OCHRANA INFORMÁCIÍ V GRAFICKÝCH INFORMAČNÝCH SYSTÉMOCH A ANALÝZA RIZÍK

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

Úvod

Spôsoby neautorizovaného prieniku do informačných systémov spracovávajúcich grafické informácie a zneužitie chránených informácií sú rovnaké, ako v prípade bežných druhov informačných systémov. Oproti týmto systémom majú snáď len jedinú odlišnosť - prenos, spracovanie a uchovávanie veľkého objemu dát. V prípade GIS budovaného v TOPÚ B.Bystrica sa náročnosť zvyšuje spracovávaním aj obrazových informácií. Preto aj spôsoby možného narušenia a princípy zabezpečenia potrebnej úrovne ochrany sú identické s inými systémami.

Cieľom príspevku je poukázať na vážnosť situácie bezpečnostných rizík pôsobiacich v prostredí grafických informačných systémov a uviesť **analýzu rizík ako nástroj optimalizácie komplexného zabezpečenia systémov**. To znamená minimalizácia ceny bezpečnostných opatrení pri súčasnej maximalizácii úrovne zabezpečenia systému.

1. Problémy bezpečnosti informačných systémov

Prakticky žiaden súčasný distribuovaný systém nebol konštruovaný ako integrovaný celok. Tieto systémy vznikli až "zlepením" existujúcich pracovných staníc, lokálnych sietí všetkého druhu, minipočítačov a napojením na vonkajšie siete. To samozrejme nesie so sebou veľké bezpečnostné riziká v podobe pravdepodobných trhlín v nehomogénnej štruktúre takýchto systémov. **V prípade systému budovaného v TOPÚ sa to potvrdilo doslova. Vážna bezpečnostná slabina hore uvádzaného druhu tu bola odhalená a následne odstránená až na základe aplikovania metódy analýzy rizík.**

Ďalším problémom je, že mnohé spoločnosti často nevedia, koľko počítačov vlastne majú (niektoré ani približne). Nemajú tak ani tušenie, čo sa v nich deje a kto každý sa im môže do siete napojiť. Zložitosť sietí tak vytvára veľa príležitostí pre ich zneužitie, zvlášť v podobe nedovoleného prístupu k dôverným informáciám.

Nedávna štúdia organizácie Price Waterhouse odhalila, že **ak spoločnosť stratí svoje informácie na viac ako 3 dni, je 60% šanca jej nezvratného konca. Čím dlhšia strata, tým horší následok. Ak sú informácie stratené počas mesiaca, je 90% šanca bankrotu.**

Price Waterhouse tiež zistila, že 7% zo skúmaných spoločností už bolo potrestaných značnými obchodnými škodami v dôsledku neprimeranej informačnej bezpečnosti. Ich záverom je neradostné konštatovanie, že tento problém sa stále zhoršuje: **čoskoro bude jedna z desiatich organizácií vážne poškodená zo spomínaných dôvodov, čo môže viesť priamo k jej zániku.**

Konzultačná agentúra Intrusion Detection z New Yorku zistila prekvapivú a alarmujúcu skutočnosť, že 11% užívateľov nemusí na začiatku práce uvádzať vôbec žiadne heslo, 22% užívateľov má dokonca právomoci supervízora (čo je mimoriadne vysoké číslo, keď uvážime, aký široký prístup tieto právomoci umožňujú). Ďalej takmer 90% organizácií od svojich zamestnancov nepožaduje dostatočne často meniť svoje heslá (v závislosti od ceny údajov by to mal byť interval zmeny 30 až 60 dní).

A ako je to v našich podmienkach?! Podľa našich zistení je situácia ešte oveľa horšia. Pritom nejde len o Armádu SR, ale aj iné organizácie.

2. Možné príčiny existujúceho stavu

Zaostávanie, ako jedno z nemilých dedičstiev nedávnej minulosti, sa snáď najvýraznejšie prejavilo v oblasti informačných technológií a toto informačné zaostávanie sa následne negatívne premieta aj do ďalších oblastí. V rámci znižovania tohoto zaostávania v informačnej oblasti preto možno v súčasnej dobe sledovať doslova masové nasadzovanie výpočtovej techniky vo všetkých oblastiach činnosti aj v rámci Armády SR. Súčasne je vidieť aj výrazný rozvoj informačných technológií, predovšetkým 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 ešte stále nie sú schopní dostatočne zodpovedne posúdiť nebezpečenstvá a úskalia existujúce (a neustále sa vyvíjajúce) pri počítačovom spracovávaní 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, ktorými môže zlomyseľný užívateľ ohroziť počítačový systém, ako získať prístup k jeho výpočtovej kapacite a dostať sa k tomu najcennejšiemu, čo systém obsahuje - 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.

Dokazujú to aj údaje organizácie CERT (Computer Emergency Response Team), ktoré sú skutočne alarmujúce. Počet nahlásených 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 - v prípade komerčných subjektov, ako sú napr. banky, by prípadné správy o narušení počítačovej siete mohli viesť k odvráteniu zákazníkov.

U vládnych úradov a štátnych 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 zriedkakedy) alebo ak informácie zverejní niekto iný a nie je možné tomu zabrániť (napr. novinári).

Hlavným vinníkom poškodenia alebo úniku informácií potom býva najčastejšie nedokonalé alebo lajdácke zabezpečenie systému. Preto je potrebné na niektoré otázky ochrany počítačovo spracovávaných dát upozorniť a uviesť aj ich vhodné riešenie.

Počítačová kriminalita je nielen výnosná, ale skoro beztrestná. Dokazujú to nedávne štatistické údaje z USA: zo sto počítačových zločinov je odhalený len jeden, z odhalených je potom len pätnásť percent ohlásených a len jeden z 33 ohlásených zločinov je dotiahnutých až do konca, t.j. až k trestnému postihu páchateľa zločinu. **Celkovo teda na 22 tisíc počítačových zločinov pripadá len jeden potrestaný páchateľ (čo predstavuje skutočne len zanedbateľný podiel - 0,0045%).**

Iné zdroje uvádzajú, že v USA je v oblasti počítačového zločinu zistený iba jeden prípad zo sto, k stíhaniu dôjde v jednom prípade z ôsmich a iba jeden z 33 obžalovaných skončí vo väzení. **Pravdepodobnosť, že počítačový zločinec uvidí mreže väzenia, je teda 1:26 400 ...!**

Napriek mierne odlišným údajom vo výsledkoch oboch hore uvádzaných prameňov je možné si všimnúť, že ich závery sú pozoruhodne podobné a dostatočne výstižne charakterizujú výhodnosť a "motiváciu" počítačových zločinov na jednej strane a zároveň z toho prameniacu ich veľkú nebezpečnosť na strane druhej. Pritom nebezpečenstvo odhalenia a trestného postihu je oproti iným druhom kriminality skutočne zanedbateľné.

3. Analýza rizík a obnovenie funkčnosti

Každý budovaný informačný systém musí mať v zmysle zákona č.100/86 súčasne spracovaný bezpečnostný projekt. Súčasťou každého bezpečnostného projektu je posúdenie

potrebnej úrovne implementácie bezpečnostných opatrení. Proces, v rámci ktorého sa posudzuje potrebnosť a rozsah bezpečnostných opatrení, sa nazýva analýza rizík. Výsledkom analýzy rizík uvedenom v bezpečnostnom projekte je stanovenie množiny bezpečnostných hrozieb pôsobiacich na tento systém a množiny bezpečnostných slabín a rizík systému. V nadväznosti na výsledky analýzy rizík sú v bezpečnostnom projekte potom navrhnuté bezpečnostné opatrenia, ktoré majú eliminovať zistené bezpečnostné riziká. Analýza rizík je procedúra používajúca odhad potenciálnych strát, ktoré môžu vzniknúť ako dôsledok zraniteľnosti systému, a kvantifikáciu strát, ktoré môžu vzniknúť ako dôsledok existujúcich hrozieb.

Analýza rizík musí byť vykonaná ako jedna z prvých činností pri tvorbe budovaného informačného systému.

Analýza 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 primerane redukovať na prijateľnú úroveň. Jednoducho povedané, analýza rizík vytvára obraz toho, ako dôležitý je váš systém a ako ďaleko ste ochotný zabezpečiť ho - z hľadiska zariadení, ľudí a rozpočtu.

Štandardná analýza rizík zahrňuje pohľad na hmotné hodnoty - napríklad budovy, počítače, ďalšie zariadenia a určenia, ako ich najlepšie chrániť. Vzhľadom k tomu, že najcennejšie aktíva bývajú predstavované informáciami, je potrebné sa veľmi starostlivo zamerať tiež na to, ako najlepšie chrániť práve informácie.

Dôležitou súčasťou automatizačných systémov pre analýzu rizík sú aj syntetické činnosti, tzv. "recovery" činnosti (t.j. **činnosti plánovanej regenerácie systému po narušení alebo zrútení**). Pomocou počítača sú presne rozvrhnuté a naplánované detailné akcie po každom type možného prieniku a realizovania hrozby. Plány akcií sú presne rozvrhnuté na jednotlivé osoby, ich povinnosti, spúšťanie špeciálnych programov, rekonštrukcie a regenerácie systému, ich postupnosť krokov ako i činnosti súvisiace s auditom a s opatreniami na identifikáciu a elimináciu narušiteľa, resp. hrozby (napr. RecoveryPAC).

Schematické znázornenie štruktúry automatizačných prostriedkov je uvedené na obrázku 1.

4. Systém pre analýzu rizík RiskPAC

Systém RiskPAC je expertný systém určený ako nástroj na podporu rozhodovania v procese analýzy a riadenia rizík a pri tvorbe bezpečnostných projektov informačných systémov. Primárne je určený na ohodnocovanie bezpečnostných rizík.

Systém predkladá otázky týkajúce sa daného subjektu v hodnotenom prostredí. Následne priraďuje hodnoty (určité váhy) uvedeným odpovediam, zobrazuje výsledky v popisnom formáte a predkladá doporučenia a opatrenia.

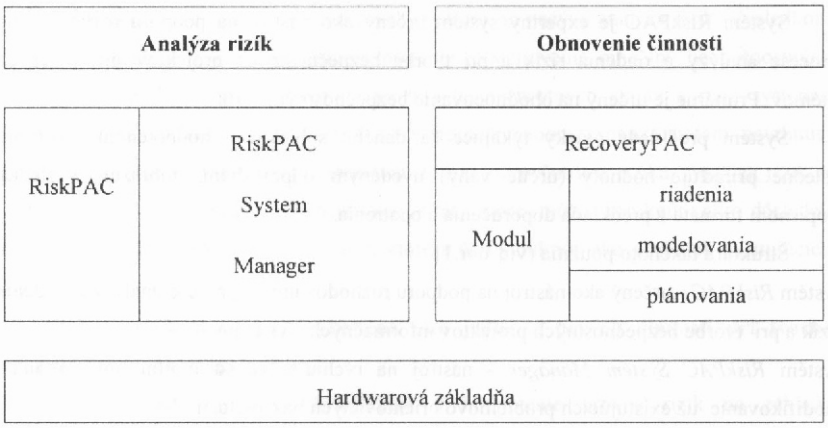
Štruktúra takéhoto použitia (viď obr.1):

- systém *RiskPAC* - určený ako nástroj na podporu rozhodovania v procese analýzy a riadenia rizík a pri tvorbe bezpečnostných projektov informačných systémov,
- systém *RiskPAC System Manager* - nástroj na rýchlu a ľahkú tvorbu nových alebo modifikovanie už existujúcich problémovo orientovaných báz znalostí.

V systéme RiakPAC sú integrované znalosti a mnohoročné skúsenosti odborníkov z oblasti bezpečnosti informačných systémov. Kvalifikované použitie takéhoto systému vnáša do inak značne heuristického procesu novú kvalitu.

Jedna z najmnohostrannejších funkcií systému RiskPAC je schopnosť ukázať zmeny v profile rizík a doporučenia ako odpoveď na otázky typu "Čo ak ...". Napríklad, čo ak je pridaný nový procesor do špecifikácie prostredia? Alebo ak je pridaný nový súbor aplikácií do existujúceho procesora? Čo ak boli zmenené rôzne parametre týkajúce sa riadenia logického prístupu do systému? Čo ak boli systému pridané telekomunikačné funkcie?

Systém RiskPAC System Manager je nástroj na rýchly a ľahký vývoj dotazníkov systému RiskPAC. Pritom je možné vytvoriť nový dotazník alebo modifikovať existujúci. Systém RiskPAC System Manager poskytuje možnosť vytvoriť alebo editovať otázky, riadiť tvorbu ohodnotenia dotazníkov a poskytuje rady založené na odpovediach užívateľov na dotazník. Ďalej je možné vytvoriť knižnice doporučeni nazývaných *štandardy*. Tieto štandardy je potom možné pripájať k odpovediam na špecifické otázky alebo k ich ohodnoteniam (nazývaným aj *skóre*).



Obr.1. Blokové znázornenie štruktúry prostriedkov automatizácie analýzy rizík a obnovenia funkčnosti

5. Systém pre riadenie obnovenia činnosti RecoveryPAC

Systém RecoveryPAC je pružný nástroj, ktorý umožňuje produkovať na mieru stavané plány obnovenia činnosti systémov. Systém plánovania obnovenia činnosti vytvára ľahko udržiavané plány obnovenia pre celé organizácie, jednotlivé oddelenia a dátové centrá. Systém podporuje najefektívnejšie procesy používané pri vývoji úspešných plánov. Plne integrované moduly plánovania projektov pomáhajú užívateľovi identifikovať kritické prostriedky a úlohy a integrovať ich vo vytváranom pláne.

Systém riadenia obnovenia činnosti sa skladá z troch základných modulov:

- modul riadenia projektov,
- modul modelovania obnovenia dát,
- modul plánovania obnovenia činnosti.

Plány obnovenia činnosti produkuje systém RecoveryPAC ako pomoc pri identifikovaní životne dôležitých prostriedkov a operačných funkcií. Pre účely obnovenia všetkých dôležitých funkcií systému je treba určiť pracovné skupiny. Systém RecoveryPAC potom priraďuje úlohy a prideľuje dôležité prostriedky týmto skupinám ako pomoc pri uvádzaní systému na pôvodnú úroveň prevádzkyschopnosti.

Systém poskytuje veľmi bohatú a rozsiahlu možnosť tvorby správ. Správy môžu byť zobrazené na obrazovke, vytlačené na tlačiarni, uchované v ASCII súbore alebo okamžite prenesené do určeného textového procesora. Navyše môže systém zlučovať text vytvorený

v textovom procesore so správami databázového systému tak, aby bolo možné vytvoriť plán celkovej organizácie obnovenia činnosti.

Záver

V súčasnej dobe dokonca aj tie najobyčajnejšie počítačové systémy môžu obsahovať strategicky dôležité informácie. Hodnota podniku sa už nevyjadruje len v počte strojov a v hodnote kapitálu, ale tiež v mierkach intelektuálnych hodnôt. Informačnému bohatstvu je preto potrebné venovať minimálne rovnakú pozornosť, ako napr. výrobnému zariadeniu za milión korún.

Čím viac sietí sa navzájom prepojuje a čím viac kritických aplikácií v nich prebieha, tým viac sa stáva ochrana sietí a celých informačných systémov súčasťou zdravého myslenia. *"Čo myslíte, kedy som si kúpil poplašné zariadenie do svojho domu? Keď vykradli prvý dom v našej ulici! To isté sa vzťahuje aj na užívateľov sietí,"* hovorí Vijay Ahuja, manažér sieťovej divízie IBM pre bezpečnostné produkty.

To samozrejme platí aj pre využitie analýzy rizík ako metódy na dosiahnutie reálnej bezpečnosti a ochrany počítačových systémov.

O analýze rizík mnohí "odborníci" hovoria, ale len niektorí jej naozaj rozumejú a chápu ju komplexne a len skutočne málokto ju dokáže vykonať zodpovedne a na požadovanej úrovni. Využívanie automatizačných prostriedkov je zatiaľ takmer neznáme a pritom ovlyvňuje kvalitu riešenia zásadným spôsobom.

Každý systém poskytuje takú celkovú úroveň zabezpečenia a ochrany spracovávaných údajov, akú úroveň má najslabší článok jeho zabezpečenia. Teda ak bezpečnosť nie je riešená komplexne, môžu byť ostatné už navrhnuté a imlementované opatrenia úplne zbytočné a môžu spôsobiť aj zbytočné vynaloženie nemalých finačných prostriedkov.