Marek Čandík
Katedra managementu a informatiky
Fakulta bezpečnostního managementu
Policejní akademie ČR v Praze

Informační bezpečnost

Information security

Úvod

Informační technologie zpracovávají stále více a více informací s velkou hodnotou. Pokud hovoříme v souvislosti s informačními technologiemi o *zpracovávání informací*, pak tím rozumíme použití těchto technologií k uchovávání, přenosu, vyhodnocování a prezentaci informací.

Protože se mnohdy jedná o informace s nezanedbatelnou hodnotou (např. zdravotní záznamy,daňová přiznání, bankovní účty, elektronické platební nástroje, výsledky vývoje nebo výzkumu,obchodní záměry), musí být chráněny tak:

- aby k nim měly přístup pouze oprávněné osoby
- aby se zpracovávaly nefalšované informace
- aby se dalo zjistit, kdo je vytvořil, změnil nebo odstranil
- aby nebyly nekontrolovaným způsobem vyzrazeny
- aby byly dostupné tehdy, když jsou potřebné.

Narušení bezpečnosti zpracovávání informací lze provést například:

- narušením soukromí či utajení informací
- vydáváním se za jinou oprávněnou osobu a zneužíváním jejích privilegií
- distancováním se od odpovědnosti nebo od závazků plynoucích z manipulace s informacemi
- tvrzením, že se nějaká informace někam poslala a toto se nikdy nestalo
- tvrzením, že se informace získala od nějakého podvodníka
- neoprávněným zvýšením svých privilegií přístupu k informacím
- modifikací privilegií ostatních osob
- zatajením výskytu důvěrné informace v jiných informacích
- zjišťováním, kdo a kdy si zpřístupňuje které informace
- zařazením se jako skrytý mezičlánek v konverzaci jiných subjektů
- pokažením funkcionality softwaru doplněním skrytých funkcí
- narušením protokolu činností jiných subjektů zavedením nesprávných, nekorektních informací

- podkopáním důvěryhodnosti protokolu způsobeným zjevným, byť možná jen zdánlivými poruchami
- bráněním jiným uživatelům legitimně komunikovat.

Zranitelnost informačních systémů

Zranitelnost informačních systémů představuje jejich obecnou vlastnost. Jedná se vlastně o zranitelná místa (zranitelné komponenty, prvky) těchto systémů jak z hlediska funkčnosti, tak i správnosti (přesněji, míry záruky za správnost).

V této souvislosti nutno poznamenat, že zranitelnost fyzického prostředí řady informačních systémů je dosud značná. Dále pak, že u celé řady firem a institucí je zcela neopodstatněně podceňována zranitelnost organizačního prostředí, především pak personálních (lidských) prvků informačních systémů. Poněkud více pozornosti, ale stále to není dost, je věnováno logickému a komunikačnímu (WAN) prostředí.

Prakticky to znamená, že informační technologie bývá nevhodně dislokována a neautorizovaný přístup do prostor jejího umístění bývá často snadný. Samostatnou kapitolou je "úroveň" služeb ochrany a ostrahy objektů. Využívání automatizovaných systémů kontroly vstupu a pohybu osob v objektech je ojedinělé, a snad jen systémy EZS (elektronická zabezpečovací signalizace) lze vidět v provozuschopném stavu v některých objektech.

Velkým problémem zranitelnosti informačních systémů v praxi bývá nedokonalost jejich organizačních zázemí, to znamená dokumentování (formalizace) všech informačních toků a procedur, představované celou řadou směrnic a jiných písemných dokumentů. Lze také předpokládat, že jen nemnoho ze správců informačních systémů má k dispozici tzv. havarijní plány, stejně tak, že jen málo firem a institucí má k dispozici kvalifikovaný bezpečnostní management.

Specifickou oblastí při posuzování zranitelnosti organizačního prostředí je pak personální management. Výběr a výchova pracovníků informačních systémů má celou řadu slabin a je smutné, že teprve několik kriminálních případů v posledním období způsobilo na tomto úseku, jak lze doufat, obrat k lepšímu.

Zatím největší pozornost byla věnována zranitelnosti informačních systémů z hlediska jejich logického prostředí. Odborníci vědí, že například některá hardwarová vybavení mají vlastnosti Fault Tolerant System, některá jsou certifikována (spolu s operačními systémy, ale zatím pouze dle TSEC), budují se záložní výpočetní centra. Jsou aplikovány řízené přístupy k objektům a začínají se projevovat počátky odklonu od systému přístupových hesel směrem k využívání personálních inteligentních čipových karet Smart Cards.

Ve vztahu k eliminaci zranitelnosti komunikačního prostředí (z hlediska dostupnosti) již dnes řada firem a institucí využívá záložních spojovacích cest a některé z nich se začaly zajímat o šifrovou ochranu, enkrypci, svých datových přenosů (z hlediska integrity a důvěrnosti).

Rizika informačních systémů

Pravděpodobnost, že se uplatní některá z výše uvedených hrozeb nebo zranitelných míst informačních systémů je vyjádřena hodnotou informačního rizika. Teoretické odhady jsou potvrzovány praktickými zkušenostmi, ze kterých vyplývá, že nejpravděpodobnější riziko pramení z uplatnění hrozby - systém je dodán, instalován nebo používán způsobem, který není bezpečný. Přitom nejčastějšími příčinami tohoto rizika bývají omyly a nedbalost personálu spolu s nesprávnou manipulací.

Je zajímavé, že již zmíněné aktuální případy uplatněné hrozby - autorizovaný uživatel se pokouší získat přístup k prostředkům, ke kterým nemá přístup povolen - zaujímají z pohledu dlouhodobých zahraničních statistik místo ve spodní části žebříčku četnosti. V našich podmínkách však bude situace poněkud odlišná, vzhledem k rozdílu mezi úrovní bezpečnostních systémů našich a zahraničních institucí.

V této souvislosti je vhodné poznamenat, že za velký nedostatek řady informačních systémů je nutno považovat nedostatky v kvalitní formalizaci informačních procedur a toků. Například je naprosto nepřípustné, aby firemní programátor měl přístup do systému v provozu, nebo naopak, aby ladění programů byl prováděno na tzv. ostrých datech. Rovněž tak je nepřípustné, aby třeba informaci jisté klasifikační úrovně bylo možno neautorizovaně získat i tak, že jsou autorizovaně získány její jednotlivé části s nižší klasifikační úrovní.

Bezpečnostní systém

Některé z firem a institucí již přišly na to, že nejefektivnějším a z dlouhodobého hlediska nejhospodárnějším způsobem řešení bezpečnosti (důvěryhodnosti) jejich informačních systémů, je odborně provedená výstavba bezpečnostního systému. Takovýto krok vyžaduje ze strany firemního managementu zájem o řešení informační bezpečnosti na straně jedné, na straně druhé přijetí dlouhodobého programu informační bezpečnosti. Realizace tohoto programu předpokládá v prvé fázi provedení bezpečnostní analýzy firemního informačního systému, na základě které by měla být vypracována bezpečnostní politika, a v případě potřeby vypracován bezpečnostní projekt. Výstavba konkrétního bezpečnostního systému se pak obvykle provádí buď na základě bezpečnostního projektu, nebo dle závěrů bezpečnostní analýzy. Na tomto místě je vhodné poznamenat, že v rámci firemních a institucionálních informačních systémů lze, vzhledem k odlišným a specifickým vlastnostem, naprosto samostatně řešit informační bezpečnost zpracování dat a informační bezpečnost přenosu dat.

Kvalitní ochrana informací a informačních systémů je nejen vizitkou firmy nebo instituce, ale i nezbytným předpokladem bezproblémových auditů prováděných například s cílem získat např. certifikát kvality dle ISO 9001.

Napadení informačního systému

V době stále se zvyšující komplexnosti operačních systémů i aplikačního programového vybavení dochází ke stále častějším objevům bezpečnostních děr (security holes) v těchto produktech. Různé skupiny, sdružující se převážně na internetu, těchto "děr" využívají a tvoří programy, které mohou kompromitovat informační systém. Tyto programy jsou pak volně dostupné pro všechny uživatele Internetu. To znamená, že pro narušení systému již nejsou potřebné žádné speciální znalosti a techniky - narušení může provést kdokoli, kdo si daný program zrovna "stáhne".

Velmi alarmující jsou statistiky, které uvádějí, že až 90% realizovaných útoků na informační systém probíhá zevnitř organizace, to znamená, že je provádějí vlastní zaměstnanci

V současnosti existuje více než 800 různých způsobů, kterými lze napadnout zařízení, připojená do počítačové sítě.

Tyto útoky se liší použitými prostředky a cíli. Útoky mohou způsobit následující škody:

- **Nedostupnost služby** - tzv. DoS útoky (Denial of Service) - způsobí, že případná služba (http, ftp…), na kterou byl prováděn útok přestane být funkční - může dojít i k "zatuhnutí", případně restartu serveru apod.
- **Neoprávněný přístup** - výsledkem útoku může být to, že útočník neoprávněně získá plný nebo částečný přístup k zařízení, a to mu následně umožní provádět neautorizované změny v konfiguraci, mazání nebo modifikaci souborů apod. Často bývá takto napadený server využíván jako základna pro provádění útoků na další zařízení.
- **Získání důvěrných informací** - výsledkem útoku může být získání citlivých informací - např. seznam uživatelských jmen a hesel apod.

Zabezpečování IT

Pojmem zabezpečování IT označujeme proces dosažení a udržení důvěrnosti, integrity, dostupnosti, prokazatelnosti odpovědnosti, autenticity a spolehlivosti informací a služeb IT na přiměřené úrovni.

Bezpečnost IT použitých v organizaci se dosahuje především plněním manažerských funkcí, souvisejících s bezpečností IT jako integrální součásti plnění globálního plánu správy organizace.

Mezi takové manažerské funkce typicky patří:

- určení cílů, strategií a politiky zabezpečení IT organizace
- určení požadavků na zabezpečení IT organizace
- identifikace a analýza hrozeb pro aktiva IT v rámci organizace
- identifikace a analýza rizik pro organizaci plynoucích z používání IT
- specifikace přiměřených bezpečnostních opatření eliminujících nebo snižujících rizika

- sledování implementace a provozu bezpečnostních opatření použitých pro účinnou ochranu informací a služeb IT v rámci organizace
- vyvinutí a zavedení programu zvyšování bezpečnostních znalostí a vědomí nutnosti u držovat bezpečí všech, kdo IT v organizaci používají
- detekování bezpečnostních incidentů a adekvátní reakce na ně.

Bezpečnostní politika v oblasti IT je nedílnou součástí všeobecné *bezpečnostní politiky organizace*, která představuje souhrn bezpečnostních zásad a předpisů definujících způsob zabezpečení organizace od fyzické ostrahy, přes ochranu profesních zájmů až po ochranu soukromí a lidských práv.

Bezpečnostní politika IT organizace (také *celková bezpečnostní politika IT*) se v tomto kontextu zabývá výběrem bezpečnostních zásad a předpisů splňujících bezpečnostní politiku organizace a obecně definujících bezpečné používání informačních zdrojů v rámci organizace nezávisle na konkrétně použitých informačních technologiích (určuje, která data jsou pro organizaci citlivá, kdo je za ně odpovědný, předpisuje infrastrukturu zabývající se v rámci organizační struktury organizace bezpečností, vymezuje základní omezení, která se musí respektovat apod.).

Určení detailních konkrétních norem, pravidel, praktik, předpisů konkrétně definujících způsob správy, ochrany, distribuce citlivých informací a jiných konkrétních informačních zdrojů v rámci organizace, specifikace bezpečnostních opatření a způsobu jejich implementace, určení způsobu jejich použití, který zaručuje přiměřenou bezpečnost odpovídající požadavkům bezpečnostní politiky IT organizace, při respektování konkrétně použitých IT pro realizaci IS organizace, to vše je náplní *bezpečnostní politiky IS* organizace (také *systémové bezpečnostní politiky IT*).

Bezpečnostní mechanismy

Pro implementaci funkcí prosazujících bezpečnost se používají bezpečnostní mechanismy. *Bezpečnostní mechanismus* je logika nebo algoritmus, který hardwarově (technicky), softwarově (logicky), fyzicky nebo administrativně implementuje bezpečnostní funkci. Rozpoznáváme (podle publikace [ITSEC]):

- *slabé bezpečnostní mechanismy* pro ochranu před amatéry, proti náhodným útokům, lze je narušit *kvalifikovaným útokem*, tj. *útokem střední síly*
- *bezpečnostní mechanismy střední síly* pro ochranu před hackery, proti úmyslným útokům s omezenými příležitostmi a možnostmi, hovoříme o běžných útocích
- *silné bezpečnostní mechanismy* ochrana před profesionály, ochrana proti útočníkům s vysokou úrovní znalostí, s velkými příležitostmi, s velkými prostředky, používajícími *útoky vymykající se běžné praxi*.

Podle použité technologické základny rozeznáváme bezpečnostní mechanismy:

- *softwarové bezpečnostní mechanismy* (mnohdy označované jako *logické bezpečnostní mechanismy*) princip řízení přístupu v daném operačním systému, kryptografie – symetrická (s tajným klíčem), asymetrická (s veřejným a privátním klíčem), standardy pro návrh, kódování, testování, údržbu programů, ochranné nástroje v operačních systémech, např. ochrana paměti, ochrana souborů řízením přístupu, obecná ochrana objektů, tj. přístupové matice, přístupové seznamy, hesla, autentizace přístupu k terminálu, mechanismy *určené pro autentizaci zpráv*
- *hardwarové* bezpečnostní mechanismy (mnohdy označované *jako technické bezpečnostní mechanismy*) šifrovače a autentizační a identifikační karty
- *fyzické bezpečnostní mechanismy* stínění, trezory, zámky, protipožární ochrana, generátory náhradní energie, chráněná místa pro záložní kopie dat a programů
- *administrativní bezpečnostní mechanismy* (výběr důvěryhodných osob, hesla, právní normy, zákony, vyhlášky, předpisy).

Mezi bezpečnostní mechanismy patří i ochranné nástroje v aplikačních systémech.

Lidský faktor a jeho podíl na útocích na informační systém

Více než 90 % veškerých mimořádných událostí a narušení bezpečnosti informačního systému je způsobeno úmyslným (krádež, pomsta, zlomyslnost) i neúmyslným (nezkušenost, neznalost, nedbalost) jednáním člověka - zaměstnance společnosti.

Stalo se již téměř každodenní praxí, že novináři uvádějí jako zdroj svých informací dobře informovaného pracovníka banky, ministerstva, policie a dalších organizací, který si nepřál být jmenován. Tato krátká informace by měla být velkým varováním pro vedoucí pracovníky příslušné organizace, protože se v její struktuře nachází slabý článek - pracovník, jehož zájmy nejsou shodné se zájmy společnosti. Může mít přístup k důvěrným informacím, často i vysoká nebo dokonce správcovská práva v informačním systému dané společnosti, což mu umožňuje kopírování a modifikaci vybraných záznamů. Pokud se pracovník společnosti rozhodne spolupracovat s novináři a data, která odcizí ve své společnosti jsou uveřejněna v tisku, ve velké většině případů se podaří tohoto pracovníka odhalit.

Daleko nebezpečnější jsou rezidenti, kteří skrytě a mnohdy po velmi dlouhou dobu poskytují informace získané v rámci svého pracovního zařazení třetí straně nebo ve prospěch třetí strany směřují činnost "své" společnosti (v uvozovkách úmyslně, protože takový pracovník vlastně pracuje pro dvě strany). To v konečném důsledku může velmi vážně poškodit kredit nebo dokonce ohrozit samotnou existenci společnosti, ve které tuto činnost provádí.

Závadová činnost takovéhoto člověka uvnitř firmy může oblasti informatiky a správy informačního systému společnosti může spočívat především v :

- modifikaci vlastních přístupových práv
- úpravě v centrálních a pobočkových databázích a příslušných auditních souborů
- znepřístupnění dat dalším spolupracovníkům
- přerušení datových okruhů
- modifikaci přístupových práv ostatních uživatelů
- změně konfigurace počítačů nebo komunikačních prostředků
- nedodržování antivirové ochrany
- neprovádění nebo pouze částečném zálohování dat
- porušování pravidel platných pro tvorbu a používání přístupových hesel

Pro zajištění trvale dobrého jména společnosti a důvěryhodnosti jejího informačního systému je tedy nutné, vedle stálého monitorování všech funkcí, které zajišťují bezpečnost a spolehlivost informačního systému, věnovat pozornost i personálnímu obsazení jednotlivých důležitých funkcí v organizaci a každodenní práci s lidmi.

Způsoby ochrany informačních systémů

Při hodnocení bezpečnosti informačních technologií v dnešních podmínkách je možné konstatovat, že dochází k určitému přibližování se úrovni vyspělých států. Ve většině našich firem došlo k výraznému posílení fyzických bezpečnostních opatření, zejména v oblasti ostrahy, fyzického přístupu, vytváření bezpečnostních zón, běžně se provádí antivirová ochrana. Bezpečnostní úroveň operačních systémů středních počítačů již v řadě případů odpovídá obvyklé minimální úrovni amerických kritérií TCSEC (Trusted Computer Security Evaluation Criteria). Dosud však není dostatečné povědomí o nutnosti implementovat zásady bezpečnosti ve všech částech životního cyklu automatizovaného zpracování, prosazení a naplnění všech aspektů bezpečnosti (personální, administrativní, technický).

V roce 1993 byla vydána Ministerstvem hospodářství první verze přeložených harmonizovaných evropských kriterií pro hodnocení bezpečnosti informačních technologií ITSEC (Information Technology Security Evaluation Criteria). Byly tím vytvořeny předpoklady pro to, aby jak ze strany výrobců produktů a systémů IT, tak ze strany jejich uživatelů bylo pohlíženo na hodnocení bezpečnosti IT jednotně. Jako formální základ pro vzájemné mezinárodní uznávání hodnocení uzavřely Kanada, Francie, Německo, Velká Británie a Spojené státy americké v roce 1998 dohodu "Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security", zkráceně nazývanou CCRA (CC Recognition Arrangement). Česká republika se připojila k dohodě v září roku 2004 jako certifikáty využívající účastník.

Přijímáním izolovaných řešení, do kterých nejsou začleněny podmínky pro některé nové standardní přístupy, vzniká určité nebezpečí budoucích zvýšených nákladů. Ve světě např. dochází k pronikání systému EDI (Elektronic Data

Interchange) z oblasti průmyslu a obchodu do oblasti celní a do světa bank. Zavádění EDI je provázeno při výměně dokumentů všeho druhu mezi jednotlivými hospodářskými subjekty logickým sjednocováním a přijímáním standardů. V našich firmách nebyla při vytváření nových systémů problematika EDI dostatečně známa. Při přechodu na on-line propojení mezi firmami a jejich klienty (i mezi klientskými IS) má při využití systému EDI stěžejní význam zabudování bezpečnostních prvků do těchto systémů.

V souladu s vývojem ve světě je jedním z hlavních úkolů v oblasti bezpečnosti informačních technologií prosadit implementaci mezinárodních a evropských standardů, které dávají záruku vysoké úrovně bezpečnostních řešení.

Při řešení otázek bezpečnosti informačních systémů je nutné především stanovit úroveň rizika a její nejvýznamnější atributy, tj. co má největší negativní vliv na důvěrnost, integritu a dostupnost informačního systému. Dále je nutné se zabývat problémem jak na tyto negativní vlivy reagovat. Nabízí se zde celá řada reakcí, od jejich akceptování až po přijímání opatření na jejich eliminaci.

Úroveň rizika může být zmenšena tím, že se v rámci procesu zvládání rizik implementuje taková architektura systému, která zahrnuje organizační, administrativní, personální, fyzické a technické bezpečnostní komponenty. Proces zvládání rizik tvoří plánování, organizování, řízení a kontrola zdrojů za účelem zajištění přijatelné zbytkové úrovně rizika a úměrných nákladů.

V oblasti bezpečnosti informačních systémů se setkáváme s určitými obtížemi, které vznikají jako důsledek dynamických změn rizikových faktorů a prudkého vývoje informačních technologií. Nejsou-li včas a adekvátně vzaty v úvahu všechny faktory rizika, může to vést k neefektivním a zbytečně drahým opatřením. Zvládání rizik musí být považováno za jeden z rozhodujících kroků řešení bezpečnosti

Závěr

Kvůli obavám z bezpečnostních rizik zvažují soukromé společnosti co nejkvalitnější systémy zabezpečení přístupu do svých prostor a sítí obsahujících citlivá data. Při snaze efektivně zabezpečit informační systém je obvyklým problémem, jaká bezpečnostní opatření přijmout k zajištění přiměřené ochrany informačního systému tak, aby byla dostatečně účinná a současně finančně a organizačně přiměřená povaze chráněné věci. Je třeba poznamenat věc nejdůležitější, a to, že absolutní bezpečnost je nedosažitelná, není ani stálá, a proto si musíme pamatovat, že : *bezpečnost je trvalý proces.*

Literatura

1. BATT, E., SIECHERT, C., *Zabezpečení Microsoft Windows 2000 a XP,* Computer Press, 2004, ISBN 80-7226-878-3
2. ENDOR, C., a kol., *Detekce a prevence počítačového útoku*, Grada, 2005, ISBN 80-247-1035-8

3. JIROVSKÝ, V. *Kybernetická kriminalita.* Praha : Grada a.s., 2007, ISBN 978-80-247-1561-2
4. KOCMAN, R., LOHNINKSKY, J., *Jak se bránit virům, spamu a spyware*, Computer Press, 2005, ISBN 80-251-0793-0
5. KRÁL, M. *Bezpečnost domácího počítače.* Praha : Grada a.s., 2006, ISBN 80-247-1408-6
6. NORTHCUTT, S., a kol., *Bezpečnost počítačových sítí*, Computer Press, 2005, ISBN 80-251-0697-7
7. POŽÁR, J. Manažerská *informatika.* Praha : PAČR, 2003, ISBN 80-7251-139-4
8. RENDL, J., *Bezpečnosti Informací*, materiály pro výuku, PAČR, 2008.
9. SZOR, P., *Počítačové viry*, Zoner press, 2006, ISBN 80-86815-04-8

Tento článek byl zpracován v rámci Projektu vědeckovýzkumného úkolu č. 4/4 „Informační bezpečnost a kybernetická kriminalita v organizaci“, který je součástí Integrovaného výzkumného úkolu na léta 2010-2015, realizovaný Fakultou bezpečnostního managementu Policejní akademie České republiky v Praze.