Informační systémy a jejich bezpečnost

Petr Hanáček, Jan Staudek

Motto: *„My si umělé vytvoříme svá vlastní data. To je padělatelství dovedené k naprosté dokonalosti. Nepotřebujete žádný speciální papír, žádné barvy, jen čísla v počítači."*
John McNeil, Poradce

Motivace

V roce 1989 jistý hacker, pracující v Indii, vnikl ze svého počítače po síti do počítače na jednotce intenzivní péče v jedné francouzské nemocnici. Výsledkem jeho akcí byla smrt několika pacientů. Jiný hacker si může stejně snadno vybrat za cíl svého snažení například váš počítačový systém.

S rozvojem a rozšiřováním výpočetní techniky se také zvyšuje stupeň závislosti uživatelů na počítačovém informačním systému (dále jen IS). Zvyšuje se také objem investic a hodnot, které byly do IS vloženy. Pokud IS není dostatečně chráněn, může se stát z hlediska bezpečnosti slabým místem uživatelské organizace a jeho nesprávná činnost může organizaci způsobit značné škody nebo dokonce ochromit na nějakou dobu její činnost.

V současné době je věnována velká publicita činnosti hackerů a působení virů. Jsou však i jiné příčiny porušení bezpečnosti IS (například požár nebo krádež), které mohou způsobit mnohem vážnější škody. Bezpečnostní opatření musí být proto aplikována vyváženě a dostatečně důkladně, aby se zajistila dostatečná úroveň obrany proti možným narušením bezpečnosti IS.

Co to je bezpečnost IS a její narušení

Každý informační systém musí zajišťovat dodržování tří základních vlastností dat – důvěrnosti, integrity a přístupnosti. Co tyto pojmy znamenají:

Důvěrnost dat – data nesmí být přístupná neoprávněným entitám

Integrita dat – entity bez dostatečného oprávnění nesmí mít možnost data pozměnit nebo zničit

Přístupnost dat – data musí být na požádání přístupná oprávněným entitám

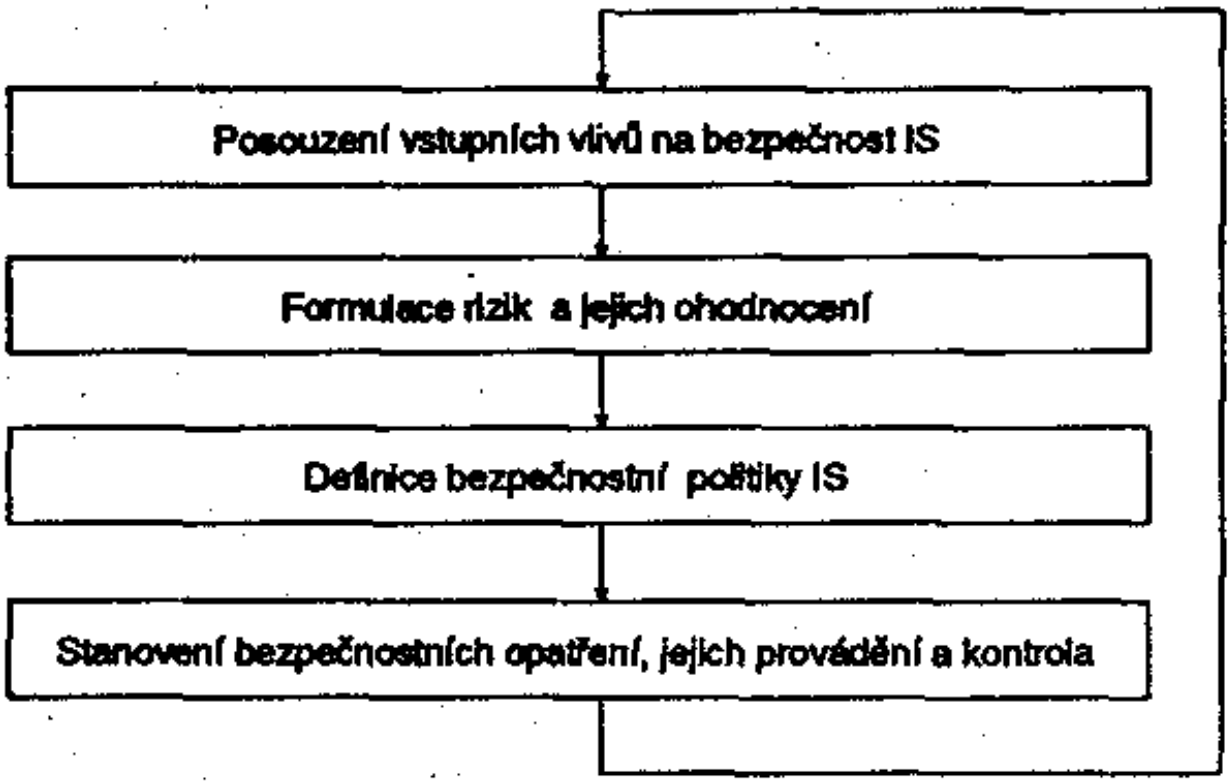
Pozn.: Pojmem entita označujeme subjekt informačního systému (např. osoba, skupina osob, proces, terminál, uzlový počítač), který lze jednoznačně identifikovat a kterému lze přiřadit určitou úroveň oprávnění.

Porušení kterékoli z výše uvedených tří zásad (tj. zpřístupnění dat neoprávněným entitám, nesprávnost nebo nekompletnost dat, nepřístupnost dat pro oprávněné entity) znamená narušení bezpečnosti IS (incident). U konkrétního IS je třeba definovat priority těchto zásad (v některých systémech může být primární důvěrnost i za cenu zhoršení přístupnosti, jindy je důležitá přístupnost bez ohledu na důvěrnost).

Vývoj bezpečnostní politiky IS

Vývoj bezpečnostní politiky informačního systému je cyklický proces. První kolo by mělo proběhnout už v okamžiku návrhu struktury IS, neboť struktura IS má velký vliv na jeho bezpečnost a naopak – požadavky na bezpečnost IS ovlivňují jeho strukturu. Další kola probíhají zpravidla při změně struktury už existujícího IS, při změně bezpečnostních požadavků nebo při zjištění bezpečnostních nedostatků.

Průběh jednoho takového kola je znázorněn na Obr. 1. Prvním úkolem při stanovování bezpečnostní politiky IS je posouzení vstupních vlivů na bezpečnost IS. Znamená to posouzení objemu investic uložených v IS, posouzení hrozeb pro IS a určení zranitelných míst IS. Další fáze (formulace rizik a jejich ohodnocení) určí pravděpodobnost a nebezpečnost jednotlivých rizik a s ohledem na cenu odpovídajících bezpečnostních opatření stanoví, která bezpečnostní opatření jsou ekonomicky vhodná a únosná. Ve fázi definice bezpečnostní politiky se formulují závazné zásady a pravidla pro jednotlivé oblasti bezpečnosti (fyzická, personální, procedurální, dokumentační a technická). Definuje se zodpovědnost za dodržování těchto bezpečnostních zásad. Poslední fází je stanovení konkrétních bezpečnostních opatření, jejich realizace a periodická kontrola dodržování zásad bezpečnostní politiky.



Obr. 1. *Jednotlivé fáze vývoje bezpečnostní politiky IS*

Co je třeba vzít v úvahu – vstupní vlivy

Při formulaci bezpečnostní politiky informačního systému je třeba vzít v úvahu tyto **vstupní vlivy na bezpečnost IS:**

- **stupeň závislosti organizace na IS** – tj. škody způsobené organizaci porušením některé ze zásad bezpečnosti IS
- **objem investic, vložených do IS** – cena vývoje, instalace a správy IS (technické i programové vybavení), spolu s hodnotou budov a zařízení
- **hodnota informací uložených v IS** – cena za pořízení a údržbu dat v IS
- **hrozby pro IS**
- **zranitelná místa IS**
- **cena bezpečnostních opatření**
- **zákonné povinnosti správce IS**

Některé z těchto vlivů probereme v následujících odstavcích podrobněji.

Hrozby pro IS

Vnější vlivy, které mohou způsobit narušení bezpečnosti IS se nazývají **hrozby**. Hrozby mohou být neúmyslné, jako například požár, záplava, technická závada, nebo úmyslné, například podvod, zpronevěra, krádež, hackerství nebo viry. Ze statistického sledování skutečných incidentů vyplývají tyto zajímavé skutečnosti:

- asi 40 % úmyslných incidentů má formu podvodu. Procentuální podíl krádeží, působení virů a hackerství je výrazně menší;
- asi 60 % incidentů ve formě podvodů není odhaleno interní kontrolou ani externí revizí ale vyjde najevo náhodně;
- asi 15 % incidentů ve formě podvodů zůstane neodhaleno po delší dobu než dva roky.

Hrozby pro IS dělíme na logické a fyzické. Fyzické hrozby se týkají zpravidla technického vybavení, logické programového vybavení. Možné fyzické hrozby (krádež, požár, výpadek napájení, porucha zařízení atd.) a jejich vliv na IS si jistě dokáže každý představit. Poněkud podrobněji se zmíníme o hrozbách logických a úmyslných.

Podvody a padělání

Podvod v prostředí IS zpravidla znamená takovou úpravu informací uložených v IS, z níž má pachatel jistý, zpravidla majetkový, neoprávněný prospěch. Podvody bývají páchány různými způsoby, uvedeme pouze některé:

– „ztrácení dat" (data didling) – data jsou nepatrně měněna (např. na posledním desetinném místě) a výsledek těchto změn je připisován ve prospěch pachatele

– „soukromý berňák" (salami slicing) – při každé aritmetické operaci se provede zaokrouhlení v neprospěch zákazníka a zaokrouhlovací chyby se střádájí ve prospěch pachatele

– neoprávněná změna vstupních dat (např. mrtvé duše – do vstupních dat jsou přidány záznamy o neexistujících osobách a na tyto osoby jsou inkasovány peníze)

- zničení, potlačení nebo úprava výstupních dat (např. sestav s výplatními listinami nebo bankovními příkazy)

Krádeže

Krádeže technického vybavení zpravidla nemají za cíl poškodit činnost IS, ale vzhledem k velké zranitelnosti dat mohou někdy nepřímo způsobit značné škody. Nebezpečnější jsou krádeže dat (porušení důvěrnosti dat), krádeže programového vybavení (softwarové pirátství), které způsobují nepřímé škody. Zdánlivě neškodné je provádění neoprávněných soukromých výpočtů na počítači, které však může způsobit snížení výpočetního výkonu nebo těžko odhalitelné náhodné havárie systému.

Zničení programového vybavení

Tento způsob počítačové kriminality bývá zpravidla páchán prostřednictvím virů a „časovaných bomb" (programů, které po určité, zpravidla velmi dlouhé, době po nainstalování způsobí havárii systému). I při případném odhalení je těžké pachateli čin dokázat a potrestat ho, neboť i v zemích s vyspělým zákonodárstvím se obtížně specifikuje trestná podstata činu.

Porušení důvěrnosti a integrity dat

S těmito činy se zpravidla pojí pojem hackerství. Pojem hacker původně znamenal člověka, který se přes telefonní linku napojí zvenčí na počítačový systém, překoná jeho bezpečnostní bariéry a poškodí jej (zpravidla pouze lehce, neboť jeho cílem není způsobit někomu škodu, ale dokázat majiteli systému svou intelektuální převahu). V současné době jsou „praví" hackeři výjimkou. Většina incidentů spočívajících v porušení důvěrnosti a integrity dat totiž bývá způsobena vlastními zaměstnanci organizace. Stejně jako u zničení programového vybavení, tak i u hackerství se vina pachatelů dokazuje velmi nesnadno.

Zákonné povinnosti správce IS

Povinnosti správce IS jsou definovány legislativou příslušného státu. V Československu prakticky neexistují zákony, vymezující práva a povinnosti správců a vlastníků dat. Na některé případy počítačové kriminality lze sice aplikovat stávající zákonné kategorie (např. podvod, krádež, poškození cizího majetku), ale to může vést k velmi kuriózním soudním procesům. Příkladem je nedávný soudní proces v Austrálii, kdy pachatel, obžalovaný z rozsáhlého podvodného zneužití telefonních úvěrových karet byl soudem osvobozen, protože podle formulace zákona lze podvést pouze osobu a nikoli stroj. Na problémy, spojené s vlastnictvím dat, však stávající zákony aplikovat nelze a v tomto směru nezbývá než alespoň uvést příklad obdobných zákonů ze zahraničí.

Ve Velké Británii existují tři zákony, zabývající se problematikou IS. Jsou to:

- Data Protection Act 1984
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990

Tyto zákony (konkrétně Data Protection Act) vycházejí z několika základních principů ochrany a správy dat:

- data smějí být shromažďována a zpracovávána pouze pro zákonné účely
- data mají vlastníka, kterým je osoba (fyzická nebo právnická), které se data týkají; tento vlastník svá data pouze propůjčil správci IS.
- vlastník má zákonné právo vědět, jaká data jsou o něm vedena v IS

- správce IS je povinen zajistit stupeň důvěrnosti dat odpovídající povaze dat a požadavkům vlastníka dat
- správce IS je povinen zajistit správnost dat
- jakmile správce dat nějakým způsobem ztratí právo na data jisté osoby, je povinen tato data zničit (životnost dat)
- výjimky z těchto zásad jsou povoleny pro účely národní bezpečnosti, prevence kriminality a evidence daní

Zákon Computer Misuse Act definuje tři nové kriminální delikty:

- neoprávněný přístup k IS (to znamená i hackerství)
- neoprávněný přístup k IS za účelem páchání dalších trestných činů
- neoprávněnou modifikaci dat

Zranitelná místa IS

Každý informační systém (nejen počítačový) je sám o sobě dosti zranitelný. U počítačových IS k tomuto faktu přistupují další specifické vlastnosti, které zranitelnost zvyšují:

- Data na počítačových médiích jsou uložena velmi efektivně (s velkou hustotou informace) a jejich redundance je poměrně malá. Tato skutečnost zvyšuje jednak nebezpečí krádeže dat (v aktovce lze odnést údaje o několika tisících osobách, což by při použití „papírového" IS nebylo možné). Vzhledem k malé redundanci se data při zničení nebo krádeži média nesnadno obnovují.
- Programové vybavení IS je velmi složité a obtížně se odhalují neoprávněné zásahy do programů.
- K počítačovému IS lze přistupovat i přes počítačové sítě nebo telefonní spoje což může dovolit zásahy cizím osobám.
- Při přenosu přes datové spoje mohou být data „odposlouchávána" a zneužita.

Cena bezpečnostních opatření

Bezpečnostní opatření zvyšují režii a snižují výkonnost IS; ztěžují přístup k datům v IS, nedovolují nejefektivnější využití IS, spotřebovávají prostředky IS (paměťový prostor, výpočetní výkon, přídavná zařízení), nepříznivě ovlivňují proces návrhu architektury IS, zvyšují pořizovací cenu a náklady na provoz IS.

Ohodnocení rizika pro IS

Ve fázi ohodnocení rizika stanovujeme pravděpodobnost a nebezpečnost jednotlivých rizik a s ohledem na cenu odpovídajících bezpečnostních opatření stanovíme, která bez-

pečnostní opatření jsou ekonomicky vhodná a únosná. Při ohodnocení jednotlivých rizik musíme vzít v úvahu tři faktory – pravděpodobnost vzniku incidentu na základě uvažovaného rizika, průměrnou výši škody způsobené incidentem a cenu bezpečnostního opatření zabraňujícího incidentu. V následujících dvou tabulkách jsou uvedeny procentuální pravděpodobnosti nejběžnějších incidentů. Údaje byly získány statistickým vyhodnocením z organizací, které profesionálně využívají počítačový IS a mají alespoň 100 zaměstnanců. Výše škod u jednotlivých druhů incidentů je průměrná, maximální škoda je podle statistiky asi pětkrát vyšší.

Fyzický bezpečnostní incident	Procento případů	Průměrná škoda v $1000
Výpadek napájení	28 %	9
Porucha zařízení	20 %	12
Krádež části zařízení	14 %	5
Výpadek komunikačních spojů	13 %	12
Škody vzniklé přepětím (blesk)	8 %	6
Požár	4 %	2000
Sabotáž	2 %	?

Logický bezpečnostní incident	Procento případů	Průměrná škoda v $1000
Použití neotestovaných programů	16 %	6
Škodlivé programy (viry)	16 %	12
Chyba uživatele	14 %	?
Chyba systémového operátora	11 %	?
Zneužití počítače vlastními zaměstnanci	10 %	2
Neoprávněný přístup pomocí místního terminálu	7 %	4
Neoprávněný přístup pomocí komunikační linky (hackeři)	4 %	23
Podvržení vstupních dat	3 %	14
Změny na výstupních datech	2 %	5
Monitorování pronajatých datových spojů	<1 %	?
Elektronické odposlouchávání	<1 %	?

Pro určení závažnosti škod, které nelze vyjádřit finanční ztrátou, slouží následující tabulka, ve které je uvedena používaná klasifikace bezpečnostních incidentů podle způsobených následků.

Závažnost incidentu	Následky incidentu			
	Finanční ztráta v $1000	Soudní stíhání	Porušení důvěrnosti	Ohrožení osob
Nevýznamná	< 10	Úřední napomenutí	Zveřejňání nedůležitých informací	Lehké zranění jednotlivce
Malá	10–100	Pokuta < $1000	Zveřejnění osobních informací	Lehké zranění několika osob
Významná	100–500	Pokuta > $1000	Kompromitace jedné osoby	Těžké zranění jednotlivce
Velká	500–1000	Trestní stíhání	Kompromitace několika osob	Těžké zranění několika osob
Velmi velká	> 1000	Několik trestních stíhání	Kompromitace mnoha osob	Smrt několika osob

Jakmile je provedeno ohodnocení rizik, je třeba u každého rizika stanovit způsob, jak s tímto rizikem nakládat. Nejobvyklejší způsoby jsou tyto:

- přijetí rizika – náklady na zamezení riziku jsou příliš velké nebo riziko příliš malé
- neprovádění riskantní činnosti
- odstranění hrozby
- snížení zranitelnosti IS
- instalace detekčních mechanismů
- vytvoření prostředků, které zajistí zotavení IS po incidentu

Definice bezpečnostní politiky IS

Bezpečnostní politika IS by měla přesně definovat oblasti, ve kterých budou aplikována bezpečnostní opatření. Ze všech možných oblastí (které budou uvedeny dále) bereme v úvahu pouze ty, které jsou pro daný IS důležité a ekonomicky účelné (což měla ukázat předcházející fáze ohodnocení rizika). Bezpečnostní opatření se dělí na fyzická, personál-

ní, procedurální, dokumentační a technická. Nyní uvedeme pro každou oblast několik příkladů:

Fyzická bezpečnostní opatření

- kontrola přístupu do budov a místností
- ochrana proti požáru, záplavě a teroristickému útoku
- bezpečnostní vybavení nábytkem

Personální bezpečnostní opatření

- programy bezpečnostního školení pro personál
- dodržování bezpečnosti práce
- zabránění zneužití zařízení
- školení a vzdělávání personálu
- havarijní plány (např. požární)
- právní otázky ochrany dat

Procedurální bezpečnostní opatření

- definice osobní zodpovědnosti za bezpečnost
- zálohování dat
- externí zálohování dat
- plánování mimořádných událostí
- údržba programového a technického vybavení
- bezpečnostní kontroly a inspekce
- havarijní smlouvy a kontrakty
- kontrola externích datových spojů
- péče o datová média
- průběžná analýza rizika
- vypracovávání zpráv o incidentech
- autorizace přístupových práv k informacím
- sledování přístupů k datům

Dokumentační bezpečnostní opatření

- klasifikace důvěrnosti a důležitosti dat

- evidence vlastníků dat
- dokumentace uložení dat na médiích

Technická bezpečnostní opatření

- kontrola přístupových práv
- technické standardy bezpečnosti
- testování programového vybavení
- správný návrh architektury IS
- inovace programového vybavení IS
- formální metody zajištění bezpečnosti IS
- správný návrh architektury telekomunikací

Stanovení a provádění bezpečnostních opatření

Po správné formulaci bezpečnostní politiky organizace je definováno, jaká bezpečnostní opatření se budou provádět. Intenzita a rozsah jednotlivých opatření se určí podle výsledků fáze ohodnocení rizika. Je však třeba dát pozor na **vyváženost** bezpečnostních opatření. Lidé pracující s výpočetní technikou mají tendenci preferovat technická a fyzická bezpečnostní opatření a ostatní druhy (personální, procedurální a dokumentační) chápou jako zbytečnou překážku vlastní práce.

Tuto skutečnost ilustruje následující statistika: Ze všech dotazovaných organizací pouze 55 % uvedlo, že má formulovanou bezpečnostní politiku. V tabulce je uveden druh bezpečnostního opatření a u něj procentuální zastoupení organizací, které aplikují tento druh bezpečnostního opatření, přičemž jsou brány v úvahu pouze ty organizace, které mají formulovánu bezpečnostní politiku.

Procento organizací, aplikujících jednotlivá bezpečnostní opatření	
Zálohování dat	96 %
Definice přístupových práv k systému	93 %
Kontrola vstupu osob do budov	71 %
Fyzická ochrana (zámky, stráže)	71 %
Zvláštní uložení cenných dat	68 %
Architektura IS navrhovaná s ohledem na bezpečnost	61 %
Osobní kontroly	51 %
Definice zodpovědnosti za bezpečnost	46 %

Z těchto čísel je zřejmé, že u většiny firem jsou bezpečnostní opatření nevyvážená, a to hlavně na úkor personálních opatření. Nelze kategoricky stanovit, jaký má být podíl

jednotlivých druhů bezpečnostních opatření; v literatuře se pouze uvádí pravidlo, podle kterého by 80 % bezpečnostních opatření mělo být netechnického rázu a pouze 20 % technických.

Implementace bezpečnostních opatření v počítačových sítích

Je třeba si uvědomit, že absolutně zabezpečený systém nelze vybudovat už jen z důvodu např. rozdílně chápané jurisdiktiky v různých zemích. Hovoříme-li proto o důvěryhodném systému, rozumíme tím systém, za který můžeme poskytnout záruku za plnění bezpečnostních zásad vždy v jisté oblasti (řízení technologických procesů, správa obecních úřadů apod.).

Implementace bezpečnostních opatření

V souladu se zásadami hierarchické výstavby informačních systémů je vhodné, aby informační systém poskytoval pro implementaci bezpečnostních opatření v nižších vrstvách vhodnou škálu služeb. Pro každý objekt tak lze zavést bezpečnostní mechanismus, který dlouhodobě prokazuje přístup k objektu jednotlivými aktivními činiteli, ať již byl tento přístup realizován vydáním příkazu či jinak.

Při prověřování každého individuálního přístupu musí být možno prokázat totožnost aktivního činitele, který daný přístup vyvolal a tam, kde je to nutné, umožnit neodmítnutelnost zodpovědnosti např. za vydání příkazu formou digitálního podpisu apod.

Před vykonáním požadovaného přístupu je třeba prověřit zplnomocnění identifikovaného žadatele. Pouze zplnomocněný původce děje neporuší zásady výstavby důvěryhodného systému.

Pro individuální prokazování přístupu k jednotlivým objektům je třeba poskytovat službu protokolování. Protokolovací službu lze využívat jak dynamicky, tak i staticky. Zatímco dynamické protokolování slouží spíše pro vyhledávání příčin anomálií, statické protokolování podporuje celkovou bezpečnost. Otázkou ovšem je, jak zpracovávat protokolovaná data. Jsou činěny pokusy jak s použitím expertních systémů, tak i s použitím statistických nástrojů.

Jak se vytváří bezpečný systém?

Nejprve je třeba stanovit co se bude chápat pod pojmem bezpečnost, tj. které bezpečnostní služby musí navrhovaný bezpečný informační systém plnit. Tato projektová fáze končí specifikací bezpečného systému. Výsledkem fáze specifikace je stanovení bezpečnostního modelu a služeb použitých pro jeho implementaci.

Po fázi specifikace následuje fáze implementace bezpečného systému, ve které se řeší jak dosáhnout splnění specifikovaných vlastností a tato fáze by měla končit ověřením, že tomu tak skutečně je. Pro implementaci bezpečného distribuovaného systému lze s výho-

dou použít hierarchický model, podle kterého systém sestává z hierarchicky uspořádaných komponent, kde každou komponentu můžeme chápat opět jako samostatně specifikovaný a implementovaný systém. Architekturu bezpečného systému podle představ ISO specifikuje ISO norma 74982, Security Architecture.

Aby byl výsledný systém bezpečný, musí být důvěryhodná každá jeho komponenta. Důvěryhodné jádro systému musí být udržována v co nejmenším rozsahu, každá jeho komponenta musí být pravidelně prověřována zda lze za její činnost dát záruku (nedošlo-li k poruše hardwaru či softwaru, je-li dodržováno zplnomocnění, nezanedbává se prokazování autorství apod.).

Důvěryhodné jádro distribovaného bezpečného systému přitom obsahuje jednak výpočetní komponenty (hardware, operační systém a aplikační systémy) a jednak komunikační komponenty. Implementaci bezpečnostních zásad v obou typech komponent si probereme samostatně.

Fáze specifikace stanovení bezpečnostních zásad

Nejrozvinutější jsou metodiky utajování, naopak prakticky nic není doposud učiněno v oblasti rozvoje metodik udržování pohotovosti z hlediska bezpečnosti. Metodiky stanovení zbývajících bezpečnostních zásad (neporušitelnost, prokazatelnost přístupu apod.) jsou v současnosti předmětem intenzívních výzkumů. Zajištění neporušitelnosti konzistentní informace je v podstatě ochranou proti podvodům.

Fáze specifikace stanovení bezpečnostního modelu

Pro zvolenou bezpečnostní zásadu utajení stanovíme bezpečnostní model řízeného toku informací. Každému objektu se přiřadí bezpečnostní úroveň a data z objektu bezpečnostní úrovně l mohou ovlivňovat data z objektu s bezpečnostní úrovní k jen když l=>k. Takový model je mnohdy idealistický, v reálných podmínkách jsou často potřebné postupy porušující takto obecně stanovené zásady.

Pro plnění takových služeb jako přidělování prostředků, zavádění nových uživatelů apod. je vhodné použít doplňkový model, model řízeného přístupu. Pravidla řízeného přístupu lze vyjádřit buďto jako seznam oprávnění přidělený každému subjektu nebo jako seznam přístupových práv přidělený ke každému objektu. V mnoha systémech je použita kombinace obou forem. Použití modelu řízeného přístupu usnadňuje implementaci prokazatelnosti přístupu subjektu k objektu. O problému manipulace s odpovídajícím protokolárním zápisem jsme se již zmínili.

Použití modelu řízeného přístupu zákonitě vede k použití referenčních monitorů. Referenční monitor objektu povolí přístup k objektu tehdy, když zjistí, po prokázání totožnosti žádajícího subjektu, že operace je přípustná, že systém (uzel sítě apod.), ve kterém požadavek vznikl, je náležitě zplnomocněn ke generování takového požadavku a že bezpečnostní zásady na obou stranách jsou vzájemně kompatibilní. V současných

distribuovaných systémech plní funkci referenčních monitorů obvykle operační systémy a velké podsystémy, resp. servery, které svoje objekty spravují přímo. Lze očekávat, že v budoucích distribuovaných systémech bude plnit funkci referenčního monitoru pro své subjekty a objekty každý aplikační systém. Připuštění existence složených objektů vede k myšlence hierarchie referenčních monitorů.

Fáze implementace služby pro implementaci modelu

– Prokazování totožnosti

Důvěryhodný systém především potřebuje službu, která mu jednoznačně identifikuje toho, kdo např. vydal příkaz k převodu bankovního konta apod., tzn. službu prokazování totožnosti autora příkazu (požadavku, ...). S její implementací úzce souvisí rozhodnutí o použitém identifikačním systému. Identifikační systém musí jednak zajistit, aby každý aktivní element měl jednoznačné jméno, a jednak musí být schopen poskytnout informaci, které další aktivní elementy je třeba prověřit, aby se zjistil autor příkazu, který byl zadán pojmenovaným aktivním činitelem.

Větší problém, než jednoznačné pojmenování, je prověřování, zda jsou všichni mezilehlí aktivní činitelé, odhalení při prokazování totožnosti, vůbec zplnomocněni takovou funkci plnit. Pokud nejsou, pak nemohou ani vystupovat jako identifikovatelní jedinci.

Pro prokázání totožnosti autora příkazu vydaného lokálním aktivním činitelem se snadno použije lokální systém ovládání souborů, pro prokázání totožnosti autora příkazu vydaného vzdáleným aktivním činitelem připojeným přes síť lze použít kryptografických metod.

Prokazování totožnosti je v současné době v relativně pokročilém stádiu normalizace jak v rámci doporučení CCITT, tak i norem ISO (ISO 95948, X.509: The Directory Authentication Framework).

– Prověřování zplnomocnění

Poté, co je známo, kdo vydal příkaz (dotaz apod.), může referenční monitor přikročit k prověření, zda takový aktivní činitel byl k tomu zplnomocněn. K prověření zplnomocnění se běžně používají seznamy přístupových práv. Aktivní činitelé mohou být seskupování do skupin a zplnomocnění může obdržet i taková skupina jako celek. Služba prověření zplnomocnění ovšem musí ověřit, zda konrétní jednotlivec žádající o přístup k objektu je členem takové skupiny.

– Implementace služeb komunikační bezpečnosti

Bezpečně komunikovat znamená vědět kdo informaci posílá (příjemce musí mít k dispozici službu prokazování totožnosti) a kdo informaci může číst (odesílatel ji způsobem smluveným s možnými příjemci utajuje). Cestu mezi dvěma nebo více komunikujícími partnery nazýváme kanál, pokud tato cesta poskytuje bezpečnou komunikaci, nazýváme ji bezpečný kanál. Bezpečný kanál nemusí nutně pracovat v reálném čase.

Pokud se zabezpečení kanálu implementuje pomocí prostředků kryptografie, pak jeho bezpečnost nezávisí na bezpečnosti užitých fyzických komunikačních prostředků a mezilehlých uzlů. Princip kryptografie spočívá v tom, že kódovací služba odesílatele vypočítá ze srozumitelného textu jiná data šifrovaný text, který se skutečně vyšle. Dekódovací služba na straně příjemce spočítá ze šifrovaného textu původní srozumitelný text. V dobrém kryptografickém systému jsou pravidla kódování a dekódování klíč jednoduchá, ovšem odvození šifrovaného textu ze srozumitelného textu a naopak je bez jejich znalosti prakticky nemožné, a to i při částečné znalosti odpovídajících si částí srozumitelného a šifrovaného textu. V současné době se používají prakticky dva typy kryptografických systémů.

Symetrický bezpečný kanál

Pro kódování i dekódování používá stejný klíč. Příkladem jeho řešení je americká norma DES. Kanál DES umožňuje vysílání rychlostí až 15 Mb/s a očekává se i rychlost 1 Gb/s. Znalost klíče je prokázáním totožnosti odesílatele a tím pádem i prostředkem zabezpečujícím neporušitelnost. Problémem, jehož řada více či méně efektivních řešení je ovšem známa, je distribuce klíče zúčastněným stranám.

Asymetrický bezpečný kanál

Pro kódování a dekódování používá různé klíče. Příkladem jeho řešení může být aplikace algoritmu RSA, [RSA78], který používá jednak utajený privátní klíč a jednak veřejně známý klíč. Jestliže odesílatel zprávu zakóduje svým privátním klíčem, kanál zabezpečuje plnění služby prokazování totožnosti. Při kódování vysílané zprávy veřejným klíčem příjemce se zpráva utajuje. Jediná kódovací operace asymetrického bezpečného kanálu neumožňuje plnit obě služby najednou. Každý aktivní činitel vlastní tedy dvojici (privátní klíč, veřejný klíč); privátní klíč si utají, veřejný zveřejní (někde v adresáři, poskytne ho na žádost apod.). Kódování algoritmem RSA je relativně pomalé, asi 1 Kb/s.

Podpisování

Jestliže příjemci jsou schopni přijmout zprávu „relativně dlouho" po jejím odvysílání a navíc třeba ani nejsou při vysílání známi odesílateli, lze službu identifikovatelnosti autora (prokazování totožnosti) plnit pomocí digitálního podpisování. Digitální podpis musí umožnit jednoduché prokázání totožnosti autora kýmkoli a musí být vytvořitelný pouze autorem. Při použití asymetrického bezpečného kanálu odesílatel vytvoří svůj podpis zakódováním např. kontrolního součtu vysílané zprávy svým privátním klíčem a takto vzniklý podpis pošle společně se srozumitelným textem zprávy. Příjemce, který zná veřejný klíč odesílatele, si může podpis ověřit přepočítáním kontrolního součtu a srovnáním s dekódovanou hodnotou podpisu. Má-li se použít jak pro prokazování identity odesilatele tak i pro utajování asymetrický, kanál musí odesilatel zprávu nejprve podepsat – zašifrovat svým privátním klíčem a výsledek zašifrovat příjemcovým veřejným klíčem. Příjemce dešifrováním přijaté zprávy pomocí svého privátního klíče získá

odesilatelův podpis, a dešifrováním tohoto podpisu veřejným klíčem odesílatele získá původní zprávu Z. Podpis příjemce vyrobit neumí, nezná privátní klíč odesílatele.

Prokazování totožnosti

Nejobecnější prokázání totožnosti, např. při zřizování bezpečného kanálu mezi klientem a serverem, je použití hesla; heslo však neposkytuje bezpečný kanál. Bitový obraz hesla v kanálu Ethernetovského či Token–Ring typu může zjistit prakticky kdokoli. Typické řešení tohoto problému spočívá v použití výzvy a odpovědi na ni na asymetrickém bezpečném kanálu.

Pamatovat si v každém aktivním činiteli veřejné klíče všech ostatních aktivních činitelů by bylo nepraktické. Problém lze řešit zavedením prověřeného síťového notáře, který udržuje bázi veřejných klíčů celého systému nebo alespoň jím obhospodařované části systému a na požádání sdělí po dodání jména vyzývaného aktivního činitele jeho veřejný klíč. Veřejný klíč síťového notáře je všeobecně znám. Na této myšlence je konečně postaveno i doporučení CCITT X.509.

Zvláštním problémem je prokazování totožnosti lidské obsluhy. Tradiční udání hesla při přihlašování se za bezpečné považovat nedá. Již v současnosti se uvádí do používání prokazování totožnosti otiskem prstů, rukopisem, resp. analýzou vzorku na sítnici oka. Použitím „smart" karet se problém prokázání totožnosti mezi člověkem a počítačem převede na problém komunikace mezi počítači.

Delegování a odebírání přístupových práv

Když v bezpečném systému uživatel prokáže svoji totožnost pracovní stanici, deleguje na ni právo vystupovat v jeho zastoupení. Odebrat jednou stanovená přístupová práva není jednoduchý proces, poněvadž komunikační podsystém si může řadu informací pamatovat dlouhodobě na mnoha místech (cache) a dále je třeba mžikově informovat o změně přístupových práv všechny systémy, které se těmito přístupovými právy řídily. Zrušení vlastnosti „cache" vede k prudkému snížení propustnosti a dále je nutno vyřešit, kdo má vědět, kdo všechno měněnou definici přístupových práv používá. Proto je třeba se smířit s tím, že se odebrání přístupových práv prostě projeví někdy později (při příštím otevření souboru, otevření relace, časovém výpadku apod.).

Závěr

Tento příspěvek je pouze přehledovým úvodem do problematiky bezpečnosti IS. Mnohé otázky jsou zde pouze nastíněny, mnohé problémy pouze vyjmenovány. Cílem není poskytnout návod, jak budovat bezpečnostní politiku IS, ale upozornit čtenáře na existenci a závažnost této problematiky.

Literatura

[1] Guidelines for Directing Information Technology Security, CCTA Security and Infrastructure Group, September 1991, ISBN 0 946683 3 6

[2] An Overview of CRAMM, HM Treasury, IT Security and Privacy Branch, 1990

[3] Gildersleeves, P. B.: The Security of IS – the Challenge to Management, Open Symposium for European Government, 9–21 October 1988, Brussels

[4] Rivest, R., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public key cryptosystems, CACM 21, 2 (Feb.), 120–126.

Autoři: Hanáček Petr
Katedra informatiky a výpočetní techniky, FE VUT
Božetěchova 2
612 66, Brno 12
tel: 05–746 111/kl. 231
e–mail: hanacek@dcse.fee.vutbr.cs

Staudek Jan
Katedra informatiky a výpočetní techniky, FE VUT
Božetěchova 2
612 66, Brno 12
tel: 05–746 111/kl. 242
e–mail: staudek@dcse.fee.vutbr.cs