BEZPEČNOSŤ A OCHRANA INFORMÁCIÍ V PROSTREDÍ ŠIS

pplk. Ing. Miloš ŠMIRJAK, CSc.
VTÚ Liptovský Mikuláš

"Dajte mi desať starostlivo vybraných hakerov a za 90 dní zrazíme túto krajinu na kolená. Chaos, ktorý možno vyvolať, bude enormný."

Jim Settle, konzultant v obore bezpečnosti a bývalý riaditeľ brigády boja proti kriminalite na poli informatiky v FBI.

Úvod

Zaostávanie, ako jedno z nemilých dedičstiev nedávnej minulosti, sa snáď najvýraznejšie prejavilo v oblasti informačných technológií a čo sa následne negatívne premieta aj do ďalších oblastí. V rámci znižovania tohoto zaostávania možno v súčasnej dobe sledovať doslova masové nasadzovanie výpočtovej techniky vo všetkých oblastiach aj v rámci štátnej správy SR. Súčasne je vidieť aj výrazný rozvoj počítačových sietí a informačných systémov.

Tento rozvoj však so sebou neprináša len pozitívne javy. Zásadne nový druh spracovávania, prenosu a uchovávania dát spôsobil nebezpečné zaostávanie bezpečnostno-informačného povedomia mnohých užívateľov, ktorí stále nie sú schopní zodpovedne posúdiť nebezpečenstvá a úskalia počítačového spracovávania informácií. Z praxe vyplýva, že podceňovanie až bagatelizovanie možných problémov a dôsledkov je dosť rozšírené a užívatelia ani nie sú si vedomí svojho nesprávneho myslenia a konania.

Existuje totiž veľa spôsobov ohrozenia systému, ktorými môže útočník získať prístup k jeho výpočtovej kapacite a dostať sa k najcennejšiemu aktívu systému – k informáciám. Vo svojej najnevinnejšej forme sa také narušenie prejaví neustálym obťažovaním legálnych užívateľov nezmyselnými správami či krátkodobým znížením výkonu. V horšom prípade bude systém nakazený rôznymi vírusmi a škriatkami. V najvážnejších prípadoch však môže byť kompromitovaná, či dokonca ohrozená bezpečnosť a suverenita štátu.

Toto dokazujú aj údaje organizácie CERT (Computer Emergency Response Team), ktoré sú skutočne alarmujúce. Počet prienikov do najrôznejších informačných systémov rastie, ale čo je možno ešte horšie, iba veľmi malá časť z tohoto počtu je hlásená. Dôvod je veľmi jednoduchý - u komerčných subjektov by prípadné správy o narušení počítačovej siete mohli viesť k odvráteniu zákazníkov. V prípade štátnych úradov a organizácií by mohol taký prípad niekoho stáť teplé miestečko, alebo sa úrady obávajú negatívnej odozvy verejnosti. V podstate sa teda na povrch dostane len zlomok údajov o narušiteľoch. Aj to väčšinou len v takých prípadoch, že sa hakera podarí chytiť (a to býva skutočne veľmi zrieka), alebo ak informácie zverejní niekto iný a nie je možné tomu zabrániť (napr. novinári).

1. Dôvody riešenia ochrany informácií a bezpečnosti IS

Jedným z faktorov, ktoré si treba uvedomiť je to, že všeobecne je vždy potrebné vyvinúť menšie úsilie a prostriedky na zneužitie či zničenie vecí, než na ich budovanie a ochranu. V oblasti informačných technológií to znamená okrem iného, že na jednej strane vyspelé štáty venujú veľkú pozornosť a obrovské prostriedky na rozvoj a využívanie informačných technológií (hlavne na dosiahnutie vyššej konkurencieschopnosti a bezpečnosti krajiny). Na druhej strane menej vyspelým krajinám často môže postačovať podstatne menej prostriedkov na zneužitie, či dokonca zničenie týchto informačných a komunikačných systémov, ktoré by vo svojich dôsledkoch mohlo dokonca viesť k ekonomickému či bezpečnostnému kolapsu krajín od takýchto technológií životne závislých.

Diaľková komunikácia (predovšetkým v prípade pripojenia k najznámejšej počítačovej sieti **Internet**) prináša veľké nebezpečie predovšetkým zo strany prienikárov (tzv. hakerov), ktorí si robia z prieniku do najrôznejších súkromných sietí doslova súťaž. V prípade štátnych sietí a systémov je ich motivácia ešte väčšia. Okrem toho je v prípade uvedených systémov a sietí nevyhnutné počítať aj s aktivitami moderne vybavených a primerane motivovaných špionážnych služieb cudzích štátov.

Tento fakt potvrdzuje aj Krajský úrad pre ochranu konštitúcie Baden-Württemberg, keď vo svojej štúdii dokazuje, že špionážne aktivity tajných služieb nepolavili a znamenajú vážne narastajúci problém. Obzvlášť priemyselná špionáž sa z aspektu čoraz tvrdšieho medzinárodného súťaženia stáva ďalším najnovším cieľom cudzích výzvedných záujmov.

Sherry Roggermanová, koordinátorka u predajcu hardveru v americkom meste Phoenix, zhrozene prehlásila po zapojení ochranného systému: "Je to hrozné. Ťažko si možno predstaviť, že niekto trávi celý čas tým, že sa snaží dostať do vášho systému".

Podľa plukovníka Johna J. Sheldona z organizácie CISS (Center for Information Systems Security) z Pentagonu sa pri používaní siete Internet pokúša CISS dostať do sietí Ministerstva obrany USA. Podľa vyjadrenia zástupcov organizácie CISS sa môžu hakeri dokonca až v deväťdesiatpäť percentách do týchto sietí neoprávnene dostať. Prijde sa pritom len na päť z týchto útokov a odhalených je z toho len päť ďalších percent.

Túto skutočnosť podporuje aj vyjadrenie Josepha Markowitza, riaditeľa kancelárie Community Open Source Program Office, ktorá vznikla pri CIA. Podľa tohoto vyjadrenia sa na Internet pripojila CIA a päť ďalších výzvedných služieb, aby tu zbierali "neklasifikované" a "verejne prístupné" informácie. Spravodajské údaje budú využívať aj sesterské agentúry typu NSA (National Security Agency) a DIA (Defence Intelligence Agency).

Pritom sa tieto špionážne agentúry sami okamžite vzačali zaujímať o hrozby pôsobiace z Internetu, predovšetkým od hakerov. Markowitz povedal, že prebieha inštalácia bezpečnostného systému, čo je prístupový server, ktorý chráni internú (vlastnú) sieť proti akýmkoľvek rušivým snahám zvonku. Špeciálne hardverové zariadenie, ktorého schéma nebola zverejnená, okrem toho umožní, aby analytici prenášali súbory z Internetu na svoje vysoko tajné pracovné stanice bez toho, aby bolo možné vykonať prenos opačným smerom.

Podľa vyjadrenia Barbary Fraserovej, manažérky vývoja v CERT, sa správcovia sietí stále viac obávajú vývojových prostriedkov počítačového podsvetia, ktoré testujú a využívajú známe slabé miesta v zabezpečovacích systémoch. "Nevítaní hostia už nemusia byť veľkými odborníkmi, aby prekonali slabé miesta," varuje B.Fraserová. "Oni proste môžu vypustiť niektorý z takýchto programov na váš systém alebo sieť a už sú vo vnútri".

Vo svete je známych nepreberné množstvo prípadov prienikov, dokonca aj do chránených štátnych systémov. Obeťami sa stali tak orgány NATO, ministerstvá obrany, veliteľstvá všetkých druhov vojsk (pozemných, vzdušných aj námorných), tajné služby rôzneho druhu v rôznych štátov, ako aj vlády mnohých štátov alebo kancelárie prezidentov. Podrobnejšie sú najznámejšie prieniky takéhoto druhu popísané a rozobraté v materiále [4].

Pre ďalšie odstrašujúce prípady netreba chodiť ani tak ďaleko a stačí si pripomenúť len dva pomerne nedávne prípady, ktoré sa stali aj u našich najbližších susedov - v Česku a Maďarsku.

Najskôr si pracovník jednej českej tajnej služby "zabudol" v reštaurácii na stoličke notebook, ktorý obsahoval utajované informácie. Po návrate ho tam už samozrejme nenašiel. **Na ochranu prístupu k informáciám v notebooku nebol použitý žiaden bezpečnostný prostriedok a aj samotné informácie boli v otvorenom tvare a neboli chránené šifrovaním.** Odcudzenými informáciami bol práve naplnený novo zavádzaný informačný systém danej služby. Oficiálne miesta sa neskôr snažili zľahčovať dopad tohoto činu tvrdením, že išlo len o cvičné dáta. To je ale dosť nepravdepodobné vzhľadom k spôsobenému rozruchu a nasledujúcemu tvrdému spôsobu prešetrovania. Navyše spomínaný pracovník už v postihnutej službe nepracuje!

Druhý prípad sa odohral v Maďarskej republike. Predsedovi branno-bezpečnostného výboru maďarského parlamentu počas jeho dovolenky pri Balatone neznámi zlodeji vykradli byt a odniesli si z neho aj jeho počítač aj so služobnými dátami týkajúcimi sa rokovaní branno-bezpečnostného výboru. Na ochranu prístupu k informáciám v tomto počítači rovnako nebol použitý žiaden bezpečnostný prostriedok a aj samotné informácie boli tiež v otvorenom tvare a neboli chránené šifrovaním. **V tomto prípade postihnutý otvorene priznal, že zverejnenie týchto dát môže mať vplyv na bezpečnostnú situáciu štátu a mohlo by ohroziť aj obranyschopnosť Maďarska!** Otvorená ale ostáva otázka, či spomínaný počítač bol len obyčajnou súčasťou všetkých ostatných odcudzených vecí alebo odcudzenie ostatných vecí malo zakryť hlavný zámer vlúpania - odcudzenie tohoto počítača aj s dátami v ňom obsiahnutými.

2. Bezpečnostný projekt informačného systému

Ak majú byť informácie chránené zodpovedajúcim spôsobom, treba **riešiť zaistenie ich ochrany a bezpečnosti v rámci celého informačného systému komplexne a veľmi dôsledne.** Ak sa opomenie čo i len jeden článok pri spracovaní informácií, môže to zapríčiniť neúčinnosť celého systému ochrany a spôsobiť zbytočnosť už realizovaných opatrení.

Spôsob využitia špeciálnych bezpečnostných prostriedkov v kombinácii s príslušnými organizačnými opatreniami je potrebné zvážiť vždy v závislosti od konkrétneho spôsobu realizácie, požiadaviek a účelu informačného systému. Pre tieto účely sa spracováva tzv. **bezpečnostný projekt,** ktorý na základe analýzy rizík

hodnoteného systému rieši optimálny spôsob zabezpečenia ochrany s ohľadom tak na každý jednotlivý prvok systému, ako aj na systém ako celok. Bezpečnostný projekt zohľadňuje špecifické vlastnosti, poslanie a druh chráneného informačného systému. Bezpečnostný projekt sa spracováva v etape konečného projektu systému. Z dôvodu špecifického charakteru riešenej problematiky a nevyhnutnej ochrany informácií o danom informačnom systéme je bezpečnostný projekt:

- posudzovaný iným, presne vymedzeným okruhom odborníkov v oblasti bezpečnosti informačných systémov,
- vydávaný ako samostatný materiál.

Ak systém predložený na posúdenie nespĺňa všetky kritériá z hľadiska charakteru spracovávaných informácií a jeho použitia a určenia, je potrebné v rámci bezpečnostného projektu navrhnúť dodatočné bezpečnostné opatrenia a ďalej postupovať nasledovne:

- ak bol na posúdenie predložený hotový vytvorený systém, následne je potrebné preveriť realizáciu navrhnutých opatrení,
- ak bol na posúdenie predložený projekt budovaného systému, je potrebné preveriť zapracovanie navrhnutých opatrení do systémového projektu.

Ako optimálne riešenie vychádza posudzovanie systému už v etape zámyslu jeho riešenia a príslušné bezpečnostné opatrenie zaintegrovať do systému už od samotného začiatku jeho budovania, tzn. systém budovať už s ohľadom na potrebné bezpečnostné prvky. Daný systém je potom kompaktnejší a odolnejší voči prejaveniu sa možných hrozieb (prostredníctvom existujúcich bezpečnostných slabín) a aj celkové náklady na riešenie takéhoto systému sú nižšie. Tomu zodpovedajú aj získané doterajšie skúsenosti v tejto oblasti dosiahnuté v ostatných krajinách s rozvinutými informačnými technológiami.

Spracovanie bezpečnostného projektu je potrebné zveriť špecializovanému pracovisku (organizácii), ktoré môže poskytnúť plné záruky za navrhnuté riešenie a realizované bezpečnostné mechanizmy.

3. Analýza rizík

Počítačová bezpečnosť je relatívna. Ak niekto uvažuje o vytvorení, nákupe alebo použití bezpečnostného produktu, musí porovnávať cenu tohoto produktu a riziko zaobídenia sa bez neho. Niektoré organizácie tento proces formalizujú a nazývajú ho alebo

analýza rizík. **Analýza rizík musí byť vykonaná ako jedna z prvých činností pri tvorbe budovaného IS.** Ide o proces, v rámci ktorého sa zisťujú hrozby, ktoré ohrozujú chránené aktíva systému. Pre každú hrozbu je zistená pravdepodobnosť ohrozenia aktív touto hrozbou. Proces analýzy rizík zahrňuje identifikáciu a hodnotenie úrovne rizík na základe matematických metód. Tieto metódy umožňujú vypočítať (stanoviť) úroveň rizík na základe ocenenia aktív, z ktorých sa hodnotený systém skladá, zhodnotenie úrovne hrozieb a charakteru slabín, prostredníctvom ktorých sa môžu hrozby prejaviť.

Hlavným cieľom analýzy rizík je pomôcť vybrať z hľadiska ceny efektívne bezpečnostné opatrenia, ktoré budú existujúce riziká buď úplne eliminovať alebo redukovať na prijateľnú úroveň. Analýza rizík tak vytvára obraz toho, ako dôležitý je systém pre užívateľa a ako ho je ochotný zabezpečiť - z hľadiska zariadení, ľudí a rozpočtu. Štandardná analýza rizík zahrňuje pohľad na hmotné hodnoty - napríklad budovy, počítače, ďalšie zariadenia a určenie, ako ich najlepšie chrániť. Vzhľadom k tomu, že najcennejšie aktíva organizácie bývajú informácie, je potrebné sa starostlivo zamerať na najlepšiu ochranu práve informácií.

Analýza rizík sa zameriava na *dáta vo všetkých komponentoch, programy, technické prostriedky (fyzické aktíva), prevádzkovo-fyzikálne aktíva, prevádzkovo-organizačné aktíva.* Posledné dve riziká môžu byť veľmi ťažko definovateľné a kvantifikovateľné (napr. živelné udalosti) a obsahujú aj ľudský faktor (vnútorná hrozba zo strany obsluhy). Odborné spracovanie analýzy rizík môže výrazne napomôcť pri stanovení primeranej úrovne zabezpečenia systému. Platí totiž, že bezpečnostné zariadenie, ktoré je drahšie než hodnota informácií, ktoré má chrániť, nie je efektívne z hľadiska hodnoty. Absolútnu bezpečnosť možno dosiahnuť len za cenu neobmedzených nákladov.

V priebehu analýzy rizík sa realizujú postupnosti činností, ktoré sú vykonávané so systémovými špecifikáciami a požiadavkami:

a) *analýza problému* - zaoberá sa prostredím a požiadavkami na systém,
b) *identifikácia* - zaoberá sa aktívami, hrozbami a obmedzeniami týkajúcimi sa systému,
c) *ohodnotenie možných riešení* - z hľadiska vhodnosti, ceny a príjemnosti protiopatrení,
d) *integrácia rozhodnutí* - zaoberá sa jednotlivými variantmi a vypracovaním správy.

Na analýzu rizík nadväzuje **riadenie rizík**, ktoré zahrňuje identifikáciu, výber a aplikáciu protiopatrení, ktoré sú adekvátne vypočítaným rizikám a umožňujú redukovať riziká na akceptovateľnú úroveň. Riadenie rizík je činnosť (proces), ktorý hrá

principiálnu úlohu počínajúc od štádia návrhu systému až po štádium jeho prevádzky a má za cieľ znižovať úroveň rizík v každej fáze životného cyklu systému.

4. Otázky bezpečnosti štátneho informačného systému

Koncepcia štátneho informačného systému na roky 1997 - 1998 a bezpečnosť informácií ŠIS

V materiále „Koncepcia štátneho informačného systému na roky 1997 - 1998“ (ďalej len Koncepcia) je venovaná pomerne veľká pozornosť bezpečnosti a ochrane spracovávaných a uchovávaných údajov. Na viacerých miestach tohoto materiálu je zdôrazňovaná potreba zabezpečenia ŠIS a uvádzaný prístup a návrh spôsobu riešenia jeho ochrany.

V uvedenej Koncepcii sú stanovené jej základné ciele na roky 1997 - 1998. Medzi týmito cieľmi je na jednom z prvých miest uvedená potreba vytvorenia podmienok pre bezpečnosť a ochranu údajov ŠIS proti ich zneužitiu. Oprávnenosť tohoto cieľa dokazuje aj tá skutočnosť, že riešenie problémov bezpečnosti sa dotýka všetkých štyroch základných okruhov, na ktoré sa orientoval „Národný program informatizácie Slovenskej republiky“ z roku 1992.

Otázky úrovne bezpečnosti v sieťovom prostredí a prístupy k riešeniu

Z analýzy súčasného stavu rozvoja ŠIS vyplýva, že sa nerealizoval požadovaný prechod na architektúru typu „klient - server“ v unixovom prostredí. Táto skutočnosť má priamy dopad aj na bezpečnostnú stránku riešenia štátneho informačného systému. Žiaden z najpoužívanejších operačných systémov Windows totiž nemá pre sieťové prostredie certifikát ani na úrovni minimálnej bezpečnostnej triedy C1 (podľa amerických bezpečnostných kritérií TCSEC [Oranžová kniha]).

Nižšie ako trieda C1 je len trieda D bez využitia akýchkoľvek ochranných mechanizmov. Pritom pre ochranu dôverných informácií je potrebná bezpečnostná trieda aspoň na úrovni C2 podľa TCSEC. Pre ochranu nižších stupňov utajovaných informácií je potrebná bezpečnostná trieda aspoň na úrovni B1 podľa TCSEC. Takúto úroveň poskytujú napríklad operačné systémy Unix.

Uvedený problém je možné riešiť dvoma spôsobmi:

1. priame požitie operačného systému Unix s certifikátom na príslušnú triedu bezpečnosti,

2. použitie operačného systému Unix s certifikátom na triedu bezpečnosti nižšiu o jeden stupeň, než je požadovaná, so súčasným použitím bezpečnostnej nadstavby nad týmto operačným systémom (čo tiež zabezpečí primeranú úroveň ochrany).

Dôvody pre riešenie úloh ochrany informácií v štátnom informačnom systéme a realizácie bezpečnostného podsystému

Zložitosť riešenia ochrany v prostredí ŠIS a dôvody pre riešenie bezpečnosti vyplývajú z viacerých skutočností:

- **vývoj a realizácia rezortných IS boli - a v súčasnosti aj stále sú - úplne nekoordinované a štátne IS určené pre ŠIS sú tak vo väčšine prípadov vzájomne nekompatibilné**, čo spôsobuje neexistencia legislatívy a jednotných štandardov v štátnej správe,
- **v ŠIS budú spracovávané informácie rôzneho stupňa utajenia a rôzneho určenia** (chránené aj verejne prístupné informácie), pretože ŠIS bude slúžiť tak pre orgány a organizácie štátnej správy, ako aj pre širokú verejnosť (jednotlivcov, organizácie aj podnikateľské subjekty) a *do systému budú mať umožnený prístup aj užívatelia nepreverení z hľadiska citlivých informácií ŠIS*,

to značne zvyšuje riziko pokusov o odcudzenie, vymazanie alebo modifikáciu chránených údajov ŠIS bez potreby pokusov o korupciu zodpovedných pracovníkov:

- *utajovaných informácií* (chránených v zmysle zákona NR SR č.100/1996 Z.z. o ochrane štátneho tajomstva, služobného tajomstva a šifrovej ochrane informácií a o zmene a doplnení Trestného zákona v znení neskorších predpisov a vyhlášky MV SR č. 129/1997 Z.z., ktorou sa vykonáva zákon NR SR č.100/1996 Z.z.),
- *osobných údajov určených iba pre špecifické použitie* (chránených v zmysle zákona NR SR č.58/1998 Z.z. o ochrane osobných údajov v informačných systémoch) - napr. informácie o zdravotnom stave, finančnej situácii, majetkových pomeroch, politickej príslušnosti a pod. - z nedávnej minulosti je známych viacero neobjasnených prípadov zneužitia osobných údajov aj u nás,

- **do ŠIS budú integrované rezortné informačné systémy vybudované a ešte aj v súčasnosti budované nekoordinovane a autonómne dokonca aj v rámci jednotlivých rezortov**, čo spôsobuje neexistencia legislatívy a jednotných štandardov v rámci týchto rezortov,
- **podľa požiadaviek má ŠIS sprostredkovať pripojenie svojich užívateľov aj k sieti Internet**, čo je medzinárodná počítačová sieť, ktorá je známa mnohými pokusmi

i úspešnými prienikmi o útok na štátne aj firemné systémy zo strany hakerov a organizovaných služieb,

- **značne zvýšená pravdepodobnosť „neuvedomelých“ a nepoučených užívateľov**, ktorí budú mať nízke bezpečnostno-informačné povedomie, ktorí budú podceňovať potrebu bezpečnostných opatrení a ktorí budú mať snahu obchádzať už implementované opatrenia pri systéme s takým veľkým množstvom užívateľov, ako je štátny informačný systém,
- **vyššie možnosti prieniku do systému** - v prípade tak rozsiahleho systému akým je ŠIS a s takým veľkým počtom prístupových miest je veľkým problémom ustrážiť prístup k chráneným údajom a zabezpečiť požadovanú úroveň ochrany.

Možné spôsoby ohrozenia ŠIS

Informácie spracovávané, prenášané a uchovávané v ŠIS, ale aj prevádzka celého systému, môžu byť ohrozené viacerými spôsobmi:

- **odcudzenie a neoprávnený prístup k chráneným informáciám** - veľmi ťažko odhaliteľný spôsob útoku vedúci k možnosti nebezpečného zneužitia odcudzených chránených informácií na rôzne ciele,
- **nepovolená modifikácia chránených informácií** - veľmi nebezpečný spôsob útoku, ktorý môže spôsobiť len ťažko odhaliteľné podvody v rôznych oblastiach (ekonomickej, daňovej, trestno-právnej, životného prostredia, zdravotníctva a hygieny, vodohospodárskej a pod.)
- **zničenie chránených informácií** - tento druh útoku je síce možné odhaliť pomerne rýchlo, ale môže dôjsť k značným, veľmi ťažko a dlho obnoviteľným škodám, ba v niektorých prípadoch môže dôjsť až k nenapraviteľným škodám,
- **úmyselné zníženie priepustnosti siete, prípadne až úplné zahltenie celého ŠIS** - vysielaním falošných správ môže dôjsť k zníženiu funkčnosti komunikačného podsystému alebo aj k úplnému znefunkčneniu ŠIS.

V prípade úspešného uskutočnenia hore uvedených bezpečnostných útokov je za normálnych okolností ich odhalenie len veľmi problematické. Ak budú aplikované bezpečnostné opatrenia vo forme vedenia **auditného záznamu**, bude možné nielen odhaliť daný útok, ale aj zistiť spôsob jeho uskutočnenia a pôvodcu útoku. Do auditného záznamu sa zaznamenávajú informácie o vybratých citlivých operáciách - alebo aj všetkých aktivitách v chránenom systéme.

Otázky bezpečnosti modelu ŠIS

V rámci budovania ŠIS sa predpokladá realizácia modelu štátneho informačného systému, čo bude znamenať výraznú podporu koordinácie prác v štátnej správe a racionalizáciu väzieb informatických aktivít. Skúsenosti pracovníkov Vojenského technického ústavu Liptovský Mikuláš, ale aj informaticky vyspelých krajín dokazujú, že z kvalitatívneho, bezpečnostného i ekonomického hľadiska je potrebné riešiť bezpečnosť a ochranu systémov súčasne s budovaním vlastných chránených informačných systémov. *Preto je potrebné v rámci realizácie modelu navrhnúť a overiť funkčnosť aj systému bezpečnostných opatrení i celého bezpečnostného podsystému.*

Bezpečnostný projekt pilotného projektu

Najbližšou úlohou budovania komunikačnej infraštruktúry ŠIS je v rámci pilotného projektu vzájomné prepojenie krajských úradov, pripojenie krajských úradov k sieti GOVNET a vo vybranom kraji aj prepojenie okresných úradov. Potom rovnako ako pri realizácii projektu ŠIS, aj *v prípade pilotného projektu je potrebné pri jeho analýze a vypracovaní zohľadniť otázky a problémy súvisiace s ochranou informácií* v ŠIS. To znamená, že prílohou pilotného projektu bude aj spracovaný bezpečnostný projekt pilotného projektu a súčasne s realizáciou a overením činnosti pilotného projektu bude realizovaný a overený aj bezpečnostný podsystém pilotného projektu.

5. Návrhy riešenia problémov ochrany a bezpečnosti informácií v ŠIS

Návrh riešenia problémov bezpečnosti v oblasti legislatívy a metodického riadenia ŠIS

V oblasti legislatívy ŠIS je potrebné vyriešiť nasledujúce okruhy problémov:

- vypracovanie a prijatie *harmonizovaných kritérií pre hodnotenie bezpečnosti IS* platných nielen pre ŠIS, ale aj pre celú štátnu správu,
- vypracovanie návrhov a prijatie *právnych predpisov o bezpečnosti a ochrane IS*:
  - vytvorenie legislatívneho rámca pre *ochranu prístupu k uchovávaným a prenášaným utajovaným informáciám* vo všetkých IS,
  - vytvorenie legislatívneho rámca pre *ochranu osobných a dôverných údajov* v IS,

- vytvorenie legislatívneho a právneho rámca pre využitie dokumentov v digitálnej forme, predovšetkým *akceptovanie digitálneho podpisu* (ako dôkazu odosielateľa neodmietnuteľnosti prijatej správy prijímateľom a potvrdenie odosielateľa),

- vytvorenie podmienok pre využitie metód elektronickej ochrany písomných dokumentov:
  - vytvorenie legislatívneho rámca pre ochranu autentickosti a obsahu písomných dokumentov na báze využitia elektronických metód šifrovej ochrany informácií,
  - vytvorenie legislatívneho rámca pre zabezpečenie písomných dokumentov a ich ochranu proti fyzickej strate, zničeniu alebo úplnej nečitateľnosti väčšej časti ich obsahu na báze využitia elektronických metód šifrovej ochrany informácií.

V „Koncepcii štátneho informačného systému na roky 1997 - 1998“, časť Bezpečnosť a ochrana informačných systémov, je medzi návrhom úloh pre ŠIS požadované, aby v oblasti metodického riadenia ochrany a bezpečnosti informačných systémov boli vykonané nasledujúce kroky:

1. Prijatie ISO normy pre bezpečnostný manažment, resp. jej vyhlásenie ako štandard pre ŠIS.
2. Vydanie metodiky bezpečnosti a ochrany IS.

Rovnakú štruktúru dokumentov prijal aj rezort Ministerstva obrany SR, v ktorom sú už niekoľko rokov zavedené materiály príbuzného obsahového zamerania. Prijatý armádny štandard má oproti štandardu požadovanému v Koncepcii, ktorý je zameraný len na bezpečnostný manažment, širší charakter s platnosťou pre celú oblasť bezpečnosti informačných systémov rezortu MO SR.

Druhý materiál vo forme smernice dopĺňa bezpečnostný štandard a definuje podmienky prevádzky bezpečnostných podsystémov chránených informačných systémov a obsah bezpečnostných materiálov rezortu.

Pre vypracovanie uvedených bezpečnostných metodických materiálov (štandardu a metodiky), ktoré sú požadované v Koncepcii štátneho informačného systému, je potom vhodné obsahovo využiť oba armádne materiály a vychádzať pri tom zo skúseností rezortu MO SR.

Návrh na doplnenie Harmonogramu realizácie úloh ŠIS o úlohy ochrany a bezpečnosti

V časti Harmonogram realizácie úloh ŠIS na roky 1997 - 1998 (ďalej len Harmonogram) Koncepcie štátneho informačného systému sú navrhnuté len dve z úloh v oblasti bezpečnosti a ochrany ŠIS:

- **Vypracovanie návrhu právnych predpisov upravujúcich bezpečnosť a ochranu informačných systémov**

Forma výstupu: návrh právnych predpisov upravujúcich bezpečnosť a ochranu informačných systémov

- **Bezpečnosť a ochrana informačných systémov**

Forma výstupu: metodika

Okrem dvoch v Harmonograme požadovaných úlohách ochrany a bezpečnosti ŠIS však je potrebné do Harmonogramu zaradiť ďalšie úlohy:

- **Vypracovanie harmonizovaných kritérií pre hodnotenie bezpečnosti IS** platných nielen pre ŠIS, ale aj pre celú štátnu správu.

Forma výstupu: kritériá pre hodnotenie bezpečnosti.

- **Vypracovanie štandardu pre oblasť bezpečnosti ŠIS**.

Forma výstupu: bezpečnostný štandard ŠIS.

- **Vytvorenie podmienok pre využitie metód elektronickej ochrany písomných dokumentov**.

Forma výstupu: legislatívny rámec použitia metód elektronickej ochrany pre písomné dokumenty.

- **Riešenie bezpečnosti modelu ŠIS.**

Forma výstupu: návrh bezpečnostných opatrení a realizácia bezpečnostného podsystému modelu.

- **Analýza a návrh bezpečnosti pilotného projektu ŠIS.**

Forma výstupu: bezpečnostný projekt pilotného projektu.

Záver

Väčšina systémov je fyzicky dosť prístupných pre verejnosť, pretože pre vstupy do týchto systémov existujú brány založené stále väčšinou iba na jednoduchom hesle. Pre skúseného „sieťara“ s trochou času nie je problém tieto brány prekonať a životne dôležité dáta sú na dosah ruky. A cieľom útokov nemusí byť len vlastné získanie dát, ale tiež ich úplné zničenie. Potom už ostávajú skutočne len oči pre plač.

Hakeri určite od nikoho pomocnú ruku priamo nedostanú. Jedna vec je ale istá - počet naivne spravovaných a chránených sietí na celom svete rastie. A to je pravé miesto, kde sa musí začať so správnym zabezpečením siete. Ďalšou skutočnosťou je, že užívatelia stále pokračujú v opakovanom používaní hesiel, ktoré sú po sieťach posielané v nezakódovanom tvare a dajú sa snoričom odchytiť.

Pokiaľ bude rozvoj Internetu pokračovať tak rýchle ako do tejto doby, budú mať hakeri zaujímavú a určite vzrušujúcu prácu na niekoľko svojich životov. Ako teda proti hakerom a všetkým ostatným útočníkom bojovať? Predovšetkým používaním najbezpečnejších ochranných prostriedkov, vzdelávaním užívateľov a informovaním správcov systémov. Bezpečnosť systémov by sa mala strážiť, ako sa hovorí od podlahy.

Isté je, že pokusov o narušenie cudzích systémov nebude ubúdať, skôr naopak. Treba urobiť všetko pre to, aby pribúdalo len tých neúspešných, ktoré stroskotajú na dostatočne vybudovanej a udržovanej obrane. Hlavnou úlohou v podmienkach SR je, aby sa počet neúspešných pokusov do systémov blížil čo najviac k sto percentám. Nie je totiž možné robiť si ilúzie, že práve naše systémy tento „záujem“ obíde. Ako ukazuje nedávna minulosť, skôr opak bude pravdou.

Literatúra

[1] Koncepcia štátneho informačného systému na roky 1997 - 1998

[2] Šmirjak, M.: Analýza rizík informačných systémov a spôsoby automatizácie. In: Počítačová bezpečnosť '95, B.Bystrica, 1995, str.64-75

[3] Šmirjak, M.: Bezpečnosť informačných a telekomunikačných systémov použitím analýzy rizík. In: 2. medzinárodná konferencia o telekomunikačných technológiách - TELEKOMUNIKÁCIE '96, Bratislava, 1996, str. 240-245

[4] Šmirjak, M.: Problémy bezpečnosti pripojenia armádnej siete k Internetu. In: Vojenské obzory č.1, Bratislava 1997

[5] Šmirjak, M.: Nevyhnutnosť používania národných prostriedkov pri ochrane utajovaných informácií. In: Vojenské obzory č.1, Bratislava 1998