BIS01 - MNG

Model 2019

Bezpečnost informačních systémů

Část 1

Základní pojmy, bezpečnostní funkce

Post 18/19

Souhrnné materiály

Ver 0.1

BIS 1

Act 2007,8
Addmat 2019

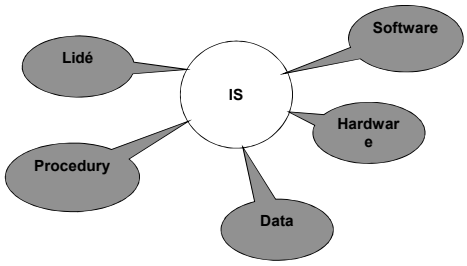
BIS 1
Bezpečnost informačních systémů

Petr Hanáček
Faculty of Information Technology
Technical University of Brno
Božetěchova 2
612 66 Brno
tel. 5 4114 1216
e-mail: hanacek@fit.vutbr.cz

Počítačová bezpečnost

- … ochrana počítačových prostředků proti náhodnému nebo úmyslnému prozrazení důvěrných dat, neoprávněné modifikaci dat nebo programů, zničení dat, software nebo hardware, a neoprávněnému zabránění v použití počítačových prostředků. Také ochrana proti jiným počítačově provedeným kriminálním aktivitám, jako je počítačem spáchaný podvod nebo vydírání. [Palmer]

Informační systém



Cíle bezpečnosti IS

- Confidentiality – důvěrnost – ochrana proti neoprávněnému prozrazení informace
- Integrity – integrita – ochrana proti neoprávněné modifikaci informace
- Availability – dostupnost – ochrana proti neoprávněnému odepření přístupu k datům nebo ke službám

Další pojmy v bezpečnosti

- Zranitelná místa (vulnerabilities) – slabiny v informačním systému, která může být využita pro provedení bezpečnostního incidentu (útoku)
- Hrozby (threats) - okolnosti, které mají potenciál způsobit bezpečnostní incident
- Aktiva (assets) – složky IS, které mají hodnotu
- Opatření (measures) – redukují pravděpodobnost vzniku bezpečnostního incidentu

Riziko

- Zranitelné místo, zkombinované s bezpečnostní hrozbou vytváří riziko.

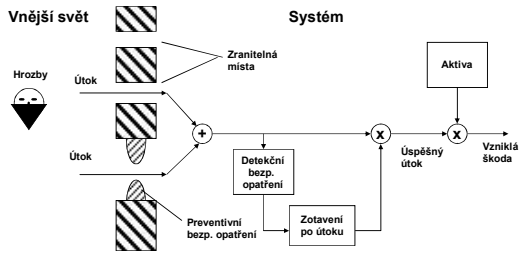
  Vulnerability + Threat → Risk

- Příklad:

  Overflow Bug
  + Hacker Knowledge & Tools & Access
  → Risk of Webserver Attack

BIS 1

Bezpečnostní incident



Aktiva

TABLE 4-1 Categorizing the Components of an Information System

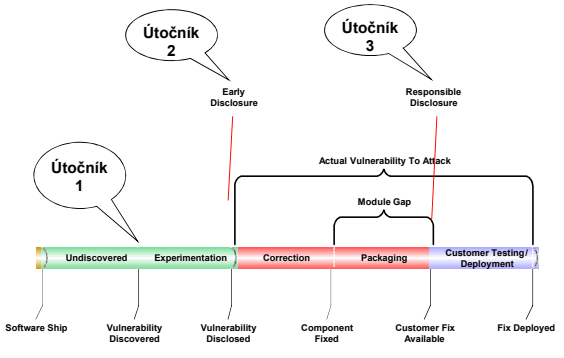
Traditional system components	SecSDLC and risk management system components	
People	Employees	Trusted employees Other staff
	Nonemployees	People at trusted organizations Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	System devices and peripherals	Systems and peripherals Security devices
	Networking components	Intranet components Internet or DMZ components

Zranitelná místa

Co je zranitelné místo?

- **Zranitelné místo (zranitelnost) je:**
  Chyba nebo slabina v návrhu, implementaci nebo provozu systému, která může být využita pro narušení bezpečnosti systému. (RFC 2828).
- **Zranitelné místo**
  - **Při návrhu – chyba architektury**
  - **Při implementaci - např. buffer overflow**
  - **Při provozu – typicky nedodržení postupů**

Chyby implementace

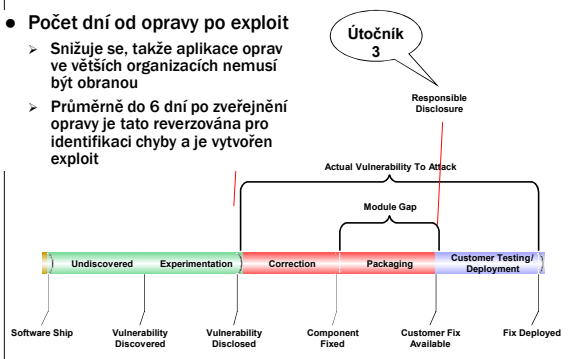


The World Today

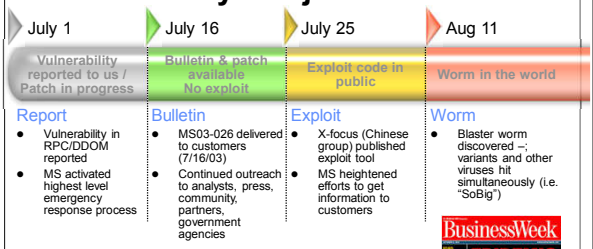
BIS 1

Chyby implementace

- Počet dní od opravy po exploit
  - Snižuje se, takže aplikace oprav ve větších organizacích nemusí být obranou
  - Průměrně do 6 dní po zveřejnění opravy je tato reverzována pro identifikaci chyby a je vytvořen exploit



Životní cyklus jednoho viru



Report
- Vulnerability in RPC/DDOM reported
- MS activated highest level emergency response process

Bulletin
- MS03-026 delivered to customers (7/16/03)
- Continued outreach to analysts, press, community, partners, government agencies

Exploit
- X-focus (Chinese group) published exploit tool
- MS heightened efforts to get information to customers

Worm
- Blaster worm discovered –; variants and other viruses hit simultaneously (i.e. "SoBig")

Blaster shows the complex interplay between security researchers, software companies, and hackers

Source: Microsoft

Hrozby

Hrozby

- **Hrozba**
  - **Hrozba je taková vlastnost prostředí, která může způsobit narušení bezpečnosti, pokud dostane příležitost.**
- **Neúmyslné (nealgoritmické, pravděpodobnostní) hrozby**
  - » **živelné události (požár, záplava, výpadek napájení)**
  - » **poruchy zařízení**
  - » **chyby v software**
  - » **selhání osob (omyly)**

Hrozby II

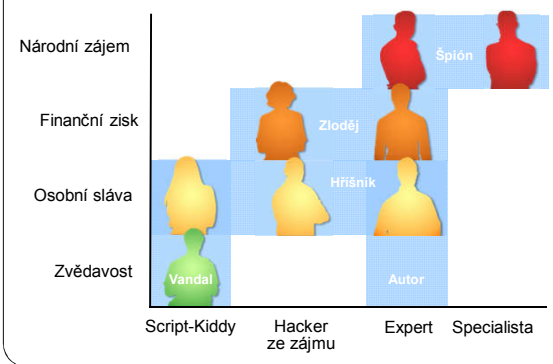
- **Úmyslné (algoritmické) hrozby**
  - **cílem nejsou data**
    - » **krádež HW a médií**
    - » **úmyslné poškození, zničení zařízení**
    - » **neoprávněné využívání HW (krádež strojového času)**
    - » **založený požár, bomba**
  - **cílem jsou data**
    - » **krádež SW**
    - » **krádež dat (prodej, zneužití dat, průmyslová špionáž)**
    - » **neoprávněná manipulace s daty (modifikace, zničení)**
  - **škodlivé programy**
    - » **viry, červi, logické bomby, trojské koně**

TABLE 4-3 Threats to Information Security

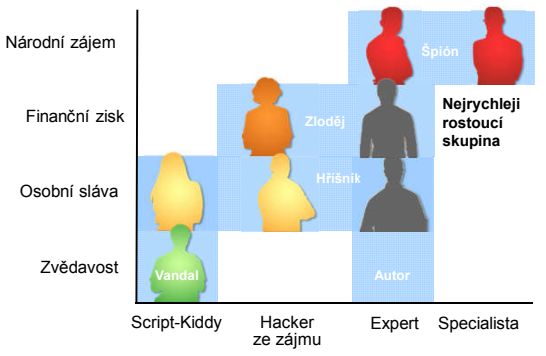
Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial of service
Forces of nature	Fire, flood, earthquake, lightning
Quality of service deviations from service providers	Power and WAN quality of service issues
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

BIS 1

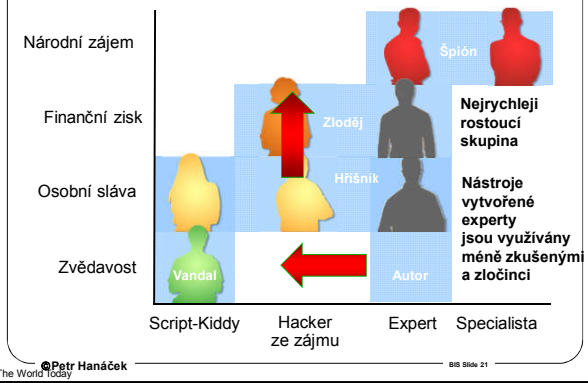
Galerie útočníků



Galerie útočníků



Galerie útočníků



Systémy Honey Pot

- Zkoumají online hrozby v síti
- Typická farma Honey Pot
  - Skupina počítačů s různými verzemi OS připojená k síti
  - Typický výsledek za týden:
    - » Počítače byly skenovány 46255 krát
    - » 4,892 přímých útoků
- Např. Windows XP bez aktualizací
  - Infikováno během 18 minut
  - Během hodiny se z něj stal "bot"

Source: StillSecure, see http://www.denverpost.com/Stories/0,1413,36~33~2735094,00.html

Malware

Co je Malware?

- „Škodlivý software“
  - Software, který je v počítačovém systému a provádí neautorizované činnosti, zpravidla bez vědomí nebo souhlasu uživatele
- Jsou to například
  - Viry
  - Trojské koně
  - Červi
  - Logické bomby
  - Žertovné programy

BIS 1

Virus

"…program který vytváří kopie sama sebe tak, aby 'infikoval' části operačního systému nebo aplikačních programů."
- Survivor's Guide to Computer Viruses, Virus Bulletin, 1993.

- Provádí replikace
  - Mezi soubory
  - Z disku na disk
- Podmínky šíření
  - široká populace počítačů se stejným operačním systémem
  - neexistence systému přístupových práv
  - rozvinutá výměna programů ve spustitelném tvaru
- Typicky vyžaduje "hostitelský program"
- Musí být spuštěn
- Může provádět destrukční činnost

Typy virů

- Boot sector viry
  - Infikuje boot record na disketě nebo disku
- Souborový infektor
  - Infikuje spustitelné programy
- Makroviry
  - Infikují dokumenty, které mohou obsahovat makra
- Scriptovací virus
  - V některém skriptovacím jazyku
- Multipartitní
  - Kombinace předchozích typů

Červ

- Samostatný program
- Nepotřebuje hostitelský program
- Replikuje se ze systému na systém
- Infikuje systémy, ne soubory
- Typicky se šíří počítačovou sítí

Internet worm

- Červ, který 2. listopadu 1988 napadl cca. 60 000 uzlů sítě Internet
  - uzly se vzpamatovaly až 5. listopadu
- Většina uzlů se odpojila od sítě
  - NASA Ames Research Center, Goddard Space Fligt Center..
- Jaká slabá místa využíval pro vniknutí
  - zadní vrátka v programu `sendmail` (příkaz *debug*)
  - programátorskou chybu v programu *fingerd*
  - slabá místa v autentizaci - *rexec* a *rsh*
- Která sezení napadal
  - se slabými hesly (žádné, přihlašovají jméno, jméno...)
  - s hesly ve slovníku s 432 slovy
  - s hesly v souboru `/usr/dict/words`
  - sezení, která důvěřovala jiným stanicím pomocí mechanismu *.rhosts*

Trojský kůň

- Program, který úmyslně provádí nějakou skrytou činnost
  - Krádež hesel
  - Mazání souborů
  - Vytváření zadních vrátek
  - Připojování přes síť k jiným počítačům
- Neprovádí replikaci

Trojský kůň - příklad

- NetBus a BackOrifice
  - Nástroj pro vzdálenou správu, Remote Administration Tools (RAT)
  - Obvykle zaslán v nějaké hře
  - Dovoluje útočníkovi získat kontrolu nad počítačem
- Subseven
  - Přichází e-mailem jako maskovaný soubor (dvojitá přípona)
  - Pomocí IRC informuje autora o úspěchu
  - Poskytuje přístup k systému a může být využit pro DDoS útoky

BIS 1

Logická bomba

- Nereplikuje se
- Část kódu, která se aktivuje na základě splnění naprogramované podmínky
- Typicky provádí nějakou destrukční činnost
- Příklad
  - Program zničí data, jakmile jeho autor zmizí z výplatní listiny

Specificky internetové typy malware

- JAVA
  - Stažený kód interpretovaný na klientském počítači
  - Ochrana pomocí „pískoviště“ - Sandbox
- ActiveX
  - Nativní spustitelný kód, stažený z internetu
  - Může provádět cokoli (žádné pískoviště)
  - Ochrana podepisováním
- …

Stále se zvyšuje rychlost šíření

Malware	*Type*	*Year*	*Time to #1*
Form	**Boot Sector**	**1990**	**3 years**
Concept	**Word Macro**	**1995**	**4 months**
Melissa	**E-mail enabled word macro**	**1999**	**4 days**
LoveLetter	**E-mail enabled script**	**2000**	**5 hours**
NIMDA	**E-mail enabled script**	**2001**	**22 minutes**

Source: ICSA/TruSecure

Techniky skrývání

- Spoofing/Stealth
  - Filtrace volání operačního systému tak, aby program byl neviditelný (rootkit)
- Šifrování
  - Šifrování kódu programu
- Polymorfismus
  - Způsobí, že virus vypadá po každé replikaci zcela jinak
  - Mutační stroje

Netradiční typy malware

- Spam
- Phishing
- Spyware
- Boty
- Root Kity

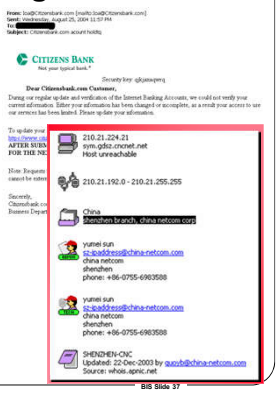
Spam

- Hromadná nevyžádaná pošta
- Nekalé obchodní praktiky
  - Direct mail
- Podvodné zvyšování provozu webu
  - Uměle vygenerované odkazy na web
- Pro podvody
  - Phishing
  - Krádež identity
  - Získávání hesel a jiných autentizačních informací

BIS 1

Phishing

- Nalákání na podvodný web
  - Více než 60% uživatelů navštíví podvodný web
- Získání dat
  - Více než 15% uživatelů poskytne nějaká osobní data
- Ekonomická ztráta
  - ~ 2% of uživatelů



Source: TRUSTe

- Vložené slajdy Phishing

Spyware

- Software který:
  - Sbírá osobní informace
  - Bez vědomí uživatele
- Zaznamenávání kláves
  - Keyloggery
- Nespolehlivé
  - Microsoft Watson
    - » Významná část havárií operačního systému je způsobena nějakým spyware

Boty a botnety

- Ekosystém botů
  - Bots
  - Botnets
  - Control channels
- První masové rozšíření červem MyDoom.A
  - MyDoom.A byl rozšířen po internetu
  - V napadených počítačích vytvořil zadní vrátka
  - Po 8 dnech útočníci skenovali počítače a hledali tato zadní vrátka
  - Nainstalovali Trojský kůň Mitglieder
  - Pak použily tyto stroje jako Boty
  - Využití pro přeposílání spamu

Příklad několika botnetů

Age (days)	Name	Server	MaxSize
02.00	nubela.net	dns.nubela.net	10725
10.94	winnt.bigmoney.biz (randex)	winnt.bigmoney.biz	2393
09.66	PS 7835 - y.eliteirc.co.uk	y.eliteirc.co.uk	2061
09.13	y.stefanjagger.co.uk (#y)	y.stefanjagger.co.uk	1832
03.10	ganjahaze.com	ganjahaze.com	1507
01.04	PS 8049 - 1.j00g0t0wn3d.net	1.j00g0t0wn3d.net	3689
10.93	pub.isonert.net	pub.isonert.net	537
08.07	irc.brokenirc.net	irc.brokenirc.net	649
01.02	PS 8048 - grabit.zapto.org	grabit.zapto.org	62
10.34	dark.naksha.net	dark.naksha.net	UNK
08.96	PS 7865 - lsd.25u.com	lsd.25u.com	UNK
UNK	PS ? - 69.64.38.221	69.64.38.221	UNK

(3 Sep 2004 snapshot)

Využití botnetů

- „Keystroke loggers“ pro získávání hesel a čísel kreditních karet
- Útoky DDOS (Distributed Denial of Service)
  - Proti významným serverům
- Přeposílání spamu: 70-80% veškerého spamu
  - Source SpecialHam.com, Spamforum.biz
- Warez
- Zásoba pro budoucí využití

BIS 1

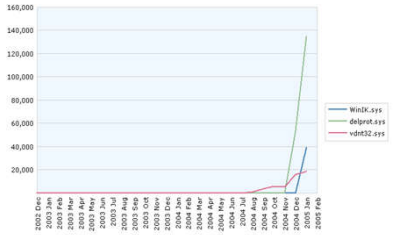
Likvidační potenciál botnetů

10,000-member botnet

Attack	Requests/bot	Botnet Total	Resource exhausted
Bandwidth flood (uplink)	186 kbps	1.86 Gbps	T1, T3, OC-3, OC-12
Bandwidth flood (downlink)	450 kbps	4.5 Gbps	T1, T3, OC-3, OC-12, OC-48 (2.488Gbps) 50% of Taiwan/US backbone
Syn flood	450 SYNs/sec	4.5M SYN/sec	4 Dedicated Cisco Guard (@$90k) OR 20 tuned servers
Static http get (cached)	93/sec	929,000/sec	15 servers
Dynamic http get	93/sec	929,000/sec	310 servers
SSL handshake	10/sec	100,000/sec	167 servers

Rootkity

- Zvyšuje se rozšíření rootkitů
  - Neodhalitelné běžnými anti-spyware systémy
  - Podporují adware & spyware
  - DRM systémy



Rootkit

- Rootkit je softwarový balík určený k tomu, aby vytvořil, utajil a spravoval prostředí pro útočníka na kompromitovaném stroji
- Binary rootkits
  - Modifikace systémových souborů
- Kernel rootkits
  - Modifikace komponent kernelu
- Library rootkits
  - Přepisují systémové knihovny

Rootkit

- Cíle
  - Správa přístupu útočníka
    - » Vytvoří zadní vrátka (backdoor) a udržuje je
    - » Poslouchá na portu a čeká na příkazy (UDP listener)
    - » Bez poslouchání na portu (sniffer) pro snížení možnosti odhalení
  - Správa lokálního přístupu
    - » Práva roota
    - » Ochrana před jinými rootkity
  - Lividace důkazů
    - » Skrývání
      - Zmodifikovaných souborů
      - Procesů útočníka
      - Používaných síťových připojení
    - » Úpravy logů

Bezpečnostní opatření

Co je bezpečnost?

- Bezpečnostní cíle
  - Proč?
- Bezpečnostní funkce
  - Jak?
- Bezpečnostní mechanismy
  - Co?

- Důvěrnost
- Integrita
- Dostupnost
- ...
- Desítky funkcí
- Neomezené množství mechanismů

BIS 1

Bezpečnostní opatření

- Cíle opatření
  - bariéra mezi hrozbami a aktivy
  - omezují zranitelná místa
- OMEZUJÍCÍ bezp. opatření
  - minimalizují ztráty vzniklé útokem (odhalí nebo odvrátí útok)
  - maximalizují zotavení po útoku
- PREVENTIVNÍ bezp. opatření
  - snižují pravděpodobnost útoku
  - zvyšují pro útočníka náklady na útok (cena útoku je pro útočníka větší než jeho dosažitelný zisk):
    - » pravděpodobnost a vliv odhalení
    - » bezprostřední náklady na útok
    - » čas, potřebný k útoku

Omezení bezp. opatření

- Periodicky musí být kontrolována
  - efektivnost implementace bezp. opatření (odpovídají skutečná bezp. opatření plánovaným?)
  - relevantnost bezp. opatření (nezměnily se hrozby?)
  - potřeba dodatečných bezp. opatření
- Omezujícím faktorem je CENA
  - Jednorázové náklady
    - » Náklady na zakoupení HW nebo SW
    - » Náklady na vývoj SW a procedur
    - » Instalace
  - Provozní náklady
    - » Snížení výkonnosti systému (režie)
    - » Potřebné prostředky (např. spotřební materiál, lidská obsluha)
    - » Údržba bezp. opatření (sledování, kontrola, modifikace)
- Principy ceny bezp. opatření
  - Cena bezp. opatření musí být menší než předpokládaná ztráta, pokud by bezp. opatření nebylo instalováno
  - Bezp. opatření by mělo cenu útoku učinit vyšší, než je předpokládaný zisk útočníka.

Typy bezpečnostních opatření

- Fyzická
  - opatření, řídící fyzický kontakt osob s informačním systémem (budovy, ploty, zámky, stráže, ...)
- Administrativní (procedurální)
  - bezpečnostní procedury, prováděné lidmi (přihlašování, evidence přístupu, zálohování dat, ...)
- Personální
  - opatření, omezující hrozby od uživatelů (přijímání a propouštění zaměstnanců, osvěta a školení, ...)
- Technická (Logická)
  - HW a SW opatření, implementovaná v počítačové části informačního systému (identifikace, autentizace, řízení přístupu, protokolování, šifrování, ...)

I. Fyzická bezpečnostní opatření

- Účel
  - Fyzická bezp. opatření fyzickým způsobem omezují přístup ke komponentám informačního systému
  - zabraňují hrozbám pro fyzické komponenty systému
- Typy
  - Fyzická kontrola přístupu - zabraňuje osobám v přístupu k IS
    - » Příklady implementace
      - fyzické umístění - do méně přístupných míst
      - stráže a kurýři
      - zámky a elektronické zabezpečovací systémy (EZS)
      - dohlížecí systémy a detektory přítomnosti osob
      - trezory a schránky
  - Ochrana proti vnějším vlivům - opatření (prevence nebo zotavení) proti vnějším vlivům (přírodním nebo umělým, úmyslným nebo neúmyslným)
    - » Příklady implementace
      - prevence adetekce požáru - požární hlásiče, protipožární prostředky, budova
      - elektrická energie - filtry, UPS (Uninterruptible Power Supply), generátory
      - prostředí (teplota, vlhkost) - snímače teploty, vlhkosti, klimatizace
      - zátopa - umístění IS, budova, senzory
  - Jiná bezp. opatření
    - zálohování komunikačních médií
    - zálohy HW

II. Administrativní bezp. opatření

- bezpečnostní procedury, prováděné lidmi
- zodpovědnost uživatelů
  - přihlašování
  - evidence přístupu
  - osobní zodpovědnost zaměstnanců
  - oddělení pravomocí / zodpovědností
- vstup / výstup
  - kontrola vstupu a výstupu dat
- dokumentační bezpečnost
  - dokumentace
- vývoj a aktualizace HW a SW
  - správa změn
- havárie
  - zálohovací procedury
  - procedury zotavení po havárii
  - havarijní plány

III. Personální bezp. opatření

Lidé jsou nejdůležitější a nejméně spolehlivou částí informačního systému.

- Personální bezp. opatření:
  - mají za cíl snížit pravděpodobnost toho, že zaměstnanci se nebudou chovat v souladu s bezpečnostní politikou
  - jsou namířena přímo na osoby (nikoli prostřednictvím IS)
  - jsou převážně preventivní
  - jsou založena na
    - » důvěryhodnosti pracovníka
    - » spolehlivosti pracovníka

BIS 1

- **Přijímání zaměstnanců**
  - **Definice pracovního místa**
    Jednoznačná a stabilní definice prac. místa -> odvození potřebného přístupu k IS
    - » **Oddělení pravomocí**
      Takové rozdělení rolí a odpovědností, které zabrání tomu, aby jediný člověk mohl narušit (padělat, zničit) kritický proces (data)
    - » **Nejmenší potřebná oprávnění**
      Každý uživatel má mít pouze ta oprávnění, která nezbytně potřebuje k výkonu své funkce
  - **Určení citlivosti pracovního místa**
    Určení potřebného stupně prověření pracovníka, který má zastávat místo.
    - » **Převážně armáda a státní správa (prověření pro práci s tajnými materiály, ..)**
  - **Prověřování pracovníků**
    - » **Zjištění důvěryhodnosti pracovníka**
    - » **Implementace**
      - **zjištění historie pracovníka - informace od předchozích zaměstnavatelů**
      - **ověření důvěryhodnosti pracovníka externí organizací**
      - **periodické zjišťování důvěryhodnosti pracovníka**

- **Správa zaměstnanců**
  - **Správa počítačových sezení zaměstnanců**
    - » **vytváření sezení**
    - » **přidělování přístupových práv**
    - » **neodmítnutelnost zodpovědnosti zaměstnanců**
  - **Přesuny zaměstnanců uvnitř organizace**
    - » **dočasné změny přístupových práv**
    - » **odebírání přístupových práv**
    - » **!! možnost porušení oddělení pravomocí**
  - **Audit**
    - » **monitorování a protokolování aktivit uživatelů**
  - **Detekce neautorizovaných nebo nelegálních aktivit**
- **Osvěta a školení**
  - **účel - zvýšení spolehlivosti zaměstnanců**
  - **zaměstnanci**
    - **neumí používat bezpečnostní mechanismy**
    - **nevědí, že by měli používat bezpečnostní mechanismy**
    - **nechtějí používat bezpečnostní mechanismy**
  - **oblasti**
    - » **zvyšování informovanosti v oblasti bezpečnosti**
    - » **zvyšování obecně technického vzdělání**
    - » **zvyšování morální uvědomělosti**

- **Propouštění zaměstnanců - přátelské ukončení práce**
  - **měl by existovat standardní postup propuštění zaměstnance**
  - **Možné problémy**
    - » **odebrání všech přístupových práv (elektronických i neelektronických)**
    - » **odevzdání všech dokumentů**
    - » **odevzdání všech médií**
    - » **předání dat**
    - » **předání všech potřebných hesel, kryptografických klíčů a hardwarových autentizačních prostředků**
    - » **zajištění změny všech hesel a klíčů, které zaměstnanec zná**
    - » **zajištění důvěrnosti informací**
- **Propouštění zaměstnanců - nepřátelské ukončení práce**
  - **dtto jako v předchozím případě, ale navíc:**
    - » **nutnost velmi rychlého odebrání všech přístupových práv**
    - » **možnost následného zneužívání systému**
    - » **možnost "logických bomb" v systému**
    - » **Co je třeba v systému změnit? Které informace si zaměstnanec odnáší?**

IV. Logická bezpečnostní opatření

- **Jsou implementována v HW a SW informačního systému**
- **Zajišťují**
  - **Confidentiality - Důvěrnost**
    - » **Zabránění neautorizovaného odhalení informace**
  - **Integrity - Integritu**
    - » **Zabránění neautorizované modifikaci informace**
  - **Availability - Dostupnost**
    - » **Zajištění toho, že autorizovaným subjektům nemůže být bráněno v přístupu k informaci nebo k prostředkům systému**
  - ***Nepopiratelnost***
    - » ***Zajištění toho, že uživatel se nemůže zbavit zodpovědnosti za akce, které provedl***

Bezpečnostní funkce

Bezpečnostní funkce

- **Důvěrnost**
  - **prevence proti neautorizovanému odhalení informace**
    - » ***Řízení přístupu, Skryté kanály, Opětné použití***
- **Integrita**
  - **prevence proti neautorizované modifikaci informace**
    - » ***Řízení přístupu, DVB, Fyzická integrita, Návrat, Oddělení rolí, Autonomní testování***
- **Dostupnost**
  - **prevence proti neautorizovanému odmítnutí informace nebo zdrojů**
    - » ***Přidělování prostředků, Opravitelnost za provozu, Robustnost, Zotavení po chybě***
- **Účtovatelnost**
  - **identifikace a monitorování důležitých událostí**
    - » ***Audit, Identifikace a autentizace, Důvěryhodný kanál***

BIS 1

Další bezpečnostní funkce

- autentizace X anonymita & pseudonymita
- audit X nemožnost sledování
- anonymita
  - možnost provést jisté akce tak, aby nebylo možno zjistit, kdo je provedl
  - mechanismus - anonymizační autorita, kryptografické protokoly
- pseudonymita
  - možnost provést akci pod pseudonymem
  - zachování všech ostatních bezpečnostních funkcí
  - mechanismus - pseudonymizační autorita, kryptografické protokoly
- nemožnost sledování
  - možnost provádět akce tak, aby nemohly být sledovány
  - kryptografické protokoly

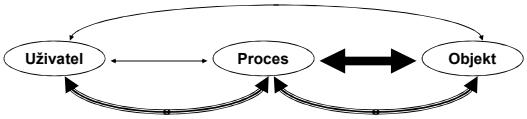
Řízení přístupu

důvěrnost
integrita

- nepovinné řízení přístupu
  - uživatel, proces a objekt dostávají identifikaci
  - přístupová práva k objektu může měnit běžný uživatel (vlastník) - UNIX
  - v rámci systému lze použít pouze jeden stupeň utajení
- povinné řízení přístupu
  - uživatel, proces a objekt mají bezpečnostní atributy <stupeň utajení, kategorie>
  - běžný uživatel nemůže měnit atributy a ani přístupová práva
  - atributy a přístupová práva
    - » administrativně určuje správce
    - » se nastavují automaticky tak, aby odpovídaly bezpečnostní politice (viz modely bezpečnosti)
  - lze použít více stupňů utajení

Řízení přístupu

důvěrnost
integrita



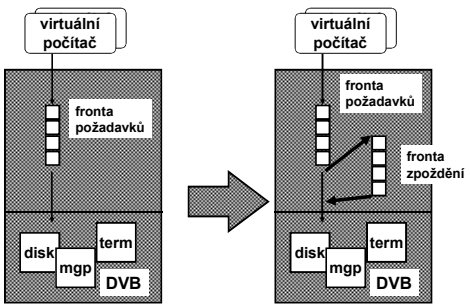
- minimální
  - k některým objektům je možno přistupovat pouze pomocí privilegovaných procesů
- základní
  - uživatel má práva k procesům a objektům (UNIX)
- vyšší
  - přístup na základě kombinace uživatel/proces/objekt (seznam přístupových práv)

Skryté kanály

důvěrnost

- předávání informace v rozporu s bezpečnostní politikou
- šířka pásma skrytého kanálu
- paměťové skryté kanály
  - existence / neexistence souboru
  - atributy souboru
  - délka souboru
  - stav sdílených prostředků (V/V zařízení)
  - NIKOLI obsah souboru - v tom zabrání
- časové skryté kanály
  - zatížení procesoru
  - zatížení V/V zařízení
- kombinované
  - směr pohybu diskové hlavy...

Skryté kanály (pokr.)



- odstranění časového skrytého kanálu

Opětné použití objektů

důvěrnost

- objekt přidělený procesu
  - nesmí obsahovat žádné informace od předchozího vlastníka
  - nesmí mít žádné autorizace zbylé od předchozího vlastníka
- mechanismy
  - fyzické zničení objektu
  - mazání obsahu objektu
  - šifrování obsahu objektu
- hrozby
  - sbírání smetí (scavenging)

BIS 1

integrita

DVB

- princip DVB (Důvěryhodná Výpočetní Báze) zajišťuje schopnost systému
  - chránit sám sebe
  - spravovat chráněné objekty
- ochrana DVB
  - DVB je je schopna chránit sama sebe před vnějšími vlivy a fyzickým útokem
- nemožnost obejít DVB
  - veškerý přístup k chráněným objektům musí být prováděn přes DVB

integrita

Fyzická integrita

- evidence fyzického útoku
  - ochranné nálepky, pečetě, světlocitlivá barva
- odezva na fyzický útok
  - zničení objektu při útoku X upozornění na útok
- odolnost proti fyzickému útoku
  - útok je velmi obtížný až nemožný
- Tamper resistance

integrita

Návrat (zálohování)

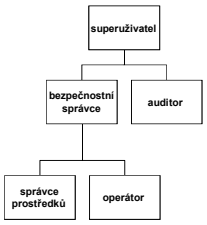
- schopnost vrátit se k předchozímu stavu
  - po chybě uživatele
  - po fyzickém útoku
  - po zničení dat (poruchou, požárem...)
- metody
  - transakce
  - zálohování dat na nezávislá média
    - » fyzické uložení záložních médií
    - » interval zálohování
    - » počet záložních kopií

integrita

Oddělení rolí

- definice různých rolí pro různé funkce
- 1 - základní oddělení rolí
  - správce X uživatel (viz UNIX)
- 2 - oddělení rolí správců
  - více rolí správců (sezení, audit, péče o programy...)
- 3 - oddělení rolí uživatelů
  - více rolí uživatelů (ne pouze skupiny)

Oddělení rolí (AIX)



- superuživatel
  - konfiguruje systém
  - vlastní většinu souborů
- bezp. správce
  - stará se o prosazení bezp. politiky
- správce prostředků
  - dělá běžnou práci správce systému
- operátor
  - rutinní práce (archivace, údržba)
- auditor
  - analýza auditních dat
  - detekce narušení bezp. politiky

integrita

Autonomní testování

- systém je schopen ověřit, že se nachází v bezpečném a správném stavu
  - testování funkce hardware
  - testování integrity software (kontrolní součty, kryptografické testy integrity)
    - » úmyslné změny software a konfigurace - viry, trojské koně
- 1 - manuální autonomní testování
  - vyžaduje zásah člověka
- 2 - autonomní testování při inicializaci
- 3 - autonomní testování během činnosti

BIS 1

dostupnost

Přidělování prostředků

- kontrola množství prostředků a služeb přidělovaných procesům a uživatelům
  - » prostor na disku
  - » čas procesoru
  - » doba relace
  - » počet tiskových stran
- 0
- 1 - kvóty
  - – uživatelům jsou přiřazeny kvóty čerpání prostředků
- 2 - opatření proti neposkytnutí služby
  - – žádný uživatel nemůže vyčerpat prostředky systému (viz 1)
- 3 - prioritní přidělování
  - – uživatelům nebo skupinám lze přiřadit priority přidělování prostředků

dostupnost

Opravitelnost za provozu

- systém je opravitelný za provozu, pokud dovoluje výměnu některých komponent při nepřerušeném poskytování služeb
- 0
- 1 - omezená opravitelnost
  - – některé komponenty lze vyměnit za provozu
- 2 - plná opravitelnost
  - – všechny komponenty lze vyměnit za provozu

dostupnost

Robustnost

- schopnost systému poskytovat služby i při poruše některých komponent
- 0
- 1 - odlonost proti poruchám některých komponent
- 2 - omezená funkčnost
  - – odolný proti poruchám všech komponent s omezenými službami
- 3 - plná funkčnost
  - – odolný proti poruchám všech komponent bez omezení služeb

dostupnost

Zotavení po chybě

- systém je schopen se po chybě vrátit zpět do bezpečného stavu
- 0
- 1 - manuální zotavení po chybě
  - – požaduje zásah správce
- 2 - automatické zotavení po chybě
  - – nepožaduje zásah

účtovatelnost

Identifikace a autentizace

- Identifikace - zjišťění totožnosti uživatele
- Autentizace - ověření totožnosti uživatele na základě to, že uživatel:
  - – něco zná
    - » heslo, PIN
  - – něco vlastní
    - » klíč, magnetická karta, smart karta, autentizační kalkulátor
  - – někým je
    - » antropometrická autentizace
    - » hlas, otisk prstu, vzorek sítnice, tvar dlaně
- slabá X silná autentizace (kryptografická)
- jednosměrná X obousměrná autentizace

účtovatelnost

Audit

Provádí rozpoznávání, záznam a možnost analýzy událostí významných pro bezpečnost.

- ochrana auditních dat
  - » bezpečnostní správce
- fyzické uložení auditních dat
  - » diskový prostor !!
- granularita auditních dat
  - » podrobnost dat X objem dat
- analýza auditních dat
  - » podpůrné prostředky, UI
- detekce a poplach
  - » okamžitá odezva systému na události
- IDS

BIS 1

účtovatelnost

Audit (pokr.)

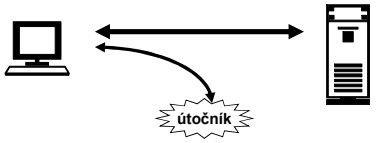
- 0
- 1 - externí audit
  - systém je schopen předávat auditní informace jinému systému
- 2 - Audit
  - lokální úschova auditních informací
  - auditní informace musí být chráněny
- 3 - Audit s poplachem
  - upozornění správce na události, které nejsou v souladu s bezpečnostní politikou
- 4 - Detekce útoku
  - průběžná analýza auditních záznamů a detekce pokusů o narušení bezpečnosti systému

účtovatelnost

Důvěryhodný kanál

Zaručené propojení mezi uživatelem a DVB

- 0
- 1 - autentizační důvěryhodný kanál
  - uživatel je schopen inicializovat důvěryhodný kanál pro účely identifikace a autentizace
- 2 - úplný důvěryhodný kanál
  - uživatel nebo DVB je schopen podle potřeby inicializovat důvěryhodný kanáol kdykoli během relace



Přenos dat

Bezpečnostní služby ISO 7498-2

- Autentizace
  - Autentizace spojení
  - Autentizace odesílatele
- Řízení přístupu
- Důvěrnost
  - Důvěrnost spojení
  - Důvěrnost přenosu zpráv
  - Důvěrnost toku dat
- Integrita
  - Integrita spojení s opravou,
  - Integrita spojení bez opravy
  - Integrita přenosu zpráv
- Nepopiratelnost
  - Nepopiratelnost odesílatele
  - Nepopiratelnost doručení

Autentizace

- Jednoznačné ověření totožnosti
- Autentizace spojení (Entity authentication)
  - Předpokládá službu se spojením
  - Ověření prohlašované identity v konkrétním okamžiku
  - Typicky při navázání spojení
  - Chrání před vydáváním se za jiného uživatele a útokem replay
- Autentizace odesílatele
  - Předpokládá zasílání zpráv (bez spojení)
  - Ověřuje identitu zdroje dat
  - Nechrání před útokem replay

Důvěrnost

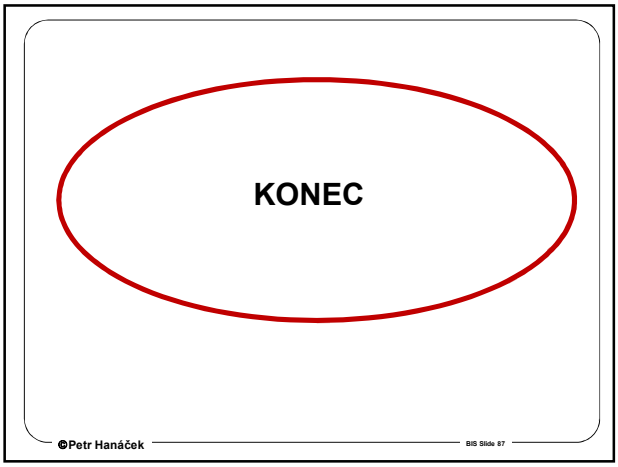
- Ochrana proti neoprávněnému prozrazení informace
- Důvěrnost spojení
  - Předpokládá službu se spojením
- Důvěrnost přenosu zpráv
  - Předpokládá zasílání zpráv (bez spojení)
- Důvěrnost toku dat
  - Proti útokům, kdy se útočník nesnaží dešifrovat přenášené zprávy ale sbírá informace o těchto zprávách (časy, délky, adresy…)

Integrita

- Ochrana proti neodhalené neoprávněné modifikaci informace
- Integrita spojení s opravou
  - Nepoužívá se
- Integrita spojení bez opravy
  - Předpokládá službu se spojením
- Integrita přenosu zpráv
  - Předpokládá zasílání zpráv (bez spojení)
  - Nechrání před útokem replay

Nepopiratelnost

- Ochrana proti popření autorství, obsahu a zaslání nebo přijetí zprávy
- Nepopiratelnost odesílatele
  - Ochrana proti popření autorství, obsahu a zaslání zprávy
- Nepopiratelnost doručení
  - Ochrana proti popření přijetí zprávy



Bezpečnost informačních systémů

Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií

Petr Hanáček,
Jan Staudek

Úřad pro státní informační systém
2000

1. Základní principy bezpečnosti při použití IT

Informační technologie[1] 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. Poněvadž 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.

1.1 Motivace pro zabezpečování při použití IT

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.

Charakteristickým rysem soudobých organizací tedy je, že svoje poslání plní pomocí propojení informačních a komunikačních systémů budovaných na bázi IT, a to jak uvnitř organizace (in-

[1] dále budeme pojem *informační technologie* zapisovat zkratkou IT

tra…, lze připomenout pojem „intranet“, vnitřní síť), tak i s ostatními organizacemi (extra… / inter…, např. „extranet“ / Internet). Tím se činnosti organizace stávají silně závislé na informacích a službách IT. Důsledkem je, že ztráta důvěrnosti, integrity, dostupnosti, prokazatelnosti odpovědnosti, autenticity a spolehlivosti informací a služeb IT má na chod organizace nepříznivý dopad. Řešením je uplatnění zásad bezpečnosti IT. Pojmem *zabezpečování IT* označujeme proces dosažení a udržení důvěrnosti, integrity, dostupnosti, prokazatelnosti odpovědnosti, autenticity a spolehlivosti informací a služeb IT na přiměřené úrovni.

Vhodným metodickým průvodcem bezpečností IT je např. technická zpráva ISO/IEC TR 13335 „Information technology – Guidelines for the Management of IT Technology“. Podle tohoto materiálu se bezpečnost IT použitých v organizaci 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 politik[2] 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 udržovat bezpečí všech, kdo IT v organizaci používají
- detekování bezpečnostních incidentů a adekvátní reakce na ně.

Organizace musí své informační systémy[3] zabezpečovat stejně jako jiné investice do své činnosti. Hardwarové komponenty IT lze zničit (teroristy nebo i nespokojenými či pomatenými zaměstnanci) nebo ukrást (a levně prodat nebo používat pro vlastní potřebu).

„Ukrást“ lze i software, který mnohdy představuje enormní a přitom špatně vyčíslitelné hodnoty. Konkurent tak může ušetřit náklady na vývoj a/nebo na pořízení softwaru. Neoprávněné užívání softwaru zaměstnanci pro osobní potřebu nebo pro jejich druhé zaměstnání je zdrojem jejich nelegálních zisků. Provozovateli kradeného softwaru mohou vzniknout škody plynoucí z trestní odpovědnosti za porušení licence.

Informační systém lze používat neautorizovaně, a tím způsobit např. zničení systému nebo porušení soukromí jiných osob („krádeží“ přístupového hesla, překonáním mechanismu řídicího přístup k IS) nebo lze využitkovávat IS i autorizovanými zaměstnanci k nepracovní činnosti, ať již osobní, nebo výdělečné.

Informace jsou v podstatě zboží, pro organizaci představují mnohdy cenná aktiva. Data uložená v bázích dat lze ukrást neoprávněným okopírováním, lze ukrást i výstupy generované IS pro potřebu organizace. Data, která jsou pro organizaci citlivá, je potřeba chránit před konkurencí.

Existují právní, morální a etická pravidla pro používání informací, existují zákonné úpravy pro ochranu dat, a ty je žádoucí, resp. nutné, dodržovat.

Organizace se musí bránit tomu, aby funkce jejich IS nebyly ať již zlomyslně, nebo neúmyslně znepřístupněny.

---

[2] *cíl* – určení toho, čeho se má dosáhnout, *strategie* – určení, jak dosáhnout splnění cíle, *politika* – pravidla řídicí dosažení cíle; běžně se vyjadřují neformálně, v přirozeném jazyku, lze ale pro zvýšení účinnosti použít i formální, resp. semiformální, logicko–matematická vyjádření pravidel

[3] dále budeme pojem *informační systém* zapisovat zkratkou IS

Tato metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií je psána především pro čtenáře, který musí z titulu své funkce nebo pracovní náplně řešit problémy související

- s vývojem bezpečnostní politiky IT
- s identifikací rolí a odpovědností za data a IT v organizaci
- se správou rizik organizace
  - identifikace, zvládnutí, odstranění nebo minimalizace událostí, které mají nežádoucí vliv na činnost a aktiva organizace
  - identifikace a ohodnocení chráněných aktiv, citlivých dat a jejich klasifikace do tříd vymezujících potřebnost jejich ochrany
  - identifikace zranitelných míst v používaných IT a s nimi souvisejících hrozeb
  - určení forem útoků a typu útočníků
  - určení pravděpodobností útoků, tj. jakým rizikům jsou IS organizace vystaveny, včetně určení potenciálních škod
  - respektovaných omezení organizačních, finančních, daných prostředím, personálních, časových, právních, technických, kulturně–sociálních apod.).

Získané znalosti čtenáři usnadní porozumět problémům, které souvisejí

- s principy, postupy
- s výběrem bezpečnostních opatření a s jejich implementací vhodnými bezpečnostními mechanismy
- se správou konfigurace IS
- se správou změnového řízení v použitých IT
- s vypracováním havarijních plánů určujících činnost organizace po narušení bezpečnosti
- s vlastní bezpečnou provozní činností v oblasti IT organizace (zajišťování údržby IS, bezpečnostní auditorské činnosti, monitorování, vyhodnocování činností IS, reakce na bezpečnostní incidenty).

V neposlední řadě se lidé, kteří se starající o bezpečnost IT, musí zabývat i školícími aktivitami v oblasti bezpečnosti a pro ty je tato příručka zvláště vhodná.

Nakonec úvodních motivací je nutné čtenáře upozornit, že bezpečnost IT nelze řešit izolovaně. 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*).

Provozní prosazování systémové bezpečnostní politiky se často označuje pojmem *bezpečnostní program*.

Ani všeobecnou bezpečnostní politiku organizace nelze řešit bez návaznosti na ostatní politiky vymezující chod a poslání organizace (finanční, obchodní, sociální atd.).

Důležité je si uvědomit, že zkušenosti útočníků v čase rostou, cíle jejich útoků se postupně upřesňují, informační technologie se vyvíjejí a zdokonalují, mění se případně i cíle profilu organizace. Proto se i cíle, strategie a politiky bezpečnosti musí periodicky korigovat. Vhodné jsou periodické oponentury bezpečnostních politik, které mohou vyvolat požadavek opakovaného provedení analýzy rizik, periodicky je potřebné provádět i bezpečnostní audit.

1.2 Výklad základních pojmů z oblasti bezpečnosti IT

1.2.1 Použitý model

Základní pojmy, vymezující oblast bezpečnosti IT, si vysvětlíme na modelu, ve kterém se použité IS skládají ze tří následujících typů komponent:

- hardware – procesor, paměti, terminály, telekomunikace atd.
- software – aplikační programy, operační systém atd.
- data – data uložená v databázi, výsledky, výstupní sestavy, vstupní data atd.

Je samozřejmé, že přirozenou čtvrtou komponentou IS jsou lidé – uživatelé, personál. Protože se ale zaměřujeme na bezpečnost IT a ne na obecnou bezpečnost, o lidské činitele se budeme zajímat jen do té míry, pokud se jejich činnosti a vlastnosti budou bezprostředně týkat bezpečnosti IT. Prvé tři z uvedených komponent představují pro organizaci provozující IS jisté hodnoty, proto se nazývají *aktiva.*

Problém bezpečnosti IS budeme probírat bez ohledu na konkrétní aplikační zaměření IS, není pro náš výklad podstatné, zda je IS orientován na výzkum a vývoj, řízení burzy, bankovní systém, získávání dat, personální agendu, konstrukční systém, knihovnický systém, regulační systém, systém řízení podniku nebo na něco jiného.

Způsob dosažení bezpečnosti a bezpečnostní vlastnosti určuje bezpečnostní politika. Pojmem bezpečnostní politika IS označujeme souhrn norem, pravidel a praktik, definující způsob správy, ochrany a distribuce citlivých dat a jiných aktiv v rámci činnosti IS. *Citlivá data* mají pro chod organizace zásadní význam, jejich kompromitací nebo zneužitím by vznikla organizaci škoda, případně by organizace nemohla řádně plnit svoje poslání. Bez explicitní definice a ohodnocení aktiv nelze implementovat a udržovat žádný bezpečnostní program.

Je třeba si uvědomit, že každý IS je zranitelný, bezpečnostní politika IS pouze snižuje pravděpodobnost úspěchu útoku proti IS nebo nutí útočníka vynakládat více peněz nebo času. Absolutně bezpečný systém neexistuje. Když analyzujeme IS z hlediska potřeb jeho zabezpečení, rozpoznáváme:

- *objekt IS*
  pasivní entita, která obsahuje/přijímá informace a je přístupná autorizovaným subjektům IS
- *subjekt IS*
  aktivní entita (osoba, proces nebo zařízení činné na základě příkazu uživatele) autorizovatelná pro získání informace z objektu, vydávání příkazů ovlivňujících udělení práv přístupu k objektu, změnu stavu objektu apod.

Pojmem *autorizace*[4] subjektu pro jistou činnost rozumíme určení, že daný subjekt je z hlediska této činnosti důvěryhodný. Udělení autorizace subjektu si vynucuje, aby se pracovalo s autentickými subjekty. *Autentizací*[5] se rozumí proces ověřování pravosti identity entity (subjektu, objektu, tj. uživatele, procesu, systémů, informačních struktur apod.).

Důvěryhodný IS (subjekt nebo objekt) je taková entita, o které se věří (je o tom podán důkaz), že je implementovaná tak, že splňuje svoji specifikaci vypracovanou v souladu s bezpečnostní politikou. Na důvěryhodnou entitu se můžeme spolehnout, chová-li se tak, jak očekáváme, že se bude chovat.

1.2.2 Zranitelné místo, hrozba, riziko, útok, útočník

1.2.2.1 Zranitelné místo

Slabinu IS využitelnou ke způsobení škod nebo ztrát útokem na IS nazýváme *zranitelné místo*. Existence zranitelných míst je důsledek chyb, selhání v analýze, v návrhu a/nebo v implementaci IS, důsledek vysoké hustoty uložených informací, složitosti softwaru, existence *skrytých kanálů* pro přenos informace jinou než zamýšlenou cestou apod.[6]. Podstata zranitelného místa může být:

- fyzická
  např. umístění IS v místě, které je snadno dostupné sabotáži a/nebo vandalismu, výpadek napětí
- přírodní
  objektivní faktory typu záplava, požár, zemětřesení, blesk
- v hardwaru nebo v softwaru
- fyzikální
  vyzařování, útoky při komunikaci na výměnu zprávy, na spoje
- v lidském faktoru
  největší zranitelnost ze všech možných variant.

Zranitelná místa vznikají jako důsledek selhání (opomenutí, zanedbání)

- v návrhu
- ve specifikaci požadavků
  IS může plnit všechny funkce a vykazovat všechny bezpečnostní rysy po něm požadované a přesto stále ještě obsahuje zranitelná místa, která ho činí z hlediska bezpečnosti nevhodným nebo neúčinným

---

[4] oprávněnost, autorizovat znamená povolit schválit, zmocnit, oprávnit subjekt používat služby IS

[5] autentický – původní, pravý, hodnověrný

[6] Jako příklady typických zranitelných míst např. v operačních systémech lze uvést: okamžik identifikace a autentizace – podvržený *login* program (trojský kůň) umí ukrást heslo, nedokonalou implementací bezpečnostního mechanismu, chybný předpoklad důvěryhodnosti – předpokládá se správnost jiného programu, místo toho, aby se pečlivě testovala správnost jím dodávaných parametrů, skryté sdílení – systém může ukládat kritické informace do adresových prostorů procesů, aniž by to bylo definováno v jeho manuálu (tajné usnadnění implementace, chyba návrhu,...), komunikace mezi procesy – testování zasíláním a čtením zpráv až do získání správného výsledku, přerušení komunikačního spojení – útočník nahradí původní spoj svým spojem, rezidua (nezničená informace v uvolněných prostředcích, skryté paměťové kanály), nekontrolování počtů neúspěšných pokusů přihlášení se apod.

- v řešení (projektu)
- v konstrukci
  IS nesplňuje svoje specifikace nebo byla do něj zavlečena zranitelná místa v důsledku špatných konstrukčních standardů nebo nesprávných rozhodnutí (voleb) při jeho návrhu či implementaci
- v provozu
  IS byl sice správně zkonstruován podle správných specifikací, ale zranitelná místa do něj byla zavlečena v důsledku použití neadekvátních provozních řídicích nástrojů.

1.2.2.2 Hrozba

Zranitelná místa jsou vlastnostmi (součástmi) informačního systému, jejichž existence způsobuje, že některé vlivy prostředí, ve kterém se informační systém provozuje, představují pro něj hrozby. Pojmem *hrozba* označujeme možnost využitkovat zranitelné místo IS k útoku na něj – ke způsobení škody na aktivech. Hrozby lze kategorizovat na:

- objektivní
  - přírodní, fyzické
    požár, povodeň, výpadek napětí, poruchy..., u kterých je prevence obtížná a u kterých je třeba řešit spíše minimalizaci dopadů vhodným plánem obnovy; v tomto případě je třeba vypracovat havarijní plán
  - fyzikální
    např. elektromagnetické vyzařování
  - technické nebo logické
    porucha paměti, softwarová „zadní vrátka“, špatné propojení jinak bezpečných komponent, krádež, resp. zničení paměťového média, nebo nedokonalé zrušení informace na něm
- subjektivní, tj. hrozby plynoucí z lidského faktoru
  - neúmyslné
    např. působení neškoleného uživatele / správce
  - úmyslné
    představované potenciální existencí *vnějších útočníků* (špioni, teroristi, kriminální živly, konkurenti, hackeři) i *vnitřních útočníků* (odhaduje se, že 80 % útoků na IT je vedeno zevnitř, útočníkem, kterým může být propuštěný, rozzlobený, vydíraný, chamtivý zaměstnanec); velmi efektivní z hlediska vedení útoku je součinnost obou typů útočníků.

Charakteristikou hrozby je její zdroj (např. vnější nebo vnitřní), motivace potenciálního útočníka (finanční zisk, získání konkurenční převahy), frekvence a kritičnost uplatnění hrozby. Jako příklady typických hrozeb pro IT lze uvést orientační přehled generických hrozeb pro distribuované systémy IT: neautorizovaná modifikace informací, informačních zdrojů a služeb, tj. porušení integrity odchytáváním a modifikací zpráv, vkládáním a replikacemi zpráv, neautorizované zpřístupnění informace odposlechem na přenosovém médiu, analýzou toku vyměňovaných zpráv nebo jejich délek, resp. frekvencí zasílání, analýza adres zdrojů a cílů zpráv, neoprávněné kopírování z dočasných paměťových míst (vyrovnávací paměti). K neautorizovanému zpřístupnění informací může útočník využít např. škodlivý software nebo elektromagnetické vyzařování. Hrozbou mohou být agregace citlivých informací z méně citlivých dílčích informací, dedukce ze znalosti, že jistá informace je uložena v databázi, dedukce z informací neoprávněně dostupných na veřejných zdrojích (např. z mnohých nedostatečně chráněných systémo-

vých tabulek), odposlech pomocí zařízení pro práci se zvukem, instalovaných na mnoha počítačích. Dalším typem hrozeb je neautorizované použití zdrojů (krádeže hardwarových a softwarových komponent, včetně používání jejich neoprávněných kopií), neautorizované používání informačních systémů a služeb jimi poskytovaných, znepřístupnění služeb, tj. akce a události, které brání autorizovaným subjektům využívat systém IT na dohodnuté úrovni poskytovaných služeb, popírání odpovědnosti za akce citlivé z hlediska bezpečnosti, např. popírání aktu zaslání nebo přijetí zprávy, popírání autorství dané zprávy[7].

1.2.2.3 Útok

Útokem, který nazýváme rovněž *bezpečnostní incident,* rozumíme buďto úmyslné využitkování zranitelného místa, tj. využití zranitelného místa ke způsobení škod/ztrát na aktivech IS, nebo neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech. Při analýze možných forem útoků na IT je třeba typicky řešit problémy typu: jak se projevuje počítačová kriminalita, jaké jsou možné formy útoků, kdo útočí, kdo může páchat počítačový zločin, jaká rizika souvisí s používáním informačních technologií, jak se chránit před útoky apod. Následně řešenými problémy jsou pak rozhodnutí typu: jak detekovat útok, jak zjistit bezpečnostní incident, jak reagovat na útok, co dělat, když dojde k bezpečnostnímu incidentu. Útočit lze:

- přerušením
  aktivní útok na dostupnost, např. ztráta, znepřístupnění, poškození aktiva, porucha periférie, vymazání programu, vymazání dat, porucha v operačním systému
- odposlechem
  pasivní útok na důvěrnost, kdy neautorizovaný subjekt si neoprávněně zpřístupní aktiva, jde např. o okopírování programu nebo o okopírování dat
- změnou
  aktivní útok na integritu, neautorizovaný subjekt zasáhne do aktiva, provede se např. změna uložených a/nebo přenášených dat, přidání funkce do programu
- přidáním hodnoty
  aktivní útok na integritu nebo útok na autenticitu, tj. o případ, kdy neautorizovaná strana něco vytvoří (podvržení transakce, dodání falešných dat).

Vhodnou formou ochrany před pasivními útoky odposlechem je *prevence*, poněvadž *detekce* odposlechu je velmi obtížná. Absolutní prevence útoků ovšem zajistitelná není, proto typická ochrana (hlavně před aktivními formami útoků) je založena na detekci útoků a na následné obnově činnosti. Velmi důležité je vzít si poučení ze zjištěných skutečností a získané zkušenosti uplatnit při vylepšování ochran, ať již preventivních, nebo detekčních či aktivních, heuristických (založených na nějakých hypotézách). Útok může být *úmyslný* nebo *neúmyslný*, resp. *náhodný.* Útok lze rovněž charakterizovat jako:

- útok s velkou škodou (také ho nazýváme *významný*)
  - je-li častý, pak organizace provozující IS obvykle vypracovává bezpečnostní politiku s cílem ochrany před takovým útokem
  - škodní důsledky řídce uplatňovaného útoku lze řešit i pojištěním
  - významný útok, jehož následky znamenají zhroucení organizace nebo její trestní odpovědnost, nazýváme *katastrofický*
- útok s malou škodou (*nevýznamný*)
  - škody způsobené nevýznamným útokem jsou přijatelným rizikem.

---

[7] Odpovědnost lze prokázat např. vedením evidenčních záznamů o provedených akcích s cílem provádění analýzy auditem nebo podpisováním informací vytvářených při takových akcích.

Rozpoznáváme:

- útoky na hardware, které lze vést
  - přerušením – přírodní havárie, neúmyslné útoky způsobené kouřením, údery, úmyslné útoky krádeží, destrukcí
  - odposlechem – krádež času procesoru, místa v paměti
  - přidáním hodnoty – změnou režimu činnosti
- útoky na software[8], které lze vést
  - přerušením – mezi neúmyslné útoky může patřit vymazání softwaru způsobené špatným konfiguračním systémem nebo archivačním systémem, použití neotestovaných programů, chyby operátora; mezi úmyslné útoky patří např. úmyslné vymazání programu
  - odposlechem – provedení neoprávněné kopie programu, pirátství
  - změnou – např. využitím „zadních vrátek“ (neveřejných spouštěcích postupů z doby tvorby softwaru)
  - přidáním hodnoty – zabudováváním trojských koňů, viry, červi, logické bomby
- útoky na data – zatímco útok na hardware lze vyřešit bezpečnostními systémy, strážemi apod. a útok na software vedou obvykle profesionálně zdatní jedinci, tak útok na data je mnohem nebezpečnější, poněvadž data umí číst a interpretovat de facto kdokoli; pro hodnotu dat je charakteristická její dočasnost, tržní hodnota dat není jedinou cenou dat, do té se musí zahrnout cena jejich rekonstrukce, jejich opětovného vytvoření apod. Útoky na data lze opět vést
  - přerušením – mezi neúmyslné útoky lze zařazovat jejich neúmyslné vymazání, mezi úmyslné útoky pak úmyslné vymazání, sabotáž
  - odposlechem – porušení důvěrnosti, krádež kopií
  - změnou – porušení integrity, neautorizované modifikace dat
  - přidáním hodnoty – opakovanými neautorizovanými dílčími odběry z peněžního konta (salámový útok), generování transakcí atd.

1.2.2.4 Útočník

Důležité je si uvědomit, kdo může útočit. Útočník může být vnější, ale v organizaci se často vyskytuje i vnitřní útočník. Podle znalosti a vybavenosti rozeznáváme:

- *útočníky slabé síly*
  amatéři, náhodní útočníci, využívající náhodně objevená zranitelná místa při běžné práci; jedná se o náhodné, často neúmyslné útoky, útočníci mají omezené znalosti, příležitosti i prostředky, pro ochranu před nimi stačí přijmout relativně *slabá bezpečnostní opatření*, která jsou levná
- *útočníky střední síly*
  hackeři, jejichž častým krédem je dostat se k tomu, k čemu nejsou autorizovaní; jedná se o *běžné útoky*, útočníci mají mnohdy hodně znalostí, obvykle ale nemají

[8] Jako příklady útoků např. na operační systém lze uvést: prohlížení pamětí, systému souborů, využití neodstraněných ladících vstupních bodů, zamezení poskytování služeb autorizovaným uživatelům (zahlcením počítače elektronickou poštou, monopolizací počítače nadměrným generováním procesů), vystupováním v identitě jiného autorizovaného uživatele, podplacení/podvedení operátora/obsluhy.

zjevné příležitosti k útokům a mívají omezené prostředky; jako ochrana proti nim se přijímají *bezpečnostní opatření střední síly*

- *útočníky velké síly*
  profesionální zločinci, kteří mají původ obvykle mezi počítačovými profesionály, je pro ně typická vysoká úroveň znalostí, mají obvykle dostatek prostředků (peněz) a mnohdy i dost času k provedení útoku, provádějí *útoky vymykající se běžné praxi*, pro ochranu před nimi je nutno přijímat *silná bezpečnostní opatření*.

1.2.2.5 Riziko

Existence hrozby představuje riziko. *Rizikem* rozumíme pravděpodobnost využitkování zranitelného místa IS. Říkáme, že se hrozba uplatní s takovou a takovou pravděpodobností.

Rizika lze charakterizovat vedle pravděpodobnosti výskytu bezpečnostního incidentu i potenciálně způsobenou škodou.

1.2.3 Bezpečnost IT

Pod pojmem bezpečnost IT obvykle rozumíme ochranu odpovídajících IS a informací, které jsou v nich uchovávány, zpracovávány a přenášeny. Součástí takto obecně chápané bezpečnosti IT je i komunikační bezpečnost, tj. ochrana informace přenášené mezi počítači, fyzická bezpečnost, tj. ochrana před přírodními hrozbami a fyzickými útočníky a personální bezpečnost, tj. ochrana před vnitřními útočníky.

Pojem bezpečnost IT, používaný v této příručce, v sobě tedy zahrnuje i takové pojmy, jakými jsou bezpečnost informačních systémů, ochrana informačních systémů, bezpečnost informací, ochrana informací, ochrana informačních technologií, počítačová bezpečnost, telekomunikační bezpečnost a ochrana informačních technologií. Tyto pojmy mohou mít pro mnohé odlišný význam a v příručce nebudeme ani diskutovat o významu těchto pojmů, ani čtenáře mást zaváděním nějakých umělých klasifikačních schémat. Všechny uvedené pojmy mají jistě svůj nezanedbatelný význam při popisu a diskusi bezpečnosti a ochrany počítačových a telekomunikačních systémů a informací uložených, zpracovávaných a přenášených v takových systémech. Pojem *bezpečnost IT* ale budeme používat jako obecný pojem, který může reprezentovat kterýkoli z ostatních uvedených pojmů.

Mezinárodní normalizační organizace ISO ve svých normách definuje bezpečnost jako zajištěnost proti nebezpečím, minimalizaci rizik a jako komplex administrativních, logických, technických a fyzických opatření pro prevenci, detekci a opravu nesprávného použití IS. Bezpečný IS je takový IS, který je zajištěn fyzicky, administrativně, logicky i technicky. IS je třeba zabezpečovat, protože se jedná o ochranu investic, neboť informace je zboží, nutí k tomu právní nebo morální pravidla, činnost konkurence a zákonné úpravy pro ochranu dat. V soudobém chápání bezpečnosti IT je bezpečnost dána zajištěním:

- *důvěrnosti*
  k aktivům (k údajům) mají přístup pouze autorizované subjekty
- *integrity* a *autenticity*
  aktiva (data, software, hardware) smí modifikovat jen autorizované subjekty a původ informací je ověřitelný
- *dostupnosti*
  aktiva (data nebo služby) jsou autorizovaným subjektům do určité doby dostupná, nedojde tedy k odmítnutí služby, kdy subjekt nedostane to na co má právo.

K těmto dnes již klasickým hlediskům bezpečnosti se v současnosti nedělitelně druží hlediska *prokazatelnosti odpovědnosti*[9], *nepopiratelnosti odpovědnosti*[10] a *spolehlivosti*[11].

Pokud budeme posuzovat útoky z hlediska takto definované bezpečnosti, rozpoznáváme útok na důvěrnost (analýza odpadu, elektromagnetické vyzařování, odposlech komunikací, analýza toku zpráv, kopírování pamětí, agregace, dedukce), útok na integritu a autenticitu (modifikace softwaru na škodlivý software, viry, trojské koně, zadní vrátka, logické bomby, použití neodsouhlaseného hardwaru, obcházení bezpečnostních opatření, narušení transakcí, změna uložených dat, změna dat při jejich přenosu, vkládání falešných zpráv, replikace zpráv), útok na dostupnost (např. znemožněním poskytnutí služby zahlcením, výpadkem energie), útok na nepopiratelnost odpovědnosti a útok na spolehlivost.

Kritéria pro hodnocení bezpečnosti Ministerstva obrany USA[12], široce používaná v osmdesátých a devadesátých letech, hodnotila bezpečnost IS:

- podle toho, jak měl IS vypracovanou svoji bezpečnostní politiku (identifikaci požadavků na ochranu vypracovanou v pojmech vnímaná rizika, hrozby a cíle organizace používající IS),
- podle toho, zda byla provedena klasifikace informací za účelem řízení přístupu k citlivým informacím,
- podle toho, jak se identifikovali jednotliví uživatelé a jak se tato identita autentizovala,
- podle toho, zda se prováděl dostatečně spolehlivý audit na potřebné úrovni granularity s cílem sledování činností jednotlivců a událostí relevantních z hlediska bezpečnosti a
- podle dosažené úrovně zaručitelnosti
  - za důvěryhodnou implementaci bezpečnostní politiky založené na implementaci důvěryhodné výpočetní báze[13] a
  - za průběžnou provozní ochranu zajišťovanou periodickým kontrolováním, zda se bezpečnostní politika neobchází.

Výrazným rysem bezpečnosti podle těchto kritérií byl způsob uplatnění principů řízení přístupu k aktivům:

- *Nepovinná ochrana*[14], tj. ochrana přenechaná k volnému uvážení, vycházela z představy, že každý objekt má svého vlastníka, který podle svého uvážení rozhoduje, kdo a jak k objektu smí přistupovat a manipulovat s ním.
- *Povinná ochrana*[15] předpisovala provedení klasifikace objektů do hierarchie podle jejich citlivosti a jejich označení bezpečnostními návěštími (pro vnitřní potřebu, důvěrné, tajné, přísně tajné apod.) a uživatelé směli k objektům přistupovat a manipulovat s nimi pouze tehdy, když měli dostatečnou úroveň prověření (clearance). Kritéria explicitně neadresovala bezpečnost síťového provozu a bezpečnostní problematiku distribuovaných systémů.

Mezinárodní normalizační organizace ISO na přelomu osmdesátých a devadesátých let doplnila svůj referenční model propojování otevřených systémů (ISO RM OSI) definicí bezpečnosti, ve které se již objevuje námi použitá klasifikace rysů bezpečnosti. Zavádí výčet bezpečnostních funkcí (služeb), kterými musí distribuovaný IS čelit identifikovaným hrozbám. Bezpečnostní cíle se podle ISO plní službami pro řízení přístupu, autentizace, zajištění důvěrnosti,

---

9 *prokazatelnost odpovědnosti* – accountability, také *účtovatelnost* nebo *protokolovatelnost*
10 *nepopiratelnost odpovědnosti* – non-repudiation
11 *spolehlivost* – konzistence zamýšleného a výsledného chování
12 tzv. „Oranžová kniha“ (Orange Book), Trusted Computer Security Evaluation Criteria, TCSEC
13 Trusted Computing Base, TBS
14 Discretionary Access Control, DAC
15 Mandatory Access Control, MAC

integrity, nepopiratelnosti, pohotovosti a účtovatelnosti (sledováním činností a událostí relevantních z hlediska bezpečnosti). Přínosem pohledu ISO na bezpečnost je oddělení funkčních a implementačních hledisek bezpečnosti, zavádí se pojem bezpečnostních funkcí a pojem bezpečnostních mechanismů, jako nástroje pro implementaci bezpečnostních funkcí.

Evropské iniciativy z počátku devadesátých let se rovněž postupně odklonily od chápaní bezpečnosti podle amerických kritérií pro nedostatečnost jejich definice bezpečnosti z hlediska globálnějších potřeb zabezpečování soudobých informačních technologií. Tzv. *harmonizovaná kritéria bezpečnosti* (Information Technology Security Evaluation Criteria, ITSEC) explicitně zahrnula do definice bezpečnosti:

- *vývojový proces* IS, tj. formu specifikace požadavků, návrhu architektury, detailního návrhu, a způsob implementace IS,
- použité *vývojové prostředí*, tj. způsob řízení projektu, použité programovací jazyky, použité kompilátory a bezpečnost aplikovanou při vývoji,
- kvalitu *provozní dokumentace* (správce, uživatele) a
- *provozní prostředí*, tj. proces dodávky, distribuce, konfigurace, spuštění a provozu IS.

V poslední kapitole této příručky se systematicky zabýváme výkladem chápání bezpečnosti podle kritérií, která zavádí normu ISO/IEC z června 1999, ISO/IEC 15408, známou pod názvem *Common Criteria*. Celkový přístup k chápání bezpečnosti v této příručce vychází z idejí zavedených právě těmito kritérii.

1.2.4 Bezpečnostní funkce

Zabezpečujeme-li IS, je třeba nejprve stanovit *bezpečnostní cíle* a způsob jejich dosažení. Bezpečnostní cíle jsou dílčí přínosy k bezpečnosti, kterou dosahuje IS z hlediska udržení důvěrnosti, integrity a dostupnosti. Pro jejich dosažení se aplikuje používání *funkcí prosazujících bezpečnost*, nazývaných rovněž *bezpečnostní funkce* nebo *bezpečnostní opatření.*

Bezpečnostní funkce přispívá buďto ke splnění jednoho bezpečnostního cíle, nebo ke splnění několika bezpečnostních cílů. Abychom mohli bezpečnostní cíle stanovit, je potřeba znát zranitelná místa, jak lze tato zranitelná místa využitkovávat, možné formy útoků, kdo může zranitelná místa využitkovat nebo jejich prostřednictvím způsobit neúmyslnou škodu, kdo jsou potenciální útočníci, s jakou pravděpodobností dochází k útoku, jak se lze proti útokům bránit a jaké škody mohou útoky způsobit. Prostředkem použitým pro dosažení stanovených bezpečnostních cílů IS jsou bezpečnostní funkce IS (bezpečnostní opatření), které mohou být administrativního, fyzického nebo logického typu, tj. mohou být implementovány takovými mechanismy, jakými jsou administrativní akce, hardwarová zařízení, procedury, programy.

Bezpečnostní funkcionalitou se systematicky zabýváme v samostatné (druhé) kapitole. Zde si jenom krátce uvedeme, že bezpečnostní funkce můžeme kategorizovat podle okamžiku uplatnění na:

- *preventivní* (např. odstraňující zranitelná místa nebo aktivity zvyšující bezpečnostní uvědomění)
- *heuristické* (snižující riziko dané nějakou hrozbou)
- *detekční a opravné* (minimalizující účinek útoku podle schématu „detekce–oprava–zotavení“).

Bezpečnostní funkce můžeme kategorizovat rovněž podle způsobu implementace. Implementující *bezpečnostní mechanismus* může mít charakter fyzického opatření, administrativní akce, může jím být technické zařízení nebo logický nástroj (procedura, algoritmus). Podle způsobu implementace pak rozeznáváme bezpečnostní funkce:

- *softwarového charakteru* (mnohdy označované jako *logické bezpečnostní funkce*)
  např. softwarové řízení přístupu, funkce založené na použití kryptografie, digitální podepisování, antivirové prostředky, zřizování účtů, standardy pro návrh, kódování, testování, údržbu programů, ochranné nástroje v operačních systémech (ochrana paměti, ochrana souborů řízením přístupu, přístupové matice, přístupové seznamy, hesla, autentizace přístupu k terminálu), ochranné nástroje v aplikačních systémech pro autentizaci přístupu, pro autentizaci zpráv atd.
- *administrativního a správního charakteru*
  ochrana proti hrozbám souvisejícím s nedokonalostí odpovědnosti a řízení systému IT; výběr a školení důvěryhodných osob, hesla, autorizační postupy, přijímací a výpovědní postupy, právní normy, zákony, vyhlášky, předpisy, etické normy, licenční politika, nástroje provozního řízení, zpravodajství o událostech a stavech významných z hlediska bezpečnosti, sběru a analýzy statistik, konfigurace systému apod.
- *hardwarového charakteru* (mnohdy označované jako *technické bezpečnostní funkce*)
  autentizace na bázi identifikačních karet, šifrovače, autentizační kalkulátory, firewally, archivní pásky – záložní kopie dat a programů
- *fyzického charakteru*
  stínění, trezory, zámky, strážní, jmenovky, protipožární ochrana, záložní generátory energie.

Jako příklady bezpečnostních funkcí lze uvést funkce (bez nároku na úplnost výčtu):

- identifikace a autentizace
- autorizace a řízení přístupu
- řízení opakovaného užívání objektů
- účtovatelnost, resp. prokazatelnost odpovědnosti
  získání záruky, že lze učinit subjekty zodpovědné za své aktivity
- audit
  manuální nebo automatické zkoumání protokolu o relevantních událostech v IS z hlediska bezpečnosti
- zajištění nepopiratelnosti
  nepopiratelnost vykonání akce či doručení zprávy (např. digitálním podepisováním)
- zajištění integrity
- zajištění důvěrnosti
- zajištění pohotovosti
  bezpečnostní funkce založené na strategiích prevence, detekce, duplikace a redundance, obnovy a návratu; patří mezi ně procedury obnovy a návratu po poruše (po útoku, po bezpečnostním incidentu), které po obnově bezpečného provozního stavu systému IT (služby) vrací systém IT nebo službu do běžného používání[16].

Bezpečnostní funkce musí být implementovaná dostatečně důvěryhodně, tj. musí být adekvátním způsobem prokázáno, že její implementace vyhovuje její žádané, resp. zadané specifikaci. Způsobem prokázání důvěryhodnosti implementace bezpečnostních funkcí se systematicky zabýváme v poslední kapitole příručky při rozboru hodnocení bezpečnosti IT.

[16] Zvláštní kategorií jsou tzv. *systémy IT odolné proti poruchám*. Smějí být dostupné pro běžné užití pouze tehdy, když se nacházejí v bezpečném provozním stavu, a to i při omezené aplikační funkčnosti po narušení původní bezpečnostní funkcionality.

1.2.5 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. Rozboru vlastností jednotlivých typů bezpečnostních mechanismů je věnována samostatná (třetí) kapitola příručky.

1.3 Zásady výstavby bezpečnostní politiky IT

Tato kapitola je věnována systematickému výkladu stanovení (celkové) bezpečnostní politiky IT organizace (provozující informační systém). Bezpečnostní politika IT organizace obecně vymezuje:

- co vyžaduje ochranu
- proti jakým hrozbám je ochrana budovaná
- jak budeme chránit to, co vyžaduje ochranu.