BEZPEČNOST PODNIKOVÝCH INFORMAČNÍCH SYSTÉMŮ

Roman Jašek

Abstrakt:
S rozvojem informačních technologií vzrůstají i možnosti jejich zneužívání. Příspěvek představuje jeden z pohledů na bezpečnost informačních systémů. Ukazuje analogické principy jak pro podnik, tak pro státní instituci. Je charakterizováno pojetí bezpečnostních funkcí a mechanizmů, bezpečnostní politika, hierarchická struktura bezpečnostní politiky, vnější bezpečnost, vnitřní bezpečnost, proces výstavby bezpečnosti informačního systému a naplňování požadavků integrity dat.

Klíčová slova: *vnější bezpečnost, vnitřní bezpečnost, komunikační bezpečnost, bezpečnost informací*

1. Úvodem

S bouřlivým rozvojem informačních technologií vzrůstají i možnosti jejich zneužívání. Toto samozřejmě vede k nutnosti hlouběji a detailněji se zabývat otázkami bezpečnosti. Ty se poprvé začaly objevovat na konci sedmdesátých let ve spojení s armádními aktivitami, které souvisely s rozsáhlejším zaváděním nových systémů na bázi výpočetní techniky. V této době byla bezpečnost zužována pouze na zajištění důvěrnosti provozovaných výpočetních systémů a v nich shromážděných údajů. Úvodní aktivity pak vyvrcholily vypracováním prvních kritérií pro posuzování bezpečnostních charakteristik výpočetních systémů TCSEC [6] a tato kritéria (původně určená pro vojenské prostředí) se stala po schválení v roce 1985 obecně uznávaným standardem bezpečnosti i mimo toto vojenské prostředí. Širší využívání a globální propojování výpočetní techniky spojené s nárůstem objemu dat vedlo koncem osmdesátých let k přesnějšímu vyprofilování potřeb bezpečnosti. To se odrazilo ve vzniku zcela nového vědního oboru, který je nazýván počítačová bezpečnost (Computer Security). Někdy je problematika chápana ještě ve větší šířce a mluví se o bezpečnosti informací (Information Security), pro kterou se vžila zkratka INFOSEC.

K eliminaci zneužívání je nutné, aby bezpečné informační systémy byly schopné čelit útokům narušitelů. Většina teoretiků i praktiků, kteří se zabývají bezpečností informací je přesvědčena, že oblast jejich zájmu je možné rozdělit do čtyř **hlavních cílů ochrany**, kterými jsou důvěrnost, integrita, dostupnost a odpovědnost [1][7][5][2]. Tyto cíle mají následující význam:

Důvěrnost je označením cíle, který v informačním systému chrání informace před jejich prozrazením a tím brání v působení následků, které jsou spojeny s neautorizovaným získáním spravovaných dat.

Integrita je cíl, který zajišťuje podmínky, za kterých data mají vždy správnou fyzickou i logickou podobu, náležitý sémantický smysl a autorizovaní uživatelé včetně všech zdrojů systému provádějí nad daty pouze korektní operace.

Dostupnost zajišťuje, že informace a potřebné systémové zdroje určené pro jejich zpracování jsou pro uživatele neustále dosažitelné resp. jejich dosažitelnost odpovídá stanoveným pravidlům a systém je schopen čelit neautorizovanému oslabení funkčnosti.

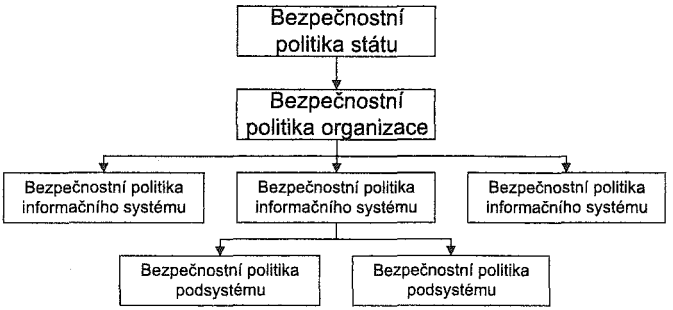
Odpovědnost je schopnost informačního systému, která vyjadřuje možnosti evidence událostí spojených s činností jednotlivých uživatelů. Tak je možné zpětně vysledovat kdo je za provedené činnosti zodpovědný.

K zabezpečení výpočetních systémů a prosazení těchto základních cílů je vytvářeno zvláštní uspořádání hardwarového, softwarového a firmwarového vybavení, tzv. důvěryhodná výpočetní základna.

Definice:

Důvěryhodná výpočetní základna (v některých překladech je používán též termín důvěryhodná výpočetní báze Trusted Computing Base - TCB [9][10]) je část systémového hardware, firmware a software, která je přímo určená pro

Obr. 1: Hierarchická struktura bezpečnostní politiky



Zdroj: vlastní

prosazování bezpečnostních pravidel a funkcí produktu nebo systému. Jedná se o množinu všech funkcí, mechanizmů a složek systému, které mají rozhodující nebo významnou souvislost s dosažením bezpečnostních cílů [6].

2. Pojetí bezpečnostních funkcí a mechanizmů

Analýzou bezpečnosti informačního systému lze požadavky zajišťující bezpečný provoz rozdělit do tří základních kategorií (jiné termíny používá dokument [9], který má označení technická bezpečnost pro bezpečnost vnitřní a netechnická bezpečnost pro bezpečnost vnější), které v dalších kapitolách rozebereme. Jde o tyto kategorie:

- **Bezpečnostní politika,**
- **Vnější bezpečnost,**
- **Vnitřní bezpečnost.**

2.1 Bezpečnostní politika

Bezpečnostní politika (Security Policy) je soubor zákonů, předpisů, pravidel, principů a praktik, které určují způsob správy, ochrany a distribuce citlivých informací a jiných zdrojů. Jinými slovy je vyjádřením záměru, jakými způsoby budou řízeny a chráněny všechny činnosti, které jsou spojeny s citlivou informací od jejího získání přes ukládání až po distribuci. Tyto činnosti a způsoby práce musí být přesně a jednoznačně definovány [6][8]. **Bezpečnostní politika popisuje aplikace standardů, které jsou využívány na systémech uvnitř organizace a definuje bezpečnost ve vztazích mezi organizací a ostatním světem.** Tím bezpečnostní politika vytváří legislativní rámec, od kterého se bezpečnost informačních systémů odvíjí, či kterému je bezpečnost systémů podřizována [12]. Takto pojatou bezpečnostní politiku lze vyjádřit ve formě hierarchické struktury, která je vidět na obrázku (Obr.1)

Vrcholem struktury v obecné rovině je **bezpečnostní politika státu,** která je vyjádřena zákonnými normami. V případě České republiky se jedná *o zákon č.148/1998 Sb., O ochraně utajovaných skutečností.* Je moderní zákonnou normou, které je v souladu se soudobými evropskými zvyklostmi. Dalšími zákony, který je nutné respektovat při tvorbě informačních systémů je *zákon č. 101/2000 Sb., o ochraně osobních údajů, zákon č. 513/1991 Sb., obchodní zákoník, zákon č. 21/1992 Sb., o bankách* apod. (vše samozřejmě ve znění pozdějších předpisů). Důležitý pro bezpečnostní politiku našeho státu je *Bezpečnostní standard státního informačního systému.*

Všechny tyto normy jsou dále rozpracovány jednotlivými částmi například státní správy a vznikají bezpečnostní politiky jednotlivých správ či samostatných organizačních celků (např. armádní bezpečnostní politika). V případě resortu Ministerstva obrany a Armády České republiky se jedná hlavně o dokumenty, které jsou vydávány Oddělením bezpečnosti informací MO. V případě státní správy jsou metodické materiály s dokumenty pro zabezpečování produktů a systémů budovaných na bázi informačních technologií k dispozici na portálu Ministerstva informatiky (http://micr.trustica.cz/scripts/detail.php?id=479). Z výše uvedeného je tedy zřejmé, že na problematiku bezpečnosti je třeba se dívat komplexně. Tedy **firemní a podniková bezpečnost musí**

přijímat stejná kriteria, jako státní sektor a naopak.

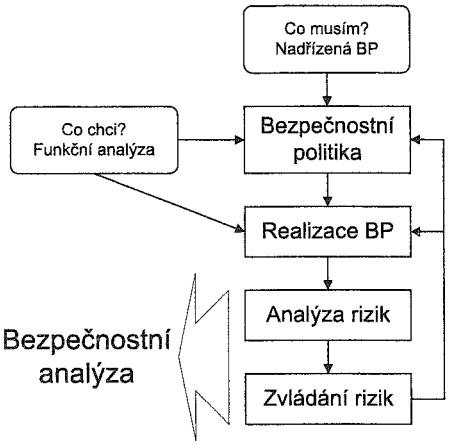
Významnou podporu pro budování informační bezpečnosti právě malých a středních firem poskytla v podobě metodické příručky s globální platností také společnost Microsoft. Příručka s názvem „Průvodce zabezpečením pro malé organizace" včetně dalších materiálů je k dispozici na adrese „http://www.microsoft.com/cze/security/business/default.mspx". Jde o hodnotný informační materiál pro organizace všech velikostí.

Další konkretizace musí být uplatněna při formulaci bezpečnostní politiky jednotlivých informačních systémů. U rozsáhlejších systémů může být ještě rozpracována i ve formě bezpečnostní politiky subsystémů.

(Security Analysis), je proces, kterým se zjišťuje míra ohrožení bezpečnosti systému a kterým se vybírají nejvhodnější protiopatření, která zajistí potřebnou bezpečnost systému. Pozici bezpečnostní analýzy, její vazby na bezpečnostní politikou a na způsoby její realizace v informačním systému zobrazuje Obr.2.

V procesu bezpečnostní analýzy se rozlišují dvě základní etapy. První se nazývá **analýza rizik** (Risk Analysis) a slouží k odhadu ztrát, které mohou vzniknout působením hrozeb na systém, a dává přehled o nebezpečnosti jednotlivých hrozeb a zranitelnostech hodnoceného systému. Reakcí na zjištěná rizika a jejich řešením se zabývá druhá etapa nazvaná **zvládání rizik** (Risk Management). V této etapě se vybírají op-

Obr. 2: Proces výstavby bezpečnosti IS



Zdroj: vlastní

Hlavním úkolem při prosazování bezpečnosti informací je vybrat a implementovat protiopatření tak, aby bylo omezováno působení hrozeb (hrozba - Threat je akce nebo událost, která může ohrozit bezpečnost) a technických i netechnických rizik (riziko je pravděpodobnost, s jakou určitá hrozba využije zranitelnost systému. informačního systému). Aby bylo možné trvale udržet potřebnou úroveň bezpečnosti systému, s ohledem na co nejvyšší míru efektivnosti vynakládaných prostředků a potřebné pokrytí rizik, je nezbytné objektivně přizpůsobovat bezpečnostní požadavky. Proces optimalizace bezpečnostních opatření, který se nazývá **bezpečnostní analýza** timální protiopatření, která vedou k eliminaci rizik stanovených při analýze rizik [11]. Zvládání rizik představuje celkový souhrn aktivit, jejichž účelem je vyřešení problematiky bezpečnosti s maximální efektivností.

Proces bezpečnostní analýzy je možné chápat i opačně v tom směru, že každá bezpečnostní politika by měla být podložena výsledky odpovídající bezpečnostní analýzy. Prakticky se vždy jedná o iterační proces, který je navíc ovlivňován řadou dalších faktorů daných životním cyklem informačního systému. Výsledkem bývá bezpečná realizace informačního systému doprovázená dodržováním zásad bezpečné implementace a bezpečného vy-

užití, které jsou vyjádřeny bezpečnostní politikou.

Vzhledem k dnešní velmi vysoké složitosti informačních systému, je provedení kvalitní bezpečnostní analýzy značně složitý a náročný proces. Z těchto důvodů se objevují snahy o podstatné zjednodušení, které se dnes odráží ve formě **základní úrovně bezpečnosti** (Base Line Security). Ta vyjadřuje minimální požadavky, které jsou nezbytné pro splnění základních bezpečnostních funkcí navrhovaného informačního systému. Protože základní úroveň bezpečnosti je závislá na obecnějším typickém nasazení, určení a umístění, je pro řadu běžných systémů obdobná a bývá v odborných materiálech popsána úzkou množinou typizovaných profilů bezpečnosti. Nespornou výhodou se tak stává realizace již ověřeného komplexu bezpečnostních opatření. Teprve po nasazení jsou na základě vzniklých zkušeností prováděny hlubší bezpečnostní analýzy, které jsou podkladem pro další optimalizaci bezpečnostních opatření systému, jež reagují na provozem zjištěné nedostatky. Tím je bezpečnostní analýza významně zjednodušena a příliš nezpomaluje budování informačního systému, protože je z velké části přenesena do období využívání informačního systému. Tento posun s sebou přináší i podstatné zvýšení objektivnosti a efektivnosti závěrů samotné bezpečnostní analýzy a její úzké svázání se skutečným životem systému.

2.2 Vnější bezpečnost

Pro zajištění přehlednosti bezpečnostní politiky a vlastně celé bezpečnosti informací jsou bezpečnostní opatření rozdělena na dvě hlavní části, které vyplývají z rozlišení vnitřních a vnějších hrozeb systému, na které je potřeba reagovat [12]. První částí je vnější bezpečnost, která pokrývá hrozby, na které nemůže přímo reagovat automatizovaná technika informačního systému. Druhou částí je vnitřní bezpečnost, která pokrývá bezpečnostní opatření zajišťovaná vlastní výpočetní technikou resp. její TCB[13].

Vnější bezpečnosti se týkají všechna opatření, která jsou realizována mimo systém informačních technologií. Vnější bezpečnost můžeme rozdělit podle oblasti působnosti do tří částí [12] [15]:

- fyzická bezpečnost;
- personální bezpečnost;
- procedurální bezpečnost;
- komunikační bezpečnost.

Fyzická bezpečnost

Fyzická bezpečnost (Physical Security) zajišťuje ochranu informačních systémů technickými prostředky před působením přírodních živlů, sabotáží, poruch apod. Lze ji dělit na dvě části. První, klasická, se soustřeďuje na ostrahu prostorů s důležitými informačními zdroji před vniknutím nepovolaných osob (fyzické zábrany vstupu, ostraha prostoru apod.). Patří sem i prostředky pro snížení rizika nebezpečí vzniku a rozsahu škod, jež je spojeno fyzikálním působením okolního prostředí (požární signalizace, klimatizace aj.).

Do druhé skupiny patří prostředky k ochraně automatizovaných pracovišť informačních systémů. Jde o technická opatření vedoucí k omezování elektromagnetického vyzařování (pasivní či aktivní elektromagnetická ochrana). Pro prostředky ochrany, které slouží k omezení elektromagnetického vyzařování, a jejich technické normativy se často používá označení **TEMPEST**.

Mezi další prvky fyzické ochrany informačních systémů se zařazují prostředky ochrany komunikačních kanálů (šifrová ochrana), prostředky pro zálohování síťového napájení (zdroje nepřetržitého napájení) atd..

Personální bezpečnost

Personální bezpečnost (Personnel Security) zahrnuje všechny techniky, které využívá organizace při rozhodování o tom, kdo bude informační systém využívat, komu bude svěřena zodpovědnost za informační systém organizace atd. Většina organizací má vypracovány postupy, na základě kterých jsou jednotlivým uživatelům přidělována práva pro přístup k důvěrným informacím.

Do personální bezpečnosti jsou zahrnuty všechny techniky, které organizace využívá pro zajištění důvěryhodnosti osob, které využívají informační systém. Jde o výběr pouze takových osob, které poskytují dostatečné záruky osobní loajality a kázně. Dále organizace musí vybrané osoby dostatečně poučit a přesně definovat jejich práva, povinnosti a odpovědnost v systému. Další složkou této oblasti je finanční ohodnocení osob a stanovení personálních postihů při porušování stanovených pravidel.

Procedurální bezpečnost

Procedurální bezpečnost (Procedural Security) určuje způsoby a postupy, které je nutné dodržovat při práci s informacemi a s informačním systémem. Pro bezpečný provoz je nutné vytvořit postupy

pro regulaci a evidenci pohybu osob, vymezení přístupové doby a pravidel pro využívání služeb informačního systému, způsob obsluhy fyzických zařízení (práce s výstupními sestavami a pravidla pro obsluhu kryptosystémů), evidence materiálu apod.. Velmi důležitou částí procedurální bezpečnosti je stanovení postupů při odhalení, nebo signalizaci pokusů o narušení bezpečnosti systému a pro případy vzniku živelných katastrof. Někdy je místo termínu procedurální použit termín administrativní, či režimová bezpečnost.

Komunikační bezpečnost

Bezpečnost aktiv a především dat a informací, se stává stále více diskutovaným problémem současných organizací. Investice do oblasti bezpečnosti se zvyšují, a proto je třeba je správně, účelně a účinně vynaložit.

Komunikační bezpečnost může být proto dnes tvořena také dvěma paralelními, ale jednu bezpečnost tvořícími pohledy (bezpečnost je totiž jen jedna). První představuje ochranu informačních systémů a dat zpracovávaných na počítačích technickými a programovými prostředky a přenášených mezi nimi, druhý je zaměřen na ochranu před působením lidského faktoru a na oblast ohroženou sociálním inženýrstvím (útoky za použití sociotechnické manipulace). K eliminaci těchto rizik zavádíme následující procesy:

- Autentizace a autorizace - jednoznačné ověření subjektu vstupujícího do informačního systému a ověření jeho přístupových práv;
- Řízení přístupu - přístup k citlivé informaci pouze určené osobě;
- Účtovatelnost - evidence procesů a činností souvisejících s IS;
- Audit - monitoring událostí a aktivit v IS;
- Bezpečné uložení a přenos dat - šifrování přenosu a ukládání dat, virtuální privátní sítě;
- Antivirová ochrana - kvalitní antivirová ochrana pracovních stanic, podnikových sítí, mailového serveru, připojení do Internetu;
- Jako nejvhodnější obrana před sociotechnickou manipulací se dnes jeví pravidelná proškolování a seznámení se se způsoby ohrožení při práci s důvěrnými informacemi doplněné modelovými tréninky situací.

2.3 Vnitřní bezpečnost

Vnitřní bezpečnost je ta část systému ochrany dat, která je realizována samotným systémem informačních technologií. Je velmi úzce spojena s bezpečností vnější a při specifikaci informačního systému je dobré najít vhodný kompromis mezi opatřeními obou částí [12]. Tato část informační bezpečnosti v sobě zahrnuje **počítačovou bezpečnost** (Computer Security), která pojímá opatření pro zajištění důvěrnosti, integrity, dostupnosti a odpovědnosti systému informačních technologií pomocí hardwarových a softwarových prvků. Počítačová bezpečnost se často označuje zkratkou **COMPUSEC**. Vzhledem ke stále těsnějšímu propojení a užší návaznosti výpočetních a komunikačních systémů lze říci, že se výrazně rozšiřuje i uplatnění **komunikační bezpečnosti** (Communication Security), která se snaží především o zajištění důvěrnosti a integrity dat při přenosu informací technickými prostředky (viz kapitola 2.2) . Komunikační bezpečnost je známa i pod zkratkou **COMSEC** a v této práci je soustředěna do části výměna dat.

Zásady vnitřní bezpečnosti lze podle jejich působnosti rozdělit do následujících oblastí: **důvěrnost, integrita, dostupnost, odpovědnost, výměna dat** a **záruky** [3]. První tři oblasti, které čelí základním ohrožením systému, je nutné doplnit o oblast odpovědnosti, která nutí každého uživatele a správce postupovat v souladu s procedurálními a dalšími závaznými předpisy. Se zvyšujícím se objemem přenášených dat a širokým uplatněním počítačových sítí vzrůstají i nároky na bezpečnost výměny dat. Poslední oblast, záruky, vyjadřuje úrovně prověření, spolehlivost a nenarušitelnost bezpečnostních vlastností TCB.

Důvěrnost

Do oblasti důvěrnosti (Confidentiality) se řadí ochranné funkce, které mají za cíl předcházet hrozbám neautorizovaného přístupu k informacím a jejich kompromitaci. Pro zvyšování důvěrnosti systému jsou realizovány funkce řídící přístup k objektům podle rolí a pravomocí uživatelů. V první řadě jde o funkce výběrového řízení přístupu a povinného řízení přístupu. Přístup může být řízen na základě dalších principů. Důležitými prostředky, které také zajišťují důvěrnost, jsou i pravidla opětovného využití objektu a eliminace skrytých kanálů, které by mohly být použity pro neautorizované toky dat, což by důvěrnost ohrozilo nepřímo.

Integrita

Prostředky, jejichž úkolem je minimalizovat v důvěryhodném systému možnosti neoprávněných změn uživatelských nebo systémových dat včetně programů a procedur, patří do dalšího důležitého úseku počítačové bezpečnosti, kterým je oblast integrity. Snižování hrozeb je zajišťováno několika typy prostředků. Prvním typem jsou prostředky pro řízení přístupu k datovým objektům. Ty jsou, podobně jako u důvěrnosti, řešeny na základě výběrového řízení přístupu a povinného řízení přístupu. U některých pohledů na bezpečnost proto dochází ke spojování obou oblastí, a tak vzniká jediná oblast nazývaná řízení přístupu. Oddělený přístup umožňuje členit služby v souladu s možným ohrožením. Dále se do oblasti integrity začleňují prostředky, které zajišťují dobrou integritu vlastního systému. Jde o prostředky, které zabezpečují integritu domén, fyzickou integritu, kontrolní body provozu, oddělení povinností a samo-testování systému.

Dostupnost

Systémy, které podporují zásady dostupnosti (Availability), musí obsahovat ochranné funkce dovolující řízení dostupnosti subjektů, objektů, systémových zdrojů a služeb. Funkce musí odrážet zásady pro prevenci, detekci a zotavení z neautorizovaného oslabení systému. S dostupností systému jsou též svázány otázky odolnosti proti poruchám, které jsou však jen jednou z částí této problematiky [3].

Odpovědnost

Aby systém mohl rozlišovat pravomoci jednotlivých uživatelů, je nutné zajistit jejich identifikaci a autentizaci, stanovit místo a dobu přihlášení do systému. Proti případnému odposlechu autentizačního hesla a narušení důležitých komunikací s TCB musí zajistit chráněnou cestu a provádět monitorování událostí prováděných uživateli (revize). Všechny tyto prostředky vytváří podmínky pro zajištění individuální odpovědnosti (Accountability) uživatelů za činnosti provedené v systému . Důležité místo při prosazování odpovědnosti zastává problematika správy systému. V poslední době se objevuje potřeba řešit i otázky soukromí a zajištění anonymity uživatelů.

Výměna dat (uvnitř systému i mimo vlastní systém)

Technickou základnu moderního informačního systému dnes netvoří jen samostatná výpočetní technika. Soudobé systémy stále více využívají možností komunikačních sítí, které se tak stávají integrální součástí systému. V prostředí počítačových sítí začínají zanikat rozdíly mezi výpočetními a komunikačními prostředky, protože je řada komunikačních funkcí (včetně bezpečnostních) realizována výpočetní technikou resp. je s ní úzce integrována. Zajištění bezpečnosti komunikačního prostředí (COMSEC) informačního systému lze realizovat bezpečnostními funkcemi autentizace komunikací, důvěrnosti komunikací a integrity komunikací [4]. Pro bezpečný provoz komunikací má klíčový význam aplikace kryptografických modulů, které jediné jsou schopné ochránit důvěrnost a integritu přenášených dat [14].

Záruky

V poslední době se ustálilo dělení záruk (Assurance) bezpečné a bezproblémové činnosti TCB do dvou částí. První se týká záruk, které musí poskytovat vývojoví pracovníci při tvorbě systému. Tyto záruky jsou nazývány vývojovými zárukami. Druhá část jsou záruky poskytované nezávislým testováním systému, které jsou nazývány hodnotitelskými zárukami [8]. **Vývojové záruky** (Development Assurance) kladou požadavky na čtyři oblasti vývoje systému, kterými jsou vývojový proces, operační podpora, vývojové prostředí a vývojové důkazy. K zajištění věrohodnosti bezpečného systému musí být uskutečněno hodnocení nezávislou organizací. **Hodnotitelské záruky** (Evaluation Assurance) se skládají z testování, vytvoření hodnotitelských posudků a vytvoření hodnotitelských analýz [6]. Pro bezpečnost informačních systémů mají oba typy záruk nezastupitelný význam, který je při návrhu a implementaci systémů značně podceňován.

3. Závěr

Bezpečnost všech druhů informačních systémů se opírá o **tři základní stavební prvky**, kterými jsou **bezpečnostní politika, vnější bezpečnost a vnitřní bezpečnost** systémů informačních technologií. Nyní je již možné označit všechny prvky za klasické, přičemž současný rozvoj hluboce ovlivňuje až poslední základní prvek bezpečnosti, kterým je bezpečnost implementovaná uvnitř informačních technologií. Tuto bezpečnost je možné rozdělit do několika částí. Některé z nich jsou již velice kvalitně jak teoreticky, tak i prakticky zvládány. To ale nelze plně

konstatovat o oblastech, které souvisí s integritou dat a nepřímo i s integritou celého systému.

Právě problematice integrity v podobě ochrany dat je v dnešní době věnována zvýšená pozornost, protože její zajištění není možné řešit na obecném základě, na rozdíl od většiny ostatních bezpečnostních funkcí. Požadavky integrity dat jsou vždy úzce spojeny s konkrétními implementacemi informačních systémů, protože funkce integrity dat musí zajistit správnost a konzistenci spravovaných dat včetně jejich vazeb na reálný svět. Je zřejmé, že absolutní prosazení integrity dat není reálné a bezpečnostní funkce se musí pokusit o minimalizaci nedostatků. Vzhledem k těmto skutečnostem se prosazení náležité míry integrity promítá do nutnosti prosazení správných a schválených postupů obhospodařování dat. **Tento stav vede k nezbytnosti přenesení části bezpečnostní problematiky přímo do tvorby vlastních aplikací, které jsou spojené s řešením konkrétního systému, a jejich důslednému prosazování funkcemi a mechanizmy řízení zpracování.**

Literatura:

[1] AMOROSO, E. G. *Fundamentals of Computer Security Technology.* Prentice Hall,1994. ISBN 13-305541-8,

[2] BENDA, R., ROSMAN, P. JUŘENČÁK, B., SODOMKA, P. *Základy informatiky.* 2. vyd. Zlín: UTB, FaME, 2003. ISBN 80-7318-142-8

[3] *The Canadian Trusted Computer Product Evaluation Criteria (version 3.0e)*, CSE, Ottawa 1993

[4] *Cryptographic Modules (version 1.0e)*, CSE, Ottawa 1993

[5] DOBDA, L. *Ochrana dat v informačních systémech.* 1. vyd. Praha: Grada, 1998.

[6] *Department of Defense Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD, December 1985

[7] GASSER, M. *Building a Secure Computer System.* 1st ed. New York: Van Nostrand Reinhold Company Inc., 1988.

[8] *Information Technology Security Evaluation Criteria (ITSEC): Provisional Harmonised Criteria*, Office for Official Publications of the European Communities, Brussels 1991

[9] *Kritéria hodnocení bezpečnosti informačních systémů (ITSEC): Prozatímní harmonizovaná kritéria*, European Communities, překlad MH ČR, Praha 1993

[10] *Návod pro hodnocení bezpečnosti v informačních technologiích (ITSEM): Prozatímní harmonizovaná metodologie*, European Communities, překlad MH ČR, Praha 1994

[11] JOHNSON, J. Z. *Risk Management - Theory and Practice.* 1st ed. New York: Trident Data Systems, TDS, 1995.

[12] RMO 01/93: *Minimální bezpečnostní standard ochrany informačních systémů a objektů*, Ministerstvo obrany, Praha 1993

[13] NOVÁK, L. Bezpečnostní funkce důvěryhodné výpočetní základny. *Bulletin AFOI*, 1995, roč. II, č. 3

[14] SHANNON, C. E. *Communication Theory of Secrecy Systém. Bell System Techn. J.*, 1949, Vol. 28, No. 4, p. 656-715.

[15] *Automated Information systems Security Guidelines*, Department of the NAVY, NAVY 1997

Mgr. Roman Jašek, Ph.D.
Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky
Ústav informatiky a statistiky
Mostní 5139
760 01 Zlín
jasek@fame.utb.cz

Doručeno redakci: 20. 4. 2005
Recenzováno: 29. 5. 2005
Schváleno k publikování: 7. 7. 2005

SUMMARY

THE SECURITY OF FIRM´S INFORMATION SYSTEMS

Roman Jašek

The security of information systems is based upon three basic building blocks, these are: the Security Policy, External Security, and Internal Security of information technology systems. It is possible to consider all elements as „classical", and their resolution in the main does not directly correspond to developments in information technologies. This development is profoundly influenced by the last of these basic elements of security, i.e. security measures implemented within an information technology. It is possible to break down this security aspect into several sub-components. Some of which have already been theoretically as well as practically dealt with. This cannot however be said in full for areas corresponding to the integrity of data and indirectly, with the integrity of the overall system. It is precisely this issue of integrity in the form of data protection that is today being devoted increased levels of attention, since it is impossible to resolve and assure it on a general basis - in contrast to the majority of other security functions. Data security integrity is always closely associated with concrete implementations of information systems, since the data integrity function has to ensure the correctness and consistency of the data being administered - including its relationship to the real world. It is clear that the absolute enforcement of data integrity is not realistic, and that security functions must attempt to minimalise any insufficiencies. In view this situation leads to the necessity for transferring part of the security problem and attendant issues directly into the creation of those applications themselves that are directly associated with the solutions designed for a concrete system, and the consistent enforcement of the functions and mechanisms of data processing management.of these facts, the enforcement of a commensurate degree of data integrity is projected onto the necessity for the enforcement of the correct and approved procedures for administering and working with data.

Key words: *Trusted Computing Base, Computer Security, Date Security, Communication Security*