SLOVENSKÁ POĽNOHOSPODÁRSKA UNIVERZITA

V NITRE

FAKULTA EKONOMIKY A MANAŽMENTU

2125652

BEZPEČNOSŤ DIGITÁLNEHO PROSTREDIA V SR

2011 Bc. Miroslava REMEŠOVÁ

SLOVENSKÁ POĽNOHOSPODÁRSKA UNIVERZITA

V NITRE

FAKULTA EKONOMIKY A MANAŽMENTU

Bezpečnosť digitálneho prostredia v SR

DIPLOMOVÁ PRÁCA

Študijný program:	Ekonomika podniku
Študijný odbor:	6284800 - ekonomika a manažment podniku
Školiace pracovisko:	Katedra informatiky
Školiteľ:	doc. Ing. Klára Hennyeyová, CSc.

Nitra 2011 Bc. Miroslava Remešová

ABSTRAKT

Informačná bezpečnosť je proces ochrany dát pred ich náhodným a úmyselným zneužitím osobami. Narušenie bezpečnosti môže zahŕňať rôzne činnosti, napr. poškodenie vzhľadu webovej stránky, napadnutie počítačovým vírusom, zlyhanie zamestnanca, ktorý neúmyselne prezradí svoje heslo. Bezpečnosť digitálneho prostredia je spojená so zvyšovaním pripojenia na Internet. Prenikavé zvýšenie bezpečnosti na Internete je dnes jednou zo základných podmienok jeho ďalšieho úspešného rozvoja. Informačné a komunikačné technológie a informačné systémy v podniku, musia byť schopné poskytovať aktuálne a hodnoverné informácie manažérom v reálnom čase, musia byť dostatočne bezpečné. Bezpečnosť digitálneho prostredia je veľmi dôležitá pre všetkých užívateľov informačných technológií.

Kľúčové slová:

informačná spoločnosť, informačná bezpečnosť, bezpečnosť informačných technológií, Internet, informačné a komunikačné technológie.

ABSTRAKT

Die Sicherheit in der Informationstechnik ist der Prozess der Datenschutz vor versehentlichem und absichtlichem Missbrauch durch Personen. Angeschlagene Sicherheit kann die verschiedene Aktivitäten einbeziehen, zum Beispeil: die Schäden an einer Web-Seite, der Angriff durch einen Computervirus oder Ausfall eines Mitarbeiters, der versehentlich sein Pasword verratet. Die Sicherheit der digitalen Umwelt ist mit zunehmender Internet-Anschluss festverbunden. Ein durchdringendes Erhöhung der Sicherheit im Internet ist eine der grundlegenden Bedinungen für ihre weitere erfolgreiche Entwicklung. Informations- und Kommunikationstechnologien und Informationssysteme in der Wirtschaft müssen die rechtzeitige und präzise Informationen für die Managers anbieten in realen Zeit und sie müssen natürlich auch ausreichend sicher zu sein. Sicherheit der digitalen Umfeld ist wichtig für alle Anwender von Informationstechnologie.

Die Schlüsselwörter:

die Informationgesellschat, die Sicherheit in der Informationstechnik, die Sicherheit in der Informationstechnologie, die Informationsicherheit, das Internet-Anschluss, die Informations- und Kommunikationstechnologien.

ČESTNÉ VYHLÁSENIE

Podpísaná Miroslava Remešová vyhlasujem, že som záverečnú prácu na tému „Bezpečnosť digitálneho prostredia v SR“ vypracovala samostatne s použitím uvedenej literatúry.

Som si vedomá zákonných dôsledkov v prípade, ak uvedené údaje nie sú pravdivé.

V Nitre, 10.04.2011 .....

Bc. Miroslava Remešová

POĎAKOVANIE

Touto cestou vyslovujem poďakovanie pani doc. Ing. Kláre Hennyeyovej, CSc. za pomoc, odborné vedenie, cenné rady a pripomienky pri vypracovaní mojej diplomovej práce.

POUŽITÉ OZNAČENIE

BBS	- bulletin board service
IKT	- informačné a komunikačné technológie
IEC	- International Elecktric Committrr
IS	- informačný systém
ISO	- International Standardization Organization
ISO TR	- ISO Technical Report
ISO TS	- ISO Technical Specification
NCSC	- National Computer Security Center
NOD	- Norton antivírus

ZOZNAM ILUSTRÁCIÍ

ZOZNAM TABULIEK

SLOVNÍK TERMÍNOV

Autentickosť - vlastnosť údajov vyjadrujúca to, že údaje sú pravé, čo sa dá aj overiť (autentifikácia), a preto im možno dôverovať, dôvera v platnosť prenosu informácie prenesenej správy alebo v to, že správu poslal ten, kto sa za jej odosielateľa vydáva.

Autentifikácia - overenie identity používateľa, procesu alebo zariadenia, alebo pôvodu správy.

Bezpečnostný incident - porušenie alebo bezprostredná hrozba porušenia bezpečnostných politík, bezpečnostných zásad alebo štandardných bezpečnostných pravidiel prevádzky IKT.

Digitálny priestor - údaje a informácie v digitálnej forme, programy, technické zariadenia, siete slúžiace na spracovanie informácií, dokumentácia k programom a technickým zariadeniam na spracovanie informácie, pravidlá normy, štandardy a legislatívne normy upravujúce spracovanie informácií.

Dôvernosť - bezpečnostná požiadavka na ochranu údajov, zaistenie dôvernosti údajov znamená vylúčenie možnosti odhalenia ich informačného obsahu nepovolenou osobou.

Dostupnosť – bezpečnostná požiadavka na ochranu údajov, zaistenie dostupnosti údajov znamená, že údaje sú k dispozícií oprávnenej osobe vždy, keď o ne požiada.

Digitálny priestor - údaje a informácie v digitálnej forme, programy, technické zariadenia, siete slúžiace na spracovanie informácií, dokumentácia k programom a technickým zariadeniam na spracovanie informácie, pravidlá normy, štandardy a legislatívne normy upravujúce spracovanie informácií

Integrita - bezpečnostná požiadavka na ochranu údajov a technických zariadení. Zaistenie integrity údajov znamená prijatie opatrení, ktoré vylučujú možnosť nepozorovanej zmeny údajov. Zaistenie integrity technického systému znamená vylúčenie možnosti jeho neoprávnenej modifikácie.

OBSAH

ÚVOD

Informácie sú dnes jedny z najdôležitejších “aktív”, ktorými podniky disponujú a prirodzene majú záujem o ich primeranú ochranu. Strata dát, únik informácii, vyzradenie obchodného tajomstva, nefunkčnosť informačného systému, predstavujú vážne riziká z pohľadu ohrozenia chodu a rozvoja podniku, preto je na mieste hľadať riešenie v zavedení systému manažmentu bezpečnosti informačných systémov s cieľom dané riziká efektívne riadiť a tým znížiť pravdepodobnosť ich výskytu a zmierniť dopad vážnych škôd a strát v podniku.

Informačná bezpečnosť je proces ochrany dát pred ich náhodným alebo úmyselným zneužitím osobami v rámci či mimo organizácie, vrátane zamestnancov, alebo aj obávaných hackerov. Narušenie bezpečnosti môže zahŕňať rôzne činnosti, napr. poškodenie vzhľadu webovej stránky, napadnutie počítačovým vírusom, zlyhanie zamestnanca, ktorý neúmyselne prezradí svoje heslo, a pod. Informačná bezpečnosť je vyváženie rizík výhodami v podobe vykonávania činnosti elektronicky.

S prudkým rozvojom informačných systémov rastie aj možnosť ich zneužitia. O čo rýchlejšie napreduje vývoj v tejto oblasti, o to agresívnejšie je aj konkurenčné prostredie, a o to kratšie zlyhanie informačného systému môže spôsobiť nenahraditeľné škody obrovského rozsahu. Podniky prichádzajú o veľké finančné prostriedky, či už v dôsledku náhodných výpadkov systémov, straty dát či náhodných incidentov. Nezanedbateľné sú tiež škody v dôsledku úmyselného konania zamestnancov, či tretích osôb, s cieľom narušiť, či poškodiť informačný systém podniku.

Závislosť spoločnosti od správnej a neprerušenej činnosti zložitých IS je v súčasnosti už aj u nás dosť vysoká a s postupom času sa bude ešte viac prehlbovať. Môžeme preto očakávať, že nastupujúca informačná spoločnosť sa bude vyznačovať vysokou citlivosťou na javy a udalosti, ktoré vo svojich dôsledkoch nepriaznivo ovplyvnia schopnosť IS poskytovať svoje služby dostatočne bezpečne a v požadovanej kvalite.

Slovensko chce v oblasti informačnej bezpečnosti vytvoriť jednotnú platformu budovania informačnej spoločnosti postavenú na právnych základoch so zabezpečením primeranej ochrany a dôveryhodnosti digitálneho prostredia krajiny, vyplýva to z Národnej stratégie pre informačnú bezpečnosť v SR. Schválená stratégia má pozitívne vplývať na podnikateľské prostredie na Slovensku, nakoľko sa podľa nej má zvýšiť integrita údajov, autorita, povesť subjektov a ich transparentnosť.

1. PREHĽAD O SÚČASNOM STAVE RIEŠENEJ PROBLEMATIKY

1.1 Bezpečnostná politika a informačná bezpečnosť

Bezpečnostná politika informačného systému podľa **Khouri, S. – Al-Zabidi, D. (2010)** je vnútorný predpis, ktorý je v spoločnosti všeobecne a trvalo záväzný (formálne) zodpovedá pokynu alebo príkazu generálneho riaditeľa.

Cieľom bezpečnostnej politiky informačného systému je definovať:

- ✓ hlavné aspekty informačnej bezpečnosti vo fyzickej, logickej, personálnej a legislatívnej sfére,
- ✓ spôsob plánovania aktivít v oblasti informačnej bezpečnosti,
- ✓ rutinné činnosti v oblasti informačnej bezpečnosti.

Vyplývajú z nej práva, povinnosti a zodpovednosť pre:

- ✓ jednotlivých pracovníkov,
- ✓ riadiacu zložku informačnej bezpečnosti,
- ✓ výkonnú zložku informačnej bezpečnosti,
- ✓ kontrolnú zložku informačnej bezpečnosti.[1]

Podľa **Kučeru (2004)** je bezpečnostná politika základné východisko pre riadenie bezpečnosti IS organizácie. Vyjadruje bezpečnostné ciele, definuje zásady procesov ochrany, všetky princípy, obmedzenia, požiadavky, pravidlá a postupy, ktoré určujú spôsob správy, ochrany a distribúcie citlivých informácií a hodnôt informačného systému. Pravidlá bezpečnostnej politiky musia byť najvyššou netechnickou úrovňou definície ochranných mechanizmov informačného systému.

Cieľom bezpečnostnej politiky je minimalizovať vplyv pôsobiacich rizík. Bezpečnostnú politiku nemôžeme chápať ako poistku proti úniku informácií, alebo vzniku škody. Je to len prostriedok, ktorý redukuje riziká výskytu nebezpečia a určuje všeobecné pravidlá a postupy pre rôzne systémy. Dobre navrhnutá bezpečnostná politika je kompromisom v obmedzovaní používateľov systému a chráneným záujmom organizácie.

Bezpečnostnú politiku môžeme rozdeliť podľa konkretizácie priorít, ktoré sleduje,

1 SAMER KHOURI – DENISA AL-ZABIDI 2010. Informačné systémy podniku**.** Košice: Dekanát – Edičné pracovisko Fakulty BERG, Košice 2010, s.102 - 103, ISBN 978-80-553-0373-4.

ale aj oblastí, v ktorých sa uplatňuje:

a) **Bezpečnostná politika štátu** je vrcholom bezpečnostnej štruktúry. Tvoria ju predovšetkým zákony a z nich odvodené predpisy, nariadenia a smernice, nariadenia vlády a dokumenty s celoštátne záväznou platnosťou. Predovšetkým sem patrí:

- ✓ Zákon č. 261/1995 Zb. o štátnom informačnom systéme,
- ✓ Zákon o ochrane osobných údajov v informačných systémoch,
- ✓ Trestný zákon,
- ✓ Nariadenie vlády o ochrane hospodárskeho služobného tajomstva a pod.

b) **Rezortná (podniková) bezpečnostná politika** vychádza zo štátnych normatívov, ktoré musia jednoznačne definovať a riešiť problém, ale zároveň musia byť natoľko všeobecné, aby nezväzovali ruky rezortným bezpečnostným politikám, štátnej správy a bezpečnostným politikám organizácie, ktoré sú hierarchicky na nižšej úrovni. Rezorty a organizácie majú spravidla svoje špecifické požiadavky na zabezpečenie informačných systémov, a preto musia podrobnejšie definovať svoje požiadavky a zásady upevňovania bezpečnosti.

c) **Systémová bezpečnostná politika** je najnižším a najpodrobnejšie vypracovaným stupňom na úrovni jednotlivých IS. Vychádza z hierarchicky nadradených bezpečnostných politík a detailne rozpracúva princípy ochrany podľa konkrétnych potrieb daného informačného systému. Pri rozsiahlych informačných systémoch sa systémová bezpečnostná politika spravidla definuje v dvoch krokoch. V prvej fáze návrhu sa spracuje tzv. globálna systémová bezpečnostná politika, ktorá sa potom v druhej fáze podrobnejšie konkretizuje a spracúva do tzv. detailnej systémovej bezpečnostnej politiky.[2]

Informačná bezpečnosť je podľa medzinárodného štandardu **ISO/IEC 270001** ochrana informácie pred širokým spektrom hrozieb, ktorej cieľom je zaistenie kontinuity obchodných procesov, minimalizácia strát a maximalizácia návratnosti investícií. Informácia je obsahom údajov a vyskytuje sa v rozličných formách - písomnej, ústnej, obrazovej, elektronickej (digitálnej) a na jej spracovávanie (získavanie, prenos, spracovávanie, uchovávanie, archiváciu a ničenie) sa používajú

2 KUČERA, M a LÁTEČKOVÁ, A. (2004). Podnikové informačné systémy. Vydala Slovenská poľnohospodárska univerzita v Nitre - 22.11.2004. s. 135 – 136. ISBN 80-8069-452-4.

rozličné prostriedky. Keďže je informácia kľúčovým aktívom, bez ktorého len máloktorá organizácia môže plniť úspešné svoje poslanie, ohrozenie informácie je problém, ktorý treba rýchle a účinne riešiť. Adekvátna ochrana informácie vychádza z toho, na aký účel sa informácia používa a čo ju a akým spôsobom ohrozuje.

Základné bezpečnostné požiadavky na ochranu informácie sú dostupnosť, dôvernosť, autentickosť a integrita. Dostupnosť informácie znamená, že informácia je k dispozícií oprávneným osobám vždy, keď ju potrebujú. Zaistenie dôvernosti informácie znamená, že sa informácia nedostane do rúk neoprávneným osobám. Zaistenie integrity údajov vylučuje možnosť nepozorovanej zmeny údajov a napokon autentickosť informácie znamená zaistenie integrity a zároveň pôvodu dokumentu.

Informácia sa v čoraz väčšej miere spracováva v digitálnej/elektronickej forme pomocou počítačov a iných IKT systémov. Získať neoprávnený prístup k informáciám, narušiť ich dôvernosť, dostupnosť, integritu alebo autentickosť možno aj prostredníctvom útoku na IKT zariadenia, v ktorých sa informácia spracováva. Potenciálna možnosť narušenia informácií (či už priamo, alebo prostredníctvom útoku na technické zariadenie alebo prostredie, v ktorom sa informácia spracováva) sa nazýva hrozba. Hrozbou môže byť prírodný jav (oheň, blesk, povodeň), technická porucha systému alebo podpornej infraštruktúry (napájanie, klimatizácia), možný omyl používateľa, organizačné nedostatky (nezabezpečenie dostatočných zdrojov), nesúlad s legislatívnou (hroziace sankcie), krádež technického vybavenia, údajov, vandalizmus (poškodenie počítača alebo komunikačnej linky), nelegálny softvér ale aj možný cieľavedomý útok domáceho alebo externého útočníka (hackerstvo, zlomyseľný softvér). [3]

Informačná bezpečnosť podľa **Hennyeyovej, K. (2010)** je proces ochrany dát pred ich náhodným alebo úmyselným zneužitím osobami v rámci alebo mimo organizácie, vrátane zamestnancov, alebo aj obávaných hackerov. Narušenie bezpečnosti môže zahŕňať rôzne činnosti, napr. poškodenie vzhľadu webovej stránky, napadnutie počítačovým vírusom, zlyhanie zamestnanca, ktorý neúmyselne prezradí svoje heslo, a pod. Informačná bezpečnosť v tomto kontexte je vyváženie rizík výhodami v podobe vykonávania činnosti elektronicky.

3 ISO/IEC 27001:2005 – Information technology – Security techniques – Infromation security management systems – Requirements, prebratá aj do do STN ako STN ISO/IEC 27001.

Informačnú bezpečnosť vo všeobecnosti rozdeľujeme na informačnú bezpečnosť pre utajované skutočnosti a tzv. všeobecnú informačnú bezpečnosť, teda ochranu ostatných údajov. Utajované skutočnosti kompetenčne zastrešuje Národný bezpečnostný úrad SR, problematiku neutajovaných skutočností má vo svojej kompetencii Ministerstvo dopravy, pôst a telekomunikácií SR, pričom niektoré čiastkové oblasti majú na starosti ďalšie rezorty (napr. autorské práva v rámci digitálneho prostredia spadajú pod Ministerstvo kultúry SR). [4]

Pod pojmom bezpečnosť informačného systému sa podľa **Hrubca, J., Virčíkovej, E. a kolektívu (2009)** rozumieme ochranu všetkých údajov, ktoré systém obsahuje, sú doň vkladané, spracovávané a prenášané, ako aj ochranu všetkých častí – technických aj netechnických prostriedkov informačného systému. Bezpečnosť informačných systémov integruje fyzickú, počítačovú, komunikačnú, personálnu, administratívnu a prevádzkovú bezpečnosť. V systémoch s náročnejšími požiadavkami k týmto opatreniam pribudnú ešte opatrenia na zabránenie elektromagnetického vyžarovania. Súčasťou bezpečnosti informačných systémov sú nielen technické ale aj organizačné opatrenia.

Z hľadiska typu informačnej bezpečnosti rozlišujeme tieto druhy bezpečnosti:

- ✓ **fyzická bezpečnosť** – zahŕňa pôsobenie hrozieb na hmotné aktíva potrebné pre prevádzkovanie IS. Tieto aktíva sú nasadené do konkrétneho prostredia, ktoré sa dynamicky vyvíja. Fyzická bezpečnosť teda znamená ochranu informačného systému a jeho časti pred neoprávneným vzniknutím osôb, spôsoby zničenia už nepotrebných informácií alebo už nepotrebných médií s informáciami, ochranu pred požiarom, ochranu pred vodou, plánovanie havárií a riešenie krízových situácií.
- ✓ **komunikačná bezpečnosť** – treba eliminovať hrozby na hmotné a nehmotné aktíva nevyhnutné pre komunikáciu. Tu treba zahrnúť ako technické vybavenie, tak aj všeobecné štruktúry. Ide teda o ochranu komunikácie medzi jednotlivými časťami informačného systému, a to nielen z hľadiska výpočtovej techniky, ale aj z hľadiska prenosu faxových správ alebo telefonických rozhovorov.
- ✓ **počítačová bezpečnosť** - zahŕňa hrozby na hmotné aj nehmotné aktíva

4 Prispievatelia: HENNYEYOVÁ, K. Aspekty informačnej bezpečnosti v podnikaní, [online], [2010-11-16], Dostupné na: < http://bandlerova.weby.uniag.sk/files/web2/pdf/Hennyeyova.pdf>

potrebné pre spracovanie informácií. V praxi sa ďalej delí na bezpečnosť technického vybavenia a programového vybavenia. Pri zaisťovaní požadovanej bezpečnosti technických prostriedkov ide napríklad o výber a spoľahlivosť týchto prostriedkov, zabezpečenie ich okamžitého servisu, kontrolu prístupu k týmto prostriedkom, ich ochranu pred elektrostatickou elektrinou a elektromagnetickým vyžarovaním. Bezpečnosť programových prostriedkov smeruje napríklad k vyladeniu operačného systému takým spôsobom, aby bol skutočným filtrom prístupu k informáciám uloženým v IS – t.j. aby bola zabezpečená kontrola prístupu, identifikácia a autentizácia užívateľov, rozdelenie právomoci užívateľov, sledovanie a záznam činnosti systému aj užívateľov. Patrí sem tiež výber a spoľahlivosť programového vybavenia, jeho licenčná čistota, kontrola prístupu k nemu a pod.

- ✓ **informačná bezpečnosť** – zahŕňa pôsobenie hrozieb na nehmotné aktíva nevyhnutné pre fungovanie IS z hľadiska organizačného spracovania informácie. Tu treba zohľadniť najmä citlivosť, životnosť, platnosť dát a pod. Pri zaisťovaní bezpečnosti dát sa zaoberáme ochranou dát v súboroch a v databázach proti chybám, vírusom, ochranu citlivých dát prostriedkami autorizácie a riadenia prístupu k dátam.
- ✓ **personálna bezpečnosť** – zaoberá sa predovšetkým elimináciou hrozieb spôsobených ľudským faktorom. Ide v nej o ochranu pracovníkov ako súčastí informačného systému, ale tiež o ochranu IS pred dôsledkami udalosti spôsobených nekorektnou činnosťou pracovníkov.[5]

Vývoj informačnej bezpečnosti vo svete i na Slovensku

Prvé počítače (obdobie 1950-1975) boli umiestnené v špeciálne vybudovaných sálach s klimatizáciou, dvojitou podlahou, obsluhoval ich kvalifikovaný personál a používatelia k nim nemali priamy prístup. Údaje a programy boli zväčša uložené na diernych štítoch a magnetických páskach. Na ich zaistenie stačila fyzická ochrana prístupu, personálne a organizačné opatrenia mnohokrát využívajúce skúsenosti z vojenského prostredia. Prevažovali bezpečnostné incidenty spôsobené poruchou

5 HRUBEC, J., VIRČÍKOVÁ, E. a kolektív 2009. Integrovaný manažérsky systém. Slovenská poľnohospodárska univerzita v Nitra 2009, s.438-439, ISBN 978-80-552-0231-0.

technického vybavenia, chybou v programovom vybavení alebo údajoch, chybou obsluhy. Úmyselných útokov na počítače bolo relatívne málo, podnikali ich zväčša interní pracovníci, ktorí mali prístup k systémom, z osobných dôvodov (nespokojnosť, pomsta).

Rozvoj IKT priniesol pokles ceny počítačov a nárast oblastí, v ktorých ich bolo možné používať. V záujme zefektívnenia využívania stále ešte drahých počítačov a informačných zdrojov, ktoré predstavovali, používatelia získali vzdialený prístup k počítačom najprv prostredníctvom terminálov a neskôr pomocou lokálnych počítačových sietí. Cena, ktorú za to bolo potrebné zaplatiť, bola bezpečnosť. Používatelia získali možnosť pristupovať k cudzím údajom a zasahovať do cudzích programov. Ochrana založená najmä na fyzickej ochrane prístupu k centrálnemu systému už nepostačovala. Okrem zapojenia počítačov do lokálnych sietí bolo možné prepojiť počítače pomocou modemu a telefónnych liniek. To viedlo k vytvoreniu tzv. bulletin board service (BBS), systému umožňujúcemu posielanie a sťahovanie súborov prostredníctvom modemu a vznik prvých diskusných fór.

Zavedenie Internetu na rozhraní 80-90-tych rokov zmenilo situáciu ešte výraznejšie. Všeobecná konektivita každého s každým za prijateľnú cenu poskytla nebývalé možnosti rôznym nelegálnym aktivitám. Prvou výstrahou bolo objavenie počítačového červa (v roku 1988), autonómne sa rozmnožujúceho počítačového programu, ktorý infikoval tisíce počítačov a ochromil značnú časť internetu. Rozmohlo sa hackerstvo, najprv ako "nevinná" aktivita počítačových nadšencov, ktorí prienikom do cudzích počítačov dokazovali svoju odbornú zdatnosť, neskôr nadšencov nahradili profesionáli a exhibicionistické motívy nahradili ekonomické ciele. Objavili sa nové druhy "počítačovej hávede" zlomyseľného softvéru, ako počítačové vírusy a trójske kone, s rozvojom elektronickej pošty sa akútnou stala potreba zaistenia dôvernosti a autentickosti jej obsahu. Elektronické bankovníctvo stimulovalo aktivity zamerané na krádeže údajov umožňujúcich vyberanie peňazí z cudzích účtov, firmy ponúkajúce služby na Internete. Varovným prípadom je rozsiahly útok na web stránky Estónska (štátne orgány, finančné inštitúcie a médiá) z apríla a mája roku 2007, kde útočníci používali viacero typov útokov. Bolo to po prvýkrát v histórii, čo nejaký štát musel čeliť takému veľkému a koordinovanému útoku. IKT a najmä počítače sa stali aj nástrojom ekonomickej špionáže, či už v globálnom meradle, alebo v lokálnom (inštalácia špionážnych programov – spyware – na hostiteľské počítače za účelom získania zaujímavých informácií). Elektronická pošta sa stala kanálom na šírenie spamu,

nevyžiadaných správ s reklamou, ponukou tovarov a služieb. Hoci na rozdiel od iných foriem zneužívania IKT, spam nemá zjavne škodlivý obsah, rozmohol sa do takej miery, že predstavuje 70-80% objemu komunikácie na Internete a náklady na jeho šírenie a spracovanie (zmazanie) predstavujú v súčasnosti celosvetovo okolo 39 mld. Euro ročne. Zložitosť IKT a ich programového vybavenia zvyšuje pravdepodobnosť neúmyselnej chyby, ktorú je možné využívať na úspešný útok na systém. O stave informačnej bezpečnosti v Nemecku v roku 2007 sa uvádzajú znepokojujúce údaje:

- v roku 2006 renomovaná bezpečnostná firma objavila 7247 nových bezpečnostných slabín v systémoch, pričom vyše polovica z nich umožňovala získať prístup do systému s používateľskými, ba dokonca aj administrátorskými oprávneniami,
- časť od odhalenia bezpečnostnej slabiny po jej zverejnenie sa v priebehu 2 rokov skrátil v priemere zo 6,5 dňa na 3 dni.
- 44 % odhalených slabín bolo zverejnených spolu s návodom ako ich využiť.

Nič netušiaci používateľ sa môže stať nielen cieľom ale aj nástrojom útoku, útočník môže infiltrovať jeho počítač a vytvoriť z neho nástroj, odkiaľ bude podnikať útoky na iné systémy. S nástupom nových technológií (telefonovanie cez Internet, bezdrôtové siete, mobilná komunikácia, aktívny obsah webových stránok na Internete, rádiofrekvenčná identifikácia, riadenie technologických systémov sa objavujú aj nové bezpečnostné hrozby, ktoré treba zavčasu riešiť.[6]

1.2 Informácie a informačný systém

Podľa **Hennyeyovej, K. (2008)** sú informácie údaje (dáta) potrebné pre špecifické ciele. Umožňujú znížiť neurčitosť poznania, ovplyvňujú správanie, existencie, prácu a výrobné aktivity. Vzťah medzi dátami a informáciami možno preto prirovnávať ku vzťahu medzi surovinami a konečnými produktmi. Informácie predstavujú obrovský potenciál hospodárskeho rastu i rozvoja spoločnosti. Tvoria základ nastupujúcej informačnej spoločnosti. Informačnú infraštruktúru si v súčasnosti už nevie predstaviť bez zdieľania a prezentácie informácií prostredníctvom Internetu sú hnacou silou modernej doby. Informácie pre riadiacich pracovníkov by mali plniť nasledovné funkcie:

6 Prispievatelia: IT Asociácia Slovenska [online], [2008-09-01]. Dostupné na: <http://itas.sk/spravy/slovenskochce-mat-bezpecne-digitalne-prostredie>

- ✓ **diagnostická funkcia** – poskytuje znalosti o súčasnom stave skúmaného javu,
- ✓ **explikatívna funkcia** – vysvetľuje javy, ich súvislosti a príčiny, vytvára poznatky a skúsenosti,
- ✓ **predikačná funkcia** – využíva výsledky diagnostickej a explikatívnej funkcie na predpovedanie ďalšieho vývoja,
- ✓ **rozhodovacia funkcia** – na základe predchádzajúcich funkcií a syntéze poznatkov slúži na vypracovanie rôznych variantov a výber optimálneho riešenia.[7]

Podľa **Ivaničku (2000)** pre informácie sú charakteristické nasledujúce vlastnosti:

- ✓ znižujú neistotu, resp. neurčitosť u ich príjemcu, týkajúce sa procesov, alebo stavov systému, ktoré príjemca sleduje,
- ✓ môžu vznikať z dát buď ako výsledok prenosu dát, alebo ako výsledok transformácie dát a možno ich definovať iba priamo u príjemcu,
- ✓ nemusia byť fyzicky zaznamenané,
- ✓ majú obmedzenú životnosť, a preto sú len prechodnými veličinami,
- ✓ sú podkladom pri rozhodovaní,
- ✓ majú úžitkovú hodnotu a z nej odvodenú cenu, môžu sa teda stať tovarom so všetkými dôsledkami, ktoré z toho plynú.[8]

Podľa **Mikolaja, (2004)** informácie je "správa, údaj, hodnota, fakty, oznámenie o určitej udalosti, jave alebo činnosti, ktoré sa ďalej spracovávajú". Informáciou je označovaný aj druh poznania alebo správy, ktorý možno použiť v prospech priatia rozhodnutia alebo zlepšenia určitej činnosti, môžu existovať v mnohých formách. Môžu byť vytlačené alebo napísané na papieri, uložené elektronicky, prenášané poštou alebo pri použití elektronických prostriedkov, premietnuté vo filmoch alebo vyslovené v konverzáciách (ISO/IEC, 17799). Dátami sú informácie nachádzajúce sa na digitálnych záznamových nosičoch uložené v postupnosti určitých znakov.[9]

7 HENNEYOVÁ, K. 2001. Informačné technológie v riadení, In: Medzinárodné vedecké dni 2001, Nitra: SPU, 2001 s. 631-635. ISBN 80-7137-869-0

8 IVANIČKA, K. Manažérske informačné systémy. STU, Bratislava 2000, 153 s., ISBN 80-227-1369-4.

9 MIKOLAJ, J. – HOFREITER, L. – MACH, V. – MIHÓK, J. – SELINGER, P. 2004. Terminológia bezpečnostného manažmentu. Výkladový slovník. Košice: Multiprint s.r.o.2004, ISBN 80-969148-1-2.

1.2.1 Manažment rizika IS

Riziko informačného systému je možné chápať ako funkciu pravdepodobnosti s akou dôjde pôsobením konkrétnej hrozby k narušeniu dôvernosti, integrity a dostupnosti informácií v rámci daného systému v dôsledku poškodenia alebo zničenia informačných aktív, a výšky potenciálnych škôd.

Hrozba je skutočnosť alebo udalosť, ktorá môže spôsobiť poškodenie alebo zničenie informačného aktíva. Túto hrozbu môže predstavovať človek (vlastný zamestnanec, externý alebo dočasný pracovník, hacker a pod.), vplyvy techniky (porucha zariadení, výpadok alebo kolísanie elektrického napájania, komunikačné cesty a pod.) a iné. Poškodenia, ktoré vzniknú závadami techniky, prípadne prírodnými katastrofami, sa dajú identifikovať pomerne ľahko. Zložitejšia situácia vzniká pri nelegálnom úniku informácií, ktorý sa len ťažko dokazuje a prevádzkovateľ informačného systému nemá záujem na negatívnej publicite. Takéto odhalenie sa väčšinou na verejnosť nedostávajú.

Zraniteľnosť informačného systému predstavuje nedostatok slabé miesto celého bezpečnostného systému, ktoré môže byť zneužité hrozbou tak, že dôjde k poškodeniu alebo zničeniu informačných aktív. Veľké škody môže spôsobiť narušenie dôvernosti, integrity alebo dostupnosti tzv. citlivých údajov a informácie, preto si vyžadujú zvýšenú ochranu. Ide predovšetkým o personálne informácie (telefónne čísla, adresy a pod.), údaje chránené o účtoch, údaje o uzatvorených kontraktoch, databázy klientov.

Manažment rizika informačných systémov predstavuje proces pomocou ktorého je možné určiť, kontrolovať a obmedzovať vplyv náhodných udalostí – hrozieb. Obsahuje identifikáciu, analýzu a odhad resp. ocenenie rizík, implementáciu, testovanie a prevádzkovanie bezpečnosti. Ocenenie rizík je proces vyhodnotenia hrozieb pôsobiacich na informačný systém podniku s cieľom vyjadriť úroveň rizika, ktorému je systém vystavený. Správne ocenenie rizík umožňuje zistiť, či sú bezpečnostné opatrenia dostatočné.

1.2.2 Analýza rizika IS

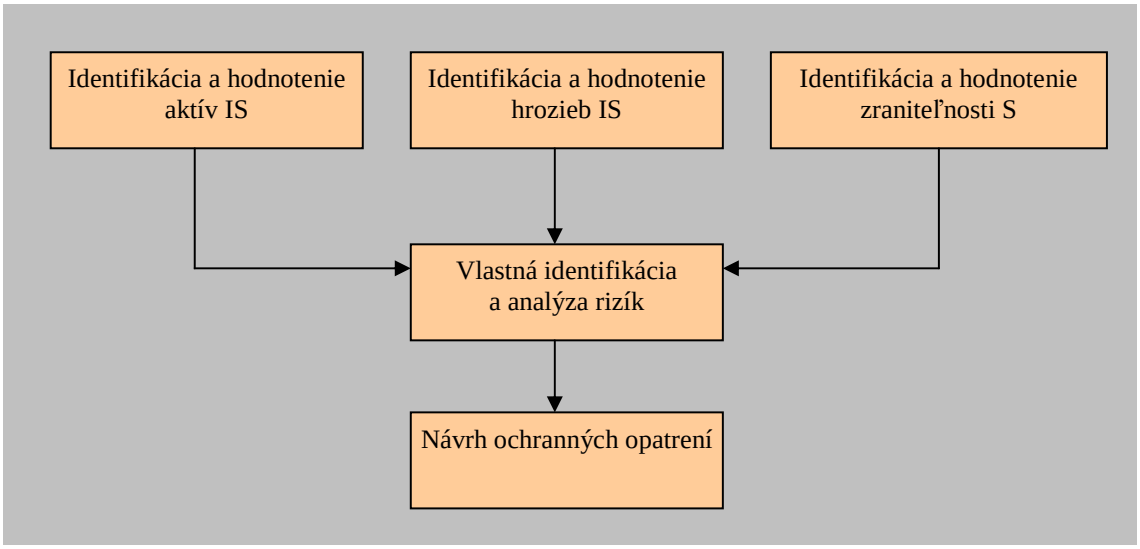
Analýza rizík je základným predpokladom na vytvorenie efektívneho systému ochrany a informačných systémov. Cieľom analýzy rizík je identifikovať a ohodnotiť hrozby, ktorým je informačný systém vystavený, aby mohli byť vybrané relevantné

ochranné opatrenia. Analýza rizík identifikuje hrozby a ich riziká, ktoré je potrebné akceptovať alebo korigovať.

V kontexte bezpečnosti systému model analýzy rizík zahrňuje:

- ✓ identifikáciu a hodnotenie aktív,
- ✓ hrozieb,
- ✓ zraniteľností,
- ✓ vlastná identifikácia a analýza rizík,
- ✓ návrh ochranných opatrení.

Riziká sú odhadnuté z hľadiska možného dopadu, spôsobeného narušením dôvernosti, integrity, dostupnosti atď. V závislosti od typu organizácie, zložitosti informačných systémov a výstupných požiadaviek, je možné zvoliť 4 základné prístupy k analýze rizík.



Obr. 1

Zjednodušený model analýzy rizík

*Zdroj: Khouri, S. – Al-Zabidi, D. 2010. Informačné systémy podniku***.**

1.2.3 Manažment bezpečnosti IS

Bezpečnosť informačných systémov môžeme identifikovať troma základnými požiadavkami:

- ✓ **dôvernos**ť – ochrana pred prezradením informácie,
- ✓ **integrita** – ochrana pred neoprávnenou modifikáciou,
- ✓ **dostupnosť** – ochrana pred neoprávneným odmietnutím služby alebo nemožnosťou poskytnúť informáciu.

Využívanie informačných systémov a technológií už dávno nie je módnou, alebo prestížnou záležitosťou, ale pre väčšinu podnikov prostriedok prežitia. Technologické, systémové a k nim pridružené personálne, fyzické a administratívne nedokonalosti spracovania informácií však využíva množstvo hrozieb. Tieto sa v závislosti od hodnoty informačných aktív, závislosti podniku na ich využívaní a pravdepodobnosti vzniku hrozby v kombinácií s jej následnou ničivosťou transformujú na väčšie, či menšie riziká.

Z rizík vznikajú množstvá menších, či väčších bezpečnostných incidentov, ktoré každý deň útočia na bezpečnosť informácií podniku. Podnik denne dostáva množstvá menších, či väčších zväčša neviditeľných "úderov" páchajúcich veľké škody. Vznikla oblasť informačnej bezpečnosti. Informačná bezpečnosť je o komplexnej ochrane informácií, kde patrí aj fyzická a objektová bezpečnosť, personálna bezpečnosť a administratívna bezpečnosť. [10]

Bezpečnostné riziká a ich identifikácia

Medzi závažné bezpečnostné riziká patria:

- ✓ **Získanie utajovaných údajov konkurenciou –** konkurencia môže využiť databázu kontaktov na podnikových zákazníkov, môže získať informácie o cenách, utajovaných výrobných technológiách alebo návodoch, tiež informácie o kľúčových zamestnancoch.
- ✓ **Strata dát -** strata databáz môže znamenať ohrozenie alebo spomalenie činnosti podniku, vysoké náklady na ich rekonštrukciu a častokrát aj stratu zákaziek

10 SAMER KHOURI – DENISA AL-ZABIDI 2010**.** Informačné systémy podniku**.** Košice: Dekanát – Edičné pracovisko Fakulty BERG, 2010, s. 99-103, ISBN 978-80-553-0373-4.

alebo reklamácie zákazníkov.

- ✓ **Prerušovanie chodu podniku –** nezvyčajne častá údržba systému, odstraňovanie porúch, nekompatibilita, znamená, že sa zamestnanci venujú inej činnosti než je zámer podniku. Zákazníci pochopia dočasné problémy iba ak sa nevyskytujú často a opakovane, najmä ak podnik prevádzkuje predajne alebo sklady.

Hlavné príčiny vzniku bezpečnostných rizík:

- ✓ **Ľudský faktor** - riziko vzniká tam, kde je informačný systém spracovávaný externe. Ani najlepšie technické riešenia nemôže zabrániť úmyslu či nedbalosti osôb s právami administrátora alebo aj užívateľov.
- ✓ **Umiestnenie serverov a iných nosičov informácií** - hovorí sa, že bezpečné dáta sú na zariadeniach, ktoré nie sú prepojené káblom. Zabúda sa na to, že niekto môže tiež toto zariadenie pripojiť alebo jednoducho odniesť.
- ✓ **Údržba** - informačné systémy vyžadujú pravidelné kontroly, údržba a upgrade softvérových častí, aby nedošlo k náhlemu zlyhaniu systému. Zavedením systému riadenia údržby je možné znížiť riziko náhleho zlyhania a obmedziť náklady tým, že sa hardware a software neobstaráva náhodne.

1.3 Medzinárodné normy informačnej bezpečnosti

Ako medzinárodný štandard pre riadenie informačnej bezpečnosti sa v poslednom období začali používať združené normy ISO a IEC, ktoré boli zaradené do novej skupiny noriem, označenej ako ISO/IEC 27000.

ISO vzniklo v roku 1947 ako organizácia, ktorej cieľom bolo zjednotiť národné normalizačné inštitúcie. V súčasnosti má ISO 151 členov. Každú členskú krajinu môže zastupovať len jedna inštitúcia. Slovenskú republiku zastupuje v ISO Slovenský ústav technickej normalizácie ako štátna inštitúcia. Pri práci s dokumentami ISO sa môžeme stretnúť s nasledujúcimi označeniami:

- **ISO Štandard** – normatívny dokument odsúhlasený požadovanou väčšinou hlasov členov.
- **ISO TR** – ISO Technical Report – technická správa z určitej technológie, na ktorú sa odvolávajú dokumenty ISO Standard.
- **ISO TS** - ISO Technical Specification technická špecifikácia, ktorú určitá technológia alebo riešenie musia spĺňať.

ISO sa zaoberá štandardizáciou väčšiny oblastí s výnimkou elektrotechniky. V tejto

oblasti sú dominantné združenia IEEE a IEC. Pre oblasti, ktoré navzájom súvisia, došlo medzi ISO a IEC k dohode o spoločnom používaní a označovaní dokumentov. Normy ISO nie sú povinné. To, že sa dostali do popredia a do používania, vyplýva skôr z potreby väčšiny entít mať určitý referenčný dokument, podľa ktorého by sa dali riadiť verejné alebo privátne kontrakty v medzinárodnom obchode. Tu sa normy ISO používajú ako nediskutovateľný dokument, ktorý zjednodušuje zmluvný vzťah, pretože obsahuje celosvetovo platné definície. Norma ISO sa však môže stať v určitom štáte povinnou, ak na ňu bude odkazovať štátny zákon. Normy ISO sa čoraz v širšom rozsahu používajú aj pri súdnych riešeniach právnych alebo technických sporov.

Odhliadnuc od normy ISO/IEC 27000, ktorá poskytuje základný prehľad v členení nových noriem a slovník základných používaných výrazov, možno začleniť existujúce normy do troch vrstiev vytváranej bezpečnostnej dokumentácie:

1. Základná vrstva bezpečnostnej dokumentácie,
2. Špecializovaná bezpečnostná dokumentácia,
3. Nadväzujúca bezpečnostná dokumentácia.

Základná vrstva bezpečnostnej dokumentácie

Do základnej vrstvy bezpečnostnej dokumentácie spoločnosti patria dokumenty Bezpečnostná politika a Bezpečnostná politika IT. Medzi základné normy, ktoré majú zásadný vplyv na tvorbu tejto bezpečnostnej dokumentácie, možno zaradiť normy 27001 a 27002.

- **Norma ISO/IEC 27001** je jedna z dvoch najstarších v tejto oblasti. Pôvodne bola vytvorená v roku 1995 vo Veľkej Británii ako britský štandard pod označením BS 7799-2 Britským úradom pre normy. V roku 2002 bola vydaná jej revízia. V roku 2005 bola táto britská norma prevzatá ako svetový štandard pod označením ISO/IEC 17799:2005, ale ešte v tom istom roku prečíslovaná do nového radu ako 270001. Uvedená norma stanovuje základné definície a definuje princípy organizácie bezpečnosti v organizácii. Definuje:

✓ ako vytvoriť a nasadiť do prevádzky bezpečnostné politiky,
✓ ako organizovať informačnú bezpečnosť,
✓ ako zabezpečiť ľudské zdroje,
✓ ako vytvoriť fyzickú bezpečnosť,
✓ ako riadiť komunikáciu a prevádzku IT,

- ✓ ako obstarávať prostriedky IT,
- ✓ ako riadiť incidenty,
- ✓ ako zabezpečiť kontinuitu činnosti spoločnosti.

- **Norma ISO/IEC 27002** je dvojčaťom normy 27001 a takisto vznikla vo Veľkej Británii pod označením BS7799-1. Organizácia ISO ju prevzala ako ISO/IEC 17799:2005. V roku 2007 bola prečíslovaná na súčasné označenie ISO/IEC 27002.

  Norma obsahuje súbor bezpečnostných opatrení (možno v nej napočítať viac ako 130 bezpečnostných opatrení v 39 bezpečnostných kategóriách), pričom sú pre kategórie a oblasti definované bezpečnostné ciele. Ku každému bezpečnostnému cieľu sa uvádzajú aj bezpečnostné opatrenia, ktoré umožňujú dosiahnuť bezpečnostný cieľ.

Špecializovaná bezpečnostná dokumentácia

Spoločnosti, ktoré sa neuspokoja so základnou bezpečnosťou dokumentáciou alebo im nepostačuje, si vytvárajú podrobnejšiu bezpečnostnú dokumentáciu. Táto bezpečnostná dokumentácia sa vytvára hlavne pre oblasti riadenia rizík, operačného riadenia, riadenia incidentov alebo napr. zlepšovanie už existujúcich bezpečnostných procesov.

- **Norma ISO/IEC 27003** štandardizuje praktický návod na implementovanie ISMS, definovaný v norme ISO/IEC 27003. Ochrana aktív (systémy, dáta, informácie, ľudia) musí byť riadená v kontexte rizík, ktoré sú s nimi spojené, a na úrovni, ktorú je ochotný akceptovať vrcholový manažment. Hlavný cieľ implementácie bezpečnostných štandardov je udržať obchodné procesy spoločnosti bez prerušenia, minimalizovať škody spojené s akýmkoľvek incidentom a zabrániť realizácii hrozieb. Táto norma je v súčasnosti ešte v štádiu finalizácie.
- **Norma ISO/IEC 27004** poskytuje návod na nasadenie procesu merania efektívnosti ISMS, pričom cieľ a opatrenia sú definované v norme ISO/IEC 27001.

Táto norma pomôže pri:

- ✓ definovaní, implementovaní a využívaní spôsobov merania stavu a kvality

dosiahnutej bezpečnosti,

- ✓ zbere, analýze a odkomunikovaním výsledkov s vlastníkmi procesov alebo inými zúčastnenými stranami,
- ✓ realizovaní zlepšovacích opatrení na základe získaných výsledkov,
- ✓ definovaní procesu kontinuálneho zlepšovania.

- **Norma ISO/IEC 27005** je norma na riadenie rizík informačnej bezpečnosti v organizáciách. Rozvíja koncept daný normou ISO/IEC 27001 a pomáha podrobnejšie definovať prístup k riadeniu rizík IT. Je použiteľná univerzálne pre všetky typy organizácií, ktoré chcú riadiť svoje riziká. Riadenie rizík je spojené s mnohými oblasťami riadenia spoločnosti od jednotlivých systémov až po komplexné obchodné procesy, a preto by malo byť integrované do väčšiny opisov procesov a väčšiny akčných plánov.

Do riadenia rizík by mali byť zahrnuté:

- ✓ potenciálne riziká, ktoré boli identifikované,
- ✓ priorita ich ošetrenia,
- ✓ vhodné opatrenia,
- ✓ analýza výskytu a následkov rizík,
- ✓ spôsoby informovanosti vrcholových orgánov,
- ✓ spôsoby monitorovania a vyhodnocovania efektivity vykonaných opatrení.

- **Norma ISO/IEC 27006 –** stojí trochu bokom od uplatnenia sa vo väčšine spoločnosti, pretože špecifikuje požiadavky a akreditačný návod pre entity, ktoré vykonávajú certifikáciu a registráciu systémov riadenia informačnej bezpečnosti budovaných podľa ISO/IEC 27001.

K zaujímavým a užitočným normám patria tiež nasledujúce:

- **ISO/IEC 27011** – Riadenie bezpečnosti pre telekomunikačné organizácie,
- **ISO/IEC 27012** – Riadenie bezpečnosti pre e-government služby,
- **ISO/IEC 27015** – Riadenie bezpečnosti pre finančné a poisťovacie služby, **ISO/IEC 27031** – Riadenie ICT pre kontinuitu procesov,
- **ISO/IEC 27032** – Riadenie kybernetickej bezpečnosti,
- **ISO/IEC 27033** – Skupina častí normy, ktoré sa budú zaoberať sieťovou bezpečnosťou: dizajn a implementácia sieťovej bezpečnosti, implementácia

bezpečnostných gateways, bezpečnosť VPN, Wireless a IP konvergenciou,

- **ISO/IEC 27034** – Bezpečnosť aplikácií,
- **ISO/IEC 27035** – Riadenie incidentov,
- **ISO/IEC 7036** – Riadenie outsourcingu.

- **Norma ISO/IEC 27013 –** ešte len vo fáze prípravy, ale ide o veľmi perspektívnu normu, pretože sa bude zaoberať prepojením noriem ISO/IEC 20000 a ISO/IEC 27000. Súbor noriem ISO/IEC 20000 sa týka problematiky obchodných procesov. Tieto normy boli vytvorené z pôvodného britského štandardu BS 15000. Hoci na rovnakom britskom štandarde bol vytvorený aj ITIL, nie sú ITIL a ISO/IEC 20000 rovnaké.

Nadväzujúca bezpečnostná dokumentácia

Existujú názory, že normy spomenuté v druhej časti už postačia na vybudovanie komplexnej bezpečnostnej dokumentácie. Tieto názory môžu byť pravdivé, ale aj nie. Existujú, totiž ešte oblastí, ktoré zatiaľ rozsah noriem radu 27xx neplánujú pokryť.

Ide napríklad o tieto problematiky:

- **ISO/IEC9796** – Elektronický podpis,
- **ISO/IEC9798** – Autentizácia entít,
- **ISO/IEC10118** – Definícia hash funkcií,
- **ISO/IEC11770** – Riadenie šifrovacích kľúčov,
- **ISO/IEC18014** – Časové pečiatky,
- **ISO/IEC18033** – Postupy šifrovania.
- V príprave sú aj nadväzujúce normy:
- **ISO/IEC19792** – Bezpečnosť biometrických informácií,
- **ISO/IEC24760** – Rámec pre identity manažment,
- **ISO/IEC29100** – Definícia rámca pre zaručenie súkromia.[11]

11 SAMER KHOURI – DENISA AL-ZABIDI 2010. Informačné systémy podniku. Košice: Dekanát – Edičné pracovisko Fakulty BERG, 2010, s. 104-108, ISBN 978-80-553-0373-4.

1.4 Prvky vplývajúce na informačnú bezpečnosť

Aktíva

Správne riadenie aktív je pre úspech spoločnosti životne dôležité a je hlavnou oblasťou, za ktorú zodpovedajú všetky stupne riadenia.

Aktíva spoločnosti zahŕňajú hmotné i nehmotné aktíva ako sú:

- ✓ **fyzické aktíva** (napr. počítačový hardvér, komunikačné prostriedky, budovy),
- ✓ **informácie/dáta** (napr. dokumenty, databázy),
- ✓ **softvér**,
- ✓ **schopnosť vytvárať určité produkty alebo poskytovať služby**,
- ✓ **personál,**
- ✓ **nehmotné hodnoty** (napr. abstraktné hodnoty spoločnosti, ako sú imidž, a dobré meno či povesť).

Väčšina alebo všetky z týchto aktív, môžu byť považované za dostatočne cenné na to, aby si zaslúžili určitý stupeň ochrany. Ak nie sú aktíva chránené, je nutné vykonať aspoň odhad rizík, ktoré sú týmto akceptované.

Z hľadiska bezpečnosti nie je možné implementovať a udržovať dobré riešenie bezpečnosti, ak nie sú identifikované aktíva spoločnosti.

V mnohých situáciách môže byť proces identifikácie aktív a určenia ich hodnoty vykonaný na vysokej úrovni, teda nie príliš podrobne a nemusí vyžadovať nákladnú, podrobnú a časovo náročnú analýzu. Potrebný stupeň podrobnosti pre túto analýzu by mal byť odvodený od pomeru času a nákladov súvisiacich s analýzou, voči hodnote aktív IT používaných spoločnosťou.

V každom prípade by mal byť stupeň podrobnosti analýzy aktív určený na základe bezpečnostných cieľov spoločnosti. V rade prípadov je užitočné združiť aktíva do určitých skupín aktív, ktoré majú svoje špecifické charakteristiky alebo vlastnosti.

Atribúty aktív, ktoré by sa mali vziať do úvahy, zahrňujú ich hodnotu alebo citlivosť a akékoľvek inhernetné ochranné opatrenia.

Požiadavky na ochranu aktív sú ovplyvňované ich zraniteľnosťou pri výskyte špecifických hrozieb. Ak sú tieto aspekty pre vlastníka aktív známe, mali by byť podchytené na tejto úrovni. Prostredie a kultúra, v ktorých organizácia vykonáva svoju činnosť, môžu ovplyvniť aktíva a ich atribúty. Napríklad niektoré kultúry považujú ochranu osobných informácií za veľmi dôležitú, zatiaľ čo iné prisudzujú tomuto

problému menší význam. Variácie prostredia a kultúr môžu mať význam pre medzinárodné organizácie a pre ich používanie systému IT bez ohľadu na medzinárodné hranice.

Hrozby

Aktíva sú predmetom pôsobenia mnohých typov hrozieb.

Hrozba má potenciálnu schopnosť spôsobiť nežiadúci incident, ktorý môže mať za následok poškodenie systému alebo organizácie a jej aktív. Táto škoda sa môže vyskytnúť ako dôsledok priameho alebo nepriameho útoku na informácie, s ktorými pracuje systém alebo služba IT, napr. ich neautorizované zničenie, sprístupnenie, modifikáciu, deformáciu a nedostupnosť alebo stratu. Aby hrozba spôsobila poškodenie aktív, využíva existujúcu zraniteľnosť aktív, ktorá je daná existujúcimi zraniteľnými miestami. Hrozby môžu mať prírodný alebo ľudský pôvod a môžu byť náhodné alebo úmyselné. Tak náhodné, ako aj úmyselné hrozby by mali byť identifikované a mala by byť odhadnutá ich potenciálna úroveň a pravdepodobnosť ich výskytu.

Tab. 1

Príklady možných hrozieb podľa ISO/IEC TR 13335

Ľudské hrozby		**Hrozby prostredia**
Úmyselné	**Náhodné**	
Odpočúvanie Zmena informácie Hacking systému Nepriateľský program Krádež	Chyby a zabudnutie Vymazanie súboru Nesprávne smerovanie Fyzické nehody	Zemetrasenie Blesk Povodeň Požiar

Zdroj: Strnád, O. 2009. Bezpečnosť a manažment informačných systémov.

Zraniteľnosť

Zraniteľnosti spojené s aktívami, zahrňujú slabé miesta existujúce vo fyzickej, organizačnej, procedurálnej, personálnej, riadiacej, administratívnej, hardvérovej, softvérovej oblasti alebo v oblasti informácií. Môžu byť využité hrozbami, ktoré môžu spôsobiť poškodenie systému IT alebo obchodných cieľov organizácie.

Zraniteľnosť sama o sebe nie je príčinou škody. Zraniteľnosť je iba podmienkou alebo množinou podmienok, ktoré môžu umožniť hrozbe, aby ovplyvnila aktíva. Je nutné zobrať do úvahy zraniteľnosti vznikajúce z rôznych zdrojov. Napríklad tú, ktorá je aktívam vlastná. Zraniteľnosť môže pretvárať do doby, pokiaľ sa aktíva samotné zmenia tak, že sa ich zraniteľnosť ďalej nedotýka.

Zraniteľnosť zahŕňa slabé miesta v systéme, ktoré môžu byť hrozbou využité a môžu viesť k nežiaducim následkom. To sú príležitosti, ktoré môžu umožniť hrozbe, aby spôsobila škodu. Všetky zraniteľné miesta vo vnútri špecifického systému alebo organizácie musia byť preskúmané z hľadiska hrozieb, ktoré im hrozia.

Okamžitú pozornosť si zaslúžia zraniteľné miesta, u ktorých bola detegrovaná určitá konkrétna hrozba. Prostredie, v ktorom organizácia pôsobí, sa môže dynamicky meniť, mali by byť všetky zraniteľné miesta monitorované, a tak identifikované tie zraniteľné miesta, ktoré začali byť ohrozované starými alebo novými hrozbami. Analýza zraniteľnosti je preskúmanie slabých miest, ktoré môžu byť využité a identifikované hrozbami. Táto analýza musí vziať do úvahy prostredie a existujúce ochranné opatrenia. Zraniteľnosť konkrétneho systému alebo aktíva voči určitej hrozbe je vyjadrením ľahkosti, s akou môže byť systém alebo aktívum poškodené.

Dopad

Dopad je dôsledok nežiaduceho incidentu, spôsobeného buď náhodne alebo úmyselne, ktorý má vplyv na aktíva. Následok bezpečnostného incidentu, ktorý vzniká vtedy, keď hrozba využila zraniteľné miesta systému, môže mať podobu zničenia určitých aktív, poškodenie systému IT a straty dôvernosti, integrity, dostupnosť dát, individuálnej zodpovednosti používateľa, autenticity alebo spoľahlivosti systému. Možné nepríjemné následky bezpečnostných incidentov zahrňujú taktiež finančné straty a stratu podielu na trhu alebo imidž organizácie.

Meranie dopadov umožňuje vytvorenie rovnováhy medzi následkami nežiaducich

incidentov a nákladmi na ochranné opatrenia slúžiace na ochranu pred nežiaducimi incidentmi. Musí sa prihliadnuť aj na početnosť výskytu nežiaduceho incidentu. To je veľmi dôležité. Aj keď je napríklad veľkosť škody spôsobenej každým výskytom nízka, môže byť súhrnný účinok mnohých incidentov v priebehu určitého času škodlivý. Odhad dopadov bezpečnostných incidentov je dôležitým prvkom pri odhade rizík a výbere ochranných opatrení.

Riziko

Riziko vyjadruje potenciálnu možnosť, že daná hrozba využije zraniteľnosť systému alebo organizácie, aby spôsobila stratu alebo poškodenie aktív alebo skupiny aktív, a teda priamo alebo nepriamo spoločnosti. Jednotlivé alebo viacnásobné hrozby môžu využiť jednotlivé alebo viaceré zraniteľné miesta.

Rizikový scenár opisuje, ako môže konkrétna hrozba alebo skupina hrozieb využiť konkrétnu zraniteľnosť alebo skupinu zraniteľností, ktorým sú vystavené aktíva s možnosťou poškodenia. Riziko je charakterizované kombináciou dvoch faktorov, a to pravdepodobnosťou výskytu nežiaduceho incidentu a jeho dopadom. Akákoľvek zmena aktív, hrozieb, zraniteľnosti a ochranných opatrení môže významne ovplyvniť riziká. Včasná detekcia alebo poznanie zmien v prostredí alebo v systéme zvyšuje príležitosť realizovať vhodné akcie pre zníženie rizika. [12]

Bezpečnostné opatrenia

Bezpečnostné opatrenia, či inak v praxi často nazývané ochranné opatrenia, sú praktiky, postupy alebo mechanizmy, ktoré môžu poskytnúť ochranu pred hrozbou, znížiť zraniteľnosť, obmedziť dopad nežiaduceho incidentu, detegovať nežiaduce incidenty a uľahčiť obnovu.

Účinná bezpečnosť konkrétneho prvku, či časti systému alebo spoločnosti obvykle vyžaduje kombináciu rôznych ochranných opatrení, aby aktívam poskytla primeraný stupeň bezpečnosti. Mechanizmus riadenia prístupu aplikovaný na počítače, by mal byť podporovaný auditnými kontrolami, personálnymi procedúrami, školením a fyzickou

12 STRNÁD, O. 2002. Manažment bezpečnosti IT. Vydala Slovenská technická univerzita v Bratislave vo Vydavateľstve STU, Bratislava 2002, 208 strán, ISBN 80-227-1696-0.

bezpečnosťou. Niektoré ochranné opatrenia môžu existovať už ako súčasť prostredia alebo ako inherentný aspekt aktív, môžu byť v systéme spoločnosti už platné.

Ochranné opatrenia môžu vykonávať jednu alebo viac nasledujúcich funkcií:

- ✓ detekciu,
- ✓ odstrašovanie,
- ✓ prevenciu,
- ✓ obmedzenie,
- ✓ korekciu,
- ✓ obnovu,
- ✓ monitorovanie,
- ✓ povedomie o probléme.

Na konkrétne implementovaný bezpečnostný program je podstatný vhodný výber ochranných opatrení. Mnoho ochranných môže plniť viacnásobné funkcie. Často je z pohľadu nákladov efektívnejšie vybrať ochranné opatrenia, ktoré spĺňajú viacnásobné funkcie.

Príklady oblastí, kde môžu byť použité ochranné opatrenia, zahrňujú:

- ✓ fyzické prostredie,
- ✓ technické prostredie (hardvér, softvér a komunikácie),
- ✓ personál,
- ✓ administratíva,

ale aj projektovanie systémov, vývoj softvéru, prevádzka IS, údržba a pod.

Povedomie o bezpečnosti je taktiež ochranné opatrenie a vzťahuje sa k personálnej oblasti. Prostredie a kultúra, v ktorých spoločnosti vykonávajú svoju činnosť, môžu mať vplyv na vybrané opatrenia a na povedomie o bezpečnosti v danej spoločnosti.

Určité ochranné opatrenia vysielajú dôrazný a jasný signál o postoji organizácie k bezpečnosti. V tomto smere je dôležité vybrať ochranné opatrenia, ktoré nie sú vo vzťahu ku kultúre alebo štátu, v ktorých spoločnosť vyvíja svoju činnosť, pohoršujúce.

Príkladmi bezpečnostných/ochranných opatrení sú:

- ✓ sieťové brány,
- ✓ monitorovanie a analýza siete,
- ✓ antivírusový softvér,
- ✓ šifrovanie dát na zaistenie dôvernosti,
- ✓ digitálny podpis,
- ✓ záložné kópie informácií,

- ✓ rezervné zdroje energie,
- ✓ mechanizmy riadenie prístupu a pod.

Obmedzenia

Obmedzenia na riešenie bezpečnosti sú obvykle určené vedením organizácie a časť z nich vyplýva z prostredia, v ktorom organizácia vyvíja svoju činnosť.
Príklady niektorých obmedzení, ktoré by mali byť brané do úvahy pri riešení bezpečností IT sú tieto:

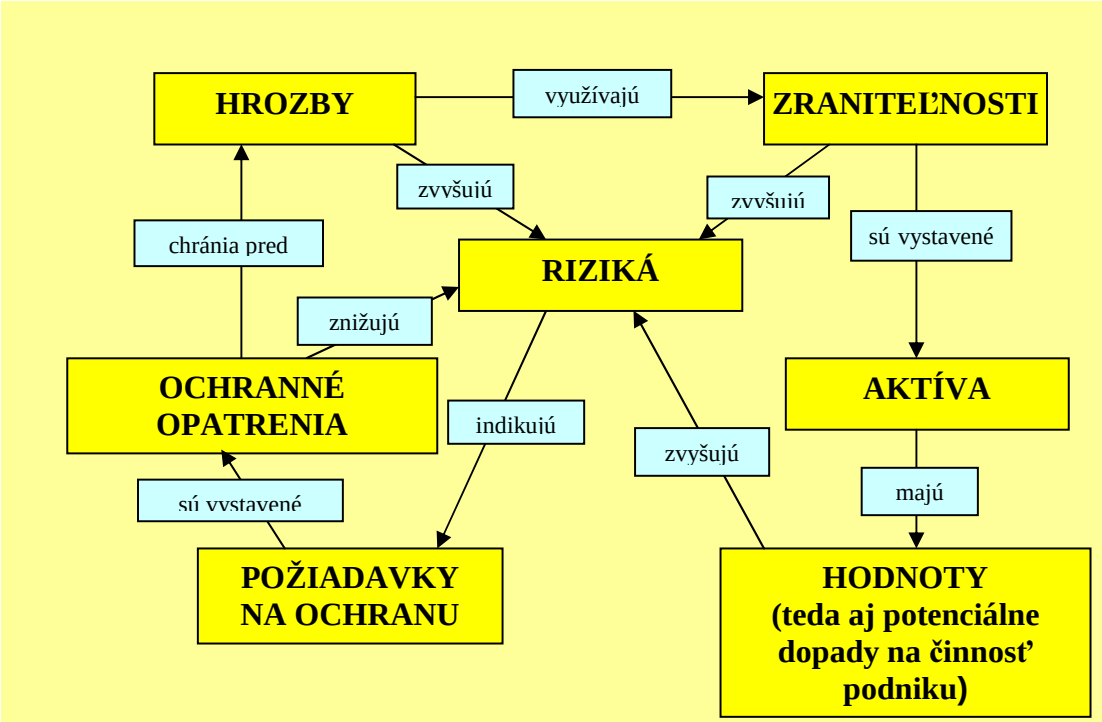
- ✓ organizačné,
- ✓ finančné,
- ✓ zníženie závislosti od prostredia,
- ✓ personálne,
- ✓ časové,
- ✓ právne,
- ✓ technické,
- ✓ kultúrno-sociálne.

Vzťahy medzi bezpečnostnými prvkami

Potreba poznať:

- ✓ čo zhoršuje informačnú bezpečnosť,
- ✓ čo ju zlepšuje,
- ✓ ako zabrániť jej zhoršovaniu,
- ✓ alebo ako dosiahnuť jej udržanie na určitej žiaducej úrovni**.**

Vedie riešiteľov k definovaniu prvkov, majúcich vplyv na informačnú bezpečnosť a súčasne k definovaniu vzťahov medzi nimi. Súčasťou prípravy rôznych subjektov na riešenie informačnej bezpečnosti, súčasťou prípravy poradensko-konzultačných firiem na realizáciu zákaziek súvisiacich s informačnou bezpečnosťou, ale aj súčasťou prípravy interných a externých auditorov systémov riadenia je vytvorenie alebo osvojenie metodiky riešiacej vzťahy medzi prvkami. Za určité zjednotenie rôznych názorov na prvky majúce vplyv na informačnú bezpečnosť a ich vzťahy možno považovať model znázornený v schéme č.1.



Obr. 2

Základné vzťahy medzi bezpečnostnými prvkami

Zdroj: Strnád, O. 2009. Bezpečnosť a manažment informačných systémov.

Základné vzťahy medzi bezpečnostnými prvkami

Zo schémy okrem iného napr. vyplýva, že:

- ✓ ochranné opatrenia chránia aktíva organizácie pred hrozbami využívajúcimi zraniteľné miesta aktív,
- ✓ zraniteľné miesta zvyšujú potenciálne bezpečnostné riziká organizácie a indikujú požiadavky na ochranu, ktoré sú splnené implementáciou bezpečnostných opatrení,
- ✓ hrozby zvyšujú bezpečnostné riziká, ktoré vyvolávajú potrebu implementácie bezpečnostných opatrení. [13]

13 STRNÁD ONDREJ. 2009. Bezpečnosť a manažment informačných systémov. Bratislava: Nakladateľstvo Slovenskej technickej univerzity 2009, 343 strán, ISBN 978-80-227-3040-2.

2. CIEĽ PRÁCE

Potreba riešiť problematiku bezpečnosti informačných technológií a systémov je v súčasnosti stále naliehavejšia. V oblasti manažmentu sa stále rýchlejšie rozvíja nová disciplína, ktorá sa nazýva manažment informačnej bezpečnosti.

Pod pojmom "informačná bezpečnosť" sa rozumie ochrana informácií počas ich vzniku spracovania, ukladania, prenosu a likvidácie, prostredníctvom technických, fyzických, logických a organizačných opatrení, ktoré pôsobia proti ich dôvernosti, strate, integrite ako aj dostupnosti.

Bezpečnosť informačného systému nie je možné úplne zaistiť, a taktiež snaha o priblíženie sa k vysokej bezpečnosti je neúmerne finančne náročná. Efektívnym fungovaním manažmentu informačnej bezpečnosti systému je, možné riziká optimálne eliminovať.

Cieľom diplomovej práce je posúdiť úroveň bezpečnosti digitálneho prostredia v SR, definovať bezpečnostné hrozby a navrhnúť ďalšie možnosti zvyšovania digitálnej bezpečnosti v podnikoch. Na splnenie hlavného cieľa diplomovej práce som si stanovila nasledujúce čiastkové ciele:

- ✓ charakterizovať vývoj informačnej bezpečnosti vo svete i na Slovensku,
- ✓ charakterizovať jednotlivé pojmy súvisiace so skúmanou problematikou,
- ✓ analyzovať bezpečnosť informačného systému z hľadiska bežného užívateľa "domácnosť" a analyzovať bezpečnosť informačného systému z hľadiska firmy "X",
- ✓ definovať bezpečnostné hrozby a riziká v podnikoch,
- ✓ navrhnúť riešenie bezpečnostnej politiky vo firme "X".

3. METODIKA PRÁCE

Predmetom diplomovej práce je riešenie problematiky bezpečnosti digitálneho prostredia. Táto problematika bezpečností informačných systémov patrí v súčasnosti k zaujímavým témam v oblasti IT. Každá organizácia by mala zabezpečovať svoje informačné systémy zodpovedne a rovnako. Sú taktiež pre organizáciu dôležité, ako ktorékoľvek iné investície. Každá organizácia, či už malá alebo veľká, je závislá od informácií, ktoré prijímajú, spracúvajú, uchovávajú, poskytujú, chránia alebo s nimi akokoľvek narábajú. Preto predmetom záujmov každej firmy, organizácie štátnej či verejnej správy by mala byť informačná bezpečnosť, čiže ochrana informácií.

V úvode diplomovej práce sa zameriavam na vývoj informačnej bezpečnosti, charakteristike a významu jednotlivých pojmov, akými sú napríklad: bezpečnostná politika, informačná bezpečnosť, bezpečnosť informačného systému, informácie a informačný systém, podľa názorov a myšlienok rôznych slovenských a zahraničných osobností. Dôležité bolo preštudovanie literatúry, ktorá sa skúmanou problematikou zaoberá, získať väčší prehľad o problematike bezpečnostného informačného systému.

Základnými zdrojmi informácií pre spracovanie diplomovej práce boli:

- ✓ odborná literatúra od slovenských a zahraničných autorov,
- ✓ články z počítačových časopisov,
- ✓ internet,
- ✓ knižnica,
- ✓ a iné dostupné informačné a programové prostriedky.

V diplomovej práci som charakterizovala bezpečnostné riziká a príčiny ich vzniku, pozornosť je venovaná manažmentu informačného systému a prvkom, ktoré vplývajú na informačnú bezpečnosť, hlavne pojmom aktíva, hrozby, zraniteľnosť, dopad, riziko a bezpečnostné opatrenia, ďalej manažmentu bezpečnosti informačného systému konkrétne pojmom dôvernosť, dostupnosť a integrita.

Firma (spoločnosť), v ktorej pracujem a budem sa aj v práci venovať, si neželá byť zverejnená, preto budem používať označenie ako firma „X“, aby som neporušila jej autorské práva.

Pozornosť je zameraná aj na medzinárodné normy informačnej bezpečnosti. Členenie sektorov národného hospodárstva máme z viacerých hľadísk, v práci som sa

zamerala na členenie podľa vlastníctva a to hlavne na sektor súkromný a sektor domácnosti. Pozornosť je venovaná sektoru domácnosti - bežnému užívateľovi internetu a sektoru súkromnému - nemenovanej firme "X".

Pri vypracovaní práce boli použité metódy analýzy, syntézy, dedukcie, indukcie, riadeného rozhovoru.

- **Analýza** predstavuje rozklad alebo rozbor určitého celku (javu) na jednotlivé časti. Táto metóda je použitá pri skúmaní vývoja a súčasného bezpečnostného informačného systému na Slovensku.
- **Syntéza** je myšlienkové spájanie súčasti predmetu alebo javu do jedného celku, predstavuje skúmanie javu a predmetu ako jednoty.
- **Indukcia** ako metóda skúmania je spôsob empirického štúdia javov, pri ktorom sa uskutočňuje prechod od jednotlivých faktorov ku všeobecným tendenciám. V reálnom poznaní indukcia vystupuje vždy v jednote s dedukciou, t. j. vyvodením záverov z jedného resp. z viacerých tvrdení. Tieto boli použité v záverečnej časti bakalárskej práce.
- **Riadený rozhovor** – predstavuje metódu získavania dôležitých informácií na základe cieľavedomého a usmerňovaného rozhovoru. Metóda riadeného rozhovoru bola použitá pri získavaní údajov o firme "X" od administratívnych pracovníkov a programátorov.

4. VLASTNÁ PRÁCA

4.1 Charakteristika podnikateľského subjektu firmy "X"

Spoločnosť „X" je jednou z najväčších IT spoločností na svete a poskytuje klientom svoje služby už viac ako 85 rokov. Celosvetovo pôsobí vo vyše 170 krajinách, pričom neustále rozširuje svoje geografické pokrytie, a zamestnáva 400 tisíc zamestnancov. Akvizíciami spoločnosť posilňuje a dopĺňa svoje portfólio produktov a riešení, urýchľuje inováciu a rozširuje príležitosti pre svojich obchodných partnerov.

Jej poslaním je pomocou integrovaných, flexibilných a efektívnych riešení pomáhať svojím zákazníkom redukovať náklady a zvýšiť tak ich konkurencieschopnosť na trhu. Pomocou širokého spektra IT technológií a riešení, od serverov a systémov na ukladanie dát až po softvér a IT služby vrátane konzultačných a implementačných služieb spoločnosť „X" spoločne so svojimi obchodnými partnermi prinášajú riešenia prispôsobené potrebám jednotlivých zákazníkov. Patrí k lídrom vo vytváraní, vývoji a výrobe priemyselne najpokrokovejších informačných technológií. Spoločnosť v roku 2009 zaregistrovala v USA 4914 patentov, čím sa už vlastne po sedemnásty rok v poradí dostala na čelo rebríčka najinovatívnejších spoločností na svete. Celkový počet patentov v spoločnosti v roku 2009 je takmer štvornásobne vyšší ako skóre spoločnosti Hewlett-Packard a je dokonca vyšší ako súčet patentov spoločností Microsoft, Hewlett-packard, Oracle, Apple, Accenture a Google dokopy.

Víziou spoločnosti je prinášať inteligentné riešenia do všetkých sfér života. V roku 2008 spoločnosť rozbehla celosvetovú kampaň Smarter Planet (Inteligentná planéta), ktorá prepája obchodnú stratégiu so stratégiou zodpovedného podnikania. Jej aktivity sú navrhnuté tak, aby zlepšili kvalitu života jednotlivcom i komunitám prostredníctvom inteligentných riešení v doprave, zdravotníctve, bankovníctve, verejnej správe či energetike a prispievali k trvalo udržateľnému rozvoju budovania inteligentnej planéty.

„X" na Slovensku

Na Slovensku spoločnosť pôsobí od roku 1990. Do rozpadu ČSFR v roku 1993 realizovala svoje aktivity na celom území Slovenska, prostredníctvom pobočiek v Bratislave a v Košiciach.

Samostatná pobočka „X" Slovensko s.r.o. bola založená 7. decembra 1992 a jej súčasným generálnym riaditeľom je Roman Brestovanský. Hlavné sídlo „X" Slovensko sa nachádza v Bratislave s pobočkami v Banskej Bystrici a Košiciach. V roku 2003

založila „X“ na Slovensku druhú spoločnosť International Services Centres s.r.o. (ISC), ktorá zastrešuje centrá poskytujúce služby interných i externých klientov na celom svete. Pred desiatimi rokmi ako prvá na slovenskom trhu prišla spoločnosť s projektom vytvorenia medzinárodných centier. Hlavne vďaka dostatočnému množstvu kvalifikovaných ľudí a výbornej geografickej polohe počet centier rástol a v súčasnosti na Slovensku funguje 32 medzinárodných centier. V centrách pracujú mladí ľudia v tímoch a priemerný vek zamestnancov s rôznymi národnosťami je 28 rokov, pričom prevahu majú ženy, tvoria 63% zamestnaných, zamestnaných je približne 1500 zamestnancov, s funkciami manažérov, teamlíderov, administrátorov, programátorov, informačných technikov, sekretárok atď.

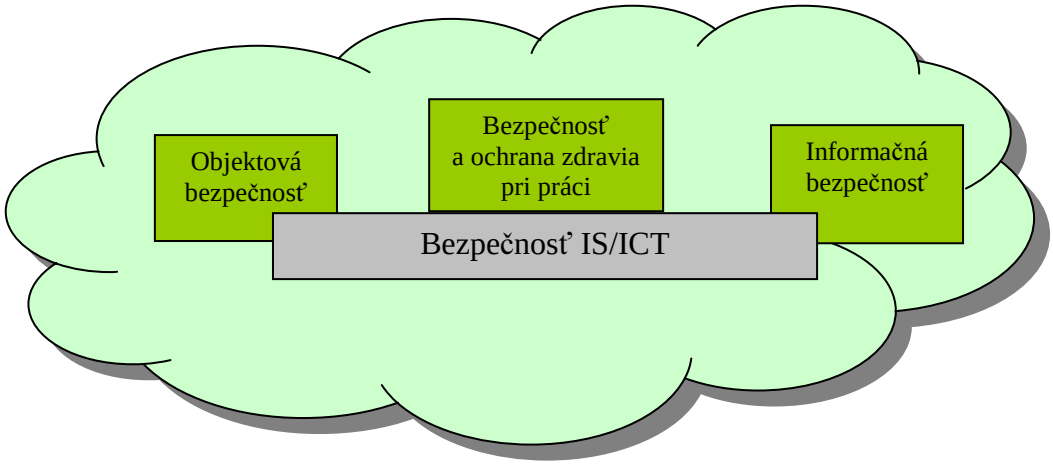
Počas svojho 20-ročného pôsobenia na Slovenskom trhu spoločnosť výrazne rozšírila portfólio svojich produktov a poskytovaných služieb v oblasti informačných technológií s dôrazom na komplexné riešenie a IT služby s vysokou pridanou hodnotou. Klient si môže vybrať so širokej škály serverov, softvéru, diskových úložných systémov, konzultačných služieb či IT služieb ako napríklad zabezpečenie kontinuity procesov, riadenie IT infraštruktúry, sieťové služby, outsourcing, bezpečnosť a mnohé iné. Svojimi riešeniami pomáha klientom upevňovať ich pozíciu na trhu a posúva environmentálnu víziu za hranice tradičných biznis oblastí. Prostredníctvom energetický úsporného „zeleného“ dátového centra, ktoré prispeje k zníženiu spotreby elektrickej energie, zabezpečí zlepšenie ochrany dát a z dlhodobého hľadiska zníži náklady na prevádzku. Dokáže zákazníkom pomôcť aj pri financovaní projektov a IT technológií.

4.2 Bezpečnosť informačných systémov firmy „X“

Problematika bezpečnosti informačných systémov v našej firme patrí k obzvlášť aktuálnym témam v oblasti IT, vzhľadom k štandardizácii a nárastu objemu výmeny dát pomocou komunikačných sietí. Informačné systémy musí naše firma zabezpečovať rovnako, ako ktorékoľvek svoje investície. Oblasť bezpečnosti a jej aktuálne zabezpečenie je pomerne komplikovaná záležitosť a skladá sa z mnohých krokov a činnosti.

Zabezpečenie bezpečnosti IS/ICT sa v našej firme „X“ premieta do riešenia:

- ✓ bezpečnosti objektov, kde je riešená ochrana budov a priestorov, t. j. ich stráženie, vrátane zabezpečenia požiarnej a ďalšej ochrany,
- ✓ bezpečnosti a ochrane zdravie pri práci, kde závislosť od podmienok a charakteru činnosti organizácie dochádza k zabezpečovaniu ochrany zdravia pracovníkov,
- ✓ bezpečnosť informačná, zahŕňajúca ochranu informačných aktív organizácie.



Obr. 3

Zabezpečenie bezpečnosti našej firmy „X“

Zdroj: vlastné spracovanie.

4.2.1 Objektová bezpečnosť

Fyzickú ochranu objektu a aj chráneného priestoru môžu vykonávať napr. príslušníci ozbrojených síl, ozbrojených bezpečnostných zborov, trvalo prítomní ozbrojení zamestnanci, zamestnanci súkromných bezpečnostných služieb (SBS) alebo vyškolení zamestnanci prevádzkovateľa objektu, alebo určení vlastní zamestnanci, u nás vo firme je to SBS. Fyzická ochrana objektu je zabezpečená aj kontrolou hranice objektu predovšetkým mimo pracovného času, použitím elektrického zabezpečovacieho systému.

Pod pojmom fyzická ochrana (Zákon 473/2005 Z.z. o poskytovaní služieb v oblasti súkromnej bezpečnosti) sa rozumie obchôdzka, stráženie, prevádzkovanie zabezpečovacieho systému alebo poplachového systému a priame riadenie a kontrola týchto činnosti.

Úlohou našej súkromnej bezpečnostnej služby (SBS) vo firme je kontrolovanie zamestnancov pri vstupe a výstupe do firmy. Každý zamestnanec sa musí preukázať čípovým preukazom, na ktorom je zobrazená fotka zamestnanca firmy. Zamestnanec SBS nemôže povoliť vstup zamestnancovi, ktorí si čipovú kartu zabudol, pretože by porušil svoju pracovnú povinnosť, aj SBS pracovníci sú vlastne sledovaní kamerovým systémom. Ak si zamestnanec kartu neprinesie so sebou do práce, z dôvodu zabudnutia si karty, dostane náhradnú čipovú kartu, ktorá mu platí 24 hodín odo dňa vystavenia, jeho pravá čipová karta je automatický deaktivovaná a môže si ju aktivovať až keď vráti náhradnú čipovú kartu, systém je nastavený tak, že nedovolí zamestnancovi používať dve karty naraz. Čipové karty slúžia taktiež na otváranie dverí, bez tejto čipovej karty sa zamestnanec nedostaneme ani do jednotlivých objektov budovy. V prípade straty čipovej karty hrozí zamestnancovi pokuta a vystaví sa mu nová karta.

Fyzické bezpečnostné opatrenia sú len jednou časťou bezpečnostnej ochrany a majú podporovať opatrenia personálnej bezpečnosti, informačnej bezpečnosti a ďalších bezpečnostných opatrení.

Opatrenia fyzickej bezpečnosti musia byť preto projektované tak, aby:

- zabránili neoprávnenému alebo násilnému vstupu narušiteľa do objektu,
- odradzovali, sťažovali a detekovali akcie nelojálneho personálu,
- umožňovali rozlišovanie personálu podľa stupňa oprávnenia prístupu k utajovaným informáciám podľa zásady,
- čo najskôr detekovali každý bezpečnostný incident.

Fyzické bezpečnostné opatrenia v našej firme musia obsahovať:

- požiadavky na organizáciu a štruktúrovanie zabezpečených oblastí,
- definovanie administratívnej zóny,
- vstupné a výstupné prehliadky,
- stráže,
- fyzická ochrana kopírovacích a faxových prístrojov,
- zariadenia pre detekovanie narušiteľa.

4.2.2 Bezpečnosť a ochrana zdravia pri práci firmy

Podľa zákonníka práce, ktorý ukladá zamestnávateľovi povinnosť preškoliť každého zamestnanca sa uskutočňuje toto školenie každé dva roky a všetci zamestnanci firmy majú povinnosť, toto školenie absolvovať. Ak sa nemôžu dostaviť na termín, na ktorý sú pozvaní, ich povinnosťou je, to príslušnému konateľovi školenia oznámiť a zúčastniť sa školenia v ďalšom možnom termíne. Na tomto školení sa vystavuje prezenčná listina zúčastnených zamestnancov. Preventívne sa v našej firme uskutočňujú cvičenia, v ktorých sa zamestnanci snažia nacvičiť si evakuáciu, v prípade ohrozenia firmy pred požiarom.

Technické prostriedky ochrany

Technické prostriedky ochrany sú systémy, ktoré slúžia na ochranu majetku a osoby pred neoprávnenými zásahmi, prostredníctvom systémov a zariadení umožňujúcich sledovanie pohybu a prejavu osoby v objekte a jeho okolí. Sú tvorené súhrnom zabezpečovacích a poplachových systémov. Zabezpečovacie systémy a poplachové systémy, nazývané aj ako technické prostriedky, tvoria systém prostriedkov na získanie a vyhodnocovanie informácií z prostredia stráženého objektu alebo z jeho časti. Sú známe:

- ✓ prostriedky protipožiarnej ochrany, ktoré predstavujú súbor hlásičov požiaru, ústrední EPS a doplňujúcich zariadení EPS, vytvárajúcich systém slúžiaci na preventívnu ochranu objektov pred požiarmi tak, že akusticky a opticky signalizuje vznik a miesto požiaru.
- ✓ prostriedky na obvodovú ochranu, ktoré zaisťujú bezpečnosť okolo chráneného objektu a signalizujú narušenie obvodu objektu. Sú to vonkajšie

technické prostriedky, vyrábané pre tento účel, napr. rôzne druhy vonkajších mechanických zábranných prostriedkov a tiež rôzne pasívne infračervené alebo mikrovlnové bariéry a snímače pohybu.

- ✓ prostriedky objektovej ochrany: plášťovej, priestorovej, predmetovej a osobnej ochrany. Patria sem všetky druhy prvkov poplachových systémov na hlásenie narušenia, ako napr.: detektory pohybu, zvuku, rozbitia skla, magnetické snímače, prostriedky predmetovej ochrany, osobné tiesňové hlásiče, prvky poplachovej prenosovej cesty, výstupná signalizácia a pod. Patria sem aj rôzne druhy kamerových systémov, systémy kontroly vstupu a dochádzky a iné.

Technické prostriedky ochrany, ktoré zohrávajú dôležitú úlohu v našej firme:

- ✓ poplachové systémy,
- ✓ elektrický zabezpečovací systém,
- ✓ elektrický požiarna signalizácia,
- ✓ systémy priemyselnej televízie.

Poplachové systémy

Samy o sebe nie sú ochranou v pravom slova zmysle, majú iba odstrašujúci účinok, páchateľovi v ničom nezabráni. Má dve základné úlohy:

- podporovať mechanické zábranné systémy - dodať informáciu o narušení a umožniť fyzickej ochrane včas zasiahnuť,
- zvyšovať efektívnosť fyzickej ochrany, použitím poplachových systémov sa znižuje počet bezpečnostných pracovníkov pri ochrane objektu.

Do poplachových systémov zaraďujeme:

-elektrické zabezpečovacie systémy (EZS),

-elektrickú požiarnu signalizáciu (EPS),

-priemyselnú televíziu (CCTV), videosystémy, počítačom riadené systémy.

Elektrický zabezpečovací systém

EZS predstavuje celý rad skupín zariadení a prvkov plášťovej ochrany, priestorovej ochrany, predmetovej ochrany, snímačov, ovládacích a signalizačných zariadení, zariadení na prenos informácií na pult centralizovanej ochrany.

Slúžia na signalizáciu nebezpečenstva, ktoré nám ohrozuje život a majetok. Ich súčasťou je aj zariadenie na spracovanie a prenos poplachových správ, vrátane napájania týchto zariadení elektrickým prúdom. Tieto zariadenia tvoria zabezpečovací reťazec, snímač je zariadenie, ktoré sleduje určité parametre svojho okolia a pri odchýlke z vopred stanovenej medze reaguje odovzdaním určitej informácie.

Ústredňa spracováva informácie zo snímačov podľa stanoveného programu a realizuje ich požadovaným spôsobom. Umožňuje aj riadenie zabezpečovacieho systému a zaisťuje jeho napájanie elektrickým prúdom. Prenosové prostriedky zaisťujú prenos informácií z ústredne do miesta signalizácie, alebo pokynov v opačnom smere. Signalizačné zariadenie zaisťuje odovzdávanie informácií do vhodnej formy.

Elektrická požiarna signalizácia

EPS je súbor technických zariadení, ktoré slúžia na to, aby zisťovali požiar už pri jeho vzniku, rýchlo privolali na miesto vznikajúceho požiaru osobu, ktorá je schopná začínajúci požiar zlikvidovať, alebo privolať ďalšiu pomoc. Medzi hlavné úlohy EPS patrí rýchle a spoľahlivé určenie miesta požiaru už v samotnom počiatku zahorenia, vyhlásenie poplachu, aktivácia a riadenie evakuačného systému v zasiahnutých oblastiach. V niektorých prípadoch realizuje aj automatickú komunikáciu s hasičským záchranným zborom. Tvorí základnú súčasť systémov požiarne bezpečnostného zariadenia, lebo jej význam vo väčšine prípadov prevyšuje ostatné zabezpečovacie systémy ako z hľadiska chráneného objektu, tak aj jej základnou, nenahraditeľnou úlohou – ochrany života a zdravia osôb.

Vznik požiaru signalizujú hlásiče, ktoré pracujú na rôznych princípoch, pôsobením mechanických, optických, akustických a iných fyzikálnych či chemických dejov.
Mechanické hlásiče – používajú sa v priestoroch obsluhy, ktorá po vyhodnotení nebezpečnej situácie, po rozbití skla, aktivuje tlačidlom systém EPS.
Automatické hlásiče – samé reagujú na zmenu fyzikálnych parametrov a aktivujú prihlasovací systém.

Systémy priemyselnej televízie (CCTV) – priemyselná televízia

Slúži na prenos pohyblivých obrazov na diaľku. Má uzatvorený okruh užívateľov a stále častejšie sa používa v kombinácii s PSN (EZS). Je to informačný prostriedok,

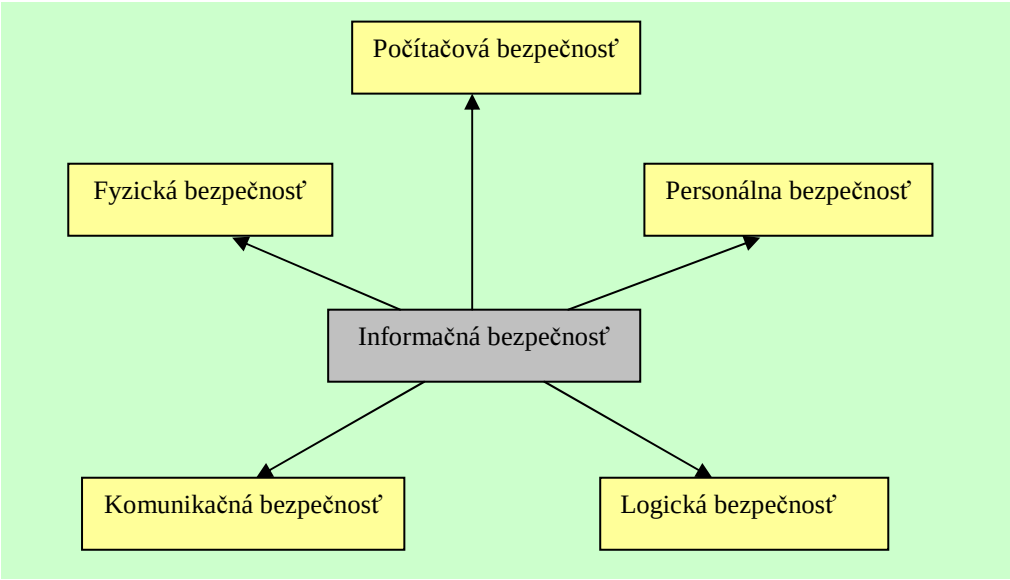
ktorý zvyšuje efektívnosť výkonu strážnej služby. Slúži aj na dokumentáciu toho, čo sa v strážených priestoroch robí.

Za zabezpečovacie zariadenie sa môže považovať, ak je doplnené videozáznamom a zmeny v stráženom objekte hlási automaticky, alebo je obsluhovaná stálou službou, ktorá neustále sleduje monitor. Na zabezpečenie objektov sa nasadzuje priemyselná televízia najmä na stráženie brán a vchodov, pozemkov a objektov, plotov, atď.

4.2.3 Informačná bezpečnosť

Firma musí stále čeliť rôznym bezpečnostným hrozbám ako napr. počítačové podvody, počítačová špionáž, resp. sabotáž, vandalizmus, požiare alebo záplavy. Väčšina informačných systémov nebola navrhnutá so zreteľom na bezpečnosť, ale na funkčnosť. Úroveň bezpečnosti možno dosiahnuť výhradne technickými prostriedkami, je obmedzená a mala by byť podporovaná vhodným riadením. Komplexné riadenie informačnej bezpečnosti si vyžaduje účasť zamestnancov organizácie, dodávateľov, ale aj zákazníkov.

Z hľadiska pohľadu na informačnú bezpečnosť je možné rozlišovať aj v našej firme tieto druhy bezpečnosti:



Obr. 4

Rozdelenie informačnej bezpečnosti firmy "X"

Zdroj: vlastné spracovanie.

Hrozby v oblasti fyzickej bezpečnosti

Informačnú bezpečnosť ovplyvňujú hrozby. Okrem delenia na úmyselné a neúmyselné, delíme hrozby z pohľadu jednotlivých častí informačnej bezpečnosti na:

- ✓ vyhotovenie neautorizovanej kópie dokumentov (napr. pomocou skenera, fotoaparátu, kopírovacieho zariadenia),
- ✓ neautorizovaný prístup k dokumentom v papierovej forme, spôsobený prehľadávaním odpadkových košov,
- ✓ požiar,
- ✓ skrat na elektrickom vedení,
- ✓ nepovolený fyzický prístup k prenosným záznamovým médiám, napr. CD/DVD-R, FDD, sieťovým prvkom (napr. router, switsch), koncovým zariadeniam (napr. pracovná stanica, server, tlačiareň),
- ✓ dôsledok chyby úmyselne spôsobenej neautorizovaným fyzickým prístupom, ako vandalizmus, krádež, krádež vlámaním, resp. vlastný zamestnanec, pracovník tretej strany, cudzia osoba s nepovoleným vstupom.
- ✓ presakovanie vody do zariadení a následné krátke spojenie (skrat) dôsledkom chybného utesnenia atď.

Hrozby v oblasti komunikačnej bezpečnosti

- ✓ implementácia škodlivého programového kódu do IS ako napr. vírus, trojský kôň, červ, spam, makrovírusy, spyware, adware, dialer atď.,
- ✓ blokovanie firemnej komunikácie dôsledkom zahltenia e-mailových schránok firmy veľkým množstvom nevyžiadanej pošty (SPAM),
- ✓ falošný prístupový bod, silnejším signálom môže prebrať jednotlivých klientov a sledovať tak ich činnosť a mnoho ďalších hrozieb,
- ✓ nesprávne smerovanie alebo presmerovanie dát v sieti,
- ✓ problémová alebo nedostatočná aktualizácia softvéru a oprava chýb - bezpečnostné záplaty, dôsledkom nelicencovaného softvéru,
- ✓ zlyhanie prístupu k dátam v čase ich potreby,
- ✓ phishing, pharming – podvodné emaily alebo webové stránky, snažia sa

vylákať osobné údaje z užívateľov, ako sú napr. heslá, čísla kreditných kariet, PIN čísla atď.).

Hrozby v oblasti počítačovej bezpečnosti

- ✓ chyba údržby,
- ✓ časté výpadky dodávky elektrickej energie dôsledkom je kolísanie napätia v elektrickej sieti,
- ✓ výpadok elektrickej energie a zlyhanie napájaného informačného systému a mnoho ďalších,
- ✓ technické zlyhanie záznamových médií, napr. magnetické pásky, diskety, digitálne záznamové prenosné médiá, spôsobené úmyselným alebo neúmyselným konaním, napr. fyzická strata prenosnej schránky s diskom, zničenie prenosného disku mechanickým úderom, poškodenie povrchu disku**,**
- ✓ zhoršenie kvality alebo poškodenie záznamových médií, dôsledkom zlých prevádzkových podmienok, napr. vlhkosť, teplota, prašnosť.

Hrozby v oblasti logickej bezpečnosti

- ✓ uhádnutie hesla, následný nepovolený vstup do informačného systému, dôsledkom nesprávnej dĺžky a štruktúry hesla.
- ✓ uhádnutie hesla, následný nepovolený vstup do informačného systému, dôsledkom nekonečného zadávania hesla,
- ✓ nepovolený vstup do informačného systému pripojením sa na externé komunikačné porty (napr. USB, FireWire),
- ✓ možnosť korektného čítania dát z pevného disku informačného systému v inom neautorizovanom systéme,
- ✓ nepovolený vstup do informačného systému spustením vlastného operačného systému z prenosného média, napr. USB kľúč, CD.

- ✓ úmyselné alebo neúmyselné porušovanie zásad ochrany osobných údajov,
- ✓ vydierateľnosť osôb, ktoré majú autorizovaný prístup k osobným údajom,
- ✓ rutinná práca (napr. zabudnutý dokument v skeneri alebo v tlačiarni), nedôslednosť, znížená ostražitosť,
- ✓ úmyselná pasivita oprávneného užívateľa systému, ignorovanie varovných správ, príznakov chýb alebo inej nesprávnej činnosti v systéme,
- ✓ uhádnutie hesla a následný nepovolený vstup do informačného systému, dôsledkom zapisovania hesiel na rôzne médiá (napr. post-it štítky, poznámkový blok),
- ✓ zablokovanie prístupu do IS, resp. domény, po neúspešných prihláseniach oprávnenej osoby,
- ✓ zablokovanie prístupu do IS, zabudnutie prístupového heslá, alebo v dôsledku úmyselného zmenenia prístupového hesla,
- ✓ nedovolená manipulácia s otvoreným ohňom,
- ✓ nedodržanie BOZP a bezpečnostných požiarnych predpisov,
- ✓ poruchy v činnosti informačného systému vyplývajúce z omylov či neprítomnosti kľúčovej osoby, z dôvodu ochorenia, dovolenky, služobnej cesty, prípadne rozviazania pracovného pomeru alebo náhleho úmrtia.

4.3 Návrh bezpečnostnej dokumentácie vo firme "X"

Počas životného cyklu informačného systému, ako aj toku dát, dochádza vo firme k množstvu rozhodnutí užívateľov, ktorí na ich základe konajú. Rozhodnutia produkujú iné výsledky a tieto výsledky môžu viesť k tvorbe, zmene, pohybu alebo zničeniu dát. Dáta prechádzajú v každej fáze tohto cyklu rôznym prostredím, ktoré ich vystavuje špecifickým hrozbám. Jednotlivé fázy a na ne neviazané kroky riešenia bezpečnosti je možné definovať pri výstavbe informačného systému. Kroky riešenia bezpečnosti vychádzajú z bezpečnostnej dokumentácie, ktorá vzniká počas jednotlivých fáz

životného cyklu informačného systému. Pri tvorbe bezpečnostnej dokumentácie bez ohľadu na jej obsah a cieľ, je vhodné dodržať jej určitú štruktúru a obsah.

Bezpečnostný dokument vo firme, by mal predovšetkým zdôrazňovať, čo je povolené a nie čo je zakázané. Môže podľa potreby obsahovať príklady správneho , teda povoleného a nesprávneho správania sa. Vždy platí, že akákoľvek činnosť, ktorá nie je výslovne povolená, je zakázaná. Túto filozofiu je preto potrebné v dokumente dôrazne zdôrazniť.

Bezpečnostná dokumentácia býva vypracovaná k určitému dátumu a vymedzenie rozsahu, či spôsobu implementácie ochranných opatrení býva často adresné. Pri organizačnej zmene alebo pri zmene charakteristiky informačných systémov, je potrebné bezpečnostnú dokumentáciu zosúladiť s novou aktuálnou skutočnosťou. Aktualizovať bezpečnostnú dokumentáciu sa odporúča podľa potreby, minimálne raz za rok.

Platná legislatíva, ako aj medzinárodné normy pre informačnú bezpečnosť definujú rôzne požiadavky na bezpečnostnú dokumentáciu informačných systémov.
Platný zoznam jednotlivých druhov bezpečnostnej dokumentácie IS:

- ✓Bezpečnostná politika IS,
- ✓Bezpečnostný zámer,
- ✓Bezpečnostný projekt,
- ✓Bezpečnostné smernice,
- ✓Bezpečnostný audit,
- ✓Havarijný plán informačného systému.

Bezpečnostná politika IS

Chápaná je ako základný dokument firmy, obsahujúci predstavu vrcholového manažmentu o riešení bezpečnosti, obsahujúci základné požiadavky na jednotlivé bezpečnostné oblasti všetkých informačných systémov, mala by zapadať do celkovej hierarchie bezpečnostnej politiky organizácie. Obsah bezpečnostnej politiky je daný všeobecnými právnymi predpismi, napr. vyhláška Národného bezpečnostného úradu SR o priemyselnej bezpečnosti), alebo je odporúčaný niektorým zo svetových štandardov - ISO/IEC 17799, ISO/IEC TR 13335. Manažment organizácie podľa ISO/IEC 17799 by mal stanoviť jasný smer postupu v oblasti informačnej bezpečnosti, ukázať jeho podporu vydaním politiky bezpečnosti, informácií platnej pre celú organizáciu.

Dokument bezpečnostnej politiky by mal byť schválený vedením organizácie, taktiež publikovaný a vhodne daný na vedomie všetkým dohodnutým osobám. Podľa vyhlášky Národného bezpečnostného úradu SR (NBÚ SR) by bezpečnostná politika mala bezpodmienečne obsahovať:

- predpokladané prostriedky na ochranu utajovaných skutočností a spôsob ich použitia,
- štruktúru, pracovné činnosti i právomoci bezpečnostného manažmentu podnikateľa.
- cieľe podnikateľa v oblasti ochrany utajovaných skutočností,
- očakávané utajované skutočnosti a ich špecifikácia v zhode s podnikateľskými zámermi,
- makroskopická analýza možných rizík ohrozenia utajovaných skutočností (analýza bezpečnostného prostredia a systémového okolia podnikateľa vo vzťahu k osobám, miestam a technickým prostriedkom).

Havarijný plán informačného systému

Súčasťou bezpečnostnej politiky môže byť havarijný plán alebo môže ísť o samostatný dokument. Havarijné plánovanie sa venuje tým hrozbám, ktorých výskyt je málo pravdepodobný a proti týmto hrozbám nie je možné prijať dostatočné preventívne opatrenia, pričom ich dopad by bol katastrofálny.

Úlohou havarijného plánu nie je zabrániť vzniku bezpečnostného incidentu, ale pripraviť organizáciu tak, aby následky boli čo najmiernejšie a proces obnovy systému bol čo najkratší. Stratégia havarijného plánovania by mala byť zakotvená už v celkovej bezpečnostnej politike.

Bezpečnostný projekt

Informačná bezpečnostná politika je v mnohých prípadoch všeobecná a nerieši detailne danú problematiku. V takomto prípade sa často odvoláva na jednotlivé bezpečnostné projekty, vnútropodnikové nariadenia, smernice, vyhlásenia alebo plány.

Bezpečnostný projekt na rozdiel od bezpečnostných smerníc rieši rozsiahlejší alebo ucelený parciálny bezpečnostný problém a jeho súčasťou je obvykle analýza rizík.

Cieľom bezpečnostného projektu je vymedzenie rozsahu a spôsobu implementácie

ochranných opatrení, potrebných na eliminovanie a minimalizovanie definovaných hrozieb a taktiež ich rizík pôsobiacich na informačné systémy. Od účelu závisí rozsah a forma bezpečnostného projektu, ktorý je najčastejšie definovaný v bezpečnostnom zámere. Bezpečnostné projekty:

- ✓ na ochranu osobných údajov (zákon č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov),
- ✓ na ochranu technických prostriedkov, na ktorých sú spracovávané utajované skutočnosti (zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a doplňujúca vyhláška č. 339/2004 Z.z. o bezpečnosti technických prostriedkov),
- ✓ na realizáciu systému riadenia bezpečnosti informácií (STN ISO/IEC 27001:2005 resp. BS7799-2) a iné.

Bezpečnostný projekt sa skladá z troch základných častí:

- ✓ bezpečnostný zámer,
- ✓ analýza rizík a plán implementácie nových alebo doplňujúcich ochranných opatrení,
- ✓ ustanovenia, odporúčania, závery, alebo bezpečnostné smernice.

Bezpečnostný zámer

Bezpečnostný zámer vymedzuje základné bezpečnostné ciele firmy, ktoré je potrebné vždy dosiahnuť na ochranu informačného systému pred ohrozením jeho bezpečnosti. Obsahuje najmä:

- ✓ formuláciu základných bezpečnostných cieľov a minimálne požadovaných ochranných opatrení,
- ✓ vymedzenie hraníc určujúcich množinu zvyškových rizík,
- ✓ špecifikáciu technických, personálnych a organizačných opatrení na zabezpečenie ochrany aktív v informačnom systéme a spôsob ich využitia.

Bezpečnostné smernice

Určujú pravidlá používania technických prostriedkov, prístupové a správcovské práva, organizačnú štruktúru, rozdelenie zodpovednosti a právomoci a celkový proces ochrany aktív IS. Môžu byť súčasťou každého bezpečnostného dokumentu, ale rovnako môžu byť vydané ako samostatný dokument, napr. pod názvom Pravidlá prípustného

užívania počítačového vybavenia. Ich obsah sa líši od účelu použitia, od pracovníka, ku ktorému sú určené, ale taktiež od typu príslušného bezpečnostného dokumentu.

Bezpečnostný audit

Audit informačného systému môžeme chápať ako odborné nezávislé posúdenie koncepcie, návrhu, riešenia a samotnej rutinnej prevádzky informačného systému alebo jeho časti, ako napr. audit pripojenia užívateľov na internet a jeho využitia, jeho schopnosť plniť bezpečnostné požiadavky.
Základné faktory informačného systému:

- prepojenie informačného systému s externými subjektmi, z pohľadu zabezpečenia integrity a autenticity údajov,
- koncepcia bezpečnostnej politiky,
- hardvérové a softvérové riešenie informačného systému a jeho rozvoj,
- kontrolné mechanizmy informačného systému riadiace ich bezpečnosť,
- zabezpečenie prenosov dát,
- objektová a fyzická bezpečnosť,
- pripravenosť na riešenie mimoriadnych situácií s dopadom na funkčnosť informačného systému a schopnosť organizácie plniť svoje záväzky,
- zálohovanie, archivácia a likvidácia dát,
- údržba subaktív informačného systému,
- logovanie bezpečnostných incidentov v rámci informačného systému,
- pracovné zázemie (napr. pracovné podmienky, možnosti odborného vzdelávania kľúčových zamestnancov, motivácia a lojálnosť zamestnancov).

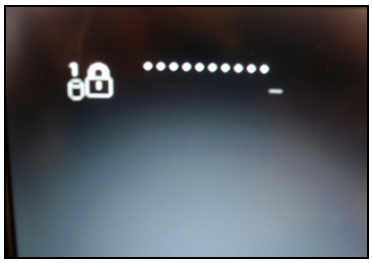
4.4 Riešenie bezpečnostnej politiky v podniku "X"

Firma "X" by sa mala nielen pred chybami chrániť, ale taktiež aj odhaľovať vzniknuté chyby a v rámci možností opravovať tieto chyby, alebo ich dôsledky. Za informačnú bezpečnosť v našej firme zodpovedá príslušné oddelenie "helpdesk", kde zamestnanci v prípade poruchy IS zavolajú a venujú sa im informační technici, ktorých úlohou je dať počítač do pôvodného stavu, tzn. odstrániť chybu, ktorá v počítači vznikla.

Každý zamestnanec našej firmy, si po príchode do práce zamyká svoj počítač (notebook) o svoj pracovný stôl pomocou bezpečnostného zámku, nazývaného "kensington", od ktorého má každý zamestnanec svoj vlastný kľúč, kľúče sú odlišné a nemôže sa stať, že sa nejaký kľúč zhoduje. V prípade straty kensingtonu musí zamestnanec zaplatiť pokutu. Zásadným programovo-technických opatrením na ochranu údajov na úrovni aplikácie je hlavne otázka **autorizácie**, oprávnenie vykonávať určité transakcie len s určitými osobami. Zabezpečuje sa prostredníctvom prístupových hesiel, ktoré odomknú príslušnú transakciu. Heslá sa musia pravidelne meniť. Autorizácia sa môže týkať, nielen oprávnenia spustiť nejakú transakciu, či získať prístup k nejakému súboru, ale aj určitých obmedzení pri zadávaní údajov a pod.

- ***Identifikácia užívateľa***

V kombinácii s ďalšími prvkami, najčastejšie s prístupovými prvkami je toto opatrenie súčasťou ochrany. Slúži na rozpoznanie, kto chce s danými prostriedkami pracovať. V našej firme skoro všetky programy fungujú prostredníctvom prístupového heslá, ktoré si vytvára každý zamestnanec a povinnosťou každého zamestnanca je, si heslá meniť po obdržaní mailu, ktorý zamestnanca informuje, že mu heslo o nejaký čas vyprší. Ak na to zabudne a heslo si nezmení, automaticky mu heslo prepadne a zamestnanec sa nedostane do programu, tzn. nemôže pracovať v programe, ktorého heslo vypršalo, musí si vyžiadať nové heslo. Niektoré programy majú a iné zase nemajú obmedzený počet zadávania hesiel, tzn. majú možnú opakovateľnosť zadávania hesiel a program sa nezablokuje, ale máme tu aj výnimky. Veľmi dôležité je vo firme heslo, ktoré zadávame po zapnutí počítača. Toto heslo si vytvára každý zamestnanec pri vstupe do zamestnania, je to jediné heslo, ktoré sa nemení a ostáva zamestnancovi v pôsobnosti vo firme rovnaké, heslo na disk. Zamestnanec musí pri zapnutí počítača zadať správne heslo, nesprávne heslo môže zadať len dvakrát, na tretí ho už nepustí a zablokuje disk, čo je pre zamestnanca veľmi vážny problém, pretože tu si už sám neporadí, musí sa obrátiť na informačných technikou, ktorí asi veľmi nadšení nebudú. Výhodu má toto vstupné heslo hlavne v prípade straty alebo krádeže počítača, je tu veľmi mala pravdepodobnosť uhádnutia hesla, teda mala možnosť dostať sa k údajom firmy.



Obr. 5

Začiatočné heslo do PC vo firme "X"

Identifikácia užívateľa je činnosť, ktorá je zdrojom záujmu ľudských infiltrácií považovaná za jednu z najčastejších. Dôvodom je vlastne to, že identifikačné heslo si užívateľ volí sám. Prieskum, ktorý bol spracovaný v USA zistil, že väčšina užívateľov si volí kratšie heslá, ktoré sú odvoditeľné z ich personálnych údajov ako napr.:

- meno a priezvisko užívateľa a jeho rodiny,
- dátum narodenia alebo svadby,
- miesto narodenia alebo bydlisko,
- obľúbený tovar alebo predmet.

Osobné údaje sú všeobecne dostupné a aj ľahko zistiteľné a skúsený „prienikár" malým počtom pokusov vie trafiť užívateľské heslo a následne využívať všetky možnosti, ktoré užívateľ má. Nevýhodou bývajú zložité heslá, ktoré sú generované počítačom alebo správcom systému. Užívatelia majú strach, že ho zabudnú a tak si ho niekde poznačia na papier, ktorý sa môže dostať do nepovolených rúk.

Dôležitým heslom vo firme "X" je heslo pre vstup do programu Windows XP, ktoré si taktiež zamestnanec musí každé tri mesiace meniť. Pri zadávaní hesla je možnosť opakovania tohto hesla niekoľkokrát, nič sa nestane, len nás systém nepustí do počítača, t. z., že zamestnanec nemôže vykonávať svoju prácu.

Obr. 6

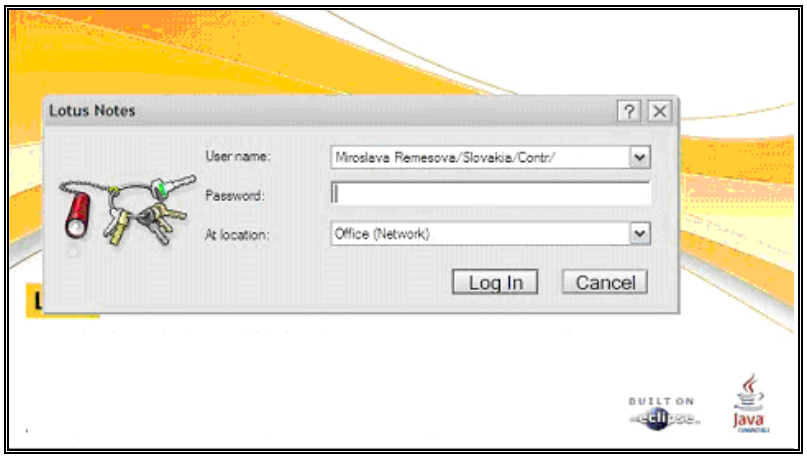
Heslo pre vstup do programu Windows XP

V súvislosti so zamknutím počítača súvisí ikona umiestnená na ploche nášho počítača. Po jej zakliknutí nám vyskočí okno na zamknutia nášho počítača (viď. obr. 7), vstúpiť do počítača môžeme prostredníctvom zadania správneho hesla, až potom je počítač opäť k dispozícii zamestnancovi.

Obr. 7

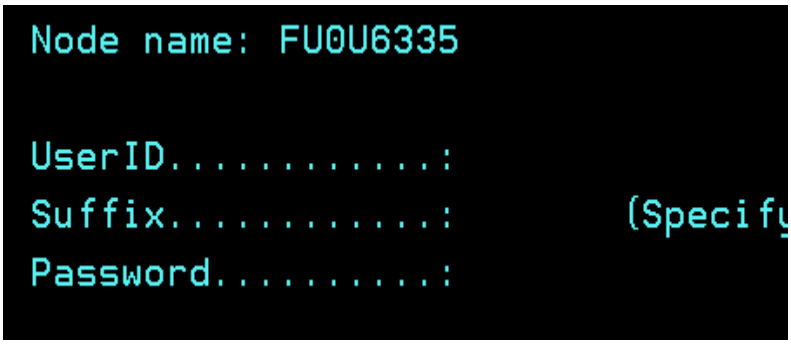
Ikona slúžiaca na zamknutie PC

Naša firma má množstvo programov, s ktorými pracujeme a každý si vyžaduje vstup prostredníctvom hesla. Každý zamestnanec má prístup do programov vo svojom vlastnom počítači, môže ich samozrejme použiť aj u kolegu, ak sa uňho naloguje pod svojimi prístupovými heslom.



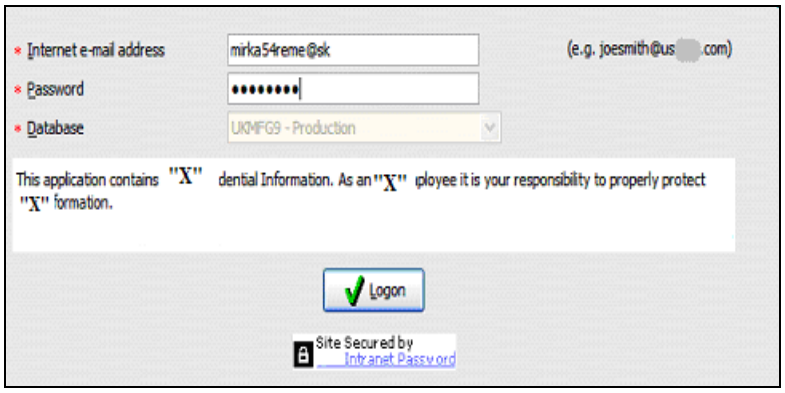
Obr. 8

Heslo pre vstup do programu Lotus Notes vo firme "X"



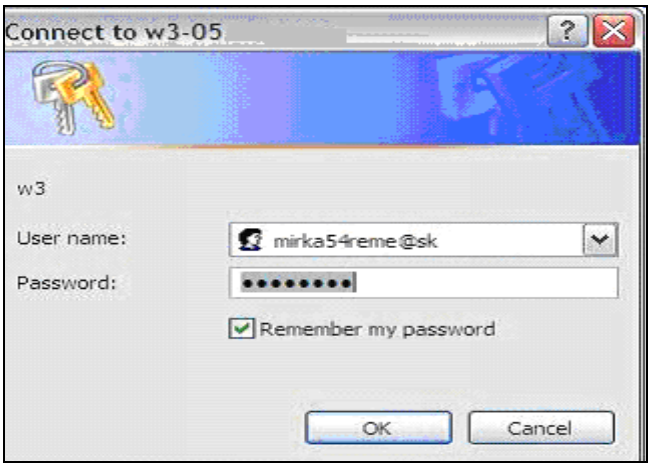
Obr. 9

Heslo pre vstup do programu bridge vo firme "X"



Obr. 10

Heslo pre vstup do programu na zakladanie zmlúv vo firme "X"



Obr. 11

Heslo pre vstup do internetovej stránky firmy "X"

- ***Audit***

Cieľom auditu je sledovať činností, ktoré sú robené užívateľom a ukladať informácie o týchto činnostiach. Dobrý audit je taký, o ktorom auditovaná osoba nevie alebo ho nevie odstaviť či modifikovať. Pomocou auditu na PC sa obyčajne sleduje, kto s akými súbormi pracuje. Z tohto možno potom, napr. zrekonštruovať, kto a kedy zaniesol vírus do počítača, alebo kto si kopíroval dôležitú databázu, sťahoval si súkromné veci, v našej firme si nemôžu zamestnanci dovoliť počúvať, napr. rádio cez internet, alebo počúvať pesničky cez youtube. Nerieši ochranu údajov priamo, ale jeho možnosť spätného zistenia, čo sa dialo, môže odradiť potenciálneho narušiteľa nášho IS.

- ***Prístupové práva***

Cieľom tohto opatrenia je vlastne umožniť prístup každému užívateľovi len k prostriedkom, ktoré potrebuje pre svoju prácu. V prostredí sieti je bežnou vecou. Medzi tieto práva patrí napr. možnosť vstúpiť do adresára, pozerať si súbory, kopírovať a spúšťať súbory, mazať súbory a adresáre. Osobitným dá sa povedať, že superprávom je možnosť definovať a meniť práva iným užívateľom. Pri používaní samostatného počítača by sa malo ujasniť, kto je hlavný užívateľ, ktorý definuje možnosti práce s daným počítačom ostatným užívateľom.

- ***Kryptovanie***

Cieľom kryptovania je utajiť obsah údajových súborov pred nepovolenými osobami. Pri kryptovaní je dôležité vedieť, aký kryptovací algoritmus, daný program používa a nakoľko je algoritmus bezpečný. Štandardom sú algoritmy DES a RSA, napr. pri DES je dôležité, koľko bitov má kódovací kľúč. Kódovací alebo dekódovací kľúč môže byť zadaný užívateľom alebo generovaný špeciálnou čipovou kartou. Spojenie oboch možností je najbezpečnejšie:

- užívateľ musí niečo poznať napr. heslo, kľúč,
- užívateľ musí niečo vlastniť - čipovú kartu.

Toto riešenie je pomerne finančne náročné. Ak používa program vlastný algoritmus mimo štandardu, je veľmi ťažké odhadnúť kvalitu algoritmu. Pomôckou bežného užívateľa je vyžiadať si zoznam referencií, prípadne informáciu o počte inštalácií.

Kryptovanie na samostatnom PC je jedným z najúčinnejších nástrojov ochrany údajov. Ani odcudzením počítača nemá narušiteľ šancu dostať sa k našim údajom.

- ***Antivírusový program Control – Symantec Client Firewall***

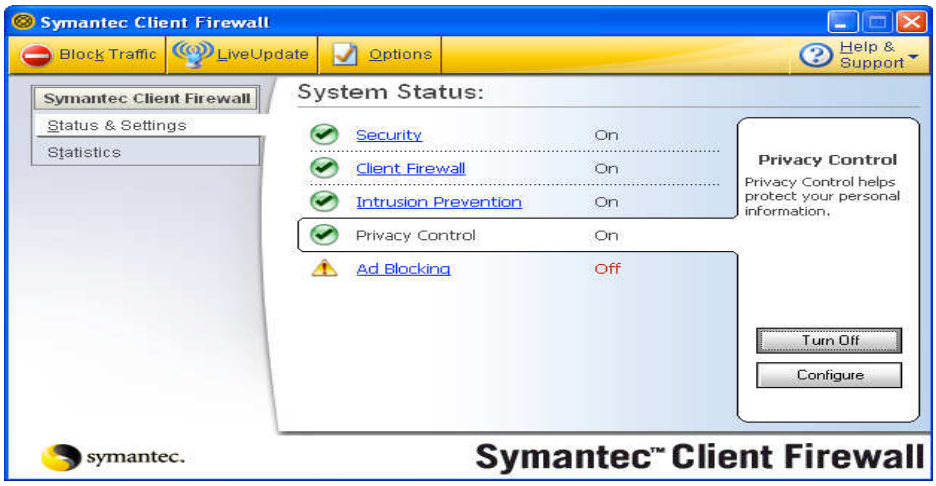
Na ochranu osobných údajov počítača v našej firme sa používa antivírusový program "Symantec Client Firewall", ktorý ma chrániť počítač pred jeho poškodením.

Obr. 12
Program Control – Symantec Client Firewall

Ikona programu Symantec Client Firewall sa nachádza na hlavnom panely a je označená takto:

Obr. 13
Ikona programu Symantec Client Firewall

Dôležité pre tento program je správnosť jeho fungovania a nastavenia a preto, by mal si mal každý zamestnanec preventívne kontrolovať, či je tento program správne nastavený. Správnosť jeho nastavenia by mala vyzerať takto:



Obr. 14

Nastavenia v programe Symantec Client Firewall

- ***Zálohovanie a archivácia dát***

Zálohovanie je mechanizmus, prostredníctvom ktorého sú vybrané dáta ukladané na iné zálohovacie záznamové médium. V prípade zničenia pôvodného záznamového média sú dáta obnovené zo zálohy. Pri obnove môže dôjsť k tomu, že sa časť dát stratí.

Snahou by malo byť zálohovať pravidelne a čo najčastejšie a záložná kópia musí byť uložená oddelene od miesta zaznamenávania dát. Ideálne je umiestnenie pokiaľ je možné v inej budove a vo vodovzdornom a ohňovzdornom trezore. Pri zálohovaní je potrebné prijať ďalšie opatrenia:

- ✓ pri informáciách, ktoré sú citlivé, by sa mali uchovávať najmenej tri generácie záložných kópií dát,
- ✓ zálohovaným záznamovým médiám by mala byť poskytnutá primeraná úroveň fyzickej ochrany a ochrany prostredia,
- ✓ záznamové médiá so zálohami dát, by mali byť pravidelne testované, aby sa zaistilo, že sa na ne dá v prípade potreby spoľahnúť, minimálne jedenkrát za rok,
- ✓ je potrebné určiť obdobie a čas zálohovania informácií a taktiež všetky požiadavky na archívne kópie, ktoré majú trvalo uchované.

Dôležité je rozlišovanie medzi zálohovaním a archiváciou. Pod zálohovaním sa rozumie uchovávanie dát so zámerom, čo najpresnejšie obnoviť systém, do stavu tesne pred bezpečnostným incidentom. Archivácia slúži na uchovávanie časovo definovaného

prierezu dát, nie na účely obnovenia systému (napr. súbor výročných správ organizácie za obdobie 2009-2010). Potrebné je archivovať všetky dôležité dáta v organizácii a to po dobu 3 až 5 rokov. Medzi základné spôsoby zálohovania patrí:

- úplné zálohovanie – ide o zálohovanie všetkých dát na pevnom disku bez rozdielu,
- diferenciálne zálohovanie – zálohovanie sa dotýka len tých dát, ktoré sa zmenili alebo pribudli od doby posledného úplného zálohovania,
- prírastkové zálohovanie – zálohovanie sa dotýka len tých dát, ktoré sa zmenili alebo pribudli do doby posledného zálohovania (napr. po ukončení celodennej práce),
- centralizované alebo decentralizované zálohovanie.

- ***Ochrana dát pred výpadkami zdroja***

V dôsledku krátkodobého alebo dlhodobého výpadku zdroja elektrického napájanie môže dôjsť k narušeniu integrity alebo dostupnosti dát. Preto fyzické subaktíva, ktoré sú napájané zo zdroja elektrickej energie, by mali byť chránené pred výpadkami elektrickej energie a inými elektrickými anomáliami. Mala by sa zabezpečiť vyhovujúca dodávka elektrickej energie, ktorá je v zhode so špecifikáciami výrobcu zariadení. Možnosti pre dosiahnutie kontinuity dodávky elektrickej energie zahŕňajú:

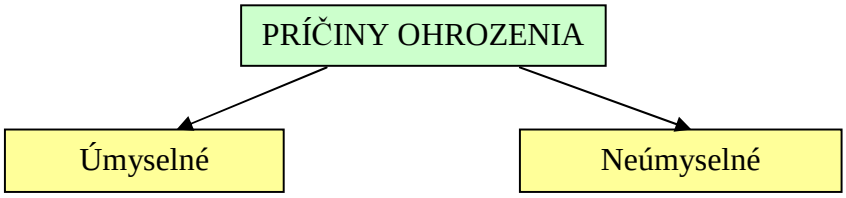
- ochranné filtre proti bleskom,
- viacnásobné napájanie s cieľom predísť jedinému bodu výpadku dodávky prúdu,
- neporušiteľný zdroj prúdu (UPS),
- záložný generátor.

4.5 Bežný užívateľ PC – domácnosť

Poruchy IS v domácnostiach súvisia hlavne s používaním internetu. V súčasnosti je Internet veľmi nebezpečným miestom, ktorý môže nainfikovať počítač nebezpečným vírusom.

Užívateľ využíva počítač na svoje bežné účely, má možnosť prijímať a odosielať maily, pomocou pošty môže takto ohroziť a nainfikovať aj ďalších účastníkov.

Klasifikácia a identifikácia možných príčin ohrozenie IS je nevyhnutná k tomu, aby sa dokázali správne určiť potrebné ochranné opatrenia.



Obr. 15

Príčiny ohrozenia IS

Zdroj: vlastné spracovanie.

- ***Príčiny ohrozujúce užívateľa PC***

K **úmyselným príčinám** zaraďujeme počítačové pirátstvo, ktorého cieľom je preniknúť do IS alebo neoprávnene získať dáta, ktoré sú predmetom utajenia alebo ich neoprávnene meniť. Niekedy môže byť cieľom aj úmyselné zničenie IS. Treba rozlišovať, či ide o poškodenie príležitostné (náhodné) alebo o systematickú cieľavedomú činnosť. Medzi úmyselné príčiny možno tiež zaradiť ohrozenie IS prostredníctvom počítačových vírusov, aj keď toto ohrozenie väčšinou nie je motivované poškodením určitého konkrétneho IS.

Neúmyselné príčiny môžu byť spôsobené:

- ✓ **ľudským faktorom, resp. chybou obsluhy** – predovšetkým chybami operátorov, chybami vstupných dát, neautorizovaným prístupom a pod., je častým zdrojom problémov, ide najmä o nechcené vymazanie dôležitých súborov, ďalším problémom v dôsledku nepresnej evidencie je premazanie novšej verzie pracovného súboru staršou,
- ✓ **programovým vybavením** – chybami v systémových alebo aplikačných programoch,
- ✓ **technickým vybavením** – zlyhaním niektorej časti počítača alebo komunikačného vybavenia,
- ✓ **prostredím** – napr. klimatizáciou, výpadkom napájania, prírodnou katastrofou a pod.

- ✓ **infiltrácia IS** – najčastejším problémom sú dnes počítačové vírusy,
- ✓ **nesprávny beh softvéru** – súvisí hlavne s prostredím OS Windows, kde môže mať program niekoľko chýb.

Chyby pochádzajú z rôznych úrovni softvéru:

- systémový softvér
- bežný aplikačný softvér

Tieto chyby sa prejavujú napr. tým, že sa údajový súbor nedá uložiť na disk a tiež zamrznutím aplikácie alebo aj celkovým spadnutím Windows.

- ✓ **chyba poškodenia alebo strata hardvéru** – môže isť o mechanické poškodenie počítača, prerušenie prepojovacieho kábla, posunutú hlavičku disketovej jednotky, chybu radiča pevného disku, zanesenie hlavy tlačiarne, odcudzený hardvér (najčastejšie notebook) atď.

Ochrana užívateľov, pretože zámery útočníka môžu byť rôzne:

- ✓ hlavne pred zneužitím identity – tzn. mali by používať dobré heslá,
- ✓ emailovými správami, ktoré môžu obsahovať vírusy alebo spam,
- ✓ podvodníckymi stránkami – hrozí samoinštalácia škodlivého softvéru, phishing (bankové podvody),
- ✓ škodlivé programy, ktoré sa tvária, že sú na niečo užitočné,
- ✓ sociálne inžinierstvo,
- ✓ neotvárať podozrivé správy (neznámy odosielateľ, predmet správy)
- ✓ v žiadnom prípade na tieto správy neodpovedať.
- ✓ môžu získať privátne údaje (e-mailové adresy, čísla kreditných kariet, priemyselná špionáž, prístupové heslá..)
- ✓ možnosť využitia výpočtového výkonu,
- ✓ taktiež je tu možnosť využitia internetového pripojenia pri útoku na ďalšie počítače alebo maskovaní sa.

- ***Bezpečné heslá užívateľa PC***

Dôležitým prístupovým heslom pre domáceho užívateľa je heslo do Windows XP. Systém Windows XP prichádza s niekoľkými novými prvkami, ktoré sa týkajú podpory viac užívateľov a lepšie využitie počítača v domácom prostredí.

Obr. 16

Účet jedného užívateľa PC

Ak počítač v domácnosti využíva viacero užívateľov, tak výhodou tohto systému, je vytvorenie prístupového účtu pre každého užívateľa. Užívateľský účet si vytvára administrátor počítača. Každý tento účet je identifikovaný podľa užívateľského mena s možnosťou použitia hesla. Užívateľ po spustení počítača zadáva alebo si vyberie meno, doplní heslo a získa tak prístup k nastaveniam.

Obr. 17

Účet viacerých užívateľov PC

Zmeny sa uložia a prirazia do tzv. užívateľského profilu a budú platné aj pre ďalšie prihlásenie. Po zapnutí počítača sa nám zobrazí úvodná obrazovka, kde stačí kliknúť na ikonu alebo meno používateľa, zadať heslo a spusti sa prihlásenie do počítača.

Užívateľ účtu svoje prihlasovacie údaje (či už ide o meno alebo heslo) má držať v tajnosti. Heslá, ktoré si vytvára majú byť ľahko zapamätateľné a po určitom čase ich treba meniť.

- ***Počítačové vírusy a antivírusové programy***

V oblasti osobných počítačov predstavujú najčastejší a najznámejší spôsob narušenie IS. Ochrana pred nimi predstavuje nutnú vec pre každý informačný systém používajúci PC. Medzi rizikovú skupinu zaraďujeme užívateľov, ktorí prenášajú prácu medzi domácim a firemným počítačom. Ich deti si na domáci počítač prinášajú hry, niekedy aj s počítačovým vírusom a ten sa prenáša do práce.

Veľkým problémom sú vírusy, ktoré sú neznáme antivírusovým scanerom, so schopnosťou zneviditeľnenia. Najproblémovejšími sú pomalé vírusy, ktoré sa množia len pri kopírovaní a vytváraní nového programu, sú nedetekovateľné bežnými programami pre kontrolné súčty. Počítačové vírusy sú hľadané scannermi. Kvalita scanneru závisí od počtu vírusov, ktoré sú už známe a od presnosti rozpoznania polymorfných vírusov. Neznáme vírusy sú vyhľadávané heuristickými scanermi a programami pre zaisťovanie integrity kritických oblastí disku.

Škody v informačnom systéme spôsobené vírusmi

Sú veľmi nepríjemné, pretože okrem množenia spôsobujú škody. Medzi škody, ktoré sa vyskytujú patria:

- ✓ formátovanie pevného disku,
- ✓ kódovanie časti pevného disku,
- ✓ poškodenie obsahu náhodne vybraných sektorov na disku,
- ✓ konflikty s inými rezidentnými programami,
- ✓ poškodenie programov, nie sú viac schopné práce,
- ✓ zmenšenie voľnej pamäte RAM, čo môže spôsobiť znemožnenie práce niektorých programov,
- ✓ vystrašenie užívateľa varovným hlásením,
- ✓ spomalenie chodu programov.

Počítačový vírus

Program, ktorý sa nakopíruje a začne prenikať do počítača vo vhodnom operačnom prostredí. Sám, bez vedomia používateľa počítača vytvára kópie, rozmnoží sa a začína vykonávať škodlivú činnosť, ktorá môže byť rôzna. Menej škodlivé vírusy vypisujú len oznamy, spomaľujú beh programov, odosielajú dáta z počítača a agresívne verzie môžu vymazať programy alebo poškodiť vybavenie počítača.

Vírusy môžeme na počítač preniesť z rôznych, vopred nekontrolovaných zdrojov antivírovým programom, ako USB flash disk alebo USB kľúča po domácky, zapísané CD, DVD s programami, atď. Najčastejšie vírus preniká počas pripojenia počítača na internet. Najväčším zdrojom sú rôzne hry a súbory z neznámych zdrojov pôvodu, lákavé ponuky z neoverených stránok www.

Vírusy sú v podstate veľkosťou malé a jednoduché programy, ktoré sú schopné rozmnožovať sa a vykonať činnosť, pre ktorú boli naprogramované.

Vírusy sa skladajú z dvoch častí:

– jedna časť vírusov slúži na rozmnožovanie,

– druhá časť vírusov obsahuje kód pre vonkajší efekt.

Z hľadiska nebezpečnosti delíme víry takto:

- **Vírusy napádajúce programy** - do tejto skupiny patria vírusy, ktoré sú v podstate neškodné, jediná vec ktorú dokážu, je prepísanie používaných programov. Takto postihnutý súbor už väčšinou nespustíme, ale väčšinou stačí

postihnutý program vymazať a nainštalovať znovu.

- **Vírusy ničiace údaje -** sú dosť nebezpečné vírusy. Môžeme ich rozdeliť na:

✓ vírusy napádajúce a modifikujúce FAT tabuľku,

✓ vírusy meniace tabuľku partícií,

✓ vírusy formátujúce disk alebo zablokujú prístup k nemu,

✓ vírusy, ktoré prekódujú obsah disku a po ich odstránení nemožno údaje prečítať.

Ak sa liečenie antivírusovým programom nepodarí prichádzame o dáta uložené na disku. Takejto katastrofe sa dá predísť, ak máme aspoň nejaké zálohy.

- **Vírusy modifikujúce údaje - t**ento typ vírusov čaká len v počítači a sem tam zmení nejaký údaj. Niektoré víry pracujú podľa určitého algoritmu, tam je ešte šanca vrátiť údaje do pôvodného stavu, neexistujú aj také, kde nie je možné zistiť, ktoré súbory boli napadnuté. Je nepríjemné, že si ani nemôžeme byť istý tým, že sú zálohy správne.
- **Vírusy ničiace hardware -** do tejto kategórie patria vírusy, ktoré vznikli vďaka starostlivosti o užívateľa. Niekedy bolo pri skladaní počítača nutné nastavovať všetko ručne. Dnes sa skoro všetko nastavuje automaticky a zapíšu sa do pamäte príslušného zariadenia. Takže vírusy môžu nastavenia hardware zmeniť alebo zmazať.

Medzi známe vírusy patria:

- **Trójske kone** – necielená-cielená infiltrácia so schopnosťou šíriť sa prostredníctvom autorizácie užívateľom, ktorý si nie je vedomý škodlivej časti. Trójsky kôň sa nemnoží, len poškodzuje. Po preniknutí do cudzieho systému len ticho pozorujú systém a čakajú na svoju chvíľu. Trójske kone dokážu zistiť heslo, vymazať konkrétny program, nakradnúť údaje. Tieto vírusy sú skôr doménou počítačových sieti ako samostatných počítačov. Častokrát trójske kone slúžia na vypustenie nového vírusu.
- **Makrovírusy –** ide o programy naprogramované v jazyku na tvorbu makier v textovom procesore, alebo tabuľkovom kalkulátore a vložené do takého dokumentu. Väčšinou ide o programy Microsoft Word, ktoré systém vykonáva pri každom otvorení dokumentu (tzv. auto makrá), AutoExec, AutoOpen, FileSaveAs, FilePrint, FileExit. Infikovaná je najčastejšie šablóna NORMAL.DOT.
- **Súborové** - najrozšírenejšia skupina vírov. Infikujú EXE, COM, OVL, BIN, STS, OBJ, DLLsúbory a niekedy aj keď sú uložené v komprimovaných

archívoch.

- **Nerezidentné -** vírus sa po spustení infikovaného programu replikuje, najčastejšie do súborov v danom adresári, a predajú riadenie infikovanému programu.
- **Rezidentné -** tieto vírusy ostávajú v operačnej pamäti počítača aj po ukončení vykonávania infikovaného programu použitím mechanizmu TSR.
- **Softvérové bomby a míny** – zvyčajne sa nešíri. Jej nebezpečnosť spočíva v tom, že je vytvorená človekom so znalosťami IS, proti ktorému je infiltrácia zameraná. Proti SW bombám sa dá chrániť oddelením tvorby softvéru a generovania výsledného kódu, oddelením funkcie technického a bezpečnostného správcu systému. Vyskytujú väčšinou v prostredí stredných systémov a mainframov.
- **Zadné vrátka** – v programe je programátorom ponechaná možnosť, aby po zadaní tajného kódu získal plný prístup k možnostiam programu a údajom, s ktorými program pracuje. Infiltrácia je cielená.
- **Prienikár** – cieľom prienikára je dostať sa do zabezpečeného IS a nechať tam značku svojej návštevy. Občas prienikár poškodzuje aj údaje v IS, sú vo veľkou hrozbou v sieťach WAN (napr. Internet), kde je možnosť vzdialeného prístupu do IS.
- **Zlodej HW** – cieľom je získať hardvér IS. Dochádza aj k strate údajov, ktoré sú na ukradnutom hardvéri. Osobitný problém vzniká, ak sú ukradnuté aj všetky média, kde sú záložné kópie údajov.
- **Deštruktor** – cieľom je úmyselne poškodiť IS z motívov osobných, politických či nekalej konkurencie, najnebezpečnejšie je malé, ťažko detekované a zmysluplné poškodenie údajov. Veľkým problémom z hľadiska ochrany je, ak je deštruktor z vnútra organizácie.
- **Akvizítor** – jeho cieľom je získať kópie dôležitých údajov. Zvyčajne nie je odcudzenie pozorovateľné, pri snahe zakryť stopy stimuluje poškodenie IS požiarom, vytopením, elektrickým skratom, často to býva interný pracovník organizácie.
- **Modifikátor** – modifikuje údaje v IS vo svoj prospech alebo cudzí neprospech, modifikácie sú zvyčajne zistené až po dlhom čase. Cieľom modifikátorov sú najmä bankomaty a systémy pre home-banking.

Ako zabrániť nákaze vírusov?

Hovorí sa, že dôležitejšie ako samotné liečenie je **prevencia.**

Zabrániť nákaze môžeme takto:

- neotvárať neznámu poštu s prílohami,
- pravidelne zálohovať údaje,
- nenechávať pri štarte počítača napr. USB kľúč alebo CD,
- snažiť sa používať originálny software
- čo najčastejšie aktualizovať svoj antivírus a Windows.

Každý antivírus by mal dokázať toto:

- ✓ nájsť vírus ukrytý v pamäti, na disku alebo diskete (CD-čku),
- ✓ dokázať ho odstrániť, vyliečiť,
- ✓ odstrániť napáchané škody,
- ✓ mal by byť rýchly, aby príliš nespomaľoval počítač.

Mal by mať schopnosť zapnúť ochranu počítača počas činnosti a byť neustále v pamäti "strážiť" počítač pred rizikovými operáciami. Väčšina antivírusov dokáže aj zálohovať citlivé časti disku. Každý vír po zapísaní zmení kód programu. Metóda kontrolných súčtov je založená na sčítaní číselnej hodnoty znakov tvoriacich súbor. Zmena CRC súčtu nemusí vždy znamenať vírus, niektoré programy si ho menia samy.

Pri bežnom hľadaní, resp. scanovaní sa prezerajú súbory a porovnáva sa kód s kódom evidovaných vírusov. Nevýhodou scanovania je, že dokáže nájsť iba evidované vírusy. Existujú aj vírusy, ktoré počas svojej existencie menia svoj kód .V snahe o vyriešenie tohto problému tvorcovia antivírusov do svojich systémov vkladajú heurestickú analýzu, ktorá dokáže odhaliť aj neznáme vírusy, ktoré sa prejavujú typickými inštrukciami. Prepracovanejšia heurestická analýza, dokáže krok za krokom simulovať činnosť programu. Okrem polymorfných vírusov existujú aj stealth vírusy, ktoré zmanipulujú operačný systém tak, že dokáže skryť svoju existenciu pred antivírusom.

Existuje veľa výrobcov, ktorý vyvíjajú a dodávajú antivírové programy, u nás sa presadilo len niekoľko z nich, napr. Kaspersky, Symatex (Norton antivírus), ale hlavne NOD od Slovenskej firmy ESET, ktorá sa výborne etablovala aj vo svete. NOD sa používa v školstve, štátnej správe v rôznych verziách už pomerne dávno. Program pozostáva z dvoch hlavných častí. Prvú časť tvorí programová časť, ktorá je spustená používateľom, v danom čase a podľa potreby. Druhá časť (tzv. rezidentná) je spustená

pri štarte operačného systému automaticky a beží v pozadí neustále a nesmieme ju zastaviť, lebo náš počítač bude bezbranný voči vírom

4.6 Prieskum stavu informačnej bezpečnosti v SR

Tento prieskum prebiehal v SR v roku 2008 a bol zameraný na vybranú reprezentatívnu vzorku stredných a veľkých spoločností v SR. V prieskume, ktorý bol anonymný odpovedali organizácie na 59 podrobných otázok z oblasti informačnej bezpečnosti. Z 826 oslovených spoločností sa vrátilo 205 vyplnených dotazníkov.

Výsledky tohto prieskumu ukázali, že spoločnosti si u svojich bezpečnostných pracovníkov najviac cenia vecné znalosti problematiky, IT technológií a flexibilitu a najviac im chýbala znalosť finančného riadenia a taktiež schopnosť efektívnej komunikácie s vedením.

Medzi najzávažnejšie hrozby s najviac identifikovanými vplyvmi patrí výpadok elektrickej energie, SPAM a poruchy hardwaru. Najviac zarážajúce však je, že aj napriek existujúcim hrozbám až 55% spoločnosti nemá vypracované plány obnovy funkčnosti a až dve tretiny spoločností nevypracovali za posledné dva roky žiadnu analýzu rizík informačného systému, čo predstavuje vlastne klesajúci negatívny trend. Z toho jedna tretina spoločností nemá vypracovaný systém monitorovania bezpečnostných incidentov a viac ako štvrtina nemá stanovené žiadne formálne postupy.

Výsledky prieskumu ukázali, že väčšina spoločností zastavuje investície do nových IT riešení a funguje v udržiavacom režime. Prioritou, ktorá je považovaná za hlavnú v oblasti informačnej bezpečnosti sa stáva riešenie už identifikovaných známych problémov. Medzi najväčšie bezpečnostné výzvy v minulom období patrili prechod na euro a implementácie nových operačných systémov.

5. ZÁVER

Bezpečnosť informačného systému je v súčasnosti veľmi dôležitá a preto by jej mala byť venovaná dostatočná pozornosť. Užívatelia počítačov, či už domácnosti alebo firmy, by mali investovať dostatok finančných prostriedkov do IS, tz. musia informačné systémy zabezpečovať rovnako, ako ktorékoľvek svoje investície.

V práci porovnávam bežného užívateľa PC a firmu "X" a vyvodzujem, že ani užívateľ a ani firma by nemali brať bezpečnosť informačných systémov na ľahkú váhu, pretože v oboch prípadoch môže dôjsť k poškodeniu IS, ktoré môže mať nepriaznivé následky.

Obrovskú hrozbu pre oboch predstavujú vírusy, ktoré sa šíria najmä prostredníctvom internetu. Väčšina škodlivého kódu má však ekonomické pozadie a predstavuje nástroj na kriminálnu činnosť, ktorá môže mať veľa podôb, všetky majú niečo spoločné – sú výnosné. Zabezpečenie na úrovni informačných technológií by preto malo byť rovnako samozrejmé, ako je samozrejmé chrániť si osobné údaje, ako napr. platobnú kartu, či občiansky preukaz.

Ako každá firma, tak aj naša potrebuje formálne definovanie realizovaných procesov, ktoré by sa malo premietnuť do bezpečnostnej politiky, jej nedôsledné dodržiavanie vedie k úspešným útokom proti IS. Zostavenie takejto politiky nie je jednoduché, preto je vhodné jej tvorbu konzultovať so špecialistami, ktorí majú v tejto oblasti bohaté skúsenosti, poznajú medzinárodné štandardy a normy.

Pre zabezpečenie bezpečnej siete v našej firme navrhujem:

- ✓ pravidelné aktualizovanie antivírusového systému,
- ✓ aktívny firewall,
- ✓ pravidelné a bezodkladné aplikovanie opráv operačného systému a nainštalovanie programového vybavenia,
- ✓ získavanie kvalifikovaných odborníkov v oblasti IT,
- ✓ zaplatenie si odborníkov na informačnú bezpečnosť,
- ✓ pokrytie zvyšujúcich sa nákladov na rozvoj, prevádzku a riadenie funkcie IS,
- ✓ udržanie kroku s rýchlo sa vyvíjajúcimi informačnými technológiami,
- ✓ prístup k technológiám a službám IT na svetovej úrovni,
- ✓ školenie zamestnancov firmy v tejto oblasti.

Firma má mať strategický cieľ v oblasti bezpečnosti, cieľom ktorého je zabezpečiť

ochranu a dôveryhodnosť digitálneho prostredia a týmto môže smerovať k zabezpečeniu bezproblémového chodu využívania IS.

Na dosiahnutie tohto cieľa je potrebné:

- vytvoriť (legislatívne, personálne, organizačné a finančné) podmienky pre účinnú prevenciu a rýchlu a efektívnu reakciu na bezpečnostné incidenty,
- zvýšiť bezpečnostné povedomie používateľom IKT a verejnosti,
- zabezpečiť priebežný monitoring a efektívne využívanie predvstupovej a štrukturálnej pomoci EÚ v tejto oblasti,
- zabezpečiť podmienky na zapojenie sa do relevantných programov v tejto oblasti.
- vytvorenie podmienok pre ďalší rozvoj informačnej bezpečnosti, snaha dosiahnuť úroveň porovnateľnú s krajinami EÚ.

6. POUŽITÁ LITERATÚRA

BERKA a kolektív autorov. 2006. *Bezpečná počítačová síť*. Praha: Dashofer Holding, Ltd. & Verlag Dashofer nakladateľstvo 2001-2006. s. 16. ISBN 80-86229-79-3.

ENDORF, C., SCHULTZ, E., MELLANDER, J. 2005. *Hacking - Detekce a prevence počítačového útoku.* s. 355. Vydala Grada Publishing, a.s., Praha 2005. ISBN 80-247-1035-8.

HENNYEYOVÁ, K. – POPELKA, V. 2009. *Bezpečnosť IKT a IS v podnikoch*. In: Zborník príspevkov z medzinárodnej vedeckej konferencie Rozvoj vidieka a Spoločná poľnohospodárska politika (CD ROM). Račková dolina, 2009, s. 116-119. ISBN 978-80-552-0200-6.

HENNYEYOVÁ, K. 2008. *Proces informatizácie a informačná bezpečnosť v podnikoch na Slovensku.* In: Zborník z medzinárodného vedeckého seminára Aktuálne problémy riešené v agrokomplexe (CD ROM). Nitra, 2008, s. 419-422, ISBN 978-80-552-0151-1.

HENNYEYOVÁ.K. 2008. *Aspekty informačnej bezpečnosti v podnikoch na Slovensku*. In: Zborník príspevkov z medzinárodnej vedeckej konferencie Vybrané otázky agrárneho práva EÚ (CD ROM). Nitra, 2008. s. 47-50. ISBN 978-80-552-0014-9.

HOFREITER, L. 2008. *Systémy prenosu informácii v bezpečnostných aplikáciách*. Vydala Žilinská univerzita v Žiline, 2008. s. 95. ISBN 978-80-8070-823-8.

HOFREITER, L. – KRIŽOVSKÝ, S. 2007. *Manažérstvo bezpečnostných systémov*. Vysoká škola bezpečného manažérstva v Košiciach 2007. s. 68. ISBN 978-80-89282-16-6.

HOWARD, M. 2008. *Bezpečný kód*. Vydavateľ Computer Press, Brno, 2008. s. 895. ISBN 978-80-251-2050-7.

HRUBEC J., VIRČIKOVÁ E. a kolektív 2009. *Integrovaný manažérsky systém*. Slovenská poľnohospodárska univerzita v Nitre 2009. s. 543. ISBN 978-80-552-0231-0.

IVANIČKA, K. 2000. *Manažérske informačné systémy*. STU, Bratislava 2000, 153 s. ISBN 80-227-1369-4.

JIROVSKÝ, V. 2007. *Kybernetická kriminalita*. Vydavateľ: Grada Praha, 2007. s 284, ISBN 978-80-247-1561-2.

KOPÁČIK, I. 2007. *Riadenie a audit v informačnej bezpečnosti*. Vydaveteľ: TATE International Slovakia, 2007. s.322. ISBN 978-80-969747-0-2.

KOKLES, M. a kol. 1999. *Informatika*. Bratislava 1999. 380 strán. ISBN 80-225-1179-X.

KOKLES, M. a ROMANOVÁ, A. 2007. *Informačný systém podniku*. Vydavateľstvo

Ekonóm 2007. 183 strán. ISBN 978-80-225-2286-1.

KUČERA, M a LÁTEČKOVÁ, A. 2004. *Podnikové informačné systémy*. Vydala Slovenská poľnohospodárska univerzita v Nitre 22.11.2004. s. 135 – 136. ISBN 80-8069-452-4.

LEVICKÝ, D. 2010. *Kryptografia v informačnej a sieťovej bezpečnosti*. Vydavateľ: Elfa, 2010, s. 277, ISBN 978-80-8086-163-6.

LOVEČEK, T. 2007. *Bezpečnostné systémy. Bezpečnosť informačných systémov*. Vydala Žilinská univerzita v Žiline 2007. s.15-30. ISBN 978-80-8070-767-5.

MESÁROŠ, M. (2009). *Riadenie bezpečnostných systémov*. Vydala Vysoká škola bezpečnostného manažérstva v Košiciach 2009. s. 61-66. ISBN 978-80-89282-37-1.

MIKOLAJ, J. – HOFREITER, L. – MACH, V. – MIHÓK, J. – SELINGER, P. 2004. *Terminológia bezpečnostného manažmentu*. Výkladový slovník. Košice: Multiprint s.r.o.2004, ISBN 80-969148-1-2.

SAMER KHOURI – DENISA AL-ZABIDI 2010. *Informačné systémy podniku***.** Košice: Dekanát – Edičné pracovisko Fakulty BERG, Košice 2010, 127 strán, ISBN 978-80-553-0373-4.

STRNÁD, O. 2009. *Bezpečnosť a manažment informačných systémov*. Bratislava: Nakladateľstvo Slovenskej technickej univerzity 2009, 344 strán, ISBN 978-80-227-3040-2.

STRNÁD, O. 2002. *Manažment bezpečnosti IT*. Vydala Slovenská technická univerzita v Bratislave vo Vydavateľstve STU, Bratislava 2002, 208 strán, ISBN 80-227-1696-0.

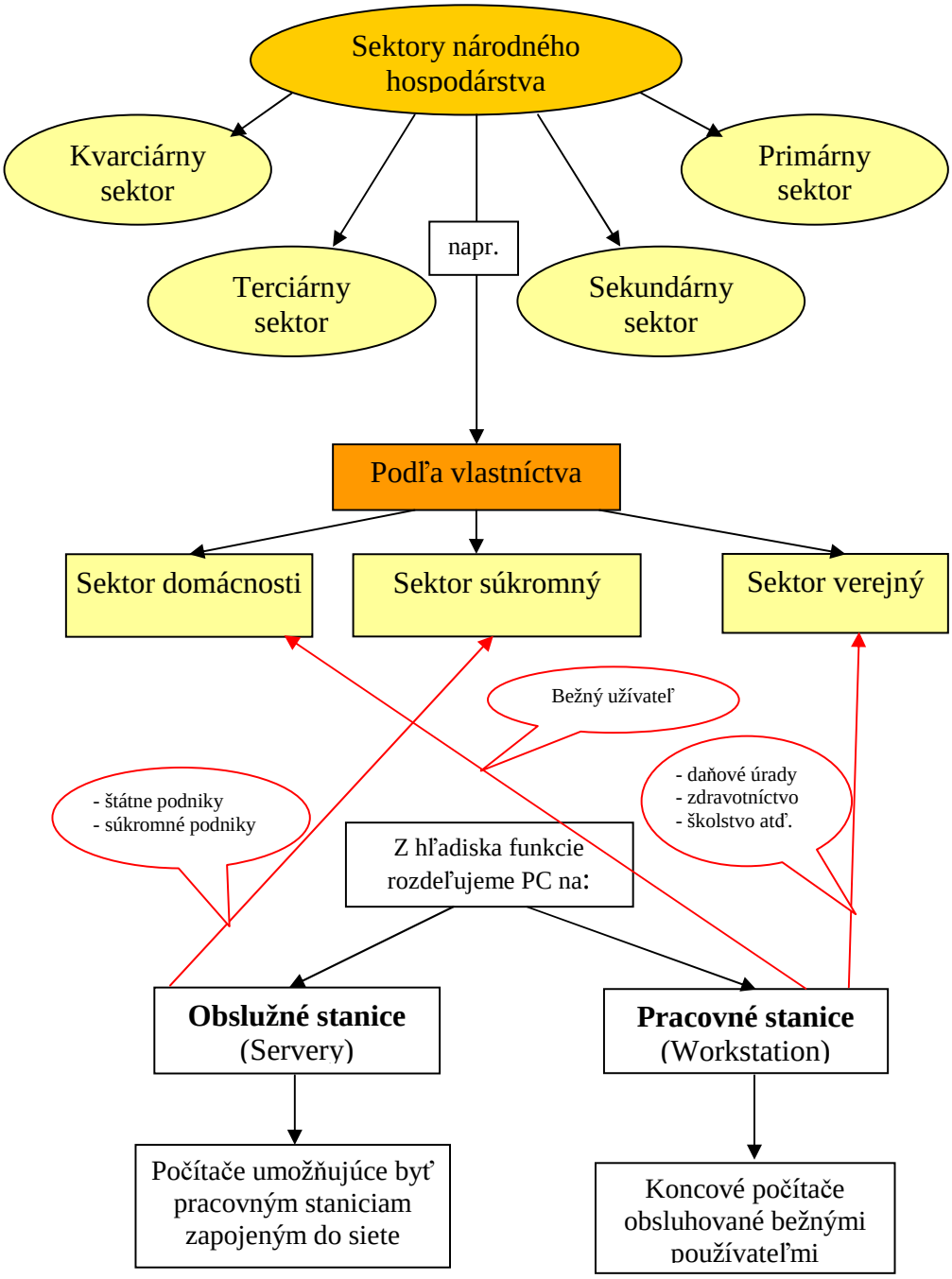
STRNÁD, O. 2009. *Systémový prístup k riadeniu informačnej bezpečnosti.* Vydavateľstvo Tripsoft v Trnave, 2009. s. 233. ISBN 978-80-89291-20-5.

- **NAGI, P. 2003.** *Bezpečnosť informačných systémov*, [online], fel.utc.sk~nagy\Skriptá IS [cit. 9.1.2005]. dostupné na: <http://fel.utc.sk/~nagy/>
- Prispievatelia: Hennyeova, K. *Aspekty informačnej bezpečnosti v podnikaní*, [online], [2010-11-16], Dostupné na: <http://bandlerova.weby.uniag.sk/files/web2/pdf/Hennyeyova.pdf >
- Prispievatelia: *IT Asociácia Slovenska* [online], [cit. 2008-09-01]. Dostupné na: <http://itas.sk/spravy/slovensko-chce-mat-bezpecne-digitalne-prostredie >
- Prispievatelia: IT News. Martin Pavlis. Ako chrániť informácie, keď sa dostanú mimo firmy. [online], [27.04.2010]. Dostupné na:
- <http://www.itnews.sk/tituly/infoware/free-clanky/2010-04-27/c133289-iw-irm-ako-chranit-informacie-ked-sa-dostanu-mimo-firmy>
- Prispievatelia: IT News. Peter Dekýš. Kto by mal mať vo firme na starosti riadenie bezpečnosti. [online], [27.05.2010]. Dostupné na:
- <http://www.itnews.sk/tituly/infoware/free-clanky/2010-05-27/c133797-iw-kto-by-mal-mat-vo-firme-na-starosti-riadenie-bezpecnosti>

PRÍLOHY

Príloha 1

Členenie sektorov národného hospodárstva



Príloha 2

Legislatívny rámec informačnej bezpečnosti v SR

1. **Legislatívny rámec tvoria najmä:**

- Zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a naň nadväzujúce
- Metodické usmernenie Úseku bankového dohľadu NBS č. 7/2004 k overeniu bezpečnosti informačného systému banky a pobočky zahraničnej banky
- Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení zákona č. 678/2006 Z.z.
- Výnos Ministerstva dopravy, pôšt a telekomunikácií SR č. 1706/M-2006 o štandardoch pre informačné systémy verejnej správy (obsahujúci aj bezpečnostné štandardy)
- Zákon č. 618/2003 Z. z. o autorskom práve a o právach súvisiacich s autorským právom (autorský zákon) v znení neskorších predpisov
- Zákon č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov
- Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov
- Zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení zákona č. 284/2002 Z.z., v znení č. 160/2005 Z. z.
- ústavný zákon č. 254/2006 Z. z. o zriadení a činnosti výboru Národnej rady Slovenskej republiky na preskúmanie rozhodnutí Národného bezpečnostného úradu
- Nariadenie vlády č. 216/2004 Z. z., ktorým sa ustanovujú oblasti utajovaných skutočností
- Zákon č. 300/2005 Z. z. z 20. mája 2005, trestný zákon v znení neskorších

predpisov

- Zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov.
- Zákon č. 540/2001 Z. z. o štátnej štatistike v znení neskorších predpisov
- Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Zákony s informačno-bezpečnostným charakterom sú:

- Zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov
- Zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov

Vyhlášky NBÚ upravujúce ochranu utajovaných skutočností sú:

- Vyhláška NBÚ č. 314/2006 Z. z., ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 337/2004 Z.z., ktorou sa upravujú podrobnosti o certifikácii mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov a o ich používaní
- Vyhláška NBÚ č. 315/2006 Z. z., ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti
- Vyhláška NBÚ č. 325/2004 Z. z. o priemyselnej bezpečnosti
- Vyhláška NBÚ č. 331/2004 Z. z. o personálnej bezpečnosti a o skúške bezpečnostného zamestnanca
- Vyhláška NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti
- Vyhláška NBÚ č. 337/2004 Z. z., ktorou sa upravujú podrobnosti o certifikácii mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov a o ich používaní v znení vyhl. NBÚ č. 314/2006 Z.z.
- Vyhláška NBÚ č. 453/2007 Z. z. o administratívnej bezpečnosti

- Vyhláška NBÚ č. 339/2004 Z. z. o bezpečnosti technických prostriedkov
- Vyhláška NBÚ č. 340/2004 Z. z. , ktorou sa ustanovujú podrobnosti o šifrovej ochrane informácií**.**

2. Ďalšie záväzné legislatívne predpisy vyplývajúce SR z členstva v organizáciách EÚ, OSN, NATO, OECD sú:

- Smernica Európskeho parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci spoločenstva pre elektronické podpisy (transponovaná do zákona o el. podpise).
- Smernica Európskeho parlamentu a Rady 95/46/EC z 24. októbra 1995 o ochrane jednotlivcov pri spracovaní osobných údajov a voľnom pohybe týchto údajov (transponovaná do zákona o ochrane osobných údajov)
- Rezolúcia o rešpektovaní ľudských práv v EÚ v roku 1994 zo zasadnutia Európskeho parlamentu, pod číslom A4-0223/96 zo dňa 17. 9. 1996
- Stratégia pre bezpečnú informačnú spoločnosť – „Dialóg, partnerstvo a aktívne pôsobenie“ – SEK (2006) 656 (globálna stratégia EÚ, ktorá vychádza z kultúry bezpečnosti a zakladá sa na dialógu, partnerstve a aktívnom pôsobení).
- smernica Európskeho parlamentu a Rady o službách na vnútornom trhu č. 2006/123/ES z 12. decembra 2006, ktorá má byť do Slovenskej legislatívy zapracovaná do konca roku 2009.
- Európsky dohovor o počítačovej kriminalite č. 185 z roku 2001 (transponovaný v Trestnom zákonníku SR). Podpísali ho členské štáty Rady Európy a ďalšie účastnícke štáty, SR podpísala a ratifikovala dohovor vo februári 2005)
- Dodatkový protokol k Dohovoru o počítačovej kriminalite týkajúci sa kriminalizácie činov rasistickej a xenofóbnej povahy spáchaných prostredníctvom počítačových systémov (č. 189 z roku 2003, ktorý SR zatiaľ neratifikovala)

- Nariadenie komisie (ES) č. 885/2006 - ktorým sa ustanovujú podrobné pravidlá uplatňovania nariadenia Rady (ES) č. 1290/2005 pokiaľ ide o akreditáciu platobných agentúr a iných orgánov a zúčtovania EPZF a EPFRV

3. Nezáväznými dokumentmi sú:

- OECD smernice pre zabezpečenie informačných systémov a sietí: Za kultúru bezpečnosti smernice OECD pre bezpečnosť a prácu v informačných systémoch a sieťach predstavujú dôležitý informačný prameň v oblasti ochrany osobných údajov a v informačných systémoch a ich znenie má byť zohľadnené pri príprave materiálov koncepčného a strategického charakteru.

- Antispamová príručka OECD, OECD v rámci pracovnej skupiny pre oblasť spamu vytvorila príručku tzv. *„Anti-Spam Toolkit“* pre podporu rozvoja komplexných odpovedí na otázky ohľadne spamu. Išlo o prvý krok pri iniciatíve pomôcť riadiacim pracovníkom na najvyššej úrovni, regulátorom, ako aj súkromnému sektoru orientovať ich politiku na riešenie problémov ohľadne spamu a zvyšovať dôveru v internet a emailovú poštu.

- Vzorový zákon o elektronickom podpise UNCITRAL. Bol zohľadnený pri vypracovaní zákona o elektronickom podpise.

Špeciálne postavenie má členstvo v NATO, ktoré v oblasti informačnej bezpečnosti vydáva dokumenty zamerané na utajované skutočnosti, ktoré preberá NBÚ.

Príloha 3

Príklad obsahu bezpečnostnej politiky IS ako písomného dokumentu

Bezpečnostná politika IS

1. Úvod

2. Vymedzenie uvažovaného systému a jeho hraníc

3. Definícia cieľov (ktoré sa chcú dosiahnuť pomocou daného systému a ktoré môžu mať vplyv na návrh bezpečnostného skeletu)

4. Potenciálne nepriaznivé dopady na organizáciu v dôsledku nefunkčnosti IS z dôvodov ako sú:

- nedostupnosť, odmietnutie alebo deštrukcia služieb alebo aktív vrátane informácií
- neautorizovaná modifikácia informácií a softvéru
- neautorizované prezradenie informácií s kvantifikovanim následkov

5. Úroveň investícií do IT v rámci predmetného IS

6. Významné hrozby pre systém a spracovanie informácií

7. Zraniteľnosť zahŕňajúca slabé miesta vyskytujúce sa v systéme, vystavujúce IT identifikovaným rizikám

8. Bezpečnostné riziká, potenciálne ohrozujúce systém a ich finančné ohodnotenie

9. Akceptovateľné zostatkové riziká systému

10. Požadované kategórie bezpečnostných opatrení úmerne identifikovaným rizikám

11. Náklady na bezpečnosť ako výdavky na ochranu aktív IS

12. Vzájomné vzťahy a princípy výberu poskytovateľov vonkajších zdrojov

13. Záver

Príloha 4

Príklad obsahu Bezpečnostného projektu IS ako písomného dokumentu

Bezpečnostný projekt IS

1. Úvod
- dôvod vypracovania
- väzba na bezpečnostnú politiku IS

2. Ciele bezpečnostnej politiky IS alt. bezpečnostného zámeru

3. Vymedzenie IS
3.1 Opis architektúry IS
3.2 Funkčný opis IS
3.3 Klasifikácia dát a dokumentácie z hľadiska nutnej ochrany
3.4 Špecifikácia hrozieb, zraniteľných miest a rizík

4. Riešenie bezpečnosti IS ako celku
4.1 Prierezové oblasti bezpečnosti
4.2 Oblasti bezpečnosti riešené individuálne

5. Bezpečnosť funkčných a systémových celkov
5.1 Centrálny výpočtový systém
5.2 Záložný výpočtový systém
5.3 Uzly siete
5.4 Koncové pracoviská siete
5.5 Komunikačné trasy
5. 6 Vývojové pracovisko
5.7 Externí používatelia systému

Poznámka: Uvádzané členenie IS je potrebné brať ako príklad.

6. Bezpečnosť prepojení systému s inými IS
6.1 Prehľad IS a IT využívaných spoločnosťou, majúcich väzby s riešeným systémom
6.2 Riešenie bezpečnosti vzájomných prepojení
6.3 Postup overovania bezpečnosti prepojení

7. Ekonomika realizácie bezpečnostného projektu
- za jednotlivé funkčné a systémové celky a za IS ako integrovaný celok

8. Harmonogram realizácie projektu

9. Záver

10. Prílohy