Zdeněk DVOŘÁK*

MOŽNÉ OHROZENIA MANAŽÉRSKYCH INFORMAČNÝCH SYSTÉMOV V DOPRAVE

Riadiace a informačné systémy v doprave sa stávajú rozhodujúcim kvalitatívnym nástrojom pre vytvorenie konkurenčnej výhody. Veľa dopravných firiem je nútených hľadať cesty na ochranu svojich informačných systémov. Táto problematika je natoľko významná, že v rámci štúdia na Fakulte špeciálneho inžinierstva Žilinskej univerzity (ďalej FŠI) vytvárame veľký priestor pre teoretické i praktické zvládnutie tejto problematiky.

VLASTNOSTI INFORMÁCIÍ

Aby informácia bolo užitočná pre rozhodovanie musí spĺňať určité charakteristiky. Vo všeobecnosti je známych päť týchto charakteristík.

- informácia je relevantná, t.j. vzťahuje sa k aktuálnemu rozhodovaniu,
- informácia je presná, t.j. je dostatočne správna aby tvorila základ pre účinné rozhodovanie,
- informácia je včasná, t.j. je k dispozícii vtedy, kedy to je potrebné,
- informácia je úplná, t.j. pochádza z vhodného zdroja a pokrýva všetky oblasti ktoré rozhodovanie vyžaduje,
- informácia je stručná, t.j. poskytuje takú úroveň sumarizácie ktorá je vhodná pre príslušné rozhodnutie.

Úmerne s tým, ako sa správna činnosť informačných technológií (ďalej IT) stáva nevyhnutnou podmienkou prijatia správneho rozhodnutia, by sa mala zvyšovať aj pozornosť venovaná opatreniam na zaistenie korektnej a neprerušenej činnosti jednotlivých komponentov IT systému spracovania údajov v organizácii. Cieľom takéhoto snaženia je vytvorenie bezpečného informačného systému (ďalej IS), teda systému v ktorom je zaistené:

- ochrana údajov, ktoré IS spracováva a uchováva tak, aby nedošlo k ujme na užitočnosti informácií, ktoré poskytuje, a aby nedošlo k úniku informácií neoprávneným osobám (t.j. chránené údaje resp.

* Fakulta špeciálneho inžinierstva Žilinskej univerzity v Žiline

informácie sú sprístupnené len vymedzenému okruhu subjektov, ktorí nad týmito údajmi, resp. informáciami, môžu vykonávať len určené operácie),
- IS poskytuje svoje služby v požadovanej kvalite, sortimente a čase, a to aj v prípade značných odchyliek okolia IS od normálneho stavu.

Problémom, spojeným so zaistením ochrany IS sa venuje oblasť tzv. informačnej bezpečnosti. Je nutné konštatovať, že problém bezpečného IS nevznikol len s príchodom moderných IT, ale patrí k problémom, ktoré ľudstvo riešilo už v rokoch dávno minulých. Úroveň spoločenského vývoja však viedla k tomu, že techniky zaisťovania bezpečnosti vtedajších systémov spracovania a prenosu údajov a informácií boli využívané prakticky len v diplomatickej a vojenskej oblasti a podliehali prísnemu utajovaniu. V súčasnosti sa situácia dosť zmenila.

MOTIVÁCIA ZABEZPEČENIA INFORMAČNÝCH SYSTÉMOV

S prudkým rozvojom informačných technológii sa stále viacej a viacej sa spracovávajú informácie s veľkou hodnotou. Často ide o informácie s nezanedbateľnou hodnotou a preto musia byť chránené tak:
- aby k nim mali prístup len oprávnené osoby,
- aby sa spracovávali nefalšované informácie,
- aby sa dalo zistiť, kto ich vytvoril, zmenil nebo odstránil,
- aby neboli nekontrolovaným spôsobom vyzradené,
- aby boli dostupné vtedy, keď sú potrebné.

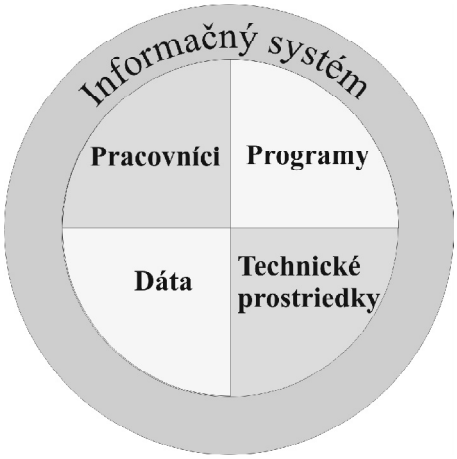
S týmto rozvojom sa začínajú objavovať pojmy ako počítačová kriminalita, hackeri, ochrana informácií, ochrana informačných systémov a pod. Po počiatočnom nadšení z nových možností, ktoré nám prinášajú tieto technológie sa začína ukazovať aj odvrátená strana tohto pokroku. V dnešnej dobe už nestačí len pripustiť, že existujú určité riziká a hrozby spojené s používaním informačných systémov. Firma, organizácia alebo inštitúcia sa musí brániť tomu, aby funkcie ich IS neboli či už úmyselne, nebo neúmyselne zneprístupnené. Od ľudí, ktorí prevádzkujú informačné systémy sa očakáva, že príjmu opatrenia na zabezpečenie ochrany týchto systémov.

Moderný manažér, je tak postavený pred neľahkú úlohu. Čo je to vlastne "bezpečnosť"? Ktoré faktory a do akej miery ju ovplyvňujú? Ako vlastne vybudovať účinný, odôvodnený a ekonomicky efektívny systém opatrení na zaistenie "bezpečnosti"? A ako vlastne "dokázať", že vybudovaný systém opatrení poskytuje "dostatočnú bezpečnosť"?

V dnešnej dobe si až príliš často vrcholový manažment neuvedomuje do akej miery je organizácia, jej zisk či schopnosti plniť svoje poslanie a svoje záväzky závislé od správnej a neprerušenej činnosti informačného systému a od údajov, ktoré sa v ňom spracovávajú. A práve účinná ochrana pred hrozbami, ktoré prinášajú informačné technológie, je predovšetkým záležitosťou manažmentu. V súčasnosti za azda najsilnejšiu motiváciu k aktivitám pre zabezpečenie informačných systémov je existencia právnych úprav na ochranu dát, a tie je žiaduce, resp. nutné, dodržovať. Ochrana informačných systémov sa dotýka v týchto zákonoch: Zákon č. 52/1998 Z.z. o ochrane osobných údajov v informačných systémoch. A zvlášť pre orgány štátnej správy je dôležitý zákon č. 100/1996 Z.z. o ochrane štátneho tajomstva, služobného tajomstva a o šifrovej ochrane informácií.

VÝKLAD ZÁKLADNÝCH POJMOV Z OBLASTI OCHRANY IS

Základné pojmy, vymedzujúce oblasť ochrany IS, si vysvetlíme na modelu, v ktorom sa IS skladá z štyroch nasledujúcich typov komponent:



Obrázok č. 1 Časti informačného systému
Fig.1. Parts of Information System

· technické prostriedky - procesor, pamäte, terminály atd.,
· programy - aplikační programy, operační systém atd.,
· dáta - dáta uložená v databáze, výsledky, vstupné dáta atd.,
· pracovníci - užívatelia, personál.

Prvé tri z uvedených komponent predstavujú pre organizáciu prevádzkujúcu IS isté hodnoty, preto sa nazývajú aktíva. Spôsob dosiahnutia bezpečnosti určuje bezpečnostná politika. Pojmom bezpečnostná politika IS označujeme súhrn noriem, pravidiel a praktík, definujúce spôsob správy, ochrany a distribúcie citlivých dát a iných aktív v rámci činnosti IS. Citlivé dáta majú pre chod organizácie zásadný význam, ich kompromitáciou alebo zneužitím by vznikla organizácii prevádzkujúcej IS škoda, nemohla by riadne plniť svoje poslanie, prípadne by aj porušila zákon o ochrane osobných údajov. Je treba si uvedomiť, že každý IS je zraniteľný, bezpečnostní politika IS iba znižuje pravdepodobnosť úspechu pri útoku proti IS alebo núti útočníka vynaložiť viac prostriedkov alebo času. Absolútne bezpečný systém neexistuje!

ZRANITEĽNÉ MIESTO

Slabinu IS využiteľnú k spôsobeniu škôd alebo strát útokom na IS nazývame zraniteľné miesto. Existencia zraniteľných miest je dôsledok chýb v návrhu alebo v implementácii IS, dôsledok vysokej hustoty uložených informácií, zložitosti softwaru, existencie skrytých kanálov pre prenos informácie inou ako zamýšľanou cestou apod.
Podstata zraniteľného miesta môže byť:

· fyzická - napr. umiestenie IS v mieste, ktoré je ľahko dostupné sabotáži alebo vandalizmu, výpadku napätia,
· prírodná -objektívne faktory typu záplava, požiar, zemetrasenie, blesk v hardwaru nebo v softwaru,
· fyzikálne - vyžarovanie, útoky pri komunikácii pri výmene správy, na spoje,
· v ľudskom faktore -najväčšia zraniteľnosť zo všetkých možných variant,
· v návrhu IS,

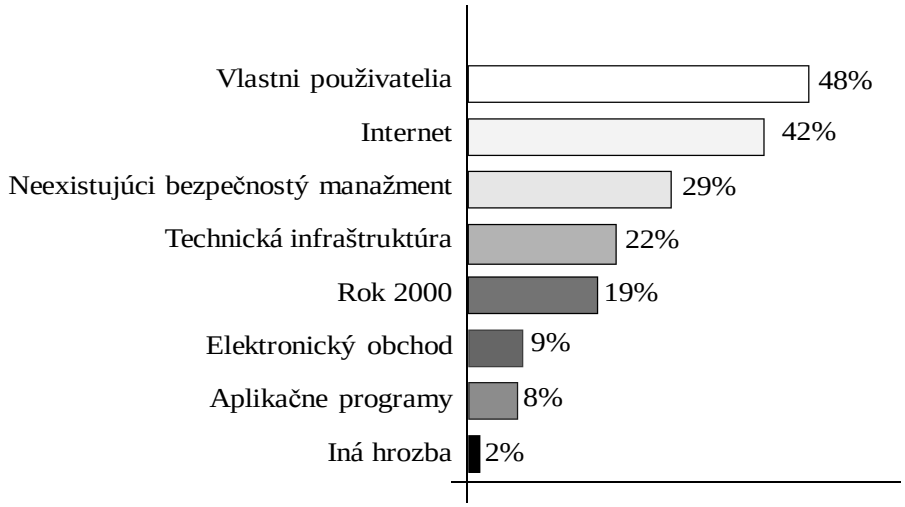
Zraniteľná miesta sú vlastnosťami (súčasťou) informačného systému, ktorých existencia spôsobuje, že niektoré vplyvy prostredia, v ktorom sa informačný systém prevádzkuje, predstavujú preň hrozby. Pojmom hrozba sa označuje možnosť využiť zraniteľné miesto IS k útoku na naň - k spôsobeniu škody na aktívach. Treba si uvedomiť, že hrozby pre informačný systém môžu byť výsledkom nielen úmyselnej činnosti "útočníka", ale aj nedbalosti osoby, ktorá sa podieľala na návrhu, vývoji, implementácií, testovaní, inštalácií, údržbe či prevádzke systému, je jeho oprávneným používateľom, prípadne môžu byť aj dôsledkom výskytu neovládateľných udalostí "zásahom vyššej moci" v okolí systému (napríklad požiar).

Hrozby môžeme kategorizovať na:
· objektívne
1. prírodne, fyzické - požiar, povodeň, výpadok prúdu, poruchy..., u ktorých je prevencia obtiažna a u ktorých je treba riešiť skôr minimalizáciu dopadov vhodným plánom obnovy; v tomto prípade je treba vypracovať havarijní plán,
2. fyzikálne - napr. elektromagnetické vyžarovanie,
3. technické nebo logické - porucha pamäti, softwarové "zadné vrátka", zlé prepojenie inak bezpečných komponent, krádež, resp. zničenie pamäťového média, alebo nedokonalé zrušenie informácie na ňom,

· subjektívne, t. z. hrozby plynúce z ľudského faktora
1. neúmyselné - napr. pôsobení neškoleného užívateľa / správca,
2. úmyselné - predstavované potencionálnou existenciou vonkajších útočníkov (špióni, teroristi, kriminálne živly, konkurenti, hackeri) i vnútorných útočníkov (odhaduje sa, že 80 % útokov na IT je vedené zvnútra, útočníkom, ktorý môže byť prepustený, nahnevaný, vydieraný, chamtivý zamestnanec); veľmi efektívne z hľadiska vedenia útoku je súčinnosť oboch typov útočníkov.

Z uvedeného by malo byť jasné, že človek, ktorý sa seriózne pokúša zaistiť bezpečnosť nejakého IS, prípadne posudzuje účinnosť existujúcich ochranných opatrení, by mal mať k dispozícií poznatky o možných hrozbách, technikách útoku a nedostatkoch či obmedzeniach existujúcich ochranných prostriedkov. Je len logické, že kvalita výsledku jeho práce bude priamo úmerná rozsahu jeho znalostí v tejto špeciálnej oblasti, resp. jeho schopnosti predstaviť si ďalšie možné postupy pri útoku na systém. Našťastie, obzvlášť pre technickejšie orientované útoky využívajúce bezpečnostné nedostatky používaných systémov, existuje množstvo prístupných informačných zdrojov.

V nasledujúcom grafe môžeme vidieť najväčšie hrozby z hľadiska bezpečnosti podľa prieskumu NBÚ ČR z.r. 1999.



Obrázok č.2 Hrozby v informačných systémoch
Fig. 2. Threats in Inforamtion Systems

Z uvedeného grafu jasne vyplýva, že človek je najslabším článkom ochrany. Ľudia si často sebakriticky priznávajú, že "človek je tvor omylný". Keďže človek zohráva podstatnú úlohu pri návrhu, implementácií, testovaní, prevádzke a údržbe jednotlivých komponentov informačného systému i informačného systému ako celku, je potrebné rešpektovať jeho obmedzenia. Pri úvahách o bezpečnosti informačného systému je preto potrebné dôsledne rátať s ľudskou nedokonalosťou, a to vo všetkých fázach - od návrhu jednotlivých komponentov systému až po bežnú prevádzku informačného systému ako celku, a použiť opatrenia, ktoré by aspoň čiastočne kompenzovali túto nedokonalosť (vzdelávanie, kontroly, zdvojené procedúry, a podobne).

RIZIKO

Existencia hrozby predstavuje riziko. Pojem rizika je spravidla manažérovi dobre známy - vo svojej bežnej práci musí zohľadňovať množstvo potenciálnych rizík, hodnotiť ich "reálnosť", možný dopad, rozhodovať sa o potrebe vhodnej reakcie (niektorými opatreniami je možné zmenšiť možnosť výskytu rizikového faktora, inými opatreniami zas veľkosť možných dôsledkov) a podobne. Vzhľadom na obvyklú kľúčovú úlohu informačného systému pre chod samotnej organizácie je teda prirodzené zvažovať aj riziká súvisiace práve s informačným systémom.

V súvislosti s informačným systémom pod pojmom riziko rozumieme pravdepodobnosť využitia zraniteľného miesta IS. Hovoríme, že sa hrozba uplatní s takou a takou pravdepodobnosťou. Rizika ide charakterizovať vedľa pravdepodobnosti výskytu bezpečnostného incidentu i potenciálne spôsobenou škodou.

ÚTOČNÍK

Skúsenosti z praxe nám ukazujú, že prevádzkovatelia, alebo používatelia informačných systémov pri úvahách o zabezpečení ich systému málokedy uvažujú o tom, akými spôsobmi by mohol prípadný útočník zaútočiť na ich systém. Bezpečný informačný systém chápu ako systém, v ktorom je zabudovaná nejaká množina bezpečnostných prostriedkov bez toho, aby sa zamysleli nad tým, pred akými postupmi útočníka sa vlastne majú chrániť. Vytrvalé pokusy primeť ich k presnejšiemu vyjadreniu v tomto smere obvykle vedú v najlepšom prípade k sformulovaniu niekoľkých jednoduchých scenárov. Ľudia, ktorí majú na starosti zaistenie bezpečnosti informačného systému, by sa však mali pokúsiť pozrieť na "svoj" systém očami potenciálneho protivníka, vcítiť sa do jeho pozície, skrátka skúsiť do značnej miery "uvažovať zločinecky". Ak si čo len trochu vážia svoj informačný systém, nemali by sa uspokojiť s predstavou primitívne uvažujúceho protivníka, iba ak by chceli svoj systém chrániť len pred takouto kategóriou a rezignovali by pred predstavou útoku inteligentnejšie konajúceho útočníka. Dôležité je si uvedomiť, kto môže útočiť. Útočník môže byť vonkajší, ale v organizácii sa často vyskytuje i vnútorný útočník. Podľa znalosti a vybavenosti rozoznávame:

- **útočníkov slabej sily**
  amatéri, náhodný útočníci, využívajúci náhodne objavené zraniteľná miesta pri bežnej práci; ide o náhodne, často neúmyselné útoky, útočníci majú obmedzené znalosti, príležitosti i prostriedky, pre ochranu pred nimi stačí prijať relatívne slabé bezpečnostné opatrenia, ktoré sú lacné,
- **útočníkov strednej sily**
  hackeri, ktorých častým krédom je dostať sa k tomu, k čomu nie sú autorizovaní; jedná sa o bežné útoky, útočníci majú veľa krát veľa znalostí, obvykle ale nemajú zjavné príležitosti k útokom a mávajú obmedzené prostriedky; ako ochrana proti nim sa prijímajú bezpečnostní opatrenia strednej sily,
- **útočníkov veľkej sily**
  profesionálni zločinci, ktorí majú pôvod medzi počítačovými profesionálmi, je pre nich typická vysoká úroveň znalostí, majú obvykle dostatok prostriedkov (peňazí) a veľakrát i dosť času k prevedení útoku, prevádzajú útoky vymykajúce sa bežnej praxi, pre ochranu pred nimi je nutné prijímať silná bezpečnostní opatrenia.

ÚTOK NA INFORMAČNÝ SYSTÉM

Útokom, ktorý nazývame tiež bezpečnostným incidentom, rozumieme buď úmyselné využitie zraniteľného miesta, t. z. využitie zraniteľného miesta k spôsobeniu škôd/strát na aktívach IS, alebo neúmyselné uskutočnenie akcie, ktorej výsledkom je škoda na aktívach. Pri analýze možných foriem útokov na IS je treba riešiť problémy typu: ako sa prejavuje počítačová kriminalita, aké sú možné formy útokov, kto útočí, kto môže páchať počítačový zločin, aká rizika súvisia s používaním informačných technológií, ako sa chrániť pred útokmi apod. Následne riešenými problémami sú potom rozhodnutia typu: ako detekovať útok, ako zistiť bezpečnostní incident, ako reagovať na útok, čo robiť, keď dôjde k bezpečnostnému incidentu.

Možné formy útokov:

- **prerušením**
  aktívny útok na dostupnosť, napr. strata, zneprístupenie, poškodenie aktíva, porucha periférie, vymazanie programu, vymazanie dát, porucha v operačnom systéme,
- **odpočúvaním**
  pasívny útok na dôveryhodnosť, kedy neautorizovaný subjekt si neoprávnene sprístupní aktíva, ide napr. o okopírovanie programu alebo o okopírovanie dát,

· **zmenou**
aktívny útok na integritu, neautorizovaný subjekt zasiahne do aktíva, prevedie sa napr. zmena uložených alebo prenášaných dát, pridanie funkcie do programu,
· **pridaním hodnoty**
aktívny útok na integritu alebo útok na autenticitu, t.z. prípad, kedy neautorizovaná strana niečo vytvorí (dodanie falošných dát).

Vhodnou formou ochrany pred pasívnymi útokmi odpočúvaním je prevencia, pretože detekcia odpočúvania je veľmi obtiažna. Absolútna prevencia útokov samozrejme zabezpečiteľná nieje, preto typická ochrana (hlavne pred aktívnymi formami útokov) je založená na detekcii útokov a na následnej obnove činnosti. Veľmi dôležité je vziať si poučenie zo zistených skutočností a získané skúsenosti uplatniť pri vylepšovaní ochrán. Útok môže byť úmyselný alebo neúmyselný, resp. náhodný. Útok ide tiež charakterizovať ako:
· **útok s veľkou škodou** (tiež ho nazývame významný)
ak je častý, potom organizácia prevádzkujúca IS vypracováva bezpečnostnú politiku s cieľom ochrany pred týmto typom útoku. Škodlivé dôsledky nie často uplatňovaného útoku ide riešiť aj poistením. Významný útok, ktorého následky znamenajú zrútenie organizácie alebo jej trestnú zodpovednosť, nazývame katastrofický,
· **útok s malou škodou** (nevýznamný)
škody spôsobené nevýznamným útokom sú prijateľným rizikom.

Rozoznávame:
· útoky na hardware, ktoré sa dajú viesť:
- prerušením - prírodná havárie, neúmyselne útoky spôsobené fajčením, údery,
- úmyselné útoky krádežou, deštrukciou,
- odpočúvaním - krádež času procesoru, miesta v pamäti,
- pridaním hodnoty - zmenou režimu činnosti,

· útoky na software , ktoré sa dajú viesť:
- prerušením činnosti IS - medzi neúmyselné útoky môžu patriť vymazanie softwaru spôsobené zlým konfiguračným systémom alebo archivačným systémom, použitie neotestovaných programov, chyby operátora; medzi úmyselné útoky patrí napr. úmyselné vymazanie programu,
- odpočúvaním - neoprávnené kópie programu, pirátstvo,
- zmenou - napr. využitím "zadných vrátok" (neverejných spúšťacích postupov z doby tvorby softwaru),
pridaním hodnoty - zabudovaním trójskych koňov, víry, červy, logické bomby.

ZÁVER

Treba poznamenať, že útoky na hardware sa dajú riešiť bezpečnostnými systémy, strážami apod. Ale útok na software vedú obvykle profesionálne zdatní jedinci, a tak útok na dáta je omnoho nebezpečnejší, pretože dáta vie čítať a interpretovať de facto ktokoľvek. Pre hodnotu dát je charakteristická ich dočasnosť, tržná hodnota dát nie je jedinou cenou dát, do tejto ceny sa musí zahrnúť cena ich rekonštrukcie, ich opätovného vytvorenia.

Článok bol vytvorený s finančnou podporou VTP TASID 2005, časť Riešenie krízových situácií.

ANOTÁCIA:

Článok popisuje aktuálny pohľad na hrozby, ktoré ohrozujú informačné systémy. Sú tu uvedené jednotlivé časti informačných systémov, hrozby a riziká. Ďalej sú definované možné útoky a útočníci, ktorí ohrozujú informačné systémy.

THE POSSIBLE THREAT OF MANAGERIAL INFORMATION SYSTEMS IN TRANSPORT

The article describes actual view for threats which threaten information systems. There are various parts of information systems, threats and risks. Next are defined possible attack and attackers which threats information systems.