OBSAH

ÚVOD

Súčasné obdobie sa vyznačuje vysokým stupňom automatizácie. Sprievodným znakom rozvoja informačných technológií je nárast dostupných informácií aplikovateľných pre riadenie rozhodovacích procesov.

Jedným z najdôležitejších predpokladov ďalšieho rozvoja podnikateľských subjektov v trhovom hospodárstve je istota, že majú vybudované také informačné systémy, ktoré poskytujú informácie podnikovému manažmentu nielen o stave minulom, ale aj stavy do budúcnosti. Zároveň musí poskytnúť aj informácie o prieskume trhu, kde sa pracuje s informáciami sekundárneho charakteru (burzové správy, ročenky, štatistiky a pod.) a predovšetkým informácie primárneho charakteru určené pre potreby manažmentu a marketingu.

Práve špecifické požiadavky manažmentu založené na požiadavkách na kvalitu informácií, rýchlosť ich získavania a ich orientácia na trh a tým aj konkurenčnú schopnosť, si vyžadujú špecializované prístupy k poskytovaniu informácií, ich výberu, dostupnosti spracovania, forme a ostatných atribútov, ktoré z údajov robia skutočné informácie pre rozhodovanie.

Nároky podnikov sa dynamicky menia a internetové aplikácie nachádzajú čoraz častejšie uplatnenie. Tým, ako sa organizácie otvárajú smerom ku svojim zákazníkom, tak táto otvorenosť zároveň zvyšuje riziko neoprávneného prístupu ku citlivým obchodným údajom z internetu. Čím je však aplikácia komplexnejšia, tým väčšie riziko predstavuje. Riešenia, ktoré vyhovovali útokom spred pár rokov sú dnes nepostačujúce. Podniky musia dnes čeliť sofistikovaným útokom cielene zameraným na slabé miesta špecifických aplikácií.

Bezpečnosť podniku a informačných systémov predstavuje v súčasnosti komplexný systém technických a organizačných opatrení. Predstavuje kompromis medzi otvorenosťou dnešných informačných systémov a ich ochranou pred napadnutím prípadne zneužitím citlivých dát organizácie. Podniky potrebujú takú informačnú bezpečnosť, ktorá zodpovedá ich obchodným a prevádzkovým potrebám ako aj rizikám ich informačných aktív. Vždy ide o nájdenie istého rovnovážneho stavu. Pretože najväčšiu hodnotu v každej organizácii tvoria jej informácie.

1 PREHĽAD O SÚČASNOM STAVE RIEŠENEJ PROBLEMATIKY

Pod pojmom bezpečnosť podniku sa rozumie sústavné a efektívne využívanie všetkých zdrojov, zabezpečujúcich stabilné fungovanie podniku v súčasnosti a stály rozvoj v budúcnosti. To však predpokladá aktívny prístup objektu , najmä v smere:

- nepretržitého odhaľovania proximatívnych (bezprostredných) príčin ohrozenia svojej bezpečnosti, tzn. identifikovania, AKO môže byť ohrozená jeho bezpečnosť,
- nepretržitého odhaľovania ultimatívnych (konečných) príčin ohrozenia svojej bezpečnosti, tzn. zisťovania, PREČO môže byť ohrozená jeho bezpečnosť,
- včasného vytvorenia efektívneho bezpečnostného systému na ochranu svojich aktív.

Systém bezpečnosti podniku by mal zabezpečovať:

- rozvoj, ktorý predstavuje jeden z činiteľov ekonomickej bezpečnosti podniku. Ak sa podnik nerozvíja, potom veľmi rýchlo stráca schopnosť prežiť a prispôsobovať sa meniacim sa vnútorným i vonkajším podmienkam.
- pevnosť, stálosť – odráža odolnosť a spoľahlivosť štruktúr podniku, vertikálnych, horizontálnych a iných väzieb v štruktúrach podniku a schopnosť odolávať vonkajším i vnútorným negatívnym javom,
- odolnosť a bezpečnosť – dôležité charakteristiky podniku ako systému. Nemôžu byť dávané do protikladu, pretože každá z nich určitým spôsobom charakterizuje stav podniku. Zabezpečujú sa:

    1. nepretržitou analýzou bezpečnostných rizík podniku,
    2. včasným vytvorením efektívneho bezpečnostného systému a jeho trvalou akcieschopnosťou.

- Podstatou procesu projektovania bezpečnosti ľubovoľného podniku spočíva v realizácii troch krokov :
- definovanie aktív, resp. chráneného záujmu (KOHO alebo ČO chrániť),
- analýza rizík (pred KÝM, pred ČÍM chrániť),

prijatie bezpečnostnej politiky a vytvorenie bezpečnostného systému na ochranu aktív podniku (AKO chrániť). (**URL 1**).

KORCOVÁ (2007) vo svojich príspevkoch neustále zdôrazňuje potrebu kvalitného databázového systému pre účely databázových skladov. Rozvoj databázových systémov bezprostredne súvisí s rozvojom informačných technológií. Nové technické, programové a komunikačné prostriedky ovplyvňujú kvalitu databázových systémov, a tým aj kvalitu informačných systémov. Jednoduchá obsluha, tvorba databáz, rýchle a kvalitné výstupy, ochrana a bezpečnosť údajov sú dôležité tak pre aplikačného programátora ako aj pre užívateľa. Tvorba, aktualizácia a poskytovanie údajov z rôznych databáz prostredníctvom počítačovej siete je dnes bežná požiadavka riadiacich pracovníkov. Týmto aspektom sa venuje pozornosť pri výučbe rôznych druhov databázových systémov v informačných technológiách.

STRANYÁNEK, T. (2003) píše, že bezpečnostná politika IS musí presne definovať postup v prípadoch, keď dôjde k úniku informácií uchovávaných v rámci systému. Predstavuje spracovanie obecných zásad informačnej bezpečnosti pre konkrétny informačný systém.

Bezpečnostná politika IS:

- definuje ciele pre ochranu informácií,
- určuje spôsoby, ako sa pre informačný systém rieši problematika bezpečnosti,
- stanovuje právomoci a zodpovednosť.

BRADLEY (2003) uvádza, že aspoň vo veľkých podnikoch by mal za bezpečnosť informačných systémov zodpovedať bezpečnostný manažér podriadený priamo vedeniu firmy, nakoľko bezpečnosť je prierezový faktor, ktorý sa prelína cez celú organizáciu. Napriek tomu sa o ňu aj vo veľkých firmách stará odbor informačných technológií, pre ktorý je ochrana informačných systémov len jedna z mnohých kompetencií. Môže sa preto stať, že ten istý človek , napríklad administrátor siete, zodpovedá za zmeny a nadstavenia technických zariadení, pričom sa zároveň sám kontroluje. A ak rieši aj bežné prevádzkové problémy a požiadavky používateľov, na bezpečnosť mu nezostáva veľa času. Okrem toho manažéri informačných technológií nemusia mať dostatočné komunikačné schopnosti nato, aby vedenie firmy presvedčili o prioritnom postavení ochrany informačných systémov. Ďalším rizikovým faktorom firemnej bezpečnosti hlavne vo veľkých firmách je nedostatočná motivácia

zamestnancov. Každý si robí svoju prácu a snaží čo najmenej vyrušovať okolie. Táto klíma spoľahlivo otupí aj najväčších nadšencov, ktorí potom robia len to, čo sa od nich bezprostredne vyžaduje a svoje nápady či postrehy si nechávajú len pre seba.

Podľa **ODEHNALA (1999)** existuje jediná 100% spoľahlivá ochrana pred počítačovými vírusmi. Stačí vložiť počítač do veľkej drevenej bedne, poctivo prestrihnúť všetky k nemu vedúce šnúry a zaliať ho betónom. Aj viac-menej dobrý antivírus je k ničomu, ak s ním jeho užívateľ nevie zaobchádzať a nerozumie jeho výsledkom. Porozumieť znamená predovšetkým porozumieť tomu, ako jednotlivé technológie hľadania vírov pracujú. Ich implementácia sa síce v konkrétnych produktoch nepatrne líši a antivírové programy často používajú súčasne niekoľko technológií ako napríklad scanovanie a heuristickú analýzu, princípy ale ostávajú rovnaké.

Internet obracia model IT naruby. To, čo bol starostlivo strážený poklad organizácie ako napríklad obchodné a ekonomické dáta, dnes je zdieľané, spravované a prístupné skoro bez obmedzenia. Chápanie Internetu ako informačnej „super diaľnice" bolo prekonané využívaním Internetu ako nosného prvku komunikačnej stratégie podnikových informačných technológií. Prekrývanie podnikového intranetu s Internetom alebo prepájanie pobočiek podniku cez VPN (Virtual Private Network) úplne stiera donedávna jasné hranice medzi prísne stráženou vnútrofiremnou sieťou a okolím „zvonku". Očakávaným stavom je vyššia prístupnosť a otvorenosť dát a aplikácií smerom na užívateľov, partnerov a zákazníkov podniku. Cenou za lepšiu dostupnosť informácií a dát je zvýšenie bezpečnostných rizík. S rastúcou mierou integrácie web technológií do IT v podniku rastie aj zložitosť a komplexnosť zaistenia bezpečnosti. Už nestačí inštalovať iba firewall a antivírus.

Bezpečnosť sa z kategórie produktu dostala do kategórie komplexného riešenia. Stáva sa ďalšou infraštruktúrnou vrstvou, ktorá je veľmi úzko previazaná s architektúrou samotnej IT infraštruktúry a sú naň kladené podobné očakávania. Musí byť ľahko škálovateľná, flexibilná a centrálne spravovateľná. Ohrozenia a potenciálne straty plynúce z nedostatočného riešenia bezpečnosti sú nepredvídateľné, od zníženia funkčnosti cez odcudzenie citlivých informácií, až po totálnu stratu historických dát podniku. Cesta na elimináciu týchto rizík na predvídateľnú a akceptovateľnú mieru sa začína spísaním základného dokumentu strategického významu. Je ním bezpečnostná politika podniku **(URL 2).**

Podľa **KUCHAŘA, M. (1999)** informačná bezpečnosť predstavuje široký pojem. Ide viac než len o fyzickú bezpečnosť – uzamknutie počítačov a ich umiestnenie v uzamykateľných miestnostiach. Ide predovšetkým o zabezpečenie ochrany informácií počas ich vzniku, spracovávania, ukladania, prenosu a likvidácie prostredníctvom logických, technických, fyzických a organizačných opatrení, ktoré musia pôsobiť proti strate dôvernosti, integrity a dostupnosti týchto hodnôt, z ktorých sa ľahko môžu stať hodnoty trhové, ktoré sú predmetom obchodovania ale i odcudzenia.

Ministerstvo dopravy, pôšt a telekomunikácií definuje *informačnú bezpečnosť* ako 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 čokoľvek - počnúc poškodením vzhľadu webovej stránky, cez napadnutie počítačovým vírusom, až po zlyhanie zamestnanca, ktorý neúmyselne prezradí svoje heslo, či bývalého zamestnanca, ktorý sabotuje zákaznícku databázu a špiónov, ktorí zistia, koľko tovaru si zakúpil váš najlepší zákazník v minulom mesiaci. Informačná bezpečnosť, to je vyváženie rizík výhodami v podobe vykonávania činnosti elektronicky.

HENNYEYOVÁ, K. (2001) uvádza, že informačný systém je integrovanou sústavou informačných zdrojov, technického a programového vybavenia, komunikačných prostriedkov, informačných a komunikačných služieb, organizačných postupov, inštitucionálneho a personálneho zabezpečenia. Súčasný stav informačného systému je charakterizovaný obsahovou rozmanitosťou informačných zdrojov, rozdielnymi metodikami použitými na ich tvorbu a často aj rozdielnymi technológiami použitými na ich implementáciu a prevádzku.

MRNUŠTÍK (1998) uvádza, že tak ako sa objavili stovky hardvérových obchodov a softvérových firiem či odborníkov, objavili sa aj ľudia, ktorí sa rozhodli využiť svoje schopnosti, znalosti a skúsenosti na druhej strane pomyslenej čiary. A okrem nesmierne inteligentných a šikovných programov sa začali objavovať aj produkty, ktorých cieľom nebolo užívateľovi pomáhať, ale škodiť. Je samozrejmé, že vznik týchto produktov a ich postupné a pomerne rýchle šírenie malo za následok aj vznik opozície. Vznikol tak úplne nový odbor, nové produkty a okruh úplne nových služieb poskytovaných zákazníkom. Táto „správna“ strana vznikla a dnes sa už len málokto dokáže rozpamätať na úplne pôvodnú

príčinu jej začiatku. Postupne sa zo softvérovej ochrany stalo softvérové odvetvie, ktoré živí tisíce ľudí. Ide pravdepodobne o oblasť softvérovej tvorby s najväčšou konkurenciou vôbec.

Podľa **KOKLESA, M. a ROMANOVEJ A. (2000)** informačné systémy sú systémy, ktoré sú určené na zhromažďovanie, organizovanie, distribúciu údajov. Údaje spracovávané v informačných systémoch získavajú informačný význam. Informačné systémy sú určené predovšetkým pre manažérov na všetkých úrovniach riadenia. Poskytovaním informácií podporujú ich prácu zvlášť vo fázach plánovania a kontroly riadiaceho procesu. Informačné systémy sú veľmi často automatizované pomocou informačných technológií.

Prakticky sú informačné systémy realizované vo formách:

- neautomatizované (manuálne) informačné systémy, kde sa uskutočňujú všetky operácie klasickými metódami a technickými pomôckami (predtlačené doklady, evidenčné knihy, papier a ceruza, písací stroj, kalkulačka, zakladače, kartotéky).
- automatizované informačné systémy, kde väčšinu rutinných prác vykonáva počítačový systém, ktorý produkuje na základe programu výstupy vtlačenej podobe, príp. na obrazovke.
- kombinované informačné systémy - využívajú koexistenciu manuálneho spracovania (úlohy, ktoré nie sú automatizované počítačovým spracovaním, alebo úlohy, pri ktorých by takéto spracovanie z nejakého dôvodu nebolo možné) a automatizovaného - počítačového spracovania, obidva spôsoby sa navzájom dopĺňajú.

Vírusy dnes predstavujú najznámejšiu a najrozšírenejšiu formu hrozby v IT. Denne sú hlásené desiatky nových vírusov, ktoré sa vďaka Internetu dokážu rozšíriť do celého sveta behom niekoľkých dní. Preto je dnes už nevyhnutné dostatočne sa chrániť pred počítačovými vírusmi a to na úrovni serverov, ako aj pracovných staníc. Pri návrhu antivírusovej infraštruktúry sa preto musí dbať na to, aby sa nevynechal žiaden potencionálny zdroj počítačových vírusov a aby všetky počítače v sieti boli pravidelne updatované. Základom bezpečnej prevádzky IT vo firme je zavedenie celofiremnej bezpečnostnej politiky, ktorá pokrýva všetky faktory počítačovej bezpečnosti. Aj keď veľa firiem má vytvorené bezpečnostné pravidlá, je pre nich veľmi náročné bezpečnostnú politiku uplatňovať **(URL 3).**

McCLURE, S. – SCAMBRAY, J. (2003) vysvetľujú, že na rozdiel od TCSEC sa v ITSEC chápe bezpečnosť systému ako zachovanie atribútov dôvernosti, integrity

a dostupnosti údajov. Bezpečnosť objektu (môže ním byť ucelený systém, ako aj jeho jednotlivé komponenty – produkty) sa hodnotí podľa bezpečnostných funkcií, ktoré poskytuje, a podľa stupňa istoty v účinnosť týchto mechanizmov. V druhom prípade sa ešte rozlišuje medzi istotou v účinnosť bezpečnostných mechanizmov a istotou v správnosť ich návrhu a implementácie.

BAREŠ (2006) uvádza, že výrobcovia dnešných antivírových softvérov vylepšujú a zdokonaľujú svoje produkty v mnohých ohľadoch. V móde je dnes „bundlovanie" tradičných antivírových programov s inými bezpečnostnými komponentmi ako sú firewally či nástroje pre boj so spywarom. V niektorých prípadoch sú to zakomponované doplnkové aplikácie priamo do antivírusov. Spoločnosť sa taktiež snaží skrátiť čas potrebný pre zverejnenie modernizovanej databázy popisujúcu chovanie jednotlivých vírov. Tieto definície potom jednotlivé antivírové aplikácie sťahujú do užívateľských počítačov a používajú ich k rozpoznávaniu a ničeniu novo identifikovaných hrozieb. Producenti antivírusov takisto vybrusujú heuristiku svojich programov, teda matematické algoritmy, ktoré dokážu rozpoznať bezpečnostnú hrozbu podľa podobnosti so skôr identifikovanými časťami škodlivého kódu. Heuristické scanovanie súborov antivírových programov sa v mnohom vylepšilo a v súčasnosti vykazuje úspešnejšiu detekciu a menej falošných poplachov. Jednotlivé programy používajú taktiež rozpoznávanie kódu podľa typu chovania. Táto technológia sleduje časti, na ktoré sa útočníci najčastejšie zameriavajú, a akékoľvek podozrivé chovanie hneď hlási či zastavuje.

Každý systém, u ktorého jeho prevádzkovateľ predpokladá spracovanie dôverných informácií by mal obsahovať prvé dve skupiny požiadaviek. Požiadavky na vnútornú bezpečnosť systému sú aktuálne až pri informačných systémoch, u ktorých sa vytvára zvláštne hardwarové a softwarové vybavenie, tzv. dôveryhodná výpočtová základňa. V niektorých prekladoch je tiež používaný termín dôveryhodná výpočtová báza.

Takto konštruovaný systém, teda systém ktorý spĺňa všetky analyzované bezpečnostné požiadavky, môže čeliť základným útokom na jeho bezpečnosť, ktorými sú:

- neautorizovaný prístup k informáciám vedúci k strate dôveryhodnosti,
- neautorizované zmeny informácií, ktoré vedú ku strate integrity,
- neautorizované oslabenie funkčnosti, ktoré vedie k obmedzeniu dostupnosti požadovaných informácií **(URL 4).**

ŽITŇANSKÝ (2006) uvádza, že straty vyplývajúce z počítačovej kriminality sú dosť vysoké. Čoraz viac činností aj vo verejnom sektore sa presúva na Internet. Bezpečnosť bude z roka na rok dôležitejšia. Vlády sa zatiaľ nejako neprejavujú, akoby si neuvedomovali riziká. Nik sa nepozastaví nad tým, že na bezpečnosť v cestnej premávke vynakladajú prostriedky štáty, súkromné podniky aj občania. Existujú zákony, ktoré určujú povinnosti vlastníkom ciest, výrobcom áut a účastníkom premávky. Tí sa musia správať tak, aby doprava bola čo najbezpečnejšia. Zahŕňa to obrovskú škálu vecí od značenia ciest, používania bezpečnostných pásov a cez autosedačky až po konštrukciu áut. To všetko je upravené v zákonoch. Tak je to aj v iných oblastiach života. Ale takmer vôbec sa legislatíva nezaoberá elektronickou komunikáciou. Určite sa dá pre elektronickú komunikáciu veľa urobiť zákonmi. Zaujímavé však je, že aj zákony ktoré už pre túto komunikáciu platia sa nedodržujú. Represívne zložky štátu nie sú pripravené nato, aby vedeli zasiahnuť. Policajti nevedia zabezpečiť dôkazy, prevádzkovatelia systémov nemajú povinnosť uchovávať záznamy. Akékoľvek dokazovanie je potom veľmi problematické.

Podľa **VYSKOČA, J. (2006)** keď sa rieši bezpečnosť informačného systému, pozornosť sa zameriava predovšetkým proti úmyselným útokom zvonku. O možnosti, že by škody mohol spôsobiť aj niekto zvnútra organizácie sa príliš nehovorí. Dá sa teoretizovať, prečo to tak je. Či preto, že sa ľudia akosi zdráhajú pripustiť možnosť výskytu čiernej ovce medzi sebou, alebo preto, že bezpečnosť sa až príliš často rieši nesystematicky, bez aspoň základnej analýzy možných rizík, čiže jednoduchým hromadením bezpečnostných produktov, ktoré sú spravidla stavané proti útokom zvonku. Oveľa zriedkavejšie sa prípadné bezpečnostné opatrenia proti vnútorným hrozbám orientujú na síce počtom menšiu, ale možnosťami spôsobiť škody oveľa významnejšiu skupinu „insiderov“ – správcov, prípadne programátorov. Prečo to tak je, sa dá celkom logicky odôvodniť. Sú to ľudia, na ktorých spočíva praktická realizácia veľkej časti bezpečnostných opatrení, no a niekomu predsa musíme dôverovať. Nedá sa od nich vyžadovať, aby boli špecialisti na bezpečnosť, len zriedkakedy majú hlbšie znalosti o informačných technológiách ako bežný používateľ, svojimi rozhodnutiami však pritom môžu v podstatnej miere ovplyvniť riešenie bezpečnosti informačného systému organizácie.

Otázka je, či si to uvedomujú. Či si uvedomujú, že ak pri rozdeľovaní balíka peňazí, ktorý je samozrejme vždy menší ako by sa žiadalo, uprednostnia vybavenie nových áut klimatizáciou na úkor požiadavky informatikou na náhradu za zastaraný server, že to môže mať dôsledky na bezpečnosť a spoľahlivosť prevádzky celého informačného systému .

JAROŠOVÁ (2006) uvádza, že najnebezpečnejšie infiltrácie sú dnes výsledkom tvorby profesionálnych autorov. Na svojich výtvoroch chcú zarobiť. Odhaduje sa, že počítačová kriminalita má už väčší objem ako obchod s drogami. Používatelia majú o svoje dáta oprávnený strach a chcú si ich chrániť. Na pomoc im prichádzajú spoločnosti vytvárajúce bezpečnostný softvér. Ponúkajú čo najspoľahlivejšie riešenia, ale aj softvér, ktorý priamo s bezpečnosťou nesúvisí. Pre používateľov Internetu už nie sú najväčšou hrozbou počítačové vírusy. Oveľa viac sa musia obávať škodlivého softvéru označovaného ako adware alebo spyware či trójskych koní.

MANDOK (2006) hovorí, že zachovanie dôveryhodnosti, dostupnosti a integrity informácií spracovávaných a uchovávaných v informačných systémoch, je základnou podmienkou funkčnosti informačného systému ako celku. Dáta, ktorým nemôžeme dôverovať, ktoré nie sú pre nás dostupné alebo sú len čiastočné či poškodené, nemajú pre nás praktický význam. Akákoľvek business aktivita, ktorá je ovplyvnená funkčnosťou informačného systému je závislá i na jeho bezpečnosti. Ochrana informačného systému teda predstavuje ochranu investícií vložených do vybudovania tohto systému a ochranu obchodnej aktivity realizovanej informačným systémom. Každá koruna vložená do budovania a rozvoja infraštruktúry či aplikácií je bez zodpovedajúcej ochrany IKT v ohrození.

POPELKA (1999) prezentuje informačné systémy ako spracovateľa, uschovávateľa a poskytovateľa informácií pre potreby riadenia. V trhovej ekonomike sa musí prispôsobiť aj informačný systém poľnohospodárskeho subjektu. Nevyhnutným je hľadanie a nájdenie spôsobov a metód pre určenie objektívnej potreby informácií pre riadenie daného systému. Ide o vhodný a racionálny výber informácií a zabezpečenie ich tokov v systéme riadenia a ich spracovanie pre potreby riadenia.

Rezort poľnohospodárstva patril k popredným rezortom národného hospodárstva v oblasti aplikácie prostriedkov výpočtovej techniky a automatizácie spracovania informácií. S neustálym kvantitatívnym i kvalitatívnym rastom informácií sa mení vzťah k nim, ale aj k informačným technológiám. Úspešnosť a konkurencieschopnosť akéhokoľvek hospodárskeho subjektu čoraz výraznejšie ovplyvňujú informácie získavané z rôznych zdrojov. Je účelné analyzovať informačné potreby a viac sa orientovať na smery vývoja v medzinárodnom meradle. Aj rezort poľnohospodárstva musí počítať, že sa stane súčasťou informačnej štruktúry, ktorá spolu s príslušnými informačnými technológiami umožní vytvorenie globálnej informačnej spoločnosti.

Nasadzovanie informačných a komunikačných technológií vo všetkých oblastiach života spoločnosti už dávno nie je len otázkou módy či prestíže, ale je v podstate nevyhnutnou podmienkou existencie i rozvoja jednotlivých organizácií. S tým nutne súvisí prirodzená snaha o čo najefektívnejšie využívanie informačných a komunikačných systémov. Čím je IKS pre organizáciu efektívnejší, tým je činnosť organizácie a jej schopnosť plniť svoje poslanie, závislejšia na správnej a neprerušenej činnosti tohto systému. Fungovanie súčasnej spoločnosti závisí od informácií spracovávaných pomocou moderných IKT do takej miery, že ich poškodenie alebo znefunkčnenie môže mať pre spoločnosť vážne následky. IKS sa pritom vyznačujú takou vysokou vnútornou zložitosťou, že aj malá chyba v technickej či programovej realizácii, alebo odchýlka od predpokladanej či požadovanej aktivity používateľov, môže mať vážne až nezvratné dôsledky. Navyše sústreďovaním veľkého množstva údajov na relatívne malom a fyzicky spravidla nedostatočne chránenom priestore, ktoré býva prístupné prostredníctvom komunikačných sietí aj z geograficky vzdialených miest, vznikajú nové hrozby, ktoré súvisia s neoprávnenou manipuláciou s údajmi – od zneužívania dôverných údajov cez neoprávnené zásahy (zmeny) do údajov, až po pokusy podsúvať do systému falošné údaje ako pravé a na tomto základe ovplyvňovať nadväzujúce činnosti **(URL 5).**

McCLURE, S. – SCAMBRAY, J. (2003) pomenovali atribúty, ktoré sú najčastejšie uvažované v kontexte pojmu „ochrana údajov“ (tri z nich – *dôvernosť*, *integrita* a *dostupnosť* sú známe aj pod skratkou CIA, vytvorenou z ich anglických názvov confidentiality, integrity, availability):

- **dôvernosť** – stav, v ktorom je informácia (údaj) utajená, známa iba vymedzenému okruhu subjektov; strata tohto atribútu znamená, že informácia je prezradená (únik informácie), teda že sa stane známou mimo vymedzeného okruhu subjektov,
- **integrita** – informácia (údaj) je celistvá, v pôvodnom, nezmenenom stave, je neporušená; strata tohto atribútu znamená, že informácia je neúplná, nie je v pôvodnom stave, bola (neoprávnene) zmenená,
- **autenticita** – stav, v ktorom je informácia (údaj) pravdivá, skutočná, zodpovedajúca skutočnosti, nespochybniteľného pôvodu, teda je správnou reprezentáciou toho, čo je úmyslom, aby reprezentovala; strata tohto atribútu znamená, že údaj je nesprávny, nezodpovedá skutočnosti, ktorú by mal reprezentovať, je „falošný“ (sfalšovaný),

> **dostupnosť** – stav, v ktorom je informácia (údaj) k dispozícii, schopná bezprostredného použitia na nejaký účel; strata tohto atribútu znamená, že údaj nie je tam, kde je očakávaný, nie je schopný okamžitého použitia.

Pri formulovaní požiadaviek na zabezpečenie ochrany údajov je teda mimoriadne dôležité správne určiť, ktoré údaje (a ktoré ich atribúty) konkrétneho systému je potrebné chrániť.

MADLEŇÁK, R. (2004) zastáva názor, že neustály tok veľmi citlivých a dôležitých informácií, akými nepochybne bankové informácie sú, vyžaduje dostatočnú bezpečnosť a zabezpečenie pred zneužitím. Preto pri využívaní elektronického bankovníctva najdôležitejšiu úlohu hrá vysoká bezpečnosť. Tá je zabezpečená rôznymi formami, akými sú: firewall, elektronický podpis, šifrovanie a ďalšie prvky bezpečnosti. Najdôležitejším sa ukazuje elektronický podpis.

V prípade elektronického bankovníctva má klient možnosť zvoliť si spôsob bezpečného prístupu do systému elektronického bankovníctva, ako aj spôsob elektronického podpisovania dôležitých správ, pričom pri jeho rozhodovaní by malo platiť: väčší objem peňazí vyžaduje dokonalejšiu ochranu. V zásade má klient možnosť výberu medzí niektorou zo symetrických metód alebo môže použiť asymetrickú metódu RSA.

V prípade symetrických metód na strane klienta i na strane banky existuje ten istý tajný kľúč, tento kľúč používajú obe strany na vytváranie jednorazových prístupových hesiel OTP a na výpočet elektronického podpisu, ako aj na overenie správností OTP, resp. certifikačného kódu, ktorý klient poslal banke.

V prípade asymetrickej metódy RSA má kľúč dve časti - tajnú a verejnú. Pomocou tajnej časti kľúča, ktorú si klient dôkladne chráni na diskete alebo čipovej karte, podpisuje klient svoje správy, ktoré odosiela banke. Pomocou verejnej časti kľúča klienta, ktorú má banka k dispozícii, banka overuje integritu a pôvod správy. Tento kľúč má dĺžku 2048 bitov, čo je 256 znakov.

Aj keď je RSA spoľahlivá metóda na zabezpečenie elektronických dát, je dobré mať na pamäti, že bezpečnosť tejto metódy závisí na bezpečnosti uchovávania tajného kľúča uchovávateľa.

ADAMEC, P. (2006) hovorí, že chápanie bezpečnosti ako čisto technologickej záležitosti vedie často k nesprávnemu stanovovaniu priorít a k podceňovaniu dôležitých rizík. Často sa stretávame s názorom, že odbor IT má vedieť, aká úroveň bezpečnosti je adekvátna pre organizáciu. Potreba zabezpečiť ochranu informácií je však v prvom rade odvodená od

dôležitosti a citlivosti informácií pre jednotlivé podnikateľské činnosti. Túto potrebu respektíve mieru citlivosti je primárne schopný posúdiť používateľ údajov a nie IT pracovník, ktorý prevádzkujúci firemný server nemusí mať ani potuchu o tom, že projektová dokumentácia uložená na jeho serveri predstavuje niekoľko rokov práce zamestnancov spoločnosti, a v prípade jej straty alebo získania konkurenciou spoločnosť prichádza o veľké hodnoty, čo môže byť aj dôvodom jej zániku. Je takisto len ťažko možné predpokladať, že IT pozná všetky legislatívne požiadavky vzťahujúce sa na spracúvanie rôznych druhov informácií (napr. osobné údaje, obchodné tajomstvo, bankové tajomstvo, intelektuálne vlastníctvo a pod.) a dosahy na organizáciu, ak tieto požiadavky nebudú splnené. Veľké množstvo informácií existuje v spoločnostiach v neelektronickej forme. Pokiaľ sa informačná bezpečnosť nechápe ako komplexná oblasť prechádzajúca celou organizáciou a nielen cez IT, veľmi ľahko sa môže stať, že informácie prísne strážené v informačných systémoch sa jednoducho vynesú z organizácie napríklad v tlačenej podobe .

HORÁK, J. (2003) zdôrazňuje, že pri hodnotení prínosu prostriedkov fyzickej ochrany k celkovej bezpečnosti informačného systému je potrebné si uvedomiť proti akým protivníkom a za akých predpokladov sú tieto prostriedky účinné. Keďže o oprávnených používateľoch sa obvykle nepredpokladá, že by ignorovali viditeľný pokus o neoprávnený prístup do chránených priestorov, prostriedky fyzickej ochrany sú najčastejšie určené pre použitie v čase neprítomnosti oprávnených používateľov. Je riskantné predpokladať, že samotné prostriedky fyzickej ochrany poskytujú dostatočnú zábranu pred prípadmi zneužitia pridelených práv oprávnenými používateľmi informačného systému alebo inými osobami s povoleným vstupom do chránených priestorov (upratovanie, servis zariadení, strážna služba).

GOSSANÝI (2005) hovorí, že domáci používatelia sú stále častejšie terčom útočníkov, ktorí páchajú krádeže identity, podvody a inú finančne motivovanú trestnú činnosť. Dôvodom tohto nárastu je to, že u týchto používateľov je menšia pravdepodobnosť, že majú zavedené patričné bezpečnostné opatrenia. Útočníci teraz navyše používajú rôzne techniky, ktoré sťažujú zistenie útoku, a pretrvávajú v napadnutých systémoch dlhšie. Majú teda viac času na krádeže informácií, na zneužitie počítača na marketingové účely, umožnenie vzdialeného prístupu alebo na iné ohrozenie dôverných informácií na účel zisku. Prieskumy upozorňujú, že najčastejším terčom útokov je práve sektor domácich používateľov. Pripadá naň 86 % všetkých cielených útokov, a až po ňom nasleduje odvetvie finančných služieb.

Prieskumy zistili nárast útokov zameraných na klientske aplikácie, zvýšené použitie taktík, ktoré sťažujú detekciu, a že veľké a široko rozšírené internetové červy umožnili menšie, viac cielené útoky zamerané na podvody, krádeže dát a trestnú činnosť. Útočníci vidia v koncových používateľoch najslabší článok reťaze zabezpečenia a neustále sa na ne zameriavajú v snahe o vlastné obohatenie.

VYSKOČ, J. (2006) hovorí, že prínos moderných informačných a komunikačných technológií pre ďalší rozvoj jednotlivcov, organizácií i celej spoločnosti je jasný a nespochybniteľný. Na druhej strane, rýchlosť s akou sa tieto technológie vyvíjajú a nasadzujú do reálneho života je výrazne vyššia, ako schopnosť väčšiny ľudí „stráviť" zmeny, ktoré tieto technológie prinášajú. Väčšina ľudí sa tak stáva používateľmi zložitých zariadení, o ktorých podstate a vnútornej činnosti majú v najlepšom prípade len veľmi hmlistú predstavu. V súčasnej dobe je už neodškriepiteľnou skutočnosťou, že vitálne funkcie nielen organizácií ale aj celej spoločnosti, sú čoraz viac závislé od správnej a neprerušenej činnosti čoraz zložitejších systémov, a to tak zložitých, že nie je v ľudských silách detailne postihnúť súvislosti medzi ich jednotlivými komponentmi a následne presne predikovať chovanie sa takýchto systémov za okolností odchyľujúcich sa od bežných stavov. Za daných okolností je používanie moderných technológií prakticky vždy spojené s implicitnou, ale obvykle nevyslovenou vierou v ich správnu činnosť a spoľahlivosť. Činnosť takýchto zložitých systémov pritom však môžu ovplyvniť okolnosti neraz úplne banálneho charakteru.

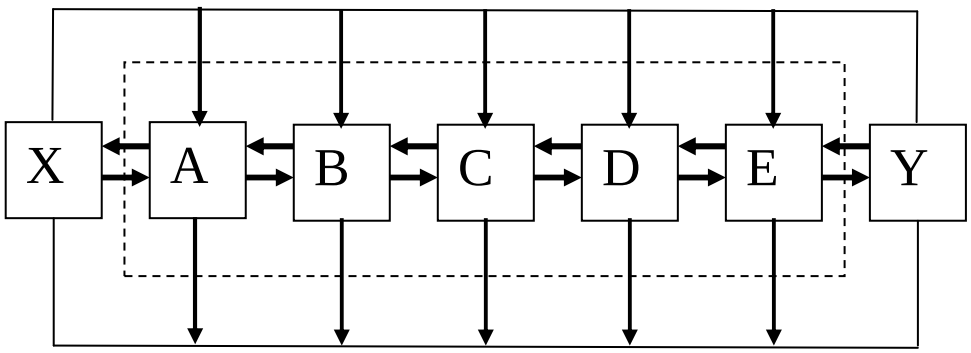
HOCHMAN, J. (2006) tvrdí, že cieľom informačnej bezpečnosti je zabezpečiť, aby elektronické služby poskytované verejnou správou aj súkromným sektorom, boli bezpečné a dôveryhodné pre všetkých občanov štátu. Najväčším nebezpečenstvom je v súčasnosti organizovaný zločin súvisiaci s nezákonným obohacovaním sa, resp. získanie iných informácií za účelom nezákonného konania. Do tejto oblasti spadá aj hrozba zo strany kybernetického terorizmu. Prioritou, ako aj povinnosťou každého štátu, je zabezpečiť informácie proti zneužitiu a eliminovať prípadné následky v čo najväčšom rozsahu. Táto úloha spočíva v starostlivosti a dozore o štátnu a verejnú správu, ako aj samosprávy a podnikateľské prostredie, ktoré súvisí s inými štátnymi systémami.

VYSKOČ, J. (2002) hovorí, že problém bezpečnosti informačných systémov je obvykle chápaný ako „technický" problém, na ktorého riešenie stačí len inštalácia dostatočného množstva technických a programových bezpečnostných prostriedkov. Následne

sa u jednotlivých prevádzkovateľov týchto systémov zužuje aj vnímanie zodpovednosti za zaistenie bezpečnosti systému len na „informatikov“ a to bez ohľadu na skutočnosť, že aj u nich spravidla absentuje primeraná kvalifikácia pre túto oblasť, a čo je horšie, na presadenie prípadných opatrení nemajú ani zodpovedajúce kompetencie. V dôsledku toho je úroveň zabezpečenia jednotlivých informačných systémov spravidla katastrofálna a to ako v rovine koncepcie, tak aj v rovine praktickej implementácie bezpečnostných opatrení. Pri riešení bezpečnosti jednotlivých systémov prevláda „pasívna“ filozofia prístupu k problému ich bezpečnosti, t.j. dôraz sa kladie predovšetkým na určenie zodpovednosti pre prípad bezpečnostného incidentu, na úkor aktívnejšieho prístupu charakterizovaného väčším dôrazom na opatrenia na predchádzanie výskytu týchto incidentov. Dôsledkom sú nedostatočné proaktívne opatrenia na zaistenie bezpečnosti, predovšetkým v oblasti vzdelávania všetkých zainteresovaných, tj. pracovníci útvarov IT, manažment, bežní používatelia IK systémov**.**

HAŠKOVÁ, A. (2004) uvádza, že informačné systémy sú systémy pozostávajúce z ľudí, potenciálnych informácií (dokumentov, údajov, dát), technických prostriedkov, metód a pravidiel zabezpečujúcich zhromažďovanie, spracovanie, uchovávanie a vyhľadávanie informácií za účelom uspokojenia potrieb ich užívateľov. V užšom zmysle slova pod termínom informačný systém rozumieme systém sprostredkovania informácií. V širšom chápaní sa týmto pojmom označuje súbor troch systémov (subsystémov informačného systému):

- systém tvorby informácií,
- systém sprostredkovanie informácií,
- systém využívania informácií.



Obrázok č. 1 : Schéma informačného systému v širšom chápaní,
zdroj: HAŠKOVÁ, A

Legenda k obrázku č.1:

X – vytváranie informácií (zdroj, tvorba informácií)

A – vstup zdrojov informácií (akvizícia)

B – systematizácia informácií (vstupné spracovanie)

C – vytváranie databázy informácií (informačného fondu)

D – vyhľadávanie relevantných informácií (výstupné spracovanie)

E – šírenie informácií (distribúcia), poskytovanie informačných služieb (výstup)

Y – využívanie informácií (užívatelia informácií)

A-E – sprostredkovanie informácií ➔ informačný systém v užšom chápaní

Podľa **DOSEDĚLA, T**. **(2004)** za informačný systém označujeme skupinu počítačov, serverov, diskov a iných záznamových médií, prepojovacích a sieťových káblov, inštalovaných programov a používaných dát. Neoddeliteľnou súčasťou IS sú jeho aktíva – dáta, programy, ktoré je možné presne finančne ohodnotiť. Informačný systém nikdy nie je úplne izolovaný, ale vždy je umiestnený v nejakom prostredí, ktoré ho nezanedbateľnou mierou ovplyvňuje.

Podľa **MOLNÁRA, Z (2000)** je informačný systém definovaný ako súbor ľudí, technických prostriedkov a metód, zabezpečujúcich zber, prenos, uchovanie a spracovanie dát za účelom tvorby a prezentácie informácií pre potreby užívateľov činných v systémoch riadenia. Informačné systémy môžeme deliť do kategórií podľa rôznych hľadísk ako sú účel a obsah, veľkosť, štrukturálna zložitosť, počet a typy užívateľov, územný rozsah, časové charakteristiky a pod.. Za základné druhy informačných systémov autor považuje nasledovné:

- Transakčné systémy
- Priame riadenie procesov (je to zvláštny prípad transakčných systémov pracujúcich v on-line-real-time režime)
- Informačné systémy pre riadenie
- Systémy pre podporu rozhodovania
- Automatizácia podnikovej administratívy
- Útvarové systémy
- Expertné systémy
- Informačné systémy pre vrcholové riadenie
- Strategické informačné systémy
- Metainformačné systémy

JACKOVÁ, A. – ĎURIŠOVÁ, M. (2001) uvádzajú, že informačný systém je účelové usporiadanie vzťahov medzi ľuďmi, dátovými zdrojmi a procedúrami ich spracovania vrátane technologických prostriedkov. Informačný systém predstavuje súbor ľudí, technických prostriedkov a metód zabezpečujúcich zber, prenos, spracovanie a uchovanie informácií. Jeho účelom je tvorba a prezentácia informácií pre potreby ich užívateľov. Taktiež tvrdia, že informačné systémy prešli vo svojom vývoji týmito etapami:

- IS zamerané na spracovanie dát – prispeli k zvýšeniu účinnosti podnikových operácií,
- IS pre riadenie – prispeli k zvýšeniu účinnosti riadenia,
- IS, ktorých cieľom je zvýšenie konkurencieschopnosti podniku.

Za cieľ informačného systému považujú získať z počítača správne informácie pre správnych ľudí, v správnom čase, v potrebnom rozsahu a v požadovanej forme. Základnou funkciou je zabezpečiť nevyhnutné vstupné informácie kombinovaním piatich typických skupín operácií:

- Zabezpečenie vstupných informácií prostredníctvom zberu dát.
- Uchovanie vhodne organizovaných dátových štruktúr umožňujúcich rýchli výber na základe daných požiadaviek.
- Prenos dát z miesta vzniku na miesto ich spracovania a z miesta spracovania na miesto využitia.
- Prezentácia dát vo vhodnej forme.
- Spracovanie dát, ktoré prebieha na základe presne stanovených exaktne vyjadrených postupov, ktorých algoritmy sú uložené vo forme rôzne spracovaných programov.

Podľa **KOKLESA, M. (2000)** je manažérsky informačný systém komplexný a koordinovaný súbor informačných podsystémov, ktoré sú racionálne integrované a ktoré transformujú dáta na informácie rozmanitými cestami za účelom zvýšenia produktivity práce v súlade so štýlom a vlastnosťami manažérov na základe stanovených kvalitatívnych kritérií.

MIŽIČKOVÁ, Ľ. (2004) rozlišuje informačný systém v širšom a užšom zmysle. Informačný systém v širšom zmysle obsahuje celý komunikačný proces obsahujúci zhromažďovanie podkladov k informácií, vypracovanie informácií a ich odovzdanie adresátovi. Informačný systém v užšom zmysle začína zberom informácií a končí vykonávaním informačných služieb, čiže odovzdávaním príslušných informácií

a informačných dokumentov jednotlivým žiadateľom. Vyjadruje iba sprostredkovaciu funkciu komunikačného procesu. Informačný systém sa skladá zo súboru informácií, materiálnych prostriedkov a pracovníkov potrebných na uskutočňovanie informačných tokov, pracovných postupov a väzieb medzi nimi. Definuje sa ako súbor informačných zložiek (informačných činností) a informačných prvkov (jednotlivých informačných prostriedkov) spolu s ich vlastnosťami a vzťahmi, ktoré tvoria usporiadaný celok smerujúci k naplneniu určitého cieľa.

HENNYEYOVÁ, K. (2001) prvky informačného systému rozdeľuje do niekoľkých základných skupín:

- technické prostriedky (hardware) - počítačové systémy rôzneho druhu a veľkosti, doplnené o potrebné periférne jednotky, ktoré sú v prípade potreby prepojené prostredníctvom počítačovej siete,
- programové prostriedky (softvér) — tvorené systémovými programami riadiacimi chod počítača, efektívnu prácu s dátami a komunikáciu počítačového systému s reálnym svetom a programy aplikačne riešiace určité triedy úloh pre určité triedy konkrétnych užívateľov,
- organizačné prostriedky (orgaware) - tvorené súborom nariadení a pravidiel definujúcich prevádzkovanie a využívanie informačného systému a informačných technológií,
- ľudská zložka (peopleware) - riešenie otázky adaptácie a účinného fungovania človeka v počítačovom prostredí, do ktorého bol zaradený,
- reálny svet (informačné zdroje, legislatíva, normy) - kontext informačného systému.

SUCHÁNEK, P. (2000) informačný systém definuje ako súbor ľudí, technických prostriedkov a metód, zabezpečujúcich zber, prenos, ukladanie a spracovanie dát za účelom tvorby a prezentácií informácií pre potreby užívateľov činných v riadiacich systémoch.
Cieľom informačného systému je pritom zhromažďovanie a ukladanie, spracovávanie, vytváranie a prijímanie informácií z okolitého prostredia informačného systému práve tak, ako aj vysielanie informácií do okolia tohto informačného systému.

Podľa **VANĚKA a kol. (2004)** informačné systémy musia v súčasnom ekonomickom, sociálnom a právnom prostredí odpovedať požiadavkám podniku na získanie dôležitých informácií nutných pre udržanie podniku v konkurencieschopnom prostredí:

- manažment znalostí - kapitál znalostí predstavuje jeden z najdôležitejších zdrojov podniku. Kapitál znalostí predstavuje celkovo dôležitú konkurenčnú výhodu, Cieľom manažmentu znalostí je vytvorenie učiaceho sa systému, ktorý je integrovaný do informačného a ligistického systému podniku, monitorujúceho toky dát a informácií a následne zlepšujúceho rozhodovanie a riadenie znalostí, ktoré sú prístupné v informačnom systéme.
- ochrana informácií - rastúca potreba podniku spolupracovať s partnermi v dodavateľsko - odberateľskom reťazci núti podniky poskytovať stále viac informácií. Ochrana informácií sa stáva pre podnik strategickou záležitosťou. Je nutné pritom zabezpečiť jednotné dátové základne, do ktorého sú sústredené všetky dáta, predtým značné rozptýlené. Takto integrované dáta sa ale stávajú dostupnejšie pre ostatných pracovníkov z iných útvarov podniku a súčasne taktiež pred vniknutím nežiaduceho užívateľa z vonkajšieho prostredia. Zneužitie informácií môže pre podnik znamenať nepríjemné straty.
- informačný odpad - informácie sa stali jedným z významných podnikových zdrojov, informácie sú nemateriálnej povahy, nespotrebovávajú sa vo výrobnom procese a nastoľuje sa tu otázka ako ich ďalej uchovávať. Jedná sa predovšetkým o efektívny spôsob ukladania a triedenia dát od každého pracovníka na jeho počítači až po dáta útvaru, podniku. Rovnako dôležitá je efektívna komunikácia - spoločné adresáre umožňujú prostredníctvom mailu distribuovať správu značnému množstvu príjemcov, ktoré môžu pre značnú časť príjemcov znamenať záťaž.

KUČERA, M. – LÁTEČKOVÁ, A. (2004) tvrdia, že s rozvojom informačných technológií a následne informačných systémov sa riešia rôzne spôsoby ich zabezpečenia. Vzniká nový pojem - informačná bezpečnosť (Information Security). Celá táto problematika je tak rozsiahla a závažná, že si vytvorila presnú definíciu. Pod pojmom "informačná bezpečnosť" budeme chápať ochranu informácií v priebehu ich vzniku, spracovania, ukladania, prenosov a likvidácie prostredníctvom logických, technických, fyzických a organizačných opatrení, ktoré musí pôsobiť proti strate dôveryhodnosti, integrity a dostupnosti týchto hodnôt.

Pojmom *hrozba* sa označuje možnosť využiť zraniteľné miesto IS k útoku, k spôsobeniu škody na aktívach. **BOTT, E. – SEICHERT, C. (2004)** hrozby kategorizujú na:

- **objektívne**
  1. *prírodné, fyzické* (požiar, povodeň, výpadok elektrického napätia, poruchy – u ktorých je prevencia obtiažna a u ktorých je potreba riešiť skôr minimalizovanie dopadu vhodným plánom obnovy, havarijný plán),
  2. *fyzikálne* (elektromagnetické vyžarovanie),
  3. *technické, logické* (porucha pamäte, softwarové „zadné dvierka“, nevhodne prepojenie inak bezpečných komponentov, krádež resp. zničenie pamäťového média alebo nedokonalé zrušenie, odstránenie informácií na ňom).
- **subjektívne**
  1. *neúmyselné* (pôsobenie neškoleného užívateľa, správcu),
  2. *úmyselné* (predstavované potenciálnou existenciou *vonkajších útočníkov* (špióni, kriminálne živly, konkurenti, hackeri) i *vnútorných útočníkov* (80% útokov je vedená zvnútra prepusteným, rozhnevaným, vydieraným, chamtivým zamestnancom).

Podľa **KOKLESA, M (2000)** je vírus program, ktorý sa pripája k iným programom alebo údajom a stáva sa ich súčasťou. Je schopný preniknúť do operačného systému alebo používateľského programu, pripojiť sa k nemu a na ňom potom parazitovať. Program, ktorý je napadnutý vírusom, môže byť nakazený, chorý alebo mŕtvy. Vírus je v zásade schopný rozmnožovať, maskovať sa a škodiť.

2 CIEĽ PRÁCE

Súčasná podnikateľská prax si vyžaduje také nasadenie informačných systémov, aby riadiaci pracovníci na všetkých stupňoch riadenia, a taktiež výkonný personál mal stály prísun dostatočné množstvo kvalitných informácií.

Len dostatočne zabezpečený informačný systém je schopný poskytovať služby na požadovanej úrovni. Nakoľko pod pojmom informačný systém rozumieme celý proces spracovania informácie od jej vzniku až po jej odovzdanie či uloženie, musíme brať do úvahy často vysoké množstvo ľudí, ktorí sa do celého tohto procesu zapájajú. Jedine komplexné zabezpečenie celého uvedeného procesu a jeho okolia je schopné zaistiť dostatočnú ochranu informačného systému. Aj keď treba mať stále na zreteli, že dokonale zabezpečený systém nikdy neexistoval, neexistuje a na základe skúseností z minulosti a sledovania súčasných trendov ani existovať nebude.

Cieľom diplomovej práce bolo:

- Nadobudnúť široké rozpätie vedomostí z oblasti počítačovej bezpečnosti, ochrany údajov, infiltrácií a ostatných hrozieb pre informačné systémy podnikov.
- Preskúmať dôkladnú situačnú analýzu v spoločnosti PRASTAV s.r.o., ako aj jej hardvérového a softvérového vybavenia.
- Zanalyzovať celkový stav bezpečnosti informačného systému a bezpečnosti ako celku v danom podniku.
- Na základe získaných poznatkov a vedomostí nájsť slabé miesta v bezpečnosti podniku, predložiť návrh na ich odstránenie a dopomôcť k vytvoreniu novej bezpečnostnej politiky pre danú spoločnosť.

Nakoľko problematika bezpečnosti podniku a počítačovej bezpečnosti je veľmi široká, diplomová práca je zameraná hlavne na ochranu počítačových systémov pred infiltráciami, technickú a programovú bezpečnosť.

3 METODIKA PRÁCE

Na základe získaných vedomostí sme zhodnotili situáciu v stavebnej spoločnosti PRASTAV s.r.o., našli slabé miesta v počítačovej bezpečnosti a sformulovali návrh na komplexné zlepšenie celkového stavu ochrany informačného systému a celkového stavu IKT.

Pre vypracovanie diplomovej práce sme zdroje a podklady získali viacerými spôsobmi:

- Vytypovaním vhodného podniku na zozbieranie praktických poznatkov, ako aj aplikáciu návrhov na zlepšenie.
- Štúdiom dostupnej literatúry (domácej i zahraničnej) zaoberajúcej sa problematikou bezpečnosti podniku, počítačovej bezpečnosti, ochrany dát a informačných systémov.
- Štúdiom týždenníkov zaoberajúcich sa počítačovou problematikou a iných vhodných ekonomických periodík.
- On-line konzultáciami so správcami bezpečnosti informačných systémov v iných podnikoch ale aj konzultáciami so zamestnancom spoločnosti PRASTAV určeného pre oblasť informačných technológií.
- Dôkladným sledovaním stavu informačných a komunikačných technológií v danom podniku a prístupu zamestnancov k počítačovej bezpečnosti.
- Využívaním teoretických poznatkov v praxi.

Hlavné metódy použité v diplomovej práci:

1) **Analýza** – daný podnik bolo potrebné dôsledne analyzovať pre presné zistenie jeho silných a slabých stránok v počítačovej bezpečnosti, zároveň boli analyzované aj jeho príjmy a výdavky.
2) **Syntéza** – výsledky získané analýzou poslúžili pri metóde syntézy, boli vytvorené komplexné návrhy na zlepšenie danej situácie v počítačovej bezpečnosti podniku, analýza príjmov a výdavkov poslúžila pre nájdenie možných finančných zdrojov použiteľných na zlepšenie bezpečnosti IKT v podniku.
3) **Komparácia** – metóda komparácie bola použitá ako posledná, pri porovnávaní návrhov bezpečnostnej politiky pre podnik s jeho pôvodným stavom.

Práca je rozčlenená do siedmich kapitol. Prvá kapitola obsahuje prehľad o súčasnom stave riešenej problematiky, druhá kapitola pojednáva o cieli diplomovej práce, v tretej je uvedená metodika práce. Úvod štvrtej kapitoly je venovaný teórii týkajúcej sa informačných systémov všeobecne a ich bezpečnosti, softvérové zabezpečenie IS, druhom počítačových hrozieb a možnosťami ochrany systémov pred týmito hrozbami. V štvrtej kapitole sa nachádza aj bližší popis konkrétnej spoločnosti, stavu jej počítačovej bezpečnosti a návrhy na jej komplexné zlepšenie. V piatej kapitole sa nachádza záver a návrhy pre využitie nadobudnutých poznatkov. Šiesta časť obsahuje použitú literatúru a nakoniec v poslednej časti sú uvedené prílohy.

4 BEZPEČNOSŤ INFORMAČNÉHO SYSTÉMU A OCHRANA ÚDAJOV

4.2 Informačné systémy

4.2.1 Charakteristika informačných systémov

V odbornej literatúre sa stretávame s pojmom informačný systém v dvojakom význame. V užšom – programovo-technickom chápaní, na označenie systému programov pre prácu s údajmi. V širšom chápaní rozumieme informačným systémov systém na zabezpečovanie informácií potrebných na riadenie.

V prvom prípade je hlavnou úlohou systému spracovanie údajov, ktoré v podniku vznikli. Nerieši otázky pre koho a na aké rozhodnutia budú tieto údaje slúžiť. Z tohto vymedzeného definovania informačného systému vyplýva, že systém spracovania údajov je len jeden z podsystémov informačného systému.

V druhom prípade ide nielen o spracovanie údajov, ale aj o zhromažďovanie, prenos, uchovávanie, výber a distribúciu údajov pre potreby riadiaceho subjektu. Informačný systém nemožno teda stotožňovať len so systémom spracovania údajov. Je to systém pozostávajúci z ľudí, technických a programových prostriedkov na zabezpečenie zhromažďovania, prenosu, ukladania, výberu, spracovania, distribúcie a prezentácie informácií pre potrebu rozhodovania tak, aby riadiaci pracovníci mohli vykonávať svoje riadiace funkcie vo všetkých zložkách riadiaceho systému. Jeho základnou úlohou je zabezpečiť dostatok relevantných, správnych a presných informácií v potrebných termínoch a v požadovanej forme na prípravu rozhodnutí.

Informácie hrajú veľkú úlohu v živote jednotlivca, o to väčšiu úlohu majú v hospodárskej praxi, pri riadení činnosti podniku, organizácie, štátu a pod. pre uľahčenie práce s informáciami sa vytvárajú informačné systémy. Problematika tvorby a využívania informačných systémov v praxi je veľmi zložitá a komplexná. V poslednej dobe sa snaha zameriava na čo najplnšie rozpracovanie teoretických princípov práce s informáciami pri vytváraní informačných systémov a ich automatizácií aplikáciou informačných technológií.

Informačný systém má pri riadení organizácie jednu z kľúčových úloh, prechádza celou organizáciou a spája jej jednotlivé prvky do jedného celku. Informačný systém začína získavaním informácií a končí ich využívaním. Úlohou

informačného systému je vypracovanie nevyhnutných informácií na účinné riadenie organizácie a spojenie jej riadiaceho a riadeného systému. Informačný systém podporuje *manažérske činnosti 2 spôsobmi*:

1. umožňujú manažérom *pochopiť komplex vzťahov* medzi riadenou organizáciou a okolím. Mali by poskytovať spravodajské informácie o vplyve okolia na riadení organizáciu a zároveň i verejné informácie o vplyve organizácie na jej okolie.
2. manažérom na rôznych úrovniach organizačnej hierarchie umožňuje *rozhodovanie a riešenie problémov* pri riadení organizácie, vrcholní manažéri formulujú a optimalizujú dlhodobé plány a robia strategické rozhodnutia, manažéri na strednej úrovni implementujú a konkretizujú strategické rozhodnutia. Manažéri na najnižšej úrovni riadenia vytvárajú a objektivizujú operatívne plány a robia operatívne denné riadiace činnosti.

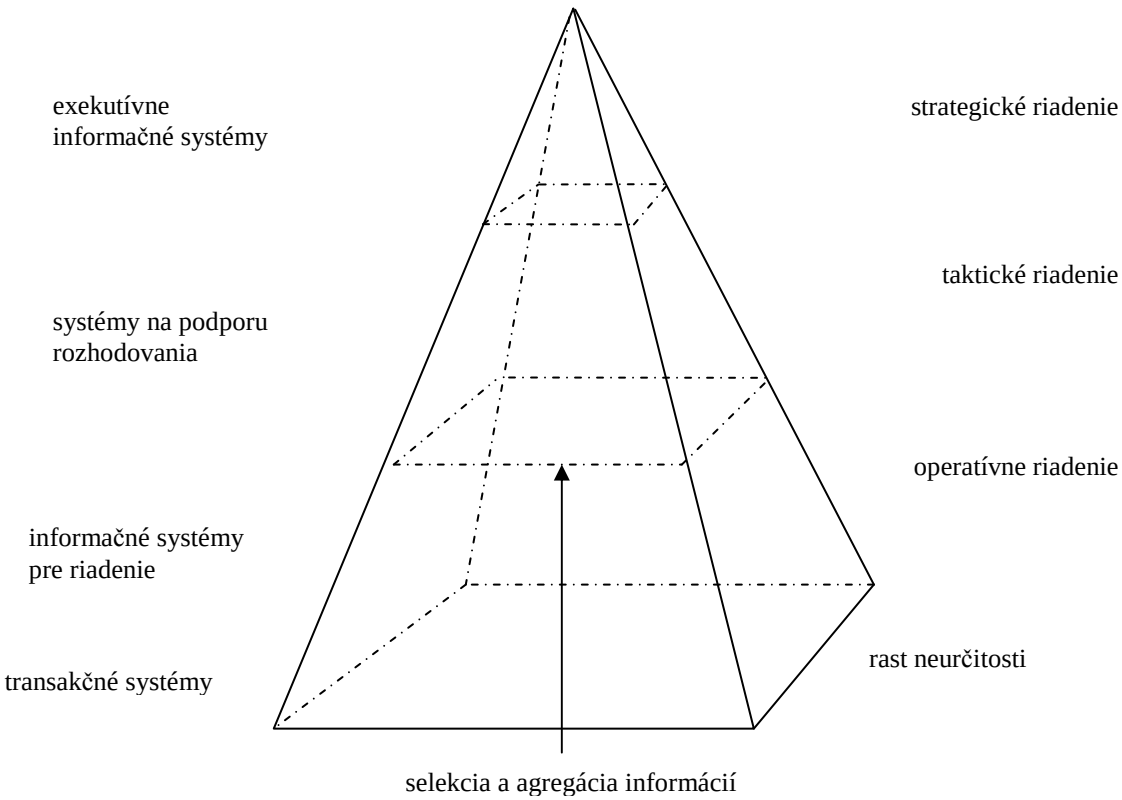
4.2.2 Členenie informačných systémov

Informačné systémy môžeme deliť do kategórií podľa rôznych hľadísk, ako sú účel, obsah, veľkosť, štrukturálna zložitosť, počet a typy používateľov, územný rozsah, časové charakteristiky a pod.

Z hľadiska podpory informačného systému manažérskej práce, čiže jeho postavenia v systéme riadenia rozdeľujeme informačné systémy na:

- **Transakčné systémy** - zahrňujú rutinné, každodenné účtovné operácie. Tieto operácie spájajú odberateľa, podnik, sklad a výrobu, pohľadávky, záväzky, kontrolu zásob a podobne. Transakčný systém spravidla zasahuje do všetkých oblastí činností podniku a prepája celý podnikový finančný systém, výrobu, spotrebiteľov a dodávateľov.
- **Systémy pre priame riadenie procesov** - majú minimálny podiel vstupov a výstupov realizovaných prostredníctvom človeka. Pracujú ako on-line a real-time režime na priame riadenie technologických procesov.
- **Systémy na priame riadenie** - vznikli z účtovných a ekonomických systémov podnikov a organizácií. V oblasti týchto informačných systémov sa objavujú aktuálne informácie prezentované tlačenými výstupmi na papieri alebo vo forme elektronickej pošty. Informačné systémy na riadenie však vo väčšine prípadov nepoužívajú predmetové databázy z transakčných systémov.

- **Exekutívne informačné systémy** – často označovaný aj ako informačný systém pre vrcholové riadenie. Sú to systémy, ktoré informačne zabezpečujú vrchol pyramídy. Slúžia predovšetkým vrcholovému vedeniu podniku.
- **Systémy na podporu rozhodovania** - majú schopnosť vykonávať rôzne analýzy rovnakých dát bez potreby zložitejšieho programovania. Jedná sa o počítačovú podporu metód rozhodovacej analýzy a operačnej systémovej analýzy. Systémy na podporu rozhodovania sú flexibilnejšie ako transakčné systémy alebo systémy na riadenie. Nie sú založené na nemenných rozhodovacích pravidlách.
- **Strategické informačné systémy** – sú to aplikácie informačných systémov, ktorých cieľom je zvýšenie konkurencieschopnosti podniku. Pôsobia prevažne v oblasti trhu, teda v okolí podniku a ich účinok musí byť revolučný.
- **Metainformačné systémy** – slúžia pre riadenie projekčných prác, výstavbu a prevádzku IS. Pre potreby používateľov je potrebné mať priebežne k dispozícii dokonalý a podrobný obraz podnikového informačného systému, ktorý nazývame metainformačný systém.



Obrázok č. 2: Informačná pyramída
Zdroj: Kučera M.: Informačné systémy v poľnohospodárstve

4.2.3 Softvérové zabezpečenie informačných systémov

Existuje veľké množstvo softvérov na zabezpečenie IS. Medzi známe či menej známe softvéry patria napríklad: Etos Soft, Insurence Contract Manager, Chastia FM a veľa ďalších. Všetky tieto softvéry sa veľmi nelíšia od seba, preto som spomedzi týchto softvérov rozobral softvér Chastia FM.

Chastia Facility Manažment

Je prvým slovenským komplexným graficko-databázovým programovým systémom pre podporu správy majetku. Rieši evidenciu majetku, správu projektovej, obchodnej, prevádzkovej a inej dokumentácie, automatizáciu tvorby zmlúv a faktúr pre správcovské činnosti a nájomné vzťahy, rozúčtovanie energií a služieb, energetický manažment budov (areálov, veľkých územných celkov), údržbu objektov a zariadení atď..

Informačný systém je určený najmä pre:

- správcov majetku vo všetkých oblastiach činnosti,
- výrobcov tepla,
- bytové družstvá a bytové podniky,
- hotely, administratívne budovy, priemyselné podniky,
- realitné kancelárie,
- každého, kto potrebuje spravovať nejaký majetok,
- ...

Systém rieši tieto hlavné oblasti

- grafickú evidenciu nehnuteľností, technických zariadení objektov a inžinierskych sietí,
- elektronický archív všetkej súvisiacej dokumentácie (projektovej, obchodnej, prevádzkovej),
- evidenciu a vyhodnocovanie prevádzkových veličín (energií, služieb, technologických údajov atď.),
- rozúčtovanie energií a služieb,
- automatizáciu tvorby zmlúv a faktúr za správcovské činnosti, nájmy ...
- údržbu technických zariadení,
- sledovanie nákladov na správu a prevádzku objektov,
- ...

Moduly

Univerzálne moduly

- Základný modul - je jediným povinným modulom. Obsahuje jednak základnú evidenciu objektov IS a jednak všetky funkcie a evidenčné tabuľky, ktoré sú spoločné pre všetky ostatné moduly.
- Grafika - obsahuje grafický prehliadač, grafický editor, editor a prehliadač výkresových tlačových zostáv a všetky funkcie a evidenčné tabuľky potrebné pre tvorbu a udržiavanie grafickej časti projektu.
- Katalógy - modul umožňuje katalogizovať často sa opakujúce informácie.
- Dokumenty - zabezpečuje správu všetkej potrebnej dokumentácie (projektová, obchodná, prevádzková a pod.).

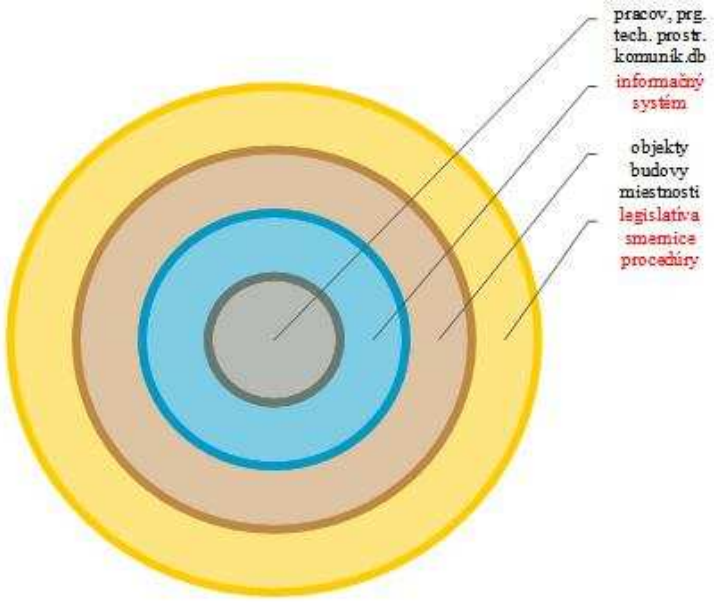
Špecializované moduly

- *Majetok* - rieši celý životný cyklus objektu IS od nadobudnutia až po vyradenie, vr. plánovania a vyhodnocovania údržby.
- *Plochy a priestory* - slúži na rozšírenú evidenciu plôch a priestorov, ich vlastností, výmer a spôsob ich využitia pri ich správe a nájmoch.
- *Energie a služby* - obsahuje riešenie dvoch hlavných oblastí - rozúčtovanie energií a služieb a energetický manažment.
- *Správa majetku a nájmy* - modul zastrešuje správcovské činnosti v Chastii FM. Jeho obsahom sú zmluvné vzťahy a fakturácia pre štyri oblasti činnosti správcov - prideľovanie plôch a zariadení vlastným oddeleniam, nájmy cudzím firmám, správa majetku obecne a dodávky energií a služieb (napr. pre centrálnych výrobcov tepla).
- *Ľudské zdroje* - zabezpečuje evidenciu zamestnancov vo väzbe na požiadavky ostatných modulov.

4.3 Bezpečnosť informačného systému

Cieľom prevádzkovateľa IS musí byť dosiahnuť čo najvyššiu bezpečnosť systému, ktorá zaručuje minimálne účinky a možnosti zneužitia informácií.
Mnoho ľudí si myslí, že zabezpečenie IS je len použitie dômyselných hesiel. Opak je však pravdou. Bezpečnosť tu chápeme zabezpečenie systému ako celku.

Treba upozorniť na to, že rôzny pohľad na bezpečnosť bude v štátnych vojenských, policajných a komerčných – obchodných a finančných sektoroch. Funkcie počítačového zabezpečenia budú rôzne v závislosti na typu organizácie a jej veľkosti. Niekde to môže byť jeden PC pracovník, inde celý pracovný tím v ktorom každý pracovník sleduje odlišné aspekty počítačovej bezpečnosti.



Obrázok č. 3: Obecný model IS a jeho reálneho okolia

4.3.1 Základné pojmy

Bezpečnosť /Security /- pod týmto pojmom chápeme vlastnosť nejakého objektu alebo subjektu / IS alebo IT technológie /, ktorá určuje mieru ochrany proti možným škodám alebo hrozbám.

Citlivé údaje / Sensitive Data / - sú údaje a informácie, ktoré vyžadujú ochranu, pretože existuje určitá pravdepodobnosť hrozieb. Sú to údaje, ktorých neoprávnené použitie môže spôsobiť určitú škodu. V IS sa jedná predovšetkým o personálne informácie, údaje chránené

podľa zákona o štátnom s služobnom tajomstve a informácie, ktoré sa týkajú chodu organizácií – finančné agendy, jednotlivé podsystémy.
Expozícia / Exposure / - je miesto potencionálneho poškodenia alebo straty informácií. / napr. odhalenie utaj. dát, ich neoprávnená modifikácia, odmietnutie prístupu autorizovaného užívateľa /

Hodnota aktíva / Asset Value / - je cena alebo ocenenie dôležitosti a významu pre vlastníka, ktoré sa často nedá vyjadriť vo finančnom vyjadrení.

Hrozba / Thread / - je skutočnosť alebo udalosť, ktorá môže spôsobiť poškodenie, zničenie hodnoty aktíva. / vlastný zamestnanec, prírodná katastrofa, hacker a pod. /

Informačný systém / Information System / - je súbor technického / hardware/ a programového /softvér/ vybavenia, záznamových médií, dát a personálu, ktoré používa organizácia k spravovaniu svojich informácií. Tieto hmotné a nehmotné objekty sú cielene vyberané a vzájomne poprepájané za účelom zberu, výmeny, spracovania a uchovania, generovania a distribúcie informácií a údajov vo vopred definovanej štruktúre a čase a to za účelom výkonu rozhodnutí, podpory rozhodovania a informovanosti.

Informačné technológie / Information Technology / je technika, ktorá sa podieľa na spracovaní informácií a dát. Je to predovšetkým výpočtová technika, komunikačná technika a programové vybavenie.

Narušenie bezpečnosti / Security Incident / - je porušenie bezpečnostných kontrol IS, kde je získaný prístup k informáciám, ktorý porušuje bezpečnostnú politiku.

Objekt / Object / - je pasívna entita, ktorá obsahuje alebo spracováva ľubovoľné informácie . V IS je to predovšetkým súbor na pamäťovom nosiči, blok dát, záznam a pod.

Subjekt / Subject / - je aktívna entita, ktorá ovplyvňuje tok informácií medzi objektmi. / napr. užívateľ, systémový proces /

Zraniteľnosť / Vulnerability / - je nedostatok prípadne slabina celého bezpečnostného systému, ktorá môže byť zneužitá hrozbou tak, že dôjde k poškodeniu alebo zničeniu aktíva.

Riziko / Risk/ - je pravdepodobnosť, s akou bude daná hodnota / aktívum / zničená alebo poškodená pôsobením konkrétnej hrozby. Je to miera ohrozenia aktíva.

Ocenenie rizík / Risk Assessment / je proces vyhodnotenia hrozieb, ktoré pôsobia na IS a cieľom definovať úroveň rizika, ktorému je vystavený. Cieľom je zistiť, či sú bezpečnostné opatrenia dostatočné.

Prienik / Intrusion / - je neautorizované zneužitie IS.

Zvládanie rizík / Risk Manažment / - je proces, pomocou ktorého je možné určiť, kontrolovať a obmedzovať vplyv nepredvídaných udalostí – hrozieb. Obsahuje analýzu a odhad rizík, implementáciu, testovanie a prevádzkovanie bezpečnosti.

Protiopatrenia / Countermeasure / - je činnosť zariadenie alebo proces, ktorý chráni IS a jeho aktíva pred pôsobením konkrétnych hrozieb.

4.3.2 Základné spôsoby ochrany informačných systémov

Ochranné mechanizmy realizujú ochranu aktív tak, že sa snažia minimalizovať riziko pôsobenia hrozieb. Jedná sa predovšetkým o cenu ochranných mechanizmov v pomere k ich bezpečnostnému efektu. Cyklus zavádzania PC bezpečnosti je neustály proces, ktorý periodicky kontroluje úroveň bezpečnostných opatrení a podľa potreby ich aktualizuje a vylepšuje. Celkové riešenie ochrany vyžaduje kombináciu technických a netechnických postupov a metód.

Konkrétna realizácia informačnej bezpečnosti je závislá na mnohých vplyvoch ako napr. veľkosť systému, citlivosť informácií, dostupnosť technológií, finančných možnostiach a pod.

Bezpečnostná politika / Security Policy /

Základným kameňom bezpečnosti IS je ***bezpečnostná politika***.. Podmieňujúcim faktorom je integrácia všetkých súčastí IS do bezpečnostnej politiky. Ide teda o komplex personálnych, fyzických a organizačných bezpečnostných pravidiel a opatrení. Neoddeliteľnou súčasťou je určenie bezpečnostných cieľov a definovanie rizík.

Inými slovami povedané ***bezpečnostná politika*** je súhrn pravidiel, zbierka detailných špecifikácií čo chrániť, proti komu a čomu, akými prostriedkami, ktoré sú aplikovateľné na ochranu špecifických dát, identifikácia zodpovednosti a časovej následnosti.

Je základné východisko pre riadenie bezpečnosti informačného systému organizácie. Organizácia by mala mat‘ vrcholovým vedením schválenú bezpečnostnú politiku, ktorá

stanovuje ciele, ktoré je potrebné v oblasti bezpečnosti informačného systému dosiahnuť‘ a základné princípy a nástroje na dosiahnutie týchto cieľov. Ide o dokument koncepčného charakteru, ktorý zahŕňa všetky zdroje IS.

Bezpečnostná politika by mala zahŕňať najmä:

- popis IS – zabezpečenie musí byť definované na konkrétnu štruktúru IS konkrétnej organizácie. Obsahuje popis organizačnej štruktúry organizácie, ciele a úlohy, ktoré bude IS plniť a informačné toky v rámci IS,
- legislatívne východiská – právne normatívy a predpisy, ktoré musí IS rešpektovať
- stanovenie cieľov, ktoré chce organizácia v oblasti informačnej bezpečnosti dosiahnuť‘,
- určenie základných princípov, nástrojov a postupov, pomocou ktorých možno dosiahnuť‘ stanovené ciele,
- určenie právomoci a zodpovednosti za dosiahnutie stanovených cieľov a za riadenie informačnej bezpečnosti,
- určenie osoby zodpovednej za bezpečnostnú politiku ako celok a plán aktualizácie bezpečnostnej politiky.

Druhy bezpečnostných opatrení

Každý IS sa skladá spravidla z viacerých základných častí. Môžeme ho rozdeliť na dátovú, programovú, technickú a komunikačnú časť a na personál, ktorý ho prevádzkuje. Každá z týchto častí hrá dôležitú úlohu v celkovej bezpečnosti IS. Bezpečnosť IS sa realizuje kombináciou rôznych bezpečnostných mechanizmov a opatrení. Môžeme ju rozdeliť do nasledovných častí :

- personálna bezpečnosť,
- fyzická bezpečnosť,
- technická bezpečnosť,
- programová bezpečnosť.

Personálna bezpečnosť

Tieto opatrenia sú realizované na ochranu IS pred nežiaducimi vplyvmi ľudského faktora. Ich úlohou je definovať požiadavky na vlastnosti osôb, ktorí pracujú v rámci IS, ich

výber, výchovu a predbežnú kontrolu. Prax ukazuje, že sa vynakladá množstvo prostriedkov na zabezpečenie technických a programových bezpečnostných opatrení a často sa zabúda na vplyv ľudského faktoru vlastných zamestnancov. Pritom štatistiky poukazujú na to, že zo známych narušení bezpečnosti IS sa približne v 70 % prípadov jednalo o vlastných zamestnancov, ktorý zámerne alebo neúmyselne spôsobili škodu.

Cieľom personálnej bezpečnosti je znižovať riziko ľudského faktora (omyly, krádeže, podvody, zneužívanie), zabezpečiť‘ dostatočnú informovanosť zamestnancov o hrozbách bezpečnosti v podniku a zaistiť‘ ich pripravenosť‘ na bezpečnostné incidenty a nesprávnu funkciu softvéru.

Fyzická bezpečnosť

Sú to opatrenia, ktoré sú potrebné k zabezpečeniu fyzickej ochrany IS proti náhodným i úmyselným hrozbám. Je to predovšetkým zabezpečenie budov v ktorých je IS umiestnený.

Patria sem opatrenia na elimináciu vplyvu prírodných katastrôf, poveternostných vplyvov, povodne, opatrenia proti vniknutiu neoprávnených osôb, opatrenia, ktoré riešia bezpečné uloženie dátových nosičov, ochrana proti prírodným živlom, požiaru a pod. Jedná sa predovšetkým o nasledovné opatrenia:

- ochranu objektov, strážna služba, napojenie sa na PCO – pult centrálnej ochrany,
- EPS / elektronický požiarny systém /,
- EZS / elektronicky zabezpečovací systém /,
- kamerový systém , monitorovanie objektu,
- monitorovanie pohybu osôb pri vstupe do jednotlivých bezpečnostných zón prostredníctvom identifikačných kariet / magnetické, cípové, karty s čiarkovým kódom,
- trezory na uloženie dátových nosičov, opatrenia na skartáciu médií.

Fyzická bezpečnosť a bezpečnosť prostredia zahŕňa:

Vytvorenie zabezpečených oblastí, na účely zabránenia neautorizovanému prístupu:

- vypracovať procedúry pre umiestňovanie zariadení na spracovanie údajov a informácií
- vypracovať procedúry na zaistenie ochrany budov a fyzických priestorov, kde sú umiestnené informácie a zariadenia na spracovanie informácií proti neautorizovanému prístupu,

Bezpečnosť‘ zariadení znamená:

- vypracovať‘ procedúry na komplexnú ochranu zariadení pre spracovanie, ukladanie a archivovanie údajov,
- vypracoval procedúry na komplexnú ochranu prenosových trás, po ktorých sa prenášajú údaje a informácie (ochrana proti neautorizovanému fyzickému prístupu, proti ich odpočúvaniu na diaľku a pod.,
- vypracovať‘ procedúry pre záložnú dodávku elektrickej energie (UPS, záložný motorgenerátor),
- vypracovať‘ procedúry pre prípad úplného výpadku všetkých variantov záložnej dodávky elektrickej energie,
- vypracovať‘ formálne procedúry na spracovanie informácií a údajov mimo priestorov.

Technická bezpečnosť

Zabezpečuje ochranu dát, zaistenie integrity a dostupnosti pomocou vhodných technických prostriedkov, mala by odhaliť a blokovať útoky, ktoré môžu mať rozličné formy (poškodenie služby, infiltráciu, neoprávnený prístup osôb). Technická bezpečnosť zahŕňa zabezpečenie operačných systémov, serverov a jednotlivých staníc.

Programové opatrenia

Ide o ochranu informácií v PC pomocou programových bezpečnostných prostriedkov na úrovni OS a na úrovni aplikácií.

1. Riadenie prístupu do operačného systému zahŕňa:
    a. prihlasovaciu procedúru,
    b. procedúru pre stanovenie metódy identifikácie používateľov (napr. heslo, biometrické metódy, tokeny, kryptografické prostriedky, čipové karty, kombinácie),
    c. štandardný manažment zvolených metód na autorizáciu používateľa
    d. riadenie prístupu k systémovým programom a ich používania
    e. zabezpečenie neaktívnych zariadení a používateľov pred ich zneužitím (automatické odhlásenie používateľa, odpojenie zariadenia, zablokovanie úlohy alebo aplikácie, zablokovanie zariadenia a pod.).

2. Riadenie prístupu k aplikáciám zahŕňa:
    a. zabezpečenie prístupu k aplikáciám na základe individuálnych požiadaviek v súlade s definovanou politikou riadenia prístupu a s politikou prístupu k informáciám,
    b. prideľovanie prístupových oprávnení a privilégií používateľom aplikačných programových systémov v súlade s bezpečnostnou politikou,
    c. procedúry a postupy na prideľovanie a schvaľovanie prístupových práv a privilégií.

3. Výmena informácií a softvéru . Na účely ochrany pred zneužitím, stratou alebo modifikáciou informácií, softvéru a údajov vymieňaných medzi organizáciou a inou externou osobou by organizácia mala:
    a. realizovať‘ výmeny výhradne na zmluvnom základe,
    b. vypracovať‘ procedúry pre výmenu informácií a fyzických nosičov údajov
    c. vypracovať‘ procedúry a opatrenia (v oblasti hardvérovej, softvérovej, personálnej a legislatívnej) na zmierňovanie a elimináciu rizík spojených s prevádzkovaním služieb po verejných sieťach (Internet),
    d. vypracovať‘ procedúry pre zavedenie a používanie elektronických komunikačných kanálov (napr. elektronická pošta, elektronické kancelárske systémy a webová stránka),
    e. vypracovať‘ procedúry, pre zaistenie informovanosti používateľov elektronických komunikačných kanálov o ich zodpovednosti za bezpečnosť údajov, informácií a softvéru v procese ich výmeny.

4.4 Ochrana údajov

4.4.1 Počítačové infiltrácie

Počítačové infiltrácie v našich podmienkach predstavujú v oblasti osobných počítačov najčastejší a najznámejší spôsob narušenia IS. Preto ochrana pred nimi predstavuje nutnú vec pre každý informačný systém používajúci PC.

Počítačové infiltrácie tvoria veľkú skupinu programov prinášajúcich problémy užívateľom. Existuje síce veľa druhov infiltrácií, ale ich spoločnou vlastnosťou je to, že boli úmyselne vytvorené na škodlivú činnosť.

Základné typy počítačových infiltrácií

Počítačoví vírus je to program (... sekvencia kódu), ktorý sa bez vedomia používateľa počítača pripája, prepisuje alebo inak modifikuje iné programy, dokumenty, resp. systémové oblasti pevného disku a diskiet s cieľom vlastnej reprodukcie. Okrem samotnej reprodukcie môže pritom kód vírusu vykonávať rôzne grafické, zvukové a textové efekty, ale aj deštrukčnú činnosť, ako napr.: mazanie, kódovanie či inú modifikáciu súborov i sektorov pevného disku. S výnimkou možnosti vymazania Flash BIOS pamäte však v súčasnosti nie sú známe vírusy poškodzujúce hardware počítača. Niektoré vírusy podobne ako ďalej spomínané trójske kone narušujú bezpečnosť počítača, resp. údajov uložených na jeho pevnom disku zasielaním tajných PGP kľúčov, odchytených hesiel a emailových adries prostredníctvom rôznych komunikačných kanálov mimo napadnutý počítač (napr.: autorovi vírusu). Aj na pohľad neškodné vírusy však môžu spôsobiť svojou prítomnosťou problémy v súvislosti so spotrebou časti operačnej pamäti, výpočtovej kapacity procesora, ale najmä vznikom rôznych typov interferencií s inými aplikáciami, resp. aj samotným operačným systémom.

Červ (worm) je program, ktorý parazituje v jednom exemplári (... v jednej kompletnej sade súborov) na hostiteľskom počítači, pričom využíva jeho komunikačné prepojenie s ďalšími počítačmi na svoje ďalšie šírenie. Klasický červ sa teda na rozdiel od vírusu nepripája k žiadnemu hostiteľskému programu ani sa na lokálnom disku ďalej nešíri. Typickým príkladom červa je známy Happy99. Niektoré infiltrácie klasifikované ako červy sa však okrem šírenia uvedené komunikačné kanály šíria aj po lokálnych a sieťových diskoch (LoveLetter), čím sa svojimi vlastnosťami približujú k definícii vírusu využívajúceho na svoje šírenie okrem klasickej technológie šírenia (... prepisovanie iných súborov, resp. šírenie ako satelitný súbor) aj komunikačné kanály. Obdobnú kombináciu rôznych algoritmov šírenia možno pozorovať aj u niektorých makrovírusov (Melissa). Niektoré červy obsahujú tiež niektoré znaky trójskych koňov (Pretty Park), takže v tomto zmysle možno skonštatovať, že absolútne presná klasifikácia jednotlivých druhov infiltrácií nie je možná.

Trójsky kôň je program, ktorý navonok navodzuje dojem užitočnosti. V dokumentácii programu sľubovanú činnosť však buď vôbec nevykonáva alebo ju aj vykonáva, ale na pozadí realizuje nepozorovane nejaký druh deštrukcie (... vymazáva súbory, formátuje pevný disk, skrytou komunikáciou cez Internet narušuje súkromie používateľa apod.). Trójsky kôň je buď naprogramovaný ako pôvodná aplikácia alebo je vytvorený z už existujúceho programu jeho spojením s deštrukčným kódom (... ktorý sa vykonáva pred samotným programom), pričom

takýto program sa potom od pôvodného okrem dĺžky navonok ničím neodlišuje (... vzhľad prostredia aj vykonávaná akcia je zhodná, dokumentácia programu je pôvodná), čo v čase rýchleho striedania verzií programov nie je príliš nápadné. V poslednej dobe sú častými aj trójske kone, ktoré sú vlastne inštalačným súborom samotného programu, ktorý sa po svojej inštalácii spúšťa pri štarte operačného systému MS Windows a skryte vykonáva nejaký typ deštrukčnej akcie. Niektoré charakteristiky trójskych koňov v tomto zmysle spĺňajú aj niektorí reklamní klienti (tzv. spyware) aplikovaní za účelom sťahovania reklám, resp. zasielania rôznych formulárov charakterizujúcich používateľa, ktoré sú dnes bežne pridávané k skúšobným verziám niektorých programov - pokiaľ si ich používateľ zaregistruje, reklamný klient sa deaktivuje.

Obrázok č. 4: Infikácia počítača trójskym koňom (trojanom)
Zdroj: Vlastné zdroje

Od počítačového vírusu, resp. červa sa pritom trójsky kôň líši tým, že kód programu sa ďalej nereplikuje. Pokiaľ je príslušná deštrukčná akcia viazaná na nejaký dátum alebo inú podmienku, hovorí sa tiež o tzv. logickej bombe. Historicky prvým počítačovým trójskym koňom bol AIDS, šírený v roku 1989. Špeciálnu podskupinu trójskych koňov tvoria nosiče vírusov, tzv. droppery - programy, ktorých deštrukčná akcia spočíva vo vypúšťaní klasických počítačových vírusov, pričom samotný dropper nie je možné identifikovať vzorkou vypúšťaného vírusu (... ani keď samotný vypúšťaný vírus je známy).

V poslednej dobe patria medzi najčastejšie sa vyskytujúce trójske kone tzv. "zadné vrátka" – backdoor

Zadné vrátka - ide o škodlivý kód, ktorému neboli dané do vienka schopnosti šírenia sa. Jeho hlavnou úlohou je otvoriť na infikovanom počítači príslovečné "zadné vrátka", ktorými neskôr môže útočník nepozorovane vkĺznuť a robiť si, čo sa mu zapáči. Zadné vrátka v "čistokrvnej" forme sa vyskytujú len veľmi zriedka. Väčšinou sú súčasťou napr. e-mailového červa. Umožňuje zasielanie prístupových hesiel, záznamov o aktivitách počítača alebo zvolených súborov mimo počítač, resp. umožňuje jeho úplné diaľkové ovládnutie (... spúšťanie aplikácií, manipuláciu so súbormi apod.).

Osobitné typy infiltrácií

Adware - (advertising-supported softvér) je softvér, ktorý zobrazuje reklamu na počítači po svojej inštalácii alebo pri používaní tohto softvéru. Táto reklama slúži na pokrytie nákladov na tvorbu programu, a vďaka nim je možné, aby bol program dostupný zadarmo. Vo svojej podstate je teda koncept adware veľmi užitočná vec.

Adware je často zamieňaný so spyware, ale je pravda, že množstvo adware programov neobsahuje reklamy iba na podporu autorov, ale i sleduje činnosť používateľa bez jeho vedomia. V takomto prípade už ide o spyware. Je už na samotnom používateľovi či sa rozhodne používať softvér podporovaný reklamou alebo si zakúpi plnú verziu bez reklám (takúto možnosť ponúka väčšina autorov ad-supported softvér) resp. prejde ku konkurencii.

Spyware (špehovací softvér) je počítačový program, ktorý bez vedomia užívateľa získava z užívateľovho počítača rôzne citlivé dáta ako sú napr. heslá, rodné čísla, čísla kreditných kariet a iné. Tieto dáta sa potom pokúša odoslať výrobcovi spyware, ktorý ich môže zneužiť alebo predať ďalej.

Na "špehovanie" používa spyware viacero techník ako sú napr. zaznamenávanie a analýza všetkého čo zadávate klávesnicou, sledovanie adries, ktoré zadávate do Vášho Internetového prehliadača, ako aj prehľadávanie dokumentov na hard-disku počítača.
Prejavom, že Váš počítač je infikovaný spyware môže byť značné spomalenie, prípadne aj časté padanie systému. Niektoré spyware okrem samotného "špehovania" zobrazujú okná s reklamou, a to aj vtedy ak práve nesurfujete na Internete.

Vo všeobecnosti sa pod pojmom spyware dá zhrnúť všetok softvér, ktorý bol na počítač nainštalovaný bez užívateľovho vedomia resp. užívateľ ho dobrovoľne nainštaloval, ale program obsahuje skryté funkcie, ktoré závažným spôsobom narúšajú súkromie užívateľa.

Dialer je počítačový program, ktorý vytvára spojenie s Internetom alebo inou počítačovou sieťou cez analógové telefónne číslo. Zvyčajne je to číslo začínajúce s 0-800 (na Slovensku) alebo zahraničné telefónne číslo. Obyčajne dialér pracuje bez vedomia užívateľa. Dialéri, ktorí sa javia najčastejšie na pornografických stránkach sú škodliví len pre užívateľov modemu.

Dialéri sú nevyhnutne pripojení na Internet (prinajmenšom pre neširokopásmové spojenia), ale niektorí z nich sú určení na pripojenie na prémiové- rýchlostné čísla. Poskytovatelia takýchto dialérov často pátrajú po bezpečnom defekte na užívateľovom počítači a používajú ich k zmene počítača vytočenia cez ich číslo, privlastneniu dodatočných peňazí pre seba.

Niektorí dialéri taktiež informujú používateľov čo robia, s prísľubom špeciálneho obsahu, prístupným iba cez špeciálne číslo. Príklady takéhoto obsahu zahrňujú softvér pre stiahnutie, MP3 (obyčajne nelegálny), pornografiu a poprípade aspoň jednu webovú stránku ilegálnych hackerových materiálov takých ako vírusy.

V tejto dobe, termín „dialér“ často odkazuje konkrétne na dialérov s pripojením sa bez úplného vedomia užívateľa o nákladoch, s tvorcom dialéra, ktorý má v úmysle dopustiť sa podvodu.

Hoax (fáma) je poplašná správa posielaná e-mailom, ktorá na svoje šírenie využíva dôverčivosť ľudí. Šíri sa výhradne ľudským pričinením a preto jediným spôsobom, ako sa pred takouto správou dá brániť, je opatrnosť. Fáma sa vo väčšine prípadov odvoláva na dôveryhodnú firmu ("Microsoft varuje...", "CNN oznámila", a pod.), často informuje o katastrofálnych dôsledkoch, napr. epidémie počítačového vírusu. Spoločným menovateľom týchto správ je výzva na okamžité postúpenie ďalšiemu užívateľovi. Týmto spôsobom sa fáma šíri k ďalším užívateľom internetu.

Phishing (password fishing) označuje činnosť, pri ktorej sa podvodník snaží vylákať od používateľov rôzne citlivé dáta, napr. prístupové údaje k bankovému účtu. Podvodník väčšinou vytvorí webstránku, ktorá vyzerá ako kópia už existujúcej dôveryhodnej stránky. Meno a heslo zadané do phishingovej stránky, sa odošle podvodníkovi, ktorý ho môže zneužiť.

Phishing môže prebiehať i tak, že sa rozposielajú e-maily, ktoré lákajú používateľov napríklad na zmenu hesla alebo jeho obnovenie. Podvodníci môžu na vylákanie citlivých

údajov využiť aj tzv. instant messaging programy ako sú ICQ alebo MSN a dokonca aj telefón.

Pharming je oveľa nebezpečnejší ako phishing. Ide o zákernený spôsob, ktorým môže hacker pripraviť o úspory klienta, ktorý využíva internet banking . Táto metóda spočíva v presmerovaní názvu www stránky na inú adresu. Každej mennej adrese napríklad ib.vub.sk prislúcha číselná adresa napríklad 215.5.214.144. Presmerovanie takejto adresy môže hacker uskutočniť buď napadnutím servera DNS alebo zmenou súboru lmhost priamo vo Vašom počítači. Ak zadáte mennú adresu do Vášho prehliadača, miesto stránky banky sa zobrazí jej dokonalá napodobenina. Vy teda ani nezbadáte, že ste na inej stránke. Po zadaní údajov, ich získa neoprávnená osoba, ktorá takúto falošnú stránku vytvorila.

4.4.2 Možnosti zmiernenia hrozieb a útokov

Každá organizácia by mala dbať na:

1. **Používanie silných hesiel v systémoch**

Už po zapnutí počítača by mal byť užívateľ vyzvaný o zadanie vstupného hesla. Táto ochrana plní úplne rovnakú úlohu ako napríklad kľúč od bytu. Bráni cudzím ľuďom zapínať náš počítač a pristupovať k našim dátam. Ďalšie heslo by malo byť od užívateľa žiadané pri štarte operačného systému. Je nevyhnutné chrániť silnými heslami každý dôležitý program či systém bežiaci na pracovnej stanici.

Silné heslo

- musí obsahovať minimálne 8 znakov,
- obsahuje kombináciu malých a veľkých písmen, číslic a iných symbolov,
- pravidelne sa mení a vždy sa výrazne líši od predošlých hesiel,
- neobsahuje meno užívateľa, užívateľské meno ani žiadne iné slová alebo mená,
- nie je zdieľané s kýmkoľvek iným,
- malo by byť zložité,
- nemalo by byť nikde zapísané ani uložené v pôvodnej podobe,
- malo by byť vyžadované pri všetkých užívateľských účtoch.

Obzvlášť veľkou chybou je, ak má užívateľ nadstavené rovnaké heslo do všetkých programov či aplikácií. Operačný systém by mal byť chránený odlišným heslom ako napríklad jednotlivé programy, či účty na webových stránkach.

2. Pravidelné aktualizácie

Užívatelia by mali pravidelne kontrolovať zoznam vydaných záplat, a v prípade potreby ich aj nainštalovať. V opačnom prípade nechávajú voľnú cestu tvorcom škodlivých programov zneužívať objavené bezpečnostné nedostatky. Moderné operačné systémy umožňujú nadstavenie automatickej kontroly dostupných aktualizácií a ich inštaláciu takmer bez vedomia užívateľa. Pokiaľ systém tieto možnosti nemá, pravidelnosť kontroly aktualizácií závisí na tom, ako často je počítač pripájaný k Internetu. Práve tam totiž hrozí najväčšie riziko nechceného stiahnutia škodlivého programu, ktorý nejakú chybu využíva. Všeobecne by, ale užívateľ používajúci Internet mal vykonávať aktualizácie priemerne raz za týždeň. Medzi objavením chyby a vydaním záplaty ubehne vždy niekoľko dní, málokedy sa ale stane, že by niekto vytvoril program zneužívajúci chybu skôr ako niekoľko týždňov po jej objavení.

3. Pravidelné zálohovanie údajov

„Cenu svojich dát spoznáme až vtedy , keď o ne prídeme“

Zálohovanie je proces, pri ktorom sa v danom časovom okamihu vytvorí jedna alebo viac kópií požadovaných informácií na záložných dátových nosičoch. Zálohovanie slúži predovšetkým na obnovu IS po jeho výpadku. Zálohovanie obsahuje nielen dáta ale aj ďalšie informácie potrebné k tomu, aby bolo možné obnoviť celé informačné prostredie pri totálnom zrútení IS. Kópie sa po určitom období premazávajú.

Zálohovať by sa malo všetko, čo je v systéme jedinečné, teda všetky užívateľské adresáre, systémové databázy a tie dôležitejšie systémové adresáre, ktoré sú kritické alebo ktoré užívateľ mohol modifikovať. Niektorí správcovia zálohujú úplne všetko, pretože obnova kompaktného systému je ďaleko jednoduchšia ako obnova po častiach.

Existuje viacej stratégii zálohovania:

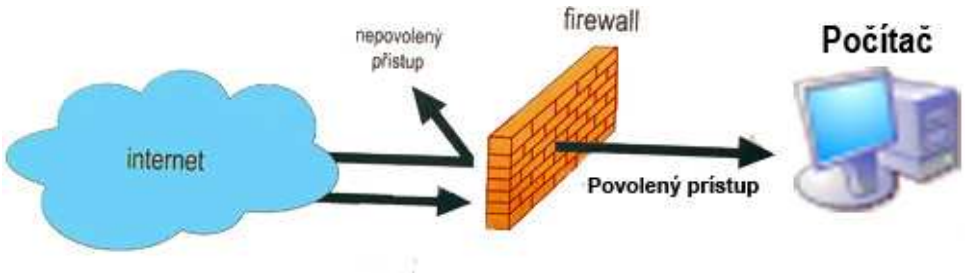
a) úplná záloha -ukladajú sa kópie všetkých dát,
b) rozdielová (diferenciálna) záloha – ukladajú sa kópie len tých súborov, ktoré sa zmenili od poslednej úplnej záložnej kópie,
c) prírastková (inkrementálna) záloha – ukladajú sa kópie len tých súborov, ktoré sa zmenili od posledného zálohovania (či už úplného alebo prírastkového).

Pre obnovenie dát sa potom musí urobiť kópia z úplnej zálohy a poslednej diferenciálnej zálohy alebo úplnej zálohy a všetkých prírastkových záloh od poslednej úplnej zálohy.

Často užívatelia zálohujú svoj systém raz do týždňa úplnou zálohou a každý deň rozdielovou alebo prírastkovou. Zálohy môžu byť ukladané na pevných diskoch (HDD), médiách CD alebo DVD, alebo špeciálnych magnetických páskach. Niektoré spoločnosti vykonávajú aj polročné či ročné zálohy, ktoré uchovávajú nastálo, nakoľko absencia nejakého dôležitého súboru sa môže často prejaviť až po týždňoch či mesiacoch. Nakoľko zálohy sú tiež kópiou citlivých dát organizácie, mali by byť ukladané na bezpečné miesto, chránené pred odcudzením alebo znehodnotením.

4. Používanie hardvérového alebo softvérového (osobného) firewallu

Nastavenie a používanie firewallu predstavuje jeden zo základných stupňov ochrany. V dobe bežného pripojenia počítača k internetu je aktívny firewall už nevyhnutnosťou.
Firewall je nástroj, ktorý oddeľuje chránenú časť siete od nechránenej časti a ponúka základné zabezpečenie systému pri pripojení do internetu.



Obrázok č. 5: Princíp práce firewallu
Zdroj: Král, M.: Bezpečnost domáciho počítače prakticky a názorně

Umiestňuje sa medzi internú sieť organizácie a externú sieť a predstavuje jednoduchý spôsob riadenia objemu a typu komunikácie, ktorá medzi nimi prebieha. Použitím firewallu sa obmedzuje možné poškodenie siete, útočník sa bude môcť dostať k jednému počítaču, neohrozí však iné. Firewally sa dajú použiť na:

- zablokovanie prístupu na určité miesta internetu, alebo sa dajú použiť k zabráneniu používania niektorých serverov alebo služieb určitým užívateľom,
- sledovanie komunikácie medzi internou sieťou a externými sieťami,
- odpočúvanie a zaznamenávanie každej komunikácie medzi internou sieťou a okolím,
- niektoré firewally umožňujú nadstavenia automatického šifrovania paketov.

Poznáme niekoľko druhov firewallov:

a) Aplikačný proxy firewall - ide o filtrovanie na aplikačnej vrstve referenčného modelu OSI, t.j. aplikačný proxy server dokáže presne analyzovať celú sieťovú

prevádzku a význam paketov na najvyššej vrstve. Tak môže chrániť napríklad pred vírusmi alebo rôznym škodlivým obsahom a umožňovať prístup na základe autentifikácie používateľa.

b) **Paketový firewall -** umožňuje sledovať sieťovú prevádzku po tretiu (štvrtú) vrstvu modelu OSI (t.j. IP adresy a porty). Je oveľa rýchlejší ako proxy, ale jeho správa je komplikovanejšia a nemá toľko možností, ako aplikačné proxy servery.

c) **Stavový paketový firewall –** je špeciálnym typom paketového firewallu. Dokáže dávať do súvisu prechádzajúce pakety a tak si uchováva stav spojenia.

Osobitnú úlohu v počítačovej bezpečnosti zohrávajú softvérové firewally, ktoré sú na rozdiel od „veľkého“ firewallu inštalované priamo v počítači. Celú dobu kedy je počítač zapnutý bežia na pozadí a monitorujú prevádzku systému. Dokážu odhaliť nielen pokusy o útoky z Internetu, zastavia aj programy pokúšajúce sa nadviazať komunikáciu priamo z počítača užívateľa. Nadstavenia osobných firewallov sú veľmi zložité a za každých podmienok by ich mali vykonávať skúsení odborníci.

5. Používanie kvalitného antivírového programu a jeho pravidelné aktualizovanie

Antivírusový program, je program ktorý slúži na lokalizáciu, následné odstránenie a maximálne napravenie škôd spôsobených vírusom. Na vyhľadanie vírusu využívajú programy rôzne metódy:

- **Vyhľadávanie** – antivírusový program má v sebe naprogramované všetky významné znaky víru (veľmi podrobne) a ak nájde v počítači nejaký program s odpovedajúcimi charakteristikami, označí ho ako vírus.
- **Skenovanie -** antivírusový program porovnáva obsah súboru so svojou internou databázou. Pokiaľ súbor obsahuje reťazec, ktorý je zhodný s reťazcom v tejto internej databáze, je vyhodnotený ako zavírovaný. Metóda je veľmi spoľahlivá, ale je potrebná veľmi častá aktualizácia.
- **Heuristická analýza** – ide o rozbor kódu víru, kedy antivírusový program skúma iný program krok po kroku a pokiaľ nájde nejakú podozrivú inštrukciu, označí ho ako vírus. Nevýhodou je možnosť veľkého množstva falošných poplachov, ale táto metóda dokáže nájsť aj víry zatiaľ neznáme. Väčšinou sa testujú súbory s príponou .com, .exe, .dat, .dll.

- **Kontrola integrity** - znamená vlastne porovnanie stavu pred možnou infiltráciou so stavom po tejto infiltrácii. Vírus sa v systéme musí nejako prejaviť (napr. tak, že sa zväčší veľkosť súboru). Táto metóda zisťuje iba možnú nákazu, ale nevie ju odstrániť.
- **Rezidentné sledovanie** – znamená, že antivírusový program sa po štartu počítača zapne a beží na pozadí počítača. Neustále tak počítač sleduje a upozorňuje na podozrivé akcie, ktoré v počítači môžu prebiehať.

Pri súčasných antivírusových systémoch je najdôležitejšie, aby dokázali nájsť a odstrániť čo najviac vírov či iných hrozieb, signalizovali čo najmenej falošných poplachov, aby antivírová spoločnosť reagovala rýchlo na nové bezpečnostné hrozby a poskytovala časté aktualizácie antivírového programu. Antivírové programy môžeme deliť na:

1) **Jednoúčelové antivírusy** - zameriavajú na detekciu, príp. aj dezinfekciu jedného konkrétneho vírusu. Nedajú sa použiť ako plnohodnotná antivírusová ochrana.
2) **On-demand skenery –** vyhľadáva vírusy až po zadaní požiadavky užívateľom. Uplatňuje sa predovšetkým pri dezinfekcii počítačov, keď napr. operačný systém MS Windows nie je schopný prevádzky.
3) **Antivírusové systémy -** Najčastejšia forma antivírusových programov. Skladá sa z častí, ktoré sledujú všetky najpodstatnejšie vstupné miesta, ktorými by sa prípadná infiltrácia mohla do počítačového systému dostať. Ich súčasťou v dnešnej dobe býva aj aktualizácia prostredníctvom internetu. Ide o komplexné antivírové riešenie v niektorých prípadoch doplnené aj o osobný firewall.

6. Používanie legálne zakúpeného softvéru

Pod pojmom legálny softvér rozumieme softvér ktorý bol zakúpený legálne.
Problematika nelegálneho softvéru sa v súčasnosti na Slovensku dotýka takmer každého druhého počítača. Vo svete sa týmto skutočnostiam venuje veľká pozornosť. Porovnanie krajín s nelegálnym softvérom je zobrazený v prílohe 1.

4.5 Bezpečnosť IS v podniku PRASTAV s. r. o.

4.5.1 Charakteristika podniku

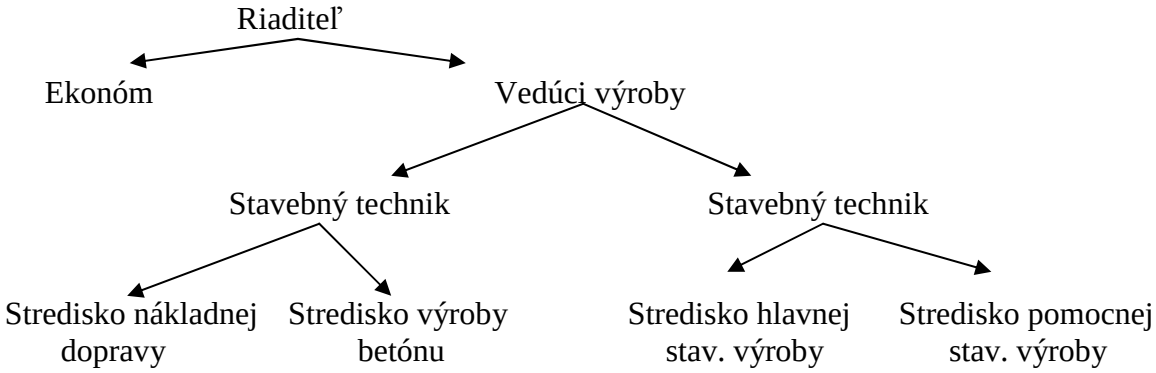
Spoločnosť PRASTAV sa nachádza vo Veľkej Lomnici v okrese Kežmarok. Firma PRASTAV bola zapísaná do obchodného registra vo auguste 1993 ako spoločnosť s ručením obmedzením. Spoločnosť bola založená Ing. Štefanom Precákom.

Medzi hlavné činnosti spoločnosti patria:

- budovanie bytových a občianskych stavieb, priemyselných stavieb, inžinierskych stavieb, jednoduchých stavieb a poddodávok,
- asanácie, zemné a demolačné práce,
- adaptácie, rekonštrukcie, modernizácie stavieb,
- prípravné stavebné práce,
- inžinierska činnosť v stavebníctve,
- kúpa a predaj stavebného tovaru,
- vodoinštalatérstvo,
- kúrenárske práce - montáž rozvodov kúrenia,
- stolárstvo,
- elektroinštalatérstvo.

Firma Prastav si počas svojho pôsobenia od roku 1993 neustále rozširovala ponuku poskytovaných služieb a tým získala stály okruh zákazníkov, ktorí sú prevažne z okresov Kežmarok a Poprad, avšak vďaka dobrému menu má zákazníkov nielen z regiónu Vysokých Tatier, ale aj z celého Slovenska.

Organizačná štruktúra podniku



Služby ponúkané touto firmou súvisia hlavne s budovaním bytových, občianskych, priemyselných či iných stavieb, rekonštrukciou a modernizáciou stavieb, inžinierskou činnosťou v stavebníctve, vodoinštalatérskom a výrobou a predajom betónu vrátane dopravy na stavenisko a s dopravnými službami. Služby neprechádzajú cez sprostredkovateľov, ale priamo k zákazníkovi.

Spoločnosť Prastav má sídlo vo Veľkej Lomnici, preto svoje služby hlavne vykonáva v okresoch Poprad a Kežmarok, v menšej miere sú to aj iné okresy Slovenka.

Pri cenovej tvorbe sa firma orientuje na ceny konkurencie, keďže firma nezaujíma monopolné postavenie na miestnom trhu. Spoločnosť Prastav sa snaží cenovo konkurovať hlavne firmám ponúkajúcim služby podobného charakteru. Priame poskytovanie služieb medzi firmou a zákazníkom bez sprostredkovateľov sa zvyčajne viaže na nižšie ceny.

Na trhu je veľký počet firiem obchodujúcich práve v tejto oblasti, preto získať dominantné a prioritné miesto je veľmi náročné. Spoločnosť Prastav predstavuje v súčasnosti malý podiel na trhu, no firma sa neustále snaží o dosahovanie cieľov z marketingového plánu, udržanie si konkurencieschopnosti a samotného rozvoja v danom segmente. Firma neustále meria a hodnotí výsledky svojej ekonomickej činnosti, pomáhajú jej v tom činitele ako: ekonomická situácia firmy, trhový podiel a jeho vývoj, tempo rastu trhu, výška nákladov a výnosov a iné.

Okrem firmy Prastav má sídlo vo Veľkej Lomnici aj firma Ekoprim, ktorá je najbližšou konkurenciou spomínanej spoločnosti. Na rozdiel od firmy Prastav firma Ekoprim sa zaoberá len líniovými stavbami, kým firma Prastav celkovým stavebníctvom. Na našom trhu je veľký počet stavebných firiem, ktoré zvádzajú silný konkurenčný boj o zákazníka, a to najmä v podobe zvýšeného propagačného úsilia a podpory predaja - reklama, letáky, predajné akcie, rabaty...

SWOT analýza spoločnosti PRASTAV s.r.o. **Tabuľka č.1**

SILNÉ STRÁNKY PODNIKU	SLABÉ STRÁNKY PODNIKU
- image firmy - dobré meno firmy - relatívne nižšie ceny v porovnaní s konkurenciou - verní a stáli zákazníci - mobilnosť vlastnými prostriedkami - kvalifikovaní pracovníci	- úroveň informačného systému - nízka reklama a podpora predaja - Pomerne zastaralé IKT
PRÍLEŽITOSTI PODNIKU	**HROZBY PODNIKU**
- rast podielu vyšších príjmových skupín - rast bytovej výstavby - rast priemernej mzdy - rast zamestnanosti	- nová konkurencia - poškodenie majetku živelnými pohromami - vstup nových podnikateľských subjektov do odvetvia - politická situácia - rast cien vstupov

4.5.2 Súčasný stav informačných a komunikačných technológií

Spoločnosť PRASTAV s.r.o. využíva informačné a komunikačné technológie hlavne pre fakturáciu, mzdové účtovníctvo a rozpočty. V čase vzniku firma začínala s 2 osobnými počítačmi Intel Pentium I 200 MHZ, z ktorých sa dodnes zachoval už len jeden kus. Tento počítač sa v súčasnosti nevyužíva. V súčasnosti sa vo firme nachádzajú 4 osobné počítače, z toho 1 počítač pre mzdové účtovníctvo, 1 počítač pre administratívne účely (fakturácie, rozpočty). Firma nevlastní server. Spoločnosť vlastní aj 2 notebooky, ktoré slúžia výhradne pre potreby riadiacich pracovníkov.

Typy počítačov v podniku **Tabuľka č. 2**

P. Č	PROCESOR	RAM	HDD	MECHANIKY	O.S.	Monitor
1.	AMD Sempron 3100	512MB	60GB	DVD-ROM, FDD	Win XP	17" LCD
2.	Intel Pentium II	32MB	2GB	CD-ROM 16x, FDD	Win 98	14" CRT
3.	Intel Pentium III 600	512MB	60G	DVD-ROM, FDD	Win XP	17" LCD
4.	Intel Pentium I 200	32MB	1,2GB	CD-ROM 6x, FDD	Win 95	14" CRT

Spoločnosť vlastní 2 farebné tlačiarne HP DeskJet 640C. Sú to tlačiarne z radu atramentových. Na dnešnú dobu sú tieto atramentové tlačiarne veľmi zastarale. Spoločnosť ich používa už 8 rokov. Medzi ďalšie informačné technológie ktoré firma využíva sú skener HP SkanJet G2410 a fax.

Na prvom a treťom počítači z tabuľky číslo 2 je nainštalovaný operačný systém Microsoft Windows XP. Na ostatných počítačoch je nainštalovaný operačný systém Windows 98 a Windows 95. Na notebookoch riadiacich pracovníkov je nainštalovaný OS Microsoft Windows XP na ktorých je nainštalovaný aj Service pack 2. Operačný systém MS Windows 95 a 98 neponúkajú ani na dnešnú dobu „základné“ bezpečnostné opatrenia.

Spoločnosť na spracúvanie údajov využíva kancelársky balík Microsoft Office 2003, ktorý je nainštalovaný na všetkých osobných počítačoch. Z kancelárskeho balíka využívajú hlavne produkty Microsoft Word, Microsoft Excel a Microsoft PowerPoint.

Microsoft Word slúži predovšetkým na písanie textov, môžeme v ňom však vytvoriť aj dokumenty s obrázkami, tabuľkami či hypertextovými odkazmi, dokonca priamo vo Worde si môžeme vytvoriť svoju webovú stránku. Microsoft Word uľahčuje používateľom vytváranie dokumentov.

Microsoft Excel sa používa na evidenciu , analýzu a na podávanie kvantitatívnych informácií napr.: vytváranie rozpočtov súpis výrobkov...

Microsoft PowerPoint slúži na tvorenie multimediálnych prezentácií.

Na mzdové účtovníctvo spoločnosť využíva program DATALOCK Wéčko od spoločnosti DATALOCK a. s.. Wéčko predstavuje komplexný ekonomický informačný systém so štandardnými nárokmi na rýchlosť získania informácií. Produkt pokrýva všetky základné podnikové procesy. Rieši oblasť financií a ekonomiky, logistických procesov dodávok a zásobovania, výkazníctva, dopravy, personalistiky a miezd.

Na fakturácie a rozpočty používa program OMEGA od spoločnosti KROS a. s..

4.5.3 Bezpečnosť informačných a komunikačných technológií v podniku

Fyzická bezpečnosť

Spoločnosť sídli v jednopodlažnej budove. Priestory sa nachádzajú na rozlohe 100m$^{2.}$ Približne pred 4 rokmi sa do spoločnosti vlámali zlodeji. Do budovy sa dostali cez okno, ktoré bolo nezabezpečené proti vlámaniu. V tom čase boli v priestoroch kancelárii uložené dôležité materiály týkajúce sa chodu a činnosti firmy. Nanešťastie v ten deň, ako došlo k vlámaniu ekonómka firmy odniesla do banky všetku finančnú hotovosť. Zlodej spoločnosti nespôsobil žiadnu vážnejšiu škodu. Po tomto incidente pribudli na oknách hrubé kovové mreže a pôvodné vstupné dvere boli vymenené za bezpečnostné. Vonkajšie priestory objektu o rozlohe 250 m^2 sú taktiež chránené strážnym psom. V budove sa nachádzajú 3 kancelárie, z toho dve pre administratívu a 1 pre riadiacich pracovníkov. V kanceláriách pre administratívu sa nachádzajú všetky počítače spoločnosti.

Vo vnútri celého podniku však nie je nainštalovaný ani kamerový, ani protipožiarny systém, dokonca chýba aj systém detekcie pohybu či senzory na oknách. Proti požiaru je spoločnosť vybavená len 4 hasiacimi prístrojmi, ktoré sa nachádzajú v každej miestnosti, ale ich funkčnosť nie je pravidelne kontrolovaná.

Technická a programová bezpečnosť

Do počítačovej siete sú pripojené iba 2 počítače. Pripojenie cez telefónnu linku T-Com ADSL poskytuje rýchlosť downloadu až 1,5 Mbit/s a upload až 256 Kbit/s, čo je rýchlosť prekračujúca potreby podniku.

Spoločnosť PRASTAV s. r. o. na zabezpečenie počítačov v podniku využíva antivírusový program Microsoft OneCare. Tento antivírusový program patrí do kategórie antivírusov, ktorý nedosahujú dobré výsledky v porovnávaných testoch. Výsledky antivírusových programov sú uvedené v prílohe 2.

Na ochranu sieťovej komunikácie a blokovanie nepovolených prístupov firma využíva iba firewall systému Windows. Tento firewall má jednu chybu, ktorá sa týka nesprávneho zobrazovania otvorených portov (TCP aj UDP) v systéme. Reálne sa táto chyba prejavuje tým, že v nastavení firewallu sa nezobrazia všetky porty ktoré sú otvorené. Tým pádom si môžete myslieť, že je všetko v poriadku, ale skutočnosť môže byť diametrálne odlišná.

Spoločnosť zálohuje svoje údaje iba raz mesačne a to na DVD média. Tieto média má spoločnosť uložené na poličke vedľa fotiek rodinných príslušníkov jedného zo zamestnancov, ku ktorým má prístup každý zo zamestnancov.

Personálna bezpečnosť

Spoločnosť PRASTAV s. r. o. doposiaľ nezaznamenala bezpečnostné incidenty zavinené niektorým z pracovníkov. Preto v personálnej bezpečnosti zatiaľ nevykonala žiadne opatrenia, neboli vydané žiadne vnútorné smernice a počítače v podstate nie sú chránené pred útokom „zvnútra“. Medzi pracovníkmi spoločnosti prevláda priateľská atmosféra, navodzujúca pocit bezpečia. Vzhľadom na časté odchody zamestnancov a prijímania nových, ale môže v tomto smere hroziť vysoké riziko (napr. pri odchode nespokojného pracovníka).

Všetky stolové počítače sú chránené tým istým prístupovým heslom, ktoré je ľahko zapamätateľné, dokonca pre skúsenejšieho hackera nie náročným na odhalenie. Notebooky riadiacich pracovníkov sú chránené heslom pri vstupe do systému. Heslá sa však nemenia a medzi jednotlivými pracovníkmi organizácie nie sú žiadnym tajomstvom. Na pripájanie do siete Internet je zabudovaný prehliadač Internet Explorer 6.0, ktorý využívajú všetci zamestnanci spoločnosti.

Bezpečnosť v spoločnosti PRASTAV s.r.o. môžeme charakterizovať ako nedostačujúcu priam až zarážajúco podpriemernú. O IKT sa stará jeden zo zamestnancov, ktorý nemá dostatočné vzdelanie ani skúsenosti v oblasti informatiky, a vzhľadom na neustále pracovné vyťaženie v iných oblastiach ani dostatok voľného času na zvyšovanie bezpečnosti podniku.

4.5.4 Návrh novej koncepcie bezpečnosti podniku

Počas analýzy príjmov a výdavkov bolo zistené, že spoločnosť so svojimi peňažnými zdrojmi nakladá efektívne. Nenašli sme neefektívne či relatívne zbytočné investície, odstránením ktorých by spoločnosť v budúcnosti mohla získať dostatočné finančné zdroje pre zvýšenie bezpečnosti v podniku. Riadiaci pracovníci si dokonca už dlhšie uvedomujú zlú situáciu bezpečnosti IKT aj jej celkový nepriaznivý stav. Navrhované koncepcie bezpečnosti podniku budú zamerané na minimalizáciu nákladov pri získaní čo najvyššieho efektu.

V oblasti **fyzickej bezpečnosti** by mali byť priestory chránené minimálne detektormi pohybu.

Technická a programová bezpečnosť tvorí kameň úrazu celkovej počítačovej bezpečnosti spoločnosti.

Spoločnosť by mala zakúpiť pomerne lacný antivírusový program NOD 32 od slovenskej spoločnosti ESET. NOD32 Antivírus je jeden z najkvalitnejších antivírusov, svedčí o tom aj fakt, že už niekoľkokrát vyhral prestížnu cenu "100% Virus Bulletin". Program funguje na výkonnom jadre "ThreatSense". Program disponuje veľmi výkonným rezidentným štítom s názvom AMON, ktorý prehliada takmer všetko čo prichádza do kontaktu s počítačom. ESET Smart Security obsahuje antivírus, antispyware, personal firewall a filter nevyžiadanej pošty. Antivírus dokáže pracovať aj s archívmi, elektronickou poštou a dáva pozor aj na internetový obsah. Pri kúpe licencie na viac počítačov (multilicencie) spoločnosť ponúka výhodné ceny.

Zároveň by mal byť nainštalovaný na všetky počítače s operačným systémom Microsoft Windows XP Service pack 2, ktorý „zapláta“ bezpečnostné chyby systému, poskytne prvotný softvérový firewall, a v kombinácii s antivírusom NOD 32 a poskytne relatívne bezpečnú prevádzku počítačov v sieti a bezpečnejšie pripájanie sa k sieti Internet.

Ako prídavný bezpečnostný softvér by mal byť nainštalovaný Kerio Personal firewall, ktorý je k dispozícii zadarmo. Prvých 30 dní po inštalácii poskytuje plnohodnotnú ochranu počítačov, po uplynutí skúšobnej doby zablokuje niektoré (menej dôležité) služby, avšak naďalej monitoruje systém a výrazne pomáha k jeho zabezpečeniu.

Proti spywarom a adwarom by sa spoločnosť mala chrániť používaním programu Spyware Terminátor, ktorý je voľne šíriteľný teda freeware. Mimo toho že tento škodlivý softvér odstraňuje podáva informácie aj o jeho činnosti. Program disponuje systémom stálej real-time ochrany, a taktiež umožňuje pred odstraňovaním spyware zálohovať momentálny stav. Týmto softvérom sa odporúča preskenovať celý pevný disk minimálne raz týždenne a vyčistiť ho od škodlivých kódov.

Spoločnosť by mala obzvlášť dbať na zvýšenie povedomia zamestnancov ohľadom užívateľských hesiel. Všetky heslá v spoločnosti by mali byť zmenené a vytvorené pomocou pravidiel budovania silných hesiel. Heslo v organizácii by malo byť predmetom tajomstva každého pracovníka, v žiadnom prípade by nemalo byť zverejnené ostatným. Heslo by malo byť od užívateľa žiadané nielen pri prihlasovaní do systému, ale taktiež pri dlhšej nečinnosti

(keď naskočí šetrič obrazovky). Ten zamedzí ostatným pracovníkom narábať s daným počítačom, ak je jeho užívateľ dlhšie neprítomný.

Každý zo zamestnancov spoločnosti, má užívateľské práva ako administrátor.

V spoločnosti k účtu administrátor by mal mať prístup jeden zodpovedný zamestnanec, ktorý by zamestnancom zredukoval práva o samovoľné inštalovanie či odinštalovanie rôznych programov, ako aj práva meniť nastavenia systému.

Účet administrátora by mal byť premenovaný nenápadným klamlivým menom, nakoľko účty s názvami Administrátor a podobnými priťahujú najvyššiu pozornosť profesionálov snažiacich sa preniknúť do systému. Sám správca by počas bežnej práce nikdy nemal používať administrátorský účet, ale taktiež bežný užívateľský účet s obmedzenými právami.

Správca môže nadstaviť v systéme MS WINDOWS XP pomocou miestnych bezpečnostných nadstavení rôzne kritériá ako napr.:

- minimálna dĺžka hesla,
- maximálna doba veku hesla,
- minimálna doba veku hesla,
- sledovania histórie hesiel,
- politiku auditu,
- politiku užívateľských skupín,
- politiku užívateľských práv.

Užívatelia na prehliadanie webových stránok by mali používať prehliadač Mozilla Firefox namiesto prehliadača Microsoft Internet Explorer. Mozilla Firefox je mnohokrát ocenený prehliadač novej generácie. Tento prehliadač je zadarmo. Vďaka Firefoxu môžu užívatelia surfovať rýchlejšie, bezpečnejšie a efektívnejšie, než s prehliadačom Microsoft Internet Explorer. O tom, že Mozilla ako prehliadač je stále bezpečnejší, svedčí aj množstvo podložených faktov (testy, prieskumy).

Zálohovanie by nemalo prebiehať len raz mesačne formou plnej zálohy, ale každý deň alebo aspoň každý druhý deň formou prírastkových záloh. Plná záloha by mala byť vykonávaná vždy na konci pracovného týždňa. Dáta zálohované na externom pevnom disku by mali byť ukladané v šifrovanej podobe. Množstvo bezpečných šifrovacích programov je možné získať priamo z internetu zadarmo. Pevný disk s týmito zašifrovanými dátami (často ide o citlivé dáta spoločnosti) by mal byť starostlivo uschovaný a zamknutý na bezpečnom

mieste (firemný trezor). Najcitlivejšie a najdôležitejšie informácie by sa mali zálohovať na média DVD, a uchovávať minimálne jeden rok.

Personálna bezpečnosť si taktiež vyžaduje nové prístupy. Pri prijímaní zamestnancov malo by byť preverené ich deklarované vzdelanie. Každý nový zamestnanec by mal prejsť vstupným školením (nielen ohľadom bezpečnosti IKT). Priebežnými školeniami by mali prechádzať aj ostatní zamestnanci. Firma by mala vypracovať základné bezpečnostné smernice. Tie nestačí len nahlas prečítať, vyvesiť na nástenku či nechať podpísať všetkým pracovníkom. Treba donútiť zamestnancov, aby si tieto základné pravidlá osvojili a dodržiavali.

Spoločnosť by mala bezpodmienečne prijať nového zamestnanca pre oblasť IKT, s požadovanými znalosťami a skúsenosťami v odbore, schopného zabezpečiť efektívne a spoľahlivé fungovanie počítačov, počítačovej siete aj informačných systémov.

5 ZÁVER

Dnes už všetky podniky vo svojej činnosti využívajú počítače, spoliehajú sa na ne pri všetkých činnostiach. Počítače sa využívajú na komunikáciu, pri uzatváraní zmlúv, pre ukladanie informácií z dôležitých obchodných rokovaní, pre vedenie účtovníctva, evidenciu majetku, pre riadenie a rozhodovanie, atď. Bezpečnosť je jedným z najdôležitejších faktorov pri práci s počítačmi. Obzvlášť dôležitá je pri práci s cennými a dôvernými informáciami, alebo informáciami, ktoré sú utajované. Bezpečnosť sa však nevzťahuje len na únik informácií, ale aj na ich poškodenie spôsobené prácou užívateľa.

Riešenie otázok bezpečnosti vytvára predpoklady na ochranu ľudského činiteľa, majetku a ostatných aktív podniku. To prispieva k vyššej kvalite života v podniku a k vyššej efektivite samotného podniku. Zvyšuje sa pocit bezpečia zamestnancov podniku, vytvára sa optimálna pracovná atmosféra a verejná mienka, čo vedie k vyššej výkonnosti podniku. V konečnom dôsledku to vytvára i pozitívny image, a goodwill podniku na trhu.

Ochrana je široký súbor aktivít, ktorých cieľom je zamedziť poškodenie prostriedkov, ako aj neoprávnený prístup k informáciám, ich zneužitie. Ochranné opatrenia by mali nielen ochrániť systém pred chybami, ale by mali odhadovať vzniknuté chyby, a pokiaľ možno aj opravovať tieto chyby alebo dôsledky. Veľmi významným preventívnym opatrením je trvalá výchova všetkých pracovníkov. Z tohto dôvodu je aj dôležitou témou v obsahu predmetu Informačné technológie v riadení, ale i v iných predmetoch, ktoré sú dôležité pri výchove budúcich manažérov a ostatných užívateľov IKT.

Bezpečnosť a ochrana je široký súbor aktivít, ktorých cieľom je zamedziť poškodenie prostriedkov, ako neoprávnený prístupu k informáciám, ich zneužitie. Bezpečnostné opatrenia majú byť zamerané na ochranu IS pred chybami, ale aj na odhad vzniknutých chýb a najmä na opravu chýb a ich dôsledkov. Problematika zálohovania a archivácie údajov dnes vyžaduje odborníkov, špecialistov pre túto oblasť IKT. Nové technológie v oblasti zálohovania a archivácie údajov by však mali zaujímať nielen odborníkov z oblasti informačných technológií, ale aj užívateľov, ktorí používajú personálny počítač na pracovné účely, ale aj na štúdium a iné informačné potreby.

Možno konštatovať, že zabezpečenie zálohovania a archivácie údajov v počítači patrí tiež do aktuálnych problémov riešených v IS podnikov všetkých rezortov, to znamená, že aj agrokomplexu, ale aj IS organizácií v školstve.

Spoločnosť PRASTAV s. r. o. je v oblasti informačno-komunikačných technológií na podpriemernej úrovni.

Z celkového počtu 4 počítačov za sa zastaralé dajú považovať 2 počítače. Spoločnosť využíva 2 tlačiarne HP DeskJet 640C, ktoré sú zastaralé, ale spoľahlivo plnia svoju funkciu už niekoľko rokov a ich výmena zatiaľ nie je potrebná.

V oblasti bezpečnosti možno súčasný stav považovať za kritický. Systém chráni pravidelne aktualizovaný antivírusový program Microsoft OneCare. Na ochranu sieťovej komunikácie a blokovanie nepovolených prístupov firma využíva iba firewall systému Windows.

Zamestnanci podniku nie sú dostatočne informovaní o bezpečnostných hrozbách, k svojím dátam či bezpečnostným heslám pristupujú ľahkovážne a nezodpovedne. V spoločnosti chýbajú vnútorné smernice navádzajúce na komplexnú starostlivosť o informačno-komunikačné technológie a ich bezpečnosť.

Aby sa spoločnosť PRASTAV s.r.o. v budúcnosti vyhla problémov v IKT, boli navrhnuté nasledovné finančne nenáročné kroky:

- inštalácia prídavného softvérového firewallu Kerio Personal firewall,
- inštalácia programu na odstránenie adware a spyware Spyware Terminator,
- zakúpenie a nainštalovanie antivírusového systému NOD 32 pre všetky počítače pripájané do siete Internet a pravidelná aktualizácia,
- zmeniť systém záloh na plné zálohovanie na konci pracovného týždňa a prírastkové zálohy na konci každého pracovného dňa,
- v celej spoločnosti zmeniť politiku tvorby hesiel a prístupu zamestnancov k nim,
- poučenie zamestnancov o význame dodržiavania zásad počítačovej bezpečnosti, vstupné školenia pre nových a priebežné pre všetkých pracovníkov,
- vykonávanie preventívnych opatrení (testovanie systému antivírusovými programami, sťahovanie aktualizácii ...),

Pri zrealizovaní týchto krokov, ale aj ostatných návrhoch uvedených v tejto práci by spoločnosť získala neporovnateľne vyšší stupeň bezpečnosti v porovnaní so súčasným stavom, pri minimalizácii finančných nákladov.

Téma bezpečnosti podniku a informačných systémov mi nebola cudzia ani v minulosti, ale pri štúdiu dostupnej literatúry a spracovávaní diplomovej práce som získal hlbšie vedomosti z oblasti informačných systémov a ich zabezpečenia a možnostiach ich ochrany, ktoré som následne využil aj v praxi.

6 ZOZNAM POUŽITEJ LITERATÚRY

1. ADAMEC, P. 2006. Informačná bezpečnosť na Slovensku. [cit. 2007-05-17]. Dostupné na internete: <http://www.itnews.sk/buxus_dev/generate_page.php?page_id= 43593>
2. BAREŠ, M. 2006. Noví zabijáci virú. In: PC World, 2006. č. 3. 68 s. ISSN 1210-1079
3. BIELIK, P. a kol. 2001. Podnikovo hospodárska teória agrokomplexu. 2. vyd. Nitra : SPU, 2001. 270 s. ISBN 80-7137-861-5.
4. BOTT, E. - SEICHERT, C. 2004. Mistrovství v zabezpečení Microsoft Windows 2000 a XP. Brno: Computer Press, 2004. 696 s. ISBN 80-7226-878-3.
5. BRADLEY, T.2003. Zastavte hrozbu pre váš počítač. In : PC World, 2003. č. 1, 44 s. ISSN 1210-1079.
6. BUDIŠ, P. 2004. Jak vypracovať bezpečnostní politiku v podniku. In PC World Security, 2004. č.4, s. 44-46.
7. DOBDA, L.1998. Ochrana dat v informačních systémech. Praha: Grada Publishing, 1998. 288 s. ISBN 80-7169-479-7.
8. DOSEDĚL, T. 2004. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.
9. DOSEDĚL, T. 2005. 21 základních pravidel počitačové bezpečnosti. Brno: CP Books, 2005, ISBN 80-251-0574-1.
10. GÁLA, L. - POUR, J. - TOMAN, P. 2005. Podniková informatika. Praha: Grada Publishing, 2005. 484 s. ISBN 80-247-1278-4.
11. GYÁRFÁŠ, F. 2005. Tichí spoločníci. Slovart, 2005. ISBN 80-8085-018-6.
12. GUBALOVÁ, J. - HUŽVÁR, M. - RIGOVÁ, Z. 2005. Informatika pre manažérov 1 (výučbové CD). Banská Bystrica: EF UMB, 2005. ISBN 80-8083-158-0.
13. HALOUZKA, J. a kol.2001. Informační bezpečnost – příručka manažéra. Praha: Tate International, 2001. ISSN 1211-8737.
14. HAŠKOVÁ, A. 2004. Informačná propedeutika. Nitra: Edičné stredisko UKF, 2004. 130 s. ISBN 80-8050-729-5.
15. HENNYEYOVÁ, K. 2001. Informačná stratégia podniku v informačnej spoločnosti. Nové informačné technológie, podnikateľské informačné systémy a finančné nástroje v riadení poľnohospodárskych subjektov. Nitra: SPU, 2001. 18 s. ISBN 80-7137-946-8.
16. HOCHMAN, J. 2006. Národná stratégia pre informačnú bezpečnosť. [cit. 2007-05-01]. Dostupné na internete: <http://www.itapa.sk/ index.php?ID=2245>

17. HOFREITER, L. 2004. Bezpečnosť, bezpečnostné riziká a ohrozenia. Žilina, 2004. 146 s. ISBN 80-8070-181-4.
18. HOFREITER, L. 2002. Bezpečnostný manažment. Žilina, 2002. ISBN 80-7100-953-9.
19. HORÁK, J. 2003. Bezpečnosť malých počítačových sítí. Praha: Grada, 2003, 200 s. ISBN 80-247-0663-6.
20. JACKOVÁ, A. – ĎURIŠOVÁ, M. 2001. Základy finančného účtovníctva. Žilina: Žilinská univerzita, 2001. 135 s. ISBN 80-7100-866-4.
21. JAROŠOVÁ, M. 2006. Počítačových hrozieb pribúda, ochrana je pohodlnejšia. In: Trend, 2006. č. 42, s. 34. ISSN 1335-0684.
22. KLANDER, L. 1998. Hacker proof. Brno: UNIS Publishing, 1998. ISBN 80-86097-15-3.
23. KOKLES, M . - ROMANOVÁ, A. 2000. Informačný vek. Bratislava : Sprint vfra, 2000. s. 130-145, ISBN 80-88848-66-0.
24. KORCOVÁ, Z. 2000. Nové trendy v sieťových databázových systémoch. In : Nové trendy vo výučbe informatiky, SPU Nitra 2000. s. 25-29, ISBN 80-7137-656-6.
25. KORCOVÁ, Z. 2005. IT pre zálohovanie a archiváciu údajov v IS podniku. In: Zborník z vedeckého seminára : Faktory podnikovej úspešnosti v podmienkach európskeho agrárneho trhu. [CD-ROM]. Nitra : SPU, 2005, ISBN 80-8069-615-2.
26. KRÁL, M. 2006. Bezpečnost domáciho počítače prakticky a názorně. Praha : Grada Publishing, 2006. 336 s. ISBN 80-247-1408-6.
27. KRBILOVÁ, I. - NAGY, P. - PENIAK, P. 1998. Informačné systémy. Žilinská univerzita v Žiline, 1998. ISBN 80-7100-545-2.
28. KRETTER, A. 2004. Marketing. 1. vyd. Nitra : SPU, 2004. 288 s. ISBN 80-8069-390-0.
29. KUČERA, M.1999. Informačné systémy podnikateľských subjektov v poľnohospodárstve pre tretie tisícročie. In : Zborník vedeckých prác z medzinárodných vedeckých dní, Nitra : SPU, 1999. s. 76-78
30. KUČERA, M. - LÁTEČKOVÁ, A. 2004. Podnikové informačné systémy. Nitra : SPU, 2004. 209 s. ISBN 80-8069-452-4.
31. KUČERA, M. – ŠKORECOVÁ, E. 2002. Integrované informačné systémy. Nitra : SPU, 2002. ISBN 80-8069-084-7.
32. KUDLÁČ, M. a kol. 2006. Moderný používateľ PC, elfa, 2006. ISBN 80-8086-040-8.
33. MADLEŇÁK, R.2004. Elektronický obchod. Žilinská univerzita v Žiline, 2004. 160 s. ISBN 80-8070-192-X.
34. MANDOK, L. 2006. Bezpečnosť. [cit. 2007-05-15] Dostupné na internete: <http://www.autocont.sk/ sluzby-ebs-infrastruktura-bezpecnostict.cml>

35. McCLURE, S. - SCAMBRAY, J. 2003. Hacking bez tajemství. Praha: Computer Press, 2003. 462 s. ISBN 80-7226-948-8.
36. MIKOLAJ, J. a kol. 2004. Terminológia bezpečnostného manažmentu. Výkladový slovník. Košice: Multiprint s.r.o, 2004. 191s. ISBN 80-969148-1-2.
37. MIŽIČKOVÁ, Ľ. 2002. Základy manažmentu. Nitra : SPU. 2002. 95s. ISBN 80-7137-983-2.
38. MIŽIČKOVÁ, Ľ. - ŠIMO, D. - UBREŽIOVÁ, L. 2004. Základy manažmentu. Nitra: SPU. 2004. 95 s. ISBN 80-8069-375-7.
39. MOLNÁR, Z. 2000. Efektivnost informačních systémů. Praha: Grada Publishing, 2000. 179 s. ISBN 80-247-0087-5.
40. ODEHNAL, P. – HOFFER, T. 1999. Chránime počítač antivirovým programem AVG. Praha: Computer Press, 1999. 108 s. ISBN 80-7226-204-5.
41. OKENKA, I. a kol.: Informatika (praktické cvičenia). 1. vyd. Nitra : SPU, 2005. 179 s. ISBN 80-8069-592-X.
42. POPELKA, V. 1999. Vývojové tendencie automatizovaného spracovania informácií v poľnohospodárskych subjektoch SR. In : Agrární perspektivy VIII, Konkurencieschopnosť agrárního sektoru a integrační procesy, Sborník prací z medzinárodní vedecké konference, Praha : ČZU, 1999. ISBN 80-224-0423-3.
43. REICH, R. 2005. Červy neohrozujú iba ovocinárov. In : Profit, 2005. č. 27, 76 s. ISSN 1335-4620.
44. SODOMKA, P. 2006. Informační systémy v podnikové praxi. Brno: Computer Press, 2006. 352 s. ISBN 80-251-1200-4.
45. STRANYÁNEK, T. 2003. Prevence predevším. In: Connect Site, komunikace, systémy a bezpečnost, 2003. č. 10, 66 s.
46. STRNÁD, O. 2002. Manažment bezpečnosti IT. 2 vyd. Bratislava: STU 2002. 208 s. ISBN 80-227-1696-0.
47. SUCHÁNEK, P. 2000. Počítačové site jako domény informačních systému. In: Elektrotechnika v praxi. r. 2000. č. 7/8, s. 4-7.
48. VANĚK, J. a kol. 2004. Informační technologie I., Česká zemědelská univerzita v Praze 2004. s. 6-7, 12-13, 146-148, ISBN 80-213-1122-3.
49. VANKA, S. 2006. Tvorcom vírusov už nejde o slávu, ale o peniaze. In : Hospodárske noviny, 2006. č. 40, 4 s. ISSN 1335-4701.
50. VYSKOČ, J. 2006. Bezpečnosť IS. [cit. 2007-05-28]. Dostupné na internete: <http://www.vaf.sk/publikacie.htm>

51. VYSKOČ, J. 2006. Hrozby z vnútra. [cit. 2007-05-13]. Dostupné na internete: <http://vyskoc.blog.sme.sk/ c/66761/ Hrozby-zvnutra.html>
52. VYSKOČ, J. 2002. Informačná bezpečnosť a stratégia informatizácie na internete. [cit. 2007-05-03]. Dostupné na internete: <http://pc.server.sk/---bezpecnost-vseobecne-informacna-bezpecnost-a-strategia- informatizacie-spolocnosti--category-je-2-x-id-je-2997>
53. ŽITŇANSKÝ, E.2006. Zmiznúť z webu je ako zmiznúť z trhu. In : Profit, 2006. č. 22, 70 s. ISSN 1335-4620.
54. URL 1: Bezpečnosť podniku. [cit. 2007-05-23]. Dostupné na internete : <http://fsi.utc.sk/kbm/sluzby/ bezpecnost_podniku.htm>
55. URL 2: Bezpečnosť IT. [cit. 2007-05-13]. Dostupné na internete: <http://www.orga.sk/bezpecnost.htm>
56. URL 3: [cit. 2007-05-13]. Dostupné na internete <http://www.posam.sk/wwwsite/index.nsf>
57. URL 4: [cit. 2007-05-13]. Dostupné na internete: <http://www.gamo.sk/gamo/web/home.nsf/pages/-1F395E559235A895C125 6BA60 03B8046>
58. URL 5: [cit. 2007-05-17]. Dostupné na internete: <http://www.rokovania.sk/appl/material.nsf/0/-CB9E83FC63691FCBC1256DFF0 046B449/$FILE/Zdroj.html>
59. URL 6: [cit. 2008-03-15]. Dostupné na internete: <http://www.av-comparatives.org/seiten/ergebnisse_2008_02.php>
60. URL 7: Vírusový radar online. 2008. [cit. 2008-02-27]. Dostupné na internete: <http://www.virusradar.com/stat_02_months/2008-03/index_month.html>

7 PRÍLOHY

Príloha č. 1: Softvérové pirátstvo vo vybraných krajinách

Príloha č. 2: Prehľad antivírusových programov a ich výsledky v porovnávaných testoch

Príloha č. 3: Pohľad na Spyware Terminator

Príloha č. 4: Pohľad na užívateľské prostredie Kerio Personal

Príloha č. 5: Najvážnejšie bezpečnostné hrozby za obdobie 26.2.2008 - 26.3.2008

Príloha 1

Softvérové prirátstvo vo vybraných krajinách		
Krajina	**Miera pirátstva (%)**	**Hodnota nelegálneho softvéru (mil. USD)**
USA	22	6 496
Rakúsko	27	109
Veľká Británia	29	1 600
Nemecko	30	2
Česko	40	106
Maďarsko	42	96
Francúzsko	45	2 311
Taliansko	49	1 127
Slovensko	50	40
Poľsko	58	301
Grécko	63	87
Bulharsko	71	26
Rusko	87	1 104

Zdroj: International Data Corporation 2007

Príloha 2

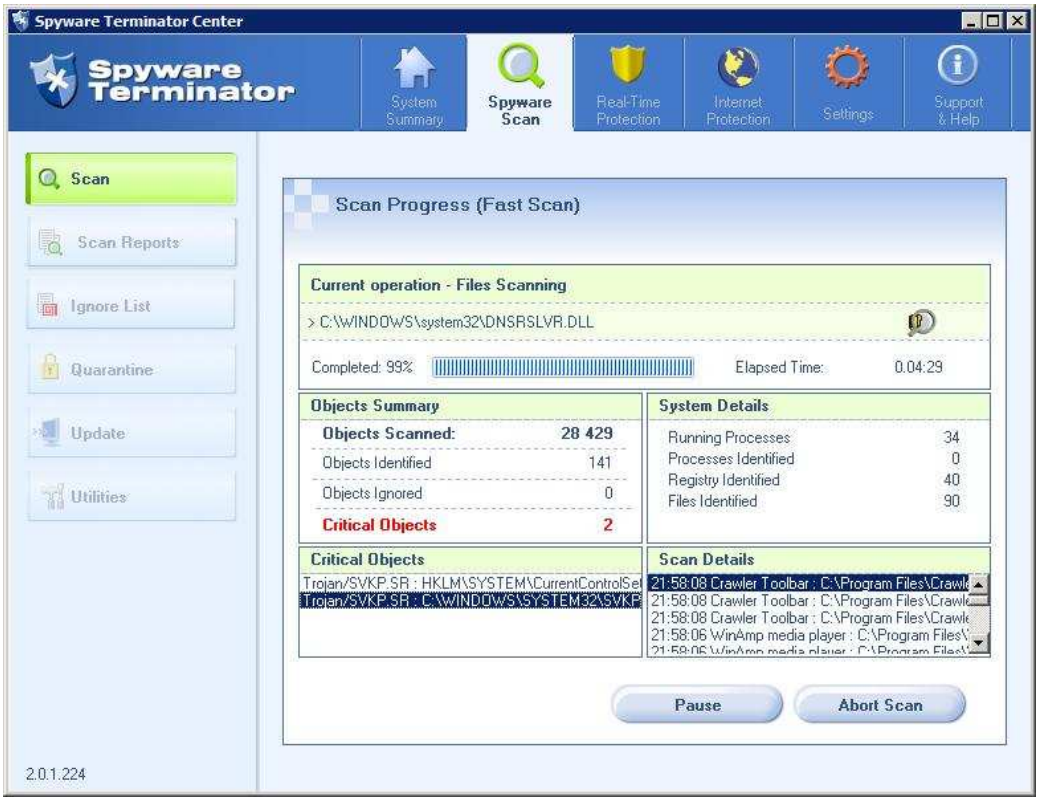
Company		AVIRA		G DATA Security		Alwil Software		AVG Technologies	
Product		**AntiVir PE Premium**		**AntiVirusKit (AVK)**		**avast! Professional**		**AVG Anti-Malware**	
Program version		7.06.00.308		18.0.7227.533		4.7.1098		7.5.516	
Engine / signature version		7.06.00.62 / 7.00.02.90		18.2654 / 18.123		080203-0		269.19.19 / 1258	
Number of virus records		*1.092.160*		*unknown*		*unknown*		*unknown*	
Certification level reached in this test		**ADVANCED+**		**ADVANCED+**		**ADVANCED+**		**ADVANCED+**	
On-demand detection of virus/malware									
Windows viruses	149.202	148.903	99,8%	149.119	99,9%	148.387	99,5%	143.393	96,1%
Macro viruses	95.059	95.034	~100%	95.059	100%	94.631	99,5%	94.823	99,8%
Script viruses	14.284	13.916	97,4%	14.165	99,2%	13.010	91,1%	12.055	84,4%
Worms	190.952	190.530	99,8%	190.564	99,8%	188.006	98,5%	188.821	98,9%
Backdoors/Bots	400.986	399.900	99,7%	399.536	99,6%	391.432	97,6%	395.103	98,5%
Trojans	817.043	813.233	99,5%	811.200	99,3%	793.223	97,1%	803.376	98,3%
other malware	15.838	15.447	97,5%	15.715	99,2%	14.402	90,9%	14.078	88,9%
TOTAL	**1.683.364**	1.676.963	**99,6%**	1.675.358	**99,5%**	1.643.091	**97,6%**	1.651.649	**98,1%**

BitDefender		MicroWorld		F-Secure		Kaspersky Labs		McAfee	
BitDefender Prof.+		**eScan Anti-Virus**		**F-Secure Anti-Virus**		**Kaspersky AV**		**McAfee VirusScan+**	
11.0.15		9.0.768.1		8.00.101		7.0.1.321a		12.0.176	
7.17325		*N/A*		7.30.13161		*N/A*		5200.2160 / 5222	
978.896		*unknown*		*unknown*		*574.209*		*371.817*	
ADVANCED		**ADVANCED+**		**ADVANCED+**		**ADVANCED+**		**ADVANCED**	
147.022	98,5%	148.683	99,7%	148.684	99,7%	148.909	99,8%	147.115	98,6%
94.736	99,7%	95.054	~100%	95.055	~100%	95.054	~100%	95.056	~100%
13.372	93,6%	13.949	97,7%	14.102	98,7%	13.949	97,7%	12.855	90,0%
189.084	99,0%	189.484	99,2%	189.515	99,2%	189.893	99,4%	188.318	98,6%
382.706	95,4%	390.205	97,3%	390.239	97,3%	392.713	97,9%	383.059	95,5%
782.493	95,8%	788.147	96,5%	788.288	96,5%	798.083	97,7%	757.305	92,7%
14.710	92,9%	15.299	96,6%	15.345	96,9%	15.390	97,2%	14.370	90,7%
1.624.123	**96,5%**	1.640.821	**97,5%**	1.641.228	**97,5%**	1.653.991	**98,3%**	1.598.078	**94,9%**

Microsoft		ESET		Norman ASA		Symantec		Sophos		AEC		VirusBlokAda	
Microsoft OneCare		**NOD32 Antivirus**		**Norman ISS AV+AS**		**Norton Anti-Virus**		**Sophos Anti-Virus**		**TrustPort AV WS**		**VBA32 Anti-Virus**	
2.0.2500.22		3.0.621.0		7.0		15.0.0.58		7.0.7		2.8.0.1629		3.12.6.0	
1.27.6270.0 / 1.3204		2847		5.91.10		100204 / 78215		2.70.1 / 4.26E+132		2.8.0.1630		*unknown*	
723.778		*unknown*		*1.310.735*		*73.845*		*345.615*		*unknown*		*unknown*	
ADVANCED		**ADVANCED+**		**ADVANCED**		**ADVANCED+**		**ADVANCED**		**ADVANCED+**		**STANDARD**	
146.690	98,3%	148.453	99,5%	140.874	94,4%	149.128	~100%	145.076	97,2%	149.037	99,9%	132.863	89,0%
94.624	99,5%	95.044	~100%	94.869	99,8%	95.059	100%	94.810	99,7%	95.053	~100%	92.909	97,7%
11.963	83,8%	13.338	93,4%	10.753	75,3%	14.049	98,4%	10.730	75,1%	13.979	97,9%	7.200	50,4%
185.743	97,3%	189.659	99,3%	185.448	97,1%	190.551	99,8%	185.065	96,9%	190.781	99,9%	171.497	89,8%
376.054	93,8%	391.015	97,5%	380.204	94,8%	384.939	96,0%	394.944	98,5%	400.503	99,9%	351.683	87,7%
753.863	92,3%	792.222	97,0%	761.830	93,2%	794.816	97,3%	783.006	95,8%	815.262	99,8%	708.649	86,7%
12.044	76,0%	14.226	89,8%	12.272	77,5%	15.464	97,6%	12.135	76,6%	15.458	97,6%	11.498	72,6%
1.580.981	**93,9%**	1.643.957	**97,7%**	1.586.250	**94,2%**	1.644.006	**97,7%**	1.625.766	**96,6%**	1.680.073	**99,8%**	1.476.299	**87,7%**

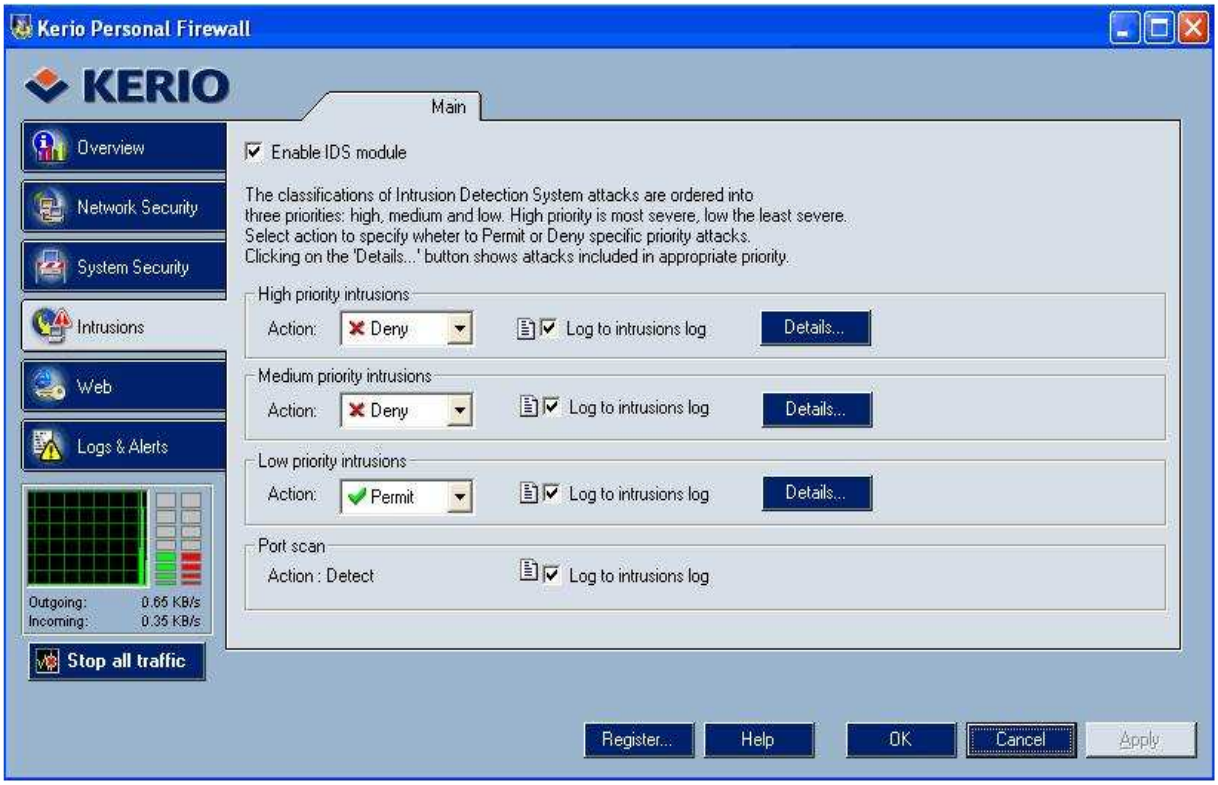
Zdroj: www.av-comparatives.org

Príloha 3



Zdroj: vlastné zdroje

Príloha 4



Zdroj: Vlastné zdroje

Príloha 5

10 najrozšírenejších ohrození v mesiaci

Všetky zachytené vírusy

Vírus	Počet	Pomer infekcie (%)	Pomer infekcie
01. HTML/Phishing.gen trojan	323 824	0.083 %	1/ 1.2 tis
02. Win32/Netsky.Q worm	176 165	0.045 %	1/ 2.2 tis
03. Win32/Stration.XW worm	166 402	0.043 %	1/ 2.3 tis
04. Win32/Netsky.D worm	19 544	0.005 %	1/ 20.0 tis
05. Win32/TrojanDownloader.Wigon.E trojan	10 641	0.003 %	1/ 36.7 tis
06. a variant of Win32/TrojanDownloader...	9 563	0.002 %	1/ 40.9 tis
07. Win32/Zafi.B worm	7 665	0.002 %	1/ 51.0 tis
08. Win32/Mytob.BK worm	6 211	0.002 %	1/ 63.0 tis
09. Win32/Bagle.HE worm	6 038	0.002 %	1/ 64.8 tis
10. Win32/Pecutex.A virus	4 881	0.001 %	1/ 80.1 tis
> OSTATNÉ VÍRUSY	27 554	0.007 %	1/ 14.2 tis
> CELKOVÝ POČET VÍRUSOV	**758.5 tis**	**0.194 %**	**1/ 515.5**
Celkový počet zdravých správ	**390.3 mil**		
Celkový počet správ	**391.0 mil**		

Zdroj: www.virusradar.com