostředí

- legislativa
- standardy tuzemské i mezinárodní
- požadavky a tlaky ze strany zákazníků
- tlaky ze strany konkurence

Výhodou Iškavova diagramu je možnost použití nejen pro hledání příčin určitého následku, ale také pro hledání řešení jak dosáhnout žádoucího stavu, to jest pro hledání alternativ. V takovém případě však zobrazujeme diagram stranově otočený tak, že požadovaný stav si napíšeme vlevo a od něj vpravo vytyčíme hlavní a vedlejší větve, kde uvedeme oblasti, ve kterých budeme hledat řešení.

2.2. Bezpečnostní prognóza

Analýza sama o sobě k získání potřebných znalostí o problému nestačí, protože pomocí ní získáme především poznatky o tom, jak se události a jevy udály v minulosti nebo dějí v současnosti a co je jejich příčinou, avšak pro naši bezpečnostní expertízu je nutná i znalost budoucnosti, abychom poznání budoucího vývoje mohli zahrnout do svých znalostí minulosti a přítomnosti. Musíme najít řešení, které bude schopno co nejdéle obstát a odolat všem změnám prostředí. Proces, který nám umožní zvýšit dosud získanou úroveň poznání, je prognózování.

Budoucnost se vyznačuje vysokou mírou neurčitosti a prognózování umožňuje tuto míru neurčitosti snížit. Význam prognózování spočívá v tom, že se soustřeďuje na předvídání budoucího vývoje prostředí a na vznik podmínek, které nastanou v budoucnu a které budou mít vliv na problém, jenž řešíme v současnosti. Prognózování je základem pro plánování a umožňuje nám posoudit námi navržená alternativní řešení v kontextu s budoucími podmínkami. Na výsledky prognózy má vliv řada trendů mezinárodních, politických, makro - ekonomických, konkurenčních a jiných.

Bezpečnostní prognózování je poznávací proces, který se zabývá událostmi a jevy, které mají přímou i nepřímou vazbu na bezpečnost organizace a které udávají nebo výrazně ovlivňují směr nutného dalšího bezpečnostního vývoje organizace ve sledovaném čase. [3]

Jako u každé metody či techniky, která pracuje s určitou mírou pravděpodobnosti, musí být její výsledek v průběhu období, na který byla vypracována, postupně porovnáván se skutečným vývojem. Z tohoto důvodu musí mít organizace k dispozici účinný monitorovací systém umožňující sledování skutečného průběhu realizace rozhodnutí. Porovnáním realizace plánovaného průběhu se skutečným bývají zpravidla odhaleny různě významné odchylky. Po analýze příčin těchto odchylek lze tyto informace použít pro korekci původní prognózy.

Protože v oblasti zabezpečení organizace pracujeme většinou s informacemi, jevy a událostmi, které lze jen částečně kvantifikovat, budou naše závěry vycházet spíše z metod kvalitativních (odhadových). Mezi ně patří osobní hodnocení, panelová shoda a metoda Delphi.

Osobní hodnocení je pravděpodobně nejčastěji používanou metodou. Podstata metody spočívá v subjektivním předvídání budoucnosti jednotlivcem (často vedoucím pracovníkem organizace). Její spolehlivost a přesnost je velmi sporná, v mnohém záleží na odbornosti a zkušenosti jednotlivce, který předpovídání provádí, lze ji používat tam, kde nejsou k dispozici statistická data nebo je jasné, že statistické údaje nemohou dát dostatečnou odpověď. Používá se především pro krátkodobé předpovědi spíše provozního charakteru.

Panelová shoda částečně omezuje vliv osobních postojů a myšlenkových stereotypů prognózujícího jednotlivce tím, že subjektem, který předpovídání provádí, není jednotlivec, ale kolektiv jednotlivců s určitou odbornou úrovní a znalostí bezpečnostní problematiky a oblastí komerční bezpečnosti zvlášť. Vzájemným sdílením svých postojů a názorů se účastníci snaží dospět ke shodě, která reprezentuje předpokládaný vývoj. Velmi důležitý je způsob dosahování vzájemné shody a usměrňování celého procesu skupinového myšlení. Metoda Delphi využívá taktéž úsudku kolektivu odborníků, činí tak však odděleně aniž by znali ostatní členy kolektivu. Své hodnocení vyplňuje každý odborník samostatně do připraveného dotazníku, které jsou nakonec vybrány, sumarizovány a vráceny zpět expertům,

kteří mají možnost původní stanovisko revidovat s ohledem na názor ostatních členů týmu. Takto se postupuje do dosažení obecné shody nebo dokud není proveden příslušný počet předem dohodnutých kol hodnocení. Nevýhodou této metody je časová a organizační náročnost, výhodou potom anonymita účastníků.

Metoda klouzavých průměrů patří mezi kvantitativní a lze ji použít i při bezpečnostním prognózování. Používá se především pokud potřebujeme zjistit dosavadní vývoj určité veličiny důležité pro posouzení úrovně bezpečnosti organizace a na základě dosavadního vývoje predikovali její budoucí vývoj. Výsledkem je grafické znázornění, kde na svislé ose nalezneme údaje o počtu krádeží a na osu vodorovnou vyneseme jednotlivé dny (týdny, měsíce, čtvrtletí), kdy ke krádežím došlo. Pokud sledujeme pouze krátké období, je prognóza vývoje v podstatě aritmetickým průměrem hodnot z předchozích 2-3 týdnů. Ve chvíli, kdy pro předpověď použijeme více předchozích týdnů, nejsme schopni vzít v úvahu např. výrazné změny, ke kterým došlo v nejbližších předchozích týdnech. Proto se zde nepoužívá aritmetický průměr ze všech předchozích období, ale tzv. klouzavý průměr, což je průměr z předem stanoveného počtu posledních týdnů. Tento způsob předpovědi je použitelný spíše pro krátkodobé předpovědi.

Metoda exponenciálního vyrovnání upřesňuje metodu klouzavých průměrů v tom smyslu, že odlišuje význam jednotlivých údajů podle toho, zda se jedná o údaje novější či starší. Metoda exponenciálního vyrovnání stanoví vyšší hodnotu pro údaje aktuálnější než pro ty starší. V principu jde o výpočet váženého klouzavého průměru skutečných hodnot, kde aktuálnější hodnoty mají větší váhu než ostatní. Před management však tato metoda staví otázku jak velké by měly být jednotlivé váhy.

Prognostické modely, které respektují určité trendy nebo sezónní výkyvy, jsou důležitou oblastí. Modely časových řad pracují s třemi základními složkami – trendovou, sezónní a náhodnou. Trend představuje rozhodující tendenci dlouhodobého vývoje analyzované proměnné veličiny. Není rozhodující, zda je stoupající či klesající nebo má stabilní průběh. Ukazuje, jak se sledovaná veličina bude dlouhodobě vyvíjet. Sezónní složka znázorňuje pravidelné kolísání sledovaného ukazatele okolo trendu v průběhu sledovaného období. Pro sezónní složku je charakteristické, že se v souměřitelných časových obdobích pravidelně opakuje. Náhodná složka trendu zapříčiňuje nepředvídatelné rozkolísání skutečných

hodnot kolem hodnot předpokládaných. Takové výkyvy mohou být způsobeny i drobnými příčinami, které se však v praxi těžko odhadují. Rozhodující je, že nepředvídatelné příčiny náhodné složky trendu nelze předem stanovit, a proto na vlastní stanovení předpovědi – prognózy- nemají vliv. Cílem analýz časových řad je vyjádřit jejich trendové a sezónní složky v kvantifikované podobě (proces kvantifikace těchto složek se také nazývá dekompozicí časových řad). Tímto postupem můžeme stanovit trend vývoje v určité oblasti a předpokládané sezónní výkyvy, což nám může pomoci např. při plánování počtu bezpečnostních pracovníků v jednotlivých obdobích nebo podle dosaženého výsledku určit intenzitu nasazení bezpečnostní techniky. [3]

Samotný prognostický proces lze rozčlenit do jednotlivých kroků:

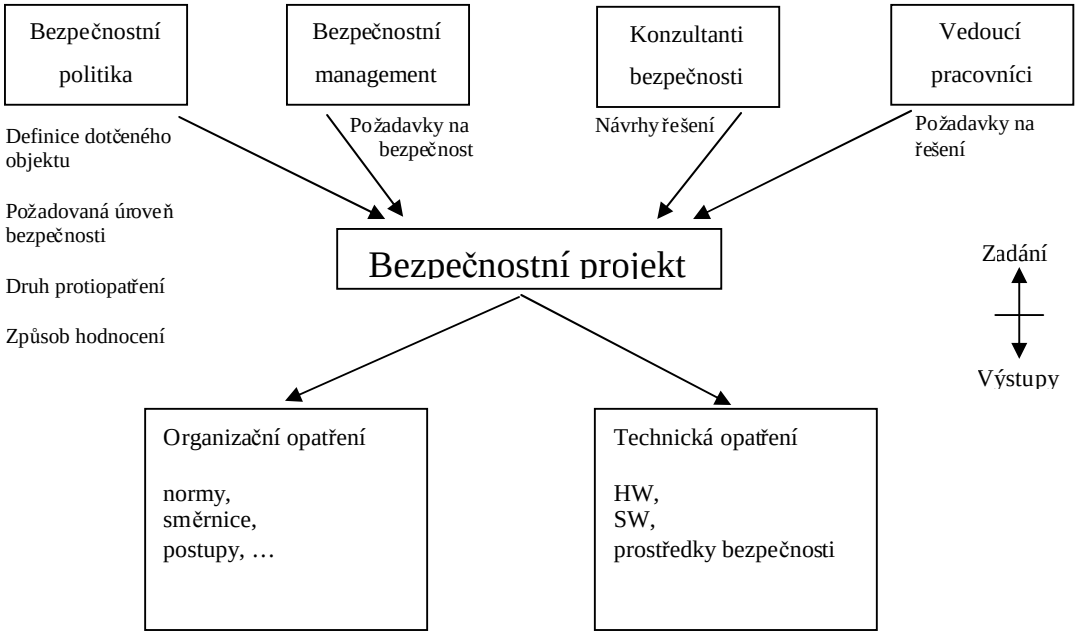
- stanovení účelu (cíle), kterého má být prognózou dosaženo
- stanovení délky prognózování období a četnosti opakování prognóz
- vybrání vhodné prognostické metody nebo metod
- provedení sběru dat potřebných ke zpracování prognózy
- vyhotovení vlastní prognózy
- další sledování prognózy a vyhodnocování její přesnosti
- zpětné zohlednění nových dat získaných vyhodnocením a upřesněním v původní prognóze a následné upřesnění prognózy

Jedním z dalších možných kroků prognostického procesu je i určení spolehlivosti a vhodnosti prognózy. Pokud jde o zpětné zohlednění nově získaných dat, nemusíme nutně už dále prognózu zpřesňovat. Nicméně vyhodnocování přesnosti a sledování prognózy musí být neoddělitelnou součástí prognostického procesu, jinak by nemělo smysl prognózu vyhodnocovat.

2.3. Bezpečnostní plánování (projektování)

Veškeré dosavadní postupy a metody směřují k dokončení rozhodovacího procesu v oblasti komplexní bezpečnostní expertízy, to jest k sestavení komplexního bezpečnostního plánu organizace a jeho podrobného rozpracování do podoby bezpečnostního projektu. Rozsah a

složitost přípravy a sestavení plánu (projektu) je přímo závislá na velikosti a složitosti plánovaného cíle.



Obrázek 4. Bezpečnostní projekty

Plán (projekt) charakterizuje jeden významný znak, jímž je dosažení určeného cíle, čímž končí. Bezpečnostní projekty se obdobně jako ostatní druhy projektů vyznačují některými charakteristickými rysy; jde především o:

- projekty mají přesně a srozumitelně definované cíle
- projekty obsahují jednoznačné termíny k jejich dokončení
- obsahují množinu činností propojenou vzájemnými vazbami
- pro jejich realizaci jsou vyčleněny zdroje
- obsahují seznamy pracovníků odpovědných za realizování projektu
- realizují je zpravidla projektové týmy, protože jejich splnění nelze zajistit jediným člověkem

Naprosto nezbytnou podmínkou každého plánu je stanovení si otázky definování cíle a to jasně a srozumitelně. Musí být také měřitelný, tzn. že jej lze kvantifikovat, nebo musí být možné jen dva stavy - ano/ne (= cíl splněn/cíl nesplněn). Formy a způsoby řešení nedostatků získané z analýzy a syntézy se promítnou do existence více navrhovaných variant řešení. Vybraná řešení pak slouží jako odrazový můstek pro konečné přesné a srozumitelné zfor-

mulování plánovaného cíle plánu. Kromě bezpečnostní analýzy má pak na konečnou formulaci cíle projektu významný vliv i bezpečnostní prognózování a bezpečnostní politika organizace. Jedním z limitujících faktorů plánu je termín dokončení projektu. Vymezuje časový prostor, ve kterém bude muset být provedena řada kroků nutných k dosažení plánovaného cíle. Pro určení celkového termínu splnění plánu je velmi důležité, v jakých termínech je možné realizovat jednotlivé dílčí kroky, které musí být nezbytně provedeny, aby plánovaného cíle bylo dosaženo.

Také projektování má vypracovány své techniky, které lze aplikovat i na bezpečnostní projektování. Jedná se o techniky, které pomáhají v organizaci projektu a při jeho realizaci:

- Ganttův diagram
- síťový diagram a jeho modifikace diagram PERT
- metoda kritické cesty

Gattův diagram je velmi jednoduchou a účinnou metodou. Zobrazuje souhrn jednotlivých činností (úkolů), dobu potřebnou k jejich provedení a vzájemné časové vazby mezi mini. Každý úkol je v tomto diagramu vyznačen jako vodorovný proužek , jednotlivé úkoly jsou zobrazeny pod sebou a mezi nimi jsou vytvořeny grafickým způsobem vazby. Veškeré úkoly v podobě proužků jsou umístěny pod vodorovnou časovou stupnicí, z níž lze snadno odečíst dobu začátku a konec konkrétního úkolu. Uvedený diagram je vhodnější používat na zobrazení délky trvání jednotlivých činností a celého projektu než na vyjádření vzájemných vazeb. Je výborným kontrolním nástrojem na zjištění stavu jednotlivých úkolů v čase.

Síťový graf obsahuje veškeré potřebné informace pro řízení realizace projektu. Charakteristickými prvky síťového grafu jsou uzly a jejich spojnice. Každý uzel reprezentuje časový bod – zahájení nebo skončení činnosti. Vlastní činnost je potom vyjádřena úsečkou – spojnicí, která oba uzly spojuje. Při kreslení síťového grafu se dodržují tato pravidla:

- síťový graf musí mít jeden počáteční a jeden koncový uzel
- každému uzlu, s výjimkou výchozího, musí předcházet nejméně jedna činnost
- po každém uzlu, s výjimkou koncového, musí následovat nejméně jedna činnost
- kterékoli dva uzly smí spojovat pouze jedna činnost

Současně je nutné dodržovat ještě jisté konvence platné pro zobrazování (např. počáteční a koncový bod se označují kosočtverci). Síťový graf je pro řízení projektu využitelný tehdy, pokud obsahuje kromě úplného výpočtu činností - úkolů i časové informace – nejdříve možná ukončení všech činností, nejpozději nutná ukončení všech činností a identifikovanou kritickou cestu síťového grafu.

PERT diagram je variantou síťového grafu, ale na rozdíl od něj nemusí zobrazovat vazby sumárních úkolů na podúkoly.

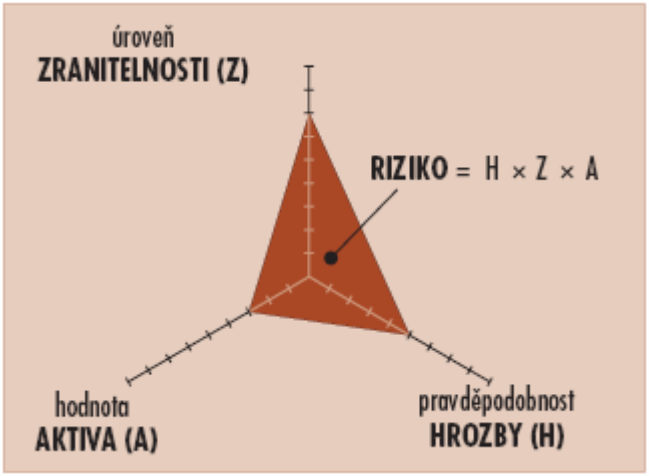
Kritický úkol je takový, jenž je kritický z hlediska dokončení celého projektu, tedy takový, který může ohrozit splnění celého projektu v plánovaném termínu. Z hlediska doby provádění jsou nekritické úkoly ty, které mají určitou časovou rezervu a úkoly kritické jsou ty, které nemají žádnou časovou rezervu. Kritická cesta začíná u počátečního uzlu a končí u uzlu konečného. Metoda kritické cesty je standardem při správě projektu pro zjištění kritických úkolů. Jejím základem je matematický model, jenž zohledňuje vztahy mezi úkoly, dobu jejich trvání a veškerá omezení týkající se dostupnosti jejich zdrojů. Tato metoda se používá především pro stanovení počátečního a konečného data jednotlivých úkolů. [3]

2.4. Analýza rizik

Analýza rizik je proces, který identifikuje a klasifikuje informační aktiva společnosti, odhaluje hrozby, stanovuje rizika a navrhuje bezpečnostní opatření. Aktiva jsou zejména informace a data zpracovávaná firmou.

Analýza rizik zpravidla zahrnuje následující kroky:

- identifikace aktiv a požadavků na jejich ochranu – klasifikace informací
- stanovení míry rizika vztahující se k jednotlivým aktivům
- návrh bezpečnostních opatření ke snížení rizika na akceptovatelnou úroveň



Obrázek 5. Vymezení oblasti rizika

Výsledky analýzy rizik obsahují:

- přehled identifikovaných aktiv, jejich klasifikace a určení odpovědnosti
- přehled nalezených rizik a slabých míst z hlediska bezpečnosti, konkrétní rizika jsou doplněna o přehled hrozeb včetně posouzení jejich závažnosti a ohodnocení jejich vazby na konkrétní aktiva
- návrh konkrétních bezpečnostních opatření včetně stanovení jejich priorit
- manažerský souhrn výsledků analýzy rizik

2.4.1. Vztahy v analýze rizik

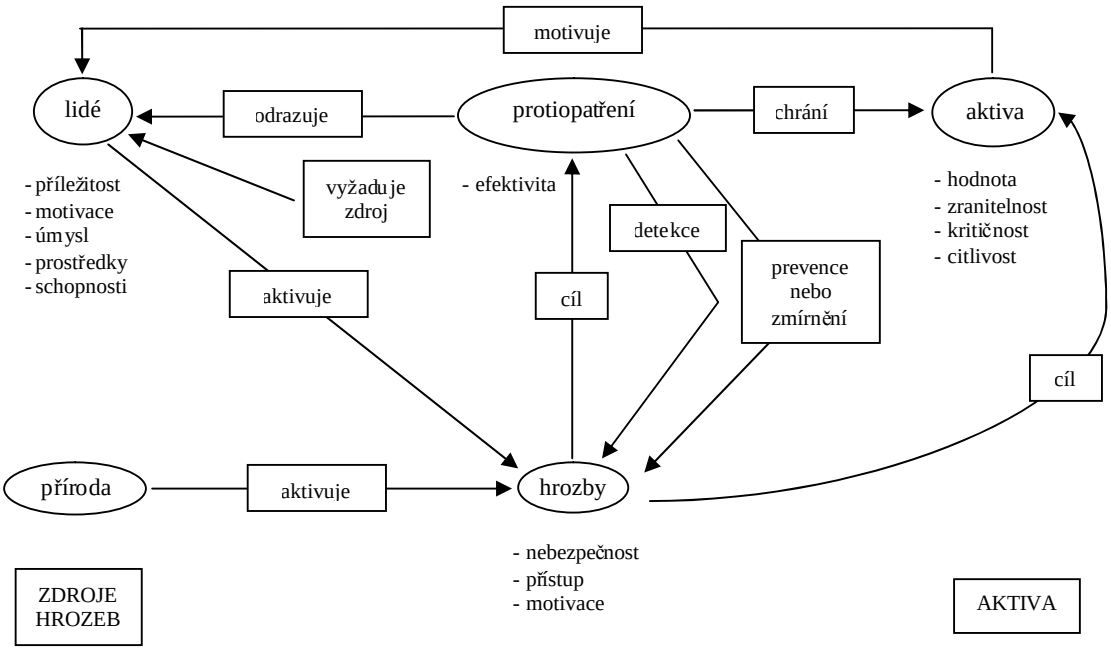
Správné pochopení vztahů v analýze rizik je pro úspěšné provedení analýzy klíčové. Základní vztahy a souvislosti v analýze rizik jsou znázorněny na obrázku níže.

Mechanizmus uplatnění rizika probíhá následujícím způsobem:

- hrozba využije zranitelnosti, překoná protiopatření a působí na aktivum, kde způsobí škodu
- aktivum svou hodnotou motivuje útočníka k aktivaci hrozby, vůči působení hrozby se aktivum vyznačuje určitou zranitelností a zároveň je chráněno proti - opatřeními před hrozbami
- protiopatření chrání aktiva, detekuje hrozby a zmírňuje nebo zcela zabraňuje jejich působení na aktiva, protiopatření zároveň odrazují od aktivování hrozeb

- hrozba působí jednak přímo na aktivum nebo na protiopatření, s cílem získat přístup k aktivu. Aby mohla hrozba působit, musí být aktivována; pro svou aktivaci vyžaduje zdroje (tedy vytvoření podmínek pro její působení)

Vztahy mezi jednotlivými prvky v procesu analýzy a řízení rizik lze popsat různými modely, například podle obrázku níže.



Obrázek 6. Vztahy v analýze rizik

2.4.2. Metoda CRAMM

Pro analýzu rizik bývá většinou použita britská metoda CRAMM (CCTA RISC Analysis and Management Method), která je uváděna i v doporučení evropské normy ITSEM.

CRAMM je formalizovaná a strukturovaná metoda analýzy a optimalizované eliminace bezpečnostních rizik, která byla původně vyvinutá pro implementaci a začlenění všech obranných opatření zabezpečujících IS , obsahující cenná nebo jinak citlivá data. Hlavním cílem je poskytnutí úplné množiny protiopatření zabezpečujících IS jak již existující, tak vyvíjené na úrovni, jež může být dle možností a přání postupně dále zvyšována. CRAMM definuje IS jako soubor provázaných aktiv následujících typů (jednotlivá aktiva jsou přitom provázána řetězcem závislostí):

- fyzická aktiva (hardware tvořící počítače a komunikační software)

- programová aktiva obsahující aplikační programové vybavení
- datová aktiva zahrnující aplikační data

Metoda CRAMM má tři stupně:

1) jsou zajištěna systémová aktiva – data, aplikační programy a technické vybavení, jež jsou ohodnocena. Ohodnocení (prostřednictvím kvalifikované debaty s odpovědnými osobami, jenž vyjádří ztrátu těchto dat) datových aktiv probíhá podle předdefinovaných stupnic reprezentující vliv na činnost software ztrátou, zničením nebo neoprávněným zveřejněním dat. Ostatní aktiva jsou ohodnocena podle ceny
2) jsou vyšetřovány míry hrozeb a zranitelnosti útočících na jednotlivá aktiva. Formou interview jsou zjišťovány odpovědi na dotazy týkající se hrozeb a zranitelnosti. Výsledkem je potom stanovení míry hrozeb a zranitelnosti ve škále malá, střední a velká. Závěrem je zjištěna míra rizika pro jednotlivé kombinace aktiv s přiřazenou hrozbou. Velikost míry rizika závisí na hodnotě aktiva, na míře hrozby a zranitelnosti. Toto číslo jasně vypovídá o potřebné míře ochrany
3) pro vybraná ohrožení jsou stanovena bezpečnostní opatření, která jsou adekvátní bezpečnostním požadavkům. Bezpečnostní protiopatření zahrnují následující aspekty bezpečnosti IS:
    - technická protiopatření – tvořící funkce a mechanizmy prosazující bezpečnost
    - netechnická protiopatření – fyzická, personální a procedurální

Výsledky analýzy rizik jsou objektivním podkladovým materiálem pro rozhodování o dalším postupu v rámci procesu řízení rizik.

2.4.3. Řízení rizik

Problematika řízení rizik (risk management) je velice široká a podle svého zaměření často velice odlišná. Základními oblastmi, v nichž hovoříme o řízení rizik, jsou především:

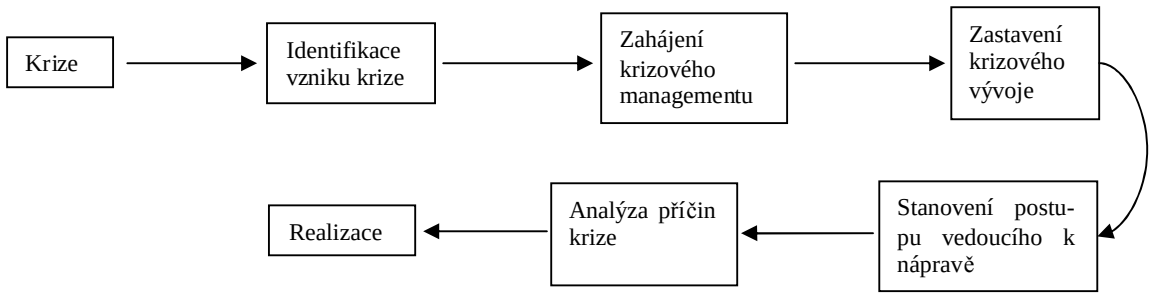
- přírodní katastrofy a havárie (technologická rizika)
- rizika ochrany životního prostředí
- finanční rizika

    - investiční riziko (odhad spolehlivosti a ziskovosti investic)
    - pojišťovací a zajišťovací riziko (odhad rizika, že dojde k pojistné události)
- projektová rizika
- obchodní rizika
    - marketingové riziko (vytvoření produktu, který nikdo nechce nebo o němž obchodní zástupci neví jakým způsobem jej prodat)
    - strategické riziko (vytvoření produktu, který už nezapadá do obchodní strategie podniku)
    - riziko managementu (ztráta podpory projektu ze strany vedení, vlivem změny zaměření nebo změny osob)
    - rozpočtové riziko (nedodržení rozpočtu, nedosažení zisku)
- technická rizika (riziko u všech typů inženýrských konstrukcí včetně materiálů a staveb)
- organizační rizika (vyplývající z neprovedených nebo špatně provedených změn v organizaci)

Existují i obecné zákonitosti řízení rizik, které je třeba znát, ať již chceme minimalizovat riziko při změnách v podniku nebo v oblasti přírodních katastrof.

Řízení rizik je proces, při němž se subjekt řízení snaží zamezit působení již existujících i budoucích rizik a navrhuje řešení, která pomáhají eliminovat účinek nežádoucích vlivů a naopak umožňují využít příležitosti působení pozitivních vlivů. Součástí procesu řízení rizik je rozhodovací proces, vycházející z analýzy rizik. Po zvážení dalších faktorů, zejména ekonomických, technických, ale i sociálních a politických, management pro řízení rizik vyvíjí, analyzuje a srovnává možnosti preventivní a regulační opatření. Posléze z nich vybere ta, která existující riziko minimalizují. Jako součást řízení rizika bývá chápáno i šíření informací o riziku (risk communication) a vnímání rizika (risk perception). Kritickou fází řízení rizik je výběr optimálního řešení. Začíná určením úrovně rizika, postupuje přes hodnocení ekonomických nákladů variantních řešení pro snížení rizika a jejich ekonomických přínosů (cost-benefit analysis). Pokračuje zhodnocením dopadů a přínosů a analýzou možných důsledků z přijatého rozhodnutí na subjekt a jeho okolí. Posléze následuje rozhodnutí o realizaci opatření na snížení rizika, respektive rozhodnutí o jeho dalším sledování

v případě vysokého stupně nejistot, spojených se stávajícím stupněm poznání a tím nemožnosti snížit riziko ve fázi tvorby rozhodnutí.



Obrázek 7. Schéma krizového řízení v užším smyslu

Management řízení rizik využívá principu zpětné vazby (reakční strategie – klasický způsob, kdy se jedná o napodobení učícího se systému) nebo predikční vazby (proaktivní strategie – způsob, kdy je subjekt seznámen se současným stavem, možnými hrozbami a má co nejúplnější informace o možném průběhu jejich naplnění). Protože však většinou není reálné mít k dispozici takto komplexní informace a zejména pak není reálné odhadnout předem vliv a hlavně význam jednotlivých faktorů, které na subjekt působí, existuje zde možnost rozhodování za neúplné informace (fuzzy), což lze částečně eliminovat pomocí nástrojů pro podporu rozhodování při neúplných (mlhavých) informacích.

Finálním výsledkem každé etapy řízení rizik je rozhodnutí. Většinou je výstupem více variant řešení. Nepřijatelná úroveň rizika vyžaduje zastavení probíhajícího procesu a přijetí opatření na snížení rizika. Je-li riziko přijatelné a přitom nikoliv bezvýznamné a potenciál zisku je značný, následuje obvykle vypracování plánu preventivních opatření za účelem jeho redukce. Pro zbytková rizika, která nelze protiopatřeními efektivně snížit, se zpracovávají krizové plány. Velký důraz je třeba klást na maximální využití fáze redukce rizika a jeho eliminace tak, aby se havarijní plány a scénáře vypracovávaly opravdu jen pro zbylá rizika. Hledáním obecně platných preventivních opatření pro významné snížení pravděpodobnosti vzniku krizí a omezení jejich případných následků se také zabývá nouzové, respektive krizové plánování jako základní součást krizového řízení.

Vytvoření rizikových plánů představuje:

- rozpoznání aktivačních procedur pro jednotlivá rizika – aktivační procedury jsou indikátory toho, že došlo nebo může dojít k riziku, takže nejlepší aktivační proce-

dury s předstihem upozorní na blížící se problém; pro jednotlivá rizika vytvoříme seznam sledovaných položek, který by obsahoval možné aktivační procedury, spolu s údaji o tom, kdy pravděpodobně nastanou a kdo by měl danou aktivační proceduru sledovat

- stanovení aktivních, rezervních či zmírňujících plánů pro jednotlivá rizika - rizikové plány lze vytvářet jedním ze tří základních způsobů:
    - zmírnit riziko předem provedenými akcemi, to jest snížením pravděpodobnosti, že k problému dojde
    - zmírnit riziko snížením následků po objevení problému, tedy snížením dopadu rizika
    - reagovat na riziko rezervním plánem v případě, že k problému dojde

Sledování a řízení rizik znamená, že sledujeme seznam určených položek, abychom zjistili, zda se neobjevují aktivační procedury, v případě potřeby použijeme rezervní plány a pravidelně znova vyhodnocujeme rizika. Pokaždé, když se skutečný průběh projektu významně odchýlí od plánu, znovu stanovíme rizika a přehodnotíme plán na řízení rizika. [10]

3. NORMY, ZÁKONY, SYSTÉMY JAKOSTI

V této kapitole se pokusím uvést stručný přehled základních norem, zákonů a systémů jakosti vztahujících se k činnosti podniku, bezpečnostní politice firmy a jejímu navrhování.

Je velmi pravděpodobné, že uvedené zákony, vyhlášky atd. jsou již v tuto chvíli pozměněny či zrušeny novými. Z toho důvodu je u většiny napsána poznámka „ve znění pozdějších předpisů“, abych předešla případným kolizím s aktuálními zákony a jejich zněním. Totéž platí i pro všechny další podkapitoly.

3.1. Normy a systémy jakosti

Norma ISO 14 001	Zavádění environmentálního systému řízení – ochrana životního prostředí
Normativní dokument OHSAS 18 001	BOZP
Norma ISO/TS 16 949	Systém managementu jakosti
Norma ISO/IEC 17 799:2000	IT – systém řízení bezpečnosti informací
Norma BS 7799-2:2000	Systém řízení bezpečnosti informací - specifikace, instrukce k použití ISO/IEC 17 799:2000
Norma SA 8000	Společenská (sociální) odpovědnost organizace
Norma ISO/IEC 17 024:2003	Posuzování shody – všeobecné požadavky na orgány pro certifikaci osob
Norma BS – OHSAS 18 001:1999	Systémy managementu bezpečnosti a BOZP – specifikace
Norma ČSN EN ISO 9000:2006	Systémy managementu jakosti
Norma ČSN EN ISO 9001:2001	Systémy managementu jakosti – požadavky
Norma ČSN EN ISO 9004:2001	Systémy managementu jakosti – směrnice pro zlepšování výkonnosti
Norma ČSN ISO 10 002:2005	Management jakosti – spokojenost zákazníka
Norma ČSN ISO /TR 10 014:1999	Směrnice pro management ekonomiky jakosti

Norma ČSN ISP/TR 10 013:2002	Směrnice pro dokumentaci systému managementu jakosti
Norma ČSN EN ISO 14 001:2005	Systém environmentálního managementu - požadavky
Norma ČSN EN ISO 14 004:2005	Systém environmentálního managementu - metodická pomůcka pro zavádění EMS do praxe
Norma ČSN EN ISO 19 011:2003	Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu
Norma BSI – OHSAS 18 002:2000	Směrnice pro zavádění OHSAS 18 001
Norma ČSN ISO/IEC 15 408	Informační metody – kritéria pro hodnocení bezpečnosti IT
Norma ČSN ISO/IEC TR 13 335-1÷5	IT – směrnice pro řízení bezpečnosti IT
Norma ISO 9000	Normy pro řízení a zabezpečování jakosti
Norma ČSN EN 54	Elektrická požární signalizace
Norma ČSN EN 50 130	Poplachové systémy
Norma ČSN EN 50 131	Elektrická zabezpečovací signalizace
Norma ČSN EN 50 132	CCTV
Norma ČSN EN 50 133	Systémy kontroly vstupu
Norma ČSN EN 50 134	Systémy přivolání pomoci
Norma EN 50 135	Systémy tísňové
Norma ČSN EN 50 136	Poplachové přenosové systémy
Norma EN 50 137	Systémy kombinované nebo integrované
Norma ČSN 33 2000 – 1	Bezpečnost elektrických zařízení

3.2. Usnesení vlády

Usnesení vlády č. 458 z 10.5.2000	Národní politika podpory jakosti
Usnesení vlády č. 235 ze 17.3.2004	o Státní politice životního prostředí 2004 – 2010
Usnesení vlády č. 475 z 19.5.2003	Národní politika BOZP

3.3. Zákony

Zákon č. 513/91 Sb. ve znění pozdějších předpisů	Obchodní zákoník
Zákon č. 40/64 Sb. ve znění pozdějších předpisů	Občanský zákoník
Zákon č. 634/98 Sb. ve znění pozdějších předpisů	o Ochraně spotřebitele
Zákon č. 59/98 Sb. ve znění pozdějších předpisů	o Odpovědnosti za škodu způsobenou vadou výrobku
Zákon č. 22/97 Sb. ve znění pozdějších předpisů	o Technických požadavcích na výrobky
Zákon č. 102/01 Sb. ve znění pozdějších předpisů	o Obecné bezpečnosti výrobků
Zákon č. 505/90 Sb. ve znění pozdějších předpisů	o Metrologii
Zákon č. 185/01 Sb. ve znění pozdějších předpisů	o Odpadech
Zákon č. 477/01 Sb. ve znění pozdějších předpisů	o Obalech
Zákon č. 65/65 Sb. ve znění pozdějších předpisů	Zákoník práce
Zákon č.237/2000 Sb.ve znění pozdějších předpisů	o Požární ochraně
Zákon č. 499/04 Sb. ve znění pozdějších předpisů	o Archivnictví a spisové službě
Zákon č.240/2000 Sb.ve znění pozdějších předpisů	o Krizovém řízení
Zákon č. 106/99 Sb. ve znění pozdějších předpisů	o Svobodném přístupu k informacím
Zákon č. 123/98 Sb. ve znění pozdějších předpisů	o Právu na informace o životním prostředí
Zákon č. 318/01 Sb. ve znění pozdějších předpisů	o Poskytování informací a další součinnosti pro účely řízení před Evropským soudem pro lidská práva a před výborem OSN pro lidská práva
Zákon č. 412/05 Sb. ve znění pozdějších předpisů	Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti
Zákon č. 413/05 Sb. ve znění pozdějších předpisů	Změna jiných zákonů v souvislosti se zákonem 412/2005 Sb.
Zákon č.101/2000 Sb.ve znění pozdějších předpisů	o Ochraně osobních údajů
Zákon č. 353/99 Sb. ve znění pozdějších předpisů	Stanovuje povinnost mít k dispozici havarijní plán
Zákon č. 35/65 Sb. ve znění pozdějších předpisů	Autorský zákon
Zákon č. 634/92 Sb. ve znění pozdějších předpisů	o Ochraně spotřebitele

Zákon č. 14/93 Sb. ve znění pozdějších předpisů	o Opatřeních na ochranu průmyslového vlastnictví
Zákon č. 237/91 Sb. ve znění pozdějších předpisů	do Ochraně označení původu výrobků
Zákon č. 174/88 Sb. ve znění 237/91 Sb.	o Ochranných známkách
Zákon č. 21/71 Sb. ve znění pozdějších předpisů	o Jednotné soustavě sociálně ekonomických informací
Zákon č. 563/91 Sb. ve znění pozdějších předpisů	o Účetnictví
Zákon č. 71/61 Sb. ve znění pozdějších předpisů	Správní řád
Zákon č. 128/75 Sb. ve znění pozdějších předpisů	o Sociálním zabezpečením
Zákon č. 1/91 Sb. ve znění pozdějších předpisů	o Zaměstnanosti
Zákon č. 455/91 Sb. ve znění pozdějších předpisů	Živnostenský zákon
Zákon č. 586/92 Sb. ve znění pozdějších předpisů	o Daních z příjmu
Zákon č. 588/92 Sb. ve znění pozdějších předpisů	o Dani z přidané hodnoty
Zákon č. 140/64 Sb. ve znění pozdějších předpisů	Trestní zákon
Zákon č. 513/91 Sb. ve znění pozdějších předpisů	Obchodní zákoník
Zákon č. 40/64 Sb. ve znění pozdějších předpisů	Občanský zákoník
Zákon č. 106/99 Sb. ve znění pozdějších předpisů	o Svobodném přístupu k informacím
Zákon č. 177/01 Sb. ve znění pozdějších předpisů	o Ochraně osobních údajů
Zákon č. 100/99 Sb. ve znění pozdějších předpisů	o Ochraně před povodněmi
Zákon č. 254/99 Sb. ve znění pozdějších předpisů	Technické podmínky požární ochrany a podmínky věcných prostředků požární ochrany
Zákon č. 227/2000 Sb. ve znění pozdějších předpisů	o Elektronickém podpisu

3.4. Vyhlášky

Vyhláška č. 345/02 Sb.	Stanovení měřidel k povinnému ověřování a měřidla podléhající schválení typu
Vyhláška č. 376/01 Sb.	o Hodnocení nebezpečných vlastností odpadů
Vyhláška č. 383/81 Sb.	o Podrobnostech nakládání s odpady
Vyhláška č. 381/01 Sb.	Katalog odpadů

Vyhláška č. 115/02 Sb.	o Podrobnostech nakládání s odpady
Vyhláška č. 432/3 Sb.	Podmínky pro zařazování prací do kategorií, hodnoty biologických testů
Vyhláška MF č. 125/93 Sb.	Odpovědnost zaměstnavatele za škodu při pracovním úrazu nebo nemoci z povolání – podmínky a sazby zákonného pojištění odpovědnosti
Vyhláška NBÚ č.76/1999 Sb.	Zajištění certifikované kryptografické ochrany
Vyhláška č. 315/1998 Sb.	o Zdravotnické způsobilosti seznamovat se z UI
Vyhláška č. 245/1998 Sb.	o Osobní způsobilosti a vzorech tiskopisů používaných v oblasti personální bezpečnosti
Vyhláška č. 338/1999 Sb.	Postup při evidenci, přepravě a ukládání UI
Vyhláška č. 12/1999 Sb.	Technická bezpečnost při režimových opatření k ochraně UI
Vyhláška č. 263/1998 Sb.	Způsob a ověřování bezpečnostní spolehlivosti organizace
Vyhláška č. 56/1999 Sb.	o Zajištění bezpečnosti IS
Vyhláška č. 76/1999 Sb.	o Zajištění kryptografické ochrany

3.5. Nařízení vlády

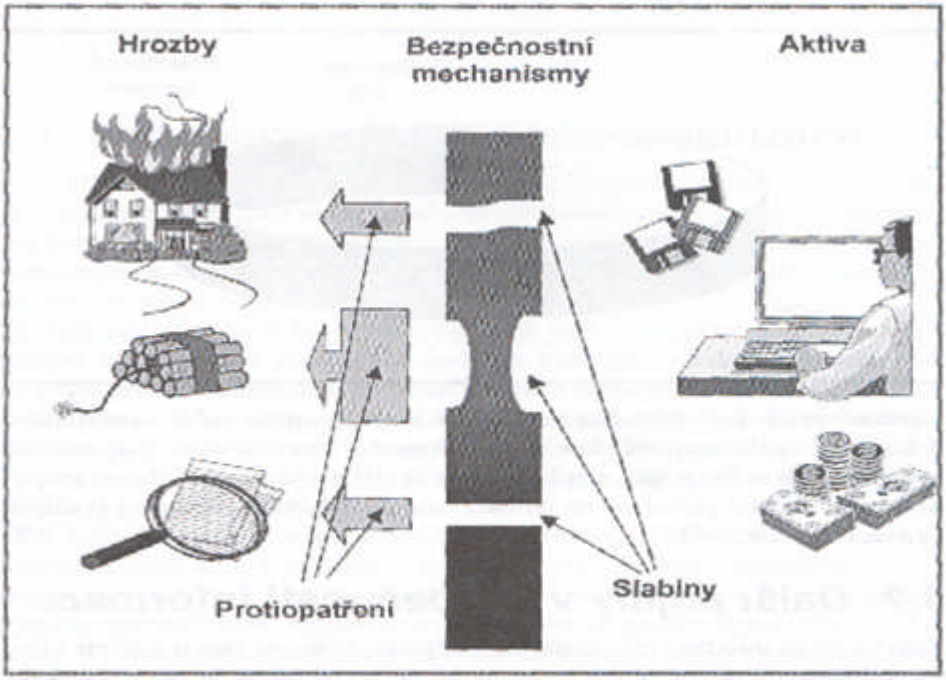
Nařízení vlády č. 184/02 Sb.	Seznam výrobků, na které se vztahuje povinnost zpětného odběru, nakládání s obaly, obalovými materiály a odpady z použitých výrobků a obalů
Nařízení vlády č. 378/01 Sb.	Požadavky na bezpečný provoz a používání strojů, technických zařízení, přístrojů a nářadí
Nařízení vlády č. 101/05 Sb.	O podrobnějších požadavcích na pracoviště a pracovní prostředí
Nařízení vlády č. 178/01 Sb.	Podmínky ochrany zdraví zaměstnanců při práci
Nařízení vlády č. 172/01 Sb.	Prováděcí zákon o požární ochraně
Nařízení vlády č. 168/02 Sb.	Doprava dopravními prostředky zaměstnanci
Nařízení vlády č. 246/98 Sb.	Seznamy utajovaných informací
Nařízení vlády č. 340/02 Sb.	Seznam citlivých činností

3.6. Jiné

Český obranný standard ČOS 051622	Požadavky NATO na ověřování jakosti při návrhu, vývoji, výrobě (AQAP 2110)
Zvláštní předpis č. 339/1999 Sb.	Vyhláška o způsobu zajištění objektové ochrany
Direktiva EU č. 91/250	Ochrana počítačových programů
Směrnice České asociace pojišťoven P2333	Požadavky na zabezpečení objektů
Zvláštní předpis č. 339/1999 Sb.	Vyhláška o způsobu zajištění objektové bezpečnosti

4. OCHRANA ZNALOSTÍ, DAT A INFORMACÍ

Nejprve si ujasníme základní rozdíl mezi daty, informace a znalostmi. Data (tedy údaje) jsou odrazem jevů, procesů a vlastností, které existují a probíhají v části reálného světa, kterého se týkají. Jsou tedy určitou konkrétní interpretací údajů, u nichž jde zejména o formu jejich vyjádření, uložení a zpracování. Mohou být strukturovaná či nestrukturovaná. Informace jsou interpretací dat v určitém kontextu. Zmíněné údaje třeba mohou znamenat velikost a barvu obuvi. Z matematického pohledu jsou informace data snižující entropii příjemce informace. Znalost je schopnost na základě zkušeností nebo aplikací formálních pravidel interpretovat data, dávat je do souvislostí a získávat z nich informace.



Obrázek 8. Bezpečnostní mechanismy

Pokud hovoříme o problematice ochrany znalostí, informací, dat, komunikačních a počítačových systémů, můžeme jinými slovy hovořit o obranném konkurenčním zpravodajství. Všeobecně se v rámci konkurenčního zpravodajství jsou hlavní devízou lidé, kteří se ale řadí k nejvážnějším problémům v rámci vlastního obranného konkurenčního zpravodajství, protože jsou nejčastějším zdrojem úniku informací a dat a jejich neznalost, nedbalost, neopatrnost a mnohdy i záměr ovlivňují spolehlivost počítačových a komunikačních systémů. Lidé jsou proto považováni za nejcitlivější a nejzranitelnější místo, ačkoliv lidský faktor je

stěžejní a primární. Technická a softwarová spolehlivost či nespolehlivost (stupeň spolehlivosti) je pouze výsledem lidské činnosti.

Rozlišujeme dvě možnosti úniku informací:

- nespolehlivost a selhání lidského faktoru
- nespolehlivost a selhání technických systémů včetně softwarových subsystémů

Při definování požadavků na ochranu informací je nutné si odpovědět na následující okruhy otázek:

- které z informací a dat je třeba považovat za důvěrné či jinak utajované a vymezit hlavní elementy takto utajovaných informací
- po jakou dobu je nezbytné uchovávat určité informace v tajnosti
- které skupiny osob, které mají být s danými informacemi seznámeny a v jakém rozsahu
- které skutečnosti jsou již známé
- které podnikové útvary a které osoby mají přístup do počítačového nebo komunikačního systému a v jakém rozsahu [3]

Nejdůležitější a nejdražší částí informačního systému jsou znalosti, informace a data v něm obsažená. Všechny ostatní prvky jsou obnovitelné, všeobecně dostupné a pouze data jsou jedinečná. Zajištění jejich bezpečnosti je součástí zajištění bezpečnosti informačního systému.

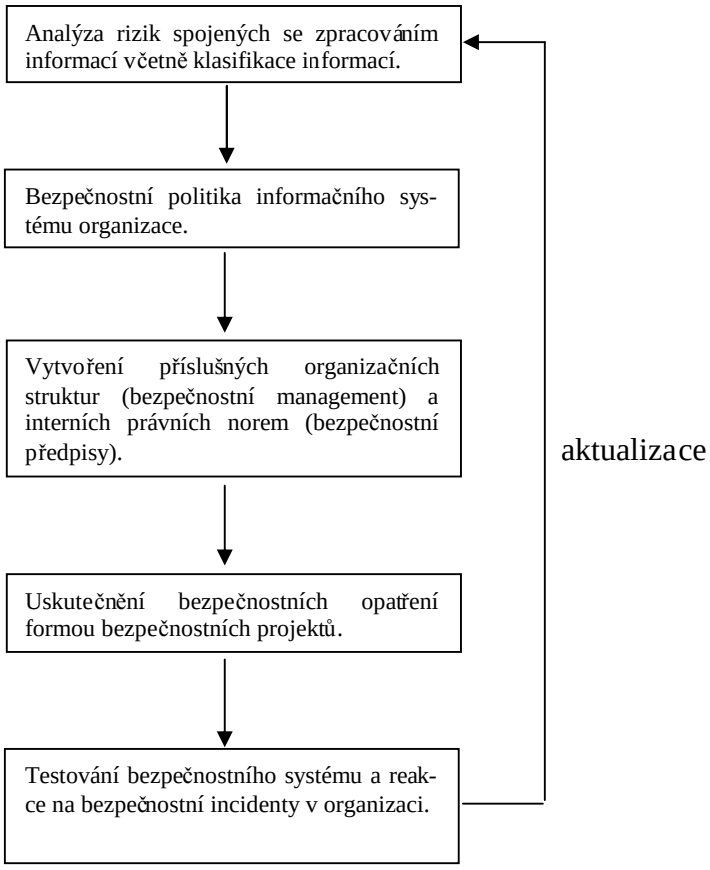
Pod pojmem bezpečnost informačních technologií obvykle rozumíme ochranu odpovídajících IS a informací, které jsou v nich uchovávány, zpracovávány a přenášeny. V soudobém chápání bezpečnosti IT je bezpečnost dána zajištěním:

- důvěrnost – k aktivům (údajům) mají přístup pouze autorizované subjekty
- integrity a autenticity – aktiva (data, software, hardware) smí modifikovat jen autorizované subjekty a původ informací je ověřitelný
- dostupnosti – aktiva (data nebo služby) jsou autorizovaným subjektům do určité doby dostupná, do doby odmítnutí služby

Pokud hovoříme v souvislosti s informačními technologiemi o zpracovávání informací, rozumíme tím použití těchto technologií k uchovávání, přenosu, vyhodnocování a prezentaci informací. Poněvadž se mnohdy jedná o informace s nezanedbatelnou hodnotou (např. daňová přiznání, bankovní účty, elektronické platební nástroje, výsledky vývoje nebo výzkumu, obchodní záměry, atd.) musí být chráněny tak:

- aby k nim měly přístup pouze oprávněné osoby
- aby se zpracovávaly pouze nefalšované informace
- aby se dalo zjistil, kdo je vytvořil, změnil či odstranil
- aby nebyly nekontrolovaným způsobem vyzrazeny
- aby byly dostupné tehdy, když jsou potřebné

4.1. Prvky informační bezpečnosti



Obrázek 9. Budování informační bezpečnosti

4.1.1. Personální bezpečnost

Jedná se o ochranu informačních systémů z hlediska konkrétních událostí způsobených pracovníky a to především z pohledu prevence. Personální bezpečnost musí být zajišťována detektivními prověrkami budoucích zaměstnanců a také periodickými detektivními prověrkami stávajících zaměstnanců. Bezpečnost v oblasti personálních opatření předpokládá zejména vymezení rozsahu a způsobu prověření nově přijímaných i stávajících pracovníků, zejména pak vedoucích a pracovníků přicházejících do styku s důvěrnými a utajovanými informacemi. Také musí být kladen důraz na zajištění dohledu nad osobami, které z organizace odešly a byly seznámeny s důvěrnými a utajovanými skutečnostmi. Detektivní prověrky potencionálních budoucích i stávajících zaměstnanců příslušného podnikatelského subjektu musí poskytnout co nejvíce informací. Nejvhodnějším způsobem vykonávání detektivních prověrek je pověření tímto aktem personální agentury.

4.1.2. Režimová bezpečnost

Zajišťuje vytvoření bezpečnostních pravidel z hlediska zásad práce s informacemi, daty, komunikačními a počítačovými systémy. Jde o významný prvek prevence. Nestačí pouze samotná existence pravidel, ale je také nutno kontrolovat i jejich dodržování.

Pojem režimová bezpečnost zahrnuje:

- režim práce s písemnostmi
- režim ukládání datovým médií
- vymezení okruhu osob pro práci s důvěrnými a utajovanými informace a daty
- opatření pro případ mimořádných událostí

Zabývat se režimovou bezpečností znamená:

- přesně vymezit a určit důvěrné a utajované informace, jejich stupně utajení
- stanovit okruh osob, které mají k důvěrným a utajovaným informacím přístup a v jakém rozsahu tento přístup budou mít
- stanovit organizaci a kontrolu režimu manipulace s důvěrnými a utajovanými informacemi

- vymezit režim a kontrolu pohybu zaměstnanců i cizích osob v objektech a prostorách podniku
- stanovit režim a kontrolu přijímání návštěv, organizace návštěv apod.

4.1.3. Bezpečnost technických prostředků

Jde převážně o jejich výběr, spolehlivost, kontrolu přístupu k těmto prostředkům a ochranu před elektromagnetickým zářením nebo elektrostatickým polem.

Technická bezpečnost vyžaduje zejména následující opatření:

- stanovení rozsahu a následnou realizaci periodických technických prohlídek
- jednorázové technické prohlídky a prověrky míst důležitých jednání
- vybavení prostor objektů technickými prostředky průběžného zjišťování odposlechů a technickými prostředky znemožňujícími realizaci odposlechů (jedná se o šifrátory, šumové generátory a další technické prostředky k ochraně telefonních, faxových, počítačových linek a sítí)

Realizace obranných technických prohlídek směřuje k ochraně informací před jejich únikem. Je nutné realizovat prohlídky specialisty vybavenými speciální technikou pro odhalování úniku informací. Vedle těchto technických prohlídek je třeba provádět průběžnou kontrolu vybranými a zaškolenými pracovníky na konkrétních chráněných úsecích činnosti. Tito pracovníci se při průběžné obranné kontrole zaměřují především na:

- funkčnost ochranných technických prostředků proti úniku informací
- dodržování režimových a organizačních opatření chránících daný úsek činnosti před únikem dat a informací
- provádění technických prohlídek s využitím jednoduchých zařízení ke zjišťování možných úniků informací z chráněných prostor a objektů

4.1.4. Bezpečnost softwarových prostředků

Je nutné zajistit kontrolu nad přístupem k těmto prostředkům, na autentičnost a identifikaci uživatele, rozdělení pravomocí mezi uživateli, výběr a spolehlivost programů apod. Bezpečnost softwarových prostředků spočívá:

- v ochraně proti virům
- v obraně proti zneužití softwarového vybavení
- v ochraně proti zničení či poškození těchto vybavení

4.1.5. Bezpečnost komunikačních systémů a cest

Bezpečnost komunikačních systémů a cest představuje především ochranu mezi jednotlivými částmi komunikačních a počítačových systémů.

4.1.6. Fyzická bezpečnost

Jde o ochranu informací, dat, komunikačních a počítačových systémů proti neoprávněnému přístupu a protiprávnímu vniknutí do prostor, kde se nacházejí.

4.1.7. Aktivní ochrana proti úniku informací a dat

Tento prvek zahrnuje ochranu proti firemní špionáži a proti aktivnímu konkurenčnímu zpravodajství. Jde o systém opatření směřujících k získání informací o aktivitách agentur zabývajících se konkurenčním zpravodajstvím (informační pronikání do takovýchto útvarů či agentur).

4.2. Odpovědnost za informační bezpečnost

Odpovědnost za bezpečnost informací vyplývá z obchodního zákoníku a podnikatel, který je z tohoto hlediska jejich majitelem, je odpovědný za zajištění jejich bezpečnosti. Ztráta informací se rovná finanční ztrátě spojené s jejich obnovou a zneužitím. V praxi je každý pracovník organizace (zaměstnanec firmy) zainteresován na plnění obchodních funkcí a zabezpečení informací je v zájmu každého, kdo s nimi přichází legálně do styku.

Jedním ze způsobů předcházení ztrátám z porušení bezpečnosti informací ze strany uživatelů informačních systémů je dosažení takového stavu bezpečnostního vědomí, že si budou

všichni vědomi své zodpovědnosti a přijmou opatření, která porušení bezpečnosti omezí. Na straně vlastníka informací je třeba udělat kroky, které informační bezpečnost co nejvíce posílí a pokud možno ji i vynutí. Je v zájmu organizace zajistit získávání, udržování a zvyšování bezpečnostního vědomí cestou specializovaných školení.

Pro implementaci bezpečnostní politiky je nezbytné, aby všichni zaměstnanci získali potřebné znalosti bezpečnostních dokumentů a opatření v rozsahu podle svého pracovního zařazení a odpovědnosti. Na tomto základě musí být připraven systém školení pro jednotlivé kategorie pracovníků. [12]

Základní bezpečnostní školení pro všechny zaměstnance by mělo zahrnovat předmět chráněných informací, zásady styku s nimi a sankce a postup při ztrátě či jejich porušení. Zaměstnanec musí mít možnost prostudovat dokument bezpečnostní politiky, musí znát pracovníka pověřeného bezpečností, na nějž se lze v případě potřeby obrátit. Takovýmto školením musí projít každý nově přijímaný zaměstnanec.

Školení pracovníků musí proběhnout minimálně jedenkrát ročně. Jeho hlavním důvodem jsou změny, k nimž dochází při příchodu a odchodu zaměstnanců, nová pracovní zařazení, odlišnosti v prostředí, v němž se s citlivými informacemi pracuje, a technologie, které se k tomu využívají. Školení nesmí být určeno pouze pro zaměstnance přicházející do styku s citlivými informacemi. Každý pracovník se totiž může stát objektem vydírání, snahy o koupi informací apod. Postavení zaměstnance v hierarchii podniku je jedním z hledisek, jenž je potřeba uplatnit při volbě obsahu i formy bezpečnostního školení.

4.3. Základní principy bezpečnosti při použití informačních technologií

Informační technologie (dále jen IT) zpracovávají stále více a více informací s velkou hodnotou. Pokud hovoříme v souvislosti s informačními technologiemi o zpracovávání informací, pak tím rozumíme použití těchto technologií k uchovávání, přenosu, vyhodnocování a prezenci informací. Poněvadž se mnohdy jedná o informace s nezanedbatelnou hodnotou

(např. zdravotní záznamy, daňová přiznání, bankovní účty, elektronické platební nástroje, výsledky vývoje a výzkumu, obchodní záměry apod.) musí být chráněny tak:

- aby k nim měly přístup pouze oprávněné osoby
- aby se zpracovávaly nefalšované informace
- aby se dalo zjistit, kdo je vytvořil, změnil nebo odstranil
- aby nebyly nekontrolovaným způsobem vyzrazeny
- aby byly dostupné tehdy, když jsou potřebné

Mezi hlavní důvody a motivace pro zabezpečení informačního systému organizace patří následující způsoby narušení bezpečnosti zpracovávání informací:

- narušením soukromí či utajením informací
- vydáváním se za jinou oprávněnou osobu a zneužíváním jejích privilegií
- distancováním se od odpovědnosti nebo od závazků plynoucích z manipulace s informacemi
- tvrzením, že se nějaká informace někam poslala aniž by se toto stalo
- tvrzením, že se informace získala od nějakého podvodníka
- neoprávněným zvýšením svých privilegií přístupu k informacím
- modifikací privilegií ostatních osob
- zatajením výskytu důvěrné informace v jiných informacích
- zjišťováním, kdo a kdy si zpřístupňuje které informace
- zařazením se jako skrytý mezičlánek v konverzaci jiných subjektů
- pokažením funkcionality softwaru doplněním skrytých funkcí
- narušením protokolu činností jiných subjektů zavedením nesprávných, nekorektních informací
- podkopáním důvěryhodnosti protokolu způsobeným zjevnými nebo zdánlivými poruchami
- bráněním jiným uživatelům legitimně komunikovat

Bezpečnost IT použitých v organizaci se dosahuje především plněním manažerských funkcí souvisejících s bezpečnostní IT jako integrální součásti plnění globálního plánu správy organizace. Mezi takové manažerské funkce patří:

- určení strategií, cílů a politiky zabezpečení IT organizace
- určení požadavků na zabezpečení IT organizace

- identifikace a analýza hrozeb pro aktiva IT v rámci organizace
- identifikace a analýza rizik pro organizaci plynoucích z používání IT
- specifikace přiměřených bezpečnostních opatření eliminujících nebo snižujících rizika
- sledování implementace a provozu bezpečnostních opatření použitých pro účinnou ochranu informací a služeb IT v rámci organice
- vyvinutí a zavedení programu zvyšování bezpečnostních znalostí a vědomí nutnosti udržovat bezpečí všech, kdo IT v organizaci používají
- detekování bezpečnostních incidentů a adekvátní reakce na ně

4.4. Bezpečnostní mechanismy

Pro implementaci funkcí prosazujících bezpečnost se používají bezpečnostní mechanismy, které představují logiku nebo algoritmus, který hardwarově, softwarově, fyzicky nebo administrativně implementuje bezpečnostní funkci.

Rozlišujeme tyto bezpečnostní mechanismy:

- slabé – pro ochranu před amatéry, proti náhodným útokům
- střední síly – pro ochranu před hackery, proti úmyslným útoků s omezenými příležitostmi a možnostmi
- silné – ochrana před profesionály, ochrana proti útočníkům s vysokou úrovní znalostí, s velkými příležitostmi, s velkými prostředky, používajícími útoky vymykající se běžné praxi

Podle použité technologické základny rozeznáváme bezpečnostní mechanismy:

- softwarové nebo také logické – kryptografie, kódování, ochranné nástroje v operačních a aplikačních systémech
- hardwarové nebo také technické – šifrovače, autentizační a identifikační karty
- fyzické – stínění, trezory, zámky, protipožární ochrana, generátory náhradní energie, chráněná místa pro záložní kopie dat a programů

- administrativní – hesla, právní normy, zákony, vyhlášky, předpisy, výběr důvěryhodných osob

4.5. Typy bezpečnostních politik

Variant jak zabezpečit informační systémy (dále jen IS) je více, odlišují se v nákladech na jejich pořízení a údržbu, transparentnosti nebo odolností proti útoku výjimečné síly. Doporučená varianta by měla vzejít z oponované a závazně přijaté bezpečnostní politiky organizace nebo alespoň z bezpečnostní politiky IS používané organizací. Přijatá bezpečnostní politika může být podle požadované úrovně záruky na zabezpečení:

- promiskuitní politika – tedy nikoho neomezující, která každému v zásadě povoluje dělat vše, tedy i to, co by neměl. Promiskuitní IS jsou obvykle provozně nenákladné, mnohdy ani nenutí povinně používat pro autentizaci alespoň hesla a zaručují pouze minimální nebo vůbec žádnou bezpečnost.
- liberální politika – každému povoluje dělat vše až na věci explicitně zakázané. Zaručuje větší bezpečí než politika promiskuitní. Z hlediska používání internetu jsou liberální bezpečnostní politiky často uplatňovány v akademických prostředích, kde se přístup ke službám internetu s výjimkou vyjmenovaných případů neomezuje. Opírá se o zásadu volitelného řízení přístupu.
- opatrná (rozumná) politika – politika zakazující dělat vše co není explicitně povoleno. Je nákladnější na zavedení ,avšak zaručuje vyšší stupeň bezpečnosti. Při aplikaci na obecný IS převážně požaduje provedení klasifikace objektů a subjektů. Opatrná politika je opřena mimo jiné o zásadu povinného řízení přístupu. Z hlediska používání internetu je obvykle počáteční bezpečnostní politikou při zavádění firewallů.
- paranoidní politika – politika zakazující vše, včetně toho, co by zakázáno být nemuselo. Zaručuje nejvyšší stupeň bezpečnosti a ve svém dů-

sledku zakazuje používání i internetových služeb. Vede k maximální izolaci systému. I přes to může být pro organizaci stále užitečná. Databázový systém zpracovává vysoce důvěrné informace a lze jej tak fyzicky a technicky izolovat na systém s konečným počtem snadno kontrolovatelných vstupů a výstupů. Paranoidní charakter bezpečnostní politiky umožní implementaci aplikace v prostředí s nízkou systémovou režií a tudíž s dosažitelnou vyšší výkonností při zachování nižší úrovně nákladů.

4.6. Důležité pojmy vymezující oblast bezpečnosti IT

4.6.1. Zranitelné místo

Zranitelné místo je slabinou IS využitelnou ke způsobení škod nebo ztrát útokem na IS. Existence zranitelných míst je důsledek chyb, selhání v analýze, v návrhu anebo v implementaci IS. Může být také důsledkem vysoké hustoty uložených informací, složitosti softwaru, existence skrytých kanálů pro přenos informace jinou než zamýšlenou cestou. Podstata zranitelného místa může být fyzická, přírodní, fyzikální nebo v lidském faktoru. Zranitelná místa vznikají jako důsledek selhání, čímž může být opomenutí nebo zanedbání při těchto činnostech:

- v návrhu informačního systému
- ve specifikaci požadavků – IS může plnit všechny funkce a vykazovat všechny bezpečnostní rysy po něm požadované a přesto stále ještě obsahuje zranitelná místa, která ho z bezpečnostního hlediska činí nevhodným nebo neúčinným
- v řešení
- v konstrukci – IS nesplňuje svoje specifikace nebo byla do něj zavlečena zranitelná místa v důsledku špatných konstrukčních standardů nebo nesprávných rozhodnutí
- při návrhu nebo jeho implementaci

- v provozu – zranitelná místa byla do IS zavlečena použitím neadekvátních provozních řídících nástrojů

4.6.2. Hrozba

Možnost využít zranitelné místo IS k útoku na něj, tedy ke způsobení škody na jeho aktivech (datech, informacích). Hrozby lze kategorizovat na:

a) objektivní
   - přírodní – sem patří požáry, povodně, výpadky napětí, různé poruchy, atd., u kterých je prevence obtížná a u nichž je třeba řešit spíše minimalizaci dopadů vhodným plánem obnovy – v tomto případě je třeba vypracovat havarijní plán. U těchto hrozeb je obtížná prevence a je lepší řešit spíše minimalizaci dopadů vhodným plánem obnovy
   - fyzikální – např. elektromagnetické vyzařování
   - technické nebo také logické – porucha paměti, softwarová „zadní vrátka“, špatné propojení jinak bezpečných komponent, krádež nebo zničení paměťového média nebo nedokonalé zrušení informace na něm

b) subjektivní – tedy hrozby plynoucí z lidského faktoru
   - neúmyslné – např. působení neškoleného uživatele nebo správce, atd.
   - úmyslné – představované potenciální existencí vnějších útočníků (teroristi, kriminální živly, konkurenti, hackeři a další) i vnitřních útočníků

c) neautorizované použití zdrojů – krádeže hardwarových a softwarových komponent včetně používání jejich neoprávněných kopií

d) neautorizované používání IS a služeb jimi poskytovaných, znepřístupnění služeb – bránění autorizovaným subjektům využívat systém IT na dohodnuté úrovni poskytovaných služeb, popírání odpovědnosti za akce citlivé z hlediska bezpečnosti

Vlastní závažnost hrozby (rizika) vidíme ve vzorci:

$$H = N \cdot P \tag{1}$$

kde:

H závažnost hrozby

N následek

P pravděpodobnost výskytu hrozby

4.6.3. Útok

Útokem rozumíme buď úmyslné využití zranitelného místa, to jest využití zranitelného místa ke způsobení škod a ztrát na aktivech IS, nebo neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech. Při analýze možných forem útoků na IT je třeba řešit otázky jako jakým způsobem se projevuje počítačová kriminalita, jaké jsou možné formy útoků, kdo útočí, jaká rizika souvisí s užíváním IT a jak se před nimi chránit a podobně. Následně řešenými problémy jsou potom rozhodnutí o způsobu detekce útoku, zjišťování bezpečnostních incidentů, způsob reakce na útok a jak se zachovat při samotném bezpečnostním incidentu. Útok může být úmyslný nebo neúmyslný, který můžeme také označit jako náhodný. Rozpoznáváme tyto druhy útoků:

a) útoky na hardware, které můžeme vést
   - přerušením – přírodní havárie, neúmyslné útoky způsobené kouřením, údery, úmyslné útoky krádeží, destrukcí, odposlechem – krádež části procesoru, místa v paměti
   - přidáním hodnoty – změnou režimu činnosti

b) útoky na software, které můžeme vést
   - přerušením – mezi neúmyslné útoky řadíme např. vymazání softwaru způsobené špatným konfiguračním systém nebo archivačním systémem, použití neotestovaných programů, chyby operátora, mezi úmyslné útoky potom řadíme např. úmyslné vymazání programu
   - odposlechem – provedení neoprávněné kopie programu, pirátství
   - změnou – např. využitím „zadních vrátek“ (neveřejných spouštěcích postupů z doby tvorby softwaru)

- přidáním hodnoty – zabudováváním virů, atd.

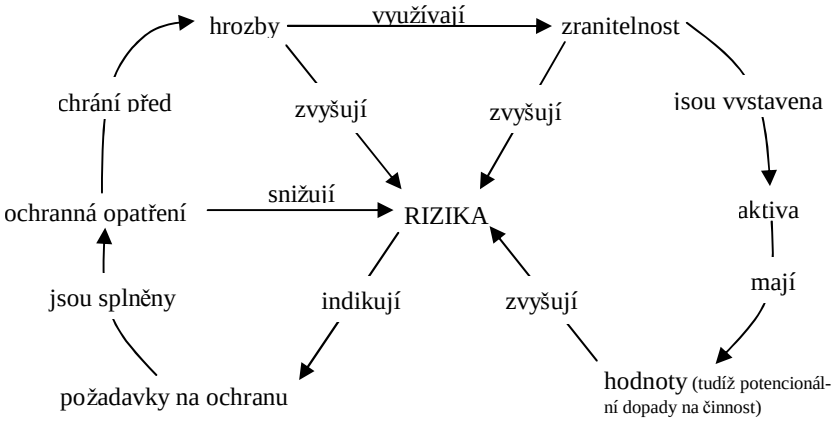
c) útoky na data, které můžeme vést

- přerušením – mezi neúmyslné útoky lze zařazovat jejich neúmyslné vymazání, mezi úmyslné útoky potom patří úmyslné vymazání, sabotáž
- odposlechem – porušení důvěrnosti, krádež kopií
- změnou – porušení integrity, neautorizované modifikace dat
- přidáním hodnoty – opakovanými neautorizovanými dílčími odběry peněžního konta, generování transakcí, atd.

4.6.4. Riziko

Riziko pro nás představuje existenci hrozby. Rizikem rozumíme pravděpodobnost využití zranitelného místa IS. Říkáme, že se hrozba uplatní s takovou a takovou pravděpodobností. Rizika lze teorizovat nejen pravděpodobností výskytu bezpečnostního incidentu, ale i potenciálně způsobenou škodou.

Rizikem pro nás mohou být např. katastrofy a živelné pohromy, chyby technického a programového vybavení, výpadek počítače, poškození stopy disku, nečitelný disk, chyba v aplikačním programu poškozuje záznam, lidská nepozornost, zavedení a aktualizace nesprávných dat, fyzické poškození nosného média, fyzické poškození nosného média, úmyslné poškození (sabotáž, špionáž, počítačová kriminalita), narušení soukromí (úmyslné nebo neúmyslné prozrazení soukromých informací).



Obrázek 10. Složky ovlivňující rizika

Riziko můžeme odhadnout jednoduchým vztahem:

$$R = \frac{10^{(P+Z-2)}}{4} \tag{2}$$

kde:

Z kategorie velikosti ztrát (Z = 0 ÷ 7)

P kategorie pravděpodobnosti výskytu jevu:

- 1 jednou za 400 let
- 2 jednou za 40 let
- 3 jednou za 4 roky (1000 dní)
- 4 jednou za 100 dní
- 5 jednou za 10 dní
- 6 jednou denně
- 7 desetkrát za den

R ztráta způsobená jevem, střední doba mezi jevy

Další jednoduchou rovnicí můžeme taktéž vyjádřit míru rizika:

$$R = P \cdot N \tag{3}$$

kde:

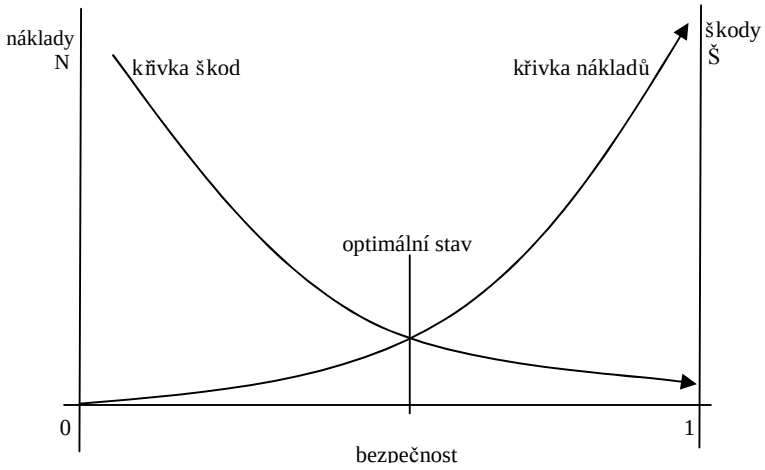
R riziko

P pravděpodobnost vzniku – dále se skládá z:

- Sa výsledek analýzy statistických údajů o skutečném výskytu krizových
- Rz reálný stav zabezpečení objektu

N následek – dále se skládá z:

- Np označení přímých následků
- Nn označení nepřímých následků



Obrázek 11. Určení optimálních nákladů na minimalizaci rizik

4.7. Bezpečnostní monitoring informačních systémů

Důležitou součástí systému řízení informační bezpečnosti je požadavek zajistit monitorování přístupu k informačním systémům a jejich použití. Implementace optimalizovaného systému bezpečnostního monitoringu IS napomáhá splnit významné bezpečnostní cíle, zejména pak musí zajistit:

- odpovědnost jedince
- rekonstrukci události
- detekci narušení
- podporu při analýze a řešení vzniklých problémů

Přínosem bezpečnostního monitoringu IS je získání určité kontroly nad aktivitami administrátorů a správců IS. Bezpečnostní monitoring IS tak významně přispívá k oddělení rolí kontrolovaného a kontrolujícího ve skupině privilegovaných (již zmínění administrátoři a správci) a k zajištění průkaznosti jejich odpovědnosti. Tento systém rovněž slouží jako jeden z nástrojů pro sledování a vyhodnocování dosažené úrovně informační bezpečnosti v organizaci. Požadovaná úroveň bezpečnosti informací v organizaci je stanovena bezpečnostní politikou.

Bezpečnostní monitoring IS se běžně dělí na následující oblasti:

- real-time monitoring, který zajišťuje průběžné sledování sítí a systémů s cílem detekovat útoky a analyzovat je
- analýza souborů s auditními záznamy, jenž zajišťuje vyhodnocování bezpečnostních událostí
- diagnostika zajišťující pravidelné prověrky systémové infrastruktury s cílem odhalit specifické zranitelnosti

Jednou z hlavních úloh bezpečnostního monitoringu IS je detekce bezpečnostních událostí, zejména pak událostí mající povahu útoku proti informačnímu systému. Bezpečnostní událost lze charakterizovat jako určitou akci proti prostředku informačního systému. Formy akcí mohou být různé a různé mohou být i prostředky proti nimž je akce namířena. K jejímu provedení je vhodný nástroj využívající existující slabiny IS.
Pochopení průběhu incidentu a především pochopení rozdílnosti v pohledu útočníka a administrátora, tedy obránce, je jedním z předpokladů pro návrh kvalitního systému bezpečnostního monitoringu a jeho začlenění do systému řízení bezpečnosti IS. Je nutné si uvědomit, že administrátor povětšinou pozoruje projevy bezpečnostních událostí bez konkrétních informací o útočníkovi a jím použitých postupech. V mnoha případech není na první pohled patrné, zda jde o bezpečnostní událost nebo pouze o podezření. Komplikaci můžeme najít i v nejednoznačně definovaným vztahem mezi detekovanou událostí a příčinou – tedy konkrétním útokem proti IS. Z tohoto důvode je tedy pozice administrátora velmi obtížná při přiřazování jednotlivých útoků ke konkrétním incidentům. [3]

4.8. Ochrana dat

Všechny IS jsou založené na využívání stejné báze dat. Ke každým datům je z hlediska jejich ochrany zapotřebí přistupovat individuálně.

Rozlišujeme tři druhy nebezpečí:

- kompromitace (prozrazení)
- modifikace (neoprávněná změna)

- zničení (úmyslná či neúmyslná likvidace)

Samotná ochrana dat se může z různých hledisek dělit na několik skupin. Pro účinnou ochranu se tyto skupiny mají vhodným způsobem kombinovat. Podle prvků, jenž je potřeba chránit definujeme tyto skupiny:

- ochrana fyzického přístupu k nosičům dat – jde především o zabezpečení proti neoprávněnému přístupu osob k diskům a zálohovým médiím především systémy EZS, ACCESS a CCTV
- ochrana logického přístupu k datům – zabránění průniku k datům obejitím bezpečnostního softwaru nebo nabouráním se prostřednictvím intranetu
- ochrana uložených dat – ochrana proti nežádoucímu čtení a využití dat
- ochrana dat přenášených počítačovou sítí – zabezpečení bezpečného přenosu dat na různým elektronických a papírových médií a ochrana před modifikacemi dat k zajištění jejich integrity
- ochrana dat před zničením – přírodní katastrofy, požár objektu, fyzický útok, před nimiž chráníme data pravidelným zálohováním, popř. duplikací souborů

Samotná data se potom v IS klasifikují podle závažnosti jejich ochrany do několika skupin. Je samozřejmé, že textové soubory uživatelů nebudou chráněny stejným způsobem jako databáze přístupových hesel. Jiný důraz je kladen na data uživatelů a jiný na auditní záznamy, spustitelné kódy či autentizační informace. [3]

4.9. Klasifikace informací

Organizace klasifikují informace, aby zjistili odpovídající úroveň ochrany svých zdrojů, kterých je v každém podniku řada a je tedy nutné určit, které dostanou prioritu a potřebují zvýšenou ochranu. Jedním z důvodů klasifikace informací je tedy napomoci správné alokaci vzácných zdrojů v organizaci, protože ne všechny informace mají stejnou hodnotu. Proto je třeba se alespoň na základní úrovni pokusit o klasifikaci informací. Už jen proto, aby se zajistilo, že při zajišťování informačních aktiv jsou podnikové zdroje náležitě využívány. Aby zaměstnanci mohli chránit tato aktiva, musí nejdříve znát mechanismus nakládání

s nimi. Vnitrofiremní systém klasifikace informací založený na zdravém rozumu, znalosti podnikové kultury a významu informací na trhu může být konkurenční výhodou.

Soubor otázek spojených s klasifikací informací se zpravidla řeší v rámci řízení klasifikace. Spadá do taktického a operativního řízení a základ je položen při tvorbě bezpečnostní politiky.

Úkolem klasifikačního řízení je:

1) vytvoření a přijetí metodiky klasifikace, která je základem pro sestavení klasifikační politiky organizace
2) nepřetržitá realizace činností, které z klasifikační politiky vyplývají

Klasifikační politika specifikuje postupy, normy, směrnice a nařízení na základě kterých:

- rozdělujeme informace do tříd, včetně klasifikace odvozených informací
- definujeme způsob deklasifikace informací
- definujeme způsob nakládání s informacemi, včetně zajištění přístupu a ochrany
- zajišťujeme označování a pojmenování klasifikovaných informací
- zajišťujeme označování a pojmenování klasifikovaných informací
- řešíme incidenty včetně specifikace sankcí
- způsob řešení chyb při klasifikaci, to jest způsoby a postupy přeřazení informací mezi třídami

Výsledkem klasifikačního řízení je kromě daných dokumentů rozdělení informací do tříd s definovanými způsoby nakládání tak, aby v součinnosti s ostatními bezpečnostními opatřeními byly zachovány dané zájmy a splněny cíle.

Obecně jsou informace rozděleny do dvou základních skupin na informace:

- klasifikované
- neklasifikované – veřejné, všeobecné

Stát klasifikuje utajované informace na základě Zákona na ochranu utajovaných informací a o bezpečnostní způsobilosti do těchto tříd:

- PT – přísně tajné (top secret)
- T – tajné (secret)
- D – důvěrné (confidential)
- V – vyhrazené (restricted)

Začlenění do tříd se určuje podle újmy, která vznikne odhalením – mimořádně vážná, vážná, prostá újma a „je to nevýhodné“.

Význam a často i citlivost informace se v čase mění, proto někdy dochází k reklasifikaci informace. Protože informace v čase většinou ztrácejí svou hodnotu, hovoříme častěji o jejich deklasifikaci. Snížení klasifikačního stupně by mělo proběhnout automaticky, jestliže vlastník informace zná datu, kdy by měla být informace reklasifikována, měla by být označena důvěrné do *xx.xx.xxxx*. Deklasifikace se většinou provádí o jeden stupeň citlivosti. O dva stupně se může neklasifikovat například čtvrtletní výsledky hospodaření firmy, které až do veřejného vyhlášení bývají klasifikovány jako důvěrné a poté veřejné. Všechny informace označené vyšším klasifikačním stupněm než veřejné by měly být alespoň jednou ročně podrobeny přehodnocovacímu procesu a reklasifikovány, pokud již nesplňují kritéria pro daný stupeň zabezpečení. Součástí klasifikace je i likvidace dokumentů, které již nejsou potřeba. Je také třeba dohlédnout na kopírování klasifikovaných dokumentů a zajistit, že dokumenty a soubory dat jsou kontrolovány, zapisován počet a příjemce vytvořených kopií, které jsou taktéž příslušně označeny. [20]

Ve firmách se používá tří až čtyřstupňový model klasifikace, přičemž použité výrazy se liší. V tabulce níže jsou příklady používaných synonym.

Klasifikační třída	Synonyma	Obsah – jaké informace?
Přísně tajné (PT)	Tajné	- poskytují organizaci velmi důležitou konkurenční výhodu - jejich ztrátou dojde k zániku organizace – mimořádně vážná újma - jsou (technickým, finančním) základem úspěchu produktu - ukazují specifika podnikové strategie a hlavní záměry
Tajné (T)	Důvěrné (doplněné o další atributy): - vysoce citlivé - se speciálním zacházením - osobní - apod.	- poskytují organizaci velmi důležitou konkurenční výhodu - jejich ztrátou může dojít k vážné újmě organizace - jsou (technických, finančním) základem úspěchu produktu - ukazují specifika podnikové strategie a hlavní záměry

Důvěrné (D)	- citlivé
	- osobní
	- privilegované
	- vyhrazené (doplněné o tyto atributy):
	  - důležité
	  - utajené
	  - apod.
		- poskytují organizaci důležitou konkurenční výhodu
		- jejich ztrátou může dojít k prosté újmě organizace
		- jsou vysoce důležité pro úspěch produktu
		- identifikují osoby

Vyhrazené (V)	- citlivé - důvěrné - pouze pro interní potřebu - k omezenému šíření - proprietární - apod.	- takové informace, které slouží zaměstnancům k realizaci obchodních zájmů organizace

Tabulka 1 – Seznam používaných synonym při klasifikaci utajovaných informací

4.10. Způsoby obrany moderních podniků

Na obranu proti útočníkům se využívají hardwarové a softwarové nástroje. Za účelem efektivního zabezpečení přenosu dat a uchování znalostí se budují systémy organizované do rozličných struktur. Systémy obrany moderních podniků úzce korespondují s vytvořenou bezpečnostní politikou IT.

4.10.1. Autentizace

Autentizace je ověření identity uživatele nebo entity v systému, většinou za účelem řízení přístupu ke zdrojům a objektům v systému. Znamená to, že totožnost uživatele nebo systému, se kterým hodláme komunikovat, je účelné nějakým vhodným způsobem ověřit před tím, než mu umožníme přístup ke zdrojům vlastního systému. Prakticky podle žádného způsobu hodnocení bezpečnosti nemůže systém bez alespoň základní autentizace získat vyšší bezpečnostní třídu než nejnižší – nevyhověl. Autentizace se skládá z několika fází. Nejprve je nutno se registrovat v systému uživatele, přiřadit mu autentizační informaci a definovat jeho práva. Tato fáze se nazývá registrační. V druhé fázi je od uživatele získána autentizační informace. Data jsou poté použity způsobem předepsaným příslušným autentizačním protokolem, k prokázání totožnosti uživatele vzdálenému systému. Tato fáze se nazývá login. V poslední fázi pak vzdálený systém po jednom či více komunikačních krocích vydá rozhodnutí, zda autentizační požadavek přijme nebo odmítne. [18]

4.10.2 Autorizace

Po úspěšné autentizaci uživatele může být udělena autorizace pro užívání určitých zdrojů a služeb. Autorizace specifikuje, jaké operace uživatelé mohou v systému provádět a jaká data jsou pro ně dostupná. Všichni uživatelé musí být před přístupem k informacím a službám systému unikátně a spolehlivě autentizováni a musí být vyžadována jejich autorizace. Tato činnost musí předcházet všem dalším aktivitám uživatelů v IS a musí zajistit ochranu důvěrnosti a integrity autorizační informace, tedy umožnit provedení změny určeným způsobem a pouze oprávněným subjektem.

4.10.3. Šifrování

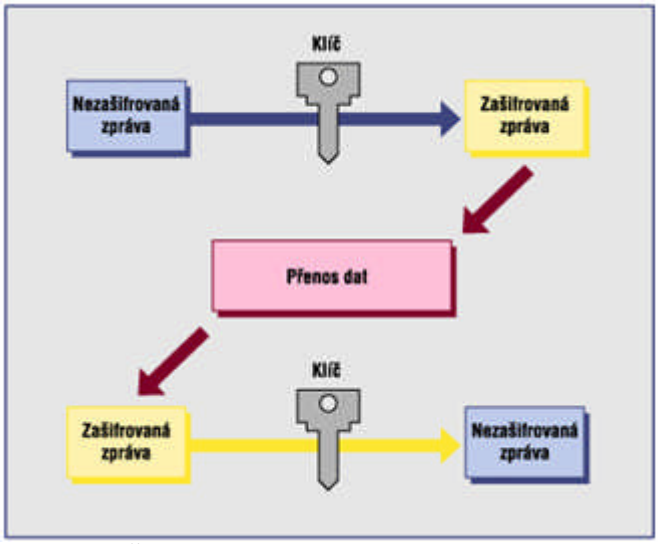
Existují dva základní přístupy k šifrování: symetricky - soukromým klíčem a asymetricky - dvěma klíči (soukromým a veřejným). Šifrování se může uplatňovat na různých vrstvách síťové infrastruktury.

4.10.3.1. Symetrické šifrování

Při šifrování soukromým klíčem obě strany komunikace sdílejí klíč, který se pak používá symetricky (pro šifrování i dešifrování). Šifrování lze použít jak pro autentizaci, tak pro ochranu dat při přenosu. Jedno z hlavních omezení používání soukromého klíče je distribuce klíče všem, kteří jej potřebují, neboť je třeba zajistit bezpečnost (silné šifrování) samotného klíče při jeho přenosu sítí. Z tohoto důvodu se soukromý klíč často mění. Soukromý klíč může být bezpečně uložen na počítači nebo na čipové kartě. [19]

Příklady šifrování soukromým klíčem:

- DES
- AES
- IDEA
- TripleDES



Obrázek 12. Šifrování zpráv symetrickou šifrou

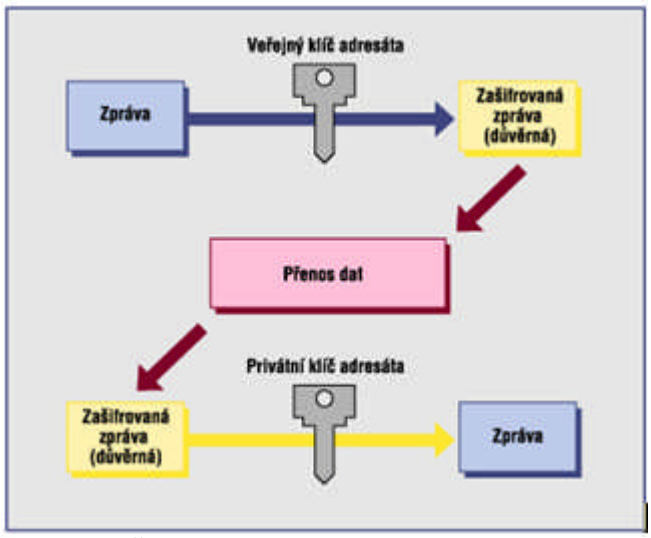
4.10.3.2. Asymetrické šifrování

S veřejným klíčem se šifrování provádí asymetricky, kdy data zašifrovaná jedním klíče lze dešifrovat klíčem druhým, přičemž oba tyto klíče tvoří jedinečný pár vzájemně korespondujících klíčů, jeden klíč je pak veřejně dostupný komukoli, zatímco druhý je přísně soukromý. Asymetrické šifrování tedy slouží k ochraně přenášených dat, ale nikoli k autentizaci původce zprávy, pokud použil dostupný veřejný klíč. Každé dvě stanice mo-

hou bezpečně komunikovat bez předchozího předávání klíčů dvojím šifrováním, soukromým a veřejným klíčem, a to v libovolném pořadí. [19]

Příklady asymetrického šifrování:

- Diffie-Hellman
- RSA



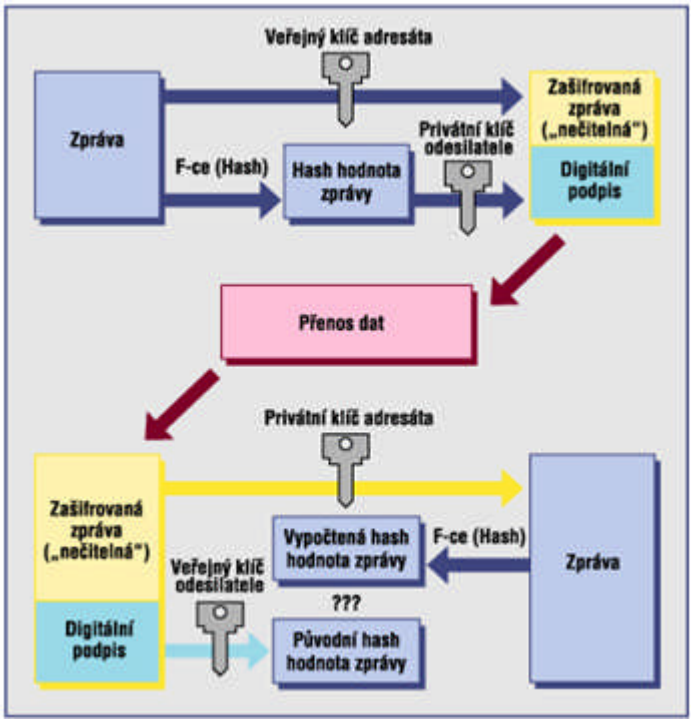
Obrázek 13. Šifrování zpráv asymetrickou šifrou

Velkou výhodou asymetrického šifrování je relativně jednoduchá správa šifrovacích klíčů, protože pro distribuci veřejných klíčů není potřeba zabezpečená komunikace. Soukromý klíč je udržován v bezpečí v lokálním systému a sítí se nedistribuuje nebo se generuje nová dvojice klíčů pro každou novou relaci nebo transakci. Při změně soukromého klíče se vygeneruje odpovídající veřejný klíč, který se inzeruje místo původního veřejného klíče. Nevýhodou tohoto šifrování je složitost použitého algoritmu, šifrování soukromým klíčem je podstatně rychlejší. Z tohoto důvodu se často přistupuje ke kombinovanému využití jak soukromého tak veřejného klíče. Rozbití klíče se provádí buďto hrubou silou, kdy se zkouší nejrůznější kombinace dešifrování, nebo technikami kryptoanalýzy, kdy se studují rozdíly mezi páry zašifrovaného textu a získané informace se používají pro nalezení šifry. [19]

4.10.4. Digitální podpisy a certifikáty

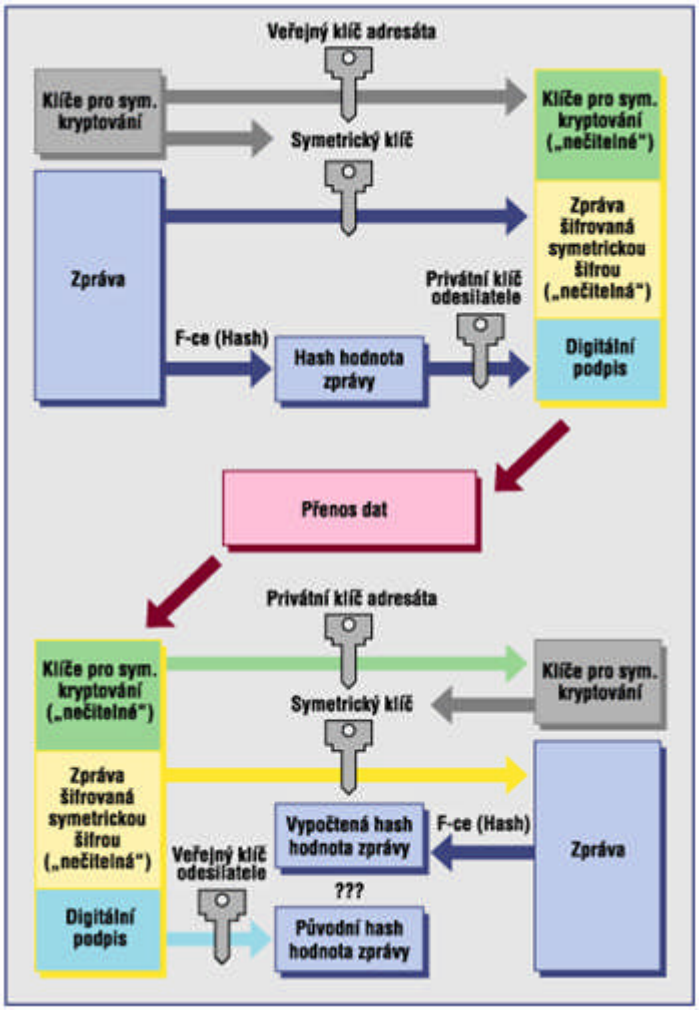
Digitální podpis je vhodný pro zajištění integrity dat a nepopiratelnosti podpisu. Samotný digitální podpis lze pak přirovnat spíše k efektu, kterým je identifikace a autentizace. Toho

lze dosáhnout různými způsoby, zákon předpokládá, že jsou tato řešení založena na metodách asymetrického šifrování, neboli na použití dvojice vzájemně komplementárních klíčů (privátního a veřejného). Pokud chceme vytvořit digitální podpis určitého souboru, musíme nejdříve určit jeho hash (identifikuje uživatele databází hashovaných hesel a ochraňuje integritu zprávy). Jakýkoli soubor nebo e-mailovou zprávu lze v podstatě chápeme jako soubor čísel, na nějž aplikujeme hash algoritmus. Na jeho výstupu získáme číslo o dané délce jednoznačně reprezentující vstupní data, tedy otisk souboru. Hash je následně zašifrován pomocí soukromého klíče podepisující osoby a digitální podpis je na světě. Zjednodušeně můžeme hash označit za zašifrovaný privátní klíč digitálního podpisu. Ten se pak může přidat k podepisovaným datům nebo může být transformován do podoby samostatného souboru. Zpravidla se k němu ještě přidává i digitální certifikát podepsané osoby, který slouží adresátovi k ověření podpisu.



Obrázek 14. Bezpečná komunikace s využitím digitálního podpisu

Digitální certifikát se skládá ze dvou základních komponentů – veřejného klíče a osobních dat jeho vlastníka. Pro důvěryhodné mapování uživatele se používá hierarchická autorita (PKI – public key infrastucture) a důvěrnost digitálních certifikátů ověřuje certifikační úřad. PKI používá dva digitální klíče – jeden pro šifrování zprávy, druhý pro její dešifrování. Certifikační úřad generuje certifikát a také certifikát opatří digitálním podpisem.



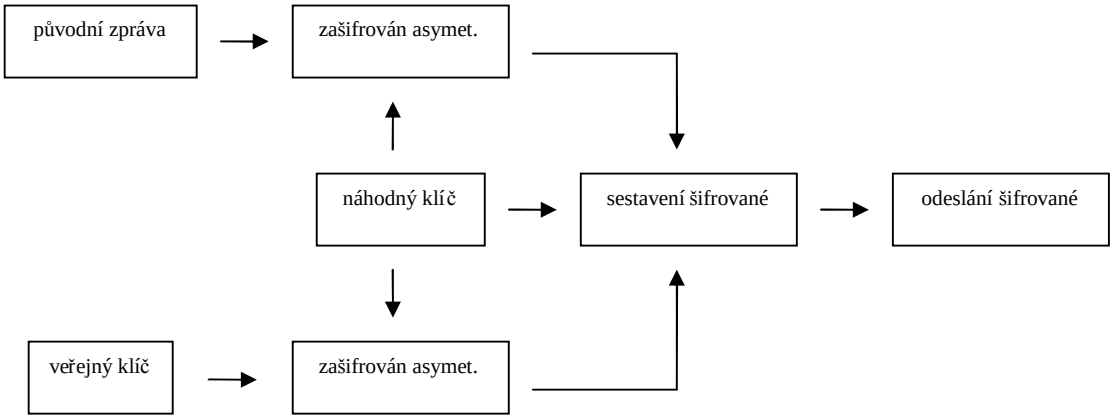
Obrázek 15. Bezpečná komunikace s využitím digitálního podpisu a šifrováním zprávy symetrickou šifrou

4.10.5. PGP – Pretty Good Privacy

PGP je kryptografický balík využívaný především pro šifrování zpráv a souborů a vytváření či ověřování digitálních podpisů. Dnes patří program PGP bezesporu mezi jedny z nejrozšířenějších prostředků pro šifrování elektronické pošty a pro ověřování její pravosti pomocí digitálních podpisů. PGP pracuje s šifrovacími algoritmy CAST, AES, TripleDES, IDEA, Twofish a patří mezi jedny z kryptograficky nejsilnějších prostředků. Nemalou výhodou je i dostupnost na většině platforem.

PGP je kombinovaný šifrovací systém. Navenek se jeví jako program s veřejným šifrovacím klíčem, plně využívající asymetrického šifrování. To se však ve skutečnosti používá pouze pro zakódování klíče symetrické šifry, kterou je pak zašifrována samotná zpráva.

Digitálním podpisem je kontrolní součet zprávy (hash), který je zašifrován asymetrickou šifrou. V PGP jsou použity tyto algoritmy: RSA jako asymetrická šifra, IDEA (128 efektivních bitů klíče), TripleDES (168 bitů).



Obrázek 16. Šifrování pomocí PGP

4.10.6. Poskytovatelé certifikačních služeb

Nutnou podmínkou pro komunikaci občanů se státní správou s použitím elektronického podpisu jsou tzv. kvalifikované certifikáty občanů. V současné době jsou akreditováni tři poskytovatelé certifikačních služeb a bylo vydáno několik tisíc těchto certifikátů a jejich počet rychle narůstá. V současné době občané využívají elektronický podpis vůči orgánům veřejné správy především v oblasti správy daní a v obecných správních řízeních.

Poř. č.	Udělena akreditace pro výkon činnosti akreditovaného poskytovatele certifikačních služeb
1.	První certifikační autorita, a. s., identifikační číslo 26 43 93 95, Podvinný mlýn 2178/6, PSČ 190 00 Praha 9
2.	Česká pošta, s. p. identifikační číslo 47 11 49 83, Olšanská 38/9, PSČ 225 99 Praha 3
3.	eIdentity a. s., identifikační číslo 27 11 24 89, Vinohradská 184/2396, PSČ 130 00 Praha 3

Tabulka 2 - Přehled udělených akreditací

5. OBJEKTOVÁ BEZPEČNOST

Objektová bezpečnost je složitým procesem, kterým se zajišťuje technické a personální zajištění ostrahy objektu tak, aby narušení, napadení nebo zcizení, respektive zničení kterékoli utajované a citlivé skutečnosti bylo eliminováno na minimum. Žijeme v době, kdy je jakékoliv napadení velice reálné z důvodů náboženských, ideologických, militantních a v neposlední řadě pro ryze zištné důvody. V obecném pojetí jde o vytvoření bezpečného prostředí pro daný subjekt. Pro návrh konkrétní ochrany musíme znát předmět a cíl ochrany. Realizace ochrany potom představuje návrh a sladění všech dostupných prostředků, které zajistí požadovanou nebo definovanou bezpečnost.

Ze systémového pohledu představuje bezpečnostní systém integrovaný celek, který zajišťuje:

- osobní bezpečnost – má nejvyšší prioritu
- informační bezpečnost
- majetková bezpečnost

V každé bezpečnostní oblasti se používají:

- mechanické ochrany (zábranné prostředky)
- elektronické ochrany (poplachové systémy)
- režimové ochrany (technicko-organizační opatření)

Ochrana objektu se zabezpečuje kombinací bezpečnostních opatření, kterými jsou:

- fyzická ostraha objektu
- klasická ochrana
- technická ochrana
- režimová opatření (ochrana)

Fyzická ochrana završuje veškeré snažení o ochranu svěřených hodnot. Na její úrovni závisí výsledná účinnost všech ostatních druhů ochrany. Všechny druhy ochrany jsou užitečné v závislosti od míry účinnosti reakce lidí. Bohužel personální situace ve fyzické ochraně objektů není nejlepší. Nedostatky v ní je potom nutné eliminovat vhodným režimovým a

technickým opatřením. Fyzická ochrana je ze všech nejzákladnější, proto je vhodné promyšleně kombinovat dostupné prostředky ochrany tak, abychom dosáhli co největší bezpečnosti chráněného zájmu. Fyzická ostraha objektu se zabezpečuje vyškolenými zaměstnanci provozovatele objektu, příslušníky ozbrojených sil nebo ozbrojených sborů nebo zaměstnanci pověřené bezpečnostní agentury. U důležitých objektů se fyzická ostraha objektu zajišťuje nepřetržitě. Fyzickou ostrahu objektu zajišťují na stanovišti určeném pro stálý výkon fyzické ostrahy objektu nejméně 2 pracovníci fyzické ostrahy objektu. Délka přístupové trasy od stanoviště určeného pro stálý výkon fyzické ostrahy objektu ke vstupu do nejvzdálenější zabezpečené oblasti by neměl být větší než 500 metrů. Na stanoviště určené pro stálý výkon fyzické ostrahy objektu bývají vyvedena výstupní hlášení technických prostředků. Provádění fyzické ostrahy objektu je upraveno bezpečnostními standardy.

Klasická ochrana je základem každého systému ochrany. V lepší či horší podobě se s ní setkáváme u každého objektu,byť jeho ochrana nebyla zatím vůbec řešena. Patří sem zdi, střechy, okna, dveře, zámky, trezory, mříže, nerozbitelná skla atd. Každý prostředek klasické ochrany je nutno posuzovat z hlediska času, po který vydrží odolávat kvalifikovanému napadení. Proto je v ochraně zaveden pojem průlomová odolnost MZS, který vyjadřuje jak dlouho je ochranný prostředek schopen odolávat napadení různými metodami a nástroji. Proto se prostředky klasické ochrany kombinují s ostatními druhy tak, aby se vzájemně doplňovaly a podporovaly.

Režimová ochrana je souhrnem organizačně administrativních opatření a sama nevyžaduje téměř žádné výdaje. I její role je však důležitá, protože je sjednocujícím a řídícím prvkem celého systému ochrany. Teprve kvalitně zpracované režimové směrnice a jejich důsledné dodržování mohou zajistit účinnou funkci ostatních druhů ochrany, včetně vzájemné součinnosti. Směrnice musí jednoznačně stanovit osobní zodpovědnost jednotlivých pracovníků objektu za určená bezpečnostní opatření, nebo prostředky, jejich dodržování a využívání. Součástí režimu jsou i veškeré pokyny pro návštěvníky, zaměstnance a pro strážní službu. Režimová opatření musí zahrnovat řádné využívání ostatních druhů ochrany a upravovat ostatní činnost personálu tak, aby byl objekt ochráněn co nejlépe. Jedná se tedy o postupy vedoucí k zabezpečení správných funkcí bezpečnostních systémů v rámci vnějších režimových opatřeních (vstupní a výstupní podmínky v rámci chráněné oblasti) a v oblasti

vnitřních režimových opatřeních (podmínky uvnitř chráněného objektu). Režimová opatření jsou tato:

- režim vstupu a výstupu osob a vjezdu a výjezdu dopravních prostředků, který stanoví oprávnění osob a dopravních prostředků pro vstup a vjezd do objektu, výstup a výjezd z objektu a způsob kontroly, stanovení podmínek a způsobů kontroly vynášení a vyvážení věcí nebo utajovaných skutečností z objektu
- režim pohybu osob, věcí, dopravních prostředků a utajovaných skutečností v objektu a jeho jednotlivých částech v pracovní a mimopracovní době
- režim manipulace s klíči, identifikačními prostředky a médii, které se používají pro systémy zabezpečení vstupů, kterým se zejména určuje systém a způsob označování, přidělování a odevzdávání klíčů, jejich úschovy a evidence, uložení duplikátů a způsob jejich použití
- režim manipulace s technickými prostředky a jejich používání

Vnější ochrana objektu je zajišťována souborem bezpečnostních opatření k zajištění ochrany hranice objektu, vstupů do objektu a ochrany nouzových cest a jiných průstupových a průlezných otvorů do objektu. V případě, že hranice objektu je zároveň i hranicí zabezpečené oblasti, se používají certifikované technické prostředky podle požadavků a kategorizace zabezpečených oblastí. V pracovní době mohou být, podle provozních podmínek, vyřazena některá bezpečnostní opatření použitá pro ochranu hranice objektu. V těchto případech se však činí opatření pro zabránění nepovolané osoby vstupu do objektu a seznámení se nejen s utajovanými skutečnostmi. V mimopracovní době se celá hranice objektu nepřetržitě zabezpečuje stanovenými bezpečnostními opatřeními. Nouzové cesty a jiné průstupové a průlezové otvory se zabezpečují v místě, kde protínají hranice objektu technickými prostředky.

Vnitřní ochrana objektu je zajišťována souborem bezpečnostních opatření k zajištění zabezpečených oblastí. Rozsah a podmínky zabezpečení vnitřní ochrany objektu stanoví statutární orgán provozovatele objektu v souladu s dokumentací objektové bezpečnosti. K zajištění ochrany zabezpečených oblastí se používají certifikované technické prostředky příslušných kategorií. Necertifikované technické prostředky lze použít pouze za předpokladu, že nesníží úroveň ochrany požadovanou pro daný stupeň utajení. Jednotlivé varianty

stavebního provedení hranice zabezpečené oblasti jsou uvedeny v bezpečnostních standardech.

Podoba technických prostředků k ochraně osob, majetku a dalších hodnot, po staletí výhradně mechanických, se s rozvojem lidské společnosti měnila. Spolu s rozvojem lidstva a rozvojem technických zkušeností a dovedností, společně s vývojem jednotlivých prostředků ochrany stejně jako s rozvojem organizace lidské společnosti. Pokrok zasáhl všechny druhy prostředků ochrany, avšak nejvíce patrný je v oblasti technických prostředků. Počítačové technologie zásadním způsobem ovlivnily celou oblast technických prostředků ochrany. Přesto i nadále v technické oblasti existují prostředky, které svými technickými principy a filozofií přístupu k řešení bezpečnosti zůstávají víceméně neměnné, avšak jejich technická úroveň se mění, protože mají vyšší odolnost a jejich násilné překonání je stále těžší. Vedle nich již ale existují technická řešení, která jsou založena na zcela nových technologických procesech a řešeních. Tato „stará“ a „nová“ řešení koexistují vedle se, navzájem se doplňují, a proto jsou v praxi často kombinována. [3]

Technickým prostředkem je bezpečnostní prvek, jehož použitím se zabraňuje, ztěžuje nebo oznamuje narušení ochrany objektu nebo zabezpečení oblasti. Nejjednodušší a také nejvíce užívané členění technických prostředků je jejich třídění podle základního technického principu, na kterém jsou zhotoveny. V tomto smyslu rozeznáváme dvě základní skupiny technických prostředků:

- mechanické zábranné prostředky
- elektrické a elektronické systémy

Technická ochrana má především odstrašující účinek a pachateli v ničem nezabrání. Plní ovšem dvě důležité úlohy: podporovat klasickou ochranu (dodat informaci o napadení a umožnit v čas fyzické ochraně zasáhnout) a úlohu zvyšovat efektivnost fyzické ochrany. Klíčovým momentem technické ochrany je přenos poplachového signálu do místa se stálou obsluhou.

Základní bezpečnostní systémy k ochraně majetku, osob a informací:

1) mechanické zábranné prostředky (MZS)
   - mříže

- zámky
- závory
- rolety
- úschovné objekty
- ploty
- bezpečnostní dveře
- bezpečnostní fólie a skla

2) elektrické a elektronické systémy
   - elektrická zabezpečovací signalizace (EZS)
   - elektrická požární signalizace (EPS)
   - kamerové systémy (CCTV)
   - vstupní systémy (ACCESS systémy)
   - komunikační systémy
   - pulty centralizované ochrany
   - systém kontroly strážní služby
   - prostředky pro detekci látek
   - technické prostředky proti aktivnímu a pasivnímu odposlechu
3) ostatní technické prostředky ochrany
   - prostředky k ochraně před požárem a únikem nebezpečných látek (kyslíkové masky, ochranné oděvy, hasicí přístroje, atd.)
   - zbraně určené k ochraně osob před útokem, ale i prostředky k osobní ochraně před zbraněmi (neprůstřelné vesty, kryty obličeje, helmy, atd.)
   - zařízení pro bezpečnou mobilní přepravu cenností a peněz (úschovné objekty, speciálně upravená osobní a dodávková vozidla)
   - prostředky k zadokumentování činnosti směřující proti chráněnému zájmu (chemické nástrahy, skryté audio nebo videomonitorování chráněného prostoru, atd.)
   - zařízení na fyzické ničení nosičů informací k ochraně informací a k jejich posílení (skartovačky, apod.)
   - zařízení k odeslání signálu v tísni
   - prostředky k ochraně provozu PC
   - prostředky k ochraně uložených dat na PC
   - prostředky k označení útočníka nebo odcizených předmětů

Při navrhování ochran platí tři základní pravidla:

- neexistuje absolutní ochrana (tzn. že každá ochrana může být překonána)
- jedna skupina ochran nic neřeší
- technické prostředky nenahradí člověka (na člověku zůstává ponecháno rozhodnutí, zda vyvolaný poplach je skutečné překonání ochrany, a všechny následné reakce)

Pro objektovou bezpečnost jsou nejdůležitější mechanické zábranné systémy, elektrická zabezpečovací signalizace, elektrická požární signalizace, kamerové systémy a systémy kontroly vstupu, jejichž stručný přehled je uveden v následujících podkapitolách.

5.1. Mechanické zábranné prostředky

Mechanické zábranné systémy (dále jen MZS) jsou historicky nejstaršími technickými zabezpečovacími prostředky. Jejich smyslem je zabránit nežádoucímu vniknutí do objektu, ať už tímto objektem je ohraničený volný prostor (pozemek) nebo budova, místnost či jen úschovný objekt, jako je skříň nebo trezor, případně dopravní pozemek.

Pro profesi bezpečnostních zábran je důležitý vývoj zámkařské techniky, datované od dob řecké a římské kultury. Nejvýraznější vývoj nastal až v 18. a 19. století, vývojem precizních zámků a úschovných objektů a ve 20. století, kdy se k mechanice připojila i elektronika. V průběhu vývoje zabezpečovací techniky vznikl samostatný obor zabezpečovací techniky, který se rozčlenil do tří sektorů: výrobu a rozvoj prostředků, montáž a instalaci, údržbu.

Mechanickými zábrannými systémy a prostředky se rozumí veškeré mechanické prvky, které ztěžují násilné vniknutí neoprávněných osob do chráněné zóny. MZS patří mezi základní pilíře objektové bezpečnosti.

Každý MZS je překonatelný v určitém reálném čase. Úkolem této zabezpečovací techniky je posunout tento časový termín do pásma bezpečnosti, tzn. do doby, kdy ohrožený zábranný systém je již pod další, například fyzickou kontrolou.

Hodnota času pro překonání MZS závisí na několika parametrech a to především:

- kvalita daného MZS,
- znalost pachatele o konstrukci překonávaného zařízení,
- umístění (instalace) MZS,
- druh a kvalita použité techniky (materiálu, nástrojů) pro překonání MZS,
- možnost použití jiných pomocných a vedlejších zdrojů (zásuvky el. proudu apod.).

Mechanické prvky MZS jsou kovové i nekovové prvky, jejich součásti a součásti jiných zařízení v objektu, které spolu tvoří komplex mechanické ochrany objektu.

Mechanické zábranné systémy tvoří páteř technického zabezpečení v průmyslu komerční bezpečnosti. Mechanické zábranné systémy dělíme do třech okruhů ochranných zón:

1) Obvodová ochrana - zajišťuje bezpečnost kolem chráněného objektu. Obvodem objektu rozumíme jeho katastrální hranice omezené obvykle přírodními nebo umělými bariérami (vodní toky, ploty, zdi apod.). Na přilehlých pozemcích zásadně se vždy jedná o mechanické zábrany vyráběné pro tento účel. Jedná se o skupinu vnějších mechanických zábran, které nejsou přímou součástí vlastního objektu (budova, místnost, dveře apod.), ale naopak jsou od něho prostorově vzdálené. Jsou na volné ploše, většinou na parcele objektu, a mnohdy vytvářejí nejen fyzickou, ale i právní hranici pozemku.
2) Plášťová ochrana - zabraňuje jakémukoliv narušení standardních, nestandardních vstupních jednotek objektu. V této oblasti hovoříme o veškerých prostředcích zajišťující bezpečnost celého pláště budovy. Jedná se o zabezpečení vstupu do všech stavebních otvorů v objektu: dveří, oken, balkónových oken, sklepních oken, vikýřů, zásobovacích a energetických šachet apod. V rámci plášťové ochrany jsou nejdůležitější dveře (což dokazuje i statistika míst průchodu pachatelů do objektu). Na druhém místě jsou potom hned okna, respektive všechny zasklené prostory staveb-

ních otvorů. Jedná se o bytová okna, garážová okna apod. a v neposlední řadě ochrana zbylých možných přístupových cest pro pachatele nacházejících se na plášti chráněných objektů.

3) Předmětová ochrana - zabezpečuje prostory či úschovná místa, kde jsou uloženy peníze, cennosti, utajované skutečnosti apod. před zcizením nebo neoprávněnou manipulací. Jedná se o prostředky, které mohou sloužit samostatně, převážně jako úschovné objekty, ale mohou být zařazeny i do předchozích systémů ochrany. Tyto prostředky jsou konečným místem pro úschovu finančních hotovostí, šperků, cenností, sbírek, cenných papírů a dokumentů. Musejí být proto na nejvyšším stupni ochrany bezpečnosti. Patří sem především mobilní i stabilní trezory, trezorové skříně, ohnivzdorné skříně, příruční pokladny, manipulační schránky, přenosné kontejnery a kufry.

Vztah ochrany mechanických a elektronických bezpečnostních zařízení. Jedná se o:

- ochranu klasickou – veškeré mechanické prostředky bránící vstupu do chráněného prostoru, nebo bránící manipulaci s chráněným předmětem
- ochranu fyzickou – zajišťovaná živou silou
- ochranu technickou – většinou elektronická zařízení schopná detekovat nežádoucí pohyb nebo činnost v chráněném prostoru a předat o tom informaci
- ochranu režimovou – soubor organizačních a administrativních opatření, sloužících jednak k zajištění účinnosti ostatních druhů ochrany, jednak ke sladění bezpečnostních pravidel a vlastního chodu zabezpečené organizace

Klasická ochrana je základem každého systému ochrany. V lepší či horší podobě se s ní setkáváme u každého objektu, byť jeho ochrana nebyla zatím vůbec řešena. Patří sem:

- zdi
- střechy
- okna
- dveře
- mříže
- trezory

- zámky
- nerozbitná skla atd.

Každý prostředek klasické ochrany je nutno posuzovat z hlediska času, po který vydrží odolávat kvalifikovanému napadení. Proto je v ochraně zaveden pojem průlomová odolnost MZS, který vyjadřuje jak dlouho je ochranný prostředek schopen odolávat napadení různými metodami a nástroji. Proto se prostředky klasické ochrany kombinují s ostatními druhy tak, aby se vzájemně doplňovali a podporovaly.

Fyzická ochrana završuje veškeré snažení o ochranu svěřených hodnot. Na její úrovni závisí výsledná účinnost všech ostatních druhů ochrany. Všechny druhy ochrany jsou užitečné v závislosti od míry účinnosti reakce lidí. Bohužel personální situace ve fyzické ochraně objektů není nejlepší. Nedostatky v ní je potom nutné eliminovat vhodným režimovým a technickým opatřením. Fyzická ochrana je ze všech nejzákladnější, proto je vhodné promyšleně kombinovat dostupné prostředky ochrany tak, abychom dosáhli co největší bezpečnosti chráněného zájmu.

Technická ochrana má především odstrašující účinek a pachateli v ničem nezabrání. Plní ovšem dvě důležité úlohy: podporovat klasickou ochranu (dodat informaci o napadení a umožnit včas fyzické ochraně zasáhnout) a úlohu zvyšovat efektivnost fyzické ochrany. Klíčovým momentem technické ochrany je přenos poplachového signálu do místa se stálou obsluhou.

Režimová ochrana je souhrnem organizačně administrativních opatření a sama nevyžaduje téměř žádné výdaje. I její role je však důležitá, protože je sjednocujícím a řídícím prvkem celého systému ochrany. Teprve kvalitně zpracované režimové směrnice a jejich důsledné dodržování mohou zajistit účinnou funkci ostatních druhů ochrany, včetně vzájemné součinnosti. Směrnice musí jednoznačně stanovit osobní zodpovědnost jednotlivých pracovníků objektu za určená bezpečnostní opatření, nebo prostředky, jejich dodržování a využívání. Součástí režimu jsou i veškeré pokyny pro návštěvníky, zaměstnance a pro strážní službu.

5.1.1. Průlomová odolnost

Jak bylo řečeno MZS mají svou zásadní nezastupitelnost zejména proto, že jsou schopny poskytnou ochranu objektu mechanickou odolností (pevností), kterou jednotlivé komponenty mají. Doba, kterou musí pachatel vynaložit na překonání mechanické pevnosti MZS se nazývá průlomová odolnost. Každý MZS je překonatelný, avšak rozlišnost jednotlivých MZS je dána množstvím vydané energie, času a druhu nářadí, kterých je třeba k překonání MZS. Tím je dána úroveň bezpečnosti jednotlivých objektů.

Postavení MZS u systému komplexního zabezpečení je dáno jejich schopností vytvořit kvalifikovanou zábranu proti průniku pachatelů do objektů chráněného zájmu, to je vyjádřeno maximálním prodloužením časového intervalu Δt, který pachatel potřebuje k překonání překážky a tím dosažení chráněného zájmu

$$\Delta t = t_2 - t_1 \text{ [min]} \qquad (4)$$

kde:

Δt časový interval potřebný k překonání překážky

t_1 čas zahájení útoku na překážku

t_2 čas konečného překonání překážky

Při stanovování minimální doby průlomové odolnosti MZS vycházíme z toho, zda se jedná o:

a) otvorové výplně
b) úschovné objekty

Pro otvorové výplně (dveřní a okenní uzávěry, mříže a vrata platí, že minimální čas potřebný pro překonání čili minimální doba průlomové odolnosti) je uveden v klasifikaci bezpečnostní třídy, tento čas je nutno 2-3 násobně navýšit neboť se jedná o zkouškový čas. Tím dostaneme čas reálný, za který lze otvorovou výplň zpravidla překonat. Tento čas aplikujeme i pro jednotlivé komponenty dveřních a jiných uzávěrů.

Doby průlomové odolnosti vlastní mříže jako takové a doby průlomové odolnosti zámku nebo použití klasifikací podle nižší bezpečnostní třídy obou těchto komponentů jsou tzv. principem kritických míst).

U úschovných objektů je nutno zjistit minimální dobu průlomové odolnosti výpočtem. Ten provádíme podle vzorce:

$$T_{vloupání} = [(V_R - B_V):C_1]x(2\div3)\ \ [min.R_U;\ R_U/min] \qquad (5)$$

Vychází se z typu úschovného objektu (komorový nebo skříňový trezor) klasifikované bezpečnostní třídy daného výrobku a poté z odpovídajícího počtu odporových jednotek R_U, které konkrétní typové odzkoušený výrobek vykázal při fyzických zkouškách.

Legenda vzorce:

$T_{vloupání}$	doba minimální průlomové odolnosti úschovného objektu
V_R	hodnota průlomové odolnosti úschovného objektu - u skříňového trezoru je rovna průměrné hodnotě částečného a úplného průlomu, u trezorových dveří a komorového trezoru jde o hodnotu pro úplný průlom
B_V	základní ocenění: číselná hodnota přidělená určitému nářadí
C_1	koeficient průlomové odolnosti úschovného objektu
$2\div3$	koeficient navýšení

Odolnost MZS proti vloupání se stanoví na základě počtu odporových jednotek R_U, které určíme na podkladě typových fyzických zkoušek úschovného objektu za použití příslušné kategorie nářadí či nástrojů. Zkušební vzorek se musí skládat z prvků, které mají všechny pro zkoušku potřebné spáry a spojení podstatné pro zkušební účely.

5.1.2. Stupně rizika ohrožených objektů

Charakteristickým znakem dané zábrany je její bezpečnostní úroveň, reprezentovaná pasivní bezpečností, resp. průlomovou odolností. Za obecně kvantitativní ohodnocení překážky považujeme časový interval, který pachatel potřebuje k jejímu překování

$$R = T_{vloupání} : t_i > 1 \qquad (6)$$

kde:

R	stupeň rizika ohrožení objektu (koeficient rizikovosti)
$T_{vloupání}$	doba minimální průlomové odolnosti úschovného objektu
t_i	čas potřebný k zásahu policie, bezpečnostní služby

Skutečné riziko ohrožení chráněného zájmu bude tím menší, čím bude koeficient R větší. Má-li být aplikovaná ochrana účelná, musí být jeho hodnota větší než 1. Bude-li rovna 1 nebo menší, nemůžeme hovořit o jakékoliv efektivitě ochrany. Naopak, čím bude tento koeficient větší, tím se bude riziko ohrožení snižovat a systém zabezpečení chráněného zájmu bude kvalitnější.

5.2. Elektrická zabezpečovací signalizace

Zařízení elektrické zabezpečovací signalizace je soubor detektorů, tísňových hlásičů, ústředen, prostředků poplachové signalizace, přenosových zařízení, jejichž prostřednictvím je opticky nebo akusticky signalizováno na určeném místě narušení střeženého objektu nebo prostoru. Jednotlivé komponenty tohoto systému plní své specifické funkce a vytvářejí tzv. zabezpečovací řetězec.

Rozdělení prvků EZS:

1) prvky plášťové ochrany
    - magnetické kontakty
    - detektory na ochranu skleněných ploch
    - mechanické kontakty
    - vibrační detektory
    - poplachové fólie, tapety, polepy
    - drátové detektory
    - rozpěrné tyče
2) prvky tísňové ochrany
    - veřejné tísňové hlásiče
    - skryté tísňové hlásiče
    - osobní tísňové hlásiče
    - automatické tísňové hlásiče
    - speciální tísňové hlásiče
3) ovládací zařízení
    - blokovací zámky

- spínací a propouštěcí zámky
- kódové klávesnice
- ovládací a indikační díly

4) poplachové ústředny EZS
   - klasické smyčkové ústředny
   - ústředny s přímou adresací
   - ústředny smíšeného typu
   - ústředny s bezdrátovým přenosem od detektorů
5) signalizační (výstražná) zařízení
   - zábleskový maják
   - siréna
6) prvky prostorové ochrany
   - pasivní infračervené detektory
   - aktivní infračervené detektory
   - ultrazvukové detektory
   - mikrovlnné detektory
   - kombinované duální detektory
7) prvky předmětové ochrany
   - otřesové detektory
   - detektory na ochranu zavěšených předmětů
   - kapacitní detektory
8) speciální detektory
   - tlakové detektory
   - nášlapné koberce
9) prvky venkovní obvodové ochrany
   - mikrofonické kabely a infračervené závory a bariéry
   - mikrovlnné bariéry a štěrbinové kabely
   - zemní tlakové hadice a perimetrické pasivní infračervené detektory
10) přenosová zařízení
   - automatické telefonní hlásiče a voliče
   - bezdrátová přenosová zařízení

Prvky plášťové ochrany slouží k hlídání otevření, destrukce prostorů pláště budovy (oken, vrat, dveří).

Prvky prostorové ochrany se dělí na:

- detektory pasivní - při zjišťování charakteristických rysů napadení pouze registrují fyzikální změny ve svém okolí
- detektory aktivní - při zjišťování charakteristických rysů napadení vytvářejí své pracovní prostředí aktivním působením na své okolí a detekují změnu takto vytvořeného fyzikálního prostředí

Každý z těchto detektorů využívá ke své funkci odlišnou část kmitočtového spektra elektromagnetického vlnění. Doplňkovou funkcí těchto detektorů může být tzv. funkce ochrany proti zastínění (antimasking). Tato funkce je aktivní v době klidu objektu a slouží k indikaci zastínění čidla.

Pro prvky předmětové ochrany je možno využít celé řady prvků určených původně pro jiné účely, např. magnetické kontakty, PIR detektory, mikrovlnné detektory, infračervené závory, optoelektronická detektory a podobně. Specifickou skupinou předmětových detektorů jsou detektory závěsové a polohové na ochranu uměleckých děl a předmětů. Jedná se o otřesové (seismické) detektory pracující na principu selektivního zpracování vlnění, jež se šíří pevnými tělesy při jejich mechanickém nebo termickém opracovávání. Nejnovější typy využívají při své činnosti digitálního zpracování signálu. Detektory na ochranu uměleckých předmětů jsou určena pro střežení předmětů zavěšených ve výstavních síních, galériích a podobně.

Prvky venkovní obvodové ochrany - jedná se o detektory, které chrání, resp. signalizují narušení vnějších částí u rozlehlých objektů, komplexů budov nebo továren na samostatném pozemku. Vzhledem k dimenzím venkovních prostor se liší od čidel pro vnitřní použití především v dosahu (řádově o 100 m). Problémem venkovního zabezpečení je velké množství podnětů, na které by neměla čidla reagovat. Jedná se o:

- vlnění travního porostu
- pohyb listí a větví stromů a keřů

- vibrace oplocení ve větru
- proudění vzduchu
- vítr
- sníh a déšť
- pohyby různých druhů zvěře
- dopravní ruch v blízkosti hranice pozemku

Podněty, které se svým charakterem přibližují situaci narušení, není možno nikdy zcela eliminovat. Z tohoto důvodu se často kombinuje systém venkovní perimetrické ochrany se systémem průmyslové televize (CCTV).

Doplňková zařízení ústředen EZS (základní):

- akustická signalizace
- optická signalizace
- grafické tablo
- tiskárny
- zařízení určená pro informování majitele objektu

5.3. Elektrická požární signalizace

Zařízení elektrické požární signalizace (dále jen EPS) představuje soubor hlásičů požáru, ústředen EPS a doplňujících zařízení EPS. Tento soubor tvoří systém, kterým je opticky nebo akusticky signalizováno ohnisko požáru nebo již vzniklý požár. Takový systém může mimo jiné rozšiřovat informace o požárně nebezpečné situaci na určená místa, ovládat zařízení bránící požáru nebo usnadňující či případně provádějící protipožární zásah a v neposlední řadě může zaznamenávat informace o stavech signalizovaných ústřednou EPS. Zařízení EPS slouží ke včasné signalizaci vzniklého ohniska požáru a výrazně urychluje předání této informace osobám určeným k zajištění konkrétního zásahu, eventuelně uvádí do chodu zařízení bránící šíření požáru nebo provádějí protipožární zásah.
Hlavní úkoly EPS je :

- rychlé a spolehlivé určení místa požáru

- vyhlášení poplachu
- aktivace a řízení evakuačního systému
- realizace automatické komunikace s HZS

Základní rozdělení EPS:

- konvenční EPS
- adresné EPS
- analogové EPS
- interaktivní EPS

Požární hlásiče EPS můžeme podle principu činnosti rozdělit na:

- manuální - tlačítkoví hlásiče
- automatické požární hlásiče
    - hlásiče ionizační
    - hlásiče optické
    - hlásiče tepelné
    - hlásiče tlakové
    - hlásiče odporové
    - hlásiče kouřové
    - hlásiče vyzařování
    - hlásiče kombinované

Ústředna EPS je zařízení, která soustřeďuje informace ze všech hlásičů k systému připojených. Informace z nich patřičným způsobem podle programu a nastavení zpracovává a reaguje na ně odpovídajícím způsobem odezvou (vyhlášení poplachu, přenos signálu na PCO, aktivace samočinných hlásicích zařízení a podobně).

Druhy ústředen EPS:

- konvenční neadresné
- konvenční adresné
- analogové
- interaktivní

Mezi doplňující zařízení EPS patří signalizační zařízení, signalizační panel, orientační tablo, indikační jednotka, signalizační prvky (zvonky, houkačky, sirény, světelné majáky), ovládací jednotka, zařízení dálkového přenosu, registrační jednotka a řídící jednotka.

Zařízení pro přenos požárního poplachu je zařízení, které zprostředkuje přenos poplachového signálu z ústředny elektrické požární signalizace do ohlašovny požáru. Tento přenos může být buď místní a nebo dálkový, kdy v případě že v objektu není stálá obsluha probíhá dálkový přenos na PCO HZS.

5.4. Kamerové systémy

Uzavřené televizní střežící a dohledové systémy (dále jen CCTV) jsou vysoce účinným prvkem zabezpečení objektů. Výrazným způsobem znásobují možnosti fyzické ostrahy objektu tím, že jsou schopny monitorovat současně množství střežených prostor, umožňují obsluze vidět, co se ve střeženém prostoru děje a v případě jakéhokoli narušení je trvale dokumentovat. Kamerové systémy jsou používány při ochraně velkých průmyslových a dopravních komplexů, ve velkoprodejnách, bankách, na benzinových čerpadlech, ale i v různých institucí nebo menších firmách.

CCTV se používají buď autonomně nebo jako doplňková zařízení pro akustickou a vizuální kontrolu objektů. Celý kamerový systém je složen z několika částí:

- z části zajišťující snímání obrazu
- z části zajišťující přenos obrazu (signálu)
- z části zobrazující přenesený signál
- z ovládací části
- z příslušenství

Z hlediska bezpečnostních funkcí slouží kamerové systémy především ke sledování určeného prostoru, dále k dokumentaci nežádoucího jednání a k identifikaci osob při jejich vstupu do objektů. Jejich nasazení bez současného nasazení ostatních prostředků ochrany

nemá žádný větší význam pro zabránění průniku nepovolané osoby do objektu nebo alespoň zpomalení takového průniku.

Kamerové systémy jsou progresivní prostředky zabezpečovací techniky a velmi účinně násobí schopnosti člověka při výkonu ostrahy objektů a jsou tudíž nepostradatelným článkem ochrany. Mají i určitý psychologický vliv na potenciální pachatele samotnou svou existencí v místě, které mají spoluochraňovat, mohou případného pachatele od nežádoucího jednání odradit. Jejich výhody spočívají v přenosu nezkreslené informace v reálném čase a době obsluze v podobě, která je naprosto srozumitelná a kterou je možné nezkresleně zadokumentovat. Při jejich použití v praxi nesmíme zapomenout, že pro ně platí stejné zásady jako pro ostatní technické prostředky zabezpečení, tedy:

- jejich plná funkce a přínos je zabezpečen jen v kombinaci s dalšími zabezpečovacími prostředky
- jejich nasazení by měla předcházet důkladná bezpečnostní analýza střeženého objektu
- před jejich realizací by měla být předem zvážena možnost postupného rozšiřování kamerového systému
- kvalitní kamerové systémy jsou výsledkem a musí být současně zastoupeny těmito třemi složkami kvality:
    - kvality jednotlivých komponentů systému
    - kvality provedení projekčních, montážních a servisních prací
    - kvality obsluhy systému

5.5. Systémy kontroly přístupu a vjezdu a docházkové systémy

Smyslem použití těchto technických prostředků je regulace vstupu do střežených objektů. Systémy umožňují rozlišit jednotlivé vstupující osoby, případně vjíždějící vozidla a automaticky zabránit vstupu nebo vjezdu neoprávněných subjektů do objektu nebo umožňují regulovat pohyb osob a vozidel po objektu způsobem předem zvoleným. V řadě případů tyto systémy plní taktéž funkce doplňkové (např. evidence docházky zaměstnanců, shromažďování informací pro mzdovou agendu, atd.).

Princip těchto systémů spočívá ve schopnosti přečíst pomocí speciálních zařízení – čteček zakódované pokyny a oprávnění osob a vozidel ke vstupu (vjezdu) do objektu a jejich pohybu uvnitř objektu. Informace (pokyn) pro vstupní systémy je zpravidla zakódován na identifikačních kartách., na které je zanesen na magnetickou stopu nebo je uložen v čipu. Samotné čtecí zařízení a identifikační karta by však nebyla dostatečně účinná, kdyby objekt nebyl chráněn systémem různých zábran, které neoprávněné osobě nebo neoprávněnému vozidlu fakticky znemožní vstup nebo vjezd do objektu. Proto jsou tyto vstupní systémy napojeny na různé typy zábran, které podle příkazu z karty vstup pro příchozího uvolní či nikoli. Pro zvýšení bezpečnosti mohou být tyto systémy navíc kombinovány i se zadáním hesla při vstupu do chráněných prostor nebo v kombinaci s biometrickými čtečkami apod.

Kvalitně vybudovaný přístupový systém v objektu umožňuje objekt rozdělit do jednotlivých zón podle různých kritérií. Následně je pak možné cizím osobám i vlastním zaměstnancům předem stanovit přístup do určitých částí podniku a naopak do jiných jejich částí vstup omezit (přístup zamítnout). V některých objektech potom pohyb cizích osob může být umožněn pouze v doprovodu průvodce. Díky využití softwarového vybavení je možno tyto systémy provázat s dalšími bezpečnostními systémy a to především EZS a CCTV.

6. KONKURENCE

Konkurence na náročných trzích velmi často způsobuje, že firma, která byla v minulosti úspěšná, musí po určité době své těžce vydobyté místo na trhu postoupit jiné, úspěšnější firmě. Každá firma prosazující se na trhu definuje své poslání, tedy svůj cíl podnikání, kterého chce dosáhnout na určitém trhu za určitý časový úsek. Na základě těchto vytyčených cílů si podnik vytváří svou firemní strategii ke splnění těchto cílů s ohledem na měnící se faktory jak vně, tak uvnitř firmy.

Všeobecně platí, že úspěch firmy závisí na schopnosti řešení problémů týkajících se jejího okolí, jako je např.:

- správná identifikace skutečných potřeb zákazníků s následným kvalitním uspokojením těchto potřeb v jednotlivých tržních segmentech
- co nejpřesnější odhad vývoje marketingového prostředí firmy a schopnost jeho ovlivnění
- působení konkurenčních firem na trhu
- předpověď vývoje makroekonomických faktorů

Konkurenční prostředí je ve své podstatě nepřátelské a základním cílem každé firmy je v tomto prostředí přežít, tedy být konkurenceschopná. Konkurenceschopnost je schopnost soustavně odhalovat vyjádřené nebo latentní potřeby spotřebitelů a tyto potřeby uspokojovat při realizaci zisku. Pojem konkurence se s postupem času stále rozšiřuje a zahrnuje soupeření mezi existujícími konkurenty, hrozby nových konkurentů a hrozby náhrady za produkt, dále je to schopnost vyjednávat s dodavateli a v neposlední řadě schopnost jednat s klienty. Konkurenční prostředí je stále agresivnější díky rostoucímu podílu vyspělých technologií, které jsou spojeny s rozsáhlými výdaji na výzkum a vývoj, mají rychlý inovační cyklus a jsou globální. Konkurenční zpravodajství je pro firmu jakýmsi radarem umožňujícím jí neustále konkurenční prostředí sledovat, změny včas identifikovat a jejich důsledky buď využít nebo se jim včas vyhnout a předejít tak krizi.

6.1. Konkurenční zpravodajství – competitive intelligence

Competitive Intelligence (dále jen CI) je systematický, legální a etický proces sbírání, zjišťování, sledování, analýzy a organizování informací o konkurenčních firmách, ekonomickém prostředí a vlastní firmě, které jsou následně analyzovány tak, aby pomohly odhalit slabé a silné stránky konkurence, rozpoznat její strategické záměry a provést správné strategické rozhodnutí, které pomůže zvýhodnit firmu oproti ostatním konkurentům. Velmi dobrým českým překladem termínu CI je výraz "konkurenční zpravodajství". CI v žádném případě nemá nic společného se špionáží, ba naopak, uvádí se, že cca 95% vstupních informací pochází z otevřených informačních zdrojů.

CI představuje významnou oblast, kde se role nových médií a technologií velmi rychle projevila (tedy i role internetu). Svým způsobem je CI ve své nejdokonalejší podobě týmovou prací, na které se nemusí podílet jen expert ve vlastní sféře obchodu a marketingu, ale i lidé z výzkumu nebo informační specialisté.

Co se myslí pod CI je možné říci i následujícími shrnujícími body:

- procesy analýzy a syntézy dat, resp. i informací, které se transformují do strategické znalosti,
- shromažďování informací o konkurenci, kdy tyto informace jsou různých typologií a dohromady skládají mozaiku obrazu o konkurenci,
- rovněž informace z okolí sledovaných subjektů: trh, stát, právo a legislativa, politické a demografické souvislosti (např. při investičních průnicích na neznámé, vzdálené, či dokonce exotické trhy).

Každý v oblasti obchodního světa potřebuje CI. Nezáleží, zda je to marketingový odborník, obchodník, pojišťovací agent, expert strategického plánování nebo prezident společnosti. Ti všichni jsou nuceni provádět neustálý průzkum trhu, sledovat konkurenci, vyhodnocovat firemní informace, informace o trzích, příležitostech i neúspěších. Shromažďování informací o konkurenci je součástí obchodních strategií. Firmy potřebují mít srovnání s jinými a mít přehled o chování a cílech konkurence, aby se předcházelo např. nepříjemným překvapením, případně se vzdálit dopředu konkurenci v podobě vyšších zisků, získaní nových

trhů apod. Pracuje se s jistými metodami, ale jejich charakter má být vždy legální. Informační zdroje a služby, kterými se v příspěvku proto zabýváme, také nesou pojmenování veřejně přístupné informační služby a veřejně přístupné informační zdroje.

CI odpovídá např. na tyto následující otázky:

- aktivity konkurentů na trhu
- silné a slabé stránky konkurence
- plánované uvedení nových výrobků konkurentů na trh
- formy komunikace směrem k zákazníkům využívané konkurencí
- trendy na trhu a v jednotlivých segmentech trhu

Nejvíce se CI uplatňuje v oborech s vysokým stupněm koncentrace konkurenčních subjektů, tedy:

- farmacie
- telekomunikace
- finanční sektor
- výrobci zboží dlouhodobé spotřeby

CI se odehrává ve třech rovinách:

- obranné konkurenční zpravodajství – ochrana vlastních informací, dat, počítačových a komunikačních systémů podniku. Je to zpravidla jedna z bezproblémových oblastí zpravodajství, kdy jde o svépomocnou a zcela legitimní a oprávněnou ochranu vlastních zájmů
- ofenzivní konkurenční zpravodajství – získávání, shromažďování, třídění a analýza informací potřebných pro podnikání včetně informací o konkurenci, marketingových informací, atd.
- vlivové (lobbyistické) konkurenční zpravodajství – systém opatření a protiopatření k ovlivňování vlastních kroků, kroků obchodních partneru, kroků konkurence a ostatních činitelů na trhu.

6.1.1. Zdroje informací pro CI

I. Otevřené (veřejné) zdroje – dostupné bez porušení právních nebo etických norem

1) Nepublikované zdroje se shánějí speciálními metodami, dá se říct, že využíváme metod primárního marketingového průzkumu. Tyto informace nejsou snadno dostupné, ale za určitých podmínek mohou být poskytnuty nebo uvolněny s vědomím zdroje.
2) "Polopublikované" zdroje (grey literature) - dokumenty typu výzkumných zpráv, technických zpráv, speciálních analýz různých institucí a center, disertací, konferenčních materiálů apod. Dokumenty nejsou publikovány, resp. zveřejněny klasickou cestou vydavatelského domu.
3) Publikované informace nalézáme v nejrůznějších zdrojích, a to buď v podobě zdrojů tištěných nebo elektronických (např. báze dat v databázových centrech, které mohou být plnotextové, faktografické nebo bibliografické). Takovými publikovanými dokumenty mohou být výroční zprávy, brokerské zprávy, zpravodajské články z ekonomického tisku, statistiky, patenty, odborné časopisy, konferenční materiály a mnohé další druhy informačních pramenů.

II. Uzavřené (neveřejné) zdroje – jejich získávání nebo použití je nelegální nebo neetické

1) Důvěrné (privátní) zdroje – bez ohledu na způsob a obtížnost získání je lze získat pouze bez vědomí zdroje.
2) Chráněné (tajné) zdroje – jejich získání je možné pouze porušením zákona nebo překonáním zdrojem prováděné ochrany.

Kategorizace (nejen on-line) přístupných informací může být různorodá a pojata z odlišných pohledů tak, aby nám získaná informace pomohla při kompletaci celkové mozaiky. Mohou to být:

- finanční, kreditní a bankovní informace (viz dále)
- přehledy, katalogy, rejstříky firem
- burzovní zprávy (včetně hodnocení brokerskými společnostmi)
- tiskové zprávy a další zpravodajské texty
- zprávy popisující trhy, průmyslová odvětví
- informace o výrobcích
- informace zaměřené na spotřebitele (vč. výsledků testů výrobků)

- informace o osobnostech oborů
- encyklopedické a výkladové zdroje
- záležitosti intelektuálního vlastnictví (ochranné známky a patenty)
- jiné materiály právního a legislativního typu
- konferenční materiály, materiály z veletrhů, výstav (resp. o nich retrospektivně i dopředu)
- zdroje tendrů, projektů a dalších nabídek
- demografické informace
- informace vázající se k teritoriím a poskytující charakteristiky zemí
- politologické prameny
- demografické informace
- sociologické informace
- psychologické zdroje (např. informace o chování spotřebitele)
- a jiné

Cestu k informacím může zprostředkovat databáze, databázové centrum, internet, informační specialista, odborné i některé veřejné knihovny v regionech, firmy provádějící marketingové průzkumy, obchodní komory, báze dat na CD-ROM a jiných nosičích, lidský faktor apod..

Velkou roli v oblasti CI sehrávají také kreditní, kancelářské a bankovní informace, které dotvářejí celkovou mozaiku o konkurentovi, resp.o celém prostředí trhu našeho zájmu.
Obsahem kancelářské informace obvykle bývají tyto údaje:

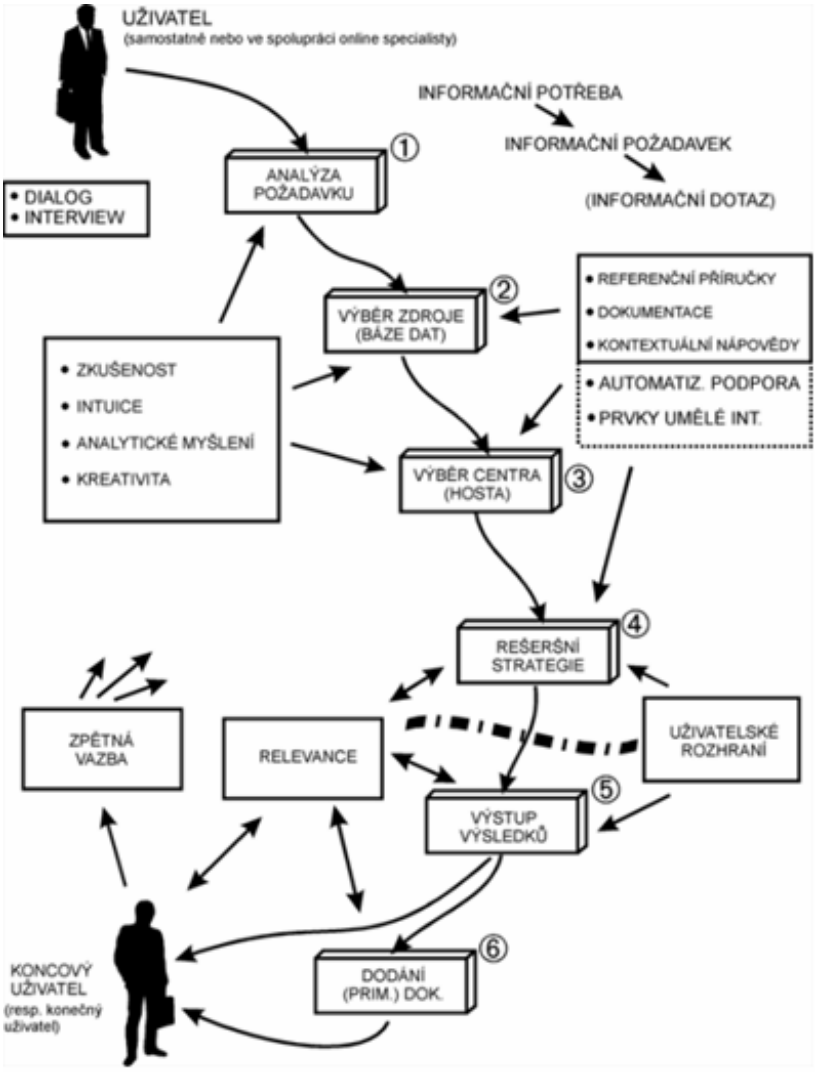
- název, adresa, kontaktní spojení
- identifikační číslo
- obor činnosti
- popis činnosti (výrobkové skupiny)
- základní informace o managementu (jména, funkce, pozice)
- počet zaměstnanců
- vlastnická forma
- dceřiné společnosti
- roční obraty a zisky (i za několik let)
- podíl exportu

- bankovní spojení

Kreditní informace patří mezi vyšší typ informace obsahující určité ohodnocení od producenta zdroje nebo auditorské firmy. Bývají v uzavřených okruzích a přístup k nim může být umožněn jen omezenému počtu subjektů, nebo mohou být uchovávány uceleně v databázových centrech. Kreditní informace nás informují pomocí hodnocení (vyjádřeného v určité škále nebo kódu) o bonitě firmy, jejím předpokládaném vývoji a také nám udávají závěr v podobě doporučení nebo nedoporučení obchodního spojení. Posledním druhem informací pro CI jsou bankovní informace shromažďované bankami, čímž jsou tedy i pod jejich ochranou. Tyto informace nejsou veřejně vystavovány v žádném centru, ale mohou být na požádání za dodržení velmi přísných pravidel dle bankovní etiky zpřístupněny. Bankovní informace tedy obsahují kromě kancelářských informací také finanční hodnocení firmy upozorňující na stav konta, platební morálku, celkovou bonitu klienta atd. Uvedeny mohou být také doplňující informace např. o emisi cenných papírů nebo exportní údaje.

Další odlišnost je v tom, že CI využívá hlavně tzv. sekundárních zdrojů. Termín sekundární zde nelze chápat jako něco podřadného, protože CI shromážděním dostatečného množství informací a dat sekundárního charakteru o tom, co dělá, jak si počíná a co chystá konkurence, může získat stejně potřebné poznatky jako průmyslová špionáž, a navíc to je často za kratší dobu, podstatně levněji a bez rizika, že někdo bude obžalován, souzen a uvězněn, když bude odhalen jako průmyslový špion.

Primárním zdrojem je průzkum trhu, který představuje dotazování, pozorování, testování, shromažďování a analyzování informací prostřednictvím osobního kontaktu s respondenty průzkumu nebo prostřednictvím výrobků konkurence. Klasickým příkladem může být shromažďování různých forem zpětných vazeb, statistik, názorů, připomínek (telefonické rozhovory, dotazníky). Zajímavou metodou je pak testování výrobků a jejich parametrů.



Obrázek 17. Proces vyhledávání znalostí pro CI

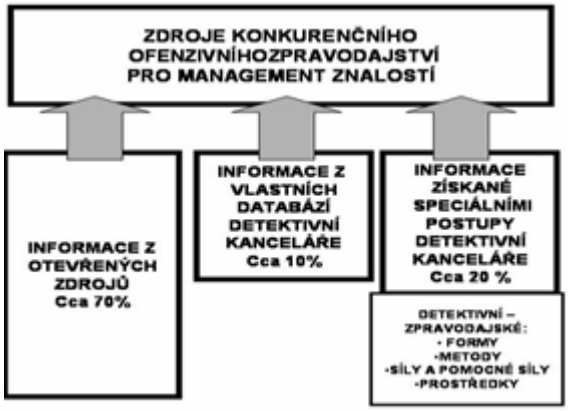
6. 2. Ofenzivní (aktivní) konkurenční zpravodajství

Úkolem ofenzivního zpravodajství je odhalit strategii konkurence a využít ji ve prospěch vlastního podniku, zajistit informace marketingového charakteru a další informace potřebné pro podnikání. Informace je ale prvním stupněm činnosti, cílem je znalost. Jde o to odhalit nebezpečí spojená se zahájením určité výroby, uskutečněním určitých obchodů, využití nové technologie, či se vstupem na nový trh apod. Dále je nutné příslušná nebezpečí paralyzovat či využít vůči konkurenci. Informace získané ofenzivním konkurenčním zpravodajstvím mohou využívat vedle vrcholového managementu podniku i střední manageři. Dopomohou jim nejen k ochraně vlastních podnikatelských subjektů a jeho záměrů, ale i

k možnosti přijmout opatření a protiopatření k tomu jak zvítězit nad konkurencí. Správné zadání úkolu ofenzivního konkurenčního zpravodajství je polovinou úspěchu. Popisuje konkrétní neznalost a umožňuje soustředit úsilí na hledání správných odpovědí. Konkurenční zpravodajství musí být cestou (nástrojem,prostředkem) k dosažení znalosti.

Veškeré zdroje použitelné pro ofenzivní konkurenční zpravodajství můžeme získat:

- z otevřených zdrojů
- ze specializovaných činností aktivního konkurenčního zpravodajství (jde např. o informační proniknutí do prostředí konkurence, provádění utajených pozorování při zkouškách prototypů či zavádění nové výroby či technologie konkurencí, infiltraci cílených informací a dezinformací do prostředí konkurence apod.)



Obrázek 18. Zdroje ofenzivního konkurenčního zpravodajství

Podnikatelské zpravodajství směřuje k zajištění dostatečného množství a kvality informací potřebných pro podnikání a k provedení potřebných opatření k ovlivnění podnikatelského prostředí ve prospěch podnikání. Podnikatelské informace jsou ty, které ovlivňují výzkumné, technologické, výrobní, obchodní a jiné rozhodování a procesy. Týkají se především vzájemných vztahů fyzických i právnických osob k podnikatelským aktivitám a v podnikatelských aktivitách, jejich vzájemného působení, potřeb, zájmů, cílů apod.. Nutnost ofenzivního konkurenčního zpravodajství vyplývá z toho, že:

- soustavně a průběžně dochází ke změnám podnikatelského prostředí
- neustále narůstá množství a různorodost informací, které na podnikání a podnikatelské aktivity působí a mají bezprostřední či zprostředkovaný vliv

- podnikání a podnikatelské aktivity probíhají v prostředí ostrého konkurenčního boje, a formy, metody a prostředky konkurenčního působení nemusí být vždy zcela korektní

Do uvedené problematiky ofenzivního konkurenčního zpravodajství řadíme především:

- informace a lobbying marketingového charakteru
- informace a lobbying v prostředí obchodních partnerů
- informace a lobbying v celém okruhu konkurenčních subjektů

Informace potřebné a nezbytné pro vlastní podnikání, které je třeba získávat ofenzivním konkurenčním zpravodajstvím se především týkají:

a) informací z oboru podnikání – výzkumné a vývojové, výrobní a technologické, ekonomicko politické
b) informace o trhu a konkurenci – informace o obchodních partnerech, stavu a trendu vývoje trhu, činnosti a trendech konkurence, …
c) informace ekonomické – informace o ekonomických výsledcích konkurence, o vývoji ekonomických vývojových trendu, …
d) informace právní – informace o vývoji a přípravách změn právní úpravy související s podnikatelskými aktivitami
e) informace organizační (včetně informačních systémů) – stav a trendy vývoje organizačních a informačních systémů obecně i u konkurence
f) informace personální – informace o pracovnících vlastního podniku a pracovnících konkurence, o vlastních a konkurenčních obchodních partnerech
g) specifické informace – bezpečnostní politika a situace, vojenská politika a její trendy, zahraniční politika a její trendy

6.3. Obranné konkurenční zpravodajství

První a nezastupitelnou zásadou, prvořadým požadavkem a také základním atributem každého konkurenčního zpravodajství je zabezpečení komplexní ochrany vlastní společnosti. Bez zabezpečení vlastní ochrany podnikatelského subjektu nemohou být účinná ani opatře-

ní ofenzivního (aktivního) či vlivového zpravodajství. Obranné podnikatelské zpravodajství je nutno, v rámci detektivní ochrany ekonomických zájmů, realizovat i tam, kde nejsou realizována další opatření ofenzivního či vlivového podnikatelského zpravodajství. Nerespektování této zásady způsobuje podnikatelskému subjektu vážné a zpravidla nevratné problémy. V této souvislosti jde i o zajištění dalších forem ochrany. Celkově v obranném konkurenčním zpravodajství jde o zajištění těchto prvků ochrany informací (viz kapitola 4.):

- personální bezpečnosti
- informační bezpečnosti
- režimová informační bezpečnost
- bezpečnost technických prostředků
- bezpečnost programových (softwarových) prostředků
- bezpečnost dat
- bezpečnost komunikačních systémů a cest
- fyzická ochrana informační bezpečnosti
- aktivní ochrana proti úniku informací a dat

Obranná složka konkurenčního zpravodajství má svůj subsystém:

- soukromé detektivní činnosti
- speciální bezpečnostně technické a softwarové ochrany
- režimová opatření

Obranná složka konkurenčního zpravodajství se musí v podniku odehrávat v těchto rovinách:

- rovina vlastní firemní personální bezpečnosti – zabránit kontaktování a vytěžování zaměstnanců podniku konkurencí, zabránit fingovaným zaměstnáním konkurenčního zaměstnance (zaměstnanec vyslaný konkurenční firmou do naší), zabránění získání informací konkurencí pomocí korupce, vydírá apod.
- rovina ochrany proti útokům na bezpečnost informací, dat, komunikačních a počítačových systémů – zabránění přímé krádeži počítačových nosičů informací, jejich nelegálnímu kopírování, technickému získávání informací z počítačových sítí a zabránit technickými prostředky odposlechům vyzařování počítačových monitorů

- rovina odposlouchávání a sledování nelegálními prostředky – nelegální využití audio, video, audio-video a dalších speciálních prostředků zpravodajské techniky konkurencí
- rovina přímého narušení vlastnických práv
- rovina získávání informací o útvarech konkurence zabývajících se podnikatelským či komerčním zpravodajstvím

Jak jsem již uvedla výše, obranná složka systému konkurenčního zpravodajství je významným a nezastupitelným subsystémem v celkovém systému situační a sociální prevence negativních jevů. Informace jsou významným a značně ceněným zbožím. Účinné zajištění ochrany podniku před únikem informací je možno docílit jen formami, metodami a prostředky detektivní činnosti doplněnými využitím speciálních technických prostředků. Stěžejní a rozhodující je lidský faktor. Rozhodující úlohu zde potom sehrávají soukromé detektivní služby (např. personální agentury) a jsou rozhodujícím subsystémem ochrany ekonomických zájmů v podniku.

6.4. Vlivové konkurenční zpravodajství

Vlivové zpravodajství je v podstatě zajišťování lobbyingu v návaznosti na předchozí roviny konkurenčního zpravodajství (obranné, ofenzivní) v návaznosti na rozhodnutí managementu znalostí. Vlivové zpravodajství představuje proces, v němž pracovník konkurenčního zpravodajství (soukromý detektiv) prosazuje (vytváří) vhodné prostřední a podmínky pro realizaci rozhodnutí podnikatelského subjektu. Vlivové zpravodajství je tedy pokračováním knowledge managementu (managementu znalostí či znalostního managementu). [3]

Vlastní lobbying může být realizován:

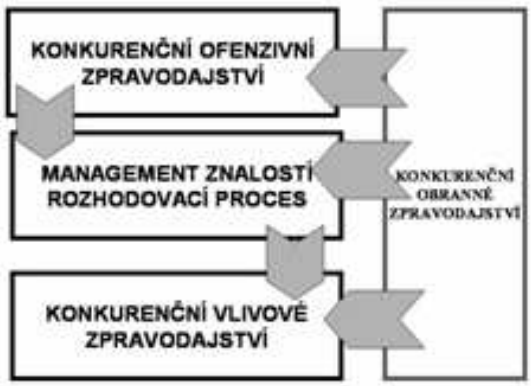
- přímo firemním detektivním útvarem (útvarem konkurenčního zpravodajství, to jest např. útvarem vnitřních nebo vnějších vztahů apod.) či soukromou detektivní agenturou zajišťující tuto činnost pro podnikatelský subjekt na komerčním podkladě

- jinými (ekonomickými, právními, provozními, tiskovými apod.) útvary podnikatelského subjektu
- zprostředkovaně (nepřímo) různými agentura či vhodnými vybranými redakcemi sdělovacích prostředků apod.

Nejčastějšími metodami vlivových opatření lobbistiky jsou:

- metody veřejné či cílené argumentace odborně věcného přesvědčování
- asertivní metody
- demonstrativní metody
- metody veřejné nebo cílené dezinformace – pro infiltraci dezorientace do zájmového prostředí nebo k zájmové osobě je možno využít jako zdroj dezinformace:
    - vědomý dezinformační zdroj (daná osoba ví, že působí jako zdroj dezinformace)
    - nevědomý informační zdroj (daná osoba neví o tom, že působí jako zdroj dezinformace)
    - technické dokumentové a věcné zdroje dezinformace (různé podvrhy, dezinformační vzorky prototypů výrobků apod.)

Informační činnost dává podnikatelským subjektům podklady pro rozhodování o jednotlivých podnikatelských krocích, ale také potřebné podklady pro realizaci protiopatření vůči své konkurenci.



Obrázek 19. Vliv dílčích konkurenčních zpravodajství na vlivové konkurenční zpravodajství

II. PRAKTICKÁ ČÁST

7. SPECIFIKACE SPOLEČNOSTI ISDIM s.r.o.

Adresy společnosti:

Provozovna	*Sídlo*
ISDIM s.r.o.	ISDIM s.r.o.
Santražiny 249	Palackého 91
760 01 Zlín	763 61 Napajedla

Firma ISDIM s.r.o. se zabývá dodávkami služeb v oblasti výpočetní techniky pro zákazníky s desítkami až stovkami počítačů. Zaměřuje se především na komplexní pokrytí potřeb zákazníků v oblasti počítačů, programového vybavení a související techniky. Firma se zabývá externím dohledem, vývojem programového vybavení na zakázku, poradenstvím a konzultacemi v oblasti informačních systémů a výpočetní techniky, službami v oblasti software a hardware, řešením havárií IT, zálohováním dat, zabezpečením firemních dat, tvorbou dokumentace IS zákazníků, zastupováním zákazníků při jednání s dodavateli nebo asistencí při jednáních a v neposlední řadě taktéž proškolováním.

Firma ISDIM s.r.o. je certifikovaným partnerem firmy Microsoft (Microsoft Gold Certified Partner). V současné době se jedná o přechodu firmy do systému jakosti ISO 9001.

Objekt společnosti ISDIM s.r.o., kterým se v této práci budu zabývat, se nachází přibližně pět minut od centra města Zlína v zastavěné obytné zóně, složené převážně z rodinných domů. V přímém sousedství provozovny firmy ISDIM s.r.o. se nachází již zmíněné rodinné domy a sídlo Městské policie Zlín. V přilehlém okolí je to poté fitness centrum, prodejna osvětlení, cukrárna, několik restauračních zařízení v okruhu 500 metrů a další menší firmy. Objekt je snadno dostupný městskou hromadnou dopravou a pravidelným železničním spojem.

Obrázek 20. Lokalizace provozovny firmy ISDIM s.r.o. ve Zlíně

Obrázek 21. Lokalizace sídla firmy ISDIM s.r.o. v Napajedlech

8. ANALÝZA SOUČASNÉ ÚROVNĚ BEZPEČNOSTNÍ POLITIKY

Firma ISDIM s.r.o. má 6 zaměstnanců (5 mužů a 1 ženu – průměrný věk zaměstnanců je 30,3 let), externí pracovnicí je spolehlivá živnostnice zabývající se účetnictvím firmy již několik let. Všichni zaměstnanci jsou pravidelně proškolování v oblasti BOZP a jsou považováni za spolehlivé, důvěryhodné a loajální. Při přijímání nových zaměstnanců není využíváno služeb personálních agentur pro prověřování zaměstnanců. Dá se tedy říci, že jsou zaměstnanci vybírání na základě svých schopností a dovedností uvedených v životopisech. Zaměstnanci nedokládají výpis z rejstříku trestů, ale pouze se zaručí za svůj čistý trestní rejstřík. Jakékoli nedodržení jednotlivých bodů v pracovní smlouvě je poté sankcionováno. Stejným způsobem jsou upraveny i smlouvy s dodavateli a odběrateli v tuzemsku či zahraničí, přičemž sankce v těchto smlouvách se pohybují řádově v milionech Kč.

Veškerá firemní data jsou ve společnosti uložena na externím, standardně zabezpečeném serveru. Standardně jsou zabezpečeny i počítače nacházející se v objektu – tedy zabezpečeny pomocí Windows firewall, antivirovým softwarem případně kryptografickou ochranou. Žádné další zabezpečení počítačů není prováděno vzhledem k tomu, že jsou tyto připojeny v rámci privátní sítě a není u ní předpokládán externí útok, ačkoli jej 50% zaměstnanců firmy považuje za větší hrozbu. Z dotazníku vyplynulo, že 83% zaměstnanců tato opatření považuje za dostatečné a firemní IS podobně jako firemní síť pokládá za dostatečně zabezpečené. Zaměstnancům je také umožněno pracovat s firemními daty i mimo firmu. Svou práci poté zabezpečují převážně kryptografickou ochranou citlivých dat a použitím běžných hesel v případě dat dostupných. Své osobní PC zaměstnanci chrání použitím hesel, případně biometrickou identifikací pomocí otisku prstu. Ochrana firemních informací a dat je chráněna doložkou o citlivých informacích v pracovní smlouvě, která zakazuje zaměstnancům vynášení veškerých informací a dat jak v průběhu pracovně-právního vztahu, tak i po jeho skončení konkurenci. Podobným způsobem jsou ošetřeny i smluvní vztahy s odběrateli, dodavateli a partnerskými společnostmi jak tuzemskými tak i zahraničními. V objektu firmy se nenacházejí žádné utajované informace.

Objekt firmy není pojištěn, pojištěn není ani majetek firmy vyjma automobilů, které zaměstnanci používají při výjezdech za klienty. Vzhledem k tomu, že objekt není ve vlastnic-

tví společnosti není touto vynakládána žádná část financí pro vybavení pronajímané části zařízením elektrické zabezpečovací signalizace, mechanických zábranných systémů, kamerovými systémy ani elektrickou požární signalizací. Vstup do objektu je podmíněn autentizací pomocí hesla případně je otevřeno zaměstnancem. Avšak po dlouhodobějším sledování tohoto systému jsem odhalila nedostatek v podobě buď otevřených dveří (neuzavřených posledním návštěvníkem) a nebo otevřením dveří návštěvníkům jedním z majitelů. Zde však nastává problém, jelikož objekt je pronajímám více subjektům. Dveře do prostor pronajímaných samotnou firmou nejsou zabezpečeny vůbec. Sami zaměstnanci mají v tomto směru na danou situaci nejednotné názory. Avšak někteří si myslí, že by bylo vhodné investovat alespoň do základních elektrických zabezpečovacích systémů pro zvýšení jejich bezpečnosti. Dalším důvodem pro zavedení EZS, MZS atd. je také fakt, že objekt je obklopen množstvím zeleně, které může sloužit jako úkryt pro případného pachatele – u vchodu do objektu (severozápadní strana) je to křoví a vzrostlé stromy, po obvodu objektu z jihozápadu a jihovýchodu jsou to taktéž vzrostlé stromy. Severovýchod stavební parcely tvoří chodník, který přímo sousedí s objektem a parcela je na této straně obehnána vysokou zdí a tím je oddělena od dalšího domu. Pozemek není oplocen a je tedy zpřístupněn všem.

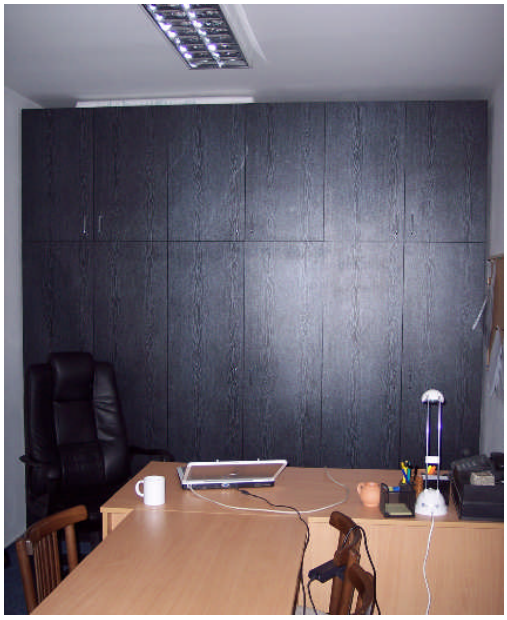
Obrázek 22. Prostory firmy

Z výzkumu také vyplynulo, že pouze určitá část zaměstnanců je informována o stávající bezpečnostní politice a krizovém plánu, zatímco zbylí zaměstnanci nemají o existenci těchto plánů žádné povědomí. Pravděpodobně k tomuto jevu dochází v důsledku manipulace jednotlivých zaměstnanců s citlivými daty a informacemi – zaměstnanci, kteří se zabývají

dílčí programovací činností potom patří do skupiny neinformované o bezpečnostní politice a krizovém plánu.

Úroveň bezpečnostní politiky je tedy, jak vyplývá ze zjištěných faktů, velmi nízká a je k ní přistupováno velmi ledabyle.

Obrázek 23. Jedno z nezabezpečených oken



Obrázek 24. Kancelář majitele firmy

9. NÁVRH ŘEŠENÍ BEZPEČNOSTNÍ POLITIKY

9.1. Oblast objektové bezpečnosti a ochrany hmotného majetku

Třída bezpečnosti:	2
Stupeň zabezpečení komponentů:	2
Min. rozsah střežení pro stupeň zabezpečení:	1
Klasifikace prostředí:	Třída I

Jak již bylo zmíněno v předcházející kapitole, není žádná část financí věnována zabezpečení objektu. Tento stav však i dle názorů některých zaměstnanců není dostačující. V rámci zajištění „jakési“ úrovně bezpečnosti v této oblasti byla majiteli domu nainstalována fotobuňka pro automatické spínání světel na rohu domu směrem ke vchodu a pak u samotného vchodu, čímž je také zajištěno osvětlení domovního zvonku a numerické klávesnice pro vstup zaměstnanců do objektu. Vzniklé osvětlení je vzhledem ke vzdálenosti od pouličního osvětlení vhodným řešením a dle mého názoru svou funkci v tomto případě plní velmi dobře.

Díky tomu, že firma ISDIM s.r.o. sídlí v přízemí rodinného domu a tento prostor je firmou pronajímán, musí být veškeré úpravy v rámci pláště a perimetru budovy odsouhlaseny majiteli. Zde však nastává problém, jelikož majitelé s žádnými většími zásahy nesouhlasí. Z tohoto důvodu pro ochranu otvorových výplní doporučuji použít bezpečnostní rolety umístěné před okenní křídla, které jsou přímo určeny k ochraně otvorových výplní, tedy oken. Ovládání rolet bude prováděno dálkovým ovladačem umístěným uvnitř objektu. Tyto rolety budou použity na všechna okna standardní velikosti v prostorech pronajímaných firmou ISDIM s.r.o., vyjma okna na toaletě, které bude zajištěno pomocí magnetického kontaktu, vzhledem ke své velikosti (viz dále). Další otvorovou výplní jsou vchodové dveře do celého objektu. Podle statistik jsou vchodové dveře nejčastěji napadenou částí pláště budovy při vloupání. V tomto případě jsou použity bezpečnostní vchodové dveře společně s bezpečnostním kováním a bezpečnostní vložkou třídy 4 pro klíč s dlouhým profilem společnosti FAB. Jak jsem již zmínila jednou z možností vstupu do objektu je také autorizace pomocí numerického kódu. Vrchní dveřní kování je v nerezovém provedení klika – koule.

Do prostoru pronajatého firmou ISDIM s.r.o. se dostaneme dalšími dveřmi. Tyto však na rozdíl od vchodových dveřích nejsou nijak zabezpečeny a jde o běžně dostupné dveře a kování. Zde bych doporučovala investovat do bezpečnostních dveří a taktéž bezpečnostního kování s bezpečnostní vložkou, jelikož není zaručeno uzavření hlavních vchodových dveří. Jako doplnění tohoto systému doporučuji dveře opatřit přídavným vrchním zámkem a magnetickým kontaktem v kombinaci s otřesovým detektorem, který umožňuje vyhlásit poplach již při pokusu o narušení dveří (např. odvrtávání zámku). Jako další bezpečnostní opatření bude na tyto dveře umístěno panoramatické kukátko pro kontrolu příchozích. Pro zvýšení bezpečnosti zaměstnanců při otevírání dveří zákazníkům musíme též zvážit možnost domácího videotelefonu, který by snížil riziko přímého ohrožení pachatelem.

Pro zabezpečení větší části pronajatého prostoru budou použity PIR detektory umístěné v následujících místnostech (viz Příloha P II):

- v místnosti, kde se nacházejí programátoři, bude umístěn detektor tak, aby střežil prostor oken a vchod do místnosti
- v chodbě v rohu u vchodových dveří do pronajímaného prostoru
- v kanceláři majitele firmy
- v prostorách skladu
- v prostoru kuchyňky

V kanceláři majitele firmy se nacházejí dvě dělená okna (obr. 22). Z důvodu konstrukce těchto oken nepovažuji za vhodné ošetřit je bezpečnostními foliemi, ale pro jejich zabezpečení doporučuji použít pasivní bezkontaktní detektor rozbití skla (tzv. Glass-break) v kombinaci s magnetickým kontaktem. Dalším oknem, které se nachází na jihozápadní straně, je okénko na toaletě. Toto okénko je poměrně malé, avšak nepovažuji za nemožné, aby se jím do prostor firmy nedostal případný narušitel, tudíž bude toto okénko opatřeno magnetickým kontaktem s vestavěnou ochrannou smyčkou. V praxi se tento magnetický kontakt přesouvá na úroveň dveří, což je i způsob který jsem zvolila v návrhu. Stejným způsobem, jako u kanceláře majitele, bude zajištěno i dělené okno na severovýchodní straně v místnosti skladu. Toto okno je snadno dosažitelné z chodníku, nad kterým se nachází. Vzhledem k jeho pozici bych i zde použila pasivní bezkontaktní detektor rozbití skla, nebo popřípadě infračervenou záclonu, která by mohla být použita také na všechna ostatní velká

okna. Vzhledem k finanční náročnosti infračervených záclon však doporučuji zmíněný detektor rozbití skla. V místnosti se samozřejmě bude ještě nacházet již zmíněný PIR detektor.

Ústředna EZS (s přímou adresací), na niž budou napojena všechna zařízení, se bude nacházet za výklenkem ve skladě. Dle mého názoru je tato pozice výhodná, neboť případný narušitel si ústředny nemusí na tomto místě delší čas všimnout. Při vyhlášení poplachu (tichý poplach – žádná zvuková signalizace narušení) zašle ústředna pomocí radiového spojení poplachovou zprávu na PCO bezpečnostní agentury, případně Policie. Tato ústředna EZS bude mít přímo implementován bezdrátový komunikátor. Dosah celého systému je závislý na nastavení vysílacího výkonu a použité antény. Ústředna, vzhledem k požadavkům majitele na dojezdnost výjezdové skupiny, nebude od PCO bezpečnostní agentury (případně Policie) větší než 2 km (vzdušnou čarou), a proto není předpokládán problém s dosahem a potřebou retranslace.

Jak jsem již zmínila, majitelé objektu si nepřejí téměř žádné zásahy do pronajímaných prostor. Z tohoto důvodu považuji za vhodné použít bezdrátová zařízení EZS, která mezi sebou komunikují rádiově a snímače jsou napájeny z baterií. Velkou výhodou, kterou v těchto systémech spatřuji, je velmi čistá a rychlá instalace (minimum vrtání a sekání) a v případě stěhování také jednoduché odinstalování. Samotestující funkce všech součástí systému upozorňuje také na případné poruchy nebo potřebu výměny baterií. Další možností je potom EZS navzájem propojená kabely, kterými se přenáší napájecí napětí a veškeré informace. V tomto případě by kabeláž byla vedena v lištách, které by však bylo třeba opatřit tampery pro případ pachatelova úmyslu „vyřadit“ EZS z provozu.

9.2. Oblast personální a režimové bezpečnosti

Jak již bylo zmíněno, všichni zaměstnanci jsou považováni za spolehlivé, důvěryhodné a loajální. Tato myšlenka je velmi hezká, avšak nevylučuje jakékoli nevhodné chování ze strany zaměstnanců. V dnešní době, kdy je konkurence mezi všemi firmami podobného zaměření velká, není možné slepě důvěřovat svým zaměstnancům a doufat v jejich „dobré

vychování“. Nejen proto by se měla v této firmě zavést kontrola činnosti zaměstnanců – tedy bezpečnostní monitoring činnosti PC a IS. To by umožnilo zaměstnavateli mít povědomí o tom, čím se jeho zaměstnanci právě zabývají. Zamezilo by se tak jednak nečinnosti zaměstnanců, ale i případnému „falešnému pracovnímu vytížení“, kdy zaměstnanec v pracovní době pracuje na věcech pro jinou společnost a nevěnuje se dostatečně svému úkolu pro danou organizaci. Tím by se také snížily náklady na takovéhoto zaměstnance, jelikož by mu nebyla placena práce navíc, případně přesčasové hodiny díky této jeho šedé činnosti. Další výhodou monitoringu firemní sítě je nepochybně kontrola manipulace s interními daty, na kterých je pracováno. Je tedy podchyceno případné vynášení informací, případně celých softwarových celků/částí zaměstnancem, přičemž vzhledem k tomu, že každý zaměstnanec má pro přístup do systému své jedinečné heslo, bylo by přesně zaznamenáno i jméno tohoto zaměstnance, případně cesta a adresa na niž byl materiál doručen (pokud by byl odesílán prostřednictvím sítě Internet). Dbát by se také mělo, aby se zaměstnanci, ačkoliv si důvěřují, při odchodu od PC odhlašovali, poněvadž by se tím zabránilo úniku nebo zcizení informací dalším zaměstnancem. Přestože tento systém není populární, jeho výsledky jsou jednoznačné a znatelné nejen pro ekonomiku firmy.

Další důležitou částí, která by měla být vyřešena, je otázka přijímání nových zaměstnanců. Rozhodně by mělo být vyžadováno předložení výpisu z rejstříku trestů a uvedení předešlých pracovních míst k ověření ve strukturovaném životopisu, včetně odkazu na kontaktní osobu, která potvrdí zaměstnancovu bývalou pozici, případně podá svá doporučení.

Co se týče režimových opatření, nejsou ve firmě nijak zvlášť specifikována. O tom svědčí již systém otevírání dveří zákazníkům. 95% zákazníků, kteří se chystají firmu ISDIM s.r.o. navštívit, ji před tímto aktem uvědomí buď telefonicky nebo e-mailem. Každá návštěva zákazníka je tak očekávána a povětšinou se i ví, který z programátorů se jí bude věnovat. Tento programátor poté také otevírá zákazníkovi dveře. Avšak tento systém není příliš dokonalý vzhledem k tomu, že objekt, ve kterém firma sídlí, je pronajímám i dalším právnickým osobám a podnikajícím fyzickým osobám. Zde je proto nasnadě využít systému domácího videotelefonu viz výše. Vzhledem k velikosti pronajímaných prostor pokládám systém kontroly vstupu za zbytečný, neboť, jak již bylo řečeno, do prostor firmy jsou návštěvy vpouštěny fyzicky zaměstnancem a v případě vstupu zaměstnanců může vstoupit do objektu pouze ten, jenž má klíče, případně má znalost numerického kódu pro vstup hlav-

ními dveřmi bez klíčů. Klíče od prostor firmy mají pouze stálí zaměstnanci firmy. Mezi režimová opatření také patří stanovení režimu nakládání s písemnostmi a ukládání datových nosičů. Díky tomu, že zaměstnanci firmy pracují výhradně s počítači, odpadá povinnost nakládání s písemnostmi, jelikož fakturační procesy probíhají přes majitele a účetní firmy, která tyto dokumenty dle Zákona o účetnictví skladuje předepsaným způsobem a jejich bezpečná manipulace je tedy zajištěna. Ukládání datových nosičů probíhá ve firmě poněkud chaoticky. Část nosičů je uložena v nezabezpečených skříních v kanceláři majitele, další část je potom zcela volně přístupná na jednotlivých stanovištích programátorů. Ve firmě převládá názor, že pokud chce někdo něco ukrást, stejně si to vezme. Vzhledem k převládajícímu názoru bych i přesto opatřila skříně uzamykacím systémem a stanovila jednotný systém ukládání datových nosičů, byť specifický pro každého zaměstnance tak, aby vyhovoval jeho osobním návykům, ale poskytoval potřebnou ochranu nosičů.

V neposlední řadě je třeba vyřešit otázku pojištění. Jak již víme, firma ISDIM s.r.o. má pojištěny pouze automobily, které slouží k dopravě k zákazníkům, dle Zákona o Silniční dani. Dle mého názoru by bylo vhodné navíc uzavřít pojištění hospodářských rizik, pojištění odpovědnosti za škodu a také pojištění pro následky živelních pohrom vzhledem ke geografické poloze obou částí společnosti v těsné blízkosti řeky. V případě posledního zmiňovaného pojištění by bylo vhodné synchronizovat délku trvání pojistky u provozovny firmy s délkou trvání nájemní smlouvy.

V závěru této kapitoly musím zdůraznit nutnost informovanosti všech zaměstnanců firmy o bezpečnostní politice a krizovém plánu, vysvětlení stěžejních pojmů v těchto dokumentech včetně kontroly dodržování bezpečnostních pravidel v nich obsažených a případné sankcionování nedodržování těchto předpisů. O každé změně těchto dokumentů musí být klíčoví zaměstnanci neprodleně informováni a dokumenty by jim taktéž měly být zpřístupněny k nahlédnutí. Zmínit také musím pravidelné proškolování v oblasti BOZP veškerého personálu firmy, které je určeno ze zákona. Všemi těmito opatřeními by mělo být dosaženo odpovědnosti jednotlivých zaměstnanců za plnění nejen režimových požadavků z hlediska bezpečnosti.

9.3. Oblast ochrany znalostí, dat a informací

V této oblasti dochází z mé strany k rozčarování, neboť jak již víte z kapitoly 8., jsou všechny PC firmy standardně zabezpečeny. Osobně si myslím, že firma zabývající se vývojem software na této úrovni by měla mít své prostředky k práci zabezpečeny mnohem lépe proti případným útokům zvenčí, avšak po konzultaci s majitelem firmy se touto částí nebudu ve své práci vůbec zabývat, poněvadž se v této oblasti na zvyklostech společnosti nebude nic měnit z těchto důvodů:

- častá výměna hardware (přibližně každé 2 roky)
- příliš velké nároky na výkon procesoru a pamětí PC již samotnou prací programátorů, natož při nadstandardním zabezpečení (příliš velké snížení operačního výkonu)
- nechuť investovat do software, které je hackery stejně prolomeno
- na PC se nenacházejí žádné utajované informace dle zákona 412/2005 Sb.
- nadstandardní ochrana know-how pod tlakem levných asijských kopií je nesmyslná
- každý lepší hacker nakonec obstojí a data stejně zcizí
- software pro důležité tuzemské i zahraničí zákazníky je šifrován samostatně
- vysoký pokles výkonu při používaní šifrovacích klíčů na úrovni hardware
- zaměstnanci, kteří si práci berou domů, ji sami šifrují → nepoužitelnost při zcizení osobního PC

ZÁVĚR

Jak plyne ze statistik Policie ČR Zlín, je každoročně nahlášeno okolo 2,5 tisíc majetkových trestných činů, přičemž objasněno je pouze asi 25% z nich. Oněch 25% potom tvoří převážně objekty, které mají nainstalovanou EZS, případně další prvky zabezpečení. Potřeba ochrany majetku je nutná a potřebná. Ačkoliv dobrá EZS pachatele trestné činnosti neodradí, jejich počínání patřičně ztíží a jejich postup zpomalí, ale především upozorní kompetentní složky na vzniklou situaci.

Podle průzkumů Computer Science Institute došlo v 97% případů narušení firem ke znatelným finančním ztrátám. Mnozí majitelé dnešních, především malých a středních firem, nepovažují za dostatečně důležité zabezpečení svého firemního majetku. Většina z nich je přesvědčena o nepravděpodobnosti útoku, ať už fyzického nebo prostřednictvím internetu, z důvodů nepochopení logiky útočníka, který podle jejich názoru útočí pouze na větší a atraktivnější podniky. Bohužel opak je pravdou a malé a střední firmy jsou napadány čím dál častěji.

Firma ISDIM s.r.o. toto stanovisko nezastává, naopak, a je to velmi překvapivé, je povědomí o možnosti útoku na firmu, především softwarového typu, velmi vysoké. Zde však nastává druhý extrém. Počítačová síť je zabezpečena pouze standardně, aby případný útočník nezpůsobil ještě více škody, prostory společnosti potom nejsou zabezpečeny vůbec, protože je popírána možnost násilného vniknutí do objektu, ve kterém někdo stabilně žije. Ačkoli všichni známe případy, kdy rodina snídá v přízemí a zloděj mezitím vykrade první patro, naše nečinnost a spořivost jde na úkor protiopatření, která by nám mohla zachránit mnohem víc.

Za nejsilnější stránku svého návrhu považuji oblast objektové bezpečnosti a ochranu hmotného majetku ve spojitosti s personální a režimovou bezpečností, která tuto oblast doplňuje. Nejslabším místem potom zůstává oblast ochrany znalostí, dat a informací, kterou jsem blíže nespecifikovala na základě pohovoru s vedením firmy. Vedení firmy totiž, dle mého názoru, do značné míry nepochopilo závažnost a možná bezpečnostní rizika vyplývající z neuskutečnění nutných bezpečnostních opatření ve spojitosti s touto oblastí.

Ve své práci jsem se snažila o co nejvyšší úroveň zabezpečení za co možná nejmenší cenu. I přesto je finanční otázka v rozhodování firmy velmi důležitá, protože do jejího prostoru zatím nebylo zaznamenáno žádné násilné vniknutí a proto zabezpečení nepovažují za důležité. Avšak s tím, že firma plánuje přejít na systém jakosti ISO 9001, bude muset vynaložit nemalé finanční výdaje na zlepšení stávajícího stavu. Má práce jim proto bude sloužit jako vodítko pro další praktické využití ke zlepšení současného stavu a zajištění další činnosti.

CONCLUSION

As the statistics of the Police of the Czech Republic in Zlín show, annually about 2.5 thousand property crimes are announced, while only about 25% of them are clarified. These 25% are mainly objects with an electronic safety appliance or other items of safeguard. Prevention of property is necessary and needed. Although an electronic safety appliance is not able to discourage intruder, it is able to complicate and slow down the intruder progress, and, above all, inform the competent units.

According to the survey of the Computer Science Institute, in 97% cases noticeable financial loss occurred after violation. Many owners of small and medium-sized companies do not consider securing the company property important. They think the assault on their company is not probable, either physical or via the internet, because they do not understand the intruder's logic which is according to their opinion interested in big and more attractive corporations. Unfortunately, this is not true and small companies are attacked more and more frequently.

The company ISDIM s.r.o. does not think so. Surprisingly, the awareness of the possibility of an attack, especially in the case of a software company, is very high. There comes another extreme. The computer network is secured only by default so that a potential intruder does not make more damage. The premises hired by the ISDIM s.r.o. are not secured at all because the possibility of violation is disclaimed as there are permanent holders living in the building. Nevertheless, we all know the cases when a house is broken into while the family is having breakfast on the ground floor. Our inactivity and thriftiness is going at the expense of countermeasures which could safe much more.

I consider the sphere of object security and tangible property protection in conjunction with personal and behavioural security to be the strongest points of my proposal. As the weakest point, there remains the sphere of knowledge, data and information protection which I did not specify closer on the basis of the discussion with the company's top executives. The top executives, in my opinion, did not have sufficient understanding of the relevancy and possible security risks resulting from the failure of the precautions in this sphere.

I was trying to propose the highest level of security at a lowest prize possible. The financial issue is very important in the company's decision-making because there was no record of forcible trespass into place and this leads into inconsequentiality of security in the eye of the possessor. However, the company plans to adopt the quality management system ISO 9001. Therefore, it will to invest a considerable amount to improve the current state. This work will serve as a guide to be practically used in the process of improving the current state and ensuring the company's further activities.

SEZNAM POUŽITÉ LITERATURY

Monografické publikace:

[1] Látal, I., Štantejský, M.: *Bezpečnostní zásady ochrany podniku: prevence a řešení krizových situací*, 4. vydání, PROSPEKTUM, Praha 2001, 120 str., ISBN 80-7175-091-3

[2] Musil, R.: *Ochrana utajovaných skutečností*, 1. vydání, EUROUNION, Praha 2001, 380 str., ISBN 80-85858-93-2

[3] Brabec, F. a kol.: *Bezpečnost pro firmu, úřad, občana*, 1. vydání, Public History, Praha 2001, 400 str., ISBN 80-86455-04-06

[4] Veber, J. a kol.: *Management kvality, environmentu a bezpečnosti práce – Legislativa, metody, systémy a praxe*, 1. vydání, Management Press, Praha 2006, 359 str., ISBN 80-7261-146-1

[5] Bartes, F.: *Konkurenční strategie firmy*, 1. vydání, Management Press, Praha 1997, 125 str., ISBN 80-85943-41-7

[6] Vodáček, L., Vodáčková, O.: *Malé a střední podniky: konkurence a aliance v Evropské unii*, 1. vydání, Management Press, Praha 2004, 193 str., ISBN 80-7261-099-6

[7] Devátý, S., Toman, P.: *Ochrana dobré pověsti a názvu právnických osob*, 2. aktualizované a doplněné vydání, Linde Praha, Praha 2001, 200 str., ISBN 80-7201-297-5

[8] Smejkal, V., Sokol, T., Vlček, M.: *Počítačové právo*, 1. vydání, C.H. Beck, Praha 1995, 164 str., ISBN 80-7179-009-5

[9] Zuzák, R.: *Krizové řízení podniku (dokud ještě není v krizi)*, 1. vydání, Professional publishing, Praha 2004, ISBN 80-86419-74-6

[10] Smejkal, V., Rais, K.: *Řízení rizik*, 1. vydání, Grada Publishing, Praha 2003, 270 str., ISBN 80-247-0198-7

[11] Brabec, F.: *Ochrana bezpečnosti podniku*, 1. vydání, EUROUNION, Praha 1996, 204 str., ISBN 80-85858-29-0

[12] Rodryčová, D., Staša, P.: *Bezpečnost informací jako podmínka prosperity firmy*, 1. vydání, Grada Publishing, Praha 2000, 144 str., ISBN 80-7169-144-5

[13] Kindl, J.: *Projektování bezpečnostních systému I*, 1. vydání, Univerzita Tomáše Bati ve Zlíně, Zlín 2004, 134 str., ISBN 80-7318-165-7

[14] Laucký, V.: *Technologie komerční bezpečnosti I*, 2. vydání, Univerzita Tomáše Bati ve Zlíně, Zlín 2004, 66 str., ISBN 80-7318-194-0

[15] Laucký, V.: *Technologie komerční bezpečnosti II*, 1. vydání, Univerzita Tomáše Bati ve Zlíně, Zlín 2004, 123 str., ISBN 80-7318-231-9

[16] Jašek, R.: *Informační a datová bezpečnost*, 1. vydání, Univerzita Tomáše Bati ve Zlíně, Zlín 2006, 140 str., ISBN 80-7318-456-7

[17] Ernst & Young, DSM – data security management, NBÚ: *Průzkum stavu informační bezpečnosti v ČR 2005 (PSIB ČR ´05)*, Národní bezpečnostní úřad, Praha 2005, 32 str., ISBN 80-86813-07-X

[18] Doseděl, T.: *Počítačová bezpečnost a ochrana dat*, 1. vydání, Computer Press, Brno 2004, ISBN 80-7226-632-2

[19] Pužmanová, R.:*Bezpečnost bezdrátové komunikace: Jak zabezpečit Wi-fi, Bluetooth, GPRS či 3G*, 1. vydání, Computer Press, Brno 2005, ISBN 80-251-0791-4

[20] Hlaváč, J.: *Klasifikace informací jako hledisko přístupu k systému*, diplomová práce, Vysoká škola ekonomická v Praze – Fakulta informatiky a statistiky, Praha 2002, 95 str., vedoucí diplomové práce Ing. Libor Gála

Internetové zdroje:

[21] Analýza rizik [online]. [cit. 29.11.2006], dostupné z: <http://www.rac.cz/rac/homepage.nsf/CZ/2D162FC7F6C0BAFBC125692100415E80 [2005]>

[22] I. certifikační autorita [online]. [cit. 30.11.2006], dostupné z: <http://www.ica.cz/home_cs/?acc=teorie_a_principy>

[23] Obchodní rejstřík [online]. [cit. 27.2.2007], dostupné z: <http://www.justice.cz/>

[24] E-podpis [online]. [cit. 05.03.2007], dostupné z: <http://www.micr.cz/epodpis/default.htm>

[25] F.S.C. – Bezpečnostní poradenství [online]. [cit. 23.04.2007], dostupné z: <http://www.fsc-ov.cz/produkt.php?id=101 >

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACCESS	Systém kontroly vstupu
AES	Advanced Encryption Standard
Apod.	A podobně
Atd.	A tak dále
BOZP	Bezpečnost a organizace zdraví při práci
CAST	Algoritmus autorů Carlisle Adams a Stafford Taverns
CCTV	Uzavřené střežící a dohledové kamerové systémy
CI	Competitive inteligence – konkurenční zpravodajství
DES	Data Encryption Standard
EPS	Elektrická požární signalizace
EZS	Elektrická zabezpečovací signalizace
IDEA	Algoritmus F. K. Zimmermana – dostupný ve volném PGP
IS	Informační systém
IT	Informační technologie
MF	Ministerstvo financí
MZS	Mechanické zábranné prostředky
Např.	Například
NBÚ	Národní bezpečnostní úřad
PC	Počítač
PCO	Pult centrální ochrany
PGP	Pretty good privacy – volně dostupný šifrovací balíček
PIR	Passive infrared detector – pasivní infračervený detektor
PKI	Public key infrastructure – hierarchická autorita
Příp.	Případně
Resp.	Respektive
RSA	Algoritmus autorů Rivest, Shamir a Aleman
TripleDES	Data Encryption Standard with triple key usage
Tzn.	To znamená
Tzv.	Takzvaně
UI	Utajované informace

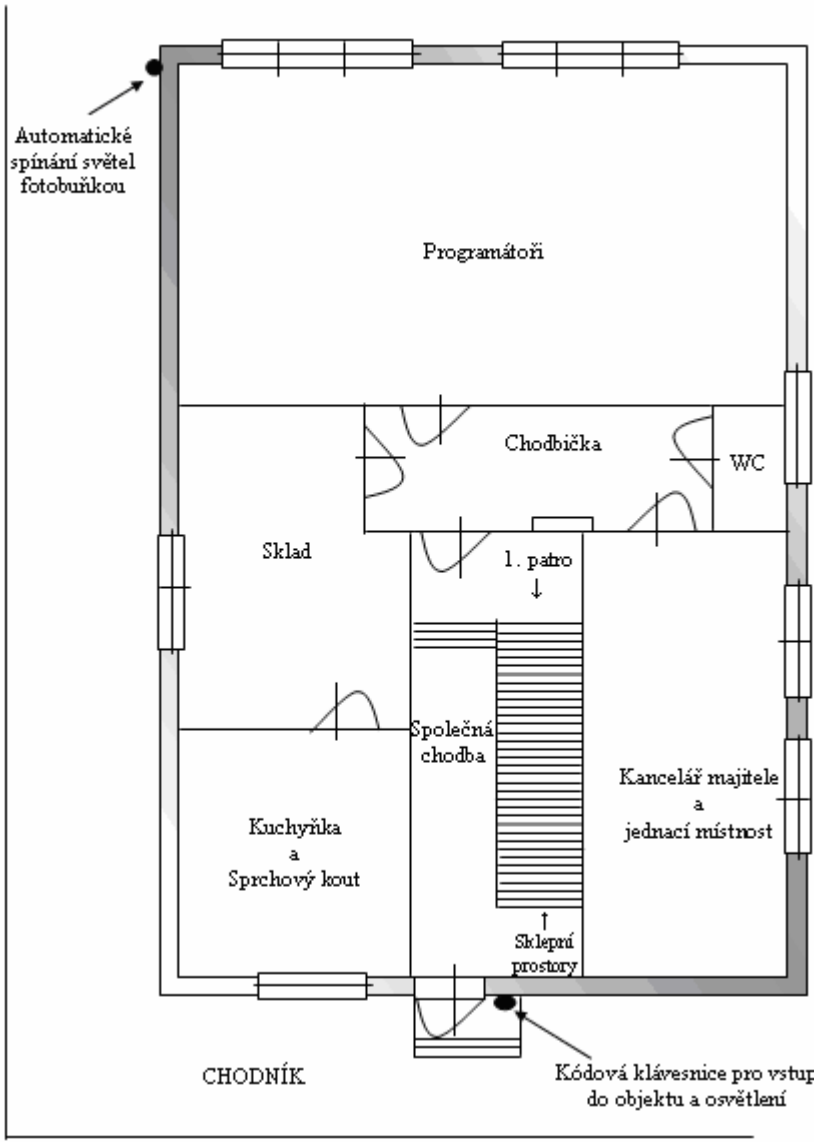
SEZNAM OBRÁZKŮ

SEZNAM TABULEK

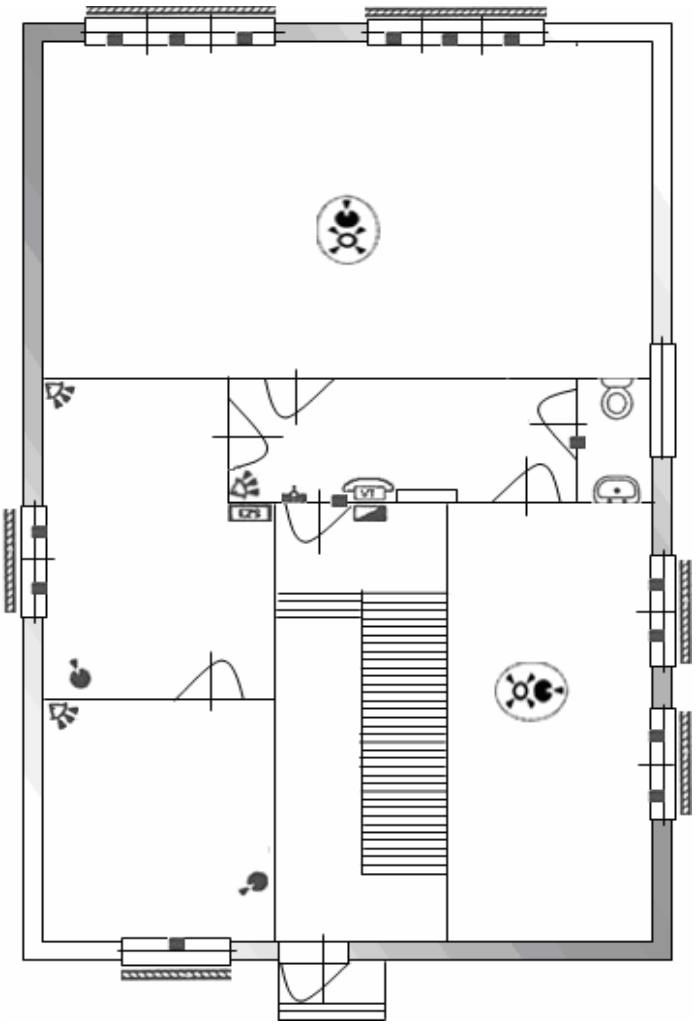
SEZNAM ROVNIC

SEZNAM PŘÍLOH

PŘÍLOHA P I: MAPA OBJEKTU



PŘÍLOHA P II: MAPA OBJEKTU S NAVRŽENÝM ZABEZPEČENÍM



Legenda

	Magnetický detektor (kontakt)
	Otřesový detektor
	Akustický detektor tříštění skla
	PIR Vějíř
	PIR stropní detektor kombinovaný s akustickým detektorem tříštění skla
	Klávesnice EZS
	Ústředna EZS
	Domácí videotelefon
	Ochranná (bezpečnostní) roleta

PŘÍLOHA P III: VÝPIS Z OBCHODNÍHO REJSTŘÍKU

Ú p l n ý v ý p i s

z obchodního rejstříku, vedeného
Krajským soudem v Brně
oddíl C, vložka 38315

Datum zápisu: 25.října 2000

Obchodní firma: ISDIM s.r.o.
Zapsáno: 25.října 2000

Sídlo: Napajedla, Palackého 91, okres Zlín, PSČ 763 61
Zapsáno: 25.října 2000

Identifikační číslo: 262 27 002
Zapsáno: 25.října 2000

Právní forma: Společnost s ručením omezeným

Předmět podnikání:

- koupě zboží za účelem jeho dalšího prodeje a prodej
Zapsáno: 25.října 2000
- poskytování software
Zapsáno: 25.října 2000

Statutární orgán:

jednatel: Michal Hrabák, r.č. 671218/0090
Napajedla, Palackého 99, okres Zlín, PSČ 763 61
Zapsáno: 25.října 2000

Způsob zastupování: za společnost jedná a podepisuje jednatel
Zapsáno: 25.října 2000

Společníci:

Michal Hrabák, r.č. 671218/0090
Napajedla, Palackého 99, okres Zlín, PSČ 763 61
Vklad: 100 000,- Kč
Splaceno: 100 %
Zapsáno: 25.října 2000

Základní kapitál: 100 000,- Kč
Zapsáno: 25.října 2000

PŘÍLOHA P IV: DOTAZNÍK

Vážená paní, Vážený pane,

věnujte prosím pár minut vyplnění následujícího dotazníku, který bude sloužit pro další zpracování. Děkuji za Váš čas.

Pohlaví (muž/žena)	**Věk**	**Dosažené vzdělání**

1. Myslíte si, že je zabezpečení Vašeho firemního informačního systému dostatečné?
☐ **ANO**
☐ **NE**
☐ **NEVÍM**

2. Myslíte si, že je zabezpečení Vaší firemní sítě dostatečné?
☐ **ANO**
☐ **NE**
☐ **NEVÍM**

3. Využíváte kryptografickou ochranu dat?
☐ **ANO**
☐ **NE**
☐ **OBČAS**

4. Jste obeznámeni o způsobu nakládání s informacemi a daty ve Vaší firmě?
☐ **ANO**
☐ **NE**

5. Máte možnost pracovat s firemními daty i mimo Vaši firmu?
☐ **ANO**
☐ **NE**
☐ **OBČAS**

6. Pokud ANO, jakým způsobem svou práci/data zabezpečujete?

7. Jakým způsobem je zabezpečeno Vaše PC?

8. Který z druhů útoků považujete v současnosti za větší hrozbu?
☐ **INTERNÍ**
☐ **EXTERNÍ**
☐ **NEDOKÁŽU URČIT**

9. Zabezpečujete Vámi vytvořený software?
☐ **ANO**
☐ **NE**
☐ **OBČAS**

10. Vypínáte své firemní PC, když jste o víkendu mimo firmu?
☐ **ANO**
☐ **NE**
☐ **KDYŽ SI VZPOMENU**

11. Zdá se Vám objekt Vaší firmy dobře zabezpečen?
☐ **ANO**
☐ **NE**
☐ **NEDOKÁŽU POSOUDIT**

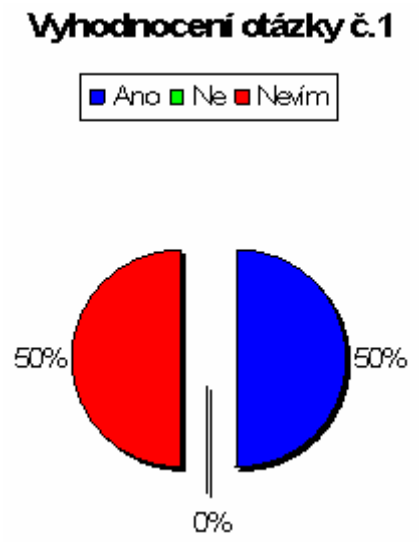
12. Pokud NE, co byste změnili, popřípadě doplnili v rámci zabezpečení objektu?

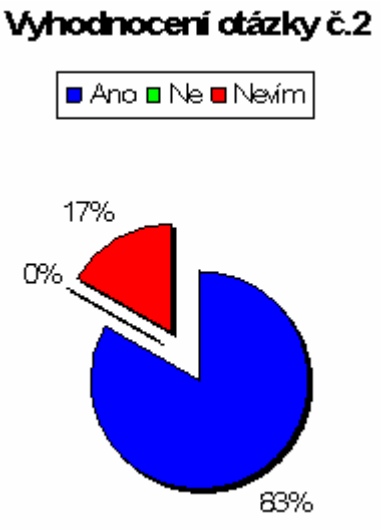
13. Máte v pracovní smlouvě doložku o nakládání s citlivými informacemi?
☐ **ANO**
☐ **NE**

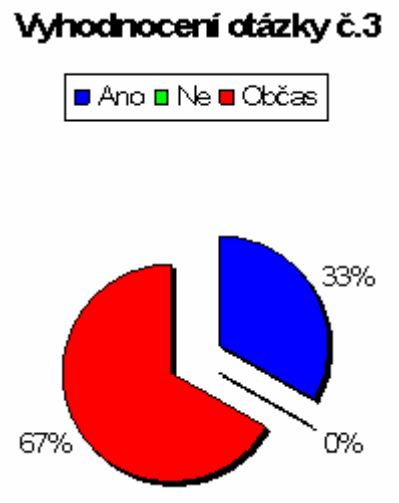
14. Který z následujících systému autentizace zaměstnanců je využíván ve Vaší firmě?
☐ **BIOMETRIKA** ☐ **TOKENY** ☐ **SMART KARTY**
☐ **FYZICKÁ KONTROLA** ☐ **DOKLADOVÁ KONTROLA** ☐ **STANDARDNÍ HESLA**
☐ **ŽÁDNÝ SYSTÉM NEMÁME** ☐ **JINÉ (uveďte)**

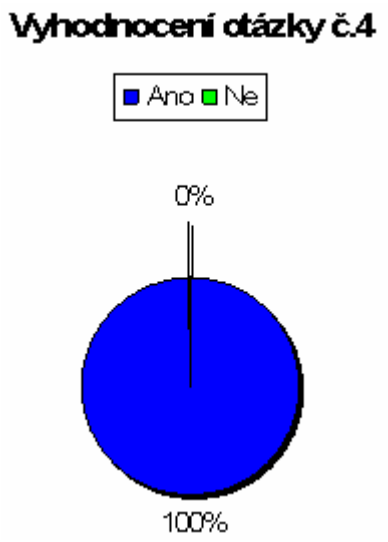
15. Má Vaše firma vypracovanou bezpečnostní politiku nebo alespoň plán pro řešení krizových situací?
☐ **ANO**
☐ **NE**
☐ **NEVÍM**

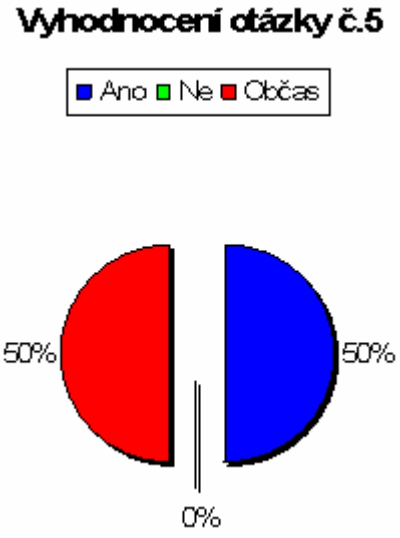
PŘÍLOHA P V: VYHODNOCENÍ DOTAZNÍKU



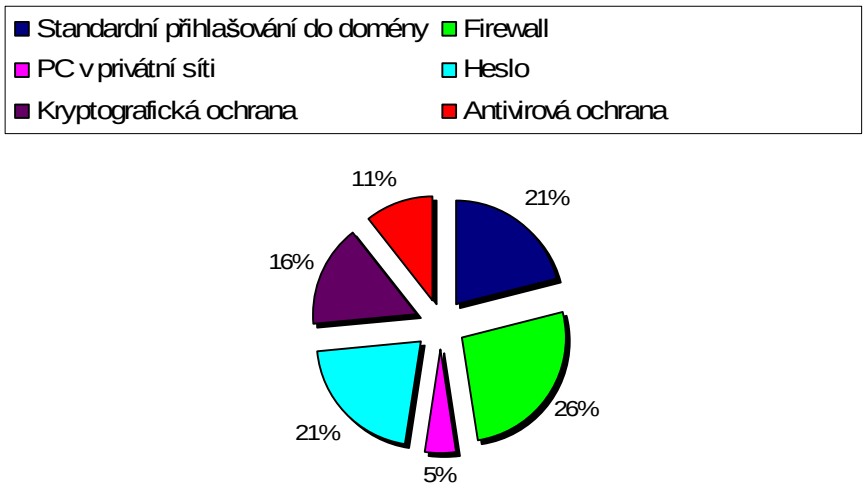




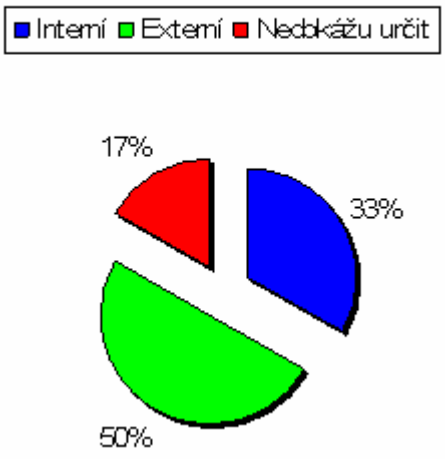




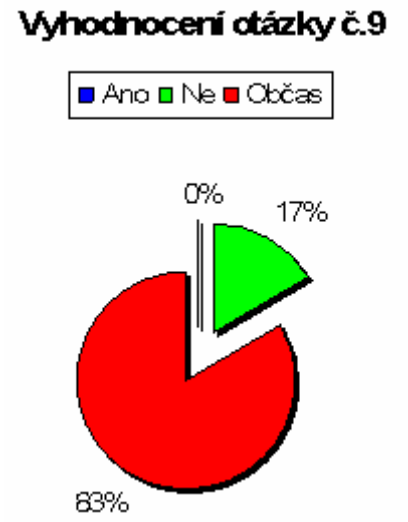
Vyhodnocení otázky č. 7



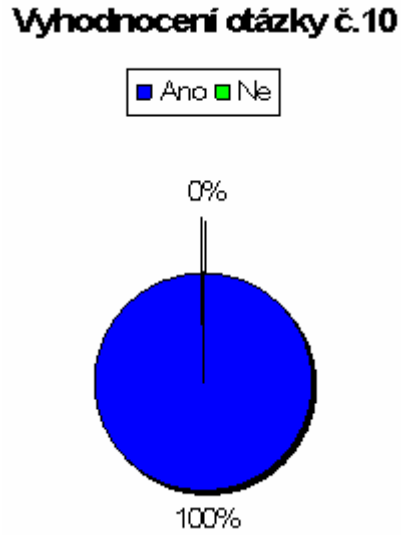
Vyhodnocení otázky č.8



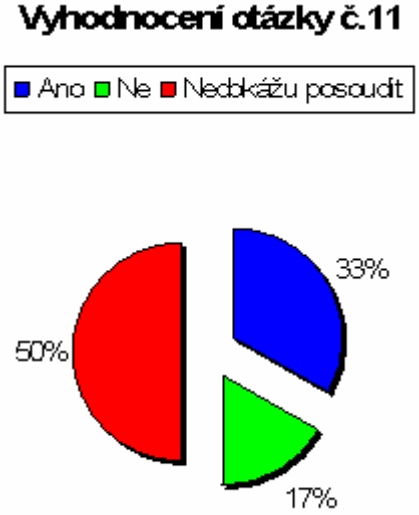
Vyhodnocení otázky č.9



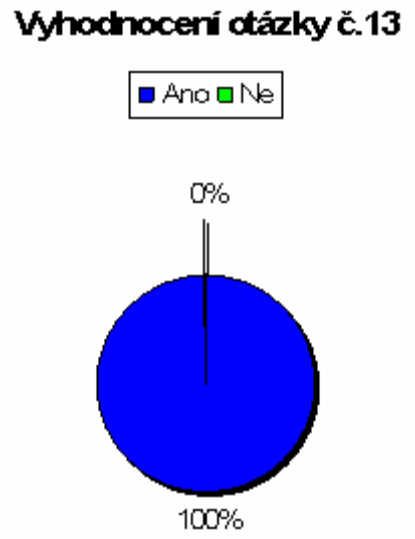
Vyhodnocení otázky č.10

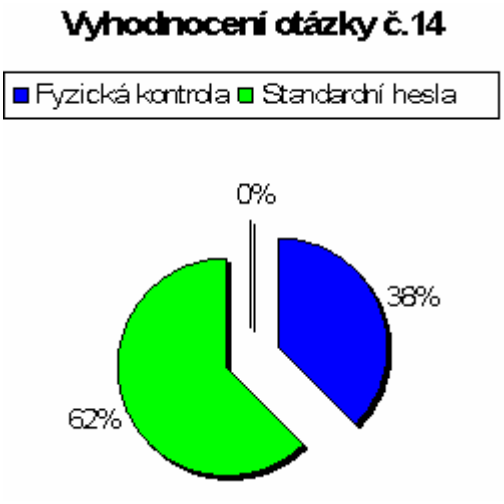


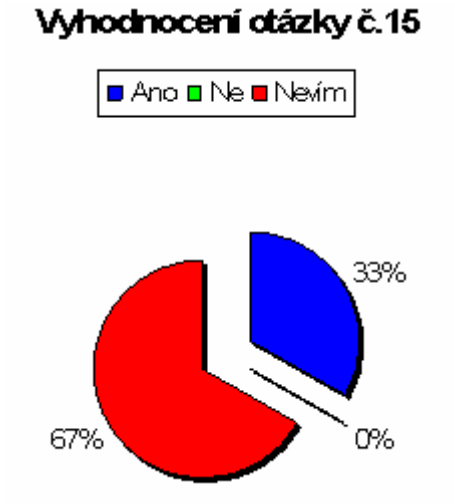
Vyhodnocení otázky č.11




Vyhodnocení otázky č.12
Použití alarmů
Dostatečně zabezpečeno
33%
67%


Vyhodnocení otázky č.13
Ano
Ne
0%
100%


Vyhodnocení otázky č.14
Fyzická kontrola
Standardní hesla
0%
38%
62%


Vyhodnocení otázky č.15
Ano
Ne
Nevím
33%
67%
0%