Informační obrana moderní firmy před interními útoky

Matúš Gaborčík

Bakalářská práce
2006

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky
Ústav informatiky a statistiky
akademický rok: 2005/2006

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Matúš GABORČÍK**
Studijní program:	**B 6208 Ekonomika a management**
Studijní obor:	**Management a ekonomika**
Téma práce:	**Informační obrana moderní firmy před interními útoky**

Zásady pro vypracování:

1. **S využitím dostupných informačních zdrojů proveďte komplexní analýzu současné situace z pohledu bezpečnosti a ochrany firemních dat.**
2. **Vypracujte návrh systému informační obrany moderní firmy a připravte jej jako nabídku účastníkům konference Internet a bezpečnost organizací v roce 2006 ve Zlíně.**
3. **Na základě požadavků vyšlých z nabídky uskutečněte konkrétní implementaci.**
4. **Proveďte vyhodnocení dopadů uskutečněných změn.**

Rozsah práce:	**80 stran**
Rozsah příloh:	
Forma zpracování bakalářské práce:	**tištěná/elektronická**

Seznam odborné literatury:

[1] BRABEC, F., a kol. Bezpečnost pro firmu, úřad, občana. 1. vyd. Praha: Public History, 2001. 400 s. ISBN 80-86445-04-06.
[2] BRABEC, F. Ochrana bezpečnosti podniku. 1. vyd. Praha: Eurounion, 1996. 203 s. ISBN 80-85858-29-0. Část B, Bezpečnostní expertíza ochrany objektů a dalších bezpečnostních zájmů podnikatelských subjektů, s. 59-96.
[3] ZELENKA, J., BAUDIŠ, P. Antivirová ochrana. 1. vyd. Praha: Plus, 1996. 183 s. ISBN 80-85297-74-4.
[4] JAŠEK, R. Ochrana znalostí a dat v podnikových informačních systémech. 1. vyd. Zlín: Univerzita Tomáše Bati, 2002. 115 s. ISBN 80-7318-095-2.
[5] LAUCKY, V. Technologie komerční bezpečnosti I. 2. vyd. Zlín: Univerzita Tomáše Bati, 2004. 64 s. ISBN 80-7318-194-0.

Vedoucí bakalářské práce:	**Mgr. Roman Jašek, Ph.D.** Ústav informatiky a statistiky
Datum zadání bakalářské práce:	**13. března 2006**
Termín odevzdání bakalářské práce:	**19. května 2006**

Ve Zlíně dne 13. března 2006

doc. PhDr. Vnislav Nováček, CSc.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta managementu a ekonomiky

doc. Ing. Rudolf Pomazal, CSc.
ředitel ústavu

ABSTRAKT

Bakalárska práca pojednáva o informačnej bezpečnosti ako o jednom z kľúčových faktorov pre dosiahnutie optimálneho zdravia modernej firmy. V dnešných tvrdých ekonomických a sociálnych podmienkach obstoja len tí, ktorí sú na boj pripravení a efektívne vyzbrojení. Internet už nie je mierumilovným prostredím, v ktorom človek môže hľadať pokoj, lež najväčšou kriminálnou scénou histórie. Okrem toho, externé útoky predstavujú iba 20 % všetkých incidentov, páchateľ sa obvykle nachádza vo vnútri organizácie. Cieľom práce je preto systematickým spôsobom oboznámiť čitateľa s problematikou bezpečnosti IS, jej aktuálnym stavom vo svete, existujúcimi hrozbami, dostupnou prevenciou a obranným vybavením - všetko bez ohľadu na stupeň jeho znalostí v príslušnej oblasti. Jedná sa o ucelenú príručku určenú všetkým (najmä budúcim riaditeľom bezpečnosti), ktorí túžia po zavedení takých opatrení, aby sa ich firma či inštitúcia stala bezpečnejším miestom pre uskutočňovanie podnikateľských aktivít. Spestrením je vyhodnotenie dotazníkového výskumu realizovaného v rámci medzinárodnej konferencie „Internet a bezpečnosť organizací 2006“.

Kľúčové slová: počítačová bezpečnosť, bezpečnostná politika, sociálne inžinierstvo, konkurenčné spravodajstvo, informačná obrana

ABSTRACT

The bachelor thesis describes information security as one of the main elements needed to maximise company’s healthy running. In today’s conditions, only those who are well prepared and rightly armed will survive the existing economic and social battle. Internet is no longer a peaceful place; it’s the most bizarre criminal scene in history. But external attacks make only 20 % of all security incidents. The culprit usually hides inside your company. The aim of this work is to systematically inform about IT security basics, global security situation, existing threats, available methods of prevention and security defence tools – all independently on reader’s competences. Basically, this tends to be a manual to all of those (especially upcoming CISOs), who wish to make their company or institution a safer place to do business activities. A bonus added is a result of realised security survey.

Keywords: computer security, security policy, social engineering, competitive intelligence, IT defence

POĎAKOVANIE

Veľmi rád by som sa týmto skromným, ale úprimným spôsobom poďakoval svojmu garantovi Mgr. Romanovi Jaškovi, Ph.D., bez ktorého by táto práca nikdy nevznikla. Vážim si a nikdy nezabudnem na jeho vysoko ústretový prístup, keď si vždy i napriek všetkým svojim pracovným povinnostiam dokázal nájsť čas pre sofistikované usmernenie a povzbudenie svojho študenta. Ako sám povedal; „...ak vás nič nového cez túto prácu nenaučím, môžem to tu rovno zabaliť“. Som presvedčený, že sa mu to u mňa podarilo a do budúcna mu prajem veľa lásky a úspechov.

Ďakujem tiež svojim drahým rodičom, ktorí mi vždy preukazovali lásku a podporovali ma počas mojich troch rokoch štúdia na UTB. Ďalej ďakujem strýkovi Štefanovi, Jaromírovi Špicovi, sestre Pavle, Jiřímu Patermannovi a Petrovi Vilímkovi za nenahraditeľné chvíle priateľstva, neoceniteľných skúseností a pomoc.

Veľmi si vážim pracovitosti, ústretovosti a trpezlivosti všetkých členov Ústavu informatiky a štatistiky. Nikdy nezabudnem na podrobné a odhodlané emaily od Ing. Mirky Brázdilovej, Ph.D., férovosti Ing. Radka Bendu, Ph.D., ktorý bol síce „tvrďas“, no len preto aby nás donútil študovať ako aj na ďalších, ktorí ma síce neučili, ale vyžarujú vysokú svedomitosť.

Motto:

„ Rozum je ako kvet. Múdrim kvitne, hlúpym vädne. “

STARÉ ŽIDOVSKÉ PRÍSLOVIE

„ Mind is like flower. It blooms when you are wise, but withers when stupid. “

OLD JEWISH SAYING

OBSAH

ÚVOD

Dnešný svet sa svojim vývojom ponára do nepoznanej jednoty politického, ekonomického, sociálneho, náboženského, etického a najmä technologického systému a prostredia. Nosnou črtou toho posledného je celosvetová sieť pre výmenu informácií – Internet. Tento opis charakterizuje globalizáciu, čiže svetovládu. Globalizácia, azda akýsi záhadný vývoj skrývajúci sa za nevinne znejúci pojem, o ktorom sa dnes, na rozdiel od svojich rodičov, učí každé moderné dieťa v školskej lavici. Otázka ostáva, kam sa rúti Zem, pre aké ciele preteká čas, čas tak vzácny, čas píšuci dejiny ľudstva, dejiny modrej planéty. Kto stojí za globalizáciou, kto sú tí, ktorým sa v hlave rodia myšlienky celosvetovo registrovať spoločnosť podkožnými čipovými implantátmi, aby už nebolo obáv o platobné a úverové karty, občianske preukazy, zdravotné kartičky, cestovné pasy, vodičské preukazy, prístupové heslá, tokeny, a iné autentizačné nástroje? V súčasnosti má v Japonsku uvedený nanotechnický počin, kedysi vedcami pokusne testovaný na väzňoch v laboratóriách amerického Phoenixu, dobrovoľne zavedených už asi tisíc ľudí. Švédsko nedávno odsúhlasilo automatické zavádzanie týchto čipov novorodencom. Najnovšie vysokoškolské odbory nesú názvy ako bioinformatika, biotechnológie, biobáze, kybernetika, neurónové siete, a pod. IT orientované vydavateľstvo IDG nám v každom čísle tlačí pred oči knihu Vzbura génov. Čo chcem týmto nezvyčajným úvodom naznačiť? Asi toľko, že či si to niekto uvedomuje alebo nie, doba kedysi označovaná titulom science-fiction je už markantne prítomná v realite. Podľa posledných správ, najvyššie kruhy z pomedzi exteritoriálnych organizácií OSN, USA a EÚ sú vo fáze ukončenia projektu na zavedenie globálneho systému identifikácie, kde sa už nikto nebude „môcť skrývať“ nastolenému svetovému poriadku. Možno by to nebolo tak dôležité, ak by tu nestála otázka, či sa nedá tento systém zneužiť. Hľadiac naň kritickými očami je jasné, že jeho implementáciou bude pohyb civilizovaného občana totálne monitorovaný. Osobne sa preto zamýšľam, či sa sloboda nevinne nenahrádza pojmom bezpečnosť, pričom bežný smrteľník sa vlastne o pravých záujmoch vladárov spoločnosti nedozvie. Mladej generácii väčšinou ani nenapadne, akým nezmyslom je prijať sofistikovane propagovanú ideu spoliehania sa na spásonosný význam strojov. Že stroje sú nedokonalé obsahujúc mnoho neobjavených chýb (ekvivalent časovanej bomby) je rovnaká skutočnosť ako to, že sa prostredníctvom zlomyseľnej vôle človeka môžu kedykoľvek stať objektom zneužitia. Podobne ako ľudstvo pretvorilo prírodnú krajinu s jej pôvodnou dokonalosťou a rovnováhou na krajinu umelú bez žiadanej harmónie, tak sa aj naša spoločnosť behom posledných tridsiatich rokov

úspešne ocitá tvárou v tvár, dovolím si tvrdiť, bizarnej dobe chladných vzťahov na čele s technokratizmom. Svojou pripútanosťou k technológiám venujeme bez ohľadu na to, či sa nám to páči alebo nie, každodennou činnosťou strojom vlastnú životnú energiu.

Sme nútení rútiť sa po vystavanej internetovej diaľnici pekelnou rýchlosťou. Po diaľnici, ktorá predstavuje najrozsiahlejšiu kriminálnu scénu histórie. Dalo by sa špekulovať, nakoľko sme „pri našej jazde pripútaní bezpečnostnými pásmi“, to je pravdaže téma veľmi komplexná, obšírne opísaná v nejednej publikácií, hlavne však nie celkom predmetom tejto teoreticko-výskumnej práce. Iná nadväzujúca úvaha hovorí; je jasné, že existuje populačný limit Zeme, dokedy však unesie intenzívne zaľudňovanie - aplikujúc na svet informatiky, počet nových hrozieb na Internete rastie, reakčná doba obranných riešení sa predlžuje pretože víry sú čoraz zložitejšie, atď. - hrozí teda o niekoľko rokov kolaps Internetu, ktorý vďaka uznávanej globalizácii spôsobí celosvetový chaos? Zo zákonov života, prírody, fyziky atď. sa vie, že všetkému je prirodzene vlastný jeho počiatok, alfa a koniec, omega. Predstavy typu „IT priemyslu niečo také nehrozí“ považujem za smiešne i z tohto pohľadu.

Ale späť do sféry IT bezpečnosti. Čo predstavuje pre podnik alebo verejnú správu rovnakú hrozbu ako útoky externé spôsobené Internetom, sú útoky interné. Internista, čiže osoba nášmu prostrediu vlastná, dokáže vedome alebo nevedome svojimi zásahmi ťažko ohroziť konkurencieschopnosť podniku a v konečnom dôsledku jej finančné zdravie. Rovnako personálna rovina vyzdvihuje tragédiu súčasnej spoločnosti - ide skôr o náhodu, ak sa dnes ešte dá niekomu dôverovať. Dožili sme sa storočia povšimnutiahodnej nedôvery, stále vynárajúcich sa pochybností a podvedomému strachu, strachu o seba, o svoje zamestnanie, budúcnosť a očividne strachu o majetok, peniaze a informácie každého charakteru. Je bežné, keď sa obľúbený obchodný partner zmení v chamtivého nepriateľa, lebo vycíti, že slabosťou druhého má príležitosť prísť k peniazom (podvody s cennými papiermi a i.). Z hľadiska práva a poriadku sa nachádzame v temnej ére. Počítačová sieť koniec koncom predstavuje akýsi panoptický obraz civilizácie. Nakoniec, je dobré si uvedomiť, že spôsob, ako dokonale predvídať a zabrániť budúcim útokom kvôli nevyspytateľnosti ľudského faktoru de facto neexistuje (vypuknutie svetových vojen). Snaha bezpečnostných riaditeľov v dnešných organizáciách preto spočíva aspoň v implementácií bezpečnostných riešení použiteľných ako možná diplomatická prevencia proti kompromitácii znalostí. O tom už táto práca.

I. TEORETICKÁ ČASŤ

1 DÁTA, INFORMÁCIE, ZNALOSTI A BEZPEČNOST

Svet zažíva epochu obrovského informačného boomu. Zatiaľ čo kedysi bolo nemalým problémom vyhľadať potrebné údaje, dnes je paradoxom, že práve vyselektovať relevantné údaje z abnormálneho kvanta informácií si vyžaduje značnú zručnosť a úsilie. Po úspechu takejto operácie nasleduje porozumenie významu konkrétnych vyhľadaných informácií, čoho výsledkom sú znalosti. Primárne najrozšírenejším formátom informácií dnešnej spoločnosti je ich elektronická podoba - dáta. V tejto súvislosti je vhodné vyzdvihnúť pár aspektov.

V súčasnosti sa dynamicky rozvíjajú technické možnosti distribuovaného spracovania dát. Rastie rada nových aplikácií a budujú sa veľké moderné systémy informatiky (IS) na rôznych úrovniach štátnej správy ako aj v rôznych oblastiach hospodárstva krajiny. Takto vznikajú rozsiahle súbory informácií, dochádza k sústreďovaniu dátových fondov z rôznych oblastí ekonomickej, spoločenskej a politickej sféry našej spoločnosti. Z hľadiska bezpečnosti sú na tom systémy informatiky veľmi podobne ako banky v minulosti. U niektorých inštitúcií sú technické prostriedky veľmi cenené a považované za hodnoty, ktoré je nutné náležitým spôsobom chrániť. Informácie v databázach sú využívané napríklad v prípadoch keď občan požíva svoju kreditnú kartu, žiada hypotéku na zakúpenie nehnuteľnosti alebo sa uchádza o pracovné miesto. Tie isté informácie slúžia policajtom v hliadkových vozoch pri sledovaní podozrivých osôb alebo lekárom predpisujúcim pacientom potenciálne nebezpečné lieky. Na druhej strane sa stáva, že stránky novín a časopisov bývajú zaplnené „senzačnými“ článkami o ľuďoch, ktorým boli omylom porušené nájomné zmluvy, o pornografii zasielanej deťom, o starých občanoch, ktorým odpojili prívod elektriny uprostred zimy a dokonca o chirurgických zákrokoch, pri ktorých boli pacientom vyoperované zdravé orgány - všetko v dôsledku chýb spôsobenej systémom. [8]

Módou ostáva zvaľovať podobné situácie na anonymitu systému. Nič menej skutočnosť ukazuje, že väčšina takýchto prípadov je skôr výsledkom nezodpovednosti ľudí, ktorí do systému vkladajú nesprávne dáta, než nejakou jeho technickou či programovou vadou. Vinou systému je nanajvýš to, že bude prijímať a spracovávať nesprávne dáta, z ktorých potom vyvodí nepravdivé závery bez akejkoľvek ďalšej kontroly. Ešte v nedávnej dobe sa problém kontroly resp. ochrany dát celkovo javil ako záležitosť okrajová. Tieto časy sú pochopiteľne dávno minulosťou a situácia je úplne odlišná.

1.1 Charakter nežiaduceho prieniku do IS

Cieľom útokov kriminálnych živlov môže byť akákoľvek časť informačného systému (IS). IS tvoria technické prostriedky, programové prostriedky, pamäťové média, dáta a osoby nejakým spôsobom zainteresované do jeho procesov. Predmetom záujmu bežnej kriminality býva predovšetkým peňažná hotovosť, predmetom záujmu počítačovej kriminality sa bežne stávajú napríklad zoznamy mien a adries bankových klientov.

1.1.1 Druhy narušení bezpečnosti informácií

Narušenie informačného procesu, nevydanie, nezískanie správnych a potrebných informácií alebo oneskorenie ich prenosu vedú k nevyhovujúcej funkcii podnikateľskej aktivity. Schopnosť podnikateľa prijať užitočné informácie a oddeľovať od svojej činnosti to, čo je zbytočné a škodlivé, záleží od jeho skúseností. Aby sa mohli prijať opatrenia proti narušeniu bezpečnosti IS, je dobré zmieniť niekoľko súvisiacich pojmov;

- *riziko* – možnosť vzniku určitej straty, škody či inej nežiaducej skutočnosti
- *zraniteľnosť* – slabé miesto bezpečnostného systému, náchylné k útokom
- *napadnutie* – využitie zraniteľnosti škodcom
- *ohrozenie* – okolnosti vedúce k potenciálnym stratám alebo škodám
- *kontrola* – ochranné opatrenie, činnosť, technika minimalizujúca ohrozenie

Pretože dáta sú často dostupné v zrozumiteľnej forme, býva ich utajenie v strede záujmu informačnej bezpečnosti.

1.1.2 Prenos informácií

Prenosom informácií sa rozumie ich predávanie v rámci prvkov vo vnútri IS alebo medzi systémami navzájom a ich zabezpečenie po prenosových kanáloch. Počas prenosu pôsobia na informácie rušivé vplyvy (šum), ktoré sa prejavujú ako skreslenie (zámerné, živelné), utajenie (zamlčanie, zašifrovanie) alebo odvedenie informácie (rozptýlenie informačného toku). Každá informácia je údajom, ale nie každý údaj uložený na počítači je informáciou, iba ten, ktorý je novinou. [1]

2 INTERNET

Čo predstavuje tento fenomén, ktorý odštartoval revolúciu vo svete, už nemá zmysel rozoberať. Azda sa hodí akurát upozorniť na rozdiel medzi pojmom Internet a www. Internet označuje celosvetovú počítačovú sieť sietí, ktorú v súčasnosti tvorí viac ako 30 000 000 vzájomne prepojených počítačov. WWW (w3, web) však nie je to isté čo Internet, ale je jeho užívateľským prostredím majúcim podobu internetových stránok. Po spustení browsera vlastne vidíme www. Dnes ich je na Internete viac ako 50 miliárd.

2.1 História

Najväčším požieračom finančných prostriedkov je zbrojný priemysel a teda podstatná časť dane, ktorú občania odvádzajú do štátneho rozpočtu (platí hlavne pre USA), končí vo forme zbraní uložených na neprístupných miestach vojenských základní, kde čakajú na možné vyhladenie života. Internet vznikol - rovnako ako jadrový reaktor, mobilný telefón, rádio, prvý počítač či iný revolučný technologický počin - prostredníctvom armádneho projektu Ministerstva obrany USA. V šesťdesiatich rokoch vrcholila studená vojna a Američania potrebovali vymyslieť spôsob, akým prepojiť počítače na rôzne umiestnených veliteľských stanovištiach tak, aby sa spojenie po zlikvidovaní niektorého z nich neprerušilo. Vedci preto vyvinuli Arpanet (1969) – komplexnú vojenskú sieť. Ako to už bežne býva, technologické tajomstvo neostalo dlho ukryté. Internet sa najsamprv účelovo dostal na akademickú pôdu až sa nakoniec plne ponechal civilnému sektoru (1983), kde sa rozšíril do dnešnej podoby. Jeho pôvodní používatelia nemali veľké nároky na bezpečnosť, plne im postačovala možnosť vzájomnej komunikácie a výmeny informácií.

2.2 21. storočie

Bruce Sterling, odborník na IT bezpečnosť, sa pre magazín o bezpečnosti v kybernetickom svete vyjadruje prostým spôsobom; „Internet zošalel.“ Skutočne. Kedysi hackeri najprv vyzerali ako celkom nápaditý a vynaliezaví experimentátori. Aj tí neposlušní, ktorí sa vkrádali do systémov, boli koniec koncom iba hraví teenageri uťahujúci si zo zákonov, mladíci s vysokou inteligenciou, ktorí obvykle žili v mestách s tradíciou technologického výskumu, ako Berkeley či Cambridge. Títo chlapíci sú tu dodnes a stále robia problémy.

Ale všetky druhy nelegálnych aktivít na webe, ktoré bolo možné zaznamenať pred desiatimi rokmi, sú dnes ďaleko rozšírenejšie a intenzívnejšie.

Kde bolo kedysi pár celkom jednoduchých vírov, sú ich teraz tisíce, naviac sa rýchlo vyvíjajú a mutujú do najrôznejších podôb. Tam, kde sme sa mohli stretnúť s malým podvodom s kreditnou kartou, nachádzame v súčasnosti medzinárodne organizované gangy zneužívajúce kreditné karty. Krádeže hesiel k počítačovej sieti sa zmenili v rafinované scudzenia osobnej identity, ktoré oberajú bankových klientov a vykrádajú stránky s on-line aukciami. Spam, kedysi iba občasné hrubé porušenie „netikety“, sa na nás tentoraz rúti v ohromnom množstve (ako uvádza firma IronPort, zaoberajúca sa bezpečnosťou emailu, v máji 2005 išlo celosvetovo o 12,9 miliárd prípadov denne), niektoré z nich sú neuveriteľne bizarné alebo obscénne. Potom tu máme novšie druhy elektronickej kriminality, ktoré sa šíria tak rýchlo, že i špecialisti len s ťažkosťami stíhajú udržať krok s vývojom odborného slangu. Reč je o pojmoch phising, spear phising, pharming, DDoS, vydieračské gangy DDoS, spyware, scumware, ovládnutie webových stránok, botnets, keylogging a mnohé ďalšie. Internet skrátka vstúpil do zlatej éry kriminálnej vynaliezavosti. Je to tzv. dot-con boom – rozmach internetových zločincov a podvodníkov, kedy elektronická kriminalita bujní v nenásytnej túžbe prísť na obchodné schémy, ktoré by vyniesli peniaze. Dokonca i enkrypcia, pôvodne zamýšľaná ako obranné opatrenie, sa stala nástrojom vydierania – stávame sa svedkami vzniku nového podivného typu zločinu, spočívajúceho v tom, že sa vám niekto vláme do počítača, zašifruje jeho obsah a potom po vás chce úplatu za poskytnutie hesla k vašim vlastným dátam. [12]

Na internete sa dnes pohybuje okolo jednej miliardy ľudí (podľa *Computer Industry Almanac*), a tak sa z globálnej dediny využívajúcej vyspelé technológie čím ďalej tým viac stáva akási chladnokrvná obria metropola, zamorená slumami. Všetky klasické podvody a vydieračstvá, ktoré ostrí chlapi predvádzajú davom, je dnes možné digitalizovať. Podvodníci majú k dispozícií nekonečné množstvo obetí pretože na Internete sa vždy nájde nejaký nováčik, človek neskúsený či príliš mladý, skrátka niekto, kto sa dobre nevyzná v reči, ktorou sa v tomto špecifickom svete hovorí. [12]

Predstavte si, že si po prvý krát kupujete osobný počítač. Počítač je lacný, software vyzerá slušne, všetko sa ovláda ľahko, stačí kliknúť a môžete si robiť, čo sa vám zachce. Potom vám predavač odporučí, aby ste si dodatočne zaobstarali antivírový software, systémové utility a firewall. Pochopiteľne, zaplatili ste za počítač a operačný systém, no nechce sa

vám utrácať ďalšie peniaze, takže na dodatočný software sa vykašlete. A sotva ste on-line, poznáte, že ste priamo napojení na hostiteľský počítač zlomyseľných ľudí, ktorých vôbec nepoznáte. Hoc sa pokúsite reagovať, obvykle nebudete mať dosť znalostí ani skúseností na to, aby ste sa ubránili. Ponaučenie; obeťami malwaru nie sú ľudia znalí počítačových technológií, ale práve tí, ktorí nečítajú bezpečnostné ročenky, a takýto ľudia väčšinou prehltnú návnadu aj s navijakom. [12]

2.2.1 Nebezpečenstvo číha všade

Problémy s bezpečnosťou sa objavujú na všetkých úrovniach. Elektronické obchodovanie je zraniteľná vec keďže sa obecne opiera o rýchlo navrhnuté systémy, ktoré sú popritom nepružné, aby vyhovovali požiadavkám kolektívnych grémií. Podľa odborníkov je nevyhnutné tieto systémy navrhnúť úplne znovu a premyslieť tak, aby sa bezpečnosť stala ich integrálnym prvkom, a nie aby sa na nich nasadzovala až dodatočne. Ale koho by pred desiatimi rokmi bolo napadlo, že MS Windows budú mať niekoľko stoviek zneužiteľných chýb, nedostatkov a dier. Pritom nový priemysel jedná rovnako neuvážene ako jeho predchodcovia a je práve tak náchylný opakovať všetky omyli počínajúceho Internetu; nedbalosť, ukvapený vývoj a naivná pýcha priekopníka, ktorý si nedokáže predstaviť, že zločinci budú raz rovnako chytrý ako on sám. Napríklad, až potom, čo si užívatelia Web Acceleratoru od Googlu sťažovali, že jeho technika zberu dát umožňuje neoprávneným osobám dostať sa na servery chránené heslom, Google prestal tento software ponúkať s odôvodnením, že vraj už nedokáže podporovať viac užívateľov. Napokon je tu ešte hrozba najkrajnejšia; že by kyberteroristický útok mohol zhodiť samotný internet (CodeRed). [12]

2.2.2 Delokalizácia zločinu

Internet je globálny, zatiaľ čo právo je lokálne. Platí v určitej krajine a to je zásadný problém, s ktorým sa musia vysporiadať tí, ktorí sa chcú postaviť proti prívalovej vlne zločinu. Žijeme vo svete, v ktorom sa národy snažia chrániť pred zločincami, ktorí nemajú žiadnu spiatočnú adresu. Medzinárodné organizácie, ktoré údajne usilujú o civilizovanie siete sietí (ICANN, WSIS, IETF, W3C) sú natoľko slabé a nevýrazné, že väčšina ľudí ani nevie, aké meno sa za každou z týchto skratiek skrýva. Tieto organizácie nevlastnia žiadne prvky, ktoré by mohli s internetovou kriminalitou niečo spraviť. Nedisponujú žiadnymi zbraňami, služobnými odznakmi ani väznicami. Títo a ďalšie organizácie by teoreticky

mohli odstrániť spustu slabých miest v starnúcej architektúre siete. Napríklad National Science Foundation nedávno prišla s projektom vývoja ďalšej generácie Internetu, ktorá by nahradila dlho diskutovaný protokol IPv6, ktorý by zdokonalil dnešný IPv4. Avšak Internet je už možno príliš starý, príliš veľký a príliš v znamení anarchie na to, než aby ho dokázala napraviť akákoľvek inštitúcia. V dôsledku toho, že chýba akákoľvek bezprostredne použiteľná vízia pre globálne riešenie globálnych problémov Internetu, neostáva úradom na nadnárodnej úrovni nič iného, než len občas zdvihnúť spadnutý štafetový kolík. Štáty majú prostriedky, radu pohnútok i možností k tomu, aby právo a poriadok schválili a následne vynucovali. Majú zbrane, peniaze a väznice. A čo sa týka zásadného vplyvu na Internet, sú skutočne jedinou superveľmocou Spojené štáty. Americká vláda napríklad zabavila DNS root servery medzinárodnej organizácie ICANN: zabrala všetky mená a adresy tvoriace jadro Internetu i ústredné schéma, vďaka ktorému Internet funguje globálne. Podobne ministerstvo obchodu USA donútilo ICANN, aby zastavilo spustenie schválenej domény .xxx, kde by bola pornografia a virtuálne nevestince separované od ostatných stránok. Spojené štáty majú oficiálny plán, ktorého cieľom je učiniť Internet bezpečnejším a slušnejším miestom. Predstavuje ho Národná stratégia zabezpečenia virtuálneho priestoru (NSSC), ktorá jednak formuluje odporúčania, ako si udržať poriadok vo veci zabezpečenia a ako sa v tejto otázke náležite vyškoliť, jednak požaduje, aby vznikla mnohostranne zameraná agentúra, vlastne akási informačná sieť okamžitej reakcie na „kybernetické výstrahy“, ktorá by slúžila k riešeniu pohotovostných situácií. Ale tento plán, hoc nikdy nebol oficiálne zamietnutý, nebol ani nikdy plne akceptovaný. [12]

2.2.3 Internet je taký, aký si zaslúžime

Internet nemusí nutne každému prinášať pohodu a prosperitu. Je tým, čím bol od samého počiatku; akýmsi zrkadlom civilizácie. Internet bude taký, aký si zaslúžime. Ako by sa dalo zasadiť o jeho vylepšenie? Ľudia by sa mali najprv opäť naučiť umeniu žiť ako aktívny občania. Chcelo by to prinútiť všetkých hlavných protagonistov obchodu a štátu, aby sa prestali vyhovárať jeden na druhého, toľko sa nevystatovali a nevykrucovali sa. [12]

3 BEZPEČNOSTNÁ POLITIKA V ORGANIZÁCIÁCH

Podľa prieskumu Computer Security Institute došlo u ôsmych prípadov narušenia bezpečnosti z deviatich k cítiteľným finančným stratám. Mnohí majitelia dnešných, predovšetkým malých a stredných firiem považujú úvahy o zabezpečení za zbytočné. Hlavným argumentom a omylom zároveň ostáva presvedčenie, že je nepravdepodobné, aby si útočník vybral „malú alebo strednú korisť“, keď existujú väčšie a atraktívnejšie podniky. V podstate opak je pravdou a to z týchto troch dôvodov - malé firmy sú často súčasťou veľkých útokov, akými je hromadné šírenie červov, za druhé; väčšie organizácie bývajú viac technologicky pripravené a neustále posilňujú svoju obranu takže sa siete malých organizácií stávajú lákavejším terčom pre útočníkov, a nakoniec; nie všetky útoky sú externé. [10]

Dnes je pre každú modernú, po konkurencieschopnosti dychtiacu firmu, štátnu organizáciu či akýkoľvek druh spoločnosti nevyhnutnosťou, aby si dokázala pomocou vhodných nástrojov ustrážiť svoje firemné know-how, výrobný knowledge, investície, kompetentnosti svojich zamestnancov a s tým súvisiace všetky druhy informácií, teda obzvlášť tých v elektronickej podobe. So zavedením modernej technológie spracovania a prenosu informácií do oblastí spoločenskej aktivity vystupuje do popredia nutnosť ochrany dát pred poruchami, živelnými pohromami, kriminalitou, vandalizmom, neoprávneným prístupom ako i ľuďmi, ktorí chcú neužitočným spôsobom dokazovať svoju intelektuálnu prevahu nad technikou. Ochrana dát si vyžaduje celú radu rôznych prostriedkov, techník, noriem, štandardov a postupov z dôvodu toho, že dáta je potrebné chrániť určitým spôsobom nielen proti neúmyselnému rušeniu, ale tiež proti ničeniu, sabotáži, zvedavosti a počítačovej kriminalite (čiže rušeniu úmyselnému). V systémoch pre spracovanie a prenos dát sa musí klásť dôraz na bezpečnosť a korektnosť spracovaných dát, na dodržiavanie oprávnenosti prístupu k dátam a práva na súkromie. Tieto aspekty by mali ovplyvniť návrh systému v mnohých podrobnostiach. Musia byť takisto následne sledované všetkými systémovými analytikmi a pracovníkmi, ktorí sú za prenos dát a ich spracovanie zodpovední. Technika obrany dát by mala byť jasná všetkým kontrolným pracovníkom a vedenie organizácie by si malo uvedomovať nielen všetky možné výsledky havarijných stavov, ktoré môžu nastať, ale malo by aj poznať relevantné spôsoby k ich prekonaniu. Nakoniec je potrebné zmieniť sa o morálnej zodpovednosti každého zamestnanca za ochranu a bezproblémový chod podniku. Ľudský faktor tu má primárnu

úlohu. Technická a softwarová nespoľahlivosť je koniec koncom výsledkom ľudskej činnosti. [3]

3.1 Informačná bezpečnosť podniku

Charakteristickým rysom novodobých organizácií je, že svoje poslanie plnia pomocou prepojenia informačných a komunikačných systémov budovaných na báze IT a to v rámci organizácie (intranet) ako aj s ostatnými organizáciami navzájom (internet). Tým sa jednotlivé činnosti organizácie stávajú silne závislé na relevantných informáciách a službách. Dôsledkom toho má strata dôveryhodnosti, integrity, dostupnosti, preukázania zodpovednosti, autenticity alebo spoľahlivosti informácií a s nimi spojených služieb značne nepriaznivý dopad na chod organizácie. Prvoradým opatrením je uplatnenie zásad bezpečnosti IT. Pojmom zabezpečovanie IT sa označuje proces dosiahnutia a udržania dôveryhodnosti, integrity, dostupnosti, preukázania zodpovednosti, autenticity a spoľahlivosti informácií a služieb IT na primeranej úrovni. Organizácia musí svoje informačné systémy zabezpečovať rovnako ako ostatné investície do svojej činnosti. Hardwarové komponenty sa dajú zničiť alebo ukradnúť. Ukradnúť sa dá aj software spravidla enormnej a pritom len odhadom vyčísliteľnej hodnoty. Konkurencii sa tým umožňuje ušetriť náklady na vývoj alebo nákup vlastného softwaru. Neoprávnené užívanie softwaru zamestnancom pre osobnú potrebu alebo pre ich druhé zamestnanie zas býva zdrojom ich nelegálnych ziskov. Naopak krádežou postihnutému prevádzkovateľovi vznikajú škody plynúce z trestnej zodpovednosti za porušenie licencie. Informačný systém môže byť ďalej použitý neautorizovane a tým spôsobiť zničenie systému alebo porušenie súkromia iných osôb (krádež prístupového hesla, prekonanie mechanizmu riadiaceho prístup k IS) poprípade možno IS využitkovať i autorizovanými zamestnancami k nepracovnej činnosti – či už osobnej alebo zárobkovej. Informácie sú vo svojej podstate tovarom, cenné aktíva pre organizáciu. Existujú právne, morálne a etické pravidlá pre používanie informácií, existujú zákonné úpravy pre ochranu dát, ktoré sa majú dodržiavať. Organizácia sa musí brániť zlomyseľnému i nezlomyseľnému odopretiu prístupu funkcií jej IS. V neposlednej rade sa ľudia majúci na starosti bezpečnosť musia zaoberať školiacimi aktivitami v tejto oblasti (kap. 8.2.3). [3]

3.1.1 Prvky informačnej bezpečnosti

Celkovú bezpečnosť informácií determinujú prvky v podobe stupňov ochrany najslabších článkov. Prvky informačnej obrany sú kategorizované do skupín;

Personálna bezpečnosť – ochrana IS z hľadiska jednania na základe konkrétnych udalostí spôsobených pracovníkmi, najmä z pohľadu prevencie. Personálna bezpečnosť musí byť zaisťovaná detektívnymi previerkami budúcich i súčasných zamestnancov podniku.

Režimová bezpečnosť - vytvorenie bezpečnostných pravidiel zásad práce s informáciami, dátami, komunikačnými a počítačovými systémami. Jedná sa o významný prvok prevencie, kde nepostačuje iba existencia pravidiel, ale hlavne nutnosť kontroly ich dodržiavania. Režimová práca zahrňuje režim práce s písomnosťami, režim ukladania dátových médií, vymedzenie okruhu osôb pre prácu s výberovými, dôvernými a utajovanými informáciami a dátami ako i opatrenia pre prípad mimoriadnych udalostí.

Bezpečnosť technických prostriedkov – výber, spoľahlivosť, kontrola prístupu a ochrana IS pred negatívnymi vplyvmi (elektrostatika, žiarenie, atď.). Technická bezpečnosť si vyžaduje realizáciu obrannej technickej prehliadky a vybavenie objektov monitorovacími zariadeniami. Prehliadky tiež zabraňujú únikom informácií po technických kanáloch.

Bezpečnosť programových prostriedkov – zaistenie kontroly prístupu k programom, autentickosť, identifikácia užívateľa, rozdelenie právomocí atď. Bezpečnosť softwarových prostriedkov má ďalej charakter obrany proti škodlivým kódom, proti zneužitiu programového vybavenia a proti zničeniu či poškodeniu softwarových vybavení.

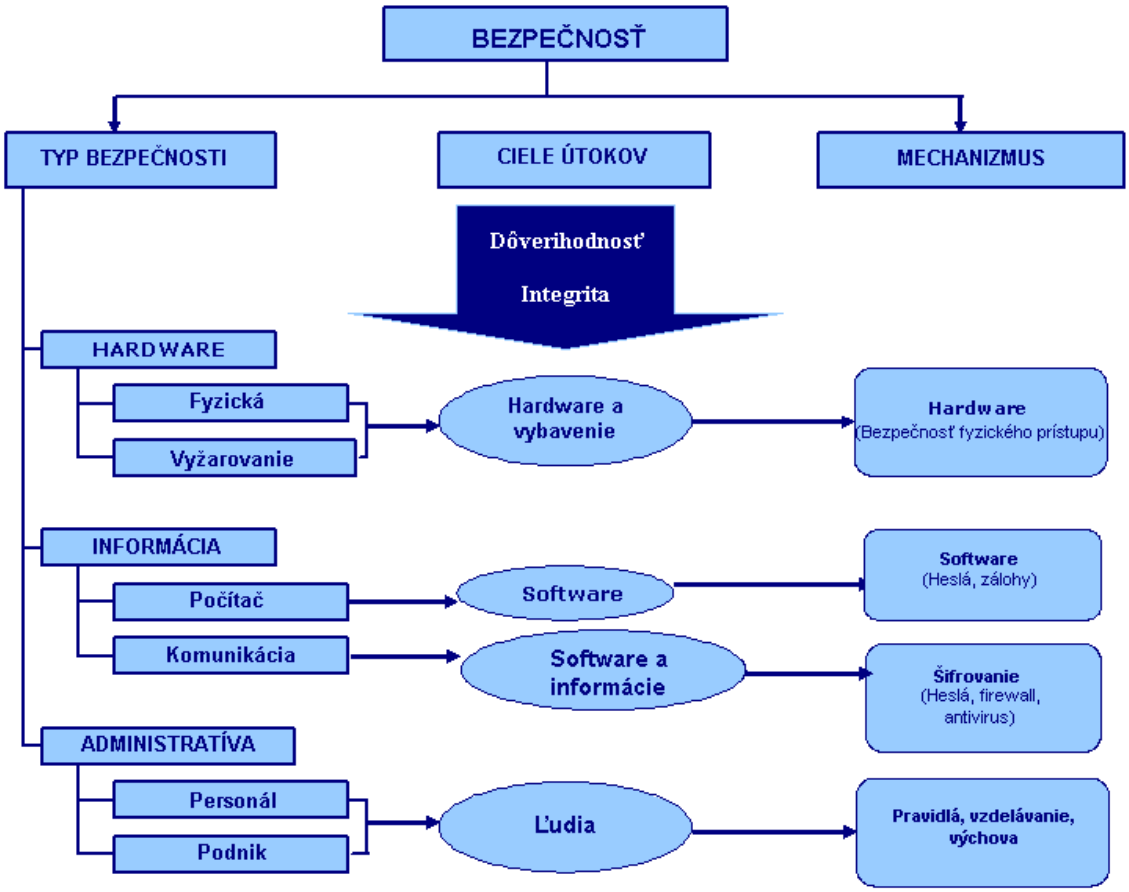
Bezpečnosť dát – ochrana dát v súboroch a databázach (elektronických i písomných), autorizácia, ochrana citlivých dát a rozlíšenie prístupov k týmto dátam.

Bezpečnosť komunikačných systémov a ciest – zaistenie ochrany medzi jednotlivými časťami komunikačných a počítačových systémov.

Fyzická bezpečnosť – ochrana informácií, dát, komunikačných a počítačových systémov proti neoprávnenému prístupu.

Aktívna ochrana proti úniku informácií a dát – ochrana proti priemyselnej špionáži / proti konkurenčnému spravodajstvu. Ide o systém opatrení smerujúcich k získaniu informácií o aktivitách konkurenčných útvarov zaoberajúcich sa konkurenčným spravodajstvom. Obranná zložka systému konkurenčného spravodajstva je významným a nezastupiteľným subsystémom v systéme situačnej a sociálnej prevencie kriminality a iných negatívnych

javov. Účinné zaistenie ochrany firmy pred únikom informácií je možno docieliť len adekvátnymi formami, metódami a prostriedkami detektívnej činnosti. Súkromné detektívne služby, či už firemné alebo komerčné, sú vhodným nástrojom ochrany ekonomických záujmov v podniku (viac kap. 7.1.1). [3]



Obr. 1. Prehľad subsystémov bezpečnosti

3.1.2 Personálne zaistenie bezpečnosti

Prvou otázkou, ktorá v súvislosti so zaistením bezpečnosti vo firme prichádza na um, je personálne zaistenie, t.j. kto to bude mať na starosti, kto za to bude zodpovedný. Príslušná osoba by mala byť členom vedenia firmy, mala by byť vybavená potrebnými právomocami k presadeniu svojich rozhodnutí. Označenie, ktoré je v skutku nové a nosí sa pre takého pracovníka, znie CISO. Hlavným poslaním riaditeľa bezpečnosti je analyzovať aktuálny stav a priebežne navrhovať zlepšenia. Za týmto účelom následne vytvára akúsi víziu spoločnosti v oblasti počítačovej bezpečnosti danej firmy – tzv. bezpečnostnú politiku IT.

Tá je súčasťou bezpečnostnej politiky organizácie (tzv. celková bezpečnostná politika), ktorá predstavuje súhrn bezpečnostných zásad a predpisov definujúcich spôsob zabezpečenia organizácie - od fyzickej ostražitosti, cez ochranu profesných záujmov, až po ochranu súkromia a ľudských práv. Prevádzkové presadzovanie bezpečnostnej politiky sa často označuje pojmom bezpečnostný program. Prostredníctvom svojich právomocí CISO zaisťuje úspešné zavedenie politiky do vnútro-firemnej praxe. Tento dokument by mal mať rozhodne písomnú podobu a mal by podľahnúť schváleniu najvyššieho vedenia. Dokumentov, z ktorých je vytváraná bezpečnostná politika, musí byť vypracovaných viac typov (diferenciácia pravidiel, právomocí a zodpovedností). Obecne platí pravidlo „menej je niekedy viac“ – smernice a postupy pre jednotlivých užívateľov by mali byť stručné a jasné. V prípade havarijnej situácie je CISO zodpovedný za čo najrýchlejšie, najefektívnejšie a najmenej finančne náročné vyriešenie problémov. Od jeho kvalifikácie sa preto okrem znalostí bežného riaditeľa IT navyše požadujú adekvátne manažérske kompetencie (predsa len riadi tým ľudí, a to v situáciách bežných, i krízových). Nemala by chýbať znalosť vnútrofiremných procesov a štruktúry organizácie obecne. Bezpečnostná politika má ako základný bezpečnostný dokument každej riadnej spoločnosti byť schopná odpovede na otázky;

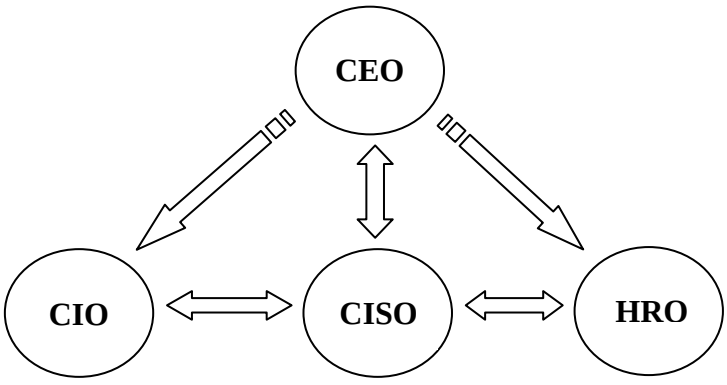
- čo chrániť
- prečo chrániť
- ako chrániť
- ako overiť, že je to naozaj chránené
- čo podniknúť, ak sa niečo pokazí

Nedeliteľnou súčasťou informačného systému, na ktoré sa útočí, sú aktíva v podobe dát a programov. Každé z nich je finančne ohodnotiteľné, v prípade incidentov sa dajú vyčísliť škody a straty z výsledku hospodárenia. Tvorba bezpečnostnej politiky preto znamená identifikovať všetky aktíva, ktoré budú chránené, ohodnotenie ich hodnota pre spoločnosť a stanovenie všetkých hrozieb, ktoré týmto aktívam hrozia. Investície do prevencie sú v konečnom dôsledku vždy lacnejšie než riešenie vypuknutých škôd. [3]

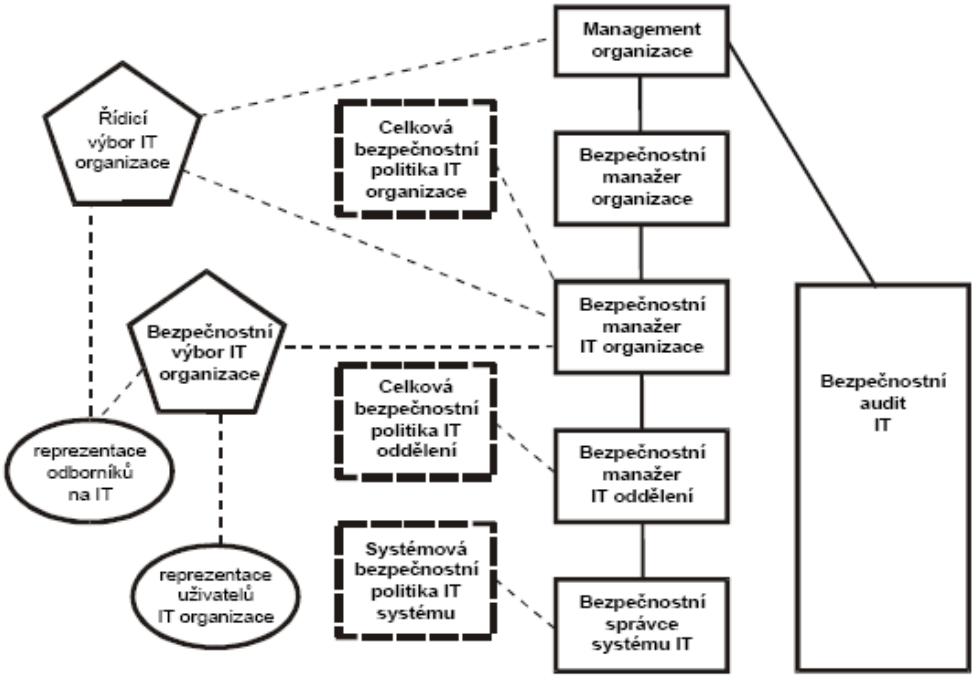
Je potrebné poukázať na to, že IS nie je nikdy úplne izolovaný, ale vždy je situovaný v nejakom prostredí. Toto prostredie tvoria jeho užívatelia, okolité počítače, ich siete,

fyzikálne javy (vlhkosť, prašnosť, teplota) avšak i spoločenská a ekonomická situácia. Samozrejmosťou je, že okolité prostredie IS nezanedbateľnou mierou ovplyvňuje samotné IS aj z bezpečnostného hľadiska, keďže v tomto prostredí existujú hrozby, ktoré je nutné definovať. Ale vzhľadom na globálnosť počítačovej siete nie je otázka prostredia tak jasná, ako kedysi. Systém umiestnený na prvý pohľad v prívetivom prostredí môže byť reálne prepojený s útočníkmi z takého prostredia, v ktorom je motivácia k útoku podstatne vyššia.

Pre prípad bezpečnostného incidentu či prírodnej katastrofy musia byť vypracované podrobné havarijne plány. V nich musí byť definované, pre aký účel sú určené (iný plán bude zhotovený pre útok hackera a iný pre boj s vodou), kto je za jeho plnenie zodpovedný, aké má právomoci a aké kroky v akom poradí sa majú podniknúť. Aby mali havarijné plány zmysel, musí byť pravidelne overovaná ich funkčnosť. Firma máva celú radu smerníc týkajúcich sa zákazu fajčenia alebo chovania sa k zákazníkom. Obvykle jej chýba nariadenie, ktoré stanoví chovanie v informačnom systéme, zodpovednosť za úmyselné i neúmyselné bezpečnostné incidenty a iné záležitosti z oblasti počítačovej bezpečnosti. CISO je ten, kto takéto smernice vytvorí a zaradiť ich do úvodného školenia pre nových zamestnancov, zaistí, aby sa s nimi oboznámili ostatní pracovníci, pravidelne monitoruje ich plnenie, vykonáva ich aktualizáciu a ďalšie činnosti, ktoré sú s tým spojené. Okrem toho je úlohou CISO sledovať v spolupráci s personálnym manažérom životný cyklus zamestnancov, dbať a definovať úkony prijatia nového zamestnanca, prepustenia starého, zmene pracovného miesta (povýšenie, degradáciu) a stanoviť nad tým všetkým dozor. Stáva sa totiž, že rada firiem zabúda rušiť prístupové práva do IS zamestnancom, ktorí opustili firmu. O rizikách a následkoch snáď nemá zmysel hovoriť. [3]



Obr. 2. Usporiadanie vzťahov topmanagementu modernej firmy



Obr. 3. Príklad bezpečnostnej infraštruktúry organizácie využívajúcej IS

3.2 Typy bezpečnostných politík

Existuje niekoľko foriem prístupu k zabezpečeniu IT. Niektoré sú zaujímavejšie z pohľadu nákladov, iné dosiahnutou transparentnosťou, ďalšie zas odolnosťou proti výnimočne silným útokom. Správny variant bezpečnostnej politiky IS má vychádzať z oponovanej a záväzne prijatej bezpečnostnej politiky organizácie. Podľa požadovanej úrovne zabezpečenia sa rozoznávajú bezpečnostné politiky štyroch obecných typov:

- ✓ *promiskuitná* - je bezpečnostná politika nikoho neobmedzujúca, každému v zásade povoľuje robiť všetko, žiaľ i vrátane toho, čo by robiť nemusel. IS s promiskuitnou bezpečnostnou politikou sú prevádzkovo nenákladné, často krát ani nenútia povinne používať autentizáciu použitím hesiel a tým zaručujú iba minimálnu prípadne žiadnu bezpečnosť. Jedným ospravedlňujúcim dôvodom používania IS s touto politikou môže byť ekonomické východisko alebo stav, že potrebná úroveň bezpečnosti je zaisťovaná prostriedkami mimo IT.
- ✓ *liberálna* – je bezpečnostná politika, ktorá každému povoľuje robiť čokoľvek až na činnosti explicitne zakázané. Liberálna bezpečnostná politika zaručuje väčšie bezpečie ako promiskuitná politika, je často uplatňovaná v prostrediach kde sa

hrozby považujú za málo až priemerne závažné a kde nepominuteľnou požiadavkou býva nízka ekonomická náročnosť bezpečnostného riešenia. Normálne sa opiera o zásadu voliteľného riadenia prístupu založeného na identite subjektov.

- ✓ *racionálna* – je bezpečnostná politika zakazujúca robiť všetko, čo nie je povolené. Racionálna (nazývaná tiež opatrná) bezpečnostná politika je nákladnejšia na zavedenie, avšak zaručuje vyšší stupeň bezpečnosti. Pri aplikácii na obecný IS požaduje vykonanie klasifikácie objektov a subjektov podľa ich schopností a citlivosti. Je opretá mimo iné o zásadu povinného riadenia prístupu založeného na rolách, v ktorých vystupujú subjekty pri styku s IS. Z hľadiska používania IS v Internete je obvykle počiatočnou bezpečnostnou politikou.
- ✓ *paranoidná* – je bezpečnostnou politikou zakazujúcou robiť všetko potenciálne nebezpečné, aj to, čo by nemuselo byť explicitne zakazované. Zaručuje najvyšší stupeň bezpečnosti. Napr. zakáže používať akékoľvek internetové služby, resp. predpíše používať IS bez možnosti on-line napojenia na komunikáciu. Vedie k maximálnej izolácii systému. I tak môže byť paranoidná bezpečnostná politika užitočná pre mnoho organizácií. Databázový systém spracovávajúci vysoko dôverné informácie možno fyzicky a technicky izolovať na systém s konečným počtom ľahko sledovateľných vstupov a výstupov. Paranoidný charakter bezpečnostnej politiky umožňuje implementáciu v prostredí s nízkou systémovou réžiou, čiže s dosiahnutím vyššej výkonnosti pri zachovaní nižšej úrovne nákladov.

Za zmienku stojí rozlišovať tzv. *celkovú* a *systémovú* bezpečnostnú politiku. Celková bezpečnostná politika uvádza špecifikáciu cieľov zabezpečenia, definíciu a klasifikáciu citlivých dát vrátane zodpovedností. Definuje bezpečnostnú infraštruktúru organizácie a potrebné sily mechanizmu pre implementáciu bezpečnostných funkčností, špecifikuje obmedzenia, ktoré je nutné rešpektovať a je vytváraná nezávisle na práve používaných informačných technológiách. V podstate má táto politika podobu verejného záväzného dokumentu – normy, ktorého cieľom je ochrana majetku, povesti a činnosti organizácie. Systémová bezpečnostná politika IT definuje spôsob implementácie celkovej bezpečnostnej politiky v konkrétnom prostredí. Zaoberá sa voľbou konkrétnych technických, procedurálnych, logických a administratívnych bezpečnostných opatrení. [3]

3.3 Ochrana dát

Všetky informačné systémy sú založené na využívaní istej báze dát. Ku každým dátam je z hľadiska ich ochrany potrebné pristupovať individuálne. Rozlišuje sa trojica nebezpečenstiev;

- kompromitácia (prezradenie)
- modifikácia (neoprávnená zmena)
- zničenie (úmyselná či neúmyselná likvidácia)

Samotná ochrana dát sa z rôznych hľadísk delí na niekoľko skupín. Pre účinnú ochranu sa tieto skupiny majú vhodným spôsobom kombinovať. Podľa prvkov, ktoré je potrebné chrániť, sa definujú tieto skupiny;

- *ochrana fyzického prístupu k nosičom dát* – predovšetkým ide o zabezpečenie proti neoprávnenému prístupu osoby (zamestnanca) k diskom a zálohovým médiám
- *ochrana logického prístupu k dátam* – zabránenie prieniku k dátam obídením bezpečnostného softwaru alebo nabúraním sa prostredníctvom intranetu
- *ochrana uložených dát* – ochrana proti nežiaducemu prečítaniu dát, napr. pri situácii krádeže disku a snahy získať uložené informácie jeho inštalovaním do iného počítača
- *ochrana dát prenášaných počítačovou sieťou* – zabezpečený prenos dát
- *ochrana dát pred zničením* – prírodné katastrofy, požiar objektu, terorizmus

Samotné dáta v informačnom systéme sa klasifikujú podľa závažnosti ich ochrany do niekoľko skupín. Je samozrejmé, že textové súbory užívateľov nebudú chránené rovnako ako databáza prístupových hesiel. Iný dôraz sa kladie na dáta užívateľov iný na auditné záznamy, spustiteľné kódy či autentizačné informácie. [3]

3.3.1 Obmedzenie fyzického prístupu

Kontrola prístupu začína už pri vstupe do budovy, na parkovisku alebo inom priestranstve pred objektom. Vo väčšine prípadov za ňu zodpovedá vrátnik či recepčný kontrolujúci oprávnenie osôb. Rada objektov disponuje automatickým dverným systémom vybaveným zariadení pre čipové alebo magnetické karty. Okná i dvere bývajú chránené snímačmi pohybu, po objektoch sú rozmiestnené bezpečnostné kamery. Obraz z kamier je obvykle

vedený na monitor ostražitosti (bezpečnostnej služby) alebo sa ukladá na video záznam. Dôvod opatrení je prostý – mať kontrolu nad tým, kto sa v objekte pohybuje. Oprávnení zamestnanci majú byť pri vstupe registrovaní do zoznamu vytváraným buď automaticky (čipové / magnetické karty) alebo rekonštrukciou (na základe dochádzkových kariet a i.), pre návštevy má byť určená návštevná kniha so záznamom doby príchodu a odchodu. Neoprávnených návštevníkov pomôžu v lepšom prípade zachytiť bezpečnostné kamery. IS bývajú v poriadnych moderných firmách umiestňované do uzamykateľných miestností, najlepšie bez okien a v čo najvyššom možnom poschodí budovy. Pokiaľ ide o skrine, je jasné, že bežné skrine ATX bezpečnostným podmienkam nevyhovujú. Disky s citlivými údajmi majú byť inštalované do skríň zaistených štandardným bankovým sejfom. [3]

3.3.2 Obmedzenie logického prístupu

Je v poriadku, ak sa operačný systém snaží nainštalovanými prostriedkami ochrániť prístup k dátam uložených na diskoch. Vykonáva to cez nakonfigurované prístupové práva jednotlivých užívateľov. Dnes je k overeniu identity nutné i predloženie dostačujúceho dôkazu, čo riešia tzv. autentizačné metódy - dôkaz znalostí (užívateľské heslo), dôkaz vlastníctvom (bezpečnostný predmet, napr. token) a dôkaz unikátnej telesnej vlastnosti (napr. biometrika). Autentizačný protokol následne použije získanú informáciu k tomu, aby presvedčil server o identite užívateľa. Hneď ako je užívateľovi systému pridelená virtuálna identita, je systému pre riadenie prístupu dovolené začať pracovať. Len správne nakonfigurovaný systém, funguje spoľahlivo. [3]

3.3.3 Obrana uložených dát

V poslednej dobe sa veľmi veľa hovorí o sociotechnikách a sociálnom inžinierstve. Je to hlavne z dôvodu zlyhania lojality či inej ľudskej vlastnosti, ktorej sa prakticky nedokážeme aktívne ubrániť, ktorá dokáže významne narušiť bezpečnosť. Príkladom je situácia, kedy útočník podplatí vrátnika, čím sa dostane k citlivým firemným dátam. Jedna existujúca alternatíva obrany je šifrovací algoritmus. Kryptografia (šifrovanie) sa požíva súborovo offline (zip), súborovo online (pgp) a komplexne (zašifrovanie celého disku). Správnou motiváciou sa má usilovať o získanie dôvery svojich zamestnancov (viac 8.2.4). [3]

3.3.4 Obrana dát prenášaných počítačovou sieťou

Dáta sú zraniteľné akonáhle opustia svoje prirodzené prostredie. Dochádza k tomu pri prenose na elektronických médiách (CD, diskety, zálohovacie média), prenose na papierových médiách (výtlačky, kópie faxových správ) a prenose počítačovou sieťou (elektronická pošta, FTP). Proti modifikácii zasielaných dokumentov je najlepší digitálny odtlačok, tzv. hash. Je to v podstate kontrolný súčet, ktorý vypočítame pred odosielaním dát. Príjemca si sám vypočíta zo získaných dát súčet a obe hodnoty porovná. Pokiaľ tieto dve údaje súhlasia, znamená to, že dáta v priebehu prenosu nikto nezmenil. Prikladaný hash je z bezpečnostných dôvodov zašifrovaný súkromným kľúčom odosielateľa, aby sa predišlo jeho editácii útočníkom. Rozšifrovanie uskutočňuje príjemca verejným kľúčom odosielateľa. Celý tento postup sa odborne označuje pojmom digitálny (elektronický) podpis. Dáta vo firme musia byť chránené pred kompromitáciou nasadením takého protokolu, ktorý dáta nielen zašifruje, ale súčasne im zaisti potrebnú integritu. K tomu je nevyhnutná spolupráca správcov siete na oboch stranách. [3]

3.3.5 Obrana dát pred zničením

K zničeniu dát dochádza dvoma spôsobmi; dáta sú zmazané, poškodené priamo na svojom nosiči alebo je fyzicky zlikvidovaný vlastný nosič. Prvý prípad nastáva chybou systému, zlomyseľnosťou užívateľa či systémovou chybou. Druhý fyzickým útokom alebo prírodnou katastrofou. K obom prípadom bežne dochádza napriek rôznym zabezpečovacím krokom.

Základnou metódou ochrany dát proti zničeniu je ich systematické zálohovanie. V prípade zničenia pôvodného média sú dáta dostupné z obnovenej zálohy. V dnešnej dobe sú už k dispozícií prepracované systémy, ktoré sa o zálohovanie dát starajú automaticky, dokážu si stiahnuť potrebné dáta, zašifrovať ich a pod. Niektoré z nich sú natoľko inteligentné, že zálohujú iba tie dáta, ktoré sa zmenili od poslednej zálohy. Na druhej strane je veľkou nevýhodou zálohovacích zariadení práca so záložnými kópiami. Dosť často sa stáva, že kópie ostávajú v týchto zariadeniach, umiestnených hneď vedľa servera, ktorého dáta sú zálohované. Záložné kópie si preto vyžadujú samostatné uloženie. To je základné pravidlo zálohovania, ktoré si kladie náročný cieľ – zaistiť, aby pri zničení pôvodných dát neboli zničené i záložné kópie. Ideálnym riešením je ich umiestnenie pokiaľ možno v inej budove, najlepšie vo vode a požiaru odolnom sejfe. Pri zostavovaní bezpečnostnej politiky

tej či onej firmy sa veľmi často zabúda na fakt, že údaje uložené na záložnom médiu predstavujú totožné dáta s tými, ktoré firemný IS pomocou softwarových a hardwarových riešení precízne chráni. CISO by teda nemal zabúdať na dôslednú evidenciu záložných kópií, ktorá zabráni chaosu kópiám s dennou periodicitou. Dôležité je vedieť, ktoré kópie sú ešte potrebné a ktoré už boli premazané novšími zálohami. Evidencia rovnako pomôže pri likvidácií zálohových médií s citlivými dátami. V prípade poškodenia disku alebo jeho významnej časti vykoná bezpečnostný management obnovu zo zálohy, čím sa vyhne nežiaducim finančným stratám, stratám firemného tajomstva atď. Je nevyhnutné uskutočňovať pravidelné testy schopnosti dáta obnoviť. Zaujímavou možnosťou ochrany dát je duplikovanie ich nosičov. Pravdepodobnosť, že dôjde k súbežnej poruche dvoch diskov je pomerne malá. Duplikáciu zaisťuje buď operačný systém programovými prostriedkami alebo špeciálny hardwarový radič, ktorý je rýchlejší. [3]

4 SYSTÉMY OBRANY MODERNÝCH PODNIKOV

Na obranu proti útočníkom sa využívajú hardwarové a softwarové nástroje. Budujú sa systémy organizované do mnohorakých štruktúr za účelom efektívneho zabezpečenia prenosu dát a uchovania znalostí. V poslednom čase sa veľa diskutuje o koncepcii tzv. deperimetru, ktorú navrhuje organizácia Jericho Forum. Zastáva myšlienku odpútať sa od budovania niekoľkých vrstiev firewall a masívnych bezpečnostných „hradieb“ stavaným proti vonkajším útokom a miesto toho považuje celý intranet za nepriateľský. Proti sebe tak stoja jednotlivé počítače vyzbrojené o potrebné bezpečnostné prvky. Systémy obrany moderných podnikov úzko korešpondujú s utvorenou bezpečnostnou politikou IT. Len tá činí informačnú bezpečnosť priehľadnou. Dodržiavanie kritérií vychádza zo stanoveného využívania predurčených softwarových a hardwarových riešení. O aké, v podnikoch a verejnej správe najčastejšie využívané metódy sa jedná, ukazujú nasledujúce kapitoly.

4.1 Šifrovanie

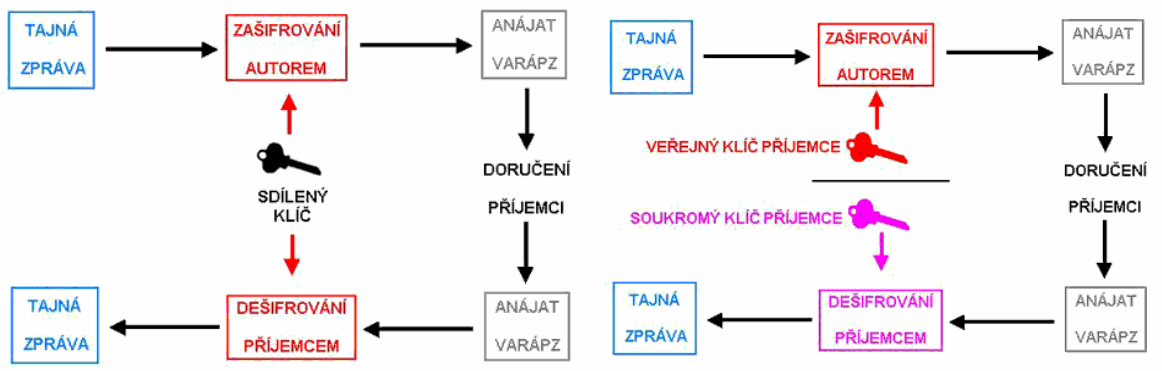
V informačnom veku sa informácie stávajú najcennejším tovarom. Deň čo deň putujú po informačných cestách stovky miliónov e-mailov. Bezpečná výmena digitálnych informácií je dnes prioritnou súčasťou internetového obchodovania a internetového bankovníctva. Problémom dnešnej komplexnej informačnej spoločnosti však ostáva, že sa príliš sústreďuje na ochranu proti externým útokom. Do tejto oblasti smerujú bezpečnostné politiky, nákupy technológií, mieria sem prakticky všetky otázky na bezpečnosť. Vývoj v poslednej dobe ale naznačuje, že je to veľkou chybou. Fyzickú bezpečnosť nikdy nezaistíme tak, ako by sme potrebovali. Pravdepodobnosť vyzradenia tajomstva naviac rastie s počtom osôb, ktoré tajomstvo zdieľajú. Ochrana znalostí je preto silne závislá na možnostiach špecializovaného oboru počítačovej vedy – kryptografie. V uplynulom storočí bolo šifrovanie významné hlavne pre vládne orgány a armádu, dnes je esenciou pre obchod, finančníctvo ako aj bežný život, keď vďaka elektronickému podpisu zastáva významnú rolu v ochrane súkromia. Koniec koncom, šifrovanie je najjednoduchším (a často i najúčinnejším) spôsobom ochrany informácií v súčasnosti.

4.1.1 Princíp šifrovania

Šifrovanie (kryptografia) je v podstate transformácia dát do nečitateľnej podoby. Dešifrovanie je postup opačný, teda transformácia šifrovaných dát do ich pôvodnej,

zrozumiteľnej podoby. Šifrovanie sa uskutočňuje pomocou kľúčov, ktorých zmysel je ten istý ako u bežných kľúčov od auta či domu. Rozdiel je v podstate – šifrovací kľúč obsahuje dáta, obvykle reťazec alfanumerických znakov. [4]

Obsahom tejto práce nie je podrobne opisovať zložitú metodiku šifrovania, následný graf však ozrejmí túto problematiku do úrovne, ktorá poslúži k porozumeniu ďalších kapitol.



Obr. 4. Symetrické a asymetrické šifrovanie dát

4.1.2 Pretty Good Privacy (PGP)

Phil Zimmermann, tvorca najpoužívanejšieho šifrovacieho programu pre emailovú komunikáciu, si dôležitosť ochrany uvedomil skôr než hocikto iný. Zimmermannovo riešenie silnej a pritom ľahko dostupnej šifry vychádza z pomerne jednoduchej myšlienky. PGP je kombinovaný šifrovací systém. Pokiaľ chce odosielateľ zaslať šifrovanú správu príjemcovi, začne tým, že zašifruje symetrickú šifru – tzv. IDEA. K šifrovaní pomocou IDEA musí odosielateľ zvoliť kľúč. Aby mohol príjemca správu dešifrovať, potrebuje k nemu odosielateľ nejakým spôsobom dostať tento kľúč. Odosielateľ problém vyrieši tak, že si vyhľadá príjemcov verejný kľuč pre RSA, ktorý potom použije pre zašifrovanie kľúča k IDEA. Odosielateľ teda nakoniec odosiela dve veci; správu zašifrovanú symetrickou šifrou IDEA a kľúč k IDEA zašifrovaný asymetrickou šifrou RSA. Na druhom konci príjemca použije svoj súkromný kľúč RSA, aby dešifroval kľúč IDEA a týmto kľúčom k IDEA potom dešifruje vlastnú správu. Na prvý pohľad sa to zdá byť komplikované, to ale nemení nič na tom, že je to veľmi rýchla a bezpečná metóda. Správa, ktorá je zašifrovaná symetrickou šifrou môže obsahovať obrovské množstvo informácií, zatiaľ čo kľúč, zostávajúci z malého množstva informácií je zašifrovaný pomalou asymetrickou šifrou.

PGP bolo vydareným produktom, niet divu, že jeho autor musel čeliť krivému trestnému stíhaniu a ďalším obvineniam zo strany vlády USA. [12]

4.2 Autentizačné systémy

Heslá, akokoľvek sú široko používané, narážajú na dva základné problémy; sú zdieľatelné a dajú sa ukradnúť. Najzávažnejšie ale je, že ak sa nejakým spôsobom naruší bezpečnosť hesla, jeho držiteľ si toho obvykle ani nie je vedomý. Na tieto problémy ponúkol IT priemysel dve riešenia. Prvé z nich predstavuje autentizáciu založenú na tokenoch, druhým sa stala biometrika. Oba systémy so sebou nesú klady i nedostatky. Na zdokonaľovaní týchto autentizačných systémov sa ešte len pracuje. Napriek obmedzeniam ich niektorí odborníci odporúčajú. Základnou motiváciou pre používanie tokenov a biometriky je ľahká náhrada skompromitovateľných hesiel. Keďže žiadny z týchto prostriedkov nepoužíva to isté heslo dvakrát, sú tokeny odolné voči trojanom (keyloggers) a užitočné proti tým, ktorí radi špehujú cez rameno. [10]

4.2.1 Tokeny

V oblasti preukazovania identity pre vzdialené systémy a servery dnes jasne víťazia autentizačné tokeny. Dajú sa používať spolu so širokou škálou variant systému a ich implementácia je jednoduchá. Náklady s nimi spojené rastú skôr s počtom užívateľov než s počtom miest, kde sa užívatelia potrebujú autentizovať. Systémy založené na tokenoch tiež vyžadujú najmenšiu nutnú mieru zaškolenia a užívatelia pomerne rýchlo spozorujú, ak token stratia alebo im ho ukradnú. Zariadenie obsahuje buď displej s číslami alebo len USB konektor. Každý token sa vyznačuje unikátnym výrobným číslom a vlastným typom utajeného kódu. Asi najznámejším je token SecureID od spoločnosti RSA Security. Máva malý LCD displej o ôsmych číslach, ktoré sa každú minútu menia. Preto nevadí, ak užívatelia zabúdajú heslo. Pri prihlasovaní sa k vzdialenému počítaču, sa vloží najprv užívateľské meno, heslo a číslice, ktoré v danú chvíľu zariadenie ukazuje. Vzdialený PC informácie prevezme a odošle ich do autentizačného serveru, ktorý matematicky porovná údaje. Pokiaľ vypočítané heslo súhlasí so zadaným, prístup je povolený. I keď je SecureID na trhu už viac ako desať rokov, do povedomia sa dostal len nedávno vďaka rozšíreniu útokov typu phising a pharming. Široko sa využívajú na rôznych konferenciách a podujatiach, avšak zabudnúť ho doma pred takouto akciou nebýva nič príjemné. [10]

Špeciálnym druhom tokenov sú tokeny založené na kryptografii verejného kľúča (tzv. kryptografické tokeny). Token sám vytvorí pár kľúčov, z ktorej verejný kľúč je certifikovaný (podpísaný organizáciou) a tento certifikát sa uloží na token. Autorizácia prístupu sa uskutoční vzdialenou službou automaticky. Bezpečnosť tohto prístupu spočíva v tom, že súkromný kľúč token nikdy neopúšťa. Po jeho vytiahnutí z USB portu nie je pravdepodobné, že by sa niekto mohol vydávať za držiteľa tokenu a nejakým spôsobom prihlásiť pod pravým účtom. Istá hrozba, že si ho niekto neoprávnene požičia z kancelária jeho majiteľa tu však je (podobne ako u hesla). [10]

4.2.2 Biometrika

Systémy založené na biometrike fungujú najlepšie v prostredí, kde sa požaduje stála fyzická kontrola prístupu. Majú plus v tom, že odtlačok prstov sa zdieľať nedá Napriek tomu, že je obsluha biometrického senzora jednoduchá, má táto forma autentizácie istý háčik. Niektorí handicapovaní zamestnanci nebudú schopní systém používať ledaže by pre nich bola vytvorená alternatíva. Zistilo sa, že väčšina detí, ázijské ženy a starší ľudia mávajú problémy s čítačkami odtlačkov prstov, pretože ich prsty sú príliš malé prípadne ich línie príliš jemné. Stáva sa, že niektorí ľudia nemajú ruky. Ani biometrika však nie je stopercentná. Totižto tak, ako sa od seba môže líšiť fotografia tváre, tak sa od seba môže odlišovať aj odtlačok prstov. Preto majú biometrické systémy komplikované algoritmy, ktoré uskutočnia dvojité meranie a potom sa pokúsia stanoviť, či je zhoda dostatočná. Biometrické systémy majú svoje nedostatky. Nedokážu si poradiť s tzv. „fuzzy“ akceptom (prípad, že má niekto špinavé / zaprášené ruky). Ak sa biometrický snímač nakonfiguruje tak, aby prepúšťal i ľudí, ktorí majú z času na čas špinavé ruky, zvyšuje sa pravdepodobnosť chybného porovnania (FAR), na druhej strane sa však zvyšuje tzv. FRR pravdepodobnosť chybného odmietnutia. Medzi ďalšie nevýhody systému patrí jej nedemokratickosť. Niektorí ľudia ju môžu používať bez problémov, ďalší s ťažkosťami a ostatní sa autentizácie biometriky nemôžu zúčastniť vôbec. Posledná skupina ľudí sa radí do tzv. FTE, percenta prípadov neschopných zapojenie do systému. Ak sa užívatelia do systému môžu zapojiť, ale ten z nejakého dôvodu zlyháva práve v okamžiku verifikácie, hovoríme o tzv. FTV. [10]

Biometrika je mladý obor, ktorý sa vyznačuje úplným nedostatkom štandardizácie. Každý rok sa v tejto oblasti objavuje nejaká novinka a CISO ju musí vždy otestovať na FAR, FRR, FTE a FTV. Systém, ktorý vykazuje FTE v oblasti 1 percenta, môže vyhovovať

spoločnosti s 500 zamestnancami, kde tí zvyšní piati obdržia napríklad USB tokeny. Systém by nikdy nebol vhodný ako základ národného identifikačného systému, ktorý by mal certifikovať totožnosť 100 miliónov ľudí. Nakoniec, sfalšovať sa dá aj odtlačok prstu – v Japonsku pomocou špeciálnej želatíny odkopírovali prst s odtlačkom a oklamali tým väčšinu komerčných čítačiek. Systémy založené na rozpoznávaní rysov tváre sa takisto podarilo nachytať priložením fotografie osoby, ktorú malo zariadenie identifikovať. Testovať takéto útoky znie možno zábavne, ale horšie to je v prípade, ak užívateľ leží s horúčkou v posteli a potrebuje, aby sa jeho asistentka dostala k počítaču a vytlačila mu poštu. [10]

Hoc sa budeme v nasledujúcich rokoch s biometrikou pravdepodobne stretávať viac a viac, zatiaľ tieto systémy fungovali neúspešne. Biometrika je dobrou alternatívou k heslám. Pre radu aplikácií sú jednoduchším a zároveň demokratickejším riešením tokeny.

4.3 Aktívna programová obrana

Podľa druhu hrozby rozoznávame predovšetkým nasledovné, na trhu informačných technológií poskytované, obranné nástroje:

- *antivírus* (Norton, NOD, AVG, Avast, McAfee, Kaspersky, Panda, F-Secure a i.)
- *antispyware* (Microsoft, Lavasoft, Safer Networking, Webroot, PC Tools a i.)
- *antiphising* (Cloudmark, Netcraft, Nobox a i.)
- *firewall* (Norton, Sygate, ZoneAlarm, AVG, Kerio, Microsoft, Outpost a i.)
- *updates / patches* (Microsoft, Adobe a i.)

Všetky moderné antivírové produkty disponujú pokročilou aktualizáciou, heuristickou analýzou a všestrannou rezidentnou ochranou. Dnes je chýbajúca prítomnosť antivírusu na počítači, ktorý je pripojený k sieti (všetky PC v organizáciách) absolútny nezmysel. Antispyware je obdobne odpoveďou na expanziu trojanov, wormov, malwaru a iných nebezpečenstiev šíriacich sa nežiaducou poštou či parazitujúcich na nevhodných stránkach. S príchodom phisingu a phamingu sa vyvinuli samostatné nástroje, ktoré možno integrovať do browsera, najmä „vždy deravého“ Internet Exploreru. V súčasnosti je rada antiphisingu ešte len vo vývoji. V najbližšom období sa dá očakávať ich štandardná súčasť webového

prehliadača. Firewall je už súčasťou Windows i keď samostatné riešenia obvykle garantujú účinnejšiu mieru protekcie. Akousi formou liečby kontinuálne objavovaných nedostatkov operačného systému sa javia záplaty poskytované jeho výrobcom. V prostredí Windows sa tým myslí klasická služba Windows Update, kde Microsoft každé dva týždne vydáva svoj vlastný bezpečnostný balík.

4.4 RSA Conference 2006 a všeobecné bezpečnostné trendy

Kam sa bude v blízkej budúcnosti uberať vývoj v oblasti zabezpečenia firiem je často kladenou otázkou. Na konferencii RSA 2006 Microsoft uviedol štyri základné strategické iniciatívy - vytvorenie bezpečnostného ekosystému, bezpečnostného inžinierstva, zjednodušenie riešení a vytváranie bezpečnostných platforiem. Podľa Billa Gatesa ide v prvom rade o užívateľov, ktorí musia chápať bezpečnosť ako bežnú súčasť svojej práce. Vzrastie význam certifikátov, ktoré budú tvoriť jednu z hlavných potvrdení toho, že webové stránky patria skutočne tomu, kto je na nich uvedený. Čo sa týka inžinieringu bezpečnosti, konferencia poukázala najmä na rôzne nástroje a inovatívne postupy, ktoré sú využiteľné k vytváraniu bezpečnostného kódu. Príkladom môže byť prostredie OneCare vo Windows Vista alebo služba InfoCard.

RSA na konferencii predstavila panel RSA SecureID Toolbar Token. Jedná sa o riešenie postavené na báze pseudonáhodných čísel, ktoré užívateľ využíva pre potvrdenie, že je oprávneným uskutočňovať transakcie. Vygenerovanie kódu je viazané na ďalšie heslo či PIN. Toolbar je v súčasnosti dostupný ako voliteľný komponent pre browser Internet Explorer a Firefox čím má zabraňovať neoprávneným osobám pristupovať na firemný web.

Spoločnosť SanDisk predstavila USB flash disky a prenosové pamäťové karty, ktoré obsahujú zabudovaný nástroj pre šifrovanie v reálnom čase. Dáta sú tak okamžite zabezpečené proti zneužitiu a obsah USB diskov budú môcť využívať len jeho príslušný majitelia. Pokiaľ sa USB disk dostane mimo firmu, je jeho obsah nečitateľný.

Rozmach zaznamená nový odbor Business Intelligence (ďalej len BI). Termín reprezentuje nástroje a systémy, ktoré hrajú kľúčovú rolu v plánovaní strategických procesov v podniku. Príslušný BI software umožňuje spoločnosti zber, ukladanie, sprístupnenie a analýzu dát za účelom prijímania rozhodnutí. Budúcnosť BI bude výhradne v rukách finančných riaditeľov. Firmy budú i naďalej pracovať so záplavou dát, stretávať sa so

zlučovaním trhu a snažiť sa vyhovieť vládnym predpisom. Organizácie vyzbrojené prediktívnou analýzou budú schopné lepšie odhadovať budúce chovanie udalostí a tým sa vopred posilňovať. Výsledkom bude konkurenčný náskok.

Z hľadiska hrozieb sa vo všeobecnosti očakávajú nárast incidentov, pričom útoky už nebudú zamerané len na operačný systém Microsoftu, ale terčom sa stanú i ďalšie aplikácie a prvky infraštruktúry. Spyware bude stále predstavovať ohromný problém a tak sa bude viac investovať do antispywarovej obrany. Široký rozmach P2P sietí a korešpondencie správ vystaví organizácie celkom novým hrozbám. Ťažiskom sa budú stávať riešenia, ktoré okrem ochrany pred vírmi a spyware zaistia dodržiavanie bezpečnostných zásad a šifrovania. V súlade s globálnym trendom správnych riadiacich postupov budú predstavenstvá firiem venovať väčšiu pozornosť ochrane informačného majetku. Rozšíri sa technológia VPN a systémy koncových bodov. [12]

5 ŠKODLIVÝ KÓD A JEHO CHARAKTERISTIKA

Na tému škodlivý kód existuje celá rada literatúry a dala by sa o tom napísať samostatná bakalárska práca. Keďže táto si kladie za cieľ byť akýmsi elementárnym IT bezpečnostným manuálom pre organizácie, len stručne charakterizuje formy moderného nežiaduceho kódu. Dnes existuje hromada malwaru a vírov vygenerovaných pre súdobé počítačové systémy. Ich počet a zložitosť neustále rastie a antivíroví programátori a vývojári aktualizačných balíčkov majú čim ďalej tým viac práce. Ak sa niekedy aktualizovala databáza antivírového programu raz mesačne, bola to významná služba zákazníkom, na ktorú sa túžobne čakalo. V súčasnosti je nevyhnutnosťou a samozrejmosťou updatovať počítač každé dva-tri dni, a to sa netýka len antivírového bezpečnostného produktu, ale i rady iných (antispyware, antiphising, firewall). Popri tom sa odporúča, aby každý zamestnanec podniku preventívne ovládal názvoslovie potenciálnych hrozieb. Praktický prehľad termínov, poprípade slovných spojení, ktoré sa môžu počas pracovnej doby vyskytnúť v systémovom hlásení je nasledovný;

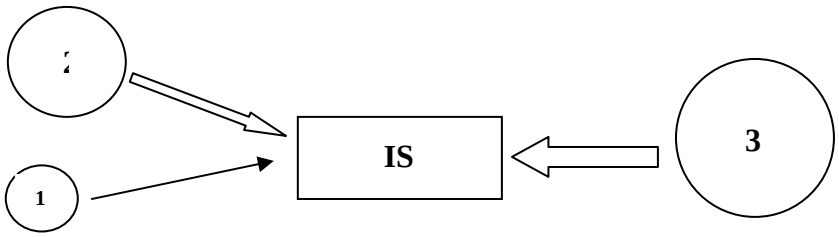
- ✓ *vírus* – najznámejší prípad infekcie kde sa telo víru pripojí k spustiteľnému zdravému súboru čím sa stane jeho súčasťou (pri aktivácii súboru sa najprv aktivuje samotný vírus, liečenie = zmazanie, pôvodný súbor ostáva nepoškodený)
- ✓ *trojan* – obecný pojem, kedysi škodlivý program tváriaci sa nevinne (užitočne)
- ✓ *backdoor* – tzv. zadné vrátka, umožňuje vzdialene prevziať kontrolu nad počítačom
- ✓ *downloader* – škodlivý kód, ktorého úloha je sťahovať víry a červy
- ✓ *dropper* – škodlivý kód, ktorý prenáša vírus a ten vypúšťa do PC pri bootovaní
- ✓ *worm (červ)* – všeobecný pojem, v súčasnosti označuje kód šíriaci sa paketmi
- ✓ *adware* – aplikácia na podporu e-marketingu, spôsobuje vyskakovanie reklamy
- ✓ *spyware* – špionážny software, ktorý vysiela informácie, heslá, atď.
- ✓ *crimeware* – skupina programov, ktorých cieľ je finančná a obchodná kriminalita
- ✓ *dialer* – nepríjemná aplikácia, ktorá má za následok vysoké účty za tel. linku
- ✓ *spam* – nevyžiadaná pošta v podobe nigérijských dopisov, phisingu, reklamy, a i.
- ✓ *scumware* – pojem pre celkové označenie nežiaduceho softwaru prítomného na PC

6 POČÍTAČOVÁ KRIMINALITA A ODCUDZENIE DÁT

„Keďže svet, v ktorom je každý spravodlivý a úprimný, je stále v nedohľadne, prihováral by som sa za to, aby sa všetci pracovníci legislatívy i justície poriadne preškolili alebo aspoň absolvovali čosi ako kurz *Úvod do sveta internetu*.“ (Patrick M. Kolla, autor Spybot S&D) [12]

6.1 Hacking

Hacking sa dá definovať ako zámerné získanie neautorizovaného prístupu k informačnému systému. V extrémnych prípadoch zastupuje navonok priemyselnú špionáž alebo aj národný bezpečnostný zločin. Oddávna sú na informačné systémy podnikané útoky. Podľa nebezpečnosti útokov delíme útočníkov do troch skupín. V prvom rade sa jedná o amatérov[1], čiže skupinu ľudí, ktorí vlastne iba skúšajú, aké to je. Niekde na internete našli popis jednoduchého útoku a tak si ho vyskúšajú na vašej spoločnosti. Účinné bývajú jednoduché bezpečnostné opatrenia. Nebezpečnejšou skupinou sú hackeri[2] – značne kvalifikovaný, často vysokoškolský študenti. Ich limit je daný časom a prostriedkami. Ich nebezpečenstvo je cítiteľné, a väčšina z nich to už nerobí len pre zábavu, ale s úmyslom škodiť (cracker). Poslednou a problematickou skupinou sú profesionáli[3], ktorí za to dostávajú zaplatené od IT gigantov. Na druhej strane zakladajú gangy a špecializujú sa na veľké firmy. Obrana voči nim je nákladná a často aj nedostupná. [3] [6]



Obr. 5. Klasifikácia útočníkov podľa rozsahu škôd

6.2 Interné útoky

Interné útoky predstavujú takú formu útokov na IS organizácie, kde hlavným vinníkom je niekto z jej vlastných pracovníkov prípadne votrelec využívajúci metódy sociálneho inžinierstva. Útoky môžu byť úmyselné i neúmyselné, každopádne na rozsahu škody to nič nemení. Dnešná architektúra bezpečnosti IS veľmi pripomína architektúru stredovekých

hradieb. Tá bola spoľahlivá v 90. rokoch, kedy takýto systém obrany celkom slušne fungoval, no dnes je na povážení, ak zamestnanec firmy po rannom príchode do svojej kancelárie nevedomky zapojí svoj zavírovaný notebook do firemnej siete. Vtedy sú hradby firewallov i precízne nakonfigurované protokoly bezmocné, pretože hriešnik je priamo v zraniteľnom centre intranetu. Zďaleka sa nejedná o jediný prípad zlyhania, sú i ďalšie - napríklad zamestnanec „stratí“ nezašifrované médium s citlivými údajmi niekde v objekte budovy, podplatia chlapíka na recepcii či niekto zavolá do firmy a predstaví sa ako kompetentná osoba (najčastejšie CISO), ktorá po zamestnancovi chce nejaké údaje. Všetky tieto druhy klamu, neférovosti, nelojality alebo nezodpovednosti sa bežne stávajú v moderných firmách po celom svete a preto je potrebné sa im adekvátne postaviť na odpor.

Detekcia a zastavenie únikov firemných dát prostredníctvom zamestnancov je enormnou výzvou, obzvlášť pre veľké organizácie so široko distribuovanými dátovými skladmi a sieťami. V dnešnej dobe je tento problém dokonca ešte zložitejší, pretože internú hrozbu nepredstavujú len nespokojný či zlomyseľný zamestnanci, ale i nedbalí pracovníci, hackeri z vonkajšieho prostredia, ktorí sa chovajú ako dôveryhodní užívatelia, či iné osoby s prístupom do podnikovej siete. Výsledkom je, že firmy musia hľadať nové pohľady na celú škálu vnútorných hrozieb a prísť na to, aké technológie, procesy a administračné kontroly je potrebné implementovať. Ako povedal Wuchner-Bruhl pre týždenník Computerworld, „Bezpečnostní špecialisti radi budia dojem, že majú všetko pod kontrolou. Faktom ale ostáva, že v oblasti ohrozenia z vnútra toho ešte veľa nevedia.“ V mnohých najväčších finančných inštitúciách už takéto útoky dokonca prekonali externé útoky, ako to vyplýva z prieskumu 2005 Global Security Survey spoločnosti Deloitte Touche Tohmatsu. Rovnako 34 % respondentov rebríčku Fortune 100 tvrdilo, že v posledných 12 mesiacoch u nich došlo k vnútornému útoku. O rok skôr to bolo len 14 %, a pre porovnanie – externých útokov bolo len 26 %. Naviac útoky insiderov je ťažké zachytiť, pretože ide o užívateľov využívajúcich legitímni prístup k nepatričným účelom. Existuje tiež mnoho ciest, akými môžu byť dáta vynesená z podniku bez toho, aby o tom ktokoľvek vedel. Patrí medzi ne využitie prenosov súborov, posielanie dát v emailových prílohách či uploading dát do vzdialených systémov. Všeobecná dostupnosť úložných zariadení s vysokou kapacitou a malým formátom, ako sú USB pamäte, CD či handheldy, ľuďom veľmi zjednodušuje možnosť stiahnuť veľký objem dát a jednoducho odísť s nepatrným rizikom, že budú vystopovaní. [13]

Hlavným dôvodom rastúceho počtu útokov zo strany insiderov sú, ako inak, finančné motívy. Takto bola vykradnutá aj Bank of America s 670 000 informáciami o klientoch. Medzi členmi gangu boli siedmi bývalí zamestnanci, čo znamená, že väčšina interných útokov býva dôkladne plánovaná vopred. [12]

6.2.1 Sociálne inžinierstvo

Sociálne inžinierstvo je metóda, prax či postup získania dôveryhodných informácií prostredníctvom manipulácie legitímnych užívateľov. Sociálny inžinier obyčajne používa telefón alebo Internet, aby dobehol pracovníkov vo vyzradení citlivých informácií alebo vo vykonaní čohosi, čo nie je v súlade s typickou firemnou politikou. Táto metóda skôr zneužíva prirodzenú tendenciu osôb dôverovať slovám iných, než aby využívala prítomnosť bezpečnostných dier IS. Je všeobecne známe, že užívatelia sú slabým prvkom bezpečnosti a presne tento fakt robí sociálne inžinierstvo reálnym. Totižto bezpečnosť je celá o dôvere – dôvere v ochranu a autenticitu. Je jedno, koľko článkov bude publikovaných o sieťových dierach, záplatách a pod. - tým možno hrozbu iba redukovať, a ďalší vývoj situácie závisí od kompetentností zamestnanca zachovať korporačnú sieť bezpečnú. [14] [17]

Základné ciele sociálneho inžinierstva sú rovnaké ako u hackovaní vo všeobecnosti; získať neautorizovaný prístup k systémom alebo informáciám za účelom spáchať podvod, sieťové narušenie, priemyselnú špionáž, krádež identít alebo jednoducho poškodiť systém alebo sieť. Medzi typické ciele sa radia telefónne spoločnosti, odkazové služby, veľké spoločnosti, finančné inštitúcie, vojenské a vládne agentúry i nemocnice. Na otázku, prečo sa organizácie stávajú terčom takýchto útokov existuje krátka odpoveď; je to jednoduchšia cesta k získaniu nedovoleného prístupu než akákoľvek forma technického hackingu. Dokonca i pre technikov je oveľa prijateľnejšie zodvihnúť telefón a poprosiť niečie heslo. To je presne to, čo hacker urobí. [17]

Sociálne inžinierstvo a jeho útoky sa odohrávajú v dvoch rovinách:

- fyzickej (pracovisko, telefón, trashing, on-line)
- psychologickej (presviedčanie, reverse social engineering)

6.2.1.1 Fyzický aspekt sociálneho inžinierstva

Hacker môže prosto vojsť cez dvere (ako vo filme) a predstierať, že je údržbár alebo konzultant majúci povolený prístup do organizácie. Potom si votrelec vykračuje po pracovisku kým nenatrafí na nejaké povaľujúce sa heslá, opustí budovu s hojnými informáciami a tie v istý večer použije k nabúraniu sa do IS spoločnosti priamo z miesta svojho bydliska. Podobnou technikou získania autentizačných informácií je postávať na pracovisku a sledovať, či nejaký nedbalý pracovník nenaťuká svoje heslo. [17]

Najbežnejší typ útoku sociálneho inžinierstva je prostredníctvom telefónu. Hacker zavolá a imituje niekoho v pozícií autority alebo významnosti a opatrne vyťahuje z užívateľa informácie. Help-desk (recepcia, call centrum, centrum podpory, ústredňa) je obzvlášť náchylný na tento typ útoku pretože ich úlohou je práve poskytovať pomoc. Zamestnanci help-desku sú trénovaný, aby boli priateľský a vedeli poskytnúť informácie, čím sa stávajú „zlatou baňou“ pre sociálne inžinierstvo. Inokedy útočníci môžu predstierať, že volajú z vnútra organizácie a zahrať sofistikovaný trik na operátora. Naproti tomu je väčšina operátorov v oblasti bezpečnosti minimálne poučená a platená za to, že odpovedá na otázky volajúcim. Následkom sú ohromné bezpečnostné diery. [17]

Tzv. trashing predstavuje ďalšiu populárnu metódu sociálneho inžinierstva. Veľká hromada informácií sa dá nájsť vo firemných kontajneroch. Periodikum The LAN Times uskutočnilo súpis nasledujúcich predmetov, ktoré potenciálne zodpovedajú za únik informácií pri ich odhodení; telefónne zoznamy, organizačné schémy, memorandá, manuály politiky, kalendáre stretnutí, udalostí a dovoleniek, systémové manuály, výtlačky citlivých dát, prihlasovacích údajov a hesiel, výtlačky zdrojových kódov, disky, kazety a napokon vyradený hardware. Všetky tieto zdroje sú flexibilne zneužiteľné. Telefónne zoznamy dodajú hackerovi kontakty osôb, na ktoré možno útočiť alebo ktorých identitu možno zneužiť. Organizačné schémy obsahujú údaje o štruktúre v rámci organizácie. Memorandá poskytnú drobné rady pre vytvorenie falošnej autenticity. Manuály politiky ukážu hackerom, nakoľko je spoločnosť reálne zabezpečená (nezabezpečená). Kalendáre sú citlivé v tom, že útočníkovi oznamujú termín, kedy je dotyčná osoba mimo svojho pracoviska. Systémové manuály, dáta a ďalšie zdroje technických informácií dokážu niekedy podať návod ako odomknúť podnikovú sieť. Vyradený hardware, najmä hard disk, sa dá stále obnoviť a poskytnúť všetky možné druhy užitočných informácií. [17]

Úrodnou pôdou sociálnych inžinierov je Internet. Majorita užívateľov obvykle opakovane používa jediné heslo ku všetkým účtom; emailu, elektronickému obchodu, internet bankingu, loginu na pracovisku, atď. Takže ak útočník získa jedno heslo, je viac než pravdepodobné, že vnikne do viacerých účtov toho istého majiteľa. Najrozšírenejšiemu spôsobu obdŕžania prístupových údajov on-line formou sa venuje ďalšia kapitola.

6.2.1.2 Psychologický aspekt sociálneho inžinierstva

Medzi psychologické aspekty sociálneho inžinierstva sa radia techniky; zosobňovanie, vtieravosť, prispôsobovanie sa, rozptyľovanie zodpovedností a „staré dobré priateľstvo“. Cieľom každej z nich je uistiť obeť, že sociálny inžinier je vlastne osoba, ktorej možno dôverovať. Hacker si dáva veľký pozor na to, aby nepožadoval mnoho informácií od jedinej osoby. Zosobňovanie, najpoužívanejšia technika, je akési tajné neformálne divadlo. Hacker si pred útokom poctivo naštuduje charakter individuálov v organizácií a čaká až dotyčný odíde na služobnú cestu, aby telefonicky sfalšoval jeho identitu. Útočník sa bežne vydáva za opravára, IT podporu, manažéra alebo spoluzamestnanca. Obecne platí, čím väčšia spoločnosť tým ľahšie uskutočniteľný útok. Väčšina hraných rol spadá pod niekoho s autoritou, čo vedie zamestnancov k vtieraniu sa (kto by nechcel zapôsobiť na šéfa). Úplne najľstivejšou taktikou sociálneho inžinierstva je tváriť sa priateľsky. Myšlienka parazituje na dôvere. Ľahká lichôtka či flirt spravia svoje, avšak skúsený hacker vie aj to, kedy prestať s vypytovaním sa skôr než si zamestnanec všimne niečo podozrivé. Stávajú sa aj také prípady, že hacker sabotuje sieť, rozšíri nejaký problém a vydá sa za kompetentnú osobu, ktorú treba kontaktovať. Až príde opraviť problém, požaduje isté drobnosti (prístupové či iné údaje) čím sa mu dostane to, po čo skutočne prišiel. Najhoršie na takomto incidente je, že nik netuší, že bol svedkom útoku. [17]

Môžete minúť celý majetok na nákup technológií a služieb a vaša sieťová infraštruktúra ostane stále bezradná voči staromódnej manipulácii. [5]

6.2.2 Spear phising

Spear phising je forma on-line identifikačnej hrozby, ktorá zamestnáva sociálne inžinierstvo spoločne s technickým podvodom zvlášť za účelom krádeže finančného prístupu. Phising, ktorého názov je parodicky odvodený od slova fishing (rybolov), bežne operuje posielaním falošných emailov načítaním vašich kontaktných listov a nič netušiacich vás presmerujú na falošné webové stránky (svojich) bánk, elektronických

maloobchodov a rôznych kreditných ústavov, ktoré sú navrhnuté tak, aby splnili svoj účel - ukradli užívateľovi PIN, prihlasovacie mená a ostatné citlivé údaje. Najviac phisingom atakovaný priemysel je sektor finančných služieb (89,3 %). Počet phising útokov neustále rastie, ako to dokladá obrázok.

Obr. 6. Prípady nových falošných stránok za posledných 12 mesiacov

Koláčový graf nám zachycuje krajiny z najväčším počtom hostovaných stránok, slúžiacich ako pasca na identifikačné údaje. V USA vzniká najviac www podvrhov (48 %).

Obr. 7. Desať najväčších hostiteľov Phisingu z geografického pohľadu

Príkladom phisingu môže udalosť, ktorá sa stala koncom marca tohto roku. Útočníci začali spamovať emailové schránky návnadami aby prilákali užívateľov na infikované stránky.. Email obsahoval skutočné útržky spravodajstva z BBC a odkaz „Čítaj viac“. Užívatelia, ktorí nasledovali tento odkaz, boli presmerovaní na falošné BBC stránky zneužívajúce slabiny IE, kde sa stali obeťou trojana, monitorujúceho pohyby klávesnice pri finančných operáciách a elektronickom obchode. Tie potom pravidelne vysielal útočníkovi. [22]

6.2.3 Instant Messaging attack

Dnes už musíme byť ostražití aj pred službou Instant Messagingu, pretože škodlivé kódy sa dostali aj tam. Ide predovšetkým o upravené červy realizujúce únos IM klienta tak, že najprv prečítajú zoznam kontaktov najbližších priateľov a potom rozošlú správu „Haha, objavil som zábavný film“ a pod. Červ infikuje počítač prečítaním emailu a celý proces sa opakuje. Jedinou obranou ostáva školenie zamestnancov. [12]

6.2.4 Lámanie hesiel

Sila hesla spočíva v jeho prelomení. Heslo sa môže skladať z ľubovoľného počtu znakov, vrátane špeciálnych znakov anglickej klávesnice, o rôznej dĺžke a zložitosti (tzv. variability znakov). Ďalším faktorom, ktorý determinuje silu hesla je frekvencia zmeny hesla. Pre podniky je neprípustné, aby si užívatelia ponechávali jedno heslo po celú dĺžku pracovného pomeru. Obecne je prelomiteľné každé heslo, je otázka za akú dobu. Človek, ktorý sa o to pokúša bez ohľadu na zámer nesie označuje kryptoanalytik. Techník používaných pri lámaní kryptografických algoritmov existuje mnoho. Elementárnym útokom je použitie hrubej sily, kedy sa s pomocou výkonného počítača skúšajú všetky možné alternatívy hesla. Preto, ak je za heslo zvolený bežný výraz, je jeho prelomenie otázkou krátkej chvíle. [23]

Sofistikovanejšie metódy sú;

- lúštenie so znalosťou šifrovaného textu
- lúštenie so znalosťou otvoreného textu
- lúštenie so znalosťou vybraných otvorených textov
- lúštenie so znalosťou vybraných šifrových textov
- lúštenie kompromitáciou užívateľov

7 KONKURENČNÉ SPRAVODAJSTVO

Správne strategické rozhodovanie managementu závisí od dostatočného množstva včasných a kvalitných informácií. Nepresná, oneskorená alebo neúplná informácia môže spôsobiť prijatie zlého rozhodnutia a tak napáchať nenahraditeľné škody a straty. Podmienkou úspešnej realizácie operatívnych zámerov a významných podnikateľských projektov je včasné a účinne čelenie zámerom konkurencie. Tomuto procesu sa vžilo označenie konkurenčné spravodajstvo (CI), niekedy tiež označované priemyselná špionáž. V dnešnej dobe je konkurenčné spravodajstvo nevyhnutné pre všetky firmy. Pre veľké a silné firmy je dôležité preto, že okolie firmy neustále podlieha zmenám, ktorým sa musí adekvátne prispôsobovať inak neochráni investície svojich akcionárov. Pre malé firmy je CI takisto dôležité, pretože tie musia využívať neustále meniace sa medzery na trhu a sú v stálom ohrození zo strany veľkých či stredných firiem. Dnes každá firma disponuje prístupom k rovnakým informáciám. Firma, ktorá bude o krok pred ostatnými, bude len tá, ktorá dokáže tieto informácie premeniť do akcieschopnej znalosti. Znalosť, čiže to čo odlišuje dvoch konkurentov, je výsledok konkurenčného spravodajstva. [2]

Podstatou CI sú postupy (formy, metódy a prostriedky), ktorými je možné odhaliť stratégiu konkurencie a využiť ju v prospech vlastnej firmy. Jeho funkcie možno zhrnúť do nasledujúcich bodov:

- predvída zmeny na trhu
- predvída kroky konkurencie
- objavuje nových alebo potenciálnych konkurentov
- učí o úspechu a zlyhaní druhých
- informuje o nových technológiách, produktoch a procesoch, ktoré môžu ovplyvniť podnikanie firmy
- otvára možnosti nových obchodov
- hodnotí vlastnú firmu s nadhľadom
- napomáha implementácií najnovších manažérskych nástrojov

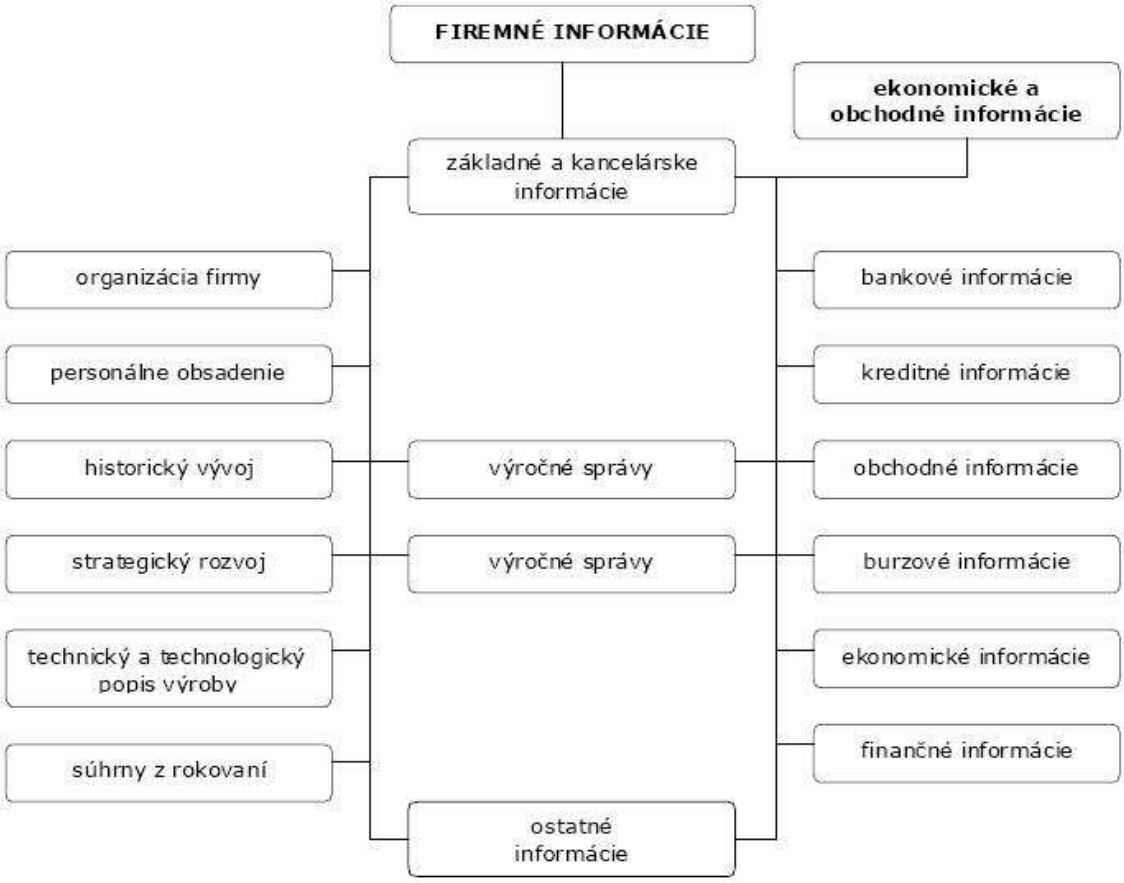
Za vedľajšie funkcie CI sa považuje odhalenie nebezpečenstva spojeného so zahájením určitej výroby, uskutočnenie určitého obchodu, využitie novej technológie, či vstup na

nový trh. Informácie získané konkurenčným spravodajstvom slúžia pre vrcholový manažment, ale aj pre stredný manažment. Podľa cieľov sa CI klasifikuje na;

- *aktívne spravodajstvo* – získavanie, zhromažďovanie, triedenie a analyzovanie informácií potrebných pre podnikanie, informácie o konkurencii, marketingových aktivitách na trhu
- *obranné spravodajstvo* – ochrana dát a znalostí, počítačových a komunikačných systémov podniku
- *lobystické spravodajstvo* – systém opatrení a protiopatrení na ovplyvňovanie vlastných krokov, krokov obchodných partnerov a krokov konkurencie

Súčasťou obranného spravodajstva (tzv. CII) je zhromažďovanie informácií pre včasné odhalenie nepriateľských aktivít, úspešný priebeh žaloby alebo zhromažďovanie dôverných informácií. Veľa firiem či organizácii vykonáva činnosť konkurenčného spravodajstva automaticky bez toho, aby si to uvedomovali. Do CI patria i rutinné činnosti, ako návšteva veľtrhov, rozhovory s kolegami z oboru a i. [1]

Obsahom CI je analýza konkurencie. Analýzu tvoria štyri ciele – *budúce ciele* (predikcia zámerov konkurenta), *stratégia* (analýza cieľov), *predpoklady* (o sebe samom a o odvetvi, reakcie na vývoj udalostí) a nakoniec *schopnosti* (prednosti a slabiny). Analýza budúcich cieľov konkurencie, jeho predpokladov, súčasnej stratégie a schopností vedie k vytvoreniu profilu pravdepodobnej reakcie konkurenta. Proces, v priebehu ktorého dochádza k definícii problému a jeho potenciálnej dekompozícii na dieľčie otázky (plánovanie, zber, analýza, distribúcia) sa nazýva cyklus konkurenčného spravodajstva. Pri komunikovaní znalostí získaných v procese CI sa odporúča dodržiavať zásady stručnosti, vysvetľujúceho štýlu písania, korektúry a atraktívnosti. Výsledný produkt CI závisí od konkrétneho cieľového používateľa. [2]



Obr. 8. Členenie firemných informácií

	formálne (technické)	neformálne (ľudské)
interné	Sú tvorené obsahom všetkých možných informačných systémom organizácie (elektronické dokumenty, e-mail, archívy, databázy a pod.).	Pracovníci organizácie. Informáciu, za ktorú je niekedy potrebné zaplatiť vysokú sumu, je často krát možné získať zadarmo od vlastného kolegu.
externé	Prístupy k rôznym komerčným alebo nekomerčným informačným zdrojom (internet, vyhľadávacie služby, komerčné databázy, registre a pod.).	Osobné kontakty s ľuďmi mimo organizáciu (zákazníci, dodávatelia, distribútori, konkurenti, združenia, zväzy, asociácie, žurnalisti, univerzity, konzultanti, experti).

Tab. 1. Zdroje informácií podľa informačných sietí

7.1 Prínos pre súčasnosť

Vo svete zúri ekonomická vojna, kde proti sebe nestoja len záujmy národov, ale i záujmy komerčných firiem. Táto vojna sa odohráva v čoraz menej stabilnom a čoraz rýchlejšie sa meniacom konkurenčnom prostredí. Hovorí sa o informačnej spoločnosti a o informačnej

vojne – útočnom používaní informácií za účelom oslabenia, destabilizácie alebo zničenia nepriateľa. Mnoho manažérov je presvedčených, že dokážu robiť správne rozhodnutia aj pri nedostatku informácií a týmto štýlom sa aj pozerajú na využitie informačných technológií. Manažér však nepotrebuje informácie, manažér potrebuje znalosti. Spravodajská agentúra Reuters vypracovala štúdiu o súčasnom stave pohltenia informáciami a jeho vplyvu na ľudí v rôznych krajinách a rôznych zamestnaniach. Zistila sa dvojica nasledujúcich faktov; za prvé, narastá nezdravá závislosť ľudí na informáciách. Ľudia, ktorí prepadnú informačnému konzumu, trpia neurózou pri pobyte mimo počítača alebo zamestnania a sú harmonicky neschopní rozvíjať ostatné zložky svojho života. To má za následok, že získané informácie nie sú schopní účelne použiť vo svoj prospech ani v prospech organizácie. Za druhé, stále narastajúci počet ľudí zaplavovaných informáciami. Už takmer polovica manažérov je neschopná čeliť rozhodnutiam a vystavení veľkosti informáciám proti svojej vôli, zmietajú sa v depresiách a sú náchylnejší k zdravotným ťažkostiam. Nielenže klesá ich výkonnosť v práci, ale to všetko prináša následné problémy i v súkromnom živote. Oba závery sa navzájom kombinujú a pre budovanie informačných systémov z toho plynie jeden základný zákon – užívateľ musí mať možnosť dostávať iba tie informácie, ktoré sú preňho celkom relevantné. [7]

7.1.1 Priemyselná špionáž a prevencia

Priemyselná špionáž, ktorá je oddávna trápením mnoho podnikov, sa teraz stala všedným chlebom pre tradičných špiónov, ktorí sa po skončení studenej vojny venujú platenému vykrádaniu firemných tajomstiev. Zahraničné korporácie a vlády využívajú služby priemyselných špiónov na voľnej nohe, aby vykrádali informácie. Obvykle ide o ľudí, ktorí predtým pracovali vo výzvedných službách a majú odpovedajúce znalosti a skúsenosti, čo im uľahčuje infiltráciu do organizácií. Týka sa to predovšetkým tých firiem, ktoré nedokázali zaviesť odpovedajúce bezpečnostné prostriedky pre ochranu svojich informácií ani vyškoliť svojich ľudí. [5]

Nebezpečenstvu špionáže je možné sa vyhnúť šifrovaním dát (kap. 8.1.8) a racionálnym prechovávaním záložných kópií. Pokiaľ firma archivuje dáta zašifrované, ich strata je nanajvýš otravná. Ak ale firma dáta nešifruje, potom najlepšie sama dokáže odhadnúť príslušný dopad. Menšie firmy majú dobrú alternatívu prechovávania záložných kópií – môžu denne posielať nové i zmenené súbory niektorým z firiem ponúkajúcich archiváciu on-line. Dáta musia byť vopred zašifrované, inak sa informácie stanú prístupné každému

votrelcovi, ktorí by sa mohol nabúrať do ich počítačového systému. Až sme zaviedli systém šifrovania zabezpečujúci naše záložné kópie, je potrebné tiež zaviesť vysoko bezpečnú procedúru prechovávania šifrovacieho kľúča alebo dešifrovacieho hesla. Tajné šifrovacie kľúče by mali byť umiestnené v trezore. Vždy majú byť aspoň dve osoby, ktoré poznajú miesto, kde sú uložené dáta, šifrovacie a dešifrovacie procedúry. Štandardný postup by mal tiež predvídať situáciu, že pracovník zodpovedný za tieto záležitosti môže náhle firmu opustiť, vtedy si procedúry vyžadujú zmenu kľúča. [5]

7.1.2 Etický kódex pre konkurenčné spravodajstvo

Aby sa zabránilo zneužitiu CI a rozširovaniu nekalej špionáži, sú ustanovené isté pravidlá pre operovanie s CI, ktoré sa musia dodržiavať. Hovorí sa im etický kódex pre konkurenčné spravodajstvo. Kódexy sa líšia v závislosti od používaných noriem, ich pravidlá sú zvyčajne;

1) Pri jednaní vo svojom mene sa nemá zavádzať, ale vo všeobecnosti sa nebude odhaľovať meno klienta. Pri rozhovoroch sa dovoľuje poskytovať názov a sídlo spoločnosti

2) So všetkými materiálmi týkajúcimi sa klienta sa narába ako s dôvernými, preto sa môže poskytnúť Dohoda o nezverejňovaní údajov alebo podpísať podobná zmluva poskytnutá klientmi z radov firiem. Všetky materiály týkajúce sa projektu klienta sa oddeľujú od ostatných spisových materiálov týkajúcich sa ich či podobného odvetvia, aby sa takto zabránilo odhaleniu neverejných informácií

3) Nemá dochádzať k výmenám cenovej informácie s konkurentmi, ani sa nebudú tolerovať uzatvárania tajných dohôd obmedzujúce súťaž na trhu. Ak sa budú získavať informácie o cenách a objeme produkcie pre klientov, nesmie sa ohroziť pozícia našich klientov porušovaním rôznych anti-trustových legislatívnych ustanovení

4) Nemá sa vedome ohrozovať pozícia alebo povesť klientov či respondentov vyžadovaním informácií, ktoré nie sú prístupné v rámci bežnej konverzácie alebo obchodu

5) Nemajú sa odhaľovať tajné plány, grafy, vzorky alebo technológie konkurentov bez súhlasu. Neprehrabáva sa v odpadkoch konkurentov. Nemá dochádzať k záujmom na získavanie, archivovanie alebo používanie obchodného tajomstva

6) Nemajú sa umiestňovať falošné inzeráty s cieľom uskutočniť rozhovory s personálom konkurencie, zneužívať konkurenčné informácie alebo používať nesprávne informácie

7) Nemá dochádzať k podplácaniu respondentov, k používaniu vydierania či iného vynucovania informácií

8) Nesmie sa robiť tajná špionáž s použitím odpočúvacích zariadení, skrytých kamier alebo sledovania. Rozhovory sa nenahrávajú na audio pásky

9) Nemá sa vedome ohrozovať pozícia žiadneho suverénneho štátu tým, že by sa poskytovali poznatky, ktoré sa týkajú ich alebo domácej národnej bezpečnosti

10) Má sa dodržiavať bezúhonnosť vo vzťahoch s klientmi, kolegami, inými organizáciami, referenčnými zdrojmi a inými profesiami tak, aby sa prispelo k optimálnemu úžitku medzi klientmi, aktívne podporila medzinárodná a domáca konkurencieschopnosť. [24]

II. PRAKTICKÁ ČASŤ

8 PROCES IMPLEMENTÁCIE SYSTÉMU DO ORGANIZÁCIE

Táto kapitola je venovaná systematickým zásadám výstavby bezpečnostnej politiky organizácie prevádzkujúcej informačný systém. Nadväzuje na teoretickú časť, hlavne na kapitolu 3 – Bezpečnostná politika v organizáciách a kapitolu 4 – Systémy obrany moderných podnikov. Jednotlivé kapitoly poukážu na praktické riešenia a možné predchádzania bezpečnostných incidentov. Rád by som však na základe vlastných skúseností v tejto svojej práci prezentoval strategické odporučenie, ako učiniť firmu resp. nejakú zložku štátnej správy stabilnejšou z hľadiska jej informačnej bezpečnosti. V jednotlivých systematicky usporiadaných kapitolách budem venovať pozornosť aktuálnym riešeniam incidentov. Kľúčový dôraz kladiem predovšetkým na ľudský faktor, pretože jeho postoj a prístup je jadrom úspechu i problémov všetkého, vrátane ekonomickej existencie podniku.

8.1 Synchronizácia technických a technologických opatrení

V tejto časti práce zmienim desať alternatívnych technologických opatrení zvyšujúcich bezpečnosť dát a znalostí modernej firmy. Pri popise jednotlivých krokov budem vychádzať z predpokladu, že v rámci bezpečnostných zásad sú už definované požiadavky, podmienky a štandardy.

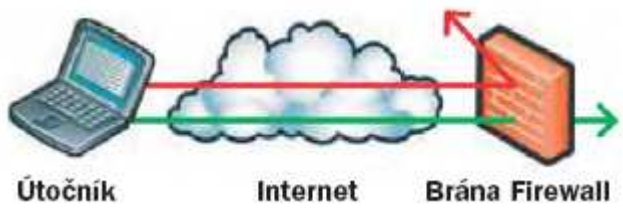
8.1.1 Využívanie brány firewall

Ako už vyplýva z predošlých kapitol, cieľom inštalácie serverovej alebo osobnej brány firewall je znemožniť externistom prenikať do siete prostredníctvom internetu alebo internistom sabotovať lokálnu vnútropodnikovú sieť. Firewall tvorí veľmi dôležitú obrannú líniu, ktorá chráni lokálne siete pred útokmi tým, že odmieta nevyžiadanú komunikáciu. Serverová brána blokuje celú prevádzku, ktorá nie je medzi internetom a sieťou organizácie dovolená, maskuje adresy počítačov za bránou, atď.

Osobný firewall integrovaný do operačného systému funguje podobne ako serverová brána, ale chráni len jediný počítač, v ktorom je osobný firewall nainštalovaný. Predstavuje vhodný doplnok serverovej brány firewall, ale vzhľadom k izolovanej činnosti nie je vyhovujúcou ochrannou celej siete. Naopak, osvedčí sa proti interným útokom. Hackeri jednajúci v rozpore so zákonmi môžu vyhľadať sieť organizácie a prípadne zamerať útok na jednotlivé počítače, bez toho aby vedeli, na koho útočia. Je to rovnaké

ako náhodná voľba čísiel z telefónneho zoznamu. Pokiaľ má organizácia trvalé (stále alebo pevné) pripojenie k internetu, existuje istá pravdepodobnosť, že jeho sieť bude predmetom náhodných sond alebo útokov niekoľkokrát denne. Pokiaľ útočníci majú k dispozícii správnu adresu počítača, môžu využiť medzier v programovom vybavení (zvlášť v prípade neuplatňovania aktualizácií) alebo sa môžu pokúsiť a prekonanie hesla tak, aby získali prístup. Samotný firewall nemôže zaručiť bezpečnosť, ale je dobrou zbraňou prvej obrannej línie. Škody, ktoré môžu hackeri napáchať na nechránenom systéme sa podľa posledného prieskumu *Datamineru* vyšplhajú až na úroveň 45000 € prevyšujúc nákupné ceny za firewall produkty.

Serverový firewall sa inštaluje medzi počítače v sieti organizácie a linkou k verejnej internetovej sieti. Správne nakonfigurovaný firewall kontroluje každý prichádzajúci a odchádzajúci paket a buď ho príjme alebo odmietne na základe vopred definovaných zásad. Firewall možno nastaviť tak, aby prijímal daný druh prevádzky spojeného s elektronickou poštou a komunikáciou s webovou sieťou, a na druhej strane odmietal iné typy prevádzky. V praxi to znamená, že vďaka príslušnému programovému vybaveniu firewallu možno určiť, že naši zamestnanci nebudú môcť prehľadať www stránky s pornografickým obsahom alebo zábavným obsahom, budú mať však bez problémov prístup k takým stránkam, ktoré sú pre ich prácu nevyhnutné, napr. stránky ministerstiev, vládnych agentúr alebo stránky iných úradov.

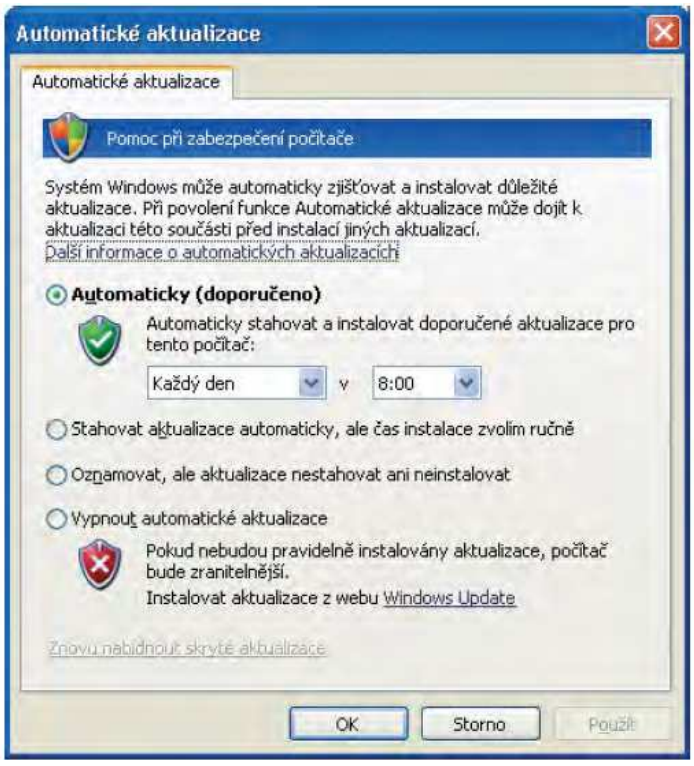


Obr. 9. Brána firewall

Inštalácia serverovej brány firewall do siete je v zásade veľmi jednoduchá. Firewall sa zapája medzi kabelový/DSL modem či iné pripojenie k internetu a počítače patriace do miestnej siete. Osobný softwarový firewall pracuje na konkrétnom počítači a kontroluje iba prevádzku tohto počítača. Tento druh obrany je implementovaný do systému Windows XP Professional SP2, odporúča sa však využívať komerčné softwarové brány od výrobcov Computer Associates, McAfee, Symantec alebo Zonelabs.

8.1.2 Sťahovanie aktualizácií

Princípom sťahovania softwarových aktualizácii by mala byť istota, že sa užívatelia nachádzajú vždy o krok pred hackermi a mali istotu, že IS je odolný proti útokom, ktoré využívajú dávno identifikované o odstránené medzery v operačnom systéme a programoch. Realita je však taká, že majorita všetkých záplat bola vydaná až po ohlásenom bezpečnostnom incidente. Ostáva teda len spoliehať sa na to, že i keď je dnes práve útočník tým, kto objavuje bezpečnostné medzery v systéme, nestihne alebo nemá prostriedky na to, aby túto chybu stihol počas tzv. reakčnej doby (t.j. doby odozvy vývojára zasiahnutého produktu) využiť na masový útok. Aktualizácie sa dnes poskytujú na radu software – známe sú predovšetkým bezpečnostné balíčky od Micrsoftu, sady aktualizácií pre antivírové a antispywarové služby, ale stretneme sa i s updatom pre kancelárske produkty (MS Office, Adobe) či multimediálne aplikácie (Media Player, www browsery, atď). Mnohým opakovaným výrovým infekciám sa týmto spôsobom možno úspešne vyhnúť. V súčasnej verzii OS Microsoft Windows (XP SP2 ver 5.1.2600) je precízne implementovaný systém automatických aktualizácií, ktorý si sám každé dva týždne stiahne bezpečnostný balík vydávaný výrobcom.



Obr. 10. Automatické aktualizácie vo Windows XP SP2

Rada; presvedčte sa, či máte na svojom počítači nastavené automatické aktualizácie. Ak bol váš počítač niekoľko dni vypnutý, nečakajte na automatické aktualizácie Windows, ale rovno zahájte navigáciu so službou Windows Update. Doplňujúcou službou Microsoftu býva tzv. *Microsoft Security Update* – bezplatná služba poskytovaná prostredníctvom elektronickej pošty určená užívateľom z rád malých a stredných firiem a úradov. Využíva sa za účelom informovanosti užívateľov v oblasti dôležitých materiálov o bezpečnosti a výrových upozornení. Užívatelia môžu týmto spôsobom zistiť nutnosť uskutočnenia určitých krokov za účelom ochrany proti novým hrozbám.

8.1.3 Využívanie antivírových riešení

Zadovážiť si a inštalovať antivírové programy a praktizovať ich aktualizáciu by malo byť v dnešnej dobe prioritou každej modernej firmy, ktorá využíva informačné systémy. Antivírové programy je nutné inštalovať na všetky počítače pripojené k sieti. Signatúra víru odpovedá unikátnej sekvencii DNA kódu počítačového víru. Pretože sa každý mesiac objavujú stovky nových vírov (viz. [21]), je nutné všetky tieto programy pravidelne aktualizovať zavedením nových definícií signatúr. Pokiaľ má organizácia pevné pripojenie, potom je možné väčšinu programov nastaviť tak, aby program sťahoval nové definície vírov na pozadí. Ako silný preventívny prostriedok je možné na serveri elektronickej pošty inštalovať program, ktorý by filtroval nevyžiadanú poštu od vírov a spamu. Stále však platí zlaté pravidlo – neotvárať každú poštu s prílohou, neotvárať žiadnu poštu bez predchádzajúcej kontroly antivírovým programom. Niektoré moderné produkty disponujúce rezidentnou ochranou to robia automaticky.

V súčasnosti existuje na trhu kvantum antivírových riešení a preto zákazník orientujúci sa na kvalitu nemá dostatočnú istotu určiť si preferencie. Z tohto dôvodu sa už pár rokov odbornými periodikami a elektronickými portálmi prinášajú rôzne benchmarky. Najznámejší je tzv. *Virus Bulletin* s jeho prestížnym ocenením VB 100%, čo znamená sto percentná úspešnosť pri detekcii neznámych hrozieb.

Obr. 11. Logo prestížneho ocenenia VB 100%

Rada vývojárov sa propaguje i uvoľňovaním voľne dostupných (freewarových) variant antivírusu či spywaru. Komparatívna analýza na konci kapitoly ponúka priestor pre úsudok.

8.1.4 Tvorba silných hesiel

Neexistuje dôvod prečo útočníkom uľahčovať prístup do systému. K tomu ale práve dochádza, ak si pracovníci vyberajú heslá, ktoré možno ľahko prekonať či odhadnúť. Zamestnancov je nutné poučiť, aby si vyberali tzv. silné heslá a pravidelne ich obmeňovali. Heslá typu mien, názvov firiem alebo rodné čísla nie sú vhodné pre zamedzenie prístupu, podobne ako bežné slová. Dnes už nepomôže ani zámena „i“ za „!“, písmena „S“ za číslicu „5“ alebo písmena „O“ za nulu keďže moderné kryptoanalytické metódy s takýmito zámenami pracujú. Preto silné heslá majú obsahovať kombináciu malých a veľkých písmen, špeciálnych znakov (tu platí pravidlo – čím viac tým lepšie), medzier a niekoľkých čísel. Podľa týchto zásad má bezpečné heslo vyzerať nasledovne; J*p2leO4>F. Na druhej strane heslo, ktoré si užívateľ nezapamätá je samozrejme nanič. I tu existujú rôzne triky uľahčujúce zapamätanie si silných hesiel, napríklad; Msmu5rv! (Môj syn má už 5 rokov !) alebo prosté frázy súvetia „K obedu som mal päť kurčiat“.

Dôležité je pravidelne a čo najčastejšie meniť heslo. Tiež treba vždy počítať so sklonom ľudí podľahnúť rôznym sociotechnickým trikom a slabostiam. Preto je nutné užívateľom zdôrazňovať, že s heslom majú zaobchádzať ako s kľúčom od kancelárie – to znamená, že nie je prípustné nechať ich ležať na všetkým na očiach ani svojvoľne predávať iným osobám. Obyčajný postup vhodného nastavenia šetriča obrazovky tak, aby počítač opätovne požadoval heslo po niekoľkých minútach nepoužívania, zníži možnosť incidentu v prípade, že sa jeho užívateľ vzdiali od pracovného stolu.

8.1.5 Zaistenie fyzickej bezpečnosti

Ochrana stolných počítačov a obmedzenie fyzického prístupu k pracovným staniciam a dokumentom je podstatnou súčasťou činnosti pri zaisťovaní bezpečnosti dát. V týchto prípadoch sa využívajú zámky, alarmy, zamykania skriniek na dokumenty, evidencie návštevníkov a označovania prístrojového vybavenia. Ani ten najlepší firewall nie je ochranou proti človeku, ktorý pracuje so serverom alebo lokálnou stanicou.

Z týchto dôvodov je nutné určiť bezpečnostné hranice okolo chránenej zóny s využitím (podľa potreby) priečiek, dverí s automatickým uzamkýnaním, alarmov a ochranných bariér a uistiť sa, že prichádzajúci i odchádzajúci hostia sú evidovaní a identifikovaní. Pokiaľ to je možné, maximálne je potrebné obmedziť možnosť prístupu do dôležitých zón (serverová miestnosť, atď.), pravidelne kontrolovať, kto má do nich prístup. Návštevníci sa musia pohybovať iba v sprievode zamestnanca. Je tiež nutné poučiť personál, ako má reagovať v situácií, keď sa cudzí človek bez sprievodnej osoby objaví v chránenej zóne. Po zamestnancoch sa má požadovať zásada „prázdneho stolu“, to znamená, že zamestnanci musia zabezpečiť dôležité alebo hodnotné materiály, pokiaľ s nimi práve nepracujú. Počítače a ich hlavné časti sa hodí označiť identifikačnými údajmi o firme, umiestnení a užívateľovi. Sériové čísla strojov a zariadení majú podliehať dôslednej evidencii, aby bola možná ich identifikácia v prípade krádeže. Zamestnancom sa má objasniť, že dokumenty z tlačiarní či kopírok je sa majú hneď odoberať. K tlači príliš dôverných materiálov a citlivých obchodných či iných firemných údajov by mali byť na to vyhradené samostatne označené a riadne zabezpečené (lokalizované) tlačiarne. Je vhodné sa uistiť, že pravidla pre chovanie zamestnancov určujú, ktoré zariadenia môžu opustiť kanceláriu. Hodnotné zariadenia je potrebné zveriť konkrétnym ľuďom, ktorý budú zodpovedný za ich vrátenie.

8.1.6 Pravidla pre používanie www

Pre zvýšenie bezpečnosti modernej spoločnosti je potrebné zaistiť, aby prehliadanie webovej siete prebiehalo racionálnym spôsobom. To znamená, že zamestnanci musia vedieť, ktoré www stránky môžu prehliadať a akým spôsobom sa dajú minimalizovať riziká s tým spojené. Pokiaľ si zamestnanci organizácie v pracovnej dobe prehliadajú stránky s pochybným obsahom, vystavujú sa pôsobeniu problémov s ohľadom na právne dôsledky takejto činnosti. V neposlednej rade je predovšetkým pre malé organizácie často

dôležitá i otázka prenosovej kapacity linky, takže obmedzenie povolených internetových operácií môže byť nápomocné pri znižovaní zaťaženia linky.

Existuje mnoho preventívnych prostriedkov, ktoré možno požívať za účelom zvýšenia bezpečnosti pri prehliadaní internetových stránok. Odporúčajú sa nasledovné zásady;

- nenavštevovať nedôveryhodné internetové stránky
- neprehliadať www stránky priamo zo serverov
- inštalácia proxy serveru za účelom filtrovania adries z www siete
- spracovať metodický pokyn so zásadami využívania internetovej siete

Je tiež nutné kontrolovať, či zamestnanci neobchádzajú požadované ochrany a napríklad sa nepripájajú k internetu pomocou súkromných telefónnych modemov inštalovaných v služobných počítačoch (tomu sa dá predísť plombovaním pracovných staníc).

8.1.7 Používanie elektronickej pošty

Elektronická pošta je jeden z najdôležitejších a najčastejšie využívaných komunikačných nástrojov, a to ako medzi firmou a okolím, tak v rámci nej samotnej. Samozrejmosťou je dodržiavanie istých bezpečnostných noriem. Viry, spam a hoax spôsobujú, že sa používanie elektronickej pošty stáva veľmi frustrujúce. Existuje celá rada jednoduchých preventívnych prostriedkov, ja sa obmedzím na tieto základné zásady, ktoré sa vyplatí dodržiavať - za prvé, je nutné aktualizovať programy elektronickej pošty (MS Outlook, Outlook Express, atď.). Pokiaľ sa používa program Outlook 2003, je vhodné aktivovať funkciu filtrovania nevyžiadaných správ. Znovu je vhodné si pripomenúť zlaté pravidlo, ktoré znie – neotvárať nevyžiadané prílohy e-mailových správ bez potvrdenia obsahu prílohy u odosielateľa. Niektoré víry sa maskujú ako neškodné typy súborov tým, že doplnia za koniec svojho názvu falošnú príponu (napr. funny.jpg.exe). Ich autor predpokladá, že v cieľovom systéme nie je nastavené zobrazovanie prípon, tzn. že je viditeľná len prípona *.jpg* a nie *.exe*. Tomu sa dá ľahko predísť nakonfigurovaním zobrazenia prípon súborov v prieskumníkovi. Rovnako, aby sa znížilo nebezpečenstvo vírovej infekcie emailom, nemá sa klikať na odkazy v podozrivých správach (text v správach môže maskovať skutočnú webovú adresu). Miesto toho sa odporúča vložiť URL ručne do adresného riadku browsera. Niektoré škodlivé správy vyžadujú k uskutočneniu špinavej práce len otvorenie emailu v automatickom náhľade. Preto sa

odporúča napríklad v programe MS Outlook túto funkciu deaktivovať. Väčšina takýchto škodcov je pritom závislá na kódoch HTML. Je možné ich dodatočne zastaviť prehliadaním emailov vo formáte čistého textu. Nikdy sa nemajú uvádzať heslá, čísla kreditných kariet alebo iné osobné informácie v odpovediach na email. Pokiaľ bude legálna firma skutočne potrebovať takéto informácie, nebude žiadať o ich poskytnutie prostredníctvom elektronickej pošty.

8.1.8 Využívanie šifrovania

Vývoj informačných technológií v súvislosti s riadením bezpečnostných rizík organizácií štátnej i súkromnej sféry sa uberá značným kryptografickým smerom – trh s bezpečnostnými produktmi zaplnili výrobky spoločnosti SecureID, systémy CryptoSafe, autošifrovacie USB kľúče, veľa sa hovorí o programe PGP a podobne. Všetko odráža reakciu na fakt, že medziročný nárast bezpečnostných incidentov predstavuje vážnu hodnotu 50 % a medzi hlavné hrozby patrí krádež, zneužitie či zámerné poškodenie citlivých dát zamestnancom organizácie. Šifrovanie samozrejme vyžaduje dodatočný čas a náklady, ale za tú námahu to stojí. Zašifrované súbory musia byť pravidelne kontrolované, aby bola istota, že šifrovanie funguje bez problémov. Akýmsi minimom pri práci s firemnými dokumentmi zvlášť na notebookoch a prenosných zariadeniach môže byť využitie mechanizmu EFS integrovaného v systéme Windows. Odporúča sa však politikou nasadené operovanie s kryptografickými softwarovými (PGP) poprípade hardwarovými riešeniami (Cisco systems, RSA tokeny, a i.) alebo najlepšie implementácia kombinácie oboch z nich vo forme nejakého balíčka (CryptoSafe a pod.). Uvedený systém sa ukázal ideálnym pre väčšinu spoločností - je ľahko nasaditeľný, umožňuje kombináciu s prvkami fyzickej bezpečnosti (vstupné systémy) a integráciu s existujúcou infraštruktúrou kontroly prístupu. Poskytuje administrátorom centralizovanú podporu nad prístupmi do firemných aplikácií, presadenie politiky silných hesiel, PKI a ochranu silných dát. Samotnú implementáciu možno uskutočniť i po etapách.

8.1.9 Pravidelné zálohovanie

Existujú dva druhy záložných kópií – kompletné a prírastkové. Kompletné záložné kópie umožňujú kopírovanie všetkých zvolených dát na iný nosič, zatiaľ čo v prírastkových sú zohľadnené len tie dáta, ktoré boli pridané alebo modifikované od doby vytvorenia poslednej kompletnej záložnej kópie. Pri štandardnom postupe založenom na kombinácií

oboch metód sa kópie vytvárajú jedenkrát týždenne a denne sa vytvárajú kópie prírastkové. V závislosti na množstve dát ku kopírovaniu a na čase, ktorý mu je možné venovať sa odporúča skôr zaobstarávanie kompletných zašifrovaných záložných kópií každú noc. Záložné kópie je nutné pravidelne testovať a v rámci skúšobnej lokalizácie obnovovať. Pred samotným zálohovaním je potrebná akási príprava. Najprv sa vyberá vhodné prístrojové vybavenie v závislosti na množstve kopírovaných dát a peňažnej čiastke určenej na tento účel.

Celková kapacita dat	Navrhovaný nosič
Do 700 MB	zapisovatelné CD nosiče
od 700 MB do 5 GB	zapisovatelné DVD nosiče
od 2 GB do 12 GB	digitální audio pásky (DAT)
Nad 12 GB	Zásobník DAT

Obr. 12. Typy zálohovacích nosičov

Predovšetkým je potrebné určiť, ktoré dáta majú pre firmu kľúčový význam a kde a akým spôsobom budú uložené. Údaje tohto typu sa môžu nachádzať v rôznych počítačoch, na centrálnom serveri, v systéme elektronickej pošty, v databáze alebo dokumentoch textového procesoru. Odporúča sa teda vytvoriť jednoduchú mapu, ktorá bude určovať lokalizáciu jednotlivých dát a špecifikovať ich význam. Tiež je potrebné menovať osobu zodpovednú za záložné kópie. Excelentne pre zálohovanie znovu poslúži program PGP Desktop, základné zálohovacie nástroje sú štandardne obsiahnuté aj v najnovších OS.

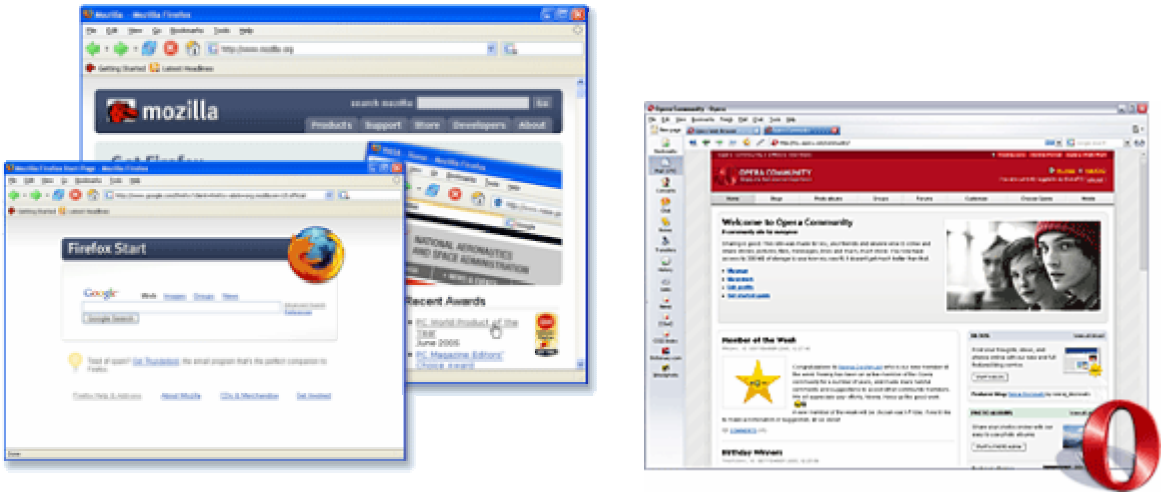
Obr. 13. Zálohovanie a obnova vo Windows XP

8.1.10 Prehľad dostupných produktových riešení bezpečnosti IS

Dnes sa firmám ponúka hromada bezpečnostných produktov – komerčných i open source. V tomto prehľade prezentujem produkty, ktoré dlhodobo testujem a považujem za veľmi prijateľné s ohľadom na základný (nie hlavný) cieľ podniku – minimalizáciu nákladov. Mojim prianím v tejto časti je presvedčiť čitateľov o existencii možnosti dosiahnutia vyššej efektivity ich podnikania v prípade implementácie nasledovných spravidla voľne dostupných alebo minimálne nákladných bezpečnostných riešení. Výsledkom bude podľa mojej skúsenosti dosiahnutie vyššej konkurencieschopnosti podniku za predovšetkým finančne nenáročných podmienok. Samozrejme, hranicou ostáva stále fakt, že sa jedná o mnou overené riešenie, kde konzekventnosť úspechu závisí na ďalších faktoroch sledovaného subjektu (úroveň kompetencie manažérov, vzdelanosť zamestnancov, personálna vyspelosť na pracovisku, organizačná štruktúra, technické a technologické vybavenie, hodnoty PEST analýzy daného podniku a i.).

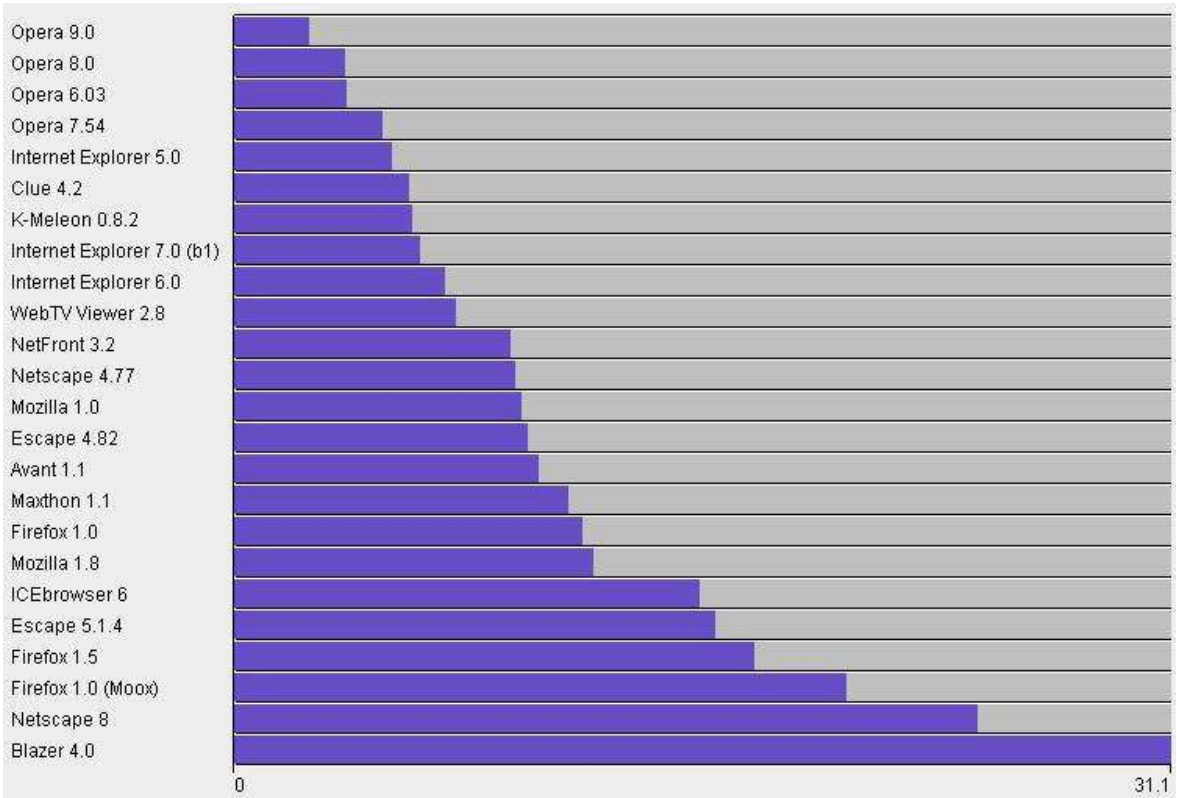
8.1.10.1 Browser

Skôr než využívať integrovaný prehliadač spoločnosti Microsoft (v súčasnosti IE6) je pre fakt, že väčšina hackerov dúfa práve v jeho prítomnosť vo firemnej sieti, racionálnejšie a z niekoľkých hľadísk úspornejšie využívať alternatívne produkty, ktorých v súčasnosti existuje desiatka no zmienim sa predovšetkým o najvýznamnejších z nich - Mozilla Firefox v1.5 a Opera 8.54. Systém www identifikácie a samotná architektúra týchto prehliadačov je v mnohých smeroch odlišná čím poskytujú vyšší komfort nielen z hľadiska bezpečnosti.



Obr. 14. Mozilla Firefox a Opera Browser

Mozilla, ktorá je absolútne zdarma dostupná, svojím užívateľom (zamestnancom firmy) ponúka intuitívne prostredie, priehľadnú tabeláciu okien, integrovaný vyhľadávací panel (Google, Yahoo), základnú obranu pred útokmi zo strany vírusov a spywaru, blokovanie vyskakovacích okien (tzv. pop-up), zmrazenie reklamných bannerov a ďalšie z hľadiska efektivity atraktívne vlastnosti. Jej najnovšia verzia má zabudované automatické aktualizácie, takže neprekáža IT nezdatným pracovníkom. Rovnako sa môže pochváliť niekoľkými oceneniami prestížnych magazínov a nezávislých testov. Druhou vysoko výkonnou alternatívou prehliadača je nórska Opera. Ide o akési synonymum, ktoré ponúka ďalšie nadštandardné služby (podpora Gmail, hlasový prenos, prepracovaný manažér hesiel, download nástroj atď.). U tohto produktu je ale prítomný skrytý ekonomický potenciál. Opera predstavuje bezkonkurenčne z hľadiska rýchlosti načítania www stránok vlajkovú loď, ktorá suverénne predčí všetky ostatné browsery v načítaní, renderovaní i spracovaní skript, ako to dokladá i nižšie priložený graf. Tým podstatne redukuje čas nutný k vykonaniu parciálnej úlohy čím pomáha zvyšovať produktivitu práce. Je rovnako voľne dostupná, inštalačný balík Opery je oproti Mozille dokonca polovičný (cca 8MB). Dovolím si tvrdiť, že jej popularita s očakávaným príchodom verzie 9.0 opäť stúpne a jej podiel na trhu sa vďaka vysokému výkonu bude zvyšovať.



Obr. 15. Komparatívna analýza výkonu momentálne dostupných browserov

8.1.10.2 Softwarový firewall

	ZoneAlarm Pro	Outpost Firewall Pro	Norton Personal Firewall 2005	Norman Personal Firewall	SurfSecret Personal Firewall	McAfee Personal Firewall Pro	Bullguard	Sygate Personal Firewall Pro	Injoy Firewall	BlackICE PC Protection
Overall Rating	■■■■	■■■■	■■■■	■■■	■■■	■■■	■■■	■■■	■■■	■■■
Ratings										
Feature Set	■■■■	■■■■	■■■■	■■■	■■■	■■■■	■■■■	■■■	■■■	■■■
Ease of Use	■■■■	■■■■	■■■■	■■■■	■■■	■■■	■■■	■■■	■■■■	■■■
Ease of Installation/Setup	■■■■	■■■■	■■■■	■■■■	■■■■	■■■	■■■■	■■■■	■■■	■■■
Reliability	■■■■	■■■■	■■■■	■■■	■■■■	■■■■	■■■	■■■■	■■■■	■■■
Help/Support	■■■■	■■■■	■■■■	■■■	■■■■	■■■	■■■	■■■■	■■■	■■■■
Features										
Email protection	✓	✓	✓				✓	✓	✓	✓
File Protection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Personal Information Protection	✓	✓	✓			✓				✓
Registry Protection	✓	✓		✓		✓	✓	✓	✓	
Port Monitoring	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Network Traffic Monitor	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data Filtering	✓	✓	✓	✓	✓	✓	✓	✓		✓
Intruder/Hacker Detection Tools										
Intruder Alert	✓	✓	✓	✓	✓	✓	✓	✓		✓
Intruder ID Lookup	✓			✓		✓				
Intruder Tracking Log	✓	✓	✓		✓	✓	✓	✓		✓
Internet Tools										
Stealth Mode	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Popup Blocking	✓	✓	✓							✓
Cookie Blocking	✓	✓	✓	✓				✓		✓
Spyware Blocking	✓	✓		✓		✓	✓	✓		✓
Browser History Blocking		✓								✓
Parental Controls		✓		✓						
Trusted Websites List	✓	✓	✓	✓	✓	✓	✓	✓		✓
Blocked Websites List	✓	✓	✓	✓	✓	✓	✓	✓		✓
Website History Log	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Setup and Management										
Password Protection	✓	✓	✓	✓	✓			✓		✓
Individual User Settings	✓	✓		✓						
Network Time Restrictions	✓	✓		✓	✓				✓	
Preset Firewall Defaults		✓	✓		✓	✓	✓	✓	✓	✓
Automatic Software Rules	✓	✓	✓	✓	✓		✓	✓		✓
Instantly Disable Firewall	✓	✓	✓	✓	✓		✓	✓	✓	
Instantly Block All Traffic	✓	✓	✓		✓	✓	✓	✓	✓	✓
Help/Support										
Phone Support	✓	✓	✓						✓	
Live Chat	✓	✓			✓					
Email or Online Forms	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Easy Upgrades	✓	✓	✓	✓	✓		✓	✓	✓	
Rank	GOLD	SILVER	BRONZE	4	5	6	7	8	9	10
TOP TEN PRODUCTS	Zone Alarm	Out Post	Norton	Norman	Surf Secret	McAfee	Bull Guard	Sygate	InJoy	BlackICE

Obr. 16. Multilaterálne hodnotenie najznámejších personálnych firewallov (r. 2006)

Za najlepší osobný firewall, ktorý je v súčasnosti dostupný na trhu sa považuje produkt ZonerAlarm Pro od firmy ZoneLabs založenej v San Franciscu. Licencia tohto riešenia je spoplatnená (cca $50 pre 1PC ročne) avšak jej light verzia v označení ZoneAlarm (momentálne ver 61.744.001) je voľne dostupný pre využitie v podmienkach domácností, malého alebo stredného biznisu. ZoneAlarm využíva prakticky všetky dostupné funkcie slúžiace k ochrane dát, je užívateľsky veľmi ľahko obsluhovateľný - táto modifikácia je plne automatická vrátane konfigurácie pri inštalácii a tak jeho prezentácia zamestnancom, ktorých náplňou pracovnej činnosti je práca s počítačom, bude nenáročná. Produkt sa okrem ochrany na úrovni vstupu a výstupu vyznačuje spoluprácou s antivírom, hlavne monitoringom aktuálnosti jeho vírovej databáze.

Za účelom zvýšenia informačnej obrany moderní firmy sa prikláňam k využitiu konceptu Jericho Forum (viz. kap 4) a produkt by som odporúčal inštalovať zvlášť na každý počítač, ktorý je napojený na podnikovú firemnú sieť. Tým by bola zabezpečená základná úroveň ochrany proti nebezpečným útokom voči obchodným informáciám a citlivým údajom (heslá, osobné materiály, atď.) ako i tých z prostredia samotnej organizácie (prevencia proti zapojeniu infikovaného laptopu manažéra v jeho kancelárii a pod.). Hlavným prínosom by bola samozrejme ochrana pri surfovaní zamestnancov v sieti Internet, kde sú pri vykonávaní podnikových cieľov vystavovaní nepravidelným externým útokom červov.

Obr. 17. Užívateľské prostredie ZoneAlarm

8.1.10.3 Softwarový antivír

K firewallu patrí jednoznačne i výkonné antivírové riešenie. Prakticky sa dnes antivír dodáva formou samoinštalačného balíka spolu s nákupom nového počítača. Azda každý antivír si je možno zadovážiť v časovo obmedzenej verzii na preskúšanie formou 30-dňovej lehoty (tzv. trial) alebo forme voľnej, spravidla o generáciu staršej a teda dnešným podmienkam už nepostačujúcej verzii (napr. AVG 7, Bit Defender 8). Ponúknuť spoľahlivý antivír, ktorý zabezpečí kvalitnú ochranu, kompatibilný a stabilný chod, minimálny zásah zo strany užívateľa či efektívny doplnkový balík služieb zo strany vývojára sa odvíja v značnej miere ani nie tak od množstva rôznych recenzií ako od dlhodobých praktických skúseností s konkrétnym produktom v konkrétnom prostredí. Keďže každý výrobca si háji svoje produkty a recenzie sa často prelínajú, rád by som prezentoval svoje skúsenosti s antivírovým softwarom.

Moje dlhoročné používanie antivírových produktov mi odhalilo niekoľko výhod i nevýhod ich používania. Samozrejme na trhu existuje celá rada produktov avšak ja uvádzam štvoricu tých, s ktorými som mal sám dočinenia, ako podklad mojej ďalšej selekcie.

Produkt	**NOD32**	**AVG**	**NORTON**	**AVAST**
Klady	vysoká miera detekcie, hlboká heuristika, kvalitatívna prestíž	vizuálne spracovanie, inštalačný sprievodca	vysoká miera podpory, vysoká miera detekcie	primitívne užívateľské prostredie, efektívny upgrade a aktualizácia
Zápory	vyššia užívateľská náročnosť	slabšia úroveň detekcie, dlhý skenovací čas	systémová náročnosť, príležitostná hardwarová nekompatibilita, inštalácia	príležitostná softwarová nekompatibilita

Tab. 2. Praktické zrovnanie slabých a silných stránok testovaných produktov

Ani jeden z mnou testovaných riešení nepriniesol kritické problémy, na druhej strane žiaden z nich nebol 100% spoľahlivý a drobným zásahom v podobe pár konfiguračných dolaďovaní alebo náznakov nestability sa samozrejme nedalo vyhnúť. Uznávam však, že práve na týchto situáciách sa budujú operačné skúsenosti. Ak by som teda mal príležitosť

inštalovať antivírové riešenie na počítače firemnej siete alebo iného ekonomického či spoločenského subjektu, zvolil by som jednoznačne NOD32 dynamického slovenského vývojára ESET. Svoje individuálne rozhodnutie by som rád utvrdil i oficiálnymi charakteristikami aktuálnej verzie (t.j. 2.5);

- najvyspelejšia heuristická analýza na svete (ThreatSense)
- minimálna hardwarová náročnosť
- multilaterálna obrana (nielen vírusy, ale i červy, spyware, adware, phising a i.)

Prostredie NOD32 je síce technickejšie koncipovaný, takže pre bežných užívateľov môže spočiatku pôsobiť chaoticky, no len po dobu kým sa oboznámi s jeho širokou ponukou nastavení a prispôsobení. Prakticky tento antivír pracuje v dvoch odlišných prostrediach – štandardnom skenovacom a komplexnom multifunkčnom (tzv. control center). Druhé z nich umožňuje individuálne operovať s týmito jednotlivými typmi skenerov;

- AMON ... rezidentný antivírusový monitor bežiaci na úrovni RAM
- NOD32 ... manuálne alebo plánom ovládaný skenovací systém
- IMON ..... skener prvej úrovne sledujúci internetovú trafiku (protokoly)
- EMON ... špeciálny mailový skener
- DMON ... skener vyvinutý na ochranu MS Office a downloadu z IE

Obr. 18. Antivírusový systém NOD32 ver. 2.5 (Windows 32 bit)

Produkt je možno zakúpiť vo väčšine špecializovaných predajní alebo elektronicky objednať priamo na stránke ESET. Cena štandardnej licencie na 1 rok vrátane ročnej podpory aktualizácií činí cca 1500 Kč. Pre podniky sú určené zvýhodnené multilicenčné balíčky a ESET dokonca poskytuje i 50% zľavy pre školské a zdravotnícke organizácie.

8.1.10.4 Antispyware a ďalšie obranné nástroje

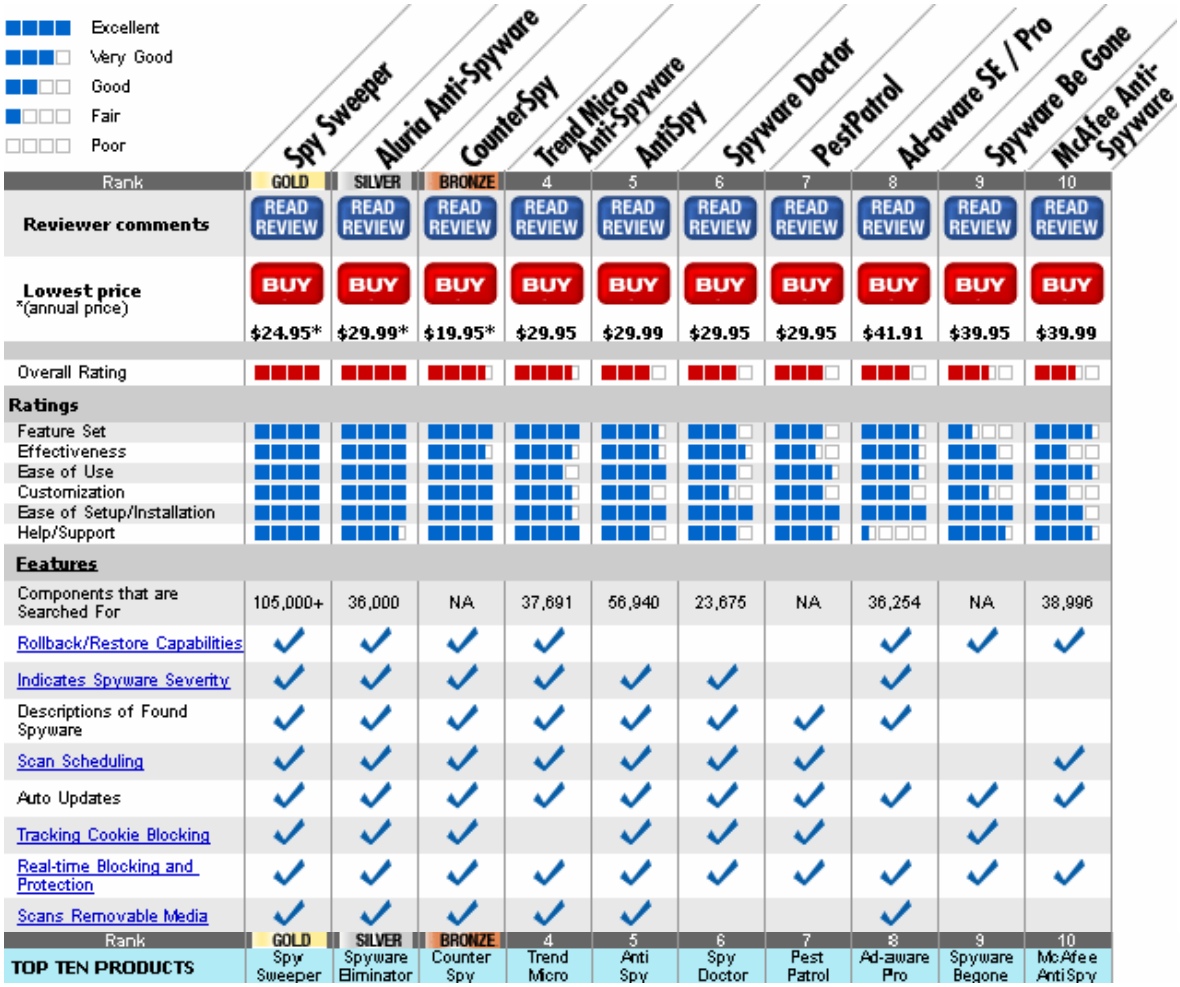
Ďalším obranným prvkom, ktorý zabezpečuje obranu na internej tak i externej úrovni sú relatívne nedávno vyvinuté a stále rozmach zažívajúce softwarové nástroje dedikované k eliminácii škodlivého kódu (spyware, adware, crimeware a i. - viz. kap. 5) nesúce prostý názov „antispyware“. Bojujú proti infiltráciám alebo usadeným formám špionážneho kódu. Ten je prítomný obvykle vo forme cookies alebo tzv. dočasných internetových súborov. Takto skryto modifikujú DNS údaje, vpašujú doplnky či skripty do prehliadača atď., avšak najhorším je skutočnosť, že všetko prebieha spôsobom, aby užívateľ nespozoroval žiadne kompromitujúce sa chovanie systému. Veľmi príležitostnými príznakmi, s ktorými som sa stretol, býva nečakaná zmena domovskej stránky, dlhší čas renderovania stránok, časté presmerovania stránok alebo prítomnosť podozrivých, opakujúcich sa reklamných odkazov.

Podľa aktuálnych štatistík vzrástol český a slovenský trh s bezpečnostným softwarom za posledné tri roky o takmer 50%. I tak mnoho organizácií v oboch krajinách ešte stále prevádzkuje výpočtovú infraštruktúru bez antispyware zabezpečenia. Na trhu v súčasnosti existuje asi 30 oficiálnych antispywarových riešení. Rád by som ale čitateľov upozornil na paradox, že mnoho takýchto voľne dostupných programov v skutočnosti predstavuje trojského koňa. Za spoľahlivé (overené) freeware antispywarové programy pre podniky preto považujem;

- Spybot - Search & Destroy (Patrick M. Kolla / Safer Networking Limited)
- Ad-Aware SE Personal (Lavasoft AB Sweden)
- Spyware Blaster (Javacool Software)
- CCleaner (Piriform)

Nakoľko sú produkty alokované zdarma, predstavujú relevantnú štartovaciu príležitosť pre všetky doposiaľ nezabezpečené ekonomické a spoločenské subjekty súkromnej i verejnej sféry. Po oboznámení sa s touto problematikou, obsluhou tohto druhu softwaru, by som ďalej budúcim CISO či manažérom podnikov, ktorí vážne prijali presvedčenie potreby bezpečnostných pravidiel nevyhnutných pre udržanie konkurencieschopnosti a zvýšenie efektivity hospodárenia, odporúčal testovať 30 dňové trial verzie komerčných vysokovýkonných nástrojov. Na rovnakom úseku IT infraštruktúry (vyznačujúcom sa rovnakou / podobnou činnosťou zamestnancov) by som zaviedol na každý počítač iný

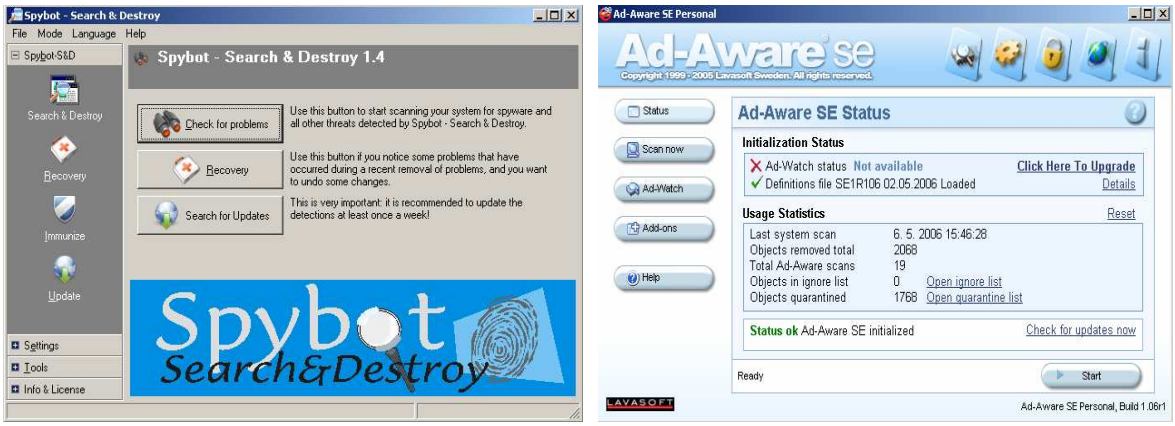
produkt a v priebehu stanovenej doby (min. 1 mesiaca) by som sledoval a zaznamenával ich efektivitu v obrane proti hrozbám. Je to z dôvodu, aby sa na príslušný predmet činnosti vykonávanej podnikateľskou jednotkou napasoval čo najprijateľnejší produkt skôr než dôjde k jeho reálnej kúpe. Ceny antispywarových programov sa pohybujú v cenovom rozpätí od 400 do 1000 Kč za jednoročnú podporovanú licenciu (systém je obdobný ako u antivírových produktov). Ponuka je v skutku veľmi široká a tak výber neadekvátneho programu by firme spôsoboval zbytočné finančné náklady, nehovoriac o miere vystavenia sa jej IS infraštruktúry zneužití dát. Pre náročných čitateľov dokladám i výsledky oficiálnych testerov komerčne dodávaných riešení. [20]



Obr. 19. Komerčný test antispyware (r. 2006)

Ako som uviedol, tieto riešenia je vhodné implementovať tam, kde sú na to vytvorené podmienky (finančné, organizačné, štrukturálne, racionálne). Pre živnosti, začínajúce podniky alebo podniky, ktorých hlavná oblasť činnosti kriticky nezávisí od informačných technológii, nemá význam investovať do drahých prostriedkov. Alternatívou k nim ostáva

vyššie uvedený freeware. Prednosťou naviac je možnosť bezplatnej vzájomnej kombinácie (napr. paralelné používanie Ad-aware SE a Spyboot S&D) produktov. Iným variantom môže byť používanie kombinácie freeware a trial verzií. (Ad-aware SE a Spy Sweeper trial). Organizáciou by bol primárne používaný freewarový produkt pričom raz za 15 (30) dní by sa využíval skener komerčnej trial verzie ako doplnok. Prínosom by bola opäť úspora nákladov za súčasného zvýšenia bezpečnosti nehmotných aktív.



Obr. 20. Sbybot a Ad-aware SE

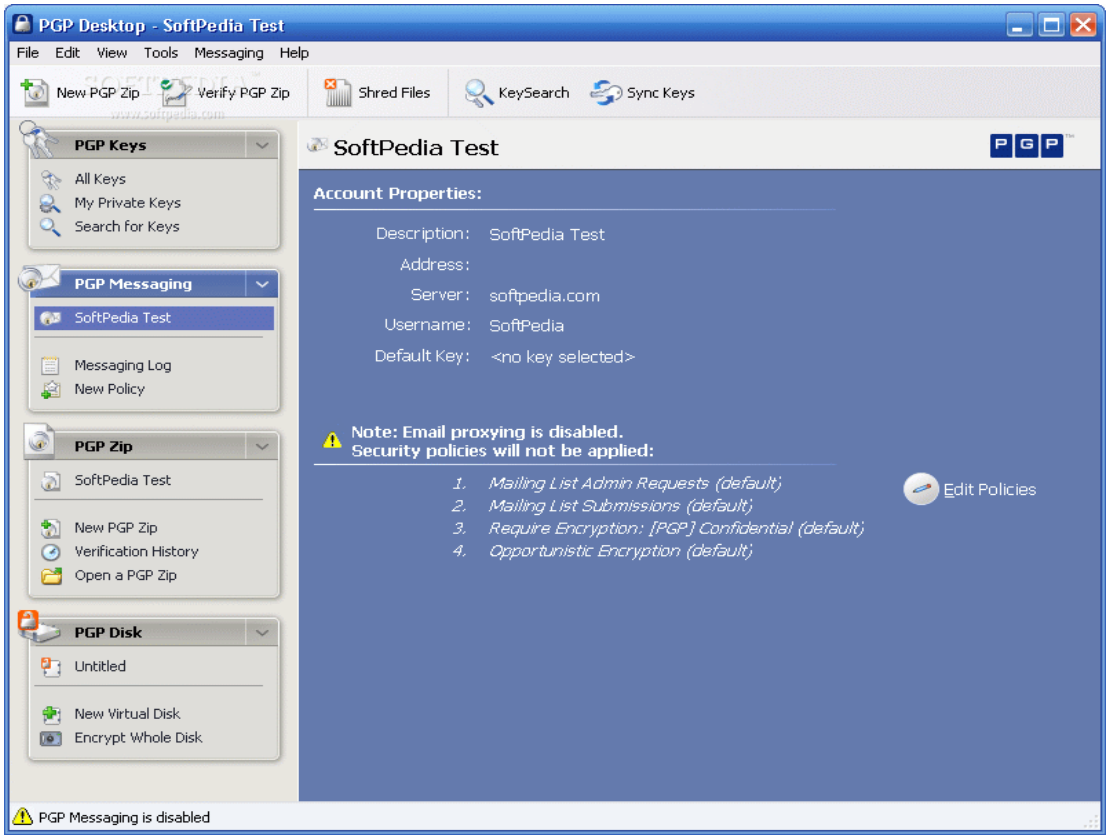
Okrem antispyware sa kvôli narastajúcim útokom využívajúcim sociálne inžinierstvo (phising, pharming a i.) v súčasnosti vyvíjajú i rôzne bezpečnostné nadstavby (addon) pre browsery, hlavne Internet Explorer. Spoločnosti by som ponúkol beta verziu špeciálnych antiphisingových panelov (toolbar), ktoré dokážu rozpoznať a včas upozorniť klienta na podozrivý obsah www stránky, a následne takéto internetové podvody zablokovať. Panely sú voľne dostupné na stránkach svojich výrobcov – Cloudmark, Netcraft alebo Nobox. Netreba zabúdať, že útoky využívajúce sociálne inžinierstvo si vyžadujú predovšetkým kompetentné preškolenie zamestnancov, bez ktorého je i implementácia technologických opatrení vo forme uvedených antiphisingových nástrojov zbytočná. Po jeho prevedení považujem panely za veľmi atraktívny a prínosný prvok.

Obr. 21. Antiphisingový toolbar Cloudmark 1.0 beta pre IE

8.1.10.5 Kryptografické a ďalšie vybavenie

Veľmi dôležitým implementačným aspektom je zabezpečenie dát a znalostí šifrovaním. To sa môže odohrávať na rovinách softwarovej a technickej (hardwarovej). K tomu sú prispôsobené i nasledovné produkty.

PGP Desktop v 9.0.5



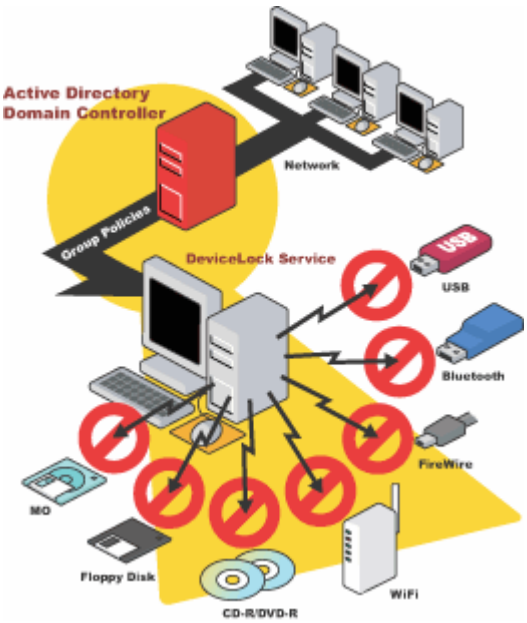
Obr. 22. PGP Desktop 9.0.5

Z pohľadu vnútropodnikového nasadenia je PGP komplexný program pre šifrovanie emailových správ, príloh, udeľovanie elektronických podpisov, vytváranie zabezpečených záloh (archívov), šifrovanie diskových jednotiek a efektívne premazanie súborov či celého disku. Samozrejme disponuje aj ďalšími nástrojmi, ktorých ponuka sa líši od druhu licencie. Čo je však podstatné, samotný PGP Desktop (ver. 9.0.5) je výrobcom dodávaný ako špeciálny trial, kde sa po uplynutí lehoty nezablokujú všetky jeho funkcie, ale tie nosné (šifrovanie dát, elektronický podpis), známe ako „PGP Freeware“ ostávajú pre klienta plne funkčné. PGP sa dnes radí medzi elementárne programové vybavenie moderných firiem, ktoré úspešne zvládli „preklopenie“ informačných znalostí do praxe.

Device Lock v 5.7.3

Všetky doposiaľ uvádzané produkty, ktoré majú umožniť zvýšiť konkurencieschopnosť, zefektívniť hospodárenie alebo prosto zaistiť ochranu dát organizácie, zaisťujú ochranu nielen proti interným ale aj externým útokom. Šifrovacie a antivírové programy sú nevyhnutným nástrojom bezpečnostnej politiky, určite by však nemali byť nástrojom jediným. Dramaticky nárast počtu zariadení pre ukladanie dát prehĺbil vážne bezpečnostné riziká, ktorým nemožno čeliť prostým nastavením zásad skupín. Kapacita prenosných zariadení sa neustále zvyšuje zatiaľ čo ich veľkosť sa zmenšuje. Proti útokom cez WiFi alebo Bluetooth sú rôzne nastavenia vo Windows bezradné. Jedným z možných riešení je nasadiť v celej počítačovej sieti software DeviceLock, vyvinutý spoločnosťou SmartLine Inc. Umožňuje správcovi siete predovšetkým;

- povoľovať / zakazovať prístup k zariadeniam / rozhraniam
- nastavovať oprávnenia pre jednotlivých užívateľov i skupiny užívateľov
- priraďovať prístupové práva pre určitý typ zariadenia či rozhranie
- povoľovať jednotkám a mechanikám čítanie, nie však zápis



Obr. 23. DeviceLock v praxi

Medzi užívateľov DeviceLock patrí rada predných firiem i vládnych inštitúcií (napr. USAF, HSBC Bank, Ferrari). Program nekompromisne reaguje voči nelojálnym alebo nespoľahlivým zamestnancom a zároveň napomáha právu na ochranu osobných údajov či obchodného tajomstva. Cena produktu je v súčasnosti 850 Kč a v ČR ho distribuuje spoločnosť Jimaz.

SafeNet iKey 1000

Medzi posledný bezpečnostný prvok, ktorý sa dá považovať za dôležitú a možno trochu kontroverznú súčasť riadnej bezpečnostnej politiky (kap. 4.2), sú USB tokeny. Na našom trhu sú zatiaľ ponúkané dva druhy tokenov – biometrické a kryptografické. Keďže biometrické tokeny nie sú ešte spoľahlivé a stále sa rieši mnoho problémov s ich prevádzkou, racionálnejšie je využívať šifrovací token. Cenovo prijateľnou alternatívou je produkt iKey 1000 od spoločnosti SafeNet, ktorý je určený na zabezpečenie prístupu do počítačových sietí, VPN, intranetu / internetu, pre uloženie digitálnych certifikátov, pre nasadenie v aplikáciách e-business, elektronického podpisu a PKI. Podporuje, obdobne ako smart karty, zabezpečenie pomocou PIN kódu (hesla), ponúka kryptografické funkcie MD5 a RSA (1024 bitov). Token je kompatibilní s USB1.1 a USB2.0. Privátny kľúč sa generuje na tokene a nemožno ho z tokenu ani vyexportovať, ten token nikdy neopúšťa).

Obr. 24. SafeNet iKey 1000

Cena produktu je 700 Kč (údaj je z 6.5.2006, www.alzasoft.cz). Nasadenie tokenov nie je vždy vítaným prvkom, zvlášť zo strany zamestnancov. Pre manažment zas predstavuje dodatočné náklady spojené s kúpou, zaškolením a monitorovaním ich využívania. Nakoľko som presvedčení o ich funkcii v bezpečnostnej politike, jedná sa skôr o prvok akejsi prestíže než výrazný úžitok z jeho implementácie.

8.1.11 Príklad kombinácie IT bezpečnostného vybavenia pre organizácie

V tejto záverečnej kapitole praktickej sekcie práce pojednávajúcej o technickej a technologickej synchronizácii uvádzam resumé navrhovaných implementačných prvkov.

č.	nástroj	produkt	výrobca	licencia	náklady
1	*browser*	Opera 8.5	Opera Software ASA	freeware	0,-
2	*firewall*	ZoneAlarm	ZoneLabs	freeware	0,-
3	*antivír*	NOD 32 Pro Edition	Eset	commercial	1500,- lic.
4	*antispyware*	Ad-aware SE	Lavasoft AB	freeware	0,-
5	*antiphising*	Cloudmark 1.0 beta *	Cloudmark	freeware	0,-
6	*šifrovací sw*	PGP Desktop	PGP Corporation	trialware	0,-
7	*bezpečnostný sw*	DeviceLock	SmartLine	commercial	850,-
8	*bezpečnostný hw*	iKey 1000 *	SafeNet	purchase	700,-

* voliteľné vybavenie **3050,-**

		prevencia							
druh útoku	**typ útoku**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
virtuálna infiltrácia	vírus			x				x	
	trojan	x	x	x	x			x	
	spyware		x	x	x				
	adaware	x	x	x	x	x			
	crimeware					x			
fyzická infiltrácia	krádež identity							x	x
	krádež dát						x	x	

	oblasť zabezpečenia							
pracovné prostredie	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
MS Office								
elektronická pošta								
www								
Windows								

Tab. 3 - 4. Resumé odporúčaných technických a technologických obranných riešení

Všetky systémy sú navrhované pre OS Windows 9X a vyšší s dôrazom na čo najnižšie hardwarové nároky. Častou chybou, na ktorú sa obzvlášť zabúda pri synchronizácii týchto opatrení je možnosť ich kolidovania, ak sa budú na počítači naďalej používať nevhodné programy typické antiefektom. Z nedávno uskutočnených výskumov plynie, že 10 % zamestnancov sa vo voľných chvíľkach oddáva on-line hrám a veľká väčšina sa priznala,

že neraz trávi svoje momenty v práci prezeraním si rodinných fotiek, siahaním na servery internetového zdieľania súborov (tie sú často ilegálne) alebo na komunikačný software. Pritom, ako uvádzajú štatistiky, len 61 % z nich tuší alebo približne vie, čo je to počítačový vírus. V záujme bezpečnosti zostáva riešením len razantný a dynamický krok stojací na týchto troch pilieroch;

- eliminovať prítomnosť alebo možnosť využitia nevhodných programov
- uskutočňovať pravidelné školenia pre zamestnancov
- prísne monitorovať dodržiavanie zásad a pravidiel bezpečnostnej politiky

Firma by mala zakázať (neinštalovať) predovšetkým používanie týchto programov;

- Windows Messenger (príkazom „msconfig“ alebo programom Xp-Antispy)
- ICQ, Skype, Miranda a pod.
- P2P klienti (napr. DC, StrongDC, DC++, Shareaza)
- Windows hry (dáma online a pod.)

Na podporu bezpečnosti sa dodatočne odporúčam oboznámiť s využitím týchto nástrojov;

I. Password Safe (www.schneier.com) ... systematická správa hesiel

II. Process Explorer (www.sysinternals.com) ... sledovanie bežiacich úloh systému

III. Autoruns (www.sysinternals.com) ... management Windows služby „Po spustení“

IV. Xp-Antispy (www.xp-antispy.org) ... utilita na konfiguráciu niektorých služieb

V. MS Baseline Security Analyser ... bezplatný nástroj k sledovaniu stavu aktualizácií

Nakoniec je dôležité, aby administrátorom (CIO) vašej firmy bola vysoko lojálna osoba. Tá totiž predstavuje mozog IT bezpečnosti a preto efektívna komunikácia medzi CISO a CIO je kľúčovým základom úspechu modernej firmy (kap. 3.1.2). Sledovanie toho istého cieľu oboma riaditeľmi a plné, jasnou víziou motivované nasadenie ich kompetencií, musí byť pre dosiahnutie pokroku samozrejmosťou. CISO má byť informovaný o činnosti

svojho kolegu a naopak. CIO nemôže implementovať riešenia bez vedomia a súhlasu CISO.

8.2 Synchronizácia sociotechnických prvkov

V teoretickej časti som definoval sociálne inžinierstvo ako bystré manipulovanie prirodzenej ľudskej dôvery útočníkom (hackerom) s cieľom obdŕžať také informácie, ktoré mu umožnia získať nepovolený prístup k systému s cennými informáciami. Výsledkom býva vždy ujma a ohrozenie chodu organizácie. Firmy, ktoré sa špecializujú na penetračné testy bezpečnostných systémov, uvádzajú, že pokusy nabúrať sa do počítačového systému zákazníka pomocou sociotechnických metód sú skoro stopercentne účinné. Existuje iba jeden spôsob ochrany – mať vyškolený, informovaný a svedomitý personál. Chyba, ktorej sa mnoho organizácií dopúšťa, spočíva v príprave obrany len na fyzickej úrovni. Management si musí uvedomiť dôležitosť rozvoja, implementácie komplexnej bezpečnostnej politiky a procedúr. Všetky peniaze, ktoré sa minú na softwarové záplaty, bezpečnostný hardware a audity budú bez adekvátnej prevencie sociálneho inžinierstva iba mrhaním času a peňažných prostriedkov. Silná politika môže byť všeobecná alebo špecifická, odporúča sa akási polovičatá. Tá poskytuje správcom istú dávku flexibility vo vývoji procedúr do budúcna a zároveň limituje personál, aby neochaboval v otázke zodpovednosti.

8.2.1 Prevencia pred fyzickým útokom

Teoreticky vyznieva fyzické zabezpečenie navonok azda nepodstatne. Pre účel zadržania úniku obchodných tajomstiev, marketingových a finančných informácií či akýchkoľvek informácii, ktoré majú pre činnosť firmy zásadný význam a nie sú určené verejnosti z objektu sa požaduje zvláštna ostražitosť. Každý, kto vstupuje do budovy má podstúpiť overenie svojho identifikačného čísla. Žiadne výnimky sa nesmú tolerovať. Niektoré obchodné dokumenty si vyžadujú fyzické uzamknutie v kartotékach a iných bezpečných skladovacích miestach (kľúče potom uložiť na skrytých miestach). Ďalšie dokumenty si zas vyžadujú skartáciu pred ich definitívnym vyradením do kontajnerov. Taktiež všetky magnetické médiá by mali byť hĺbkovo premazané, keďže dáta sa dajú obnoviť i z formátovaných diskov a pevných diskov. Kontajnery majú byť zabezpečené zámkom a uložené na mieste, kde budú pod dohľadom bezpečnostnej služby. Všetky stroje vo vnútri budovy musia byť dôkladne zabezpečené riadne implementovanými heslami a to

i heslami pre šetriče obrazoviek. PGP a ďalšie kryptovacie programy sa dajú vhodne využiť k zašifrovaniu tajných súborov alebo rovno celých pevných diskov.

8.2.2 Používanie telefónu

Jeden z podfukov poukazuje na nedovolené umiestnenie nástroja naprieč privátnou telefónnou sieťou podniku. Hacker ňou môže zavolať do firmy, zahrať svoj trik so zosobnením, požiadať o presmerovanie na vonkajšiu linku a potom telefonovať do celého sveta na účet tohto podniku. Tomuto sa dá zabrániť ustanovením politík, ktoré zakazujú presmerovania, kontrolujú zámorské hovory či hovory na dlhú vzdialenosť a vystopujú podozrivé telefonáty. Ak napríklad niekto volá a vydáva sa za telefónneho technika, ktorý potrebuje heslo k získaniu prístupu, je jasné, že klame. Telefónni technici dokážu viesť testy liniek bez podpory zamestnanca, preto akékoľvek požiadavky alebo iné autentizácie majú byť automaticky považované za podozrivé. Preto všetci zamestnanci by si mali byť vedomí takýchto sociotechnických taktík. Majoritným cieľom takýchto útokov sociálneho inžinierstva býva ústredňa, call centrum či linka zákazníkom. Najlepším spôsobom ochrany je školenie pracovníkov. Ústredňa má odmietať poskytnutia hesiel bez dostatočnej autorizácie (čo má byť nakoniec jedným z prvkov organizačnej politiky), aby heslá neboli nikdy odhaľované cez telefón alebo email. Recipročné hovory, PIN a heslá predstavujú zopár návodov pre zvýšenie bezpečnosti. Operátor má jednoducho odmietať podporu resp. vedieť povedať dotyčnému nie v prípade, že pociťuje pochybnosti.

8.2.3 Školenie zamestnancov

Školenia v oblasti SI presahujú rámec firemnej ústredne a ich význam sa dotýka celej organizácie. Podľa expertov na tajné informácie, zamestnanci musia byť trénovaný takým spôsobom, aby ľahko identifikovali všetky druhy informácii a mohli tak následne niesť zodpovednosť za ich ochranu. Niektorí odborníci tiež odporúčajú, aby 40 % rozpočtu určeného na bezpečnosť bolo pridelených na proces neustáleho precvičovania pracovníkov v oblasti SI. Organizácie, ktorým záleží na prosperite, majú prijať počítačovú bezpečnosť ako rutinnú súčasť vykonávaných podnikových činností. Každá osoba, bez ohľadu na to či pracuje s počítačom, si má byť vedomá, prečo je informáciám prideľovaná taká dôležitosť, že práve z nich profituje samotná organizácia. Z tohto dôvodu má byť povinnosťou každého pracovníka absolvovanie výcviku, ktorý pomôže ozrejmiť postupy, ako chrániť citlivé dáta pred ich nežiaducim únikom na verejnosť resp. ku konkurencii a ako byť čo

najlepšie zainteresovaný v samotnej bezpečnostnej politike firmy. Zabezpečiť aktualizáciu poznatkov zamestnancov sa obvykle darí prostredníctvom prednášok, realizovaných buď v pravidelných intervaloch (napr. mesačne) alebo nepravidelne v závislosti od potreby. Samozrejmou súčasťou prednášok by sa mali stať praktické príklady súčasných hrozieb s ukážkami ich následnej eliminácie, prevencie alebo inej príslušnej reakcie. Koordinátorom a zodpovednou osobou za školenie by mal byť CISO, poverený so súhlasom generálneho riaditeľa, asistenciu môže dotvárať riaditeľ informatiky (CIO) a personálny riaditeľ (HRO) (viz. Obr. 2). Predmetom školenia by malo byť;

- oboznámenie sa s aktuálnym stavom IT bezpečnosti v organizácii
- oboznámenie sa s aktuálnym stavom IT bezpečnosti vo svete
- aktuálne trendy vo svete
- momentálne ciele podniku (celkové a v oblasti zabezpečenia IS)
- voľná a rovnocenná diskusia (brainstorming)
- uistenie sa, že všetci účastníci rozumejú dôvodom zavedenia jednotlivých princípov

Inou možnosťou informovanosti sú vnútrofiremné periodiká, ktoré takisto môžu ponúkať aktuality z reálnych situácií života podniku. V súčasnosti organizácie pre zvyšovanie znalostí svojich zamestnancov využívajú kombinácie týchto nástrojov – stručné tematické videá, brožúrky, vestníky, symboly, plagáty, hrnčeky na kávu, perá, ceruzky, potlačené počítačové myši, šetriče obrazoviek, prihlasovacie bannery, poznámkové bloky, stolné artefakty, tričká alebo nálepky. Aby zamestnanci postupne nestrácali pohľad na zmysel týchto predmetov, malo by sa zaistiť ich účinne striedanie.

8.2.4 Zvyšovanie lojality zamestnancov

Vydanie brožúrky o bezpečnosti informácií samo o sebe riziko nezmenšuje. Každá firma musí zásady nielen písomne či inak definovať, ale musí vynaložiť dodatočné úsilie s cieľom presvedčiť všetky osoby, ktoré majú dočinenia s informáciami alebo počítačovými systémami, aby sa zásady naučili a podľa nich tiež postupovali. Lojalita zamestnancov hraje pri budovaní ich imunity voči SI útokom veľmi dôležitú rolu. Totižto zamestnanec, ktorého podstúpime odbornému školeniu, musí byť plne motivovaný

a zaangažovaný do procesov ochrany informačného majetku firmy. V opačnom prípade stráca celý proces svoj význam pretože vo firme by bol stále prítomný niekto, komu na zdraví firmy viac či menej nezáleží alebo sa k udalostiam stavia benevolentne. V dnešných tvrdých tržných podmienkach sa kvalita ľudských zdrojov nepochybne podpisuje pod konkurenčnú výhodu firmy. Totižto najväčšie bohatstvo moderného podniku tkvie v ľuďoch, ktorí tam pracujú a to v ich schopnosti myslieť, tvoriť a komunikovať. Zvyšovanie lojality sa dosahuje spoluprácou danou antropocentrickou orientáciou systému riadenia ľudských zdrojov. Tá sa vyznačuje tým, že každý pracovník je rešpektovaný ako nevyhnutná súčasť procesov, vnímaný ako základný faktor výroby a vysoký dôraz je kladený na sociálne faktory. Ako vhodný návod v rámci usilovania sa o zvýšenie lojality zamestnancov môžu poslúžiť otázky typu;

- je podriadený vnímaný ako objekt manipulácie alebo ako subjekt spolupráce
- chcú zamestnanci pracovať alebo musia pracovať
- má pracovník vytvorené aspoň také podmienky ako stroje, hodnota ergonómie
- ako efektívny je zavedený motivačný program, organizácia práce a mzdový systém
- je si každý pracovník vedomý čo, ako a prečo vykonávať svoju úlohu

Ďalej sa v otázke lojality silne odporúča prepracovaný systém odmien, potreba vyjadrovať uznanie pracovníkom, ktorí odhalili sociotechnický útok, zabránili alebo sa nejako ináč zaslúžili o úspech informačného bezpečnostného programu. Existuje ale i druhá strana mince. Ľudia si musia byť vedomí dôsledkov, keď sa nebudú prispôsobovať bezpečnostným postupom, či už z ľahostajnosti alebo z vzdoru. Všetci robíme chyby, ale opakujúce sa prípady porušovania pravidiel nemôžu byť tolerované.

8.2.5 Spozorovanie útoku

Bez poznania útočníka a štúdia jeho taktiky sa nemožno účinne brániť. Existujú tieto varovné príznaky pre identifikáciu útokov; neochota poskytnúť kontaktné údaje, naliehanie, obháňanie sa známosťami, pochlebovanie, zastrašovanie, flirtovanie, komunikačné chyby (nepresné vyslovovanie mien alebo názvov), atypické otázky a nakoniec požadovanie zakázaných informácií. Okrem toho je potrebné mať sa dostatočne na pozore pred situáciami, ktoré sa javia divne a snažiť sa premýšľať ako hacker (kto sa

nevie vžiť do role nepriateľa, nemôže ho poznať). Je dôležité, aby mal zamestnanec v momente, keď detekuje niečo podozrivé, možnosť reflexívne hlásiť incident svojim nadriadeným a CISO. V tom istom okamihu je tiež povinný čo najrýchlejšie informovať ostatných pracovníkov úseku, keďže sú vystavený tomu istému nebezpečenstvu.

Nasledujúca tabuľka obsahuje zopár najobvyklejších úrovní útoku a prisluhujúce stratégie;

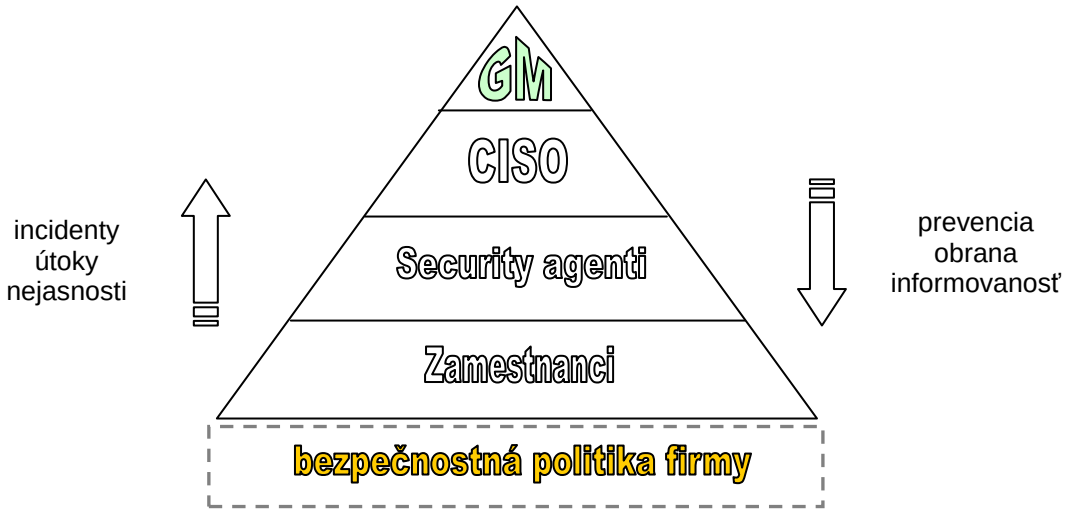
Oblasť rizika	**Taktika hackera**	**Obranná stratégia**
Telefón (ústredňa)	prehováranie	výcvik zamestnancov, nevydávanie hesiel a iných tajných informácií telefónom za žiadnych okolností, vybavenie pracovníkov špecifickým PIN
Vstup do objektu	neautorizované fyzické vniknutie	výcvik ostražitosti zamestnancov, kompetentnosť bezpečnostnej služby
Kancelária	špehovanie	obozretné zadávanie hesiel a PIN do IS
Telefón (ústredňa)	zosobňovanie	vybavenie zamestnancov PIN kódom pre prístup k help desku
Kancelária	túlanie sa po chodbách hľadajúc otvorenú miestnosť	sprevádzanie všetkých hostí, zavedenie visačiek pre zamestnancov i hostí
Poštová miestnosť	podstrčenie falošných memoránd	zamykanie a monitorovanie poštovej miestnosti
Telefón	krádež prístupu telefónnej linky	kontrolovať a mapovať diaľkové hovory, odmietať presmerovania
Kontajnery	kontajnerový lov	ponechať smeti v bezpečnej, monitorovanej oblasti, skartovávať dôležité dáta, mazať magnetické pásky
Intranet / Internet	tvorba a nasadenie trojanov do prostredia intranetu / internetu	kontinuálne sledovanie zmien v systéme, školenie používania silných hesiel
Kancelária	krádež citlivých dokumentov	označovanie dokumentov stupňom dôveryhodnosti, dbanie na ich neprístupnosť, bezpečné a zašifrované skladovanie
Všeobecne - psychologická	zosobňovania a presviedčania	udržiavanie bdelosti pracovníkov prostredníctvom bezpečnostnej politiky a školení

Tab. 5. Najbežnejšie sociotechnické prieniky a prevenčné stratégie

9 PONUKA BEZPEČNOSTNÉHO RIEŠENIA IS ORGANIZÁCIE

Tejto poslednej kapitole je venovaný návrh bezpečnostného systému informačnej obrany modernej firmy. Na základe preskúmaných aktuálnych informačných zdrojov ako aj praktických skúseností sa pokúsim ponúknuť koncepčný rámec bezpečnostného riešenia. Som presvedčený o jeho výhodnom uplatnení zvlášť v podmienkach malých a stredných podnikov vybavených modernou počítačovou sieťou, ktoré plánujú v krátkom období zostaviť a zaviesť vlastnú bezpečnostnú politiku. Bodovo usporiadané odporúčané postupy a praktiky sú zamerané na každodennú minimalizáciu rizika spojeného so sociotechnikou.

Organizačná štruktúra z hľadiska bezpečnosti:



Security agenti by boli špeciálne poverení a vysoko lojálni zamestnanci firmy, ktorý by reflexívne vykonávali všetky pokyny CISO, podliehali neustálemu školeniu a každodenne poskytovali nevyhnutnú oporu zamestnancom v oblasti bezpečnosti. Klasifikovali by sa na;

- príslušníkov zaisťujúcich fyzickú bezpečnosť (ochranka)
- príslušníkov dozoru a kontroly (recepčný, operátor, vedúci oddelenia)
- príslušníkov dátovej ochrany (správca siete, aplikácií, vedúci kryptografie)
- špecialistov pre údržbu bezpečnostného systému (technik, technológ)
- špecialistov na oblasť priemyselnej špionáže (firemný detektív)

Zložky fyzickej bezpečnosti:

1. precízna kontrola všetkých osôb na vstupe / výstupe do objektu – kontrola dokladov totožnosti vrátane fotografie, zaznamenanie účelu a času návštevy, zákaz pašovania akýchkoľvek dátových nosičov (najmä mp3 prehrávačov a CD), zákaz odnášania a donášania akejkoľvek vlastnej elektroniky na pracovisko vrátane mobilného telefónu či nadštandardných hodiniek
2. opatrenie každého nového návštevníka viditeľným (farebne odlišným) identifikátorom a zabezpečenie sprievodu na požadované miesto / k požadovanej osobe, informovanie dotyčnej osoby o návšteve a odhadnutie približnej dĺžky návštevy
3. opatrenie zamestnanca jeho firemným tokenom a identifikátorom s fotografiou, prípadne ďalším pracovným vybavením, stíhanie zamestnancov nerešpektujúcich bezpečnostné nariadenia (vykonávanie dozoru vedúcim oddelenia)
4. inštalovanie biometrických systémov autentizácie (odtlačky prstov resp. skener očnej sietnice) a zároveň PIN identifikátorov na vstupoch do jednotlivých oddelení alebo citlivých miestností, pokrytie interiéru a exteriéru objektu (aj skládky odpadu) kamerovým systémom
5. dôkladné kontrolovanie odchádzajúcej a prichádzajúcej pošty, odovzdanie pošty pre zamestnanca došlej počas dňa až po uplynutí jeho pracovnej doby, vedenie knihy o prevzatých zásielkach (vrátane údajov totožnosti)
6. neponechávanie žiadnych súkromných, pracovných alebo iných obchodných dokladov a písomností „na očiach“, dbanie na udržiavanie poriadku, systematickosti a čistoty pracoviska, nevynášanie takýchto materiálov z ich miestností (napr. na toaletu)
7. vysoké, kontinuálne fyzické (ochranka) a technologické (dvojúrovňové) zabezpečenie serverovej miestnosti, dátového centra (úložišťa záloh) a archívov s citlivými údajmi bez ohľadu na ich podobu

Zložky informačnej bezpečnosti:

1. dôsledné identifikovanie a zaznamenávanie všetkých povolených telefónnych hovorov z a do organizácie s 10-dňovou lehotou uchovania záznamu, zákaz realizovania externých hovorov zamestnancom počas riadnej pracovnej doby prípadne len

s osobným / odôvodneným povolením CISO, prenechávanie odkazov správcom ústredne zamestnancom zo všetkých prijatých hovorov do firmy (neexistuje priamy telefónny kontakt zamestnanca s volajúcou osobou), podrobné analyzovanie takýchto hovorov (kto, odkiaľ, dôvod telefonátu), po ich preverení ďalšou osobou sú v závislosti na ich urgentnosti predané príslušnému pracovníkovi

2. nepredávanie nijakých hesiel, PIN, súkromných, tajných alebo citlivých obchodných informácií po telefóne za žiadnych okolností žiadnym osobám alebo len s uvedomelým momentálnym povolením CISO, odmietanie poskytnutia pomoci či inej služby neautorizovaným osobám po telefóne, znemožnenie zamestnancom participovať na akýchkoľvek telefónnych anketách, prieskumoch, ponechávať heslá v hlasovej schránke, dôsledná identifikácia odosielateľa prijatého faxu
3. naprogramovanie hlasových schránok tak, aby sa po pár neúspešných pokusoch automaticky zablokovali, znemožnenie presmerovania hovorov prostredníctvom telefónnych čísel používaných pre fax alebo modem na vonkajšie čísla
4. vytvorenie internej horúcej linky ohlasovania incidentov či nejasností s ľahko zapamätateľným číslom
5. označenie všetkých možných nosičov dát, znemožnenie vytvárania ich kópii (s výnimkou záloh)
6. zaistenie každého počítača silným bootovacím heslom, využívanie prideleného tokenu a silných hesiel pre vstup do prostredia OS (podľa 8.1.4), implementácia bezpečnostného vybavenia a opatrení (podľa 8.1.11) využitím koncepcie organizácie Jericho fórum, aktívne šifrovanie a zálohovanie dát
7. realizovanie pravidelných povinných školení zamestnancov v oblasti sociálneho inžinierstva

10 VYHODNOTENIE BEZPEČNOSTNÉHO PRIESKUMU

Univerzita Tomáše Bati ve Zlíně v spolupráci s partnermi informačných technológií uskutočnila dňa 14. marca 2006, v rámci akcie Březen – měsíc Internetu, 8. ročník konferencie s názvom „Internet a bezpečnost organizací 2006“. Organizátorom bol Ústav informatiky a štatistiky FaME UTB a konferencia sa tešila medzinárodnej účasti. Jej cieľom bolo predovšetkým;

- predstavenie technológii podporujúcich on-line krízové riadenie a strategické rozhodovanie
- vzájomná výmena poznatkov teórie a praxe z internetových aplikácií v organizáciách štátnej správy, verejného sektoru a podniku
- metódy a možnosti predvídania bezpečnostných incidentov
- bezpečnosť informácii a elektronický marketing

V rámci akcie, ktorej hostia boli predstavitelia z rôznych oblastí súkromného sektoru a štátnej správy, bol distribuovaný dotazník (PRÍLOHA P 5) v celkovom náklade 100 ks. Dotazník bol zostavený využitím marketingových znalostí získaných v priebehu štúdia. Jeho prvotná verzia (PRÍLOHA P 4) sa podľa predstáv garanta podrobila úpravám do konečnej podoby. Deväť otázok dotazníku bolo zámerne koncipovaných štýlom, aby účastníci odhalili svoj bezpečnostný status a dostali priestor k vyjadreniu svojich pocitov i skúsenosti s riadením bezpečnostných rizík IT. Kategorizačné otázky dotazníku boli predmet činnosti organizácie a veľkosť organizácie.

Z celkového počtu 100 ks sa vrátilo naspäť 76. Niektoré dotazníky neobsahovali odpovede na všetky dotazy, odpovede boli neúplné či nejasné. Tieto boli z hodnotenia vyradené. Celkový počet relevantných dotazníkov, ktoré mohli postúpiť do fázy analýzy bol 54.

Je nutné podotknúť, že prieskum neslúžil ako primárny cieľ praktického výstupu bakalárskej práce, ale skôr ako bonus čitateľovi. Preto neboli stanovené žiadne hypotézy, jediné čo prieskum sledoval bol test kompetentností pri pojme informačná bezpečnosť. Otázky 7 a 8 boli využité pre interné potreby autora a preto ich výsledky neboli spracované do grafickej podoby. Zaujímavosťou je komplexná korelačná analýza prieskumu. Graficky

znázornené dendogramy ukazujú, ktoré položky prieskumu sa najviac ovplyvňujú a akým spôsobom. Najväčšia závislosť bola spozorovaná medzi;

- percentom výdajov na bezpečnosť a biometrikou
- fyzickou kontrolou bezpečnosti a žiadnym systémom zabezpečenia
- spokojnosťou s bezpečnostnou ponukou trhu a prítomnosťou bezpečnostnej politiky

Prvá závislosť poukazuje na nárast nákladov pri zvyšovaní kvality zabezpečenia. Biometrické bezpečnostné systémy patria medzi finančne náročnejšie produkty z pohľadu ich implementácie, údržby a spotreby energie. Preto by ich mali zavádzať také organizácie, ktoré sa vyznačujú solventnosťou a schopnosťou dosiahnuť efektívneho návratu investícií. Druhá závislosť odráža skutočnosť, že väčšina firiem stále najviac dôveruje prostej fyzickej kontrole. Avšak bez flexibility a udržiavania trendu v oblasti bezpečnosti je len otázkou času, kedy sa stanú obeťou útokov využívajúcich sociálne inžinierstvo. Poslednú silnú väzbu utvára spokojnosť tých, ktorí úspešne zvládli zavedenie bezpečnostnej politiky a IT systémov a teraz profitujú na poli konkurencieschopnosti a úspore nákladov.

Prieskum realizovaný na vzorke prítomných respondentov prakticky potvrdil to, čo bolo predmetom tejto práce, o čom informujú média a varuje Internet. Súčasná situácia vo virtuálnom svete je vážna a problém tkvie niekde v ľuďoch. Tri štvrtiny incidentov tvoria interné útoky pričom 40 % organizácií v súčasností stále nemá vypracovanú bezpečnostnú politiku. Z celkových výdajov sa v priemere na bezpečnosť odvádza 14 %, najčastejšie cca 10 %, údaje ale vysoko závisia od odvetvovej činnosti. Napriek dopytu je ponuka produktov tohto segmentu stále nepostačujúca a preto hlavným druhom obrany zostáva spomínaná fyzická kontrola. Aby nechradla, musí manažment uznať potrebu kontinuálneho vzdelávania sa personálu v oblasti bezpečnosti a sociálneho inžinierstva.

Nielen tuzemsko, ale celý región V4 zaostáva v informačných technológiách za západnými krajinami, preto sa ešte len očakáva hlavný prúd informačnej vlny do našej spoločnosti. S narastajúcou kvalitou a kvantitou technológii musíme byť vždy pripravení čeliť novým hrozbám a nepokojom.

Vyhodnotenie prieskumu je spracované v prílohe.

ZÁVER

Bakalárska práca potvrdila skutočnosť, že pre dnešné organizácie štátnej, komunálnej i súkromnej sféry je okrem prvkov ekonomického subsystému nevyhnutné poznať, efektívne riadiť a paralelne využívať i prvky technologického subsystému spoločnosti. Je to dané minimálne z týchto dvoch dôvodov;

- prítomnosť globalizácie vo svete
- snaha o efektívnu konkurencieschopnosť na trhu

Globalizácia funguje prostredníctvom rozšírenej informatizácie spoločnosti. Základom sú pokročilé on-line funkcie Internetu (využiteľné pre S.W.I.F.T. v bankovníctve a pod.) umožňujúce operácie v reálnom čase. Keďže Internet je miestom, kde denne dochádza k nežiaducim infiltráciám a kompromitáciám dát, je v záujme modernej inštitúcie, aby dokázala zaistiť obranu vlastných znalostí (obchodných a ďalších citlivých informácií) implementáciou adekvátneho technologického systému v spojení s kompetenciami managementu strategicky riadiť riziká.

Konkurencieschopnosť podniku v súdobých dynamicky sa vyvíjajúcich podmienkach si vyžaduje okrem snahy o znižovanie nákladov za súčasného zvyšovania produktivity a kvality odvedenej práce aj lojalitu zamestnancov a potrebné znalosti pre konkurenčné spravodajstvo (priemyselná špionáž) zároveň. Z posledných prieskumov totiž vyplýva, že väčšina strát je spôsobená úmyselne či neúmyselne práve vlastnými pracovníkmi. Podľa prípadových štúdii veľkých bezpečnostných firiem sa riešenie ponúka v školení so zameraním na sociálne inžinierstvo. Vzdelávanie zamestnancov v tejto oblasti pomohlo nie jednej firme minimalizovať riziká spojené so stratou dobrého mena spoločnosti a zvýšiť úspory nákladov spôsobených nedôslednými chybami organizácie práce.

Prieskum ukázal, že tretina tuzemských firiem nemá zavedenú bezpečnostnú politiku alebo aspoň plán na riešenie krízových situácií. Stredoeurópsky región zatiaľ nemá natoľko vybudovanú infraštruktúru IT, akú majú západné krajiny. Pojmy CISO, konkurenčné spravodajstvo alebo sociálne inžinierstvo ešte len dostanú priestor k plnému využitiu v našich podmienkach. Takisto ponuka technologických riešení je vo fáze testovania (napr. nedostatky biometriky) a na náš trh len pozvoľne prenikajú softwarové zabezpečovacie systémy. Firmy, ktoré sa teraz chopia skrytého potenciálu IT bezpečnosti a zavedú efektívnu politiku ako prvé, sa v budúcnu dočkajú zvýšenia svojej tržnej hodnoty.

ZOZNAM POUŽITEJ A DOPORUČENEJ LITERATÚRY

[1] BRABEC, F., a kol. *Bezpečnost pro firmu, úřad, občana*. 1. vyd. Praha: Public History, 2001. 400 s. ISBN 80-86445-04-06.

[2] BOHM-KLEIN, K. *Competitive Intelligence*. Bratislava: Univerzita Komenského. Filozofická fakulta. Katedra knižnej a informačnej vedy, 2004. 44 s. Vedúci diplomovej práce Soňa Makulová.

[3] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. 1. vyd. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

[4] JAŠEK, R. *Ochrana znalostí a dat v podnikových informačních systémech*. 1. vyd. Zlín: Univerzita Tomáše Bati, 2002. 115 s. ISBN 80-7318-095-2.

[5] MITNICK, K., SIMMON, W. *Umění klamu*. 1. vyd. Gliwice: Helion, 2003. 348 s. ISBN 83-7361-21-06.

[6] McCLURE, S., SCAMBRAY, J. *Hacking bez tajemství*. 1. vyd. Praha: Computer Press, 2003. 462 s. ISBN 80-7226-781-7.

[7] NOVOTNÝ, O., POUR, J., SLÁNSKÝ, D. *Business intelligence: jak využít bohatství ve vašich datech*. 1. vyd. Praha: Grada, 2005. 254 s. ISBN 80-247-1094-3.

[8] PŘYBIL, J., KODL, J. *Ochrana dat v informatice*. 1. vyd. Praha: ČVÚT, 1996. 299 s. ISBN 80-01-01664-1.

[9] COMPUTERWORLD: *týdeník pro IT profesionály*. Praha: IDG Czech, 1990- . Vychází týdně. ISSN 1210-9924.

[10] BUSINESS WORLD: *IT strategie pro manažery*. Praha: IDG Czech, 1998- . Vychází měsíčně. ISSN 1213-1709.

[11] IT SYSTEMS: *S přehledem ve světe podnikové informatiky*. Brno: CCB, 2000- . Vychází měsíčně. ISSN 1212-456X.

[12] PC WORLD SECURITY: *magazín o bezpečnosti v kybernetickém světe*. Praha: 2005 - . Vychází čtvrtletně. ISSN 1214-794X.

[13] VIJAYAN, J. Zaměřte se na vnitřního nepřítele. COMPUTERWORLD: *týdeník pro IT profesionály*, 2005, roč. 16, č 37, s. 25-27. ISSN 1210-9924.

[14] *Wikipedia, the free encyclopedia* [online]. 28.11.2005 [cit. 2005-11-29]. <http://en.wikipedia.org/wiki/Main_Page>.

[15] Česká komora detektívnych služeb. *Co je konkurenční zpravodajství* [online]. c2004 [cit. 2005-11-29]. <http://www.ckds.cz/cinnost/zpravodajstvi.html>.

[16] HÁK, I. *Moderní počitačové viry (třetí vydání)* [online]. 23.11.2005 [cit. 2005-11-29]. <http://www.viry.cz/ kniha/kniha.pdf>.

[17] GRANGER, S. *Social Engineering Fundamentals, Part I: Hacker Tactics* [online]. 18.12.2001 [cit. 2006-03-22]. <http://www.securityfocus.com/infocus/1527.html>

[18] GRANGER, S. *Social Engineering Fundamentals, Part II: Combat Strategies* [online]. 19.01.2002 [cit. 2006-03-28]. <http://www.securityfocus.com/infocus/1533>.

[19] RUSCH, J. *The "Social Engineering" of Internet Fraud* [online]. c1999 [cit. 2005-11-29]. <http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm>.

[20] *TopTenReviews* [online]. c2003 [cit. 2006-05-04]. <http://www.toptenreviews.com>.

[21] ESET: *Vírusový radar on-line* [online]. c2004 [cit. 2006-05-11]. <www.virusradar.com>.

[22] *Anti-Phising Working Group* [online]. c2005 [cit. 2006-05-11]. <www.antisphising.org>.

[23] BITTO, O. *Lámání hesel v praxi* [online]. 12.07.2005 [cit. 2006-03-08]. <http://www.lupa.cz/clanek.php3?show=4235>.

[24] MARKETiN: *Etický kódex pre konkurenčné spravodajstvo*. [online]. c2006 [cit. 2006-03-08]. <http://www.marketin.sk/?go=Etickykodex>.

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

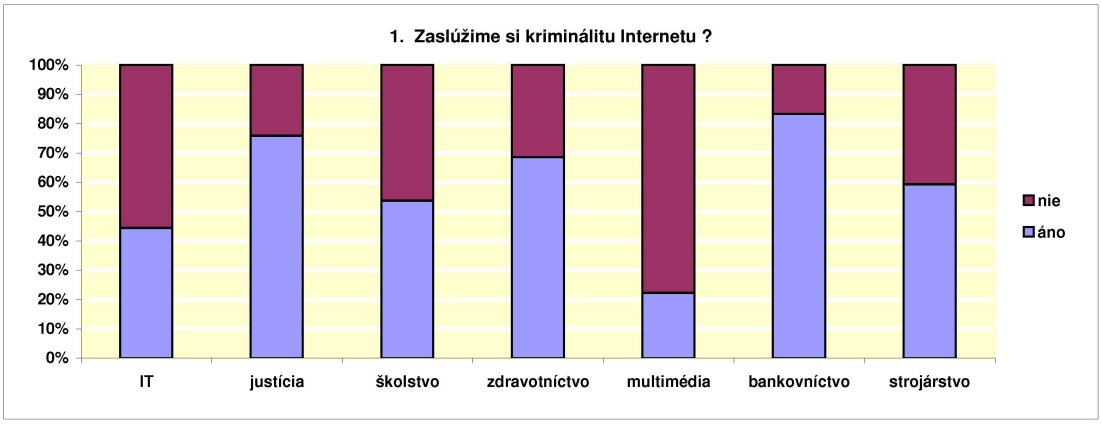
IT	Information Technology	*Informačné technológie*
IS	Information System	*Informačný systém*
SI	Social Engineering	*Sociálne inžinierstvo*
ID	Identification Number	*Identifikačné číslo*
CI	Competitive Inteligence	*Konkurenčné spravodajstvo*
FAR	False Acceptance Rate	*Miera chybných prijatí*
FRR	False Rejection Rate	*Miera chybných odmietnutí*
FTE	Failure to Enroll	*Neschopnosť zapojenia*
FTV	Failure to Verify	*Neschopnosť verifikácie*
ISP	Internet Service Provider	*Poskytovateľ internetu*
DNS	Domain Name System	
IDEA	International Data Encryption System	
VPN	Virtual Private Network	*Virtuálna súkromná sieť*
RSA	Rivest, Shamir, Adelmann	*Asymetrická šifrovacia metóda*
(D)DoS	(Distibuted) Denial of Service	*Odopretie prístupu*
CEO	Chief Executive Officer	*Generálny riaditeľ*
CISO	Chief Information Security Officer	*Riaditeľ úseku IT bezpečnosti*
CIO	Chief Information Officer	*Riaditeľ informatiky*
HRO	Human Resources Officer	*Riaditeľ personálneho úseku*
ICANN	International Corporation for Assigned Name and Numbers	
WSIS	World Summit on the Information Society	*Pobočka OSN pre IS*
IETF	Internet Engineering Task Force	
W3C	World Wide Web Consortium	
NSSC	National Strategy to Secure Cyberspace	

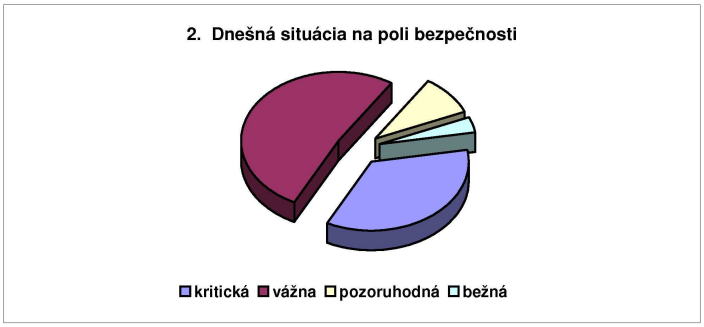
ZOZNAM OBRÁZKOV

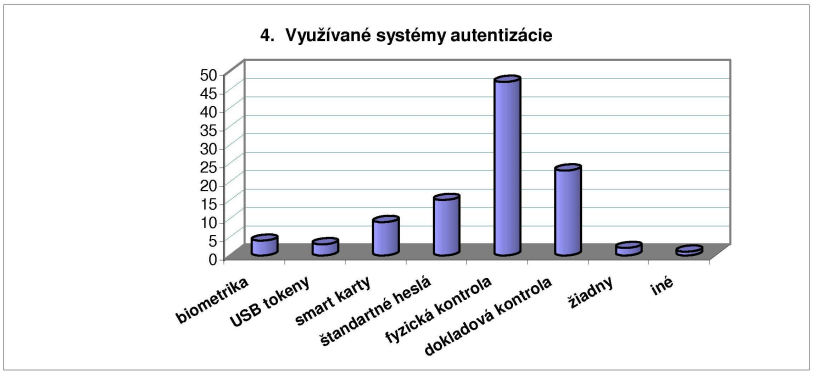
ZOZNAM TABULIEK

PRÍLOHY

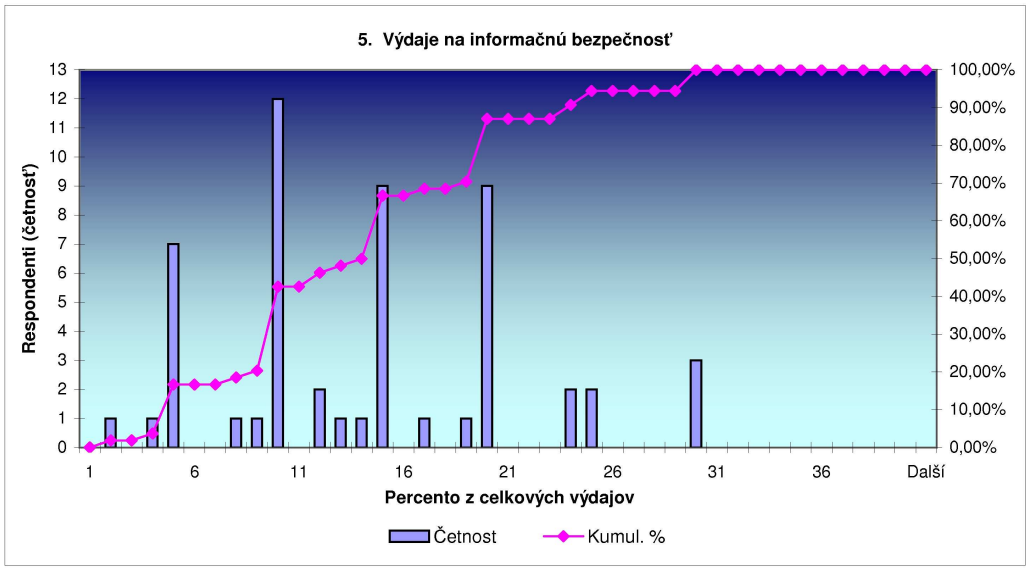
PRÍLOHA P 1: VYHODNOTENIE OTÁZOK 1 AŽ 4



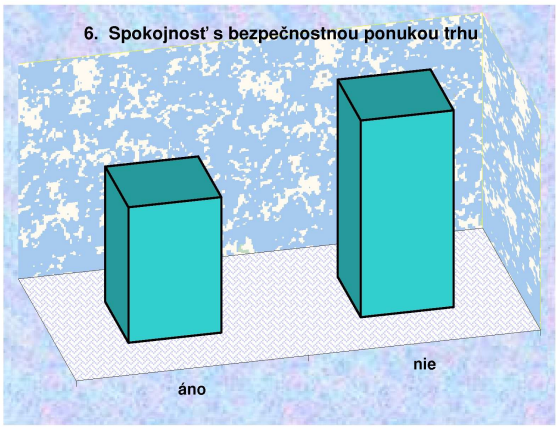


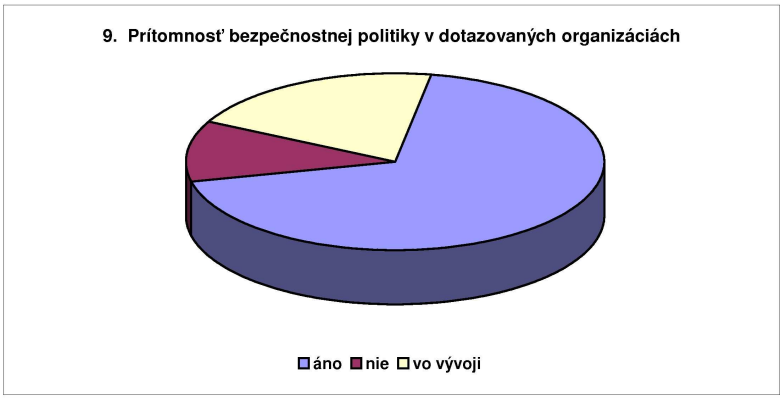


PRÍLOHA P 2: VYHODNOTENIE OTÁZOK 5, 6 A 9



Výdaje na informačnú bezpečnosť (%)	
Stř. hodnota	14,22222222
Chyba stř. hodnoty	0,961766176
Medián	14,5
Modus	10
Směr. odchylka	7,067509146
Rozptyl výběru	49,94968553
Špičatost	-0,367807982
Šikmost	0,462478658
Rozdíl max-min	28
Minimum	2
Maximum	30
Součet	768
Počet	54
Největší (1)	30
Nejmenší (1)	2





PRÍLOHA P 3: KORELAČNÁ ANALÝZA PRIESKUMU

Poradové č.	Otázka č.	Kritérium	Označenie
1.	1.	zodpovednosť	1ZI
2.	2.	situácia	2SI
3.	4.	biometrika	4BI
4.		USB tokeny	4UT
5.		smart karty	4SK
6.		štandardné heslá	4SH
7.		fyzická kontrola	4FK
8.		dokladová kontrola	4DK
9.		žiadny	4ZY
10.		iný	4IN
11.	5.	% výdajov	5PV
12.	6.	spokojnosť	6SP
13.	7.	open-source	7OS
14.	9.	politika	9PO

Software použitý k tvorbe korelačnej analýzy	MS Office Excel 2003 SP2 czech
	PDFCreator 0.8.1 RC10
	Picasa 2.2.0
Využité funkcie v programe MS Office Excel	Analýza dát - Popisná statistika
	Analýza dát - Histogram
	Analýza dát - Korelace
	MAX, MIN, KDYŽ, COUNTIF

	1ZI	2SI	4BI	4UT	4SK	4SH	4FK	4DK	4ZY	4IN	5PV	6SP	7OS	9PO	
1ZI															**1ZI**
2SI	0,19486														**2SI**
4BI	0,04881	0,23539													**4BI**
4UT	0,10810	0,01068	-0,18779												**4UT**
4SK	-0,01030	-0,05710	0,10994	-0,14384											**4SK**
4SH	-0,00820	-0,26364	0,07111	0,04581	-0,02654										**4SH**
4FK	0,10573	0,03665	0,04851	0,01231	-0,10392	-0,14113									**4FK**
4DK	0,20318	0,00136	-0,00263	-0,10677	0,14017	-0,01775	0,06427								**4DK**
4ZY	-0,11278	0,17200	-0,09409	-0,24948	-0,18257	-0,36338	-0,41016	-0,30972							**4ZY**
4IN	-0,08409	-0,02050	-0,16035	0,04734	-0,20344	0,03096	-0,21014	-0,29622	-0,21303						**4IN**
5PV	-0,13541	-0,09194	0,43625	-0,00471	-0,01639	0,33435	0,05448	0,15546	-0,29736	0,09176					**5PV**
6SP	0,07514	-0,10334	0,00401	0,15677	0,10704	0,03874	-0,14634	-0,05208	0,05330	0,12228	-0,02213				**6SP**
7OS	-0,20795	-0,06293	-0,00797	-0,23415	0,06680	-0,02239	0,08189	0,25319	-0,10592	0,01262	0,18303	-0,13036			**7OS**
9PO	0,18547	0,15170	0,18880	0,11807	-0,19873	0,08942	0,15132	0,03509	-0,04732	-0,02482	0,16781	0,33800	0,20187		**9PO**
1ZI		0,19486	0,04881	0,10810	-0,01030	-0,00820	0,10573	0,20318	-0,11278	-0,08409	-0,13541	0,07514	-0,20795	0,18547	**1ZI**
2SI			0,23539	0,01068	-0,05710	-0,26364	0,03665	0,00136	0,17200	-0,02050	-0,09194	-0,10334	-0,06293	0,15170	**2SI**
4BI				-0,18779	0,10994	0,07111	0,04851	-0,00263	-0,09409	-0,16035	0,43625	0,00401	-0,00797	0,18880	**4BI**
4UT					-0,14384	0,04581	0,01231	-0,10677	-0,24948	0,04734	-0,00471	0,15677	-0,23415	0,11807	**4UT**
4SK						-0,02654	-0,10392	0,14017	-0,18257	-0,20344	-0,01639	0,10704	0,06680	-0,19873	**4SK**
4SH							-0,14113	-0,01775	-0,36338	0,03096	0,33435	0,03874	-0,02239	0,08942	**4SH**
4FK								0,06427	-0,41016	-0,21014	0,05448	-0,14634	0,08189	0,15132	**4FK**
4DK									-0,30972	-0,29622	0,15546	-0,05208	0,25319	0,03509	**4DK**
4ZY										-0,21303	-0,29736	0,05330	-0,10592	-0,04732	**4ZY**
4IN											0,09176	0,12228	0,01262	-0,02482	**4IN**
5PV												-0,02213	0,18303	0,16781	**5PV**
6SP													-0,13036	0,33800	**6SP**
7OS														0,20187	**7OS**
9PO															**9PO**

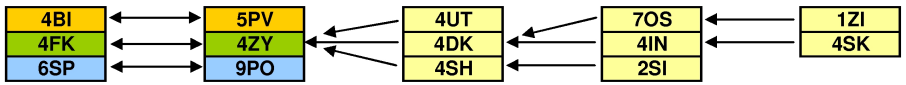
korelačné koeficienty :

MIN	-0,20795	-0,26364	-0,18779	-0,24948	-0,20344	-0,36338	-0,41016	-0,30972	-0,41016	-0,29622	-0,29736	-0,14634	-0,23415	-0,19873
MAX	0,20318	0,23539	0,43625	0,15677	0,14017	0,33435	0,15132	0,25319	0,17200	0,12228	0,43625	0,33800	0,25319	0,33800
výber	-20,79%	-26,36%	43,62%	-24,95%	-20,34%	-36,34%	-41,02%	-30,97%	-41,02%	-29,62%	43,62%	33,80%	25,32%	33,80%

najsilnejšie väzby :

stĺpce	1ZI	2SI	4BI	4UT	4SK	4SH	4FK	4DK	4ZY	4IN	5PV	6SP	7OS	9PO
	7OS	4SH	5PV	4ZY	4IN	4ZY	4ZY	4ZY	4FK	4DK	4BI	9PO	4DK	6SP

dendogramy :



PRÍLOHA P 4: PÔVODNÝ NÁVRH DOTAZNÍKU

D o t a z n í k

Vážená pani, vážený pane,

následující dotazník je zcela anonymní a slouží pro účely orientační analýzy ochrany firemních dat v českých podnicích. Výstup bude podkladem pro rozhodování o efektivní volbě bezpečnostního systému. Děkujeme Vám za předání Vašich zkušeností a přejeme hodně úspěchů.

---

hlavni předmět činnosti Vaši organizace :

přibližný počet zaměstnanců :

---

1. Souhlasíte s tvrzením, že „internet je takový, jaký si zasloužíme" (odrazem civilizace) ?

□ ano □ ne

2. Jak vnímáte dnešní situaci na poli informační bezpečnosti ?

□ kritickou □ vážnou □ pozoruhodnou □ běžnou

3. Můžete nám prosím sdělit, které útoky považujete v současnosti za větší (častější) hrozbu pro organizace ?

□ rozhodne externí □ spíše externí □ spíše interní □ rozhodne interní

4. Které z následujících systémů autentizace zaměstnanců je využíván Vaší organizací ?

□ biometrika □ USB tokeny □ smart karty □ standardní hesla

□ fyzická kontrola □ dokladová kontrola □ jiné (prosím uveďte) .....

5. Dovede-li by jste odhadnout, kolik procent výdajů vynakládá Vaše společnost na bezpečnost, ochranu dat ?

□ 0 až 10 % □ 11 až 20 % □ 21 až 40 % □ 41 a víc %

6. Jste spokojen s nabídkou bezpečnostních odborníků, řešení či produktů pro Vaši firmu na tuzemském trhu ?

□ ano □ ne proč jste toho názoru? .....

7. Myslíte si, že komerční software je bezpečnější než open-source software ?

□ určíte ano □ ano □ ne □ určíte ne

8. Prosím vyberte z následující nabídky produkty, které se intenzívně využívají při činnosti ve Vaši firmě

□ Mozilla □ Opera □ PGP apod. □ Anti-spyware □ Anti-phising □ DeviceLock apod.

□ NOD32 □ Symantec □ Sygate □ McAfee □ Panda SW □ ZoneAlarm

□ Outpost □ Keiro □ AVG □ Avast □ F-Secure □ Kaspersky

9. Má Vaše firma vypracovanou bezpečnostní politiku a plán pro řešení krizových situací Vašeho IS ?

□ ano □ zatím ne, ale pracuje se na tom □ ne

Na tomto místě by jsme Vám ještě jednou rádi poděkovali. Pokud by jste měli zájem o výsledky tohoto dotazníku anebo spolupráci v oblasti implementací bezpečnostních systémů, prosím uveďte nám své kontaktní údaje na zadní stranu dotazníku. Dotazník můžete předat na místě Vaši registrace.

PRÍLOHA P 5: POUŽITÝ DOTAZNÍK PRI VÝSKUME

D o t a z n í k

Vážená paní, vážený pane,

prosím věnujte pár minut vyplnění následujícího anonymního dotazníku. Vyplněný dotazník odevzdejte u prezentace. Děkujeme Vám

---

oblast činnosti Vaši organizace :

přibližný počet zaměstnanců :

---

1. Souhlasíte s tvrzením, že „internet je takový, jaký si zasloužíme" (je odrazem civilizace) ?

□ ano □ ne

2. Jak vnímáte dnešní situaci na poli informační bezpečnosti ?

□ kritickou □ vážnou □ pozoruhodnou □ běžnou

3. Můžete nám prosím sdělit, které druhy útoků považujete v současnosti za větší hrozbu?

□ rozhodně externí □ spíše externí □ spíše interní □ rozhodně interní

□ nedokážu určit

4. Který z následujících systémů autentizace zaměstnanců je využíván Vaší organizací ?

□ biometrika □ USB tokeny □ smart karty □ standardní hesla

□ fyzická kontrola □ dokladová kontrola □ žádný systém nemáme

□ jiné (prosím uveďte) .....

5. Dovedete odhadnout jak velké procento výdajů vynakládá Vaše společnost na informační bezpečnost?

cca ..... %

6. Jste spokojen s nabídkou bezpečnostních odborníků, řešení či produktů pro Vaši firmu na tuzemském trhu ?

□ ano □ ne

proč jste toho názoru? .....

7. Myslíte si, že komerční software je bezpečnější než open-source software ?

□ určitě ano □ ano □ ne □ určitě ne

□ nevím

8. Prosím vyberte z následující nabídky produkty, které se intenzívně využívají při činnosti ve Vaši firmě

□ Mozilla □ Opera □ PGP apod. □ Anti-spyware □ Anti-phising □ DeviceLock apod.

□ NOD32 □ Symantec □ Sygate □ McAfee □ Panda SW □ ZoneAlarm

□ Outpost □ Keiro □ AVG □ Avast □ F-Secure □ Kaspersky

9. Má Vaše firma vypracovanou bezpečnostní politiku nebo alespoň plán pro řešení krizových situací Vašeho IS ?

□ ano □ zatím ne, ale pracuje se na tom □ ne