Bezpečnost informačních systémů

Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií

Petr Hanáček,
Jan Staudek

Úřad pro státní informační systém
2000

Obsah

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.

Dosažení požadované úrovně bezpečnost IS rovněž podporuje řádné provádění:

- *správy konfigurace*
  Systematické vedení evidence změn konfigurace použitých IT. Každá změna v konfiguraci se vždy musí posoudit z hlediska dopadu na jeho bezpečnost. Systematičnost zaručí promítnutí změn i do všech relevantních dokumentů, např. do havarijního plánu, do přijatých administrativních opatření atd. Kriticky rozsáhlá změna může vyvolat přepracování systémové bezpečnostní politiky. Smyslem správy konfigurace je přitom mít vědomost o tom, co se změnilo a ne zabránit změnám.
- *správy změnového řízení*
  Jedná se o pomocný řídicí nástroj pro identifikaci nových požadavků na bezpečnost po změně vlastností IS. Změny mohou představovat zařazení nových provozních procedur, inovaci softwaru, revize hardwaru, zařazení nových uživatelů, nových skupin uživatelů, nová síťová spojení. Každá změna se opět musí posoudit z hlediska dopadu na bezpečnost. Výsledek projednání dopadu změn a případné manažerské rozhodnutí se musí dokumentovat.

1.3.1 Cíle bezpečnostní politiky IT

Jaké jsou typické cíle bezpečnostní politiky IT? V reálném prostředí se nevyhneme tlaku na zajištění potřebné úrovně důvěrnosti, autentizace, integrity dat a prevence před viry a jinými škodlivými programy, nepopiratelnosti odpovědnosti a potřebné velikosti výpočetního a paměťového výkonu. V distribuovaném prostředí, jakým síť Internet je, se k uvedeným cílům přidává požadavek bezpečnosti transakcí, např. mezi webovskými klienty a servery. Na webovských serverech se uchovávají jak veřejně dostupné soubory, tak soubory citlivé a důvěrné, a ty je třeba ochránit. Na webovském klientu je třeba přijmout opatření proti virové nákaze, prohlížeč by neměl spouštět žádné nedůvěryhodné aplikace. Legitimní javovské applety by neměly působit problémy, ale applety získané z neznámých zdrojů mohou obsahovat cokoli. K provedení programu, dovezeného do klientské stanice z WWW, by měl uživatel dát explicitní souhlas po zvážení potřeby prověření certifikace takového objektu. Takže, které vlastnosti IS vlastně konstituují bezpečnost IS? Které požadavky na bezpečnost zpracování komerčních a legislativně citlivých informací můžeme považovat za přirozené? Určitě je takovým bezpečnostním požadavkem poskytnutí potřebného rozsahu důvěrnosti. Důvěrnost má zásadní význam z hlediska ochrany soukromých dat, a to jak z hlediska zachování soukromí, tak i z hlediska možnosti zneužití informačních služeb. Důvěrnost IS lze zabezpečit pomocí šifrování, skrýváním identit počítačů organizace za firewally nebo řízením přístupu k souborům, např. na WWW serverech. Přirozeným požadavkem na šifrovací systém je dostupnost operace dešifrování. K šifrování a dešifrování je třeba znát jistá tajemství. Prokázání totožnosti pomocí znalosti těchto tajemství se využívá i při implementaci bezpečnostní funkce autentizace a nepopiratelnosti. Šifrování se může provádět na různých úrovních distribuovaného systému podle požadované úrovně transparentnosti takové operace, náročnosti na výkon procesoru a na prostor paměti.

Dalším možným bezpečnostním požadavkem může být uplatnění řízení přístupu**.** Může být žádoucí, aby byla neviditelná pouze část nějaké transakce, zatímco její zbytek může být veřejně dostupný. Takové výběrové řízení přístupu k transakcím, např. při elektronickém obchodování, umožní zákazníkovi „zabalit“ svoje identifikační informace o platební kartě do elektronické obálky, kterou může otevřít pouze jeho banka, tuto přiložit k objednávce a zaslat obchodníkovi. Obchodník obálku předá bance, která obchodníkovi potvrdí solventnost zákazníka, a tento může pokračovat v prodeji, aniž by mu zákazník svoje soukromá data zpřístupňoval.

Dalším přirozeným požadavkem je požadavek zajištění integrity. Integrita musí zajišťovat, aby aktiva, dostupná autorizovaným uživatelům, byla úplná a věrná, tj. odpovídající své specifikaci. Data při přenosu nemohou být neautorizovaně měněna. Data nelze modifikovat ani v místě

jejich dlouhodobého uložení v nějaké paměti. Pro zajištění integrity dat lze použít např. mechanismů kryptografických kontrolních součtů, elektronického podpisu a certifikátů na bázi asymetrické kryptografie. Pro zajištění integrity softwaru je přirozeně nutné používat také adekvátní aktuální antivirové nástroje.

Zajištění autentičnosti je dalším generickým požadavkem bezpečnosti IT. Komunikující strany by měly důvěřovat tomu, že komunikují s tím partnerem, se kterým komunikovat chtěly. K silné autentizaci je třeba obvykle použít mechanismů elektronického podpisu a certifikátů. Dostatečně důvěryhodné prokázání identity lze (podle výsledků analýzy rizik) také dosáhnout např. jednoduchým používáním hesel.

Požaduje-li se zajištění nepopiratelnosti, pak žádná ze spolupracujících stran nesmí mít možnost svoji účast v transakci popřít, a to i po jejím ukončení. Aby bylo možné použít nějaký mechanismus pro implementaci funkce nepopiratelnosti, je třeba ho vybavit vlastností prokazatelnosti autorství. Takovým mechanismem je např. certifikovaný elektronický podpis.

Nedílnou součástí bezpečnostní politiky on-line provozovaných IS musí být opatření zajišťující trvalou dostupnost jeho informatických služeb, tj. zamezující neoprávněnému vyčerpání zdrojů vnějším útočníkem nebo nedokonale vyškoleným vlastním zaměstnancem organizace. Tato opatření se realizují např. definicí mezí dostupného paměťového prostoru, omezením délek elektronicky vyměňovaných zpráv nebo dílu dostupného procesorového výkonu.

1.3.2 Typy bezpečnostních politik

Variant přístupů k zabezpečení IT je více, některé jsou zajímavější nákladově, jiné dosaženou transparentností, další pak odolností proti útoku výjimečné síly. Doporučená varianta bezpečnostní politiky IS by měla vždy vzejít z oponované a závazně přijaté bezpečnostní politiky organizace a bezpečnostní politiky IT organizace (při respektování výsledků analýzy rizik IS). Podle požadované úrovně zabezpečení rozpoznáváme bezpečnostní politiky čtyř obecných typů:

- *Promiskuitní bezpečnostní politika*
  je bezpečnostní politika nikoho neomezující, která každému v zásadě povoluje dělat vše, tedy i to, co by dělat neměl. IS s promiskuitní bezpečnostní politikou jsou obvykle provozně nenákladné, mnohdy ani nenutí povinně používat pro autentizaci alespoň hesla, a zaručují pouze minimální nebo vůbec žádnou bezpečnost. Důvodem používání IS s promiskuitní bezpečnostní politikou může být ekonomičnost řešení, potřebná úroveň bezpečnost může být zajišťována prostředky mimo IT.

- *Liberální bezpečnostní politika*
  je bezpečnostní politika, která každému povoluje dělat vše, až na věci explicitně zakázané. Liberální bezpečnostní politika zaručuje větší bezpečí než promiskuitní politika. Liberální bezpečnostní politika je často uplatňována v prostředích, ve kterých se hrozby považují za málo až průměrně závažné a nepominutelným požadavkem je nízká ekonomická náročnost řešení bezpečnosti. Typicky se opírá o zásadu volitelného řízení přístupu založeného na identitě subjektů.

- *Opatrná bezpečnostní politika, resp. racionální bezpečnostní politika*
  je bezpečnostní politika zakazující dělat vše, co není explicitně povoleno. Opatrná bezpečnostní politika je nákladnější na zavedení, avšak zaručuje vyšší stupeň bezpečnosti. Při aplikaci na obecný IS vesměs požaduje provedení klasifikace objektů a subjektů podle jejich schopností a citlivosti. Je opřena mj. o zásadu povinného řízení přístupu založeného na rolích, ve kterých vystupují subjekty při styku s IS. Z hlediska používání IS v Internetu je obvykle počáteční bezpečnostní politikou při zavádění firewallů.

- *Paranoidní bezpečnostní politika*
  je bezpečnostní politika zakazující dělat vše potenciálně nebezpečné, tedy i to, co by nemuselo být explicitně zakazováno. Zaručuje nejvyšší stupeň bezpečnosti. Např. zakáže používat jakékoliv internetovské služby (co kdyby se daly zneužít), resp. předepíše používat IS bez možnosti on-line napojení na komunikace. Vede pak k maximální izolaci systému. Paranoidní bezpečnostní politika stále může být pro mnoho organizací užitečná. Databázový systém zpracovávající vysoce důvěrné informace lze fyzicky a technicky izolovat na systém s konečným počtem snadno kontrolovatelných vstupů a výstupů. Paranoidní charakter bezpečnostní politiky umožní implementaci aplikace v prostředí s nízkou systémovou režií, tudíž s dosažitelnou vyšší výkonností při zachování nižší úrovně nákladů.

1.3.3 Principy určující charakter bezpečnostní politiky

Následující výčet má generický charakter, popsané principy se musí při vypracovávání bezpečnostní politiky konkrétní organizace specifikovat přesně a konkrétně.

- Princip adresné odpovědnosti
  požaduje, aby byly stanoveny odpovědnosti vlastníka, správce, uživatele IS a ostatních činitelů, stýkajících se s IS a aby jejich činnost byla na potřebné úrovni detailizace bezpečně protokolována. Pod pojmem ostatní činitelé je třeba rozumět management organizace, programátory, pracovníky údržby, operátory a pracovníky provozních složek organizace, správce sítě, externí a interní auditory.

- Princip znalosti
  požaduje, aby všechny subjekty, participující na IS, znaly cíle bezpečnostní politiky a použitá opatření a uměly je aplikovat. Rozumět a být informován o principech zabezpečení je legitimním zájmem takových subjektů. V žádném případě se nejedná o otevírání IS útokům nebo o učení se užívat nástroje pro usnadnění útoku na IS. Jestliže provozovatel nějaké sítě umožní další organizaci síť používat pro poskytování služeb třetím stranám, může si do smlouvy dát požadavek, že musí být jako provozovatel sítě seznámen s bezpečností takového IS. To platí i naopak, provozovatel takového IS může po provozovateli sítě požadovat seznámení s aplikovanými bezpečnostními opatřeními a jejich silou. Zákazník banky má legitimní právo být informován o existenci a implementaci bezpečnostních politik participujících bank.

- Princip etiky
  požaduje, aby se respektovala práva a legitimní zájmy ostatních, a to i na úrovni sociálních norem chování.

- Princip multidisciplinárnosti
  požaduje akceptovat všechna relevantní technická, administrativní, provozní, komerční, výchovná a legislativní hlediska bezpečnosti IS a organizace. Bezpečnostní politika musí být budována s respektováním zájmů a povinností managementu organizace, právního oddělení, oddělení technické podpory atd. Jiná bezpečnostní politika je pochopitelně vhodná pro vojenskou organizaci, jiná pro městský úřad, jiná pro obchodní organizaci a jiná pro školu.

- Princip úměrnosti
  požaduje, aby síla bezpečnostních funkcí byla úměrná jak možným hrozbám a jejich rizikům, tak i možným škodám. Dosažení maximálně možné bezpečnosti za každou cenu by nemuselo být ekonomické. Proto je třeba nejprve provést ocenění aktiv, pak analýzu rizik a teprve poté určovat potřebnou bezpečnostní funkcionalitu

a sílu použitých bezpečnostních mechanismů pro její implementaci. I pojištění je možným bezpečnostním opatřením.

- Princip integrity
  požaduje dosažení koherence cílů a bezpečnostní funkcionality bezpečnostní politiky s cíli, praktikami, strukturami a zvyklostmi běžně zavedenými v organizaci. Bezpečnostní politika musí zajistit celý cyklus života informací, jejich získávání, vytváření, zpracovávání, uchovávání, přenášení, rušení. Záruka za celkovou bezpečnost IS je dána úrovní bezpečnosti jeho nejslabšího článku.
- Princip aktuálnosti
  vyžaduje kooperaci partnerů při čelení aktuálním hrozbám a způsobům jejich projevu. Mnohé principy jsou platné nezávisle na fyzickém umístění.
- Princip periodického hodnocení
  je dán tím, že IS jsou obvykle dynamickou jednotkou a požadavky na bezpečnost a efektivnost se v průběhu času mění (hackeři neskládají ruce v klín a informační technologie se vyvíjejí stále rychleji).
- Princip kompatibility s legitimním použitím a toky dat v demokratické společnosti
  zabraňuje absolutizací požadavků na bezpečnost jednou stranou znemožnit oprávněnou činnost ostatním stranám.

1.3.4 Celková a systémová bezpečnostní politika IT

1.3.4.1 Celková bezpečnostní politika IT

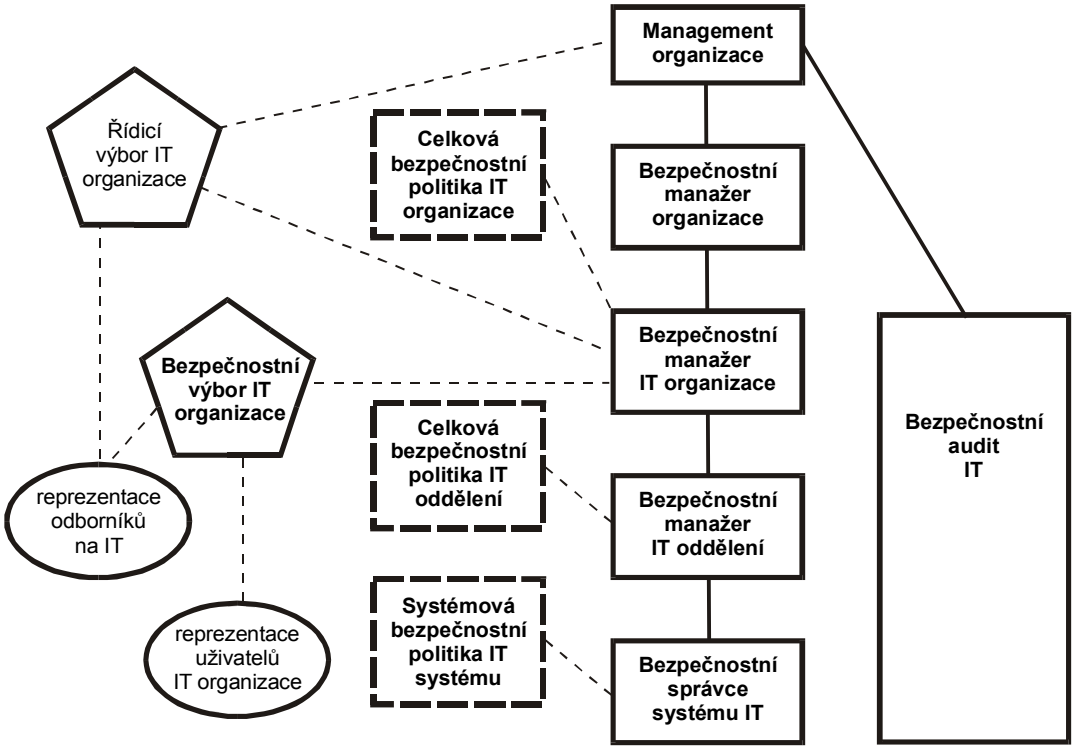
Celková bezpečnostní politika IT uvádí specifikaci cílů zabezpečení, definici citlivých dat a klasifikaci těchto dat a definici ostatních citlivých aktiv IT a definici odpovědností za ně. Definuje bezpečnostní infrastrukturu organizace a potřebné síly mechanismů pro implementaci bezpečnostní funkčnosti. Specifikuje omezení, která musí bezpečnost IT organizace respektovat. Je vytvářena nezávisle na právě používaných informačních technologiích, a to v časovém horizontu obvykle pěti až deseti let. Celková bezpečnostní politika IT je veřejný závazný dokument přijatý vedením organizace jako vnitroinstitucionální norma. Jeho cílem je ochrana majetku, pověsti a činnosti organizace. Musí být úplný (otázky a konflikty lze vyřešit odkazem na jeho paragrafy), stručný a srozumitelný. Musí jasně stanovit hierarchické vazby odpovědností a pravomocí, specifikuje povinnosti a práva jak pro lidi, tak i pro data.

Omezení, která musí bezpečnost IT organizace respektovat, definuje management organizace. Jsou obvykle závislá na prostředí, ve kterém je organizace činná, a řadí mezi ně předpisy, vyhlášky, standardy, zákony a zákonná opatření – souhrnně řečeno omezení organizační, finanční, personální, časová, právní, technická, kulturně sociální, omezení daná životním prostředím atd. Tato omezení ovlivňují volbu bezpečnostních opatření. Respektovaná omezení se musí přehodnocovat periodicky, mění se jak časem, tak i změnou sociálně politických podmínek, jsou odlišná v různých geografických podmínkách.

Je velmi vhodné, když celková bezpečnostní politika IT stanoví potřebné ohodnocení požadované úrovně bezpečnosti, např. uvedením cílové úrovně *zaručitelnosti bezpečnosti IT* podle zvolených kritérií bezpečnosti (nejnověji normalizovaná kritéria bezpečnosti jsou rozebírána v poslední kapitole této příručky).

Celková bezpečnostní politika IT neobsahuje jména konkrétních lidí, produktů, dílčích norem apod. Musí ovšem vedle jasně stanoveného účelu stanovit v souladu s organizačním řádem organizace jednoznačně role, funkční místa, odpovědná za provedení klasifikace dat a přístupových cest, provádění auditu, určení odpovědností za citlivá data, za definici bezpečnostních cílů, za výběr použitých norem, určení, kdo smí ke kterým datům přistupovat, kdo autorizuje přístup,

kdo odpovídá za aktuálnost plánu činnosti organizace po bezpečnostním incidentu, za havarijní plán. Příklad bezpečnostní infrastruktury IT organizace uvádí obr. 1.1.



Obr. 1.1 Příklad bezpečnostní infrastruktury IT organizace

Generické role *bezpečnostní infrastruktury organizace,* které uvedený obrázek odpovídá, lze charakterizovat následující výčtem:

- *Bezpečnostní výbor IT organizace*
  - řeší interdisciplinární problémy bezpečnosti IT
  - dává řídicímu výboru organizace odpovědnému za používání IT strategické podněty k řešení z hlediska bezpečnosti
  - formuluje bezpečnostní politiky, získává jejich schválení od řídícího výboru organizace odpovědného za používání IT
  - definuje bezpečnostní program a monitoruje jeho implementaci
  - schvaluje administrativní opatření a přijaté standardy
  - dozoruje implementace bezpečnostních programů podle systémových bezpečnostních politik
  - hodnotí účinnost bezpečnostních politik
  - prosazuje zvyšování bezpečnostní uvědomění
  - doporučuje potřebné zdroje (lidi, peníze, znalosti …).
- *Bezpečnostní manažer IT organizace*
  - jednoznačně stanovená role s odpovědností za bezpečnost IT organizace
  - spolupracuje s bezpečnostním výborem IT organizace a je jím metodicky řízen
  - řídí implementaci bezpečnostních programů
  - jedná se o hlavní řídicí orgán v oblasti udržování bezpečnosti IT v rámci organizace, metodicky řídí bezpečnostní správce systémů IT.

- *Bezpečnostní správce systému IT*
  - výkonný bezpečnostní orgán
  - spolupracuje s bezpečnostním manažerem IT organizace a je jím metodicky řízen
  - odpovědný za provozování bezpečnostních funkcí podle systémové bezpečnostní politiky
  - vyšetřuje bezpečnostní incidenty a reaguje na ně
  - může být sdruženou rolí s rolí administrativní správy systému.
- *Bezpečnostní auditor IT*
  - kontrolní orgán.

Na obr. 1.1 je navíc ukázána i vazba bezpečnostní infrastruktury na management organizace a její řídicí výbor odpovědný za aplikace IT.

Celková bezpečnostní politika IT se vypracovává jako dokument, jehož generickou strukturu si můžeme vyjádřit následující osnovou:

- *Popis organizace, jejího poslání a koncepcí IT organizace*
  Stručně se popisuje poslání organizace a funkce IS v organizaci, uvádějí se výsledky analýzy závislosti organizace na jejím IS a analýza právní stránky problematiky. Dále se popíše skutečné, tj. stávající provozní prostředí a předpokládané provozní prostředí chráněné vypracovávanou bezpečnostní politikou. Uvedou se dosud stanovené zodpovědnosti a pravomoci, stávající bezpečnostní struktura organizace. Důležité jsou výsledky analýzy dat zpracovávaných IT organizace, zvláště pak určení citlivých informací a míry jejich ochrany – klasifikace. Popisují se služby IT dostupné uživatelům a specifikace aplikačních rozhraní z hlediska bezpečnosti, síla dosud používaných bezpečnostních mechanismů. Pro celkovou bezpečnostní politiku jsou důležité závěry analýzy personální otázky bezpečnosti, charakteristiky uživatelů, manažerů a správců IS. Definuje se provozní dokumentace a popisují se netechnická bezpečnostní opatření, administrativní, fyzická, personální a jiná aplikovaná opatření.
- *Rámcový plán a harmonogram vybudování celkové bezpečnostní politiky*
- *Cíle CBP*
  Uvedou se explicitně vyjmenované bezpečnostní cíle v pojmech důvěrnosti, integrity, pohotovosti, autenticity, odpovědnosti, spolehlivosti aktiv a informačních technologií organizace.
- *Specifikace potřebné struktury zodpovědnosti a pravomocí*
  Vypracování bezpečnostní infrastruktury organizace včetně rolí, funkcí, odpovědností a povinností pracovníků (správců / administrátorů).
- *Identifikace (kritických) aktiv, zvláště pak citlivých dat*
- *Identifikace obecných hrozeb*
- *Výsledky orientační analýzy rizik*
- *Popis stávajícího stavu zabezpečení*
  Formou orientačního popisu aplikovaných bezpečnostních opatření.
- *Doporučení, jak dosáhnout bezpečnostních cílů*
  Formou orientačního popisu navrhovaných bezpečnostních opatření.
- *Cíle a strategie havarijních plánů*

- *Omezení respektovaná bezpečnostní politikou*
  Popisují se návaznosti na relevantní zákony (ČR, EU …), vyhlášky a předpisy, včetně analýzy práv a povinností v oblasti nakládání s informacemi, návaznosti na relevantní mezinárodní a národní normy bezpečnosti IS a doporučení.
- *Časové plány implementace a pravidelných akcí, revizí/oprav*
- *Návrh a koncepce programu školení a osvěty*
  Cílem je založit program školení a osvěty v oblasti bezpečnosti IS specifický pro organizaci. Školení bývají typicky realizována alespoň počátečně z části i spoluřešiteli bezpečnostní politiky. Program musí být konzistentní s celkovou i systémovou bezpečnostní politikou a musí napomoci jejich prosazování. Systém kursů musí pokrýt všechny úrovně pracovníků organizace od vrcholového managementu až po koncové uživatele.

1.3.4.2 Systémová bezpečnostní politika IT

Systémová bezpečnostní politika IT definuje způsob implementace celkové bezpečnostní politiky IT v konkrétním informačně technologickém prostředí. Vypracovává se obvykle pro časový horizont dvou až pěti let. Stanovuje soubor principů a pravidel pro ochranu IS (proto se o ní hovoří rovněž jako o *bezpečnostní politice IS*) a jím poskytovaných služeb, zabývá se volbou konkrétních technických, procedurálních, logických a administrativních bezpečnostních opatření v závislosti na konkrétních IT a částečně i volbou fyzických a personálních bezpečnostních opatření, pokud tyto mohou ovlivnit bezpečnost IS. Implicitně se zabývá bezpečností elektronické (počítačové) části IS. Bezpečnost neelektronické části IS řeší tam, kde by neelektronická část IS mohla výrazně ovlivnit bezpečnost elektronické části. Vše řeší v harmonické návaznosti na již existující a prosazovaná bezpečnostní opatření.

Systémová bezpečností politika IT konkrétně sděluje, jak chránit (organizovat a distribuovat) konkrétní aktiva, stanovuje konkrétní bezpečnostní cíle, vyjmenovává konkrétní hrozby zjištěné analýzou rizik, definuje konkrétní bezpečnostní opatření, tj. funkce prosazující bezpečnost – autorizace, autentizace, audit, klasifikace dat, řízení přístupu apod., které jsou již implementovány nebo se musí implementovat.

Systémová bezpečnostní politika IT musí být v souladu s celkovou bezpečnostní politikou organizace a s celkovou bezpečnostní politikou IT organizace, musí respektovat současný stav provozovaného systému i jeho plánovaných rozšíření. Z celkové bezpečnostní politiky IT přebírá stanovení kategorie minimální síly bezpečnostních mechanismů a konkrétně definuje, jak implementovat bezpečnostní funkce (šifrováním, elektronickými podpisy apod.).

Vrcholový management organizace musí schválit doporučení pro tvorbu systémové bezpečnostní politiky IT stanovující přijatelná reziduální rizika, charakter přijímaných opatření pro minimalizaci rizik.

Ten, kdo vypracovává systémovou bezpečnostní politiku, vychází dále z vymezení hranice zabezpečovaného prostředí z hlediska aplikačních cílů IS a jeho poslání, z kvantifikovaných odhadů nepříznivých dopadů na chod organizace v důsledku nedostupnosti služeb IT, odmítnutí jejich provedení, resp. omezení jejich výkonu, neautorizovaných modifikací informací a/nebo softwaru a neautorizovaných odhalení důvěrných informací, včetně kvalifikovaných odhadů dopadů realizací těchto hrozeb na pověst organizace, ohrožení života, soukromí atd. Mezi další východiska se řadí výše investic věnovaných na zabezpečení IS a stanovené meze nákladové zátěže vznikající zabezpečováním IS. Autoři systémové bezpečnostní politiky musí znát zranitelná místa, hrozby a rizika, její realizátoři musí mít k dispozici přehled dostupných bezpečnostních opatření a jejich cen a charakteristiky externích dodavatelů a vztahů organizace s nimi.

Pokud je organizace nebo její IS příliš rozsáhlý a různorodý, je vhodné vypracovat samostatně systémovou bezpečnostní politiku fyzické ochrany, systémovou bezpečnostní politiku

technické ochrany (elektronika, software), personální systémovou bezpečnostní politiku, komunikační systémovou bezpečnostní politiku atd.

- *Fyzická systémová bezpečnostní politika*
  týká se ochrany fyzických aktiv, budov, počítačů, médií, prevence krádeží, prevence přírodních, objektivních útoků.
- *Personální systémová bezpečnostní politika*
  je součástí širší personální politiky a jejím cílem je pokrytí hrozeb představovaných zaměstnanci, dodavateli, zákazníky, nezkušenými uživateli, hackery, profesionály, špióny a ochrana vlastních zaměstnanců organizace.
- *Komunikační systémová bezpečnostní politika*
  ochrana poštovních zásilek, faxu, telefonů, hlasové komunikace, přenosu dat.
- *Provozní systémová bezpečnostní politika*
  specifikuje program školení – zvyšování vědomosti potenciálních obětí o možných útocích, postupy při uplatňování preventivních bezpečnostních opatření, postupy při detekci útoků a ochranu těchto postupů, havarijní plány a vývoj metod prevence a detekce.

Generickou strukturu dokumentu, který je prezentací systémové bezpečnostní politiky a výchozím materiálem pro zahájení její implementace do bezpečnostního programu, přibližuje následující osnova:

- *Analýza současného IS respektující použité IT.*
- *Výsledky analýzy rizik IS.*
- *Výsledky analýzy zranitelných míst IS.*
- *Popis hrozeb pro IS.*
  Aby se zajistilo, že popis hrozeb bude vyčerpávající, je vhodné postupovat podle předem stanoveného systému. Může se použít aplikačně orientované třídění (ztráta důvěry, odposlech, zlomyslný operátor, modifikace dat, maškaráda, zneužití autorizace...) nebo generické třídění podle nějaké normy (třídění podle použitých bezpečnostních funkcí).
- *Technická bezpečnostní politika.*
  Uvádí se konkrétní zákony, standardy, normy, pravidla, použité praktiky pro řízení zpracování citlivých informací, pro používání hardwaru, pro používání softwaru, de jure a de facto normy. .
- *Personální bezpečnostní politika.*
- *Administrativní bezpečnostní politika*.
  Uvádí se soubor vnitroorganizačních norem a předpisů.
- *Udržovatelnost IS z hlediska bezpečnosti.*
  Jedná se o výčet kritických činností a odpovídajících opatření pro akce typu registrace uživatelů, inovace softwaru apod.
- *Formální model bezpečnosti IS.*
  Uvádění formálního modelu je volitelné podle toho, zda se požaduje odpovídající úroveň zaručitelnosti bezpečnosti IS.
- *Definice souboru relevantních bezpečnostních opatření.*
  Uvádějí se specifikace bezpečnostních funkcí zabezpečovaného IS včetně identifikace jimi pokrývaných hrozeb.

- *Použité bezpečnostní mechanismy.*
  Vhodně systematicky tříděný výčet, např. podle kategorií – logické, technické, fyzické bezpečnostní mechanismy.
- *Havarijní plán.*
- *Bezpečnostní dokumentace.*
- *Plán implementace systémové bezpečnostní politiky, bezpečnostní program*.
  Uvádějí se detailní pracovní plány implementace přijatých bezpečnostních funkcí, priority, náklady a časové plány, specifikace projekčních aktivit (závazné zdroje a odpovědnosti, kontrolní dny, zprávy o stavu řešení, oponentury). Součástí bezpečnostního programu je plán školení pro celý tým IT organizace, kam patří vývojáři IS, provozní pracovníci, bezpečnostní manažer, bezpečnostní správci, pracovníci odpovědní za autorizaci ostatních pracovníků, koncoví uživatelé atd. Stanovují se provozní a správní procedury a podmínky akreditace bezpečnostního programu, tj. připraví se hodnocení jeho implementace.

1.3.4.3 Metodika procesu vytváření bezpečnostních politik

Projekční tým celkové a systémové bezpečnostní politiky musí tvořit odborníci, jejichž znalosti pokrývají alespoň následující oblasti:

- bezpečnostní architektury výpočetních (distribuovaných, otevřených) systémů
- bezpečnostní personální struktury organizace
- zásady udržení fyzické bezpečnosti
- zákony, vyhlášky a nařízení související s posláním organizace
- zásady etiky chování z hlediska manipulace s informacemi
- způsoby zainteresování zaměstnanců organizace na bezpečnosti
- principy klasifikace důvěrnosti dat
- mechanismy řízení přístupu
- obecné kryptografické metody zabezpečení integrity a důvěrnosti
- metody zabezpečení integrity a důvěrnosti při přenosu dat
- možné hrozby a jim odpovídající rizika v cílovém prostředí
- metody správy rizik – procesů určování nejistých (nepředvídatelných) událostí ovlivňujících škody na aktivech a určování adekvátních opatření
- metody identifikace a ohodnocování aktiv, metody analýzy rizik a nástroje pro jejich automatizaci (výčtové seznamy, programy typu CRAMM apod.)
- zásady tvorby havarijních plánů
- metody hodnocení bezpečnosti.

Proces tvorby bezpečnostní politiky není jednorázový. Dobrá bezpečnostní politika nikdy nevzniká jednorázovou akcí, neboť se mění chráněná aktiva, mění se informační technologie, mění se motivace a zkušenosti útočníků atd. Životní cyklus tvorby bezpečnostní politiky lze zjednodušeně vyjádřit následujícími (opakovaně) prováděnými kroky

1. posouzení vstupních vlivů
2. analýza rizik

3. vypracování bezpečnostní politiky
4. implementace bezpečnostní politiky
5. nasazení bezpečnostní politiky, kontrola její účinnosti a vyslovování závěrů.

1.3.5 Analýza rizik

Nejdůležitější etapou stanovení bezpečnostní politiky je *analýza rizik.* Analýza rizik předchází vlastnímu stanovení bezpečnostní politiky. Jejím cílem je:

- identifikování, zvládnutí, odstranění nebo minimalizace událostí, které mají nežádoucí vliv na aktiva organizace
- zjištění hrozeb a rizik, kterým je IS vystaven
- určení, jaké škody mohou útokem vzniknout
- určení, která opatření rizika hrozeb odstraní nebo alespoň minimalizují, a co jednotlivá opatření stojí.

Projektant bude v této fázi pracovat s pojmy hrozba, bezpečnostní opatření, výše potenciálně způsobených škod a cena bezpečnostního opatření. Především ho bude zajímat, jaká jsou rizika plynoucí z jednotlivých hrozeb.

Náplň analýzy rizik lze definovat jako proces porovnávání odhadovaných rizik proti přínosu a/nebo ceně možných bezpečnostních opatření, stanovení implementační strategie v rámci vypracovávání systémové bezpečnostní politiky tak, aby byla v souladu s celkovou bezpečnostní politikou a s posláním organizace. Generický model postupu při analýze rizik lze vyjádřit výčtem následujících kroků:

1. identifikace a ocenění aktiv
2. nalezení zranitelných míst
3. odhad pravděpodobností využití zranitelných míst
4. výpočet očekávaných (ročních) ztrát
5. přehled použitelných opatření a jejich cen
6. odhad ročních úspor aplikací zvolených opatření.

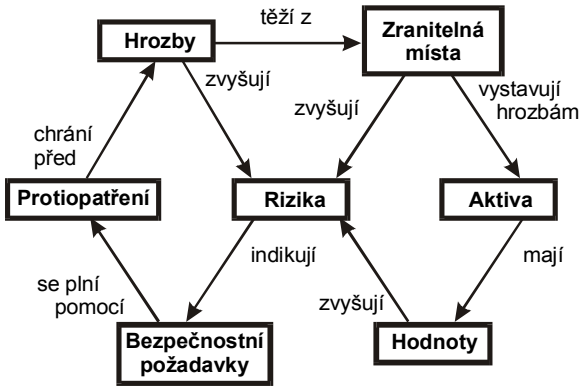
Význam důkladného provedení analýzy rizik je zásadní. U zaměstnanců se poznáním výsledků analýzy zvýší pocit nutnosti bezpečnostního uvědomění a sounáležitosti k organizaci a k provozovanému IS. Explicitně se identifikují aktiva, zranitelná místa a nutná opatření. Provedením inventury a stanovením reálné hodnoty aktiv z hlediska možných škod porušením důvěrnosti, integrity, pohotovosti a nepopiratelnosti se upřesní požadavky na nutná bezpečnostní opatření. Získají se důvěryhodné podklady pro opodstatnění pořídit nová bezpečnostní opatření nákupem a případně se zjistí nutnost vývoje nových bezpečnostních opatření. Ověří se, zda výše nákladů na zabezpečení je úměrná. Vzájemné vztahy mezi pojmy používanými při analýze rizik ilustruje obr. 1.2.

Výsledkem analýzy rizik je tedy stanovení, kterým hrozbám je IS vystaven, jaká jsou rizika jednotlivých hrozeb, jaké škody mohou vzniknout a která opatření hrozby odstraní. Generický postup při analýze rizik začíná evidencí aktiv a požadavků na bezpečnost, pokračuje vyhledáním zranitelných míst, určením hrozeb a odhadnutím rizik a výše potenciálně způsobených škod, zjištěním cen vhodných bezpečnostních opatření a jejich volbou (doporučením).

Proč se vlastně musí, resp. je vhodné, zjišťovat rizika? Protože se explicitně identifikují aktiva IS, zranitelná místa a bezpečnostní opatření. Inventura dostupných aktiv je vesměs vždy přínosná. Zjištěním výše rizik a hodnot aktiv se upřesní požadavky na bezpečnostní opatření

v IS a opodstatní se pořízení ochranných opatření. Mnohdy se zjistí nutnost vývoje nových ochranných opatření. Ověří se, zda výše nákladů na zabezpečení IS je úměrná.

Různé strategie provádění analýzy rizik se vzájemně liší podle snahy o dosažení vyrovnanosti časových a finančních nákladů, potřebné přesnosti odhadu rizik a adekvátnosti volby bezpečnostních opatření.



Obr. 1.2 Vzájemné vztahy ve správě rizik

Provádí se:

- *Orientační analýza rizik*
  Typicky se používá jako součást budování celkové bezpečnostní politiky. Jejím výsledkem je rozhodnutí o volbě jedné ze čtyř následujících strategií analýzy rizik vhodných pro tvorbu především konkrétní systémové bezpečnostní politiky
- *Elementární analýza rizik*
  Je založena na převzetí opatření na základě analogie podobných systémů a ze všeobecných norem. Její předností je vynakládání zanedbatelných finančních a časových nákladů na provedení analýzy rizik a na volbu bezpečnostních opatření. Mohou se ale volit zbytečně drahá a silná nebo naopak nedostatečně silná opatření a nelze snadno odhadnout dopad změn konfigurace IS na jeho bezpečnost.
- *Neformální analýza rizik*
  Jedná se o provedení analýzy rizik na základě znalostí jednotlivců – odborníků na bezpečnost (interních nebo externích) bez použití standardních strukturovaných metod. Její předností je vynakládání malých finančních a časových nákladů na analýzu rizik a na volbu bezpečnostních opatření. Je pro ni charakteristické rychlé provedení, je vhodnou strategií pro malé organizace. Trpí vyšší pravděpodobností opomenutí některých rizik a snadným ovlivněním voleb nedoloženými subjektivními názory řešitelů. Obtížně se dokazuje oprávněnost zvolených bezpečnostních opatření a jejich síla a rovněž nelze snadno odhadnout dopad změn konfigurace IS na jeho bezpečnost.
- *Detailní analýza rizik*
  Provedení analýzy rizik použitím standardizovaných strukturovaných metod ve všech šesti zmíněných fázích (identifikace a ocenění aktiv, nalezení zranitelných míst …). Její předností je malá pravděpodobnost opomenutí některých rizik, nesnadné ovlivnění voleb subjektivními názory řešitelů, dokazatelnost oprávněnosti zvolených bezpečnostních opatření a jejich síly a to, že lze snadno odhadnout dopad změn konfigurace IS na jeho bezpečnost. Musí se počítat s vynaložením vysokých

finančních i časových nákladů na provedení analýzy rizik a na volbu bezpečnostních opatření. Strategie je poměrně náročná na odbornost řešitelů.

- *Kombinovaná analýza rizik*
  Systémy IT organizace se při orientační analýze rizik rozdělují na kritické a na ostatní a provedení analýzy standardizovanými strukturovanými metodami ve všech šesti fázích se předepisuje jen pro kritické systémy IT a pro ostatní systémy IT se předepisuje provedení elementární nebo neformální analýzy rizik. Kladem je dosažení optimální výše nákladů vynaložených na analýzu rizik. Neodpovědné provedení orientační analýzy rizik může však opominout některé systémy IT, pro které bylo třeba provést detailní analýzu rizik nebo donutit k neadekvátnímu vynaložení nákladů na nepotřebné detailní analýzy rizik.

Určování hodnoty identifikovaných aktiv se provádí z hlediska dostupnosti, tj. náklady organizace, když se něco nerealizuje, z hlediska důvěrnosti, tj. náklady organizace, když se důvěrná citlivá informace neoprávněně zveřejní, z hlediska integrity, tj. náklady organizace, když dojde k porušení autenticity, přesnosti, úplnosti dat nebo softwaru. Každé aktivum IS je vhodné posuzovat z hlediska škod na důvěrnosti, integritě a dostupnosti samostatně a nakonec jednotlivé typy škod kumulovat. Při hledání zranitelných míst se mimo jiné kladou otázky typu:

- Co způsobí přírodní a fyzické katastrofy?
  Požár, bouře, záplava, výpadek energie, poruchy komponent atd.
- Co může způsobit zásah zvenčí?
  Zásah přes síť, přes komutované spoje, hackeři, návštěvníci, odvoz odpadu atd.
- Co může působit záměrný zlomyslný zásah zevnitř?
  Zásah vyvolaný vlastními zaměstnanci, podplácením, zvědavostí.

Odhad rizik obvykle vychází z obecných statistik, ze kterých se lze však obvykle dozvědět pouze jak často nastávají požáry, přírodní katastrofy, jak často dochází k podvodům, loupežím a krádežím v daném prostředí. Tyto informace se pak upřesňují podle statistik konkrétních systémů, zjišťují se počty poruch, neoprávněných přístupů nebo velikosti souborů. Odhadují se četnosti za daný časový interval, obvykle rok vzhledem k ročnímu finančnímu vyhodnocování, případně se odhadují pravděpodobnosti jednotlivých událostí. Pokud nejsou tyto statistické informace dostupné, je třeba vyvolat diskuse nezávislých odborníků. Při výpočtu očekávaných ročních ztrát obvykle nebývá problematické ocenění hardwaru a softwaru, problematické bývá určení ceny dat. Zde je potřeba vzít do úvahy, že umožnění neautorizovaného přístupu ke státnímu tajemství může skončit i vězením, že umožnění neautorizovaného přístupu k výrobním a obchodním údajům má za následek zvýhodnění konkurence, že umožnění neautorizovaného přístupu k bankovním datům bude mít za následek zničení pověsti, že opoždění dostupnosti služeb může mít za následek placení penále, ztrátu trhu, ztrátu zákazníka, možná i smrt. Do ceny dat je třeba zakalkulovat cenu jejich opětovného pořízení nebo rekonstrukce. Při identifikaci možných cen aktiv je dále třeba si klást otázky typu:

- Které právní závazky nutí organizaci zajišťovat důvěrnost a integritu dat?
- Způsobí zpřístupnění těchto dat škodu osobě či organizaci?
- Může být organizace za to stíhána?
- Dojde ke ztrátě pozice organizace na trhu?
- Může konkurence získat výhody nepoctivým způsobem?
- Dojde k obchodním ztrátám?
- Jaký je psychologický dopad nedostupnosti služby?
- Hrozí ztráta pověsti?

- Hrozí ztráta obchodních šancí a pokud ano, tak u kolika a jakých zákazníků?
- Lze zpracování dat opozdit?
- Lze zpracování dat provést jinde?
- Pokud ano, kolik za to zaplatíme?
- Jaká je cena zpřístupněných programů a dat pro jiné osoby nebo organizace?
- Kolik by byla konkurence ochotna za ně zaplatit?
- Co vznikne za problémy, když dojde ke ztrátě dat?
- Jsou data nahraditelná?
- Lze data rekonstruovat?
- Kolik dá práce rekonstrukce nebo opětovné pořízení dat?

Na závěr analýzy rizik se vypracuje přehled použitých opatření a jejich cen a provede se odhad ročních úspor získaných aplikací určených bezpečnostních opatření. V současné době jsou už k dispozici pro automatizaci detailní analýzy rizik standardizované nástroje, různé výčtové seznamy, speciální programové systémy.

1.3.6 Havarijní plán

1.3.6.1 Účel a struktura

Havarijní plán určuje, co dělat po odhalení útoku (bezpečnostního incidentu) a jak postupovat, aby se udržela kontinuita činnosti organizace. Stejně jako v případě obou typů bezpečnostních politik IT organizace, i při popisu havarijního plánu uvedeme pouze jeho generické rysy, které doplníme několika příklady s výraznou vypovídací schopností.

Havarijní plán určuje místa skladování a počty náhradních dílů, místa skladování a způsob organizace záloh dat, obsah pohotovostního skladu technických a softwarových náhrad, metodiku udržování aktuálnosti skladů dat, softwaru, hardwaru a metodiku aktualizace a testování hardwaru. Součástí havarijního plánu jsou návody, jak postupovat v poskytování služeb po zjištění útoku – *plán činnosti po útoku*[17], dohody o poskytování náhradních řešení informaticky orientovaných úkolů organizace, a dohody o uvedení dat IS do původního stavu po havárii (incidentu). Proto je jeho součástí i návod, jak postupovat při obnově činnosti IS po havárii – *plán obnovy*[18]. Optimální havarijní plán se „vybrušuje“ mnohdy i po dobu mnoha let, a protože IT i jejich okolí se vyvíjejí, jeho součástí bývá i specifikace způsobu testování a prověřování aktuálnosti havarijního plánu. Důvěryhodnost havarijního plánu zvýší publikace potvrzení o úspěšné oponentuře havarijního plánu. Jestliže se některé hrozby řeší pojištěním, definice systému pojištění je součástí havarijního plánu.

1.3.6.2 Plán činnosti po útoku

Plán činnosti po útoku bývá souborem scénářů pro situace vzájemně se lišící délkou přerušení činnosti, ztrátou různých typů vybavení, omezením přístupu do areálu organizace, potřebou návratu do původního stavu před útokem apod. Pro další zkvalitňování bezpečnosti plán činnosti po útoku obvykle předepisuje provedení analýzy incidentu, její dokumentace pak musí obsahovat informace o tom, co se stalo a kdy, zda se řešila reakce podle předem stanoveného plánu.

[17] Contingency Plan
[18] Disaster Recovery Plan

Po vyřešení incidentu je potřeba přijmout závěr, zda byl plán činnosti po útoku řešitelům dostupný, zda byl efektivní, co příště dělat jinak a zda je potřeba plán modifikovat.

1.3.6.3 Průběh reakce na incident

Jakmile dojde k útoku a narušení bezpečnosti IS, odhalí se, jak okamžitě reagují odpovídající *týmy 1. reakce*. Cílem jejich reakcí je ambulantní zásah, zajištění činnosti ve stavu nouze[19]. Týmy 1. reakce mají k dispozici plán činnosti ve stavu nouze, tj. návody pro činnosti po detekci útoku, seznamy adres, telefonů, e-mail adres apod. Týmy 1. reakce musí informovat pracovníka odpovědného za vyřešení incidentu, kterým je podle okolností bezpečnostní manažer organizace, bezpečnostní správce systému, člen vrcholového managementu apod.

Týmy pro řešení incidentu mají k dispozici směrnice definující postupy řešení, definice lokalit archivů, definice zdrojů náhradních dílů a provádějí posouzení důsledků útoku.

Ve třetí fázi nastupují *týmy pro obnovu*, které uvádějí IS do standardního stavu. Musí mnohdy mít jak speciální dovednosti, tak i speciální vybavení.

1.3.6.4 Plán obnovy

Plán obnovy musí obsahovat kritéria definující, co se chápe havárií, odpovědnosti za aktivaci obnovy, odpovědnosti za aktivaci dílčích činností podle plánu obnovy a návody k provádění činností podle plánu obnovy. V plánu obnovy je potřeba prosadit obvykle následující zásady:

- Je potřeba provést segmentaci informačních zdrojů podle priority obnovy
  - Nejkritičtější data a služby se obnovují nejdříve, a je proto potřeba zavést nějakou klasifikaci priorit, např.: nejkritičtější zdroje z hlediska poslání organizace se obnovují do 30 minut, ostatní kritické zdroje do 2 hodin a zbývající zdroje během 24 hodin. Zbývající zdroje lze dále kategorizovat na prioritní zdroje obnovované do 6 hodin, žádoucí obnovované do 12 hodin a zdroje vhodné pro obnovu do 24 hodin.
  - Důležité je, aby byla zavedena shodná pořadí obnovy ve všech odděleních organizace. Odpovědného pracovníka za vymezení kritičnosti a priorit stanovuje celková bezpečnostní politika. Stejná pořadí obnovy v plánu obnovy stanovují systémové bezpečnostní politiky.
- Vyhodnocování kritičnosti a priorit multiuživatelských aplikací se provádí alespoň jednou ročně
  - Vypracovávají se seznamy kritických aplikací tříděné podle priorit obnovy.
- Existuje plán činnosti organizace ve stavu nouze
  - Organizace musí mít vypracován plán udržení činnosti kritických aplikací při přerušení nebo při degradaci služeb.
- Tým 1. reakce je potřeba udržovat v pohotovosti
  - Udržuje se přehled o stavu týmu, trénuje se schopnost týmu bezprostředně zahájit svoji činnost – jeho schopnost reagovat na odhalení viru, na odhalení činnosti hackera atd.
  - Přirozeným cílem je výchova týmu k minimalizaci publicity útoku.

[19] Je potřeba rozlišovat mezi stavem nouze a havárií (katastrofou). Stavem nouze může být. výpadek bankomatu v pátek v poledne – vyžaduje se sice okamžitá pozornost, incident je však bez dlouhodobě platných a vážných důsledků. Katastrofou je požár nebo záplava.

- Existují definice činností po podezření na průnik do systému
  - Obsahují typicky nepominutelné (minimální) úkoly pro správce systému, které jsou často protichůdné vůči požadavkům a tlaku správy uživatelů, postupy při odstavení kompromitovaného počítače od ostatní sítě, postupy pro uschování záznamů o kritických činnostech uživatelů z hlediska bezpečnosti, návody jak dělat identifikace provedených změn, návody pro obnovu softwaru z důvěryhodného zdroje, návody pro re-inicializaci systému řízení přístupu (změna hesel …) atd.
- Je zaveden systém varování o podezření na průnik útočníka či jiné porušení bezpečnosti
  - Tento systém musí být nejen zaveden, ale i udržován a testován. Jeho součástí jsou seznamy potřebných čísel telefonů či faxů, e-mailových adres, faxů a osobních kontaktů nutných pro mobilizaci členů týmů 1. reakce, včetně jejich pobytů mimo pracoviště.
  - Cílem takového systému je minimalizace šance úspěchu širokého průniku.
- Je zaveden systém sběru informací o podezření na porušení bezpečnosti
  - Takový systém podporuje stav bdělosti u zaměstnanců, partnerů a konzultantů. Týká se takových skutečností, jakými jsou oznámení o poruše disku, oznámení o ztrátě souboru nebo oznámení o krádeži.
- Jsou stanoveny povinnosti zaměstnanců při účasti na procesu obnovy po porušení bezpečnosti
  - Povinnosti se mohou stanovovat u zaměstnanců, nikoli u partnerů nebo konzultantů. Povinnosti se nemohou křížit se společenskými zájmy vyšší důležitosti, jakými je např. činnost v rámci Červeného kříže při záplavách apod.
- Vyhodnocování pokrytí funkcí předepsaných v celkové bezpečnostní politice se provádí typicky s roční periodou
  - Vyhodnocování provádí vrcholový management a jeho součástí je udržování zástupnosti expertů v týmu obnovy pro kritické aplikace.
- Minimalizace automatizace znamená minimalizace ceny
  - Co lze udělat manuálně, je vhodné manuálně dělat.
- Je zavedena periodicita archivace dat
  - Plán obnovy řeší rotaci použití archivního média (dědeček–otec–syn). Periodicita je pochopitelně aplikačně závislá, může být denní, týdenní nebo třeba i měsíční.
- V současné době nabývá na významu archivace kritických dat na mobilních počítačích
  - Přirozenou nutnosti je provádět potřebné archivace před cestou.
- Musí být zaveden systém řízení přístupu k archivním kopiím
  - Koncový uživatel nemůže archivační systém využít k obejití autorizace přístupů. To vede k šifrovaným uložením archivních souborů a vyžaduje to periodické prohlížení záznamů o činnostech uživatelů bezpečnostním správcem.
- Je třeba zachovat důvěrnost off–line uschovávaných archivních kopií
  - Typickým opatřením je šifrované uložení takových dat i mimo prostory organizace a je tudíž potřebné mít zabezpečenou dostupnost klíčů při jejich obnově. Samozřejmé je ošetření povinnosti zachovávat důvěrnost dat archivačním týmem.
- Násobnost archivních kopií (alespoň duplicita)
  - Dříve než se použije archivní kopie pro obnovu, je potřeba mít alespoň jednu její kopii uloženou v archivu. Kritická data se obvykle trvale uchovávají mimo organizaci alespoň ve dvou kopiích.

- Nepominutelná je existence inventurní evidence archivních kopií
  - Musí se zavést systematizace značení kopií a zajistit on–line udržování přehledů.
- V síťových prostředích je vhodná automatizace archivace na serveru LAN
  - Musí se řešit trvalá dostupnost, tj. zapojení připojených koncových počítačů pro automaticky prováděnou archivaci např. „v nočním provozu“, aby bylo možné provádět archivaci automaticky bez zásahu koncového uživatele. Musí se ovšem vyřešit problém přístupových práv ze serveru ke stanicím chráněným heslem.
- Likvidace dále nepotřebných informací je zárukou zachování důvěrnosti
  - Existují mnohé legislativní závazky pro stanovení periody uchovávání kopií dat. Za jejich znalost běžně odpovídá právní oddělení organizace.
- Pro úspěšnou obnovu je důležitá volba archivního média
  - Určení archivního média obvykle předpisuje systémová bezpečnostní politika, stejně tak předepisuje i periodicitu testování použitelnosti archivního média.
- Plán obnovy musí splňovat požadavky dané kvantitativním cílem dostupnosti zdrojů
  - Uživatelé musí mít např. sdílené počítače dostupné po dobu rovnou alespoň 95% pracovní doby ve výrobní organizace, po dobu rovnou alespoň 99,98 % pracovní doby v telefonní společnosti apod. Tyto limity normálně stanovuje vrcholový management v celkové bezpečnostní politice.
- Zálohování kritických zdrojů lze řešit několika způsoby
  - *Horká záloha* představuje dostupnost plně provozuschopného centra obnovy po katastrofě, které je plně vybaveno technickými i logickými prostředky (hardware, software, komunikace) i technickým personálem. Předpokládá se restart provozu řádově do několika hodin a schopnost poskytovat služby i po dobu několika měsíců.
  - *Mobilní horká záloha* může být řešena např. instalací IT v dobře vybaveném „karavanu“.
  - *Teplá záloha* znamená, že lokální koncová pracoviště (displeje, tiskárny) jsou rekonfigurovatelná tak, aby umožnila přístup do vzdáleného centra obnovy po katastrofě.
  - *Studená záloha* požaduje, aby si organizace po katastrofě mohla připravit jiné pracoviště vlastním vybavením, doba reakce je obvykle několik dní.
  - Organizace může provozovat duální (záložní) datové centrum umístěné v geograficky vzdálené budově.
- Pro stanovení ekonomické optimálnosti plánu obnovy je potřeba vzít do úvahy, čím je dána cena kopie
  - Na cenu kopie má vliv výše možných ztrát (roční ztráty nebo roční náklady) a náklady na pořízení, náklady na skladování kopií. Velký problém je řešení zálohování on-line systémů provozovaných 24 hod., kdy se musí využívat techniky typu kontrolní body, žurnál transakcí, tandemové nebo zrcadlové zpracování.
- Systémová bezpečností politika předepisuje správu záloh dat
  - Kde se udržují, což je ovlivněno energetickou závislostí, fyzickou bezpečností, složitostí řízení provozu. V jaké násobnosti se udržují a jak se distribuují.
- Zálohy dokumentace, manuálů
  - Opět systémová bezpečnostní politika určuje, kde jsou uloženy a počet jejich kopií. Doporučuje se udržovat „zlatou kopii“, která slouží pouze k reprodukci provozních kopií a normálně se nepoužívá.

- Zajištění dostupnosti hardwaru
  - Požaduje existenci případně smluvního systému oprav a údržby hardwaru, provozování náhradních zdrojů apod.

1.3.7 Bezpečnostní audit

Mezi bezpečnostní zásady usnadňující prevenci útoků patří prokazatelná (individuální) odpovědnost za akce, prováděné jednotlivými uživateli IS – účtování jejich činnosti. Je zaznamenávána relevantní informace o činnostech a procesech, vykonaných uživatelem nebo jeho jménem, takže následky takových činností mohou být s dotyčným uživatelem později prokazatelně propojeny a ten může být učiněn odpovědným za svou činnost. Relevantní události musí být zaznamenávány tak, aby zaznamenávací mechanismy nemohly být zničeny a aby údaje sloužící k autentizaci a autorizaci uživatele byly bezpečně uchovány.

Důležitou zásadou je oddělení povinností výkonných a kontrolních. Audit musí být nezávislý na prosazování provozní bezpečnosti a hlavně musí být zajištěno, že se audit skutečně provádí. Auditní postup můžeme charakterizovat následujícími kroky:

- fáze detekce – je zjištěna událost, která má vztah k bezpečnosti
- fáze rozlišovací – určuje, zda je nutné zaznamenat událost do bezpečnostního auditního záznamu nebo spustit bezpečnostní poplach
- fáze zpracování bezpečnostního poplachu – je spuštěn bezpečnostní poplach nebo je vydána bezpečnostní auditní zpráva
- fáze analýzy – událost, vztahující se k bezpečnosti je posouzena v kontextu dříve zjištěných zpráv, zaznamenaných v bezpečnostním záznamu a je určen průběh činnosti
- fáze agregační – distribuované záznamy dílčích bezpečnostních auditních záznamů jsou spojeny do jednoho bezpečnostního auditního záznamu
- fáze generování zprávy – z bezpečnostních auditních záznamů jsou vytvořeny auditní zprávy
- fáze archivace – dílčí části bezpečnostního auditního záznamu jsou uloženy do archivu bezpečnostních auditních záznamů.

Politika bezpečnostního auditu definuje, co jsou události, které mají vztah k bezpečnosti a pravidla, která mají být použita pro sběr, zaznamenání a analýzu různých událostí, které mají vztah k bezpečnosti. Pokud mají být bezpečnostní auditní záznamy používány jako právně přípustné důkazy, klade to specifické požadavky na jejich uložení a ochranu, především před jejich neoprávněnou změnou. Auditní záznamy je vhodné ukládat na médium, na které je možný zápis pouze jednou, protože pak není možné záznam vymazat nebo měnit přepsáním média.

Ochrana bezpečnostního auditu je zaměřena především na dostupnost této služby. Informace určená pro bezpečnostního auditora ztrácí po určité době svoji hodnotu. Událostí relevantních pro bezpečnost může být mnoho, a proto je důležitá účinná analýza událostí. Obvykle se používá nějaký filtrovací mechanismus, který se řídí předem stanovenými kritérii. Kritéria typicky definují čas, typ události a entitu, která událost způsobila.

2. Bezpečnostní funkce

2.1 Bezpečnostní funkce podle kritérií ITSEC

Kritéria pro hodnocení bezpečnosti IT ITSEC (Information Technology Security Evaluation Criteria) byla vytvořena v roce 1990 a vydána Úřadem pro oficiální publikace Evropského společenství a schválena jako doporučení v dubnu 1995. Jejich rysy a vlastnosti jsou popsány v poslední kapitole příručky.

2.1.1 Třídy funkčnosti ITSEC

Kritéria ITSEC, viz [ITSEC], specifikují sedm *tříd míry zaručitelnosti bezpečnosti IT* označovaných E0 až E6 reprezentujících vzrůstající úrovně důvěry a v příloze definují dalších deset *tříd bezpečnostní funkčnosti* F-xx. Třídy míry zaručitelnosti kladou požadavky na:

- proces vývoje IS
- prostředí vývoje IS
- provozní dokumentace IS
- provozní prostředí IS.

Pět tříd bezpečnostní funkčnosti F-C1, F-C2, F-B1, F-B2 a F-B3 odpovídá stejnojmenným třídám kritérií TCSEC, viz [TCSEC]. Zbylých pět tříd bezpečnostní funkčnosti je orientováno aplikačně. Na rozdíl od TCSEC, která vznikala pro vojenské prostředí a orientovala se zejména na ochranu důvěrnosti informace, jsou ITSEC koncipována mnohem obecněji a pokrývají částečně i požadavky na integritu a na dostupnost informace. Oproti TCSEC definují ITSEC navíc i způsob vedení dokumentace hodnoceného předmětu, způsob definování bezpečnostního cíle a způsob provádění hodnocení.

Zatímco pro požadavky na míru zaručitelnosti bezpečnosti je v kritériích ITSEC definováno sedm tříd míry zaručitelnosti bezpečnosti E0 až E6 a nepředpokládá se, že by uživatelé kritérií definice těchto tříd měnili nebo si definovali své vlastní třídy, u požadavků na bezpečnostní funkčnost je tomu jinak. U těchto požadavků kritéria ITSEC nepředepisují žádnou apriori danou množinu tříd bezpečnostní funkčnosti. Místo toho pouze definují zásady, jak takovou třídu bezpečnostní funkčnosti vytvořit. Pro usnadnění práce uživatelům kritérií a pro kompatibilitu s jinými kritérii jsou v příloze kritérií ITSEC uvedeny příklady tříd bezpečnostní funkčnosti. Pět z těchto tříd bezpečnostní funkčnosti (třídy F-C1, F-C2, F-B1, F-B2 a F-B3) je hierarchických a přímo odpovídá požadavkům funkčnosti stejnojmenných tříd kritérií TCSEC. To umožňuje uživateli, který požaduje kompatibilitu s kritérii TCSEC, zvolit třídy ekvivalentní třídám kritérií TCSEC.

Zbylých pět tříd bezpečnostní funkčnosti (F-IN, F-AV, F-DI, F-DC a F-DX) nemá hierarchickou strukturu. Tyto třídy bezpečnostní funkčnosti jsou třídy se zvýšenými bezpečnostními požadavky v některé oblasti bezpečnosti – například F-IN je třída se zvýšenými požadavky v oblasti integrity, F-AV je třída se zvýšenými požadavky v oblasti dostupnosti atd.

Výše uvedené třídy funkčnosti jsou, na rozdíl od tříd míry zaručitelnosti bezpečnosti, pouze příklady. Nejsou závazné a mají sloužit pro usnadnění práce uživatelům kritérií ITSEC. Proto má uživatel kritérií několik možností, jak kategorizovat funkčnost produktu nebo systému.

První možností je, že uživatel přímo použije některou ze tříd bezpečnostní funkčnosti, uvedenou v kritériích ITSEC. V tomto případě si zpravidla vybere některou ze tříd, které jsou hierarchické a odpovídají třídám kritérií TCSEC.

Druhou možností je, že uživatel kritérií použije vhodné kombinace některých ze tříd bezpečnostní funkčnosti, uvedených v kritériích ITSEC. Tato možnost dává uživateli kritérií větší možnosti a dovoluje mu vytvořit třídu bezpečnostní funkčnosti, která nejlépe odpovídá jeho požadavkům.

Třetí možností je, že uživatel kritérií použije některou, již vytvořenou třídu bezpečnostní funkčnosti, která není součástí kritérií ITSEC, ale je vytvořena v souladu s těmito kritérii a nejlépe vyhovuje požadavkům uživatele.

Konečně poslední, čtvrtou možností je případ, kdy si uživatel kritérií vytvoří sám vlastní třídu bezpečnostní funkčnosti, která je v souladu s požadavky kritérií ITSEC. Tento případ nastane zejména v okamžiku, kdy je hodnocený předmět natolik specifický, že jsou všechny výše uvedené cesty neschůdné. Vzhledem k pracnosti tohoto způsobu stojí však vždy za úvahu, zda skutečně nelze využít některý ze tří výše uvedených případů.

2.1.2 Specifikace funkcí prosazujících bezpečnost podle ITSEC

Specifikace funkcí prosazujících bezpečnost (stanovení požadavků na bezpečnostní funkčnost) by měla být zpracována podle odstavců 2.18 až 2.64 kritérií ITSEC. V případě, že se uživatel kritérií rozhodne vytvořit si vlastní třídu funkčnosti, doporučuje se, aby použil systém generických záhlaví odstavců se specifikacemi, která jsou definována v kritériích ITSEC. Jedná se o následující generická záhlaví.

2.1.2.1 Identifikace a autentizace

Toto záhlaví musí pokrýt všechny funkce, které umožní přidávání nových a rušení starých identifikací uživatelů. Podobně sem musí patřit všechny funkce, které generují, mění nebo umožňují autorizovaným uživatelům prohlédnout si (zkontrolovat) autentizační informace požadované k ověřování identity uživatelů. Zahrnuje rovněž funkce, které zajišťují integritu autentizačních informací nebo brání před neautorizovaným užitím této informace. Pokrývá také funkce, které omezují příležitost k opakovaným pokusům o zadání falešné identity.

2.1.2.2 Řízení přístupu

Toto záhlaví musí pokrýt všechny funkce, určené k vytváření seznamů nebo pravidel, kterými se řídí přístupová práva pro různé typy přístupů. Patří sem funkce dočasně omezující přístup k objektům, které jsou současně přístupné několika uživatelům nebo procesům, přičemž musí být zachována konzistence a neporušenost těchto objektů. Patří sem také funkce, které zajistí vytvoření implicitních přístupových seznamů nebo přístupových pravidel k objektům. Musí obsahovat všechny funkce, které řídí šíření přístupových práv k objektům. Musí zahrnovat rovněž funkce řídící dedukci informací, které vzniknou agregací dat z jinak legitimních přístupů.

2.1.2.3 Účtovatelnost

Toto záhlaví musí pokrýt všechny funkce, které se vztahují ke shromažďování informací o činnostech a událostech relevantních z hlediska bezpečnosti, k ochraně a analýze takových informací. Některé funkce mohou splňovat požadavky, které mají vztah k účtování i k auditu a spadají tak pod obě záhlaví. Takové funkce mohou být zahrnuty pod jedno záhlaví a přitom musí být odkazovány i pod záhlavím druhým.

2.1.2.4 Audit

Toto záhlaví musí obsahovat funkce určené k manuálnímu nebo automatickému zkoumání protokolu o relevantních událostech v IS z hlediska bezpečnosti, ke shromažďování, ochraně a analýze takových informací. Prováděné trendové analýzy mohou také zahrnovat detekci potenciálních hrozeb bezpečnosti ještě předtím, než dojde k útoku. Některé funkce mohou splňovat požadavky na prokazatelnost přístupu i audit, takže mají vztah k oběma záhlavím. Takové funkce mohou být uváděny pod jedním záhlavím a zároveň musí být odkazovány i pod druhým záhlavím.

2.1.2.5 Opakované užití

Toto záhlaví musí pokrýt všechny funkce určené k inicializaci nebo mazání nepřidělených nebo opakovaně přidělených datových objektů. Obsahuje rovněž funkce určené k inicializaci nebo mazání opakovaně použitelných médií, jako jsou magnetické pásky a disky, nebo mazání výstupních zařízení, jako jsou obrazovky displejů, které nejsou právě užívány.

2.1.2.6 Přesnost

Toto záhlaví musí pokrýt všechny funkce, které určují, zavádějí a udržují přesnost vztahů mezi odpovídajícími daty. Obsahuje rovněž funkce, které zajišťují, že u dat přenášených mezi procesy, uživateli a objekty je možno detekovat nebo předcházet ztrátám nebo modifikacím a že není možno změnit předpokládaný nebo reálný zdroj a místo určení při přenosu dat.

2.1.2.7 Spolehlivost a dostupnost služeb

Toto záhlaví musí pokrýt všechny funkce, které zajišťují, aby zdroje byly přístupné a využitelné na základě požadavků autorizované entity (uživatele, procesu pod jeho jménem) a zabraňují interferencím mezi časově kritickými operacemi, případně tyto interference omezují.

Toto záhlaví musí zahrnovat funkce určené k detekci chyb a zotavení po chybě s cílem omezit vliv chyb na činnost produktu nebo systému, a minimalizovat tak přerušení nebo ztrátu služeb. Patří sem také všechny plánované funkce, které zajišťují, aby produkt nebo systém reagoval na externí události a produkoval výstupy v zadaných časových limitech.

2.1.2.8 Výměna dat

Toto záhlaví musí pokrýt všechny funkce, které zajišťují bezpečnost dat při přenosu komunikačními kanály. Doporučuje se, aby tyto funkce byly rozděleny podle záhlaví, vybraných z bezpečnostních architektur OSI (Open Systems Interconnection): autentizace, řízení přístupu, důvěrnost dat, integrita dat, nepopiratelnost.

2.2 Bezpečnostní funkce podle kritérií CTCPEC

Kanadská kritéria pro hodnocení bezpečnosti informačních systémů CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) se pokusila vytvořit prakticky použitelnější kategorizaci bezpečnostních funkcí. Je zde malá změna v terminologii – bezpečnostní funkce jsou v CTCPEC nazývány *bezpečnostními službami*. Tyto bezpečnostní funkce jsou rozděleny do čtyř kategorií: na bezpečnostní funkce zajišťující *důvěrnost*, *integritu*, *dostupnost* a *účtovatel-*

nost. V rámci každé bezpečnostní funkce je definováno několik *úrovní*. Úroveň bezpečnostní funkce je definovaný a měřitelný požadavek na granularitu nebo sílu bezpečnostní funkce vzhledem k určité množině hrozeb. Bezpečnostní funkce s vyšší úrovní poskytují účinnější ochranu proti hrozbám. Jednotlivé úrovně jsou hierarchické ve smyslu zvyšující se ochrany. To však neznamená, že následující úroveň musí nutně zahrnovat vše, co bylo požadováno v předchozích úrovních. Úrovně jsou vzestupně číslovány počínaje od nuly, která představuje nejnižší úroveň ochrany. Například bezpečnostní funkce *identifikace a autentizace*, která má zkratku WA, obsahuje úrovně WA-0, WA-1, WA-2 a WA-3.

2.2.1 Bezpečnostní funkce zajišťující důvěrnost

Bezpečnostní funkce v této kategorii jsou určeny proti hrozbám, které mohou zapříčinit odhalení informace neoprávněným subjektům (neoprávněné prozrazení informace). Jedná se o následující bezpečnostní funkce:

- *Skryté kanály* (obsahuje čtyři úrovně CC-0 až CC-3)
  Tato bezpečnostní funkce se zabývá identifikací a odstraňováním takových toků informace, které jsou v rozporu s bezpečnostní politikou. Funkce se vyskytuje pouze v systémech s povinným řízením přístupu.
- *Nepovinné řízení důvěrnosti* (CD-0 až CD-4)
  Tato bezpečnostní funkce zahrnuje ty mechanismy nepovinného řízení přístupu k informacím (např. mechanismy přístupových práv, přístupové matice nebo seznamy přístupových práv), které přispívají k zajištění důvěrnosti dat.
- *Povinné řízení důvěrnosti* (CM-0 až CM-4)
  Tato bezpečnostní funkce zahrnuje ty mechanismy povinného řízení přístupu k informacím (např. mechanismy pracující se stupněm klasifikace spravovaných objektů), které přispívají k zajištění důvěrnosti dat.
- *Opětné použití objektů* (CR-0 až CR-1)
  Funkce opětné použití objektů zajišťuje, že objekt, přidělený uživateli nebo procesu neobsahuje žádné informace, zbylé od předchozího vlastníka objektu.

2.2.2 Bezpečnostní funkce zajišťující integritu

Bezpečnostní funkce v této kategorii jsou namířeny proti těm hrozbám, které představují neoprávněnou modifikaci (pozměnění) dat. Jedná se o následující bezpečnostní funkce:

- *Doménová integrita* (IB-0 až IB-2)
  Definuje tzv. důvěryhodnou výpočetní bázi (Trusted Computing Base, TCB) informačního systému a její schopnost ochránit se před útokem a spravovat chráněné objekty.
- *Nepovinné řízení integrity* (ID-0 až ID-4)
  Zahrnuje ty mechanismy nepovinného řízení přístupu k informacím (např. mechanismy přístupových práv, přístupové matice nebo seznamy přístupových práv), které přispívají k zajištění integrity dat.
- *Povinné řízení integrity* (IM-0 až IM-4)
  Zahrnuje ty mechanismy povinného řízení přístupu k informacím (např. mechanismy pracující se stupněm klasifikace spravovaných objektů), které přispívají k zajištění integrity dat.

- *Fyzická integrita* (IP-0 až IP-4)
  Definuje fyzický ochranný perimetr centralizované části systému a poskytuje služby pro ochranu komponent, které leží uvnitř tohoto perimetru.
- *Návrat* (IR-0 až IR-2)
  Zajišťuje schopnost produktu nebo systému IT vrátit se k předchozímu stavu po chybě uživatele, po havárii nebo po útoku.
- *Oddělení rolí* (IS-0 až IS-3)
  Oddělení rolí zajišťuje rozdělení pravomocí (např. přístupových práv) a zodpovědností mezi několik rolí a tím omezuje potenciální škody, způsobené nesprávným nebo nevhodným chováním uživatele nebo správce.
- *Autonomní testování* (IT-0 až IT-3)
  Tato funkce zahrnuje mechanismy, které slouží k testování, zda se hardware a software produktu nebo systému IT nachází ve správném a bezpečném stavu.

2.2.3 Bezpečnostní funkce zajišťující dostupnost

Bezpečnostní funkce zajišťující dostupnost mají za úkol zajistit, že uživatelům nemůže být neoprávněně odepřeno poskytnutí informací nebo služeb informačního systému. Jedná se o následující bezpečnostní funkce:

- *Přidělování prostředků* (AC-0 až AC-3)
  Kontroluje přidělování prostředků jednotlivým uživatelům a jejich využití uživateli.
- *Tolerance k chybám* (AF-0 až AF-23)
  Vlastnost systému, která vyjadřuje jeho schopnost umožnit výměnu vadných komponent bez přerušení poskytování služeb.
- *Robustnost* (AR-0 až AR-3)
  Vlastnost systému zajišťovat dostupnost informací a služeb i po výpadku některých komponent systému.
- *Zotavení* (AY-0 až AY-3)
  Umožňuje, aby se systém vrátil po poruše nebo chybě do známého a důvěryhodného stavu.

2.2.4 Bezpečnostní funkce zajišťující účtovatelnost

Tyto bezpečnostní funkce se týkají zodpovědnosti uživatelů za akce, které v systému provádějí. Jde o následující bezpečnostní funkce:

- *Audit* (WA-0 až WA-5)
  Zajišťuje detekci, zaznamenávání a pozdější analýzu událostí důležitých z hlediska bezpečnosti. Především zahrnuje tzv. mechanismus protokolování událostí.
- *Identifikace a autentizace* (WI-0 až WI-3)
  Zajišťuje zjištění a bezpečné ověření identity uživatele informačního systému.
- *Důvěryhodná cesta* (WT-0 až WT-3)
  Umožňuje uživateli bezpečnou a přímou komunikaci s centralizovaným informačním systémem.

2.3 Bezpečnostní funkce podle CC

V této kapitole se budeme zabývat bezpečnostními funkcemi, definovanými v mezinárodní normě ISO/IEC 15408, s názvem "*Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční požadavky*" [ISO/IEC 15408-2]. Výklad principů kritérií CC je náplní poslední kapitoly této příručky.

Bezpečnostní funkční komponenty, definované ve druhé části ISO/IEC 15408, jsou základem pro funkční požadavky bezpečnosti produktu nebo systému IT, vyjádřené v profilu ochrany (PO) a v bezpečnostním cíli (BC). Tyto požadavky popisují požadované bezpečnostní chování, očekávané od bezpečného produktu nebo systému IT a musí splňovat bezpečnostní plán, uvedený v PO nebo BC. Tyto požadavky popisují bezpečnostní vlastnosti, které mohou uživatelé pozorovat při jejich přímé interakci s produktem nebo systémem IT (tj. při jeho vstupních a výstupních operacích) a/nebo pozorováním odezvy produktu nebo systému IT na podnět.

Bezpečnostní funkční komponenty vyjadřují bezpečnostní požadavky, jejichž cílem je zabránit hrozbám v předpokládaném provozním prostředí produktu nebo systému IT a/nebo pokrýt všechny identifikované bezpečnostní politiky organizace nebo jiné předpoklady.

Tato část ISO/IEC 15408 je určena spotřebitelům, vývojářům a hodnotitelům bezpečných systémů a produktů IT. Kapitola 3 dokumentu ISO/IEC 15408-1 poskytuje další informace o okruhu čtenářů ISO/IEC 15408 a o způsobu využití normy jednotlivými skupinami jeho čtenářů. Tyto skupiny mohou využít ISO/IEC 15408-2 následujícím způsobem:

- Zákazníci použijí ISO/IEC 15408-2 pří výběru komponent pro vyjádření svých funkčních požadavků, které splní bezpečnostní plán, vyjádřený PO nebo BC. Kapitola 4.3 dokumentu ISO/IEC 15408-1 poskytuje podrobnější informace o vztahu mezi bezpečnostním plánem a bezpečnostními požadavky.
- Vývojáři, kteří reagují na skutečné nebo předpokládané bezpečnostní požadavky spotřebitelů při vývoji produktu nebo systému IT, mohou v této části ISO/IEC 15408 nalézt normalizované metody pro porozumění požadavků zákazníků. Mohou také využít obsah této části ISO/IEC 15408 jako základ pro definici bezpečnostních funkcí a mechanismů, které splňují tyto požadavky.
- Hodnotitelé využijí funkční požadavky, definované v této části normy při ověřování, zda funkční požadavky, vyjádřené v PO nebo BC splňují bezpečnostní plány a zda byly vzaty v úvahu všechny vzájemné závislosti a bylo ukázáno, že jsou splněny. Hodnotitelé by si také měli vzít tuto část normy na pomoc při rozhodování, zda daný produkt nebo systém IT splňuje dané požadavky.

2.3.1 Rozšiřování a údržba funkčních požadavků

Norma ISO/IEC 15408 a jeho bezpečnostní funkční požadavky nejsou míněny jako definitivní odpověď na všechny problémy bezpečnosti IT. Norma naopak nabízí sadu srozumitelných bezpečnostních funkčních požadavků, které mohou být použity při vytváření důvěryhodných produktů nebo systémů, reflektujících požadavky trhu. Tyto bezpečnostní funkční požadavky jsou prezentovány jako současný stav poznání v oblasti specifikace požadavků a v oblasti hodnocení. Nepředpokládá se, že ISO/IEC 15408-2 obsahuje všechny možné bezpečnostní funkční požadavky, ale pouze ty, které jsou známé a na kterých se autoři normy v době vydání dokumentu dohodli, že jsou užitečné.

Jelikož se znalosti a potřeby spotřebitelů mohou měnit, funkční požadavky v této části ISO/IEC 15408 bude třeba dále modifikovat. Dá se předpokládat, že někteří autoři dokumentů *Profil ochrany* a/nebo *Bezpečnostní cíle* mohou mít bezpečnostní požadavky, které nejsou (doposud) pokryty třídami funkčních požadavků v ISO/IEC 15408-2. V těchto případech může

autor dokumentu PO zvážit použití funkčních požadavků nepřevzatých z normy (takzvané rozšíření), jak je vysvětleno v přílohách B a C dokumentu ISO/IEC 15408-1.

2.3.2 Organizace dokumentu ISO/IEC 15408-2

Kapitola 1 obsahuje úvodní materiál k ISO/IEC 15408-2. Kapitola 2 uvádí katalog funkčních komponent ISO/IEC 15408-2 a kapitoly 3 až 13 popisují jednotlivé funkční třídy.

Příloha A poskytuje dodatečné informace, které by mohly zajímat potenciální uživatele funkčních komponent, včetně úplné tabulky křížových referencí závislostí jednotlivých komponent. Přílohy B až M obsahují aplikační informace k jednotlivým funkčním třídám. Tyto přílohy jsou zdrojem podpůrných informací pro uživatele této části ISO/IEC 15408. Tyto informace jim mohou pomoci aplikovat relevantní činnosti a zvolit vhodné postupy pro audit a dokumentaci.

Autoři dokumentů PO a BC naleznou relevantní struktury, pravidla a návody v kapitole 2 dokumentu ISO/IEC 15408-1:

- ISO/IEC 15408-1, kapitola 2 definuje pojmy, použité v ISO/IEC 15408.
- ISO/IEC 15408-1, příloha B definuje strukturu profilu ochrany.
- ISO/IEC 15408-1, příloha C definuje strukturu bezpečnostního cíle.

2.3.3 Model funkčních požadavků

Tato podkapitola popisuje model, použitý pro bezpečnostní funkční požadavky, uvedené v ISO/IEC 15408-2. Obrázky 2.1 a 2.2 zobrazují některé z klíčových konceptů modelu. Tato podkapitola obsahuje popisný text pro tyto obrázky a pro další klíčové koncepty, které nejsou na těchto obrázcích zobrazeny. Diskutované klíčové koncepty jsou zvýrazněny *kurzívou*.

ISO/IEC 15408-2 je katalogem bezpečnostních funkčních požadavků, které mohou být předepsány pro *Hodnocený předmět (HP)*. HP je produkt nebo systém IT (spolu s uživateli a dokumentací pro správce), který obsahuje zdroje, jako jsou elektronická paměťová média (např. disky), periferní zařízení (např. tiskárny) a výpočetní kapacitu (např. čas CPU), které mohou být využity pro zpracování a ukládání informací. HP je předmětem hodnocení.

Hodnocení HP se soustřeďuje především na zajištění, že definovaná *Bezpečnostní politika HP (BPHP)* je prosazována pro všechny zdroje HP. BPHP definuje pravidla, pomocí kterých HP ovládá přístup ke svým zdrojům, a tím i ke všem informacím a službám, kontrolovaným HP.

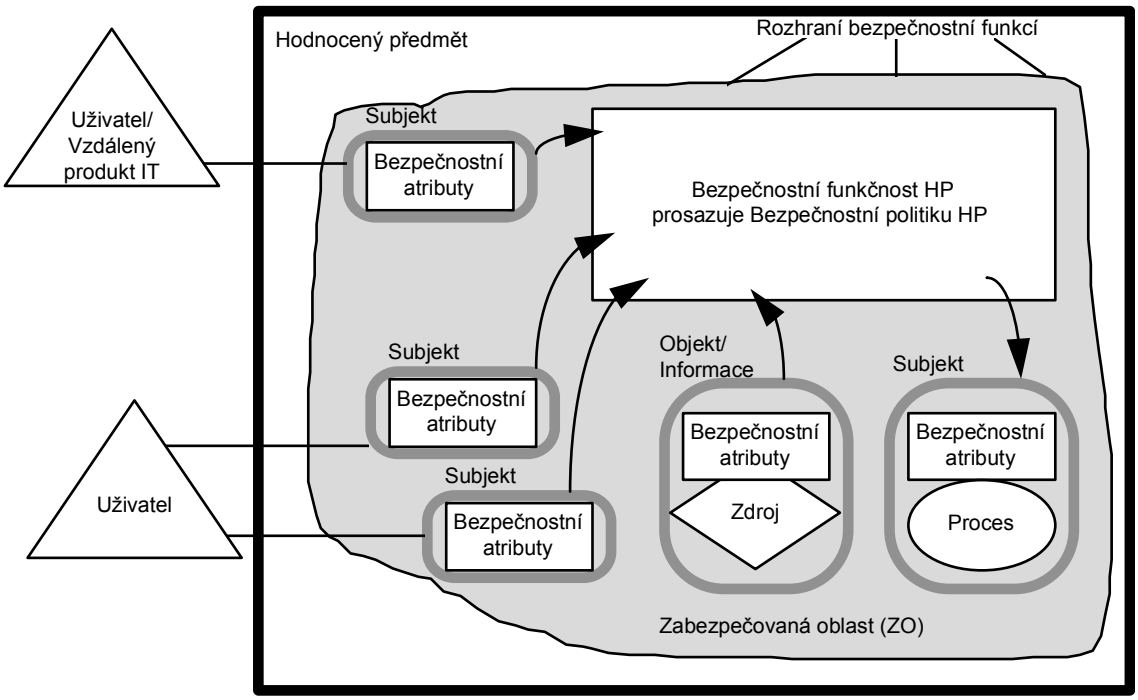
BPHP se skládá z několika *Bezpečnostních politik bezpečnostních funkcí (BPBF)*. Každá BPBF má svůj rozsah působnosti, který definuje subjekty, objekty a operace, řízené touto politikou. BPBF je implementována pomocí *Bezpečnostní funkce (BF)*, jejíž mechanismy prosazují politiku a poskytují k tomu nezbytné schopnosti.

Ty části HP, na které se musíme spolehnout, aby byla prosazována BPHP, se společně nazývají *Bezpečnostní funkcionalita HP (BFHP)*. BFHP se skládá ze všeho hardwaru, softwaru a firmwaru HP, na kterém ať přímo, nebo nepřímo, závisí prosazení bezpečnosti.

Monitor odkazů je abstraktní stroj, který prosazuje politiku řízení přístupu HP. *Mechanismus ověřování odkazů* je implementací principu monitoru odkazů, který splňuje následující vlastnosti: je odolný proti narušení, je vždy vyvolán a je dostatečně jednoduchý, aby mohl být předmětem detailní analýzy a testování. BPHP může sestávat z mechanismu ověřování odkazů a/nebo jiných bezpečnostních funkcí, nutných pro činnost HP.

HP může být monolitický produkt, obsahující hardware, firmware a software. Alternativně HP může být také distribuovaný produkt, který se interně skládá z několika oddělených částí. Každá z těchto částí HP poskytuje jistou službu pro HP a je propojena s ostatními částmi HP pomocí *interního komunikačního kanálu*. Tento kanál může být poměrně malý (jako například sběrnice procesoru) nebo může zahrnovat i interní počítačovou síť HP.

Pokud se HP skládá z několika částí, každá část HP může mít svou vlastní část BFHP, která si vyměňuje uživatelská data a data BFHP přes interní komunikační kanály s jinými částmi BFHP. Tato interakce se nazývá *přenos uvnitř HP*. V tomto případě oddělené části BFHP abstraktně tvoří složenou BFHP, která prosazuje BPHP.



Obr. 2.1 Model bezpečnostních funkčních požadavků (monolitický HP)

Rozhraní HP mohou být lokalizována uvnitř daného HP nebo mohou dovolit interakci s jinými produkty IT pomocí *externích komunikačních kanálů*. Tyto externí interakce s jinými produkty IT mohou mít dvojí formu:

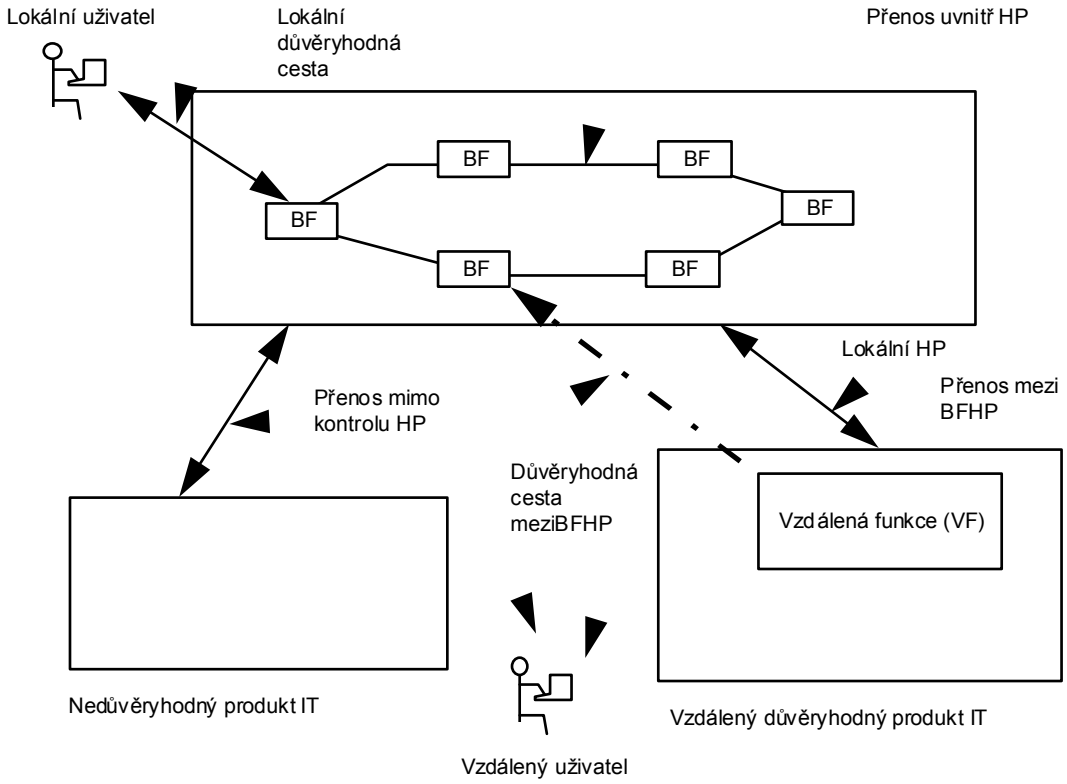
- Bezpečnostní politiky „vzdáleného důvěryhodného produktu IT“ a BP lokálního HP byly administrativně navzájem koordinovány a ohodnoceny. V tomto případě je výměna informací nazývána „*přenos mezi BFHP*“, jelikož k ní dochází mezi BFHP různých důvěryhodných produktů.
- Vzdálený produkt IT nemusí být ohodnocen, což je naznačeno na obr. 2.2 jako „nedůvěryhodný produkt IT“, tudíž jeho bezpečnostní politika je neznámá. Výměna informací je v tomto případě nazvána ”*přenos mimo kontrolu BFHP*”, protože vzdálený produkt nemá žádnou BFHP (nebo charakteristika bezpečnostní politika je neznámá).

Sada interakcí, které se mohou vyskytnout uvnitř HP a které jsou subjektem pravidel BPHP, se nazývá *zabezpečovaná oblast (ZO)*. ZO zahrnuje definovanou sadu interakcí, založených na subjektech, objektech a operacích uvnitř HP, ale nemusí zahrnovat všechny zdroje HP.

Sada rozhraní, ať interaktivních (rozhraní člověk-stroj), nebo programátorských (aplikační programová rozhraní), pomocí kterých jsou zpřístupňovány zdroje spravované BFHP, nebo přes která jsou získávány informace z BFHP, se nazývá *rozhraní BFHP (RBFHP)*. RBFHP definuje hranice funkcí HP, které přispívají k prosazování BPHP.

Uživatelé jsou mimo HP, a tedy i mimo ZO. Pokud uživatelé požadují služby, poskytované HP, pracují s HP prostřednictvím RBFHP. Z hlediska funkčních požadavků ISO/IEC 15408-2 existují dva typy uživatelů: *osoby* a *externí entity IT*. Osoby se dále dělí na *lokální uživatele*,

kteří přímo interagují s HP prostřednictvím určitých zařízení HP (např. prostřednictvím pracovních stanic) a na *vzdálené uživatele*, kteří interagují s HP nepřímo prostřednictvím jiného produktu IT.



Obr. 2.2 Diagram bezpečnostních funkcí v distribuovaném HP

Časový interval interakce mezi uživateli a BFHP se nazývá *relace* uživatele. Vytvoření relace může být podmíněno různými okolnostmi, např. autentizací uživatele, hodinou, metodou přístupu k HP nebo maximálním povoleným počtem relací uživatele. Tato část ISO/IEC 15408 používá pojem *autorizovaný* pro označení uživatele, který vlastní práva a/nebo privilegia nezbytná pro provedení dané operace. Pojem *autorizovaný uživatel* tedy označuje, že BPHP tomuto uživateli povoluje provést danou operaci.

Pro vyjádření požadavků na oddělení pravomocí správce relevantní bezpečnostní funkční komponenty ISO/IEC 15408-2 (z rodiny komponent FMT_SMR) explicitně požadují *role* správců. Role je předdefinovaná sada pravidel, která určuje povolené interakce mezi uživatelem a HP. HP může podporovat definici libovolného počtu rolí. Např. role, týkající se bezpečného provozu HP, mohou být „správce auditu“ a „správce uživatelských účtů“.

HP obsahuje zdroje, které být použity pro zpracování a ukládání informací. Primární cíl BFHP je úplné a správné prosazení BPHP nad zdroji a informacemi, které HP spravuje. Zdroje HP mohou být strukturovány a využity mnoha různými způsoby. ISO/IEC 15408-2 používá rozlišení, které umožňuje specifikaci požadovaných bezpečnostních vlastností.

Všechny entity, které mohou být vytvořeny ze zdrojů, mohou být dvou druhů. Entity mohou být aktivní, což znamená, že jsou příčinou akcí uvnitř HP a zapříčiňují operace, které jsou prováděny nad informacemi. Na druhé straně mohou být entity pasivní, což znamená, že jsou kontejnerem, ze kterého informace pocházejí nebo do kterého jsou informace ukládány.

Aktivní entity se nazývají *subjekty*. Uvnitř HP může existovat několik druhů subjektů:

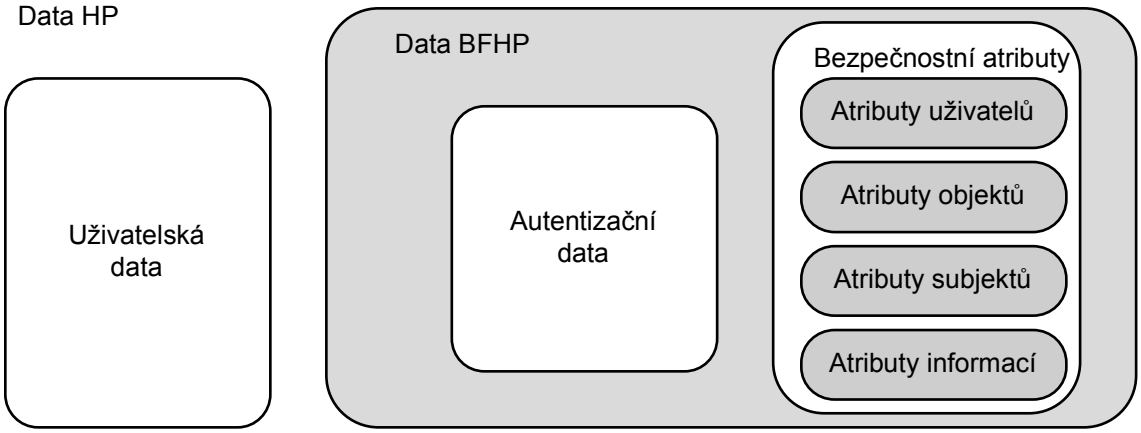
- Ty, které pracují pod kontrolou autorizovaného uživatele a které jsou subjektem všech pravidel BPHP (např. procesy v UNIXu).
- Ty, které pracují jako speciální funkční procesy, které mohou pracovat v zájmu mnoha uživatelů (např. funkce, které se nacházejí v architekturách klient/server).
- Ty, které jsou samotnou součástí HP (např. důvěryhodné procesy).

Nad těmito typy subjektů popisuje ISO/IEC 15408-2 prosazování BPHP.

Pasivní entity (např. kontejnery s informacemi) jsou v bezpečnostních funkčních požadavcích ISO/IEC 15408-2 nazývány *objekty*. Objekty jsou cílem operací, které jsou prováděny subjekty. V případě, že subjekt (aktivní entita) je cílem operace (např. meziprocesové komunikace), může subjekt vystupovat jako objekt. Objekty mohou obsahovat *informace*.

Uživatelé, subjekty, informace a objekty mají jisté *atributy*, které obsahují informace nutné k tomu, aby se HP choval správně. Některé atributy, jako jsou jména souborů, mohou být pouze informativní (tj. zvyšují uživatelskou přívětivost HP), zatímco jiné, jako jsou např. informace pro řízení přístupu, existují pouze za účelem prosazení BPHP. Tato druhá skupina atributů se nazývá "*bezpečnostní atributy*". Pokud není definováno jinak, je slovo atribut v ISO/IEC 15408 použito jako zkratka místo pojmu „bezpečnostní atribut". BPHP však může požadovat kontrolu nad všemi atributy, bez ohledu na to, jakého jsou typu.

Data uvnitř HP jsou kategorizována na dvě skupiny - uživatelská data nebo data BFHP. Obrázek 2.3 ukazuje jejich vztah. *Uživatelská data* jsou informace, uložené ve zdrojích HP, které mohou být uživateli zpracovávány v souladu s BPHP a kterým BFHP nepřisuzují žádný zvláštní význam. Např. obsah schránky elektronické pošty jsou uživatelská data. *Data BFHP* jsou informace, které používají BFHP pro provádění rozhodnutí podle BPHP. Pokud to BPHP dovolí, data BFHP mohou být ovlivněna (měněna) i uživateli. Příklady dat BFHP jsou bezpečnostní atributy, autentizační data a seznamy přístupových práv.



Obr. 2.3 Vztah mezi uživatelskými daty a daty BFHP

Některé BPBF se vztahují konkrétně na ochranu dat, jako např. *BPBF řízení přístupu* a *BPBF řízení toku dat*. Mechanismy, které implementují BPBF řízení přístupu, zakládají svá rozhodnutí na atributy subjektů, objektů a operací, které jsou pod kontrolou bezpečnostní politiky. Tyto atributy jsou použity v sadě pravidel, která řídí operace, jež mohou subjekty provádět na objektech. Mechanismy, které implementují BPBF řízení toku informace, zakládají svá rozhodnutí na atributech subjektů, kontrolovaných informacích a sadě pravidel, které řídí operace subjektů nad informacemi. Atributy informace, které mohou být sdruženy s atributy kontejneru

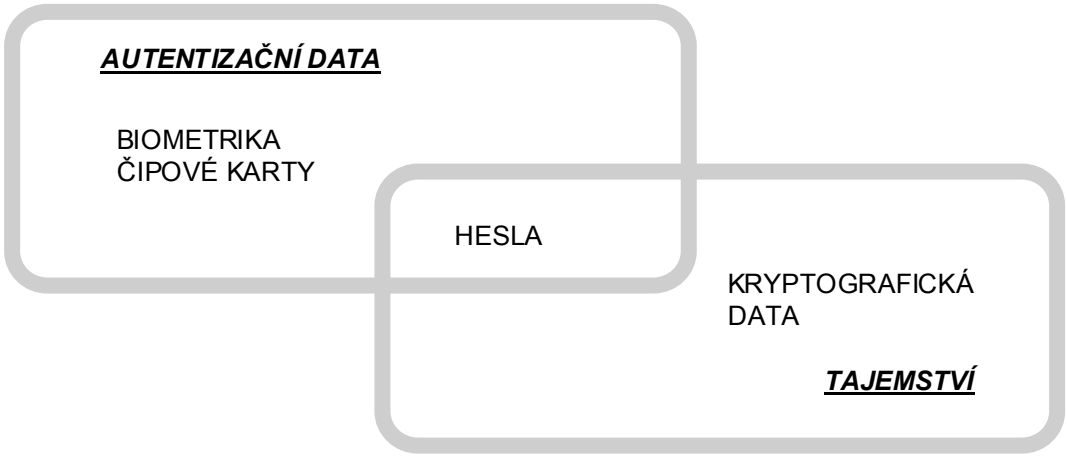
(nebo nemusí, jako v případě víceúrovňové databáze) se pohybují zároveň s pohybujícími se informacemi.

Dva specifické typy dat, které jsou uvedeny v ISO/IEC 15408-2, mohou, ale nemusí být totožné. Jde o *autentizační data* a *tajemství*.

Autentizační data se používají pro ověření identity uživatele, který požaduje služby od HP. Nejobvyklejší druh autentizačních dat je heslo, které musí být pro svou funkci účinného bezpečnostního mechanismu udrženo v tajnosti. Ne všechny formy autentizačních dat musí být tajné. Biometrická autentizační zařízení (např. snímače otisků prstů nebo snímače oční sítnice) nezávisí na utajení dat, ale na tom, že data představují něco, co má pouze jeden uživatel a co nemůže být paděláno.

Pojem tajemství, tak jak jej používají funkční požadavky ISO/IEC 15408-2, je sice aplikovatelný na autentizační data, ale je také aplikovatelný na jiné typy dat, která musí být udržena v tajnosti, aby byla prosazena konkrétní BPBF. Například mechanismus důvěryhodného kanálu, jehož schopnost udržet přenášené informace v tajnosti využívá kryptografie, je pouze tak silný, jak je silná metoda, použitá pro utajení kryptografických klíčů před neoprávněným odhalením.

Proto některá, ale nikoli všechna, autentizační data je třeba držet v tajnosti, a některá, ale ne všechna tajemství jsou použita jako autentizační data. Obrázek 2.4 ukazuje typická autentizační data a tajemství.



Obr. 2.4 Vztah mezi ”autentizačními daty” a ”tajemstvími”

2.3.4 Katalog komponent funkčních požadavků

Seskupení komponent funkčních požadavků v ISO/IEC 15408-2 neodpovídá žádné formální taxonomii. Bezpečnostní funkce jsou rozděleny do kategorií, které se nazývají *třídy* (např. třída Bezpečnostní audit nebo třída Komunikace). Každá třída se skládá z *rodin*, které odpovídají např. bezpečnostním funkcím v kritériích CTCPEC. Konečně každá rodina se skládá z *komponent*, které plní požadavky rodiny s různou mírou ochrany. Na rozdíl od kritérií CTCPEC nemusí být jednotlivé komponenty nutně hierarchické (viz dále).

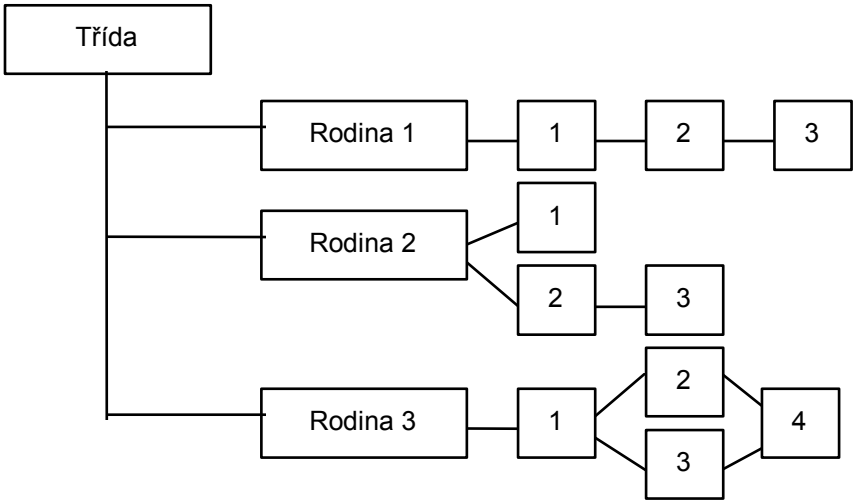
Katalog funkčních požadavků obsahuje třídy rodin a komponent, které jsou pouhým seskupením podle podobné funkce nebo podobného účelu a komponenty v rámci třídy jsou uvedeny v abecedním pořadí. Katalog obsahuje následující třídy:

- Třída *FAU*: Bezpečnostní audit
- Třída *FCO*: Komunikace
- Třída *FCS*: Kryptografická podpora

- Třída *FDP*: Ochrana uživatelských dat
- Třída *FIA*: Identifikace a autentizace
- Třída *FMT*: Správa bezpečnosti
- Třída *FPR*: Soukromí
- Třída *FPT*: Ochrana bezpečnostní funkcionality
- Třída *FRU*: Využití zdrojů
- Třída *FTA*: Přihlášení do HP
- Třída *FTP*: Důvěryhodné cesty/kanály

Na začátku každé třídy je uveden v dokumentu ISO/IEC 15408-2 informativní diagram, který ukazuje strukturu této třídy, rodiny v této třídě a komponenty v každé rodině. Tento diagram je užitečný pro objasnění vztahů, které mohou existovat mezi jednotlivými komponentami.

V každé třídě je v dokumentu ISO/IEC 15408-2 uveden obrázek, ilustrující hierarchii rodiny, podobný obr. 2.5.



Obr. 2.5 Ukázka rozdělení třídy na rodiny a komponent

Na obr. 2.5 je první rodinou rodina 1, která obsahuje tři hierarchické komponenty. Komponenta 2 a komponenta 3 mohou obě splňovat požadavky komponenty 1. Stejně tak komponenta 3 může splňovat požadavky komponenty 2. V rodině 2 jsou tři komponenty, které nejsou všechny navzájem hierarchické. Komponenta 3 může splňovat požadavky komponenty 2, avšak nemůže splňovat požadavky komponenty 1.

V následujících kapitolách si ukážeme přehled jednotlivých tříd a rodin, definovaných v katalogu funkčních požadavků ISO/IEC 15408-2. Vzhledem ke značnému počtu komponent v katalogu zde nemůžeme uvést přehled komponent – zájemce odkazujeme na dokument ISO/IEC 15408-2.

2.3.5 Třída FAU: Bezpečnostní audit

Bezpečnostní audit zahrnuje rozpoznávání, zaznamenávání, ukládání a analyzování informací, které mají vztah k aktivitám, významným z hlediska bezpečnosti (tj. aktivit, pokrytých bezpečnostní politikou). Výsledné auditní záznamy mohou být následně zkoumány, aby se zjistilo, které bezpečnostně významné aktivity se staly a kdo (který uživatel) je za ně zodpovědný. Třída bezpečnostních funkcí Bezpečnostní audit obsahuje tyto rodiny komponent:

- FAU-ARP Automatická reakce bezpečnostního auditu
- FAU-GEN Generování dat bezpečnostního auditu
- FAU-SAA Analýza bezpečnostního auditu
- FAU-SAR Kontrola bezpečnostního auditu
- FAU-SEL Výběr událostí bezpečnostního auditu
- FAU-STG Ukládání událostí bezpečnostního auditu

2.3.6 Třída FCO: Komunikace

Tato třída obsahuje dvě rodiny, které se zabývají bezpečným zjištěním identity protistrany, která se účastní výměny (přenosu) dat. Tyto rodiny se vztahují k zajištění identity původce přenášené informace (důkaz původu) a k zajištění identity příjemce přenášené informace (důkaz přijetí). Zajišťují, že ani původce nemůže popřít odeslání zprávy, ani příjemce nemůže popřít její přijetí. Třída bezpečnostních funkcí Komunikace obsahuje tyto rodiny komponent:

- FCO-NRO Nepopiratelnost původu
- FCO-NRR Nepopiratelnost přijetí

2.3.7 Třída FCS: Kryptografická podpora

BFHP může zahrnovat i kryptografické funkce, které pomohou splnit některé bezpečnostní plány vyšší úrovně. Tyto plány zahrnují (mimo jiné): identifikaci a autentizaci, nepopiratelnost, důvěryhodnou cestu, důvěryhodný kanál a oddělení dat. Tato třída se použije, pokud HP obsahuje kryptografické funkce, jejichž implementace může být pomocí hardwaru, firmwaru a/nebo softwaru.

Třída FCS se skládá ze dvou rodin: FCS-CKM Správa kryptografických klíčů a FCS-COP Kryptografické operace. Rodina FCS-CKM se zabývá aspekty správy kryptografických klíčů, zatímco rodina FCS-COP se zabývá jejich provozním použitím.

- FCS-CKM Správa kryptografických klíčů
- FCS-COP Kryptografické operace

2.3.8 Třída FDP: Ochrana uživatelských dat

Tato třída obsahuje rodiny, definující požadavky na bezpečnostní funkce HP a bezpečnostní politiky HP, které se vztahují k ochraně uživatelských dat. Třída FDP se dělí na čtyři skupiny rodin, které se starají o uživatelská data uvnitř HP během jejich importu, exportu a uložení a o bezpečnostní atributy, které se přímo vztahují k uživatelským datům. Rodiny třídy FDP se dělí na následující čtyři skupiny:

a) Bezpečnostní politiky bezpečnostních funkcí ochrany uživatelských dat

- FDP-ACC Politika řízení přístupu
- FDP-IFC Politika řízení toku informace

Komponenty v těchto rodinách umožňují, aby autor profilu ochrany nebo bezpečnostního cíle definoval bezpečnostní politiky bezpečnostních funkcí, týkajících se ochrany uživatelských dat a definoval rozsah působnosti politik, nutný pro stanovení bezpečnostních plánů. Názvy těchto politik by měly být použity v ostatních funkčních komponentách, jejichž činnost je vyžadována v „bezpečnostní politice řízení přístupu“ nebo v „bezpečnostní politice řízení toku informace“. Pravidla, definující funkčnost vyjmenovaných politik řízení přístupu a řízení toku dat, budou definovány v rodinách FDP-ACF a FDP-IFF.

b) Jednotlivé způsoby ochrany uživatelských dat

- FDP-ACF Funkce řízení přístupu
- FDP-IFF Funkce řízení toku informace
- FDP-ITT Přenos uvnitř HP
- FDP-RIP Ochrana zbytkových informací
- FDP-ROL Odvolání operace (rollback)
- FDP-SDI Integrita uložených dat

c) Off-line uložení, import a export dat

- FDP-DAU Autentizace dat
- FDP-ETC Export mimo oblast řízení TSF
- FDP-ITC Import z oblasti mimo řízení TSF

Komponenty v těchto rodinách se zabývají důvěryhodným přenosem do a ze zabezpečované oblasti.

d) Přenos mezi BFHP

- FDP-UCT Ochrana důvěrnosti uživatelských dat při přenosech mezi BFHP
- FDP-UIT Ochrana integrity uživatelských dat při přenosech mezi BFHP

Komponenty v těchto rodinách se zabývají přenosem mezi BFHP a jiným důvěryhodným produktem IT.

2.3.9 Třída FIA: Identifikace a autentizace

Rodiny v této třídě se zabývají požadavky na funkce, které zjišťují a ověřují identitu uživatele.

Identifikace a autentizace jsou nutné k tomu, aby bylo zajištěno, že uživateli jsou přiřazeny odpovídající bezpečnostní atributy (tj. například jeho identita, příslušnost ke skupinám uživatelů, role, bezpečnostní úrovně integrity).

Jednoznačná identifikace autorizovaných uživatelů a správné přiřazení bezpečnostních atributů uživatelům a subjektům je z hlediska prosazení bezpečnostních politik kritická. Tato rodina se ve svých třídách zabývá určením a verifikací identity jednotlivých uživatelů, určením jejich

oprávnění k interakci s HP a správným přiřazením bezpečnostních atributů každému autorizovanému uživateli. Některé jiné třídy požadavků (např. ochrana uživatelských dat a bezpečnostní audit) jsou pro svou efektivní činnost závislé na správné identifikaci a autentizaci uživatelů. Třída bezpečnostních funkcí Identifikace a autentizace obsahuje tyto rodiny komponent:

- FIA-AFL Obsluha neúspěšné autentizace
- FIA-ATD Definice atributů uživatele
- FIA-SOS Specifikace tajemství
- FIA-UAU Autentizace uživatele
- FIA-UID Identifikace uživatele
- FIA-USB Vazba uživatel-subjekt

2.3.10 Třída FMT: Správa bezpečnosti

Cílem této třídy je specifikovat správu některých aspektů BFHP: bezpečnostních atributů, dat BFHP a funkcí BFHP. Mohou zde být také specifikovány různé role správců a jejich vztahy, jako je např. oddělení pravomocí. Třída bezpečnostních funkcí Správa bezpečnosti obsahuje tyto rodiny komponent:

- FMT-MOF Správa funkcí BFHP
- FMT-MSA Správa bezpečnostních atributů
- FMT-MTD Správa dat BFHP
- FMT-REV Odvolání bezpečnostních atributů
- FMT-SAE Vypršení platnosti bezpečnostních atributů
- FMT-SMR Role správy bezpečnosti

2.3.11 Třída FPR: Soukromí

Tato třída obsahuje požadavky na zachování soukromí uživatelů. Požadavky v této třídě poskytují ochranu uživatele před zjištěním jeho identity a zneužitím jeho identity jinými uživateli. Třída Soukromí zahrnuje následující rodiny:

- FPR-ANO Anonymita
- FPR-PSE Pseudonymita
- FPR-UNL Nespojitelnost
- FPR-UNO Nepozorovatelnost

2.3.12 Třída FPT: Ochrana bezpečnostní funkcionality

Tato třída obsahuje rodiny funkčních požadavků, které se vztahují k integritě a správě mechanismů, které poskytuje BFHP (nezávisle na specifikách BPHP) k integritě dat BFHP (nezávisle na specifickém obsahu dat BPHP). V jistém smyslu se mohou rodiny v této třídě zdát duplicitní ke komponentám ve třídě FDP (ochrana uživatelských dat). Je dokonce možné, že tyto funkce mohou být implementovány pomocí stejných mechanismů. Rozdíl je však v tom, že FDP se soustředí na ochranu uživatelských dat, zatímco FPT se soustředí na ochranu dat BFHP. Kom-

ponenty třídy FPT jsou nezbytné k tomu, aby existovaly požadavky na to, že BPBF v HP nemohou být narušeny nebo obejity.

Z hlediska této třídy se BFHP skládá ze tří významných částí:

- Z *abstraktního stroje* BFHP, který je virtuálním nebo fyzickým strojem, na němž běží hodnocené implementace BFHP.
- Z *implementace* BFHP, která běží na abstraktním stroji a implementuje mechanismy, které prosazují BPHP.
- Z *dat* BFHP, která tvoří administrační databázi, která řídí prosazování BPHP.

Pro ochranu těchto tří částí nabízí třída bezpečnostních funkcí Ochrana bezpečnostní funkcionality tyto rodiny komponent:

- FPT-AMT Testování abstraktního stroje
- FPT-FLS Bezpečnost při výpadku
- FPT-ITA Dostupnost exportovaných dat BFHP
- FPT-ITC Důvěrnost exportovaných dat BFHP
- FPT-ITI Integrita exportovaných dat BFHP
- FPT-ITT Přenos dat BFHP uvnitř HP
- FPT-PHP Fyzická ochrana BFHP
- FPT-RCV Důvěryhodná obnova
- FPT-RPL Detekce přehrání
- FPT-RVM Zprostředkování odkazů
- FPT-SEP Oddělení domén
- FPT-SSP Protokol synchronizace stavu
- FPT-STM Časové známky
- FPT-TDC Konzistence dat BFHP mezi BFHP
- FPT-TRC Konzistence replikace dat BFHP uvnitř BFHP
- FPT-TST Autonomní testování BFHP

2.3.13 Třída FRU: Využití zdrojů

Tato třída obsahuje tři rodiny, které podporují dostupnost požadovaných zdrojů, jako je výpočetní kapacita nebo kapacita uložení dat. Rodina Tolerance k chybám poskytuje ochranu proti nedostupnosti kapacit, způsobených výpadkem HP. Rodina Priorita služeb zajišťuje, že zdroje budou přednostně přidělovány důležitějším nebo časově kritickým úlohám a že si je nebudou moci monopolizovat úlohy s nižší prioritou. Rodina Alokace zdrojů zajišťuje limity na využití dostupných zdrojů, a tím zabraňuje uživatelům v monopolizaci zdrojů.

- FRU-FLT Tolerance k chybám
- FRU-PRS Priorita služeb
- FRU-RSA Alokace zdrojů

2.3.14 Třída FTA: Přihlášení do HP

Tato třída specifikuje funkční požadavky na kontrolu ustavení uživatelské relace. Obsahuje tyto rodiny komponent:

- FTA - LSA Omezení rozsahu volitelných atributů
- FTA -MCS Omezení vícenásobných současných relací
- FTA -SSL Uzamykání relace
- FTA-TAB Varování při přihlášení
- FTA -TAH Historie přihlášení
- FTA -TSE Ustavení relace

2.3.15 Třída FTP: Důvěryhodné cesty/kanály

Rodiny komponent v této třídě obsahují požadavky na důvěryhodnou komunikační cestu mezi uživateli a BFHP a pro důvěryhodný komunikační kanál mezi BFHP a jinými důvěryhodnými produkty IT. Důvěryhodné cesty a kanály mají tyto obecné vlastnosti:

- Komunikační cesta je vytvořena pomocí interních a externích komunikačních kanálů (podle typu komponenty), které izolují definovanou podmnožinu dat a příkazů BFHP od zbytku BFHP a uživatelských dat.
- Použití komunikační cesty může být iniciováno uživatelem anebo BFHP (podle typu komponenty).
- Komunikační cesta je schopna poskytnout záruku, že uživatel komunikuje se správnou BFHP a že BFHP komunikuje se správným uživatelem (podle typu komponenty).

Důvěryhodný kanál je v tomto modelu komunikační kanál, který může být iniciován na jednom z jeho konců a poskytuje vlastnost nepopiratelnost identity stran na jeho koncích.

Důvěryhodná cesta poskytuje uživatelům prostředky pro provádění činností se zaručením přímé interakce s BFHP. Je obvykle požadována pro některé akce uživatele, jako je počáteční identifikace a autentizace, může však být vyžadována i v jiných okamžicích v průběhu relace. Důvěryhodná cesta může být iniciována buď uživatelem, nebo BFHP. Je zaručeno, že příkazy uživatele, jdoucí přes důvěryhodnou cestu, jsou chráněny před modifikací a prozrazením nedůvěryhodným aplikacím.

Tato třída zahrnuje následující rodiny:

- FTP-ITC Důvěryhodný kanál mezi BFHP
- FTP-TRP Důvěryhodná cesta

2.3.16 Minimální požadavky funkčnosti v návrhu bezpečnostního standardu SIS

V návrhu standardu bezpečnosti pro státní informační systém (publikace [BSSIS]) jsou v kapitole s názvem “Minimální programově technické požadavky” definovány funkční požadavky na (tehdejší) státní informační systém. Pro ilustraci požadované bezpečnostní funkce uvádíme v následujícím přehledu:

Identifikace a autentizace

- FIA-UID.1 Základní identifikace uživatele
- FIA-UAU.1 Základní autentizace uživatele
- FIA-ATD.1 Definice atributů uživatele
- FIA- ATA. Inicializace bezpečnostních atributů uživatele
- FIA- ADP.2 Rozšířená ochrana autentizačních dat uživatele

Audit

- FAU-GEN.1 Generování dat revize bezpečnosti
- FAU-GEN.2 Generování dat revize bezpečnosti s identitou uživatele
- FAU-STG.1 Stálé ukládání záznamů revize bezpečnosti
- FAU-PRO.1 Omezený přístup k záznamům revize bezpečnosti
- FAU-MGT.1 Správa záznamů revize bezpečnosti
- FAU-SEL.1 Selektivní revize bezpečnosti
- FAU-SEL.2 Run-timová selektivní revize bezpečnosti

Řízení přístupu

- FDP-ACC.1 Částečné řízení přístupu k objektům
- FDP-ACF.1 Řízení přístupu jednoduchými bezpečnostními atributy
- FDP-ACI.1 Statická inicializace atributů
- FDP-SAM.2 Modifikace bezpečnostních atributů uživatelem
- FDP -RIP.1 Částečná ochrana zbytkových informací na základě přidělení zdroje

Ochrana bezpečnostních funkcí hodnoceného předmětu

- FPT-TSA.1 Základní administrace bezpečnosti
- FPT-TSU.1 Prosazení vedení při administraci bezpečnosti
- FPT-SEP.1 Separace domén TSF
- FPT-RVM.1 Nemožnost obejít bezpečnostní politiku TOE
- FPT-AMT.1 Testování abstraktního počítače

Je třeba upozornit na to, že v době, kdy byl tento návrh standardu vytvářen, byla kritéria CC, ze kterých vychází funkční požadavky, ještě ve své předchozí verzi. V následující verzi (která byla vzata za základ normy ISO/IEC 15408) byla klasifikace bezpečnostních funkcí poněkud pozměněna, takže uvedené požadované bezpečnostní funkce nekorespondují s bezpečnostními funkcemi normy ISO/IEC 15408.

Číslice, uvedená za zkratkou komponenty (FPT-AMT.1), je pořadovým číslem komponenty v rodině bezpečnostních funkcí.

3. Bezpečnostní mechanismy

Bezpečnostní mechanismy jsou nástroje používané pro implementaci bezpečnostních funkcí. Mohou být administrativního, fyzického, logického nebo technického typu. Tyto mohou být při implementaci bezpečnostních funkcí spolu různými způsoby kombinovány tak, aby implementace bezpečnostní funkce byla přesná, účinná a ekonomická. Omezený rozsah příručky neumožňuje provést ani vyčerpávající výčet možných bezpečnostních mechanismů, natož pak rozbor jejich vlastností. Proto se s koncepcemi vybraných příkladů bezpečnostních mechanismů seznámíme pouze orientačně a v dalších kapitolách se budeme věnovat nepatrně obšírnějšímu rozboru kryptografických bezpečnostních mechanismů.

3.1 Příklady bezpečnostních mechanismů

Některé bezpečnostní mechanismy mohou být použity pro implementaci několika i aplikačně odlišných bezpečnostních funkcí. Například kryptografický algoritmus lze použít pro implementaci bezpečnostní funkce zajišťující důvěrnost, bezpečnostní funkce zajišťující integritu i bezpečnostní funkce zajišťující identifikaci a autentizaci. Magnetickou kartu lze použít jak pro identifikaci při používání bankomatu, tak i pro řízení přístupu do zabezpečovaných prostorů.

Některé bezpečnostní funkce mohou být implementovatelné jediným bezpečnostním mechanismem, jiné pouze více bezpečnostními mechanismy současně. Například bezpečnostní funkce zajišťující důvěrnost bývá typicky implementovaná vhodným šifrovacím mechanismem a administrativními předpisy pro zacházení s kryptografickými klíči. Bezpečnostní funkce zajišťující nepopiratelnost je obvykle implementovaná kryptografickým digitálním podpisem a administrativními mechanismy podporujícími důvěryhodnost takového podpisu.

Většina bezpečnostních funkcí bývá implementovatelná několika způsoby, tj. různými typy bezpečnostních mechanismů. Například bezpečnostní funkci identifikace a autentizace můžeme implementovat:

- ověřováním znalosti nějaké tajné nepadělatelné informace (heslo nebo osobní identifikační číslo – PIN, Personal Identification Number; správa PIN viz např. norma ANSI X9.8 z r. 1982)
- ověřováním vlastnění nějakého předmětu (klíč, magnetická nebo čipová karta)
- ověřováním nějakých fyzických charakteristik (otisk prstu, vzorek oční duhovky).

Tři ze zmíněných bezpečnostních mechanismů – hesla, magnetické karty a čipové karty, si alespoň orientačně přiblížíme.

3.1.1.1 Hesla a osobní identifikační čísla

Hesla a osobní identifikační čísla se přidělují individuálním subjektům, ne jejich skupinám. Důvěrnost hesel (osobních identifikačních čísel) pak bývá zajišťována individuální účtovatelností a dalšími administrativními opatřeními, např. zakazujícími uchovávání hesel jinde než v paměti subjektu a připouštějícími používání pouze obtížně uhodnutelných hesel, případně i aplikací mechanismů generujících jednorázově použitelná hesla (na bázi seznamů jednorázově používaných hesel mnoho let pracovala bankovní síť SWIFT – Society for World-wide Interbank Financial Transfers).

Jestliže heslo má být použito pro autentizaci subjektu žádajícího přístup do počítače, potom musí být v počítači dostupný jeho vzor, aby bylo možno zadané heslo kontrolovat. Uchovávání seznamu hesel je ovšem bezpečnostní problém. Kompromitované heslo může použít neoprávněný subjekt k „maškarádě“, k útoku vedeném formou falšování své identity. Proto se místo pamatování hesel (osobních identifikačních čísel) v původní podobě uchovávají v počítači výsledky jejich zpracování jednosměrnými funkcemi (snadno se spočítá výsledek, obtížně se k výsledku hledá jednoznačně odpovídající vstup). Zadané heslo (PIN) se zpracuje stejnou funkcí a autentizační bezpečnostní funkce porovnává výsledky a ne originály.

Přenos hesel nezabezpečenou sítí (běžná lokální síť, telefonní spoj) v otevřené podobě je velmi zranitelný z hlediska požadavku zachování soukromí a důvěrnosti. Jejich šifrováním problém zasílání hesla nevyřešíme, útočník může šifru hesla odchytit a replikovat ji stejně jako by to udělal s jeho originální hodnotou. Jedním možným řešením tohoto bezpečnostního problému je použití mechanismu „výzva–odpověď“ následujícím způsobem, který umožňuje přenášenou autentizační informaci dynamicky měnit: uživatel i vzdálený počítač znají tajné heslo P a oba umí řešit vhodnou jednosměrnou hašovací funkci *a*. Jakmile uživatel požádá vzdálený počítač o povolení přístupu (udá mu své jméno), vzdálený počítač ho vyzve k dodání důkazového materiálu potřebného pro autentizaci udané identifikace tím, že mu zašle nějakou náhodnou hodnotu R. Uživatel odpoví vzdálenému počítači hodnotou získanou aplikací jednosměrné hašovací funkce *a* na hodnoty hesla P a výzvy R, tj. *a* (P, R). Vzdálený počítač nyní provede stejný výpočet a udanou identitu uzná za autentickou, pokud oba vypočtou stejnou hodnotu.

3.1.1.2 Magnetické karty

Magnetická karta se používá jako identifikační bezpečnostní mechanismus již poměrně dlouho a v mnoha aplikacích (bankomaty, placení v obchodech, řízení přístupu do zabezpečovaných prostorů). Formát takové karty a magnetického proužku na ní definuje mezinárodní norma ISO 7810. Magnetická karta obvykle poskytuje paměť přibližně pro řádově stovky bitů dat. Může obsahovat např. informaci identifikující uživatele, číslo jeho bankovního účtu apod. Pro ověřování prohlašované identity uživatele magnetické karty se používá nějaký typ aplikace osobního identifikačního čísla. V on-line systémech lze osobní identifikační čísla ověřovat centrálně, nemusí se tudíž pamatovat na magnetické kartě. PIN bývá kombinován s informací identifikující uživatele, případně s její částí, aby se útočníkům zabránilo sestavovat si seznamy osobních identifikačních čísel a jejich šifer. Magnetické karty lze snadno falšovat nebo neoprávněně kopírovat. Jako ochranný prostředek před falšováním se používají např. hologramové obrázky na lícní straně karty. Existuje řada propracovaných prostředků chránících magnetické karty před jejich neoprávněným kopírováním.

3.1.1.3 Čipové karty

V nedávné době se vyvinuly karty s mikroprocesory, pamětmi RAM a ROM, vesměs nazývané čipové karty (smart cards). Čipové karty poskytují větší paměťovou kapacitu než magnetické karty a navíc poskytují nezanedbatelný zpracovatelský výkon přímo na kartě. Umožňují uložená data fyzicky chránit. Kontakty na vnitřní obvody se realizují prostřednictvím plošek, realizovaných na povrchu čipové karty. Jejich pozici, rozměr karty a protokoly, používané pro řízení komunikace mezi čipovou kartou a snímačem čipové karty, zavádí norma ISO/IEC 7816. Čipové karty lze obtížně kopírovat, vnitřní uspořádání čipových karet bývá výrobci karet tajeno.

První generace čipových karet z druhé poloviny 80. let obsahovala jednoduché 8bitové procesory a poskytovala relativně omezenou kryptografickou funkcionalitu. Čipové karty druhé generace jsou vybavovány výkonnějšími procesory, mají více paměti a poskytují větší varietu kryptografických funkcí. Poslední typy čipových karet dokáží realizovat výpočty, potřebné pro digitální podpisy, ve zlomcích sekund. Čipové karty druhé generace se typicky používají jako

interaktivní identifikační zařízení. Mohou obsahovat i tajný kryptografický klíč uživatele. Proto dříve než čipová karta umožní provádění svých funkcí, uživatel používající čipovou kartu musí zadat svůj PIN (na nějakém terminálu a snímači karet). Karta se tak chrání před krádeží.

Ve Francii čipové karty již vesměs vytlačily z používání magnetické karty jako platební karty. Ve Velké Británii byl projekt náhrady magnetických karet v oblasti aplikace kreditních a debetních karet zahájen v r. 1997 a proces náhrady koncem devadesátých let stále ještě běží. Telefony GSM požadují před svým použitím vložit do těla přístroje modul SIM (Subscriber Identity Module). SIM si pamatuje informaci identifikující uživatele a jeho tajný klíč (GSM telefony nemusí být používány pouze jako osobní prostředek). Modul SIM bývá implementován jako čipová karta. Existují obchodní systémy s elektronickými pokladnami založené na používání čipových karet. Jsou dostupné čipové karty realizující digitální podpisování v reálném čase. Čipové karty lze používat jako kalkulačku s displejem pro výpočet identifikační informace při autentizaci. Příkladů použitelnosti čipových karet lze uvést mnoho.

3.2 Síla bezpečnostních mechanismů

Podle toho, jak silným útokům jsou bezpečnostní mechanismy odolné, rozpoznáváme:

- *bezpečnostní mechanismy základní síly*, tzv. slabé bezpečnostní mechanismy
  Jsou používány jako ochranný nástroj proti náhodným neúmyslným, útokům a jako ochrana proti laickým útočníkům. Lze je narušit kvalifikovaným útokem střední síly. Jako příklady slabých bezpečnostních mechanismů lze uvést implementaci autentizační funkce heslem nebo implementaci likvidace skrytého paměťového kanálu na vnější magneticky orientované paměti zrušením katalogizační informace.

- *bezpečnostní mechanismy střední síly*
  Jsou používány jako ochrana proti úmyslným útokům s omezenými příležitostmi a možnostmi, ochrana proti hackerům, tj. kvalifikovaným útočníkům. Síla jejich útoku bývá omezována vesměs jejich časovými a ekonomickými důvody, nikoli znalostmi. Jako příklady bezpečnostních mechanismů střední síly lze uvést implementaci autentizační funkce kryptografickými nástroji nebo implementaci likvidace skrytého paměťového kanálu na vnější magneticky orientované paměti vymazáním uložené informace jejím přepisem nějakým bitovým vzorkem.

- *silné bezpečnostní mechanismy*
  Jsou používány jako ochrana proti útočníkům s vysokou úrovní znalostí, s velkými příležitostmi a prostředky, umožňujícími vést útoky vymykající se běžné praxi. Slouží jako ochrana proti profesionálním útočníkům. Jako příklady silných bezpečnostních mechanismů lze uvést implementaci autentizační funkce pomocí biometrik (vzorek oční duhovky, otisk prstu) nebo implementaci likvidace skrytého paměťového kanálu na vnější magneticky orientované paměti vymazáním uložené informace jejím násobným přepisem vhodnými bitovými vzorky, aby se odstranila stopa původně uložené informace i ve zbytkové magnetizaci. Silnými bezpečnostními mechanismy mohou být i kryptografické mechanismy, pokud je jejich správa klíčů dostatečně bezpečná.

3.3 Kryptografické bezpečnostní mechanismy

Poněvadž kryptografické bezpečnostní mechanismy jsou pravděpodobně nejvíce používané, v omezeném prostoru této příručky se budeme věnovat pouze jim. Cílem kapitoly totiž je, aby čtenář porozuměl tomu, co to bezpečnostní mechanismy jsou a jaké vlastnosti mají, nikoli po-

znání všech možných bezpečnostních mechanismů. V této části uvedeme stručné informace o některých kryptografických bezpečnostních mechanismech podle nejdůležitějších mezinárodních norem ISO/IEC. Všechny tyto normy byly vytvořeny výborem ISO/IEC JTC1/SC27 a především pracovní skupinou WG2[20].

3.3.1 Registrace kryptografických algoritmů

Problém registrace kryptografických algoritmů poprvé vyvstal s kryptografickým algoritmem DES. Na konci sedmdesátých let byl algoritmus DES přijat jako federální standard státní správy USA FIPS Pub46 (zkratka FIPS znamená Federal Information Processing Standard) a později byl přijat národní normalizační agenturou USA jako národní norma ANSI (X3.92). Rozšíření tohoto algoritmu vedlo ke snahám normalizovat jej jako mezinárodní normu ISO a tato snaha téměř vedla k úspěchu, než byl tento proces normalizace z politických důvodů zastaven (stejně tak byl zastaven proces normalizace algoritmu RSA). Byl přijat názor, že nebude vyvíjena iniciativa ve směru normalizace kryptografických algoritmů jako ISO norem, ale že místo toho bude zaveden proces vytváření mezinárodního registru algoritmů. Proces registrace je definován v normě ISO/IEC 9979. Tento registr umožňuje, aby komunikující strany identifikovaly použité algoritmy a při komunikaci se mohly jednoznačně dohodnout na používaném algoritmu. Slovy normy ISO/IEC 9979 registr slouží jako společný referenční bod pro identifikaci kryptografických algoritmů pomocí jedinečného jména. Registrační autorita spravuje registr a zajišťuje, že položky registru odpovídají registračním procedurám tak, jak jsou definovány v dokumentu ISO/IEC 9979. Registrační autorita nehodnotí kryptografické algoritmy v registru a nevynáší žádné soudy o jejich kvalitě. Registrovaný algoritmus může být:

- Algoritmus, jehož úplný popis je obsažen v registru.
- Algoritmus, jehož úplný popis je definován v některém ISO dokumentu, v normě spravované některým členem ISO nebo spolupracující organizací.
- Algoritmus, který není úplně popsaný.

Pro každý registrovaný algoritmus musí odpovídající položka registru algoritmů obsahovat:

- formální jméno algoritmu
- obchodní jméno algoritmu
- předpokládaný rozsah aplikací
- parametry kryptografického rozhraní
- sadu testovacích hodnot
- název organizace, která žádá o registraci
- datum registrace a modifikací
- informace, zda algoritmus je předmětem národních norem nebo standardů
- informace o relevantních patentech.

Volitelně mohou být v registru uvedeny informace typu:

- seznam odkazů na příbuzné algoritmy
- popis algoritmu
- režimy činnosti (a některé další informace).

[20] význam těchto zkratek je vysvětlen v páté kapitole této příručky.

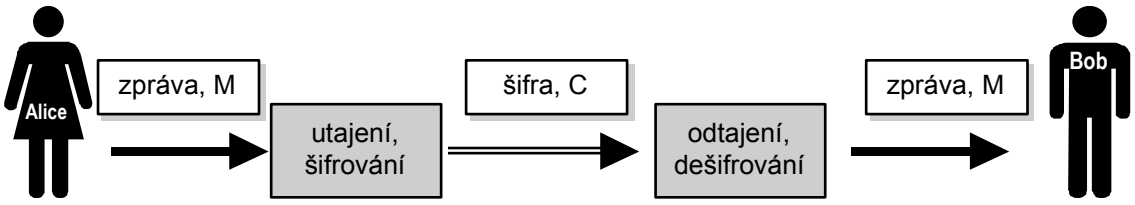
Tvůrci registru kryptografických algoritmů vytvořili tento registr jako reakci na neochotu normalizovat kryptografické algoritmy klasickým způsobem.

Příloha A dokumentu ISO/IEC 9979 definuje, co to je *kryptografický algoritmus pro utajení*, ačkoli obsah registru není omezen pouze na tyto algoritmy. Definice zní: *Kryptografický algoritmus pro utajení je algoritmus, který provádí transformaci dat za účelem ukrytí nebo znovuobjevení jejich informačního obsahu a který používá nejméně jeden tajný parametr.*

3.3.2 Typy kryptografických algoritmů

Kryptografie se používá pro dosažení důvěrnosti (utajení) informace (ochrana proti neautorizovanému zpřístupnění důvěrné informace), pro zaručení *integrity* informace (ochrana proti neautorizované změně dat, resp. ochrana proti nasazení virů do programů), při *autentizaci* (prokázání totožnosti subjektu), při řízení přístupu k objektům i při zaručeném prokazování původu zprávy (*nepopiratelnost*). Kryptografický mechanismus je tvořen dvěma samostatnými (komplementárními) algoritmy, algoritmem šifrování a algoritmem dešifrování, viz obr. 3.1.

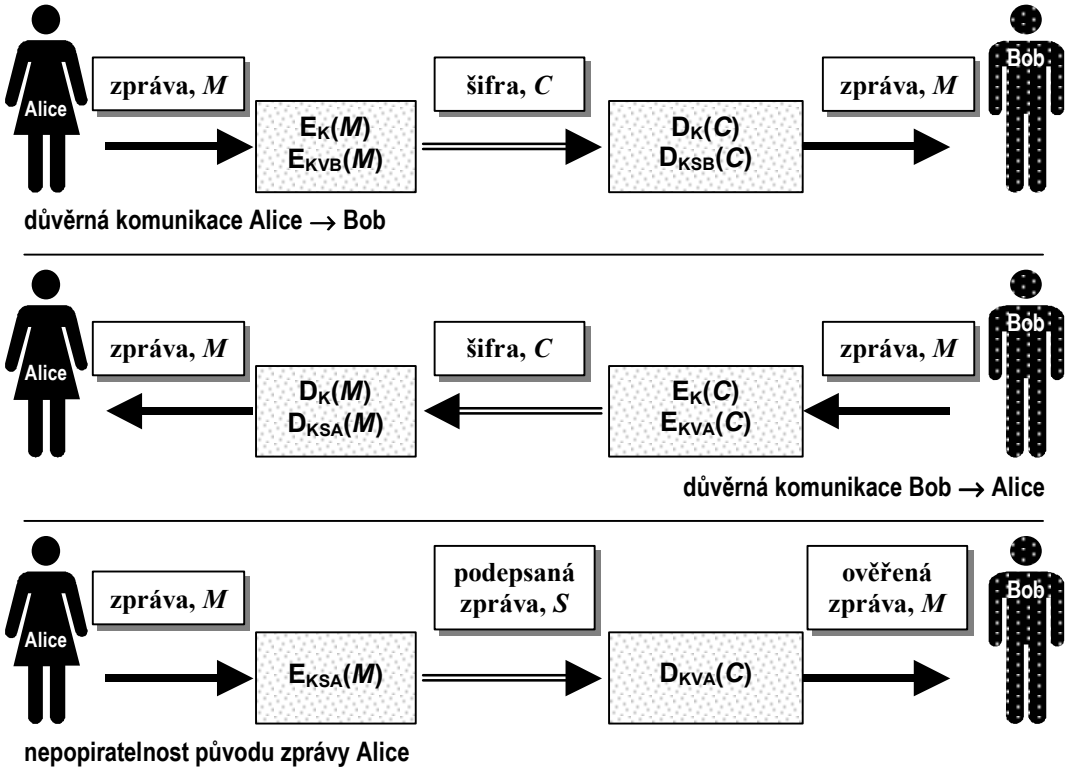
Kryptografický mechanismus je ale tvořen nejen kryptografickým algoritmem, ale i kryptografickým klíčem – jedním ze dvou vstupních parametrů algoritmů šifrování a dešifrování. Pokud komunikující partneři používají stejný kryptografický klíč, $K = K'$, hovoříme o modelu *symetrické kryptografi*e nebo také o *kryptografii s tajným klíčem* – sdílený klíč nazýváme *tajný klíč*. Znalost tajného klíče navíc může sloužit jako důkaz identity, symetrickou kryptografii mimo služby zajištění důvěrnosti lze použít i pro autentizaci. Pokud se kryptografické klíče komunikujících partnerů vzájemně liší, jde o model *asymetrické kryptografie*. Typickým příkladem aplikace asymetrické kryptografie je *kryptografie s veřejným klíčem*, přesněji řečeno dvojicí {*veřejný_klíč, soukromý_klíč*} – kdokoli může srozumitelný (otevřený) text zprávy použitím všeobecně známého veřejného šifrovacího klíče K_V zašifrovat, šifru však může převést zpět do srozumitelného textu pouze ten, kdo vlastní (zná) soukromý dešifrovací klíč K_S.



Obr.3.1 Kryptografický systém

Jedinečnost znalosti soukromého klíče umožňuje použít asymetrický model pro implementaci nejen důvěrnosti a autentizace, ale při splnění jistých, později vyložených, organizačních požadavků i pro implementaci nepopiratelnosti aplikací digitálního podpisu – určité formy šifry, viz obr. 3.2. Princip asymetrické kryptografie je poměrně nová myšlenka, která vznikla teprve v polovině 70. let. V této době matematici zvládli potřebný matematický základ, teorii složitosti, tj. umění pracovat s prokazatelně výpočetně těžkými problémy.

Šifrovač, který po sobě jdoucí části (posloupnosti bitů, resp. bloky) srozumitelného (otevřeného) textu, zprávy M, šifruje stejným klíčem K, se nazývá *blokový šifrovač*. Šifrovač, který generuje „proud“ klíčů K1, K2 ..., kterými jsou šifrovány po sobě jdoucí prvky srozumitelného textu (resp. otevřeného textu nebo zprávy M), se nazývá *proudový šifrovač.*



Obr.3.2 Symetrická a asymetrická kryptografie

3.3.3 Režimy činnosti kryptografických algoritmů

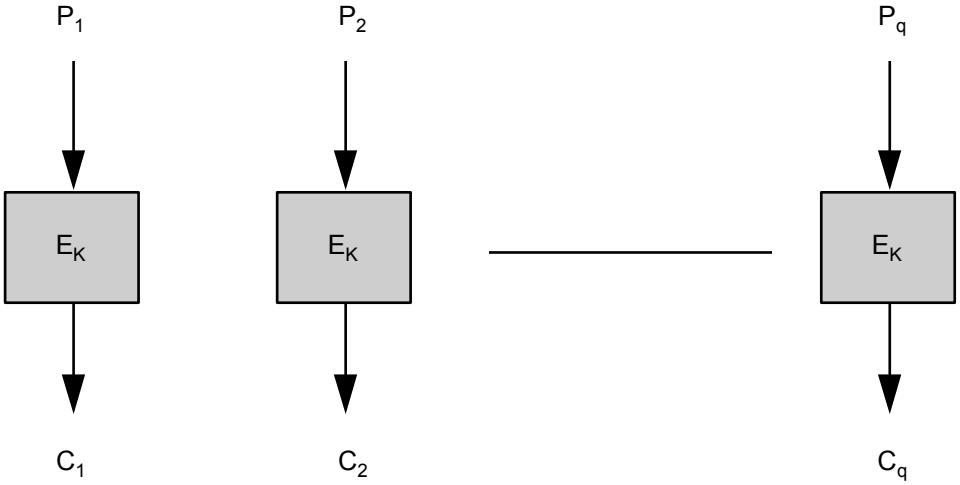
Režim činnosti je pojem, který je používán při blokovém šifrování (tj. kryptografické algoritmy, které šifrují zprávu po blocích pevné délky, např. o velikosti 64 nebo 128 bitů) při šifrování delších dat (zpráv), než je velikost bloku. Režimy činnosti pro kryptografický algoritmus DES byly v USA standardizovány už v roce 1980 v publikaci FIPS Pub. 81 a později v národní normě ANSI X3.106-1983. Tyto režimy činnosti jsou doporučeným způsobem, jak použít algoritmus DES pro zašifrování delšího proudu bitů.

I organizace ISO měla v úmyslu normalizovat režimy činnosti algoritmu DES. Jakmile však bylo rozhodnuto, že algoritmus DES nebude normalizován organizací ISO, byly tyto režimy činnosti normalizovány jako režimy činnosti libovolného blokového šifrovače a výsledkem byly dvě normy: ISO 8372: 1987 (režimy činnosti pro 64bitový blokový šifrovač) a ISO/IEC 10116: 1997 (režimy činnosti pro n-bitový blokový šifrovač). Všechny zmíněné normy (FIPS, ANSI a ISO) zavádějí čtyři režimy činnosti:

- Režim *ECB* (Electronic Code Book)
- Režim *CBC* (Cipher Block Chaining)
- Režim *OFB* (Output FeedBack)
- Režim *CFB* (Ciphertext FeedBack).

3.3.4 Režim ECB

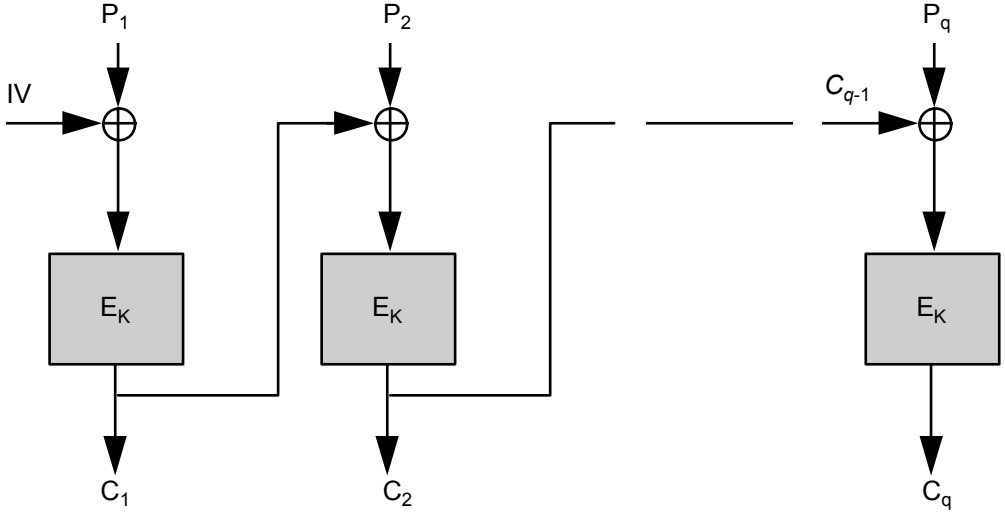
Režim ECB pracuje tak, že srozumitelný otevřený text *P* (Plaintext) je rozdělen na bloky P_i o délce odpovídající délce bloku blokového šifrovače a každý blok je samostatně zašifrován blokovým šifrovačem *E* aplikací stále stejného klíče *K* (viz obr. 3.3). Výsledné bloky se opět spojí do jedné zprávy – šifry C (Ciphertext). Dešifrování se provádí opačným způsobem. Režim ECB se v praxi používá řídce, neboť je vhodný pouze pro případy, kdy šifrovaná zpráva není výrazně delší než velikost bloku blokového šifrovače (např. při šifrování kryptografických klíčů).



Obr. 3.3 Režim ECB

3.3.5 Režim CBC

Podobně jako u režimu ECB i režim CBC pracuje tak, že otevřený text P je rozdělen na bloky o délce odpovídající délce bloku blokového šifrovače a každý blok je blokovým šifrovačem zašifrován samostatně (viz. obr. 3.4).



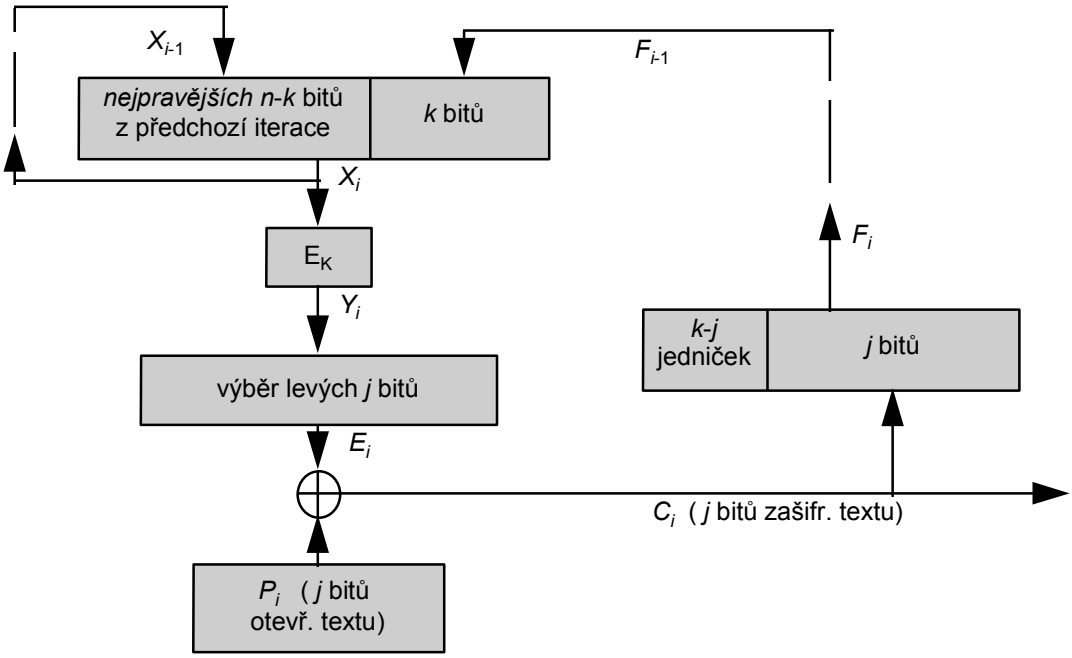
Obr. 3.4 Režim CBC

Na rozdíl od režimu ECB je však pro každý blok před jeho zašifrováním provedena operace XOR (non-ekvivalence, součet mod 2) s předchozím zašifrovaným blokem. Pro první blok zprávy (který nemá žádný předchozí blok) se provádí operace XOR s tzv. *inicializačním vektorem* IV. Tento režim je asi nejpoužívanější režim pro šifrování delších zpráv. Jistou nevýhodou režimu CBC je, že délka šifrované zprávy musí být celistvým násobkem velikosti bloku (pokud tomu tak není, je třeba zprávu na potřebnou délku doplnit).

3.3.6 Režim CFB

U režimu CFB se na rozdíl od předchozích režimů zpráva nerozděluje na bloky, odpovídající velikosti bloku blokové šifry. Místo toho je možno zprávu chápat jako plynulý proud symbolů o libovolné velikosti (velikost symbolu musí být samozřejmě vyjádřena celistvým počtem bitů). Proto musí být pro režim CFB stanoveny dva parametry *j* a *k*, kde *j* odpovídá velikosti symbolu zprávy. V praxi mají parametry *j* a *k* často stejnou hodnotu (viz obr. 3.5).

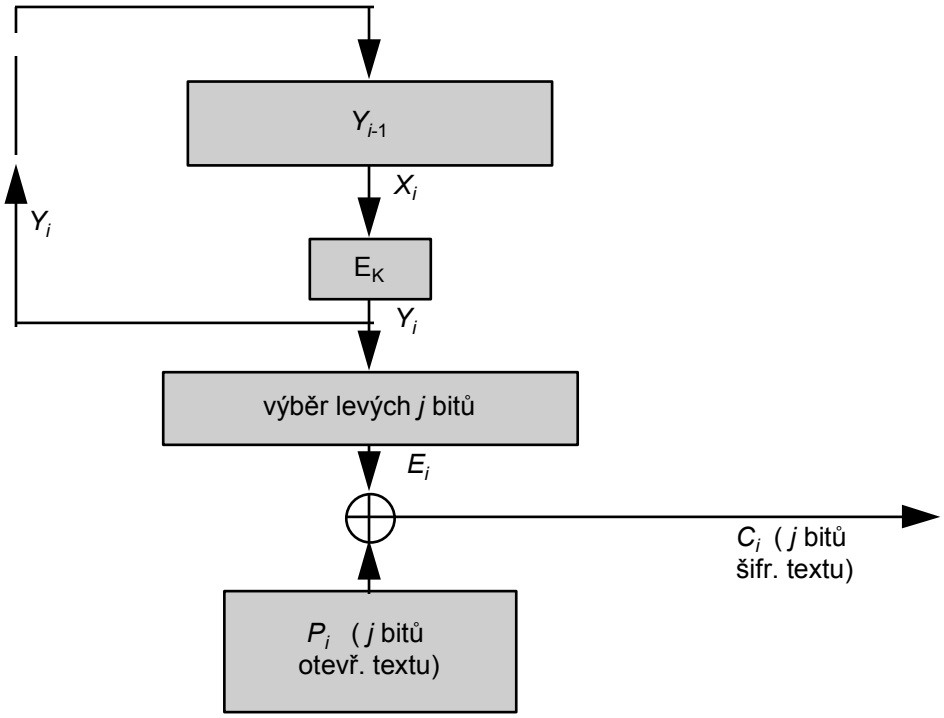
V tomto režimu se šifrovaný text vůbec nestává blokovou šifrou, bloková šifra slouží jako generátor pseudonáhodné posloupnosti (hodnota E), která je pak použita pro zašifrování otevřeného textu (zprávy) operací XOR. Generátor je ovlivňován zpětnou vazbou, branou ze zašifrovaného textu (hodnota F). Zpětná vazba dala tomuto režimu i název – *Ciphertext FeedBack*.



Obr 3.5 Režim CFB

3.3.7 Režim OFB

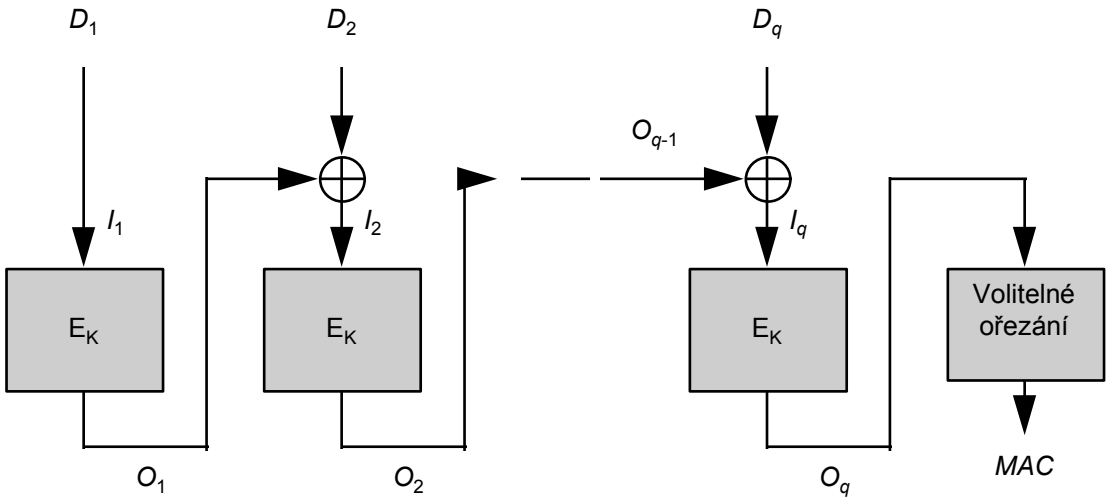
I u režimu OFB se zpráva nerozděluje na bloky, ale opět se chápe jako plynulý proud symbolů o libovolné velikosti. Pro režim OFB je stanoven parametr *j*, který odpovídá velikosti symbolu zprávy (viz obr. 3.6). Šifrovaný text se opět nestává blokovou šifrou, bloková šifra slouží jako generátor pseudonáhodné posloupnosti (hodnota E), která je použita pro zašifrování otevřeného textu (zprávy) operací XOR. Generátor není ovlivňován zašifrovaným textem, ale pouze výstupem samotného generátoru (Y). Zpětná vazba dala tomuto režimu název – *Output FeedBack*.



Obr. 3.6 Režim OFB

3.3.8 Autentizační algoritmus MAC

Autentizační algoritmus MAC (Message Authentication Code) má následující účel: pokud je aplikován na přenášenou zprávu, může si příjemce zprávy ověřit, kdo zprávu zaslal a zda zpráva nebyla změněna při přenosu. První normy, definující algoritmus MAC, jsou normy USA (ANSI X9.9 a ANSI X9.19), které definovaly použití algoritmu MAC v bankovnictví. Později byl tento algoritmus normalizován také mezinárodní normou ISO 8731/1.



Obr. 3.7 Algoritmus MAC

Všechny tyto normy předepisují použití kryptografického algoritmu MAC v režimu CBC (viz předchozí definice) pro vytvoření informace, která je připojena k přenášené zprávě. Tento typ algoritmu MAC se nazývá někdy CBC-MAC. Další mezinárodní normy, definující algoritmus MAC pro použití v bankovnictví, jsou ISO 8730: 1986 (která definuje obecné požadavky na tyto mechanismy) a ISO 8731/2: 1987 (která normalizuje zcela jiný a téměř nepoužívaný algoritmus, zvaný *Message Authenticator Algorithm* (*MAA*)).

V roce 1989 ISO vydala normu pro obecný algoritmus MAC pod číslem ISO/IEC 9797. Tato norma také používá blokovou šifru v režimu CBC. Novější a zpřesněná verze normy ISO/IEC 9797: 1994 definuje metodu, pomocí které se za pomocí klíče a *n*-bitové blokové šifry spočte *m*-bitová kryptografická kontrolní hodnota, kterou je možno použít pro detekování neoprávněné modifikace zprávy. Data jsou zpracovávána v následujících krocích:

- Data jsou zarovnána, aby jejich délka byla celistvým násobkem *n* bitů.
- Data jsou zašifrována pomocí tajného klíče v režimu CBC.

Poslední blok zašifrovaného textu tvoří hodnotu MAC, která může být volitelně „ořezána“.

3.4 Elektronický podpis

Jedním z nejdůležitějších bezpečnostních požadavků, kladených na proces zpracování, ukládání a přenášení informací, je požadavek na zajištění *integrity* těchto dat, tj. požadavek na zabránění neodhalené a neoprávněné modifikaci dat. U samostatných dokumentů je toho obvykle dosahováno tím, že se k datům připojí jistá informace, která příjemci *autentizuje* (tj. prokazuje totožnost) odesílatele nebo tvůrce těchto dat a to pouze v tom případě, že ji příjemce přijal spolu s daty neporušenou. Někdy nastává situace, že nepostačuje, aby příjemce byl přesvědčen o autentičnosti dat, ale aby také byl schopen prokázat tuto skutečnost nezávislé třetí straně. Tato vlastnost se nazývá *nepopiratelnost*.

Technická realizace zajištění autentičnosti dat vychází z předpokladu, že u dat na papírových médiích je autentičnost zajišťována pomocí manuálního podpisu. To přináší potřebu spolehlivé a efektivní náhrady manuálního podpisu podpisem elektronickým (digitálním). Elektronický podpis může být, stejně jako manuální podpis, použit pro identifikaci a autentizaci původce informace. Elektronický podpis může být také použit pro kontrolu, že informace nebyla po podepsání změněna. Tím lze zajistit integritu informace. Na rozdíl od manuálního podpisu však nelze pomocí elektronického podpisu rozlišit originál informace od její kopie.

3.4.1 Vlastnosti elektronického podpisu

Elektronický podpis lze použít pro podepsání elektronického dokumentu (např. souboru) libovolné délky a libovolného obsahu. Elektronický podpis je tvořen řetězcem bajtů, který je připojen k podepisovanému dokumentu. Délka tohoto řetězce bývá obvykle 50 až 300 bajtů podle použitého algoritmu a požadovaného stupně bezpečnosti a nezávisí na délce podepisovaného dokumentu. Elektronický podpis poskytuje příjemci dokumentu následující funkce:

- zajišťuje autenticitu dokumentu
  Příjemce dokumentu bezpečně ví, kdo je autorem dokumentu.
- zajišťuje integritu dokumentu
  Příjemce dokumentu má jistotu, že obsah dokumentu nebyl během přenosu nebo zpracování modifikován.
- zajišťuje nepopiratelnost autora elektronického podpisu
  Autor dokumentu nemůže popřít autorství dokumentu ani jeho obsah.

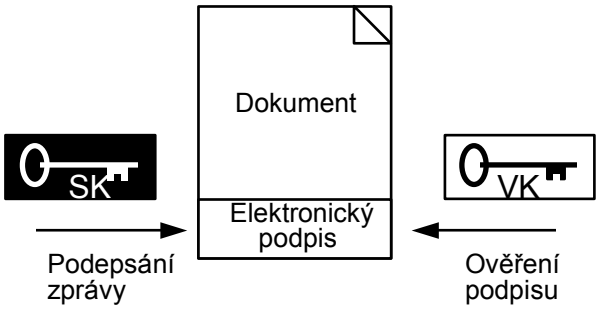
Elektronický podpis má následující vlastnosti:

- Je spojen s jedním konkrétním elektronickým dokumentem (tj. potvrzuje pravost a autenticitu tohoto dokumentu) a nemůže být použit pro podepsání jiného dokumentu.
- Může být vytvořen pouze tím, kdo zná jisté tajemství (nazývané např. *soukromý klíč*).
- Je nemožné vytvořit jiný dokument, sebeméně odlišný od původního dokumentu, pro který by byl původní elektronický podpis stále platný.
- Jakmile je jednou elektronický podpis dokumentu vytvořen, kdokoli si může ověřit pravost tohoto podpisu, a to bez nutnosti znát tajemství (soukromý klíč), kterým byl podpis vytvořen.

Jak je vidět, elektronický podpis zachovává téměř všechny vlastnosti manuálního podpisu vyjma jediné – u dokumentu, podepsaného manuálním podpisem, lze rozlišit jeho kopii od originálu. U dokumentu, podepsaného elektronickým podpisem, kopii od originálu rozlišit nelze.

3.4.2 Kryptografie a elektronický podpis

Pro elektronický podpis se používají kryptografické algoritmy s veřejným klíčem. Nejvíce se používají algoritmy RSA (Rivest Shamir Adleman) a DSA (Digital Signature Algorithm). Proces podepsání zprávy (dokumentu) probíhá v obou případech následovně: nejdříve se spočte zkrácená *charakteristika zprávy* (hash, resp. nepěkně česky – haš). Ta se spočte vhodnou, kryptograficky bezpečnou, jednocestnou hašovací funkcí (v případě algoritmu RSA se používá funkce MD5, v případě algoritmu DSS se používá funkce SHS).



Obr. 3.8 Podepsání dokumentu elektronickým podpisem

Z haše se pak pomocí *soukromého klíče* SK spočte elektronický podpis zprávy, který se připojí ke zprávě. Kdokoli, kdo zná odpovídající *veřejný klíč* VK odesílatele, si může ověřit platnost elektronického podpisu. Pokud je elektronický podpis v pořádku, příjemce má jistotu, že zpráva byla podepsána vlastníkem soukromého klíče a že po podepsání nebyla modifikována.

Příjemce navíc může předložit nezávislé třetí straně zprávu, její elektronický podpis a doklad o veřejném klíči odesílatele jako důkaz o tom, že odesílatel tuto zprávu odeslal a odesílatel tuto skutečnost nemůže popřít. Tato vlastnost se nazývá nepopiratelnost. Elektronický podpis na druhé straně nezajišťuje důvěrnost (utajení) zprávy. Pokud si odesílatel přeje zprávu při přenosu utajit, musí ji ještě navíc zašifrovat (např. algoritmem DES).

3.4.3 Aplikace elektronického podpisu

Jelikož elektronický podpis zajišťuje jak identitu autora, tak i integritu podepsané zprávy, může být použit v nejrůznějších aplikacích. Může být použit např. v systému elektronické pošty. Jakmile odesílatel vytvoří zprávu, může ji podepsat svým soukromým klíčem. Podepsaná zpráva pak může být zaslána příjemci. Jakmile příjemce přijme zprávu a zkontroluje její elektronický podpis, má jistotu, že zpráva byla skutečně odeslána výše zmíněným odesílatelem. Má však také jistotu, že zpráva nebyla po podepsání modifikována.

V právních systémech se často vyskytuje požadavek přiřadit dokumentu časové razítko, které určuje datum a čas, kdy byl dokument vyřízen nebo kdy vstoupil v platnost. K dokumentu v elektronické podobě může být připojeno časové razítko rovněž v elektronické podobě a celý dokument může být podepsán elektronickým podpisem. Použití elektronického podpisu zajistí integritu dokumentu i připojeného časového razítka.

Elektronický podpis může být také použit v systémech pro elektronické provádění plateb EFT (Electronic Fund Transfer). Předpokládejme, že v systému EFT je vytvořena zpráva, která má provést převod 1 000,- Kč z jednoho účtu na druhý. Pokud je tato zpráva zaslána přes nechráněnou datovou síť, může být útočníkem změněna, aby byla převáděná částka 10 000,-Kč. Bez dodatečné informace je pro příjemce velmi obtížné (pokud ne nemožné) určit, zda zpráva byla nebo nebyla modifikována. Pokud je zpráva před odesláním podepsána elektronickým podpisem, příjemce bezpečně pozná, že zpráva byla modifikována a odmítne ji.

Elektronický podpis může být také zabudován do velkého množství obchodních aplikací, které požadují elektronickou náhradu manuálního podpisu. Jedním z příkladů je elektronická výměna dat EDI (Electronic Data Interchange). EDI je systém výměny elektronických informací mezi počítači, ve kterém přenášené informace představují obchodní dokumenty (doklady). EDI lze použít např. pro bezhotovostní platební styk nebo pro elektronický styk s finančním ústavem. Při přenosu dokladu pomocí EDI je elektronický podpis využíván jako přímá náhrada manuálního podpisu přenášených dokladů. Při správné implementaci má elektronický podpis stejnou právní sílu a průkaznost jako podpis manuální.

Uveďme příklad uzavření kontraktu mezi státní správou a dodavatelem pomocí EDI. Orgán státní správy vytvoří poptávkový dokument, podepsaný elektronickým podpisem. Dodavatel, který má zájem odpovědět, si před odpovědí ověří elektronický podpis poptávkového dokumentu. Tím získá jistotu, že poptávkový dokument nebyl během přenosu modifikován a že skutečně pochází od orgánu státní správy. Pak dodavatel vytvoří svou nabídku a podepíše ji elektronickým podpisem. Jakmile orgán státní správy přijme nabídku, zkontroluje její elektronický podpis a ověří si, že nabídka nebyla modifikována a skutečně pochází od dodavatele. Je-li nabídka přijata, orgán státní správy s dodavatelem sjedná smlouvu, která je oběma účastníky podepsána elektronickým podpisem a také oběma účastníky archivována. Pokud by později došlo ke sporu, obsah smlouvy a elektronické podpisy mohou být prověřeny nezávislou třetí stranou (například soudem).

Elektronický podpis může být také užitečný při distribuci softwaru. Software může být po schválení pro distribuci podepsán elektronickým podpisem. Před instalací softwaru na počítači může být elektronický podpis zkontrolován, aby se zajistilo, že se softwarem nebyla provedena žádná změna (jako je např. infekce virem nebo úmyslná modifikace). Elektronický podpis může být později periodicky kontrolován, a tím se zajistí, že ani později během činnosti nebyl software modifikován.

V databázových aplikacích je často velmi důležitá integrita informací, uložených v databázi. Proto v nejrůznějších databázových aplikacích může být použit elektronický podpis pro zajištění integrity. Dokument může být např. podepsán před jeho vložením do databáze. Po pozdějším vyhledání dokumentu v databázi je elektronický podpis zkontrolován. Je-li elektronický podpis správný, uživatel má jistotu, že dokument nebyl modifikován ani podvržen neautorizovaným subjektem. Systém také může ukládat podpisy do auditního záznamu, čímž se získá přehled o uživatelích, kteří informaci v databázi modifikovali.

3.4.4 Bezpečnost elektronického podpisu

Bezpečnost každého kryptografického systému s veřejným klíčem závisí na několika faktorech. Mezi ně patří zejména matematická bezespornost použitého algoritmu, bezpečná správa použitých kryptografických klíčů a bezpečnost implementace systému v konkrétní aplikaci. Například bezpečnost algoritmu DSS je dána množstvím práce, nezbytné k nalezení nebo vypočtení diskrétního logaritmu velmi velkého čísla. V současné době je jediným prostředkem pro zrychlení nalezení diskrétního logaritmu pouze zvyšování výpočetní síly počítačů, které má inkrementální charakter. Parametry zvoleného algoritmu jsou navrženy tak, že zrychlování výpočetní techniky nemůže bezpečnost elektronického podpisu v potřebném časovém horizontu (desítky let) ohrozit. Z toho plyne, že útočník, který nezná soukromý klíč subjektu, nemůže vypočíst elektronický podpis subjektu. To znamená, že elektronický podpis nemůže být podvržen.

Elektronický podpis bývá někdy zaměňován s digitalizovaným podpisem. Digitalizovaný podpis se vytvoří tak, že se manuální podpis zkonvertuje do podoby elektronického obrazu. Nejenže však digitalizovaný podpis nemůže nahradit elektronický podpis, nemůže dokonce nahradit ani samotný manuální podpis. Digitalizovaný podpis může být podvržen. Může být duplikován nebo připojen k jinému dokumentu. A nemůže být ani použit ke kontrole, zda dokument nebyl po podepsání modifikován.

3.4.5 Podpůrné funkce

Mezi funkce, které jsou nezbytné pro použití elektronického podpisu, patří:

- Funkce pro vytvoření kryptografického kontrolního součtu zprávy. Kryptografický kontrolní součet je zhuštěnou reprezentací informace, která má být podepsána. Použitý algoritmus kryptografického kontrolního součtu musí zajistit, že je výpočetně nezvládnutelné nalézt k danému kontrolnímu součtu odpovídající zprávu nebo nalézt dvě různé zprávy, které mají stejný kryptografický kontrolní součet. Mezi vhodné algoritmy patří zejména MD5 a SHS.
- Pro generování páru veřejný klíč/soukromý klíč je nezbytný kryptograficky bezpečný generátor náhodných čísel. Lze použít buď hardwarový šumový generátor náhodných čísel, nebo softwarový generátor pseudonáhodných čísel.
- Pro rutinní používání elektronického podpisu je nezbytný mechanismus spojení veřejného klíče a jeho vlastníka. To znamená, že musí existovat bezpečný způsob, jak ke každé identifikaci subjektu zjistit jeho veřejný klíč. Mechanismus může být založen např. na certifikační autoritě, která generuje certifikáty, obsahující identifikaci subjektu a jeho veřejný klíč.
- Pro úspěšnou implementaci je však třeba zvládnout i některé systémové, organizační a právní otázky. Například může být nezbytné zajišťovat centrální registraci veřejných klíčů uživatelů v adresáři nebo získávání časových razítek dokumentů. Zde musí být vzaty v úvahu právní náležitosti, jako např. zodpovědnost certifikační autority, přijímání elektronicky podepsaných dokumentů orgány státní správy a důkazní síla elektronického podpisu u soudu. V konkrétní aplikaci je rovněž třeba vyřešit některé technické detaily, jako jsou mechanismy generování a distribuce certifikátů a mechanismy rušení platnosti certifikátů.

3.4.6 Příklad aplikace elektronického podpisu ve státní správě

Ve státní správě mnoha zemí je elektronický podpis běžně používán. Zde uvedeme pouze několik příkladů z USA. Všechny federální orgány USA (včetně orgánů ministerstva obrany) mohou používat elektronický podpis (implementovaný na základě standardů DSS a SHS) pro podepisování neklasifikovaných informací. Ministerstvo obrany ve vybraných aplikacích používá DSS i pro podepisování klasifikovaných dat. Ústřední účetní úřad (GAO) vydal rozhodnutí, že elektronický podpis může být použit pro vytváření platných hospodářských smluv a závazků. Tento úřad rovněž rozhodl, že dokumenty, vytvářené v systémech EDI (Electronic Data Interchange), které jsou podepsány pomocí DSS, budou chápány jako platné důkazní materiály.

3.4.7 Normy ISO pro elektronický podpis

Existující mezinárodní normy ISO, které definují mechanismy pro elektronický podpis, se zabývají pouze elektronickými podpisy, založenými na asymetrické kryptografii, které nazýváme digitálním podpisem. Jedná se především o normy ISO/IEC 14888 (definuje digitální podpis s „přívažkem“), ISO/IEC 10118 (definuje rozptylovací funkce), ISO/IEC 13888 (definuje mechanismy pro nepopiratelnost) a ISO/IEC 15946 (definuje mechanismy pro kryptografii pomocí eliptických křivek).

3.4.7.1 ISO/IEC 14888

Norma obsahuje definici několika mechanismů pro tzv. digitální podpis s „přívažkem“ (kde pojmem „přívažek“ se chápe zašifrovaná hodnota samotného digitálního podpisu, která se přidává k přenášené zprávě). V současné době obsahuje tyto části:

- ISO/IEC 14888-1: 1998: Obecný úvod
- ISO/IEC DIS 14888-2: Mechanismy založené na identitě
- ISO/IEC 14888-3: 1998: Mechanismy založené na certifikátech (včetně algoritmu DSA, *Digital Signature Algorithm*)

3.4.7.2 ISO/IEC 10118

Rozptylovací funkce (jednocestné funkce, hašovací funkce) jsou často nedílnou součástí mechanismu digitálního podpisu. Proto byla vytvořena zvláštní norma, který se zabývá těmito mechanismy. Norma obsahuje čtyři části:

- ISO/IEC 10118-1: 1994 obsahuje definice a základní vysvětlení pro ostatní části normy
- ISO/IEC 10118-2: 1994 definuje rozptylovací funkce založené na blokové šifře
- ISO/IEC 10118-3: 1998 definuje tři algoritmy, vyvinuté speciálně jako rozptylovací funkce: SHA-1, RIPEMD-128 a RIPEMD-160
- ISO/IEC 10118-4: 1998 definuje rozptylovací funkce založené na modulární aritmetice: MASH-1 a MASH-2

3.4.7.3 ISO/IEC 13888

Norma ISO/IEC 13888, která byla nedávno dokončena, se zabývá mechanismy, které poskytují funkci nepopiratelnosti. Nezabývá se pouze digitálním podpisem, ale všemi mechanismy, které

mohou poskytovat službu nepopiratelnosti. Část 1 této normy se zabývá obecným modelem pro poskytování funkce nepopiratelnosti, včetně vymezení role důvěryhodné třetí strany (TTP, Trusted Third Party). Část 2 diskutuje mechanismy zajištění nepopiratelnosti pomocí symetrické kryptografie. Tato schémata vyžadují in-line zapojení důvěryhodné třetí strany. Část 3 pokrývá nejčastější implementaci funkce nepopiratelnosti pomocí asymetrické kryptografie.

3.4.7.4 ISO/IEC 15946

Norma ISO/IEC 15946 se zabývá kryptografickými mechanismy, založenými na eliptických křivkách (Elliptic Curve Cryptography). Tato norma je zatím v raných začátcích svého vývoje.

3.5 Bezpečnostní požadavky na kryptografické moduly

Kryptografické bezpečnostní mechanismy mohou být využity v nejrůznějších počítačových a telekomunikačních aplikacích (např. uchovávání dat, řízení přístupu a identifikace, datová, hlasová a obrazová komunikace) a v nejrůznějších prostředích (státní správa, bankovnictví a finančnictví, podnikání). Úroveň bezpečnosti kryptografického modulu musí být zvolena tak, aby zajišťovala dostatečnou ochranu dat v závislosti na bezpečnostních požadavcích, provozním prostředí a poskytovaných službách. Následující požadavky specifikují bezpečnostní požadavky, které musí splňovat kryptografické moduly, použité v bezpečnostních mechanismech, ochraňujících neklasifikované i klasifikované informace v počítačových a telekomunikačních informačních systémech. Zahrnují implementace kryptografických modulů ve formě hardwarových komponent nebo modulů, softwarových programů nebo modulů, firmwarových modulů a v libovolné kombinaci předchozích případů. Ve standardu [FIPS140] jsou definovány čtyři kvalitativní třídy bezpečnosti – třída 1, třída 2, třída 3 a třída 4. Tyto třídy pokrývají širokou škálu potenciálních aplikací a provozních prostředí, ve kterých je kryptografický modul nasazen. Bezpečnostní požadavky se vztahují zejména na oblasti návrhu a implementace kryptografického modulu, jako je základní návrh, dokumentace, rozhraní modulu, autorizované role a služby, fyzická bezpečnost, bezpečnost softwaru, bezpečnost operačního systému, správa klíčů, použitý kryptografický algoritmus, elektromagnetická kompatibilita a autonomní testy.

3.5.1.1 Třída 1

Třída 1 poskytuje nejnižší míru bezpečnosti. Tato třída specifikuje pouze základní bezpečnostní požadavky na kryptografický modul (např. použití *standardizovaného nebo registrovaného* algoritmu). Pro kryptografický modul v této třídě nejsou požadovány žádné fyzické bezpečnostní mechanismy. Příkladem hardwarových kryptografických modulů ve třídě 1 jsou zásuvné šifrovací karty do osobních počítačů a přenosné šifrovací adaptéry (např. PCMCIA karty), které slouží k distribuci klíčů nebo k samotnému šifrování. Třída 1 také zahrnuje softwarové kryptografické mechanismy, implementované na osobních počítačích. Tyto implementace mohou být odpovídající v prostředích s nízkými požadavky na bezpečnost. Softwarová implementace kryptografických mechanismů na osobních počítačích je cenově mnohem přístupnější než hardwarové řešení. Zahrnutí softwarových kryptografických mechanismů na PC do třídy 1 dovoluje uživatelům, aby se vyhnuli situaci, kdy z důvodů vysoké ceny hardwarového řešení raději neimplementují žádné bezpečnostní mechanismy.

3.5.1.2 Třída 2

Pro hardwarové kryptografické moduly třída 2 zavádí požadavky na fyzické zabezpečení kryptografického modulu pomocí obalu s evidencí fyzického útoku nebo uzamčení zámkem. Obal s evidencí fyzického útoku, jenž je dnes běžně dostupný, musí být nevratně porušen při každém pokusu o fyzický přístup ke kryptografickým klíčům nebo jiným kritickým parametrům. Zámky jsou umístěny na skříň nebo dvířka modulu za účelem zabránění fyzickému přístupu k modulu. Tyto bezpečnostní mechanismy jsou cenově dostupné pro širokou škálu aplikací. Třída 2 musí zajistit autentizaci rolí, která zajišťuje, že modul autentizuje roli operátora a kontroluje jeho autorizaci k prováděným operacím s modulem. Třída 2 rovněž dovoluje implementaci softwarových kryptografických modulů ve víceuživatelských operačních systémech s certifikací alespoň (E2, F-C2) podle kritérií ITSEC, tj. C2 podle kritérií TCSEC.

3.5.1.3 Třída 3

Třída 3 předepisuje pro hardwarové moduly zvýšenou míru fyzické bezpečnosti. Zatímco ve třídě 2 je požadován pouze zámek nebo obal s evidencí fyzického útoku, ve třídě 3 jsou požadovány bezpečnostní mechanismy, které zabrání útočníkovi v získání kritických parametrů, umístěných uvnitř modulu. Například vícečipový kryptografický modul musí být umístěn v pevné schránce a musí být zajištěno, že při pokusu o otevření této schránky budou kritické parametry v modulu vynulovány. Kryptografické moduly s těmito fyzickými bezpečnostními mechanismy jsou dnes běžně komerčně dostupné. Třída 3 musí zajistit autentizaci subjektů, jež je silnější než autentizace rolí, požadovaná ve třídě 2. Modul musí autentizovat identitu operátora a kontroluje jeho autorizaci k prováděným operacím s modulem. Třída 3 obsahuje přísnější požadavky na vstup a výstup kritických parametrů. Datové brány, používané pro tyto parametry, musí být fyzicky odděleny od ostatních datových bran. Pokud parametry jsou do modulu vkládány přímo (tak, že neprocházejí jinými částmi systému), mohou být vkládány v nezašifrované podobě. V opačném případě musí být vkládány v zašifrované podobě. Třída 3 dovoluje implementaci softwarových kryptografických modulů ve víceuživatelských operačních systémech s certifikací alespoň (E3, F-B1) podle kritérií ITSEC, tj. B1 podle kritérií TCSEC. Systém musí poskytovat důvěryhodný kanál pro vkládání kritických parametrů. Systém s certifikací (E3, F-B1) nebo lepší je požadován proto, aby bylo zajištěno oddělení kryptografického modulu od jiného nedůvěryhodného softwaru, který běží v systému.

3.5.1.4 Třída 4

Moduly ve třídě 4 poskytují nejvyšší úroveň bezpečnosti. Ačkoli většina běžně komerčně dostupných kryptografických modulů nesplňuje požadavky této třídy, existují informační systémy, kde je tato nejvyšší úroveň bezpečnosti požadována. Pro hardwarové moduly požaduje třída 4 nepřekonatelnou fyzickou ochranu modulu. Zatímco fyzická bezpečnostní opatření modulů ve třídě 3 mohou být překonána vysoce motivovaným a technicky vybaveným útočníkem, třída 4 požaduje ochranu proti jakémukoli fyzickému útoku. Pokud se například útočník pokusí proříznout obal kryptografického modulu, pokus musí být detekován a kritické parametry musí být vymazány. Moduly ve třídě 4 jsou v zásadě určeny pro práci v prostředí bez jakékoli fyzické ochrany, kde útočník může do modulu jakkoli zasahovat. Moduly ve třídě 4 musí být také chráněny proti prozrazení kritických parametrů v důsledku změny provozní teploty nebo provozních napětí mimo povolený rozsah. Modul musí být zabezpečen proti takovýmto změnám vnějšího prostředí nebo musí tyto změny detekovat a následně vymazat kritické parametry. Třída 4 dovoluje implementaci softwarových kryptografických modulů ve víceuživatelských operačních systémech s certifikací alespoň (E4, F-B2) podle kritérií ITSEC, tj. B2 podle kritérií TCSEC.

4. Správa bezpečnosti IT

Problematiku správy bezpečnosti systémů IT si budeme schematicky ilustrovat na několika příkladech řešení z oblasti distribuovaných systémů IT. Použití distribuovaných systémů IT je pro stávající éru a nejbližší budoucnost bezesporu nejrozšířenější informační technologií.

4.1 Bezpečnostní architektura sítí podle ISO 7498-2

Jako první ilustrační příklad řešení problematiky správy bezpečnosti uvedeme mezinárodní normu ISO 7498-2 ISO/OSI Security Architecture, která definuje *základní bezpečnostní služby pro komunikační sítě*. Norma ISO 7498-2, vydaná rovněž jako doporučení mezinárodní telekomunikační unie ITU-T X.800, ve svých částech definuje sféry své platnosti charakterizovatelné následujícím výčtem: bezpečnostní domény a politiky, funkce prosazující bezpečnost (bezpečnostní služby), bezpečnostní mechanismy a správa bezpečnosti. Jedná se o dodatek normy ISO 7498, Referenční model propojování otevřených systémů (RM OSI, Reference Model of Open System Inter-connection) z konce osmdesátých let. Zabývá se bezpečnostní architekturou otevřených systémů, zavádí standardní definice termínů z bezpečnosti IT, uvádí standardní popisy bezpečnostních funkcí a bezpečnostních mechanismů, definuje, ve které vrstvě hierarchicky uspořádané architektury OSI lze bezpečnostní funkce poskytovat a zavádí pojem *správy bezpečnosti*. Jednotlivé vrstvy RM OSI v sestupném pořadí plní následující funkce:

- vrstva 7 – *aplikační*:
  poskytuje aplikačně orientované služby
- vrstva 6 – *prezentační*:
  koordinuje kódování a syntaxi vyměňovaných dat
- vrstva 5 – *relační*:
  poskytuje pro IS nástroje pro řízení a synchronizaci jejich dialogů
- vrstva 4 – *transportní*:
  zvyšuje kvalitu komunikačních spojů na požadovanou úroveň
- vrstva 3 – *síťová*:
  směruje tok dat komunikačními spoji sítě(í); data jsou za účelem směrování a přenosu komunikačními spoji organizována do paketů
- vrstva 2 – *spojová*:
  organizuje telekomunikační provoz po datovém spoji; prostý proud bitů přenášený fyzickou vrstvou mění na spolehlivou cestu přenosu bloků dat (rámců)
- vrstva 1 – *fyzická*:
  přenáší prostý proud bitů přenosovým médiem.

Na komunikační relaci mezi dvěma vzdálenými aplikačními partnery se účastní

- v koncových komunikujících uzlech sítě protokoly všech vrstev,
- v mezilehlých uzlech na komunikační cestě protokoly dolních tří vrstev (fyzická, spojová, síťová).

Typická implementace aplikačního systému využívá pro komunikační účely služeb transportní, relační, prezentační a aplikační vrstvy.

4.1.1 Bezpečnostní služby ISO 7498-2

Bezpečnostní služby, popsané v normě, mohou být v praxi implementovány na různých vrstvách komunikačních protokolů. V souladu s normou ISO 7498-2 dělíme bezpečnostní služby do následujících skupin:

- služby pro autentizaci
  V počítačových sítích je mnoho typů subjektů, které musí nebo mohou být identifikovány a autentizovány. Jde především o fyzické subjekty (např. uzly sítě, směrovače atd.), logické subjekty (typicky procesy) a lidské subjekty (např. uživatele a správce). Identifikací rozumíme určení jednoznačné identity subjektu bez jejího ověřování. Autentizací rozumíme ověření proklamované identity subjektu.
  Služby pro autentizaci mají za úkol provádět autentizaci (ověření totožnosti) jedné nebo obou stran při komunikaci. Služby pro autentizaci se dělí na služby *autentizace odesílatele* a služby *autentizace spojení*. Služby *autentizace odesílatele* autentizují pouze odesílatele zprávy a nemusí poskytovat ochranu před duplikováním zpráv útočníkem. Služby *autentizace spojení* poskytují autentizaci platnou během celého navázaného spojení a zabraňují duplikování zpráv útočníkem.

- služby pro řízení přístupu
  Služby, poskytující *řízení přístupu*, zajišťují ochranu před neautorizovaným použitím prostředků, dostupných prostřednictvím distribuovaného systému. Tyto služby však bývají málokdy součástí síťových protokolů a často jsou implementovány až v operačním systému či aplikaci.

- služby pro zajištění důvěrnosti
  Tato skupina služeb poskytuje ochranu přenášených dat před neautorizovaným odhalením. Služba pro *důvěrnost přenosu zpráv* poskytuje ochranu před neautorizovaným odhalením bez ohledu na navázaná spojení. Proto je tato služba vhodná pro bezkontextové aplikace. Služba pro *důvěrnost spojení* zajišťuje ochranu před neautorizovaným odhalením v rámci navázaného spojení. Tato služba vyžaduje navázání spojení. Služba *důvěrnost toku dat* (Traffic Flow Confidentiality) má za úkol zabránit útočníkovi, aby ze znalosti toku dat (adresy přenášených zpráv, délky přenášených zpráv, časové intervaly mezi přenášenými zprávami atd.) dokázal odvodit důvěrné informace o přenášených datech. Služba *selektivní důvěrnost* má za úkol zajistit důvěrnost pouze některých částí přenášené zprávy.

- služby pro zajištění integrity
  Tato skupina služeb poskytuje ochranu přenášených dat před neautorizovanou modifikací. Služba *integrita přenosu zpráv* poskytuje ochranu před neautorizovanou modifikací bez ohledu na navázaná spojení. Služba *integrita spojení* zajišťuje ochranu před neautorizovanou modifikací v rámci navázaného spojení. Tato služba vyžaduje navázání spojení. Služby *selektivní integrita spojení* a *selektivní integrita zpráv* mají za úkol zajistit integritu pouze některých částí přenášené zprávy.

- služby pro nepopiratelnost zodpovědnosti.
  Služby *nepopiratelnost odesílatele* a *nepopiratelnost doručení* slouží k tomu, aby příjemce (odesílatel) mohl prokázat protistraně odeslání (přijetí) zprávy, a tím zabránil pozdějšímu popření této akce protistranou.

4.1.2 Implementace bezpečnostních služeb ve vrstvách OSI

Následující tabulka ukazuje, ve kterých vrstvách referenčního modelu ISO OSI by měly být bezpečnostní služby implementovány. V tabulce písmeno A znamená, že vrstva je vhodná pro implementaci odpovídající bezpečnostní služby. Z tabulky je zřejmé, že samotná aplikační vrstva 7 může teoreticky implementovat všechny bezpečnostní služby. Z ostatních vrstev jsou nejvhodnější pro implementaci bezpečnostních funkcí vrstvy 3 a 4. Jak tuto skutečnost interpretovat? Lze říci, že veškerá bezpečnostní opatření je potřeba přijmout nejníže na úrovni transportu dat, nižší vrstvy, tj. směrování, datový spoj a přenos médiem, nemusí být důvěryhodné.

	Vrstva, na které může být služba zajišťována						
Bezpečnostní služba	1	2	3	**4**	**5**	**6**	**7**
Autentizace spojení			A	**A**			**A**
Autentizace odesílatele			A	**A**			**A**
Řízení přístupu			A	**A**			**A**
Důvěrnost spojení	A	A	A	**A**		**A**	**A**
Důvěrnost přenosu zpráv		A	A	**A**		**A**	**A**
Selektivní důvěrnost						**A**	**A**
Důvěrnost toku dat	A		A				**A**
Integrita spojení s opravou				**A**			**A**
Integrita spojení bez opravy			A	**A**			**A**
Selektivní integrita spojení							**A**
Integrita přenosu zpráv			A	**A**			**A**
Selektivní integrita zpráv							**A**
Nepopiratelnost odesílatele							**A**
Nepopiratelnost doručení							**A**

V dokumentech ISO jsou mimo výše uvedené bezpečnostní služby také definovány bezpečnostní mechanismy, kterými se služby mají implementovat. Jedná se o následující mechanismy:

- šifrování (kryptografické zabezpečení)
- elektronický podpis
- mechanismy řízení přístupu
- integritní mechanismy (kryptografické)
- kryptografická autentizace
- zarovnávání zpráv
- řízení směrování
- notářské služby.

Přiřazení bezpečnostních mechanismů jednotlivým službám ilustruje následující tabulka.

Bezpečnostní služba	Mechanismus							
	Šifrování	El. podpis	Řízení přístupu	Integritní mecha-nismy	Krypt. autenti-zace	Zarovná-vání zpráv	Řízení směrová-ní	Notářské služby
Autentizace spojení	A	A			A			
Autentizace odesílatele	A	A						
Řízení přístupu			A					
Důvěrnost spojení	A						A	
Důvěrnost přenosu zpráv	A						A	
Selektivní důvěrnost	A							
Důvěrnost toku dat	A					A	A	
Integrita spojení s opravou	A			A				
Integrita spojení bez opravy	A			A				
Selektivní integrita spojení	A			A				
Integrita přenosu zpráv	A	A		A				
Selektivní integrita zpráv	A	A		A				
Nepopiratelnost odesílatele	A	A		A				A
Nepopiratelnost doručení	A	A		A				A

4.1.3 ISO služby pro bezpečnou komunikaci podle ISO 7498-2

Bezpečná komunikace v normě ISO 7498-2 je definována jako komunikace, při které:

- lze důvěřovat, že oba komunikující partneři komunikují s oznámeným partnerem
  byla tedy provedena vzájemná autentizace nebo alespoň autentizace zdroje dat při použití nespojované, datagramové služby
- nikdo nemůže provádět odposlech
  protože je zajištěna důvěrnost
- nikdo nemůže přenášenou informaci měnit
  protože jsou přijata opatření zajišťující integritu
- komunikační služby jsou dostupné jen pro autorizované uživatele
  bylo tedy aplikováno odpovídající řízení přístupu,
- nikdo nemůže popřít komunikaci
  je zajištěna jak nepopiratelnost vyslání, tak i nepopiratelnost příjmu.

Bezpečná spojovaná relace podle normy ISO 7498-2 je tvořena následujícími kroky:

- Navázání spojení se zaručenou vzájemnou autentizací pomocí asymetrické kryptografie, tj. veřejným a privátním klíčem.
- Při navázání spojení se získají klíče pro symetrické šifrování tajnými klíči zabezpečujícími integritu a důvěrnost následující fáze.
- Proběhne přenos informace se zabezpečenou integritou a důvěrností.
- Spojení se zruší tak, aby v síti nezůstala žádná data.
- Ověří se ty podepsané informace, u nichž je to předepsáno nebo vyvoláno podezřením o narušení bezpečnosti apod.

Integrita spojení se zajišťuje tak, že buď postačí tzv.

- *slabá integrita*
  aplikují se kontrolní součty, CRC, číslování zpráv apod.; slabá integrita zajišťuje ochranu proti modifikaci zpráv šumem, proti náhodné změně pořadí, náhodným duplicitám apod.,

nebo v *případě* hrozby útoku aktivním útočníkem se musí použít tzv.

- *silná integrita*
  je zaručena prostředky pro zajištění slabé integrity doplněné o aplikaci prostředků kryptografie symetrickým klíčem — zabezpečení je důvěrné.

Podíváme-li se na problém, kde lze implementovat funkce a mechanismy OSI SA, pak lze vyslovit následující závěry.

- Pro *autentizaci* je vhodné využít mechanismy z oblasti asymetrické a symetrické kryptografie. Oba komunikační partneři se autentizují při vzájemné spojované komunikaci, při nespojované komunikaci se autentizují pouze původci dat. Aplikačně orientovanou autentizaci lze implementovat v aplikační, 7. vrstvě RM OSI, implementace autentizace v nižších vrstvách má jistý globalizační charakter – vztahuje se na všechny procesy z daného uzlu při implementaci v síťové, 3. vrstvě (virtuální privátní sítě), resp. na všechny akce v rámci jedné relace při implementace na úrovni transportní, 4. vrstvy.
- Zajišťuje se *slabá* nebo *silná integrita*, silná využívá pro utajení kontrolních informací prostředků symetrické kryptografie společně sdíleným tajným klíčem. Integrita se může zajišťovat i s opravami nebo může být bez oprav, pouze detekční. Lze integritně zabezpečovat celé zprávy nebo jen vybraná pole zpráv. Provádět ji lze prakticky nejníže ve 4. (transportní) vrstvě, vybraná pole zpráv se musí integritně zabezpečovat v 7. (aplikační) vrstvě.
- Pro *utajování* se opět používá z důvodu rychlosti symetrická kryptografie tajným sdíleným klíčem. Může se provádět utajování jak celých zpráv, tak i vybraných polí zpráv, nebo i utajování toku zpráv. Utajování se smí de facto dělat nejníže ve 4. (transportní) vrstvě, pokud se má uplatnit na vybraná pole zpráv, pak se musí realizovat v 7. (aplikační) vrstvě.
- *Nepopiratelnost* se zajišťuje jednak *s prokázáním původu* a jednak *s prokázáním doručení*. Princip je opřen o existenci třetí, nezávislé strany, *notáře*. Je třeba si uvědomit, že autentizace znamená, *že vím, s kým komunikuji*, a nepopiratelnost, resp. neodmítnutelnost, znamená, že *vím, s kým komunikuji a navíc to mohu dokázat*. Implementace nepopiratelnosti je záležitost 7. (aplikační) vrstvy.
- Pro *řízení přístupu* se obvykle používají dostupné mechanismy použitých podpůrných operačních systémů, případně se doplňují mechanismy v 7. (aplikační) vrstvě.

4.1.4 Správa bezpečnosti podle ISO 7498-2

ISO 7498-2 definuje správu bezpečnosti jako řízení a distribuci informací pro:

- poskytování bezpečnostních funkcí a bezpečnostních mechanismů
- generování zpráv o bezpečnostních funkcích a bezpečnostních mechanismech
- generování zpráv o událostech souvisejících s bezpečností.

ISO 7498-2 zavádí pojem *informační báze správy bezpečnosti* (Security Management Information Base, SMIB), která je součástí celkové informační správní báze (Management Information Base, MIB). SMIB může obsahovat tabulky dat, soubory a data nebo pravidla zabudovaná v softwaru / hardwaru. Správa bezpečnosti se dělí do čtyř kategorií:

- správa systémové bezpečnosti
  - správa bezpečnostních aspektů celého systému
  - správa bezpečnostní politiky
  - interakce s ostatními správními funkcemi (protokolování, správa chybového řízení)
  - správa reakcí na události
  - správa bezpečnostního auditu a obnovy
  - správa politiky řízení přístupu
- bezpečnost správy sítě (OSI)
- správa jednotlivých bezpečnostních funkcí
  - výběr bezpečnostních mechanismů pro implementaci bezpečnostních funkcí
  - nalezení dostupných bezpečnostních mechanismů
- správa bezpečnostních mechanismů
  - správa šifrování, správa řízení přístupu, správa integrity dat, správa autentizace, správa utajení přenosu, správa řízení směrování, správa notarizace.

Důležitou součástí správy bezpečnosti je *bezpečnostní audit*, tj. zkoumání a prohlížení auditních záznamů o událostech a o aktivitách souvisejících s bezpečností. Cílem je především testování adekvátnosti zvolených systémových nástrojů pro plnění zavedené bezpečnostní politiky provozních procedur a získání podkladů pro vyslovení doporučení pro změnu přijatých bezpečnostních opatření, politiky a procedur. Zdrojem pro bezpečnostní audit jsou auditní záznamy. Mezi zásadní rozhodnutí o bezpečnostním auditu patří rozhodnutí o tom, co se bude sledovat a jak výběrové sledování bude probíhat. Bezpečnostní audit bohužel součástí normy ISO 7498-2 nebyl.

Správa klíčů je základem všech kryptograficky orientovaných bezpečnostních mechanismů. Zahrnuje rozhodování o tom, kdy je potřeba obnovit klíče, vlastní generování klíčů a bezpečnou distribuci klíčů. Existuje mnoho norem správy klíčů v bankovních sítích a existuje i norma ISO/IEC 11770. Ta ve své prvé části ISO/IEC 11770-1 z r. 1997 definuje systém správy klíčů, ve své druhé části ISO/IEC 11770-2 z r. 1996 specifikuje techniky distribuce klíčů založené na bázi symetrické kryptografie a její třetí část ISO/IEC 11770-3, která bude v dohlednu zveřejněna, specifikuje techniky distribuce klíčů a techniky dohody na klíči, založené na bázi asymetrické kryptografie.

Konečně součástí správy bezpečnosti je i plnění podmínek předepisovaných požadovanou (stanovenou) úrovní *zaručitelnosti bezpečnosti IT*. Při návrhu bezpečného IS s určenou úrovní zaručitelnosti bezpečnosti je potřeba vyřešit dva základní problémy:

- určení adekvátní bezpečnostní funkcionality IS – co a jak (kvalitně, dokonale, silně …) musí systém umět
- dosažení požadované úrovně jistoty, že IS se z hlediska bezpečnosti provozuje tak, jak byl specifikován.

Dosažená úroveň zaručitelnosti bezpečnosti se odvozuje z vyhodnocování vlastností IS podle stanovených hodnotících kritérií. Jejich aplikace je vysvětlována v poslední kapitole příručky.

4.2 Norma bezpečnostních služeb IT ISO/IEC 10181

Novější norma, zabývající se bezpečnostními službami v otevřených systémech, je dokument ISO/IEC 10181 Security Frameworks for Open Systems. Rozsah ISO/IEC 10181 je širší než byl rozsah dokumentu ISO 7498-2. Dokument ISO/IEC 10181 je navržen tak, aby pokrýval všechny otevřené systémy a ne pouze ty, které odpovídají OSI modelu (např. databázové systémy, návrhové systémy). Každá z jednotlivých částí ISO/IEC 10181 se detailně zabývá tím, jak je vytvářena konkrétní bezpečnostní služba (např. autentizace, důvěrnost atd.) a pokouší se klasifikovat hlavní typy mechanismů, které podporují tuto službu. Jelikož souběžně s vývojem tohoto dokumentu probíhal také vývoj kryptografie, korespondence jednotlivých služeb a odpovídajících relevantních mechanismů není vždy ideální.

Dokument ISO/IEC 10181 má sedm částí. Pět z těchto částí pokrývá pět soustav bezpečnostních služeb, které byly definovány už v dokumentu ISO 7498-2. Jedna část je obecným úvodem do problematiky a poslední část se zabývá bezpečnostním auditem, který v dokumentu ISO 7498-2 zmíněn nebyl. Názvy jednotlivých sedmi částí ISO/IEC 10181 jsou následující:

- ISO/IEC 10181-1: 1996: Úvod, Přehled soustav
- ISO/IEC 10181-2: 1996: Soustava autentizace
- ISO/IEC 10181-3: 1996: Soustava řízení přístupu
- ISO/IEC 10181-4: 1997: Soustava nepopiratelnosti
- ISO/IEC 10181-5: 1996: Důvěrnostní soustava
- ISO/IEC 10181-6: 1996: Integritní soustava
- ISO/IEC 10181-7: 1996: Soustava bezpečnostního auditu a poplachů.

Rolí (bezpečnostních) soustav je především zavést dohodnutý systém pojmů a terminologii. Soustavy nejsou určeny ani tak pro přímé použití implementátory, jsou určeny spíše pro tvůrce jiných norem a systémů IT. Soustavu správy klíčů vyvinul normalizační orgán JTC1/SC27[21] samostatně, tj. mimo normu ISO/IEC 10181, jako jednu část normy správy klíčů, ISO/IEC 11770. Norma ISO/IEC 10181-1 zavádí základní obecné pojmy z oblasti bezpečnostních služeb de facto stejným způsobem, jaký používáme v této příručce.

Bezpečnostní politika IT se chápe jako množina obecně platných pravidel pro uplatňování aktivit prvků, souvisejících s bezpečností, přičemž prvkem může být počítač, síťová komponenta (komunikační kanál …). Bezpečnostní politika IT se uplatňuje v rámci bezpečnostní domény, případně i mezi doménami.

Autorita (manažer, správce …) odpovědná za implementaci a uplatňování bezpečnostní politiky se nazývá *bezpečnostní autorita*.

Množina prvků řídících se nebo řízených danou bezpečnostní politikou a z hlediska aktivit souvisejících s bezpečností spravovaných jednou bezpečnostní autoritou se chápe jako *bezpečnostní doména*.

[21] strukturu normalizačních orgánů rozebírá následující kapitola

Informace požadované pro plnění bezpečnostních služeb, *bezpečnostní informace*, zavádí připravovaná norma ISO/IEC 15816 Security Information Objects. Mezi bezpečnostní informace podle ISO/IEC 15816 patří

- bezpečnostní, klasifikační návěští
  množina atributů prvku používaná pro podporu řízení přístupu, pro definici úrovně důvěryhodnosti a definici citlivosti dat
- kryptografické kontrolní hodnoty
  autentizační charakteristiky zpráv[22] a digitální podpisy použité pro podporu integritních služeb, služeb autentizace původu a služeb nepopiratelnosti
- bezpečnostní certifikáty
  bezpečnostní informace důvěryhodně potvrzující nějakou skutečnost související s více bezpečnostními službami; musí být integritně chráněné např. pomocí kryptografických kontrolních hodnot a jsou generované bezpečnostní autoritou nebo důvěryhodnou třetí stranou[23]
- bezpečnostní příznaky
  integritně chráněné bezpečnostní informace související s více bezpečnostními službami, na rozdíl od certifikátů typicky generované komunikující entitou.

4.3 Důvěryhodné třetí strany (TTP)

Důvěryhodná třetí strana (Trusted Third Party, TTP) je organizace, která poskytuje bezpečnostní služby a které ostatní účastnící (v rámci těchto služeb) důvěřují.

TTP může nabízet služby s přidanou hodnotou subjektům, které si přejí zvýšit míru důvěry a obchodní spolehlivosti službám, které nabízejí. TTP také podporují bezpečnou komunikaci mezi partnery. TTP musí nabízet bezpečné a trvale dostupné služby. Subjekty musí mít možnost vybírat si z více TTP a TTP by měly být schopny vybírat, které subjekty budou podporovat a které nebudou podporovat. Aby TTP mohla pracovat efektivně, musí:

- pracovat bezpečně
- pracovat v právním rámci společném nebo přijatelném pro všechny zúčastněné strany
- nabízet širší sortiment služeb s jejich definovanou minimální sadou služeb
- být v souladu s národními a mezinárodními standardy a normami
- dodržovat všeobecně akceptované odborné zvyklosti a postupy
- umožnit nezávislou arbitráž bez porušení bezpečnosti
- být monitorována dozorovým úřadem
- být nezávislou a nestrannou entitou a pracovat v rámci pravidel akreditace
- mít veřejnou politiku odmítnutí služby z hlediska bezpečnosti
- poskytovat záruky za dostupnost a kvalitu svých služeb[24].

Služby TTP lze využít, když je tento subjekt důvěryhodný. To znamená, že jí důvěřují všechny entity, které ji používají. Tato důvěra pramení z jistoty, že TTP provozuje svou činnost správně a v souladu s definovanou bezpečnostní politikou a dohodou o poskytování služeb.

---

22 MAC – Message Authentication Code
23 TTP – Trusted Third Party
24 QOS – Quality of Services

Tato jistota je zajištěna prokázáním toho, že:

- existuje a je dodržována odpovídající bezpečnostní politika
- jsou v provozu správně implementované bezpečnostní procedury a mechanismy, které čelí potenciálním bezpečnostním hrozbám
- bezpečnostní funkce TTP jsou prováděny správně a s přesně definovanými rolemi a odpovědnostmi
- rozhraní a procedury pro komunikaci s uživateli jsou vhodné pro poskytované funkce
- management i zaměstnanci TTP dodržují platné směrnice a nařízení
- proběhla akreditace kvality procesů a operací
- TTP dodržuje smluvní závazky ke svým uživatelům
- jsou jasně definovány záruky a zodpovědnosti TTP
- je zajištěno a auditováno dodržování zákonů a jiných nařízení
- jsou identifikovány potenciální hrozby a jsou implementována odpovídající bezpečnostní opatření
- předem byla provedena analýza rizik a její vyhodnocení a tato analýza je pravidelně revidována.

4.3.1 Typy důvěryhodných třetích stran

Z hlediska komunikace mezi jednotlivými entitami může být několik možných forem umístění TTP. Konkrétně jde o tyto varianty:

- *in-line TTP, mezilehlá důvěryhodná třetí strana*

  Mezilehlá důvěryhodná třetí strana leží přímo v komunikační cestě mezi dvěma komunikujícími entitami. Je zvláště důležitá tehdy, pokud komunikující entity jsou umístěny v rozdílných bezpečnostních doménách a používají rozdílné bezpečnostní mechanismy (a proto nejsou schopné spolu přímo bezpečně komunikovat). Jako příklady mezilehlých důvěryhodných třetích stran (in-line TTP) lze uvést:

  – in-line (mezilehlá) autentizace – TTP autentizuje žadatele o autentizaci a zaručí se za jeho identitu komunikující protistraně (která si autentizovala TTP)

  – in-line TTP může podporovat i jiné bezpečnostní služby, jako je nepopiratelnost, řízení přístupu, důvěrnost a integrita dat.

- *on-line TTP*

  On-line TTP se účastní bezpečné komunikace mezi dvěma entitami, ačkoli neleží na komunikační cestě mezi těmito entitami. Místo toho je TTP žádána jednou nebo oběma komunikujícími entitami o poskytnutí nebo zaregistrování informace, potřebné pro zabezpečení komunikace. Jako příklady on-line TTP lze uvést:

  – *on-line autentizace* – služba pro autentizaci entit může použít on-line TTP jako část mechanismu autentizace

  – *on-line řízení přístupu* – on-line TTP může na požádání poskytovat informace o přístupových právech entit

– *on-line správa (kryptografických) klíčů* – on-line TTP může pracovat jako distribuční centrum (kryptografických) klíčů, KDC[25], nebo přenosové centrum (kryptografických) klíčů, KTC[26], pro podporu správy klíčů kryptografických systémů používajících symetrickou kryptografii

  Distribuční centrum (kryptografických) klíčů je entita důvěryhodná z hlediska distribuce klíčů entitám sdílejícím s ní klíč. Proces ustanovení sdíleného tajného klíče zahrnuje jak techniky dohody na hodnotě klíče oběma zúčastněnými stranami, tak i techniky bezpečného předávání klíče jednou entitou entitě druhé. Přenosové centrum (kryptografických) klíčů je entita důvěryhodná z hlediska přenosu klíčů mezi entitami sdílejícími s ní klíč.

– *on-line nepopiratelnost* – on-line TTP může podporovat služby pro zajištění nepopiratelnosti, a to mnoha způsoby, včetně generování digitálních podpisů, generování časových značek a poskytování notářských služeb

– on-line TTP může poskytovat i další bezpečnostní služby, jakými je zajištění důvěrnosti a/nebo integrity dat.

- *off-line TTP*

  Off-line TTP také může podporovat mnohé bezpečnostní služby, avšak nemůže se účastnit žádných on-line transakcí. Off-line TTP místo toho poskytuje své služby někdy před činností vlastní bezpečnostní služby. Off-line TTP může komunikovat buďto přímo s komunikujícími stranami, nebo s jinou třetí stranou, která nutně nemusí být důvěryhodná a která má on-line přístup ke komunikujícím entitám. Jako příklady off-line TTP lze uvést:

– *off-line autentizace* – off-line TTP může dopředu generovat certifikáty veřejných klíčů, které mohou být použity jako součást mechanismů pro autentizaci entit. Tyto certifikáty mohou být uloženy přímo u autentizujících se entit nebo mohou být dostupné prostřednictvím on-line adresářových služeb

– *off-line nepopiratelnost* – off-line TTP může generovat certifikáty veřejných klíčů pro podporu služeb nepopiratelnosti.

4.3.2 Správa a provoz důvěryhodných třetích stran

Management (správa a řízení provozu) TTP se musí zabývat následujícími aktivitami:

- výběrem odpovídajících mechanismů s ohledem na druh poskytovaných služeb a na platnou bezpečnostní politiku
- správnou implementací těchto mechanismů zvláště s ohledem na fyzickou bezpečnost, kontinuitu činnosti atd.
- definicí odpovídajících procedur, například pro personální správu, klasifikaci informací, autorizaci, řešení incidentů atd.

TTP musí být proti vytypovaným hrozbám chráněna a musí poskytovat svoje služby trvale i při možnosti výskytu přírodních hrozeb apod.

Koncept převzetí záruky TTP za poskytované služby a právní rámec pro tuto činnost je v různých zemích značně rozdílný. Proto jakýkoli obecný návod musí být upraven podle aktuál-

[25] KDC – Key Distribution Centre
[26] KTC – Key Translation Centre

ního právního prostředí. Činnost TTP musí být v souladu se všemi národními a mezinárodními právními dokumenty, především v oblasti

- ochrany osobních dat
- zajištění důvěrnosti komunikace
- ochrany autorských práv
- použití kryptografických mechanismů
- zpřístupnění informací orgánům činným v trestním řízení.

TTP musí také definovat a dodržovat své zodpovědnosti a záruky a tam, kde je to nezbytné, krýt svá rizika pojištěním. Formální kontrakt mezi TTP a uživatelem TTP služeb musí jasně definovat míru zodpovědnosti TTP a kvalitu poskytovaných služeb (QOS). Kontrakt by mimo jiné měl obsahovat podmínky pro nezávislou arbitráž v případě sporu, měl by definovat hranice záruk, poskytovaných TTP a měl by obsahovat popis použití služeb TTP.

Poskytovatel služby TTP musí také specifikovat rozsah své zodpovědnosti za bezpečný provoz TTP a také rozsah záruk za škody, které vzniknou jako následek případného bezpečnostního incidentu. Například TTP, která provádí certifikaci kryptografických klíčů, musí být zodpovědná za:

- manipulaci s veřejným klíčem
- splnění slíbené úrovně služeb
- kontrolu identity uživatele před vygenerováním certifikátu.

TTP má také povinnost nabízet a provozovat bezpečnostní služby na bázi formálně dokumentované bezpečnostní politiky organizace TTP. Tato bezpečnostní politika se skládá ze dvou částí: z obecné bezpečnostní politiky a z technické bezpečnostní politiky.

- *Obecná bezpečnostní politika TTP*, která obsahuje netechnické aspekty bezpečnosti a důvěry ve služby, poskytované TTP, cílené na zaměstnance TTP a uživatele.
- *Technická bezpečnostní politika TTP*, která definuje všechny povinně dodržované technické aspekty, včetně praktik a procedur.

TTP se velmi často používají v síťových prostředích. V takovém prostředí každá TTP poskytuje služby podle své bezpečnostní politiky v rámci své domény. Jako typické relace interagujících stran v takové doméně lze uvést interakce typu TTP – uživatel, uživatel – uživatel, TTP – TTP, TTP – legislativní autorita a TTP – akreditační autorita.

4.3.3 Služby poskytované třetími důvěryhodnými stranami

4.3.3.1 Služby časových razítek

TTP může také poskytovat službu *časových razítek* (time-stamps). Tato služba přidá k elektronickému dokumentu časové razítko a dokument i s časovým razítkem podepíše digitálním podpisem. Tím je zajištěno, že bude v budoucnosti možno prokázat, že daný dokument v této podobě existoval v čase, který udává časové razítko. Vytvoření časového razítka se obvykle skládá z následujících kroků:

- entita, žádající o časové razítko, předloží dokument
- TTP vrátí digitálně podepsaný dokument, který obsahuje datum a čas podpisu, obsah předloženého dokumentu nebo jeho charakteristiku a volitelně i pořadové číslo.

4.3.3.2 Služby nepopiratelnosti

Služby zajišťující *nepopiratelnost* mohou být založeny na použití symetrické nebo asymetrické kryptografie. Převážně je používán mechanismus digitálního podpisu, založený na použití asymetrické kryptografie (kryptografie s veřejným klíčem), viz třetí kapitola.

4.3.3.3 Služby správy klíčů

Sestavy *služeb pro správu klíčů* typicky zahrnují:

- *služby pro generování klíčů*, tj. generování náhodných a nepředpověditelných čísel, která jsou použita jako klíče pro kryptografické algoritmy.
  Generování klíčů závisí na schopnosti vygenerovat tajná a nepředpověditelná čísla. "Náhodná" čísla mohou být generována buď kryptograficky bezpečnými generátory pseudonáhodných posloupností, nebo pomocí zdrojů čistě náhodného signálu. Pro symetrické kryptografické algoritmy by klíče měly být voleny rovnoměrně z celého prostoru hodnot klíčů, pro asymetrické kryptografické algoritmy by klíče měly být voleny téměř rovnoměrně z alespoň dostatečně velké podmnožiny prostoru klíčů. Problém generování klíčů je předmětem internetovského standardu RFC 1750.
- *služby pro registraci klíčů*, tj. registrace klíčů pro jednotlivé entity
- *služby pro certifikaci klíčů*, tj. poskytování certifikátů veřejných klíčů
  Certifikační služba časově razítkuje a podepisuje veřejný klíč nebo jiné atributy. Uživatelé certifikátu musí důvěřovat buď této certifikační autoritě, nebo nějaké vyšší obecné certifikační autoritě v hierarchii certifikačních autorit. Certifikované klíče lze generovat službou generování klíčů TTP, nebo jejich vlastníky. Tato služba podporuje rovněž zrušení platnosti certifikátu.
- *služby pro distribuci klíčů*, tj. distribuce klíčů pro jednotlivé entity
  Cílem služby distribuce klíčů (TTP v roli *distribučního centra kryptografických klíčů, KDC*) je generování a distribuce tajných klíčů mezi komunikující entity. Používají se mechanismy podporující jak dohodu dvou stran na hodnotě klíče, tak i jednostranné generování hodnoty klíče používané dvěma stranami i sdílení klíče, kdy se jedné straně poskytuje důkaz, že druhá entita vlastní daný sdílený klíč. Těmito problémy se zabývá norma ISO/IEC 11770.
- *služby pro přenos klíčů*, tj. přenos klíčů mezi jednotlivé entity
  Cílem služby přenosu klíčů (TTP v roli *přenosového centra kryptografických klíčů, KTC*) je přenos tajných klíčů mezi komunikující entity sdílejícími s KTC tajný klíč. Přenos klíče sestává z fáze, ve které KTC dešifruje získaný šifrovaný klíč a z fáze opětovného šifrování klíče v KTC a předání této šifry odpovídající druhé komunikační entitě. Touto službou se zabývá norma ISO/IEC 11770-1.
- *služby pro instalaci klíčů*, tj. způsob, jak klíč učinit dostupným konkrétním službám
- *služby pro uložení klíčů*, tj. bezpečné (krátkodobé nebo dlouhodobé) uložení klíčů
- *služby pro derivaci klíčů*, tj. odvození klíčů z jiných klíčů (z nadřízených klíčů v klíčové hierarchii)
- *služby pro archivaci klíčů*, tj. dlouhodobé uložení klíčů
- *služby pro odvolání klíčů*, tj. bezpečná deaktivace klíče v okamžiku, kdy je podezření na jeho prozrazení
- *služby pro likvidaci klíčů*, tj. bezpeční zničení klíče.

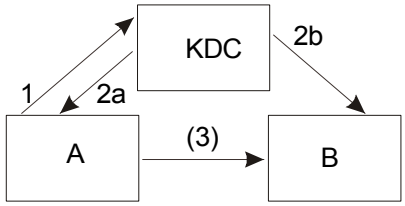
Schémat správy kryptografických klíčů je více. Entity požadující nějakou formu správy klíčů mohou např. spolu komunikovat přímo, mohou náležet do společné bezpečnostní domény nebo mohou náležet do různých bezpečnostních domén.

Pokud spolu komunikují přímo, ustanovují si společný kryptografický klíč bez zprostředkující důvěryhodné třetí strany (nepoužívají služeb ani žádné certifikační autority, ani žádného centra typu KDC nebo KTC). Klíč si distribuují nějakým existujícím bezpečným kanálem implementovaným např. již existujícím sdíleným kryptografickým tajným klíčem nebo vzájemně důvěryhodnými kopiemi veřejných klíčů zúčastněných stran.

Pokud zúčastněné strany náleží do jedné bezpečnostní domény, pro ustanovení klíče lze použít techniky založené jak na asymetrické, tak i na symetrické kryptografii.

V prvém případě se obvykle distribuují certifikáty, každá zúčastněná strana musí kontaktovat svoji autoritu, od které obdrží certifikát veřejného klíče partnera. Komunikující partneři si mohou certifikáty vyměnit i přímo.

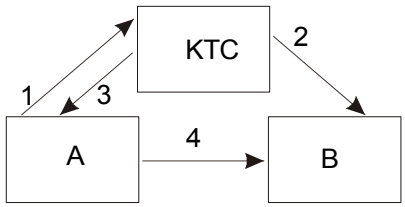
Ve druhém případě se používá služeb KDC nebo KTC. Jeden možný princip použití centra typu KDC v rámci jedné domény ilustruje obr. 4.1.



Obr. 4.1 Použití distribučního centra klíčů

Centrum typu KDC sdílí tajný klíč s každou entitou A a B samostatně. Entita A požádá KDC, aby vygenerovalo a distribuovalo klíč K_{AB} sdílený entitami A a B (1). Jakmile KDC takový požadavek přijme, vygeneruje klíč K_{AB} a jeho hodnotu šifrovanou tajným klíčem sdíleným s entitou A zašle entitě A (2a) a jeho hodnotu šifrovanou tajným klíčem sdíleným s entitou B zašle entitě B (2b). Centrum KDC ale nemusí s entitou B komunikovat přímo. Hodnotu vygenerovaného klíče K_{AB}, zašifrovanou klíčem, který sdílí s entitou B, může vrátit entitě A společně s hodnotou vygenerovaného klíče K_{AB} zašifrovanou klíčem sdíleným KDC s entitou A (2a) a ta tuto šifru předá entita A entitě B (3).

Možný princip použití centra KTC v rámci jedné domény ilustruje obr. 4.2. Centrum KTC opět sdílí tajný klíč s každou entitou A a B samostatně. Nyní klíč K_{AB} generuje entita A. Požádá centrum KTC, aby klíč K_{AB} distribuovalo entitě B. Entita A předává klíč K_{AB} centru KTC zašifrovaný klíčem, který s ním sdílí (1). Jakmile KTC takový požadavek přijme, dešifruje hodnotu klíče K_{AB} a znovu ji zašifruje pomocí tajného klíče, který sdílí s entitou B. Tuto zašifrovanou hodnotu přímo pošle entitě B (2) nebo ji vrátí entitě A, aby ji tato teprve předala entitě B (3, 4).

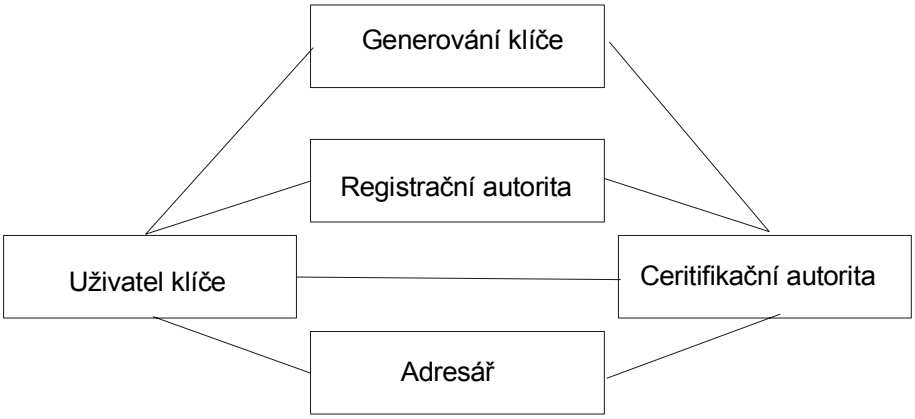


Obr. 4.2 Použití transformačního centra klíčů

Pokud žádají ustanovení klíče entity A a B náležející různým doménám, je potřeba si uvědomit, že každá z nich důvěřuje pouze autoritě, v jejíž doméně se nachází. Entita A si může přát získat certifikát veřejného klíče entity B nebo si entity A a B mohou přát sdílet tajný klíč. Službu ustanovení klíče v obou případech lze implementovat jak symetrickou, tak asymetrickou kryptografií. Možných scénářů řešení takových zadání je více.

Uvažme asymetrickou distribuci asymetrických klíčů. A i B v takovém případě požádají svoje autority o kopie certifikátů veřejných klíčů partnerů. Autority si případně tyto certifikáty vymění a předají je svým žadatelům. Entity A a B pak mohou bezpečně komunikovat přímo, dále již nezprostředkovaně.

Uvažme nyní symetrickou distribuci symetrických klíčů. Entity A a B v takovém případě požádají svoje autority o ustanovení klíče sdíleného entitami. Autority se na tajném klíči sdíleném entitami A a B dohodnou a jeho hodnotu šifrovanou klíčem, který sdílí s entitou ve své doméně, svým entitám distribuují. Entity A a B pak mohou bezpečně komunikovat přímo, dále již nezprostředkovaně.



Obr. 4.3 Entity podílející se na správě klíčů

Obecný model entit, které se podílejí na správě klíčů, ilustruje obr. 4.3. Je potřeba si uvědomit, že v každé implementaci certifikačního procesu se nemusí použít všechny uvedené entity, resp. nemusí být implementovány jako samostatně existující entity. Certifikační autorita je odpovědná za certifikaci informace o veřejném klíči entity, adresář odpovídá za uchovávání certifikátů dostupných on-line uživatelským entitám, generátor klíčů má na starosti generování dvojic klíčů (veřejný, soukromý), registrační autorita je odpovědná za poskytování důvěryhodných identifikačních informací certifikační autoritě. Generátor klíčů může být jak součástí uživatelské entity, tak i funkcí plněnou v certifikační autoritě.

4.3.3.4 Certifikační služby

Certifikační služby se poskytují v pěti různých formách:

- *služba certifikace veřejných klíčů* – generuje certifikáty veřejných klíčů
  Certifikační autorita (CA) je TTP, která může provádět širokou škálu funkcí souvisejících s digitálními podpisy. Její základní funkcí je autentizace vlastnictví a vlastností veřejného klíče. CA generuje certifikát veřejného klíče, jakmile CA ověří jeho správnost.
- *služba certifikace atributů* – generuje certifikáty dalších vlastností entit (přístupových práv apod.)

Generuje certifikáty vesměs vázané na certifikát veřejného klíče. Často se měnící atributy je vhodné autentizovat samostatnými certifikáty.

- *služba on-line autentizace* – činná jako autentizační server (např. v autentizačním protokolu „Kerberos“)
- *služba vzájemné certifikace* – generuje certifikáty veřejných klíčů pro veřejné klíče jiných certifikačních autorit
- *seznam zrušených certifikátů* – udržování podepsaného seznamu neplatných certifikátů. CA je odpovědná za správu doby platnosti certifikátů, do které patří i jejich obnova, aktualizace a rušení. Rušení certifikátu se provádí tehdy, pokud je třeba jej zneplatnit ještě v době jeho platnosti. K takové situaci dochází např. po změně jména, po kompromitaci veřejného klíče, po změně organizace apod. Rušení platnosti se provádí dvěmi způsoby:
  - vydává se *seznam neplatných certifikátů* podepsaný CA (Certification Revocation Lists, CRLs); CRL musí být korigovány periodicky, i když k žádným rušením certifikátů nedochází, aby si byli uživatelé CLR jisti, že používají poslední vydání CRL
  - použije se *likvidační certifikát*, podepsané vyhlášení, že daný certifikát je neplatný.

Obnovou certifikátu se rozumí generování nového certifikátu pro stejný veřejný klíč, jaký byl certifikován předchozím certifikátem, ale se kterým byly sdruženy jiné informace. Starý certifikát musí být zrušen, pokud nevypršela jeho platnost. Veřejný klíč entity přitom nemusel být kompromitován, entita např. změnila svoje jméno. Aktualizací certifikátu se rozumí vydání nového certifikátu entitě po vygenerování nové dvojice klíčů asymetrické kryptografie.

Všeobecný přehled aspektů správy CA uvádí materiál ISO TR 14516, ve svém dodatku C, včetně procedur registračního procesu a příkladu akreditačních podmínek CA.

4.3.3.5 Notářské služby

Veřejná notářská služba získá dokument od uživatele a potvrdí nebo certifikuje jeho existenci (např. svým podpisem). Služba může potvrzovat, že dokument v daném čase existoval, což může být použito jako důkazní materiál při soudním řízení. Služba může rovněž certifikované dokumenty dlouhodobě uchovávat nebo je uživateli služby vracet. *Služba digitálního archivu* poskytuje služby zaznamenávající dokumenty. Mezi takové služby patří:

- *archiv dokumentů* – TTP může potřebovat, aby se datovaná kopie dokumentu dlouhodobě uchovávala v bezpečné paměti
- *kopírování dokumentů* – TTP na požádání vydává podepsanou kopii dokumentu včetně iniciálního data žádosti o registraci službou.

Udržení integrity uložených dokumentů je vnitřním problémem TTP a pro zachování integrity se nutně nemusí používat kryptografické mechanismy.

Dlouhodobé uchovávání dokumentů (např. po dobu 30 nebo 50 a více let) vyvolává potřebu řešení celé řady specifických problémů:

- některá paměťová média (např. magnetická média) ztrácejí za takovou dobu své paměťové vlastnosti a jejich obsah je potřeba obnovovat, aby se předešlo jejich ztrátám
- mohou se měnit metody zpřístupňování archivovaných dat a uložená data se musí přenášet z jednoho média na jiné
- s dokumentem je potřebné uchovávat informaci o jeho formátu (ASCII, PostScript, HTML, RTF …) a je potřebné mít k dispozici software, který umí „staré“ formáty zpracovávat.

4.3.3.6 Další služby poskytované TTP

Adresářová služba poskytuje důvěryhodné informace o entitách. Na použití bezpečnostních informací, resp. informací relevantních bezpečnosti, poskytovaných nějakým katalogem, adresářem (např. on-line bází dat) je založen princip mnoha bezpečnostních služeb. Bezpečnostní informace musí být důvěryhodné. Jako příklady takových informací lze uvést certifikáty veřejných klíčů, seznamy neplatných certifikátů, certifikáty atributů apod. Správu adresářové služby má na starosti více rolí (entit). Bezpečnostní manažer je odpovědný za definici přístupových práv (veřejná přístupnost, omezení dostupnosti na uzavřenou skupinu uživatelů …). Auditor periodicky zkoumá auditní záznamy a zjišťuje, zda nedošlo k narušení bezpečnosti. Za udržování části adresáře související s bezpečností je odpovědný správce báze dat.

Identifikační a autentizační služby TTP mohou podporovat několik způsobů vzájemné autentizace zúčastněných stran. Jde především o *on-line autentizační službu*, kde TTP sdílí tajný klíč s každou z entit a slouží jako autentizační server, o *off-line autentizační službu*, kde TTP vytváří certifikáty veřejných klíčů pro podporu autentizace a o *in-line autentizační službu*, kde se TTP sama autentizuje oběma entitám a slouží jako důvěryhodný zprostředkovatel. Tyto tři přístupy jsou detailně rozebrány v dokumentu ISO/IEC 10181-2. Konkrétní příklady autentizačních mechanismů jsou v dokumentu ISO/IEC 9798.

4.3.4 Relevantní normalizační materiál

Činnost důvěryhodných třetích stran (TTP) je předmětem normalizačního materiálu ISO/IEC JTC1/SC27 N2138, PDTR 14516: Information technology – Security techniques – Guidelines on the use and management of Trusted Third Party Services z listopadu 1998. Jeho stávající verze se zabývá následujícími oblastmi: definice pojmů z oblasti používání TTP, obecné požadavky na TTP (potřebná důvěryhodnost, právní a smluvní vazby …), legislativní a provozní hlediska TTP, síťové propojení TTP, služba časového razítkování, služba nepopiratelnosti, služby správy klíčů, služby správy certifikátů, notářské služby, služby digitálních archivů, správa CA.

5. Normalizace bezpečnosti IT

O potřebě směrnic, resp. pravidel, a nezbytnosti jejich dodržování nejen v oblasti informačních technologií, ale rovněž v oblastech etiky, práva apod., nikdo nepochybuje. Proto se zaváděním takových směrnic zabývají samostatné instituce, které přirozeně mají i mezinárodní charakter. Dříve než budeme systematicky procházet světem těchto mezinárodních směrnic či předpisů souvisejících s bezpečností, je potřeba si úvodem říci několik slov k použité terminologii. V českém prostředí, které historicky dlouhodobě existuje spíše v německy než anglicky orientovaném prostoru, se pro takové směrnice zavedl pojem *norma*. Normalizací prakticky ve všech oborech lidské činnosti se v Česku zabývá *Český normalizační institut*.

Informační technologie mají bezesporu vývojové i produkční zázemí především v prostředí, které používá jako základní komunikační nástroj angličtinu. V českém prostředí se často používají produkty lokalizované do české varianty z anglické verze nebo se používají v původní anglicky orientované podobě. Německé či francouzské mutace se používají v zanedbatelném počtu. A tak je přirozené, že se pro označení uvedených směrnic vesměs používá pojem *standard*. Český normalizační institut tento trend pochopitelně neuznává a prosazuje používání termínů typu mezinárodní norma, evropská norma, normalizace, normalizační atd. Jeho snahou je ponechat termín standard spíše pro označení směrnic (předpisů) vydávaných jako tzv. „de facto" směrnice různými konsorcii uživatelů a výrobců IT (např. pro oblast Internetu).

5.1 Kdo je kdo ve světě norem (bezpečnosti IT)

5.1.1 Mezinárodní normalizační organizace

Cílem této kapitoly je získat přehlednou informaci o světě norem souvisejících s bezpečností informačních technologií. Mezi nejvýznamnější *mezinárodní normalizační organizace*, které se zabývají vedle ostatních normalizačních iniciativ i bezpečností informačních technologií, patří:

- *International Organization for Standardization* (ISO)
- *International Electrotechnical Commission* (IEC)
- *International Telecommunications Union* (ITU)
  ITU je následnický orgán výborů CCITT a CCIR.

Tyto organizace vydávají tzv. *základní normy*, které mají celosvětovou působnost. Uvedené organizace při vypracovávání norem úzce spolupracují, v oblasti informačních technologií např. ISO s IEC ustanovily Společný technický výbor číslo 1 (Joint Technical Committee), *JTC1*.

Na evropské úrovni působí tři následující normalizační organizace, které zhruba odpovídají organizacím ISO, IEC a ITU-T:

- *Comité Européen de Normalisation* (CEN) – odpovídá svojí působností ISO
- *Comité Européen de Normalisation Eléctrotechnique* (CENELEC) – odpovídá IEC
- *European Telecommunications Standards Institute* (ETSI) – odpovídá ITU.

5.1.2 Národní normalizační organizace

Normalizaci v oblasti informačních technologií v jednotlivých státech obvykle zajišťují *národní normalizační organizace*, které jsou vesměs členskými organizacemi ISO a IEC. Vydávají vlastní národní normy. Jako významné (uznávané i mezinárodně) národní normalizační organizace s působností v oblasti bezpečnosti IT lze uvést:

- ANSI (U.S.A.), American National Standards Institute
- BSI (U.K.), British Standard Institute
- DIN (Německo), Deutsches Institut für Normung
- SCC (Kanada), Standards Council of Canada
- AFNOR (Francie), Association Française de Normalisation.

Členem ISO je rovněž *Český normalizační institut* (ČSNI). V Evropě působí ještě nadnárodní normalizační asociace

- *European Computer Manufacturers Association* (ECMA).

ECMA vydala např. velmi propracovanou normu bezpečnosti distribuovaných systémů.

Významnou roli v oblasti normalizace (a to nejen v oblasti bezpečnosti IT) hrají severoamerické normalizační orgány. Normalizační orgány USA si během doby vzhledem k úrovni severoamerických technologií prosadily mezinárodní respektování a uznávání. Z hlediska bezpečnosti je potřeba si všímat normalizační činnosti vykonávané v USA následujícími organizacemi:

- *Institute of Electrical and Electronics Engineers* (IEEE)
  profesionální orgán inženýrů v oblasti elektroniky a elektrotechniky, který se mj. výrazně zaměřuje na i normy bezpečnosti, lokálních sítí (IEEE 802.x) a operačních systémů (POSIX); normy IEEE vesměs mají mezinárodní význam a dopad
- *National Institute for Standards and Technology* (NIST)
  vládní standardizační orgán, nástupce NBS (National Bureau of Standards), vydává standardy pro federální vládu USA
- *American National Standards Institute* (ANSI)
  vystupuje jako zástupce USA v organizaci ISO a výrazně se věnuje mj. i normalizační činnosti v oblasti bezpečnosti IT, zvláště pak normám bezpečnosti bank.

5.1.3 Ostatní standardizační organizace

Vedle oficiálních mezinárodních a národních normalizačních organizací, které vydávají normy mnohdy označované jako „de jure“ standardy, působí v oblasti bezpečnosti řada organizací, konsorcií a různých sdružení, které vydávají tzv. „de facto“ standardy. Jejich standardy se vesměs prosazují díky technologické propracovanosti a potřebami a tlakem z výrobních a uživatelských sfér. Mnohé „de jure“ standardy, normy, vznikají následným přijetím (po případném upravení a přepracování) „de facto“ standardů některou z normalizačních organizací.

Typickým příkladem „de facto“ standardů jsou standardy sítě Internet. Tyto standardy jsou známé pod označením *RFC* (Request for Comment). Síť Internet vznikla jako výsledek úzké spolupráce vlády, průmyslu a vysokých škol, propojuje jejich počítačové sítě a privátní počítačové sítě. Projekt Internet vznikal za podpory vlády USA a rozšířil se především díky iniciativám akademických a výzkumných institucí. V posledních letech síť Internet propojuje stále více i sítě mnohých privátních organizací, pro které jsou komunikační služby poskytované touto sítí zajímavé. Chod Internetu je řízen vesměs nepřímo, především prosazováním internetovských „de facto“ standardů.

Internet je manažersky spravován a provozován radou pro internetovské činnosti, *Internet Activities Board* (IAB), která deleguje hlavní odpovědnost za vývoj a posuzování svých standardů na komisi *Internet Engineering Task Force* (IETF). Konečné rozhodnutí o vydání internetovských standardů pochopitelně dělá IAB.

5.2 Proces normalizace v ISO

ISO byla založena v r. 1947. Je celosvětovou federací členských národních normalizačních organizací – ISO Member Bodies (AFNOR, ANSI, BSI, DIN, SCC …). Jako členské národní normalizační organizace jsou vybírány vždy nejreprezentativnější normalizační organizace v dané zemi.

ISO (a IEC) přiděluje odpovědnost za vývoj norem v konkrétních oblastech *technickým výborům*, *Technical Committees* (TC). Technický výbor si určuje svůj program v rámci vymezeném svojí rodičovskou organizací (ISO nebo IEC) sám, a to tak, aby zadaný úkol vyřešil. TC dělí svoji působnost na *podvýbory*, *SubCommittees* (SC). Podvýbory se dělí na *pracovní skupiny*, *Working Groups* (WG). V pracovních skupinách se skutečně pracuje, výše se jen schvaluje. Evoluce struktur TC/SC/WG je pomalá, tyto struktury pracují a existují obvykle několik let. Mezi technické výbory zabývající se normami bezpečnosti IT patří především:

- *ISO TC68* (bankovnictví)
- *ISO/IEC JTC1* (informační technologie).

Životní cyklus ISO normy lze popsat následujícími kroky:

- návrh nové pracovní položky, NWI (New Work Item) a hlasování v TC o ní
- jmenování odpovědného editora
- série návrhů normy na úrovni pracovní skupiny, WD (Working Drafts)
- návrh normy na úrovni podvýboru, CD (Committee Draft) a hlasování v SC (3 měsíce)
- návrh mezinárodní normy, DIS (Draft International Standard) a hlasování v TC (obvykle 4–6 měsíců)
- konečný návrh mezinárodní normy, FDIS (Final DIS) s dobou pro hlasování 2 měsíce a poté statut mezinárodní normy
- pětiletá perioda hodnocení mezinárodní normy.

V případě potřeby (odhalí-li se vada, byla podceněna rychlost rozvoje technologie apod.) jsou přijímána opatření, aby normy byly revidovány i dříve než v pětiletém hodnotícím cyklu. Za tímto účelem existuje *systém zpráv o vadách v normách* (Defect Report System).

Někdy TC vypracovávají technické zprávy, TR (Technical Reports). TR typu 1 se vydává tehdy, když se ve výboru nenalezla dostatečná podpora pro vytvoření normy. TR typu 2 se vydává v případě, kdy normalizovaný předmět se stále ještě z technického hlediska vyvíjí. TR typu 3 se vydávají o problémech, které běžně normalizaci nepodléhají.

5.3 ISO normy bezpečnosti IT

Jako nejvýznamnější ISO TC, které se věnují normám bezpečnosti IT, jsme uvedli ISO TC68 (bankovnictví) a ISO/IEC JTC1 (informační technologie).

ISO TC68 se sice zabývá hlavně bankovními normami, ale TC68 vydal také celou řadu obecných norem bezpečnosti – ISO 8730 a ISO 8731-1/2 definující integritní mechanismy,

ISO 8732 a ISO 11166-1/2 specifikující správu kryptografických klíčů. Činnost TC68 z hlediska bezpečnosti byla dělena mezi podvýbory a pracovní skupiny následovně:

- TC68/SC2: bezpečnost mezibankovních styků
- TC68/SC6/WG6: bezpečnost styku se zákazníky
- TC68/SC6/WG7: bezpečnostní architektura bankovních systémů na bázi čipových karet (činnost WG7 byla v současnosti pravděpodobně již ukončena).

Mezi nejvýznamnější podvýbory působící v rámci *ISO/IEC JTC1* relevantní k bezpečnosti IT patří:

- SC6: telekomunikace a výměna informací mezi systémy
  SC6 má odpovědnost za správu dolních úrovní (1-4) ISO RM OSI modelu, tj. za komunikační podsystémy sítí otevřených systémů. SC6 definoval normy ISO/IEC 11577 – Network Layer Security Protocol (NLSP) a ISO/IEC 10736 – Transport Layer Security Protocol (TLSP).
- SC17: normalizace čipových karet a s nimi souvisejících zařízení
  Z výsledků činnosti SC17 lze upozornit zejména na normu ISO/IEC 7816.
- SC27: techniky bezpečnosti IT
  SC27 je podvýbor odpovědný za normalizaci generických metod a technik bezpečnosti IT, za normy kryptografických technik a za mezinárodní normy pro hodnocení bezpečnosti. Zabývá se identifikací generických požadavků na bezpečnostní funkce, vývojem bezpečnostních technik a mechanismů, vývojem bezpečnostních návodů a vývojem dokumentace a norem pro podporu správy bezpečnosti IT. Svoji činnost dělí do tří pracovních skupin:
  - WG1: Požadavky na bezpečnost, bezpečnostní služby a návody – správa bezpečnosti a problémy kompatibility z hlediska bezpečnosti s ostatními normalizačními výbory.
  - WG2: Bezpečnostní techniky a mechanismy – kryptografické techniky, normy bezpečnostních mechanismů.
  - WG3: Kritéria hodnocení bezpečnosti – počítačová bezpečnost, kritéria hodnocení apod.

Následující podvýbory v současnosti již ukončily svoji činnost. V minulé dekádě ovšem patřily obory jejich působnosti mezi technologicky vysoce progresivní.

- SC18: zpracování dokumentů a s tím související komunikace
  SC18 se věnuje normám elektronické pošty (WG4) a architekturám otevřených (normalizovaných) dokumentů, *ODA* (Open Document Architecture).
- SC21: propojování otevřených systémů, správa dat, otevřené distribuované zpracování
  SC21 je podvýbor odpovědný za Referenční model OSI – model sítí (WG1), za adresářové služby a správu propojených otevřených systémů – Directory and OSI Management (WG4) a za protokoly horních (5–7) vrstev modelu OSI – správu procesů, prezentaci dat a aplikační služby (WG8). SC21 rovněž vypracoval v r. 1988 základní ISO normu bezpečnost sítí, OSI Security Architecture, ISO 7498-2, která je v současné době v SC21 doplňována o novou normu bezpečnostních funkcí otevřených systémů – jedná se o sedmidílný „Security Frameworks Standard“, ISO/IEC 10181, Bezpečnostní soustavy.

Některé normy těchto podvýborů přešly do správy podvýboru JTC1/SC6, kterému se tímto rozšířila oblast působnosti. Většinu norem z oblasti působnosti bývalých podvýborů SC18 a SC21, které se dále nevyvíjí, spravuje přímo sekretariát JTC1.

V oblasti působnosti *SC27/WG1* je především správa bezpečnosti. SC27/WG1 je odpovědná za udržování norem:

- ISO/IEC 9979 z r. 1999 – procedury pro registraci kryptografických algoritmů
- ISO/IEC 11770-1 – Správa klíčů, Část 1: Prostředí (připraveno k publikaci).

SC27/WG1 rovněž pracuje na:

- technické zprávě TR 13335, části 1-5, směrnice pro správu bezpečnosti IT, dosud jsou publikovány části 1–3
- technické zprávě TR 14516, směrnice pro použití a správu třetích důvěryhodných stran, TTP (Trusted Third Parties)
- normě ISO/IEC 15816, informace (objekty) požadované pro plnění bezpečnostních služeb (Security Information Objects), v současnosti ve stavu CD
- normě ISO/IEC 15945, specifikace služeb TTP (služeb třetích důvěryhodných stran) pro podporu používání digitálních podpisů, v současnosti na úrovni WD.

V oblasti působnosti *SC27/WG2* jsou normy kryptografických technik, tj. bezpečnostních mechanismů, SC27/WG2 je odpovědná za udržování norem:

- ISO/IEC 10116, režimy činnosti blokových šifrovačů
  jedná se o inovaci normy ISO 8372 z r. 1987 a normu ISO/IEC 10116 z r. 1997 (2. vydání).
- ISO/IEC 9797, integritní mechanismy
  jedná se o normu ISO/IEC 9797 z r. 1994 (2. vydání) v současné době přepracovávanou do normy ISO/IEC 9797-1, ke které se vyvíjí rovněž část 2.
- ISO/IEC 9798, autentizační mechanismy (protokoly)
  jedná se o normy ISO/IEC 9798-1 z r. 1997 (2. vydání), ISO/IEC 9798-2 z r. 1994, ISO/IEC 9798-3 z r. 1998 (2. vydání), ISO/IEC 9798-4 z r. 1995 a o normu ISO/IEC 9798-5 z r. 1999.
- ISO/IEC 11770, správa kryptografických klíčů
  jedná se o normy ISO/IEC 11770-2 z r. 1996 a ISO/IEC 11770-3 z r. 1998.
- ISO/IEC 9796, digitální podpisy s obnovou zprávy
  ISO/IEC 9796 z r. 1991, ISO/IEC 9796-2 z r. 1997 a CD 9796-4.
- DIS 14888, digitální podpisy v dodatku zprávy
  v současné době jsou vypracovány DIS 14888-1, DIS 14888-2 a DIS 14888-3.
- ISO/IEC 10118, hašovací funkce
  jedná se o normy ISO/IEC 10118-1 a -2 z r. 1994, ISO/IEC 10118-3 z r. 1998 a o DIS 10118-4.
- ISO/IEC 13888, mechanismy nepopiratelnosti
  jedná se o normy ISO/IEC 13888-1 z r. 1997, ISO/IEC 13888-2 z r. 1998 a o normu ISO/IEC 13888-3 z r. 1997.
- ISO/IEC 15946, kryptografie na bázi eliptických křivek
  norma připravovaná ve třech částech, v současnosti jsou všechny na úrovni WD.

V oblasti působnosti *SC27/WG3* jsou především kritéria hodnocení bezpečnosti IT. Výsledkem jeho činnosti je norma ISO/IEC 15408, Evaluation Criteria for IT Security, která byla vydána v červnu 1999. Jejími principy se obšírněji zabývá kapitola 6 této příručky. Vypracovávala se paralelně s projektem nazývaným „Common Criteria“ a jeho výsledky v podstatě převzala. Norma ISO/IEC 15408, Evaluation Criteria for IT Security, je vypracovaná třech částech:

- Část 1: Úvod a model
- Část 2: Funkcionalita systémů IT, produktů a komponent
- Část 3: Zaručitelnost bezpečnosti systémů IT, produktů a komponent.

Obsah všech tří částí je rozebírán v již zmíněné kapitole 6 této příručky.

5.4 Normy síťových bezpečnostních architektur (orientační přehled)

V této podkapitole se orientačně seznámíme se strukturou bezpečnostních norem síťových prostředí. Cílem není výklad bezpečnosti sítí, ale získání přehledu o tom, které problémové oblasti v oblasti propojování otevřených (normalizovaných) systémů jsou pokryty normami.

Základní bezpečnostní normou síťových prostředí je norma ISO 7498-2, OSI Security Architecture, z r. 1989. Jedná se o speciální dodatek normy ISO 7498, RM OSI, který se zabývá bezpečností IT. Tato norma je dále doplňována obecněji chápanou sedmidílnou normou ISO/IEC 10181, Security Frameworks Standard. Normalizací bezpečnosti lokálních a rozlehlých sítí se zabývá ANSI/IEEE norma 802.10 LAN/MAN Security.

Norma ISO 7498-2, OSI Security Architecture, z r. 1989 pokrývá pět základních oblastí. S jejich obsahem se v hrubých rysech seznámíme. Jejich výčet je následující:

- Úvod (Introduction)
- Bezpečnostní domény a politiky (Security domains and policies)
- Funkce prosazující bezpečnost (Security services)
- Bezpečnostní mechanismy (Security mechanisms)
- Správa bezpečnosti (Security management).

Norma ISO/IEC 10181, Security Frameworks Standard, specifikuje soustavy bezpečnostních funkcí nutných pro provoz propojených otevřených systémů.

Norma ISO 7498-2, OSI Security Architecture (OSI SA), v úvodu zavádí standardní definice termínů z oblasti bezpečnosti IT, standardní popisy funkcí prosazujících bezpečnost (FPB, bezpečnostních služeb) a bezpečnostních mechanismů. Dále definuje, kde (ve které vrstvě) v RM OSI lze bezpečnostní funkce poskytovat a zavádí pojetí správy bezpečnosti (jak pojmy chápat, co je potřeba za nimi vidět). Definuje se generický životní cyklus bezpečnosti – definice bezpečnostní politiky jako abstraktní formulace požadavků na bezpečnost, analýza hrozeb bezpečnosti (podle politiky) od hackerů, přes požáry až po legislativu a standardizaci, definice funkcí prosazujících bezpečnost (bezpečnostních služeb) pro eliminaci dopadu hrozeb a zvládnutí hrozeb, definice bezpečnostních mechanismů dostatečně silně implementující FPB a zajištění trvalé správy bezpečnosti. Podle ISO 7498-2 je třeba veškerá bezpečnostní opatření přijmout nejníže na úrovni transportu dat, nižší vrstvy, tj. směrování, datový spoj a přenos médiem, nemusí být důvěryhodné.

Jako hrozby OSI SA definuje „maškarádu“ (skrytí útočníka za cizí identitu), odmítnutí služby autorizovanému subjektu, zapuzení zprávy, popření zaslání a/nebo přijetí zprávy, únik informace, porušení důvěrnosti, neautorizované modifikace dat, porušení integrity, modifikace

toku zpráv, změny pořadí zpráv a odpovědí, změny softwaru, analýzy toku zpráv, dedukce informací z veřejných zpráv, neautorizovaný přístup a porušení autorizační politiky.

Bezpečnostní politika je představována pravidly řídícími chování tak, aby bylo bezpečné. Musí být vydána explicitně formou publikované bezpečnostní politiky. Jedná se o množinu kritérií pro uplatnění bezpečnostních služeb (FPB). Prostor platnosti bezpečnostní politiky je nazýván bezpečnostní doména. Připouští se možnost vnořování a překrývání domén, a tím pádem i vnořování a překrývání bezpečnostních politik. OSI SA zavádí např. generickou autorizační bezpečnostní politiku stylem „Kdo není přiměřeně autorizován, nemůže informaci obdržet, zpřístupnit si, nesmí mu být umožněno z informace odvozovat další informace“. Taková generická politika se zabývá pouze prevencí neautorizovaného přístupu, nezabývá se např. problémem zajištění dostupnosti (availability), nepokrývá eliminaci hrozby odmítnutí služby (denial of service). Generická politika je základ, který se předefinovává podle výsledků analýzy rizik do množiny konkrétních pravidel. OSI SA rozlišuje dva typy autorizačních bezpečnostních politik:

- autorizace řízená identitou, (identity-based)
  právo k zpřístupnění a použití zdroje je dáno identitou uživatele a zdroje
- autorizace řízená pravidly, (rule-based)
  právo ke zpřístupnění a použití zdroje je řízeno globálními pravidly aplikovanými na všechny uživatele např. pomocí porovnávání povolení vydávaných na základě klasifikace uživatelů do tříd s atributy zpřístupňovaných zdrojů.

5.4.1 Normy bezpečnostních funkcí

Funkce prosazující bezpečnost podle OSI SA spadají do pěti hlavních kategorií a ty jsme v podstatě poznali v kapitole této příručky věnované výkladu bezpečnostních funkcí. Jedná se o bezpečnostní službu autentizace, včetně autentizace entity a autentizace původu, řízení přístupu, zajištění důvěrnosti, zajištění integrity a zajištění nepopiratelnosti. Těchto pět tříd FPB je předmětem zájmu i normy ISO/IEC 10181, Security Framework Standards, částí 2 – 6, které obsahují mnohem detailnější rozbor obecných způsobů, jak poskytovat tyto služby. Norma ISO/IEC 10181 v části 7 se navíc věnuje službě bezpečnostního auditu, kterou OSI SA dostatečně nepokrývá. Normě ISO/IEC 10181 se budeme v dalším textu věnovat podrobněji.

5.4.2 Normy bezpečnostních mechanismů

Bezpečnostní mechanismy podle OSI SA implementují bezpečnostní služby (FPB). OSI SA zavádí dvě klasifikační třídy bezpečnostních mechanismů:

- specifické bezpečnostní mechanismy
  použitelné pouze pro konkrétní FPB; rozeznává se osm typů specifických bezpečnostních mechanismů: šifrování, digitální podpisy, mechanismy řízení přístupu, mechanismy pro zajištění integrity dat včetně kryptografických součtů, mechanismy výměny autentizačních dat, skrývání vlastností přenosu zpráv, řízení směrování a notarizace; definované bezpečnostní mechanismy jsou pokrývány normalizační péči ISO/IEC SC27
- univerzální bezpečnostní mechanismy
  implementují více FPB; rozeznává se pět typů univerzálních bezpečnostních mechanismů: implementace důvěryhodnosti bezpečnostních funkcí, bezpečnostní klasifikační návěští, detekování událostí, protokolování (accounting, resp. security audit trail) a bezpečná obnova.

Rozboru bezpečnostních mechanismů byla rovněž věnována samostatná kapitola této příručky, proto se omezíme jen na některá konkrétní konstatování charakterizující problematiku normalizace bezpečnostních mechanismů.

5.4.2.1 Normy kryptografických algoritmů

Šifrování vedle implementace důvěrnosti dat a důvěrnosti toku dat je bází i některých autentizačních mechanismů a mechanismů správy klíčů. Konkrétní algoritmy obecně normalizovány nejsou. Po špatné zkušenosti se normalizací algoritmů DES a RSA se kryptografické algoritmy pouze registrují. Podle normy ISO/IEC 9979: 1991 se normalizuje jméno algoritmu. Norma ISO/IEC 10116: 1997 (2. vydání) normalizuje režimy šifrování pro *n*-bitový blokový šifrovač, vzorem je norma NBS/ANSI, který specifikuje režimy blokového šifrovače DES.

5.4.2.2 Normy digitálních podpisů

Mechanismus digitálního podpisování sestává ze dvou komponent, z podepisovacího mechanismu (má soukromý, důvěrný charakter) a z ověřovacího mechanismu (má veřejný charakter). Digitální podpisy implementují bezpečnostní funkce nepopiratelnosti, autentizace původu, integrity dat a tvoří bázi některých autentizačních mechanismů a mechanismů správy klíčů. Rozeznávají se dva typy digitálního podepisování:

- digitální podpis s obnovou zprávy
- digitální podpis v dodatku zprávy.

Digitální podpis s obnovou zprávy zavádí norma ISO/IEC 9796: 1991. Je vhodný jen pro krátké zprávy. Norma ISO/IEC 9796-2: 1997 umožňuje podepisování bez omezení délky zprávy, pro velmi dlouhé zprávy však pouze s jejich částečnou obnovitelností. Další část této normy, ISO/IEC 9796-4 zabývající se mechanismy na bázi diskrétních logaritmů je stále ještě ve vývoji. Specifické mechanismy pro podpis libovolně dlouhých zpráv jsou předmětem vznikající normy ISO/IEC 14888.

Podstatnou částí výpočtu digitálních podpisů v dodatku zprávy jsou jednocestné hašovací funkce. Tyto funkce připravované normy digitálních podpisů nepokrývají, jsou předmětem samostatné normy ISO/IEC 10118. Norma ISO/IEC 10118-1:1994 zavádí základní pojmy, norma ISO/IEC 10118-2:1994 obsahuje definice dvou metod pro budování hašovací funkce na bázi blokového šifrovače, norma ISO/IEC 10118-3:1998 specifikuje tři dedikované hašovací funkce (funkci zavedenou NIST pod názvem SHS – Secure Hash Standard a dvě funkce evropského původu vzniklé v rámci iniciativy RIPE – Réseaux IP Européans, RIPEMD-160 a RIPEMD-128). Konečně norma ISO/IEC 10118-4:1998 specifikuje další dvě hašovací funkce pro digitální podepisování založené na aplikaci modulární aritmetiky.

5.4.2.3 Normy mechanismů řízení přístupu

Mechanismy řízení přístupu jako nástroje pro použití informací souvisejících s klientem a serverem k rozhodnutí, zda si klient smí zpřístupnit zdroje serveru apod., se používají pro implementaci služby řízení přístupu. Jejich normu obsahuje ISO/IEC 10181-3, Soustava řízení přístupu (Access Control Framework).

5.4.2.4 Normy integritních mechanismů

Integritní mechanismy jsou určeny pro implementaci ochrany proti neautorizované modifikaci dat, implementují integritní služby a služby autentizace původu a tvoří bázi některých autenti-

začních mechanismů a mechanismů správy klíčů. Jsou normalizovány ve dvou typech – zabezpečení integrity jednotky dat (MAC, kryptografický součet) a zabezpečení integrity plné posloupnosti dat (k mechanismům prvého typu přidávají pořadové číslování a časové razítkování). Normou integritního mechanismu je norma ISO/IEC 9797: 1994, která specifikuje použití blokového šifrovače v režimu CBC. Vychází z předchozí bankovní normy ISO 8731-1: 1987, dříve americké bankovní normy ANSI X9.9 a X.9.19.

5.4.2.5 Normy mechanismů výměny autentizačních dat

Mechanismy výměny autentizačních dat implementují služby autentizace entity a tvoří bázi některých autentizačních mechanismů a mechanismů správy klíčů. Jsou součástí mnohých autentizačních protokolů. Jedná se o specifikace posloupnosti výměn kryptograficky chráněných zpráv vyměňovaných mezi komunikujícími entitami a pravidla pro zpracování těchto zpráv. Norma ISO/IEC 9798 poskytuje ve svých pěti částech pestrý výběr takových mechanismů na bázi různých kryptografických technik:

- ISO/IEC 9798-1: 1997 (2. vydání)
  obsahuje obecný model autentizace entity
- ISO/IEC 9798-2: 1994
  obsahuje specifikaci mechanismů výměny autentizačních dat založené na bázi symetrické kryptografie
- ISO/IEC 9798-3: 1998 (2. vydání)
  specifikuje autentizační mechanismy založené na bázi digitálních podpisů
- ISO/IEC 9798-4: 1995
  specifikuje autentizační mechanismy založené na bázi kryptografických kontrolních součtů (integritní mechanismy)
- ISO/IEC 9798-5: 1999
  specifikuje autentizační mechanismy založené na technikách nulové počáteční znalosti (zero knowledge techniques).

5.4.2.6 Normy mechanismů notarizace

Mechanismy notarizace pomocí třetí důvěryhodné strany (notáře) dávají záruku za integritu, původ a cíl přenosu dat. Typicky se jedná o kryptografické transformace dat. Mechanismy notarizace pomocí třetí důvěryhodné strany mohou podporovat nepopiratelnost. Mezi normy mechanismů notarizace lze zařadit normy:

- ISO/IEC 13888
  specifikuje mechanismy pro podporu služeb nepopiratelnosti, z nichž některé zahrnují notarizační techniky
- ISO/IEC 13888-1: 1997
  specifikuje obecný model nepopiratelnosti
- ISO/IEC 13888-2: 1998
  specifikuje mechanismy nepopiratelnosti založené na kryptografických kontrolních součtech (MAC, Message Authentication Code) a použití notarizačních služeb
- ISO/IEC 13888-3: 1997
  specifikuje, jak lze mechanismus digitálního podpisu použít pro služby nepopiratelnosti.

5.5 Normy správy klíčů

Správa klíčů je základem kryptograficky orientovaných bezpečnostních mechanismů. Týká se:

- rozhodnutí, kdy je potřeba obnovit klíče
- generování klíčů
- bezpečné distribuce klíčů.

Existuje mnoho norem správy klíčů v bankovních sítích a vedle nich existuje starší norma ISO/IEC 11770. Její část ISO/IEC 11770-1: 1997 definuje systém správy klíčů, část ISO/IEC 11770-2: 1996 specifikuje techniky distribuce klíčů založené na bázi symetrické kryptografie a část ISO/IEC 11770-3 specifikuje techniky distribuce klíčů a techniky dohody na klíči založené na bázi asymetrické kryptografie.

5.6 Normy zaručitelnosti bezpečnosti

Při návrhu bezpečného systému je potřeba vyřešit dva základní problémy:

- bezpečnostní funkcionalitu systému – co a jak (kvalitně, dokonale, silně …) musí systém z hlediska zabezpečování umět
- získání záruky, přesněji jisté úrovně zaručitelnosti, že systém je implementován a provozuje se tak, jak byl specifikován.

Získání záruky se dosahuje vyhodnocováním vlastností podle stanovených hodnotících kritérií. Této problematice je věnována samostatná kapitola v závěru této příručky.

5.7 Norma bezpečnostních funkcí ISO/IEC 10181

Norma bezpečnostních funkcí ISO/IEC 10181, Security Frameworks for Open Systems, je vypracována jako následník normy ISO 7498-2. Práce na ní začaly v 1988. Normu řeší JTC1/SC21. Zde se vyvíjela i norma ISO 7498-2. Norma ISO/IEC 10181 pokrývá všechny otevřené systémy (např. i databáze), nejen OSI systémy, tj. nejen sítě.

Každá část normy ISO/IEC 10181 se zabývá jednou bezpečnostní funkcí (autentizace, důvěrnost...), popisuje, jak ji poskytovat a jak ji implementovat (mechanismy). Definice bezpečnostních mechanismů z hlediska okamžitých úrovní technologií není perfektní, mnohé systémy jednotlivých bezpečnostních funkcí se vyvíjí paralelně s vývojem kryptografických metod.

Norma ISO/IEC 10181 má 7 částí. Části 2–6 se zabývají pěti základními bezpečnostními službami (funkcemi pro prosazení bezpečnosti) definovanými v ISO 7498-2.

- Část 1: Přehled soustav bezpečnostních funkcí
- Část 2: Soustava autentizace
- Část 3: Soustava řízení přístupu
- Část 4: Soustava nepopiratelnosti
- Část 5: Důvěrnostní soustava
- Část 6: Integritní soustava
- Část 7: Soustava bezpečnostního auditu a poplachů
  Tohoto problému si norma ISO 7498-2 nevšímala.

Hlavní rolí soustav bezpečnostních funkcí je zavést dohodnutý systém pojmů a terminologii, které nejsou určeny pro přímé použití implementátory, ale jsou spíše určeny pro tvůrce jiných norem a systémů. Bezpečnostní soustavu správy klíčů vyvinul JTC1/SC27 samostatně, tj. mimo normu ISO/IEC 10181, jako část 1 normy správy klíčů, ISO/IEC 11770.

Norma ISO/IEC 10181-1 zavádí obecné pojmy z oblasti bezpečnostních služeb. Pojem *bezpečnostní politika IT* zavádí jako množinu obecně platných pravidel pro uplatňování aktivit elementů souvisejících s bezpečností (element – počítač, síťová komponenta – komunikační kanál …), která se uplatňuje v rámci bezpečnostní domény, případně i mezi doménami. *Bezpečnostní autorita* je autorita (manažer, správce …) odpovědná za implementaci a uplatňování bezpečnostní politiky. *Bezpečnostní doména* je množina elementů řídicích se nebo řízených danou bezpečnostní politikou a z hlediska aktivit souvisejících s bezpečností spravovaných jednou bezpečnostní autoritou. *Bezpečnostní informace* jsou informace požadované pro plnění bezpečnostních služeb. JTC1/SC27 vyvíjí normu ISO/IEC 15816, Security Information Objects, která je v současnosti na úrovni CD a která se bude touto problematikou zabývat systematicky. Mezi takové informace patří bezpečnostní, klasifikační návěští (množina atributů elementu, informace pro podporu řízení přístupu, definice úrovně důvěryhodnosti, definice citlivosti dat), kryptografické kontrolní hodnoty (MAC, digitální podpis, podpora integritních služeb, služeb autentizace původu a služby nepopiratelnosti), bezpečnostní certifikáty (bezpečnostní informace související s více bezpečnostními službami musí být integritně chráněné např. pomocí kryptografických kontrolních hodnot, jsou generované bezpečnostní autoritou nebo třetí důvěryhodnou stranou, TTP), bezpečnostní příznaky (bezpečnostní informace související s více bezpečnostními službami, které musí být integritně chráněné a které jsou typicky generované komunikující entitou, na rozdíl od certifikátů. Jednotlivé části normy ISO/IEC 10181 obsahují:

- ISO/IEC 10181-1, Část 1
  Uvádí přehled bezpečnostních soustav. Cílem je poskytnout obecný úvod. Zavádí pojmy z oblasti bezpečnosti a typy bezpečnostních informací.
- ISO/IEC 10181-2, Část 2: Autentizační soustava
  ISO/IEC 10181-2 byla první dokončenou částí normy ISO/IEC 10181. Zavádí terminologii pro popis způsobů poskytování autentizačních služeb a zavádí klasifikační schéma autentizačních mechanismů a modely autentizační konfigurace.
- ISO/IEC 10181-3, Část 3: Soustava řízení přístupu
  Norma ISO/IEC 10181-3 byla vyhotovena brzy po normě ISO/IEC 10181-2. Částem 2 (autentizace) a 3 (řízení přístupu) bylo od počátku věnováno velké úsilí. Normalizace soustavy řízení přístupu je velmi cenná, poněvadž řízení přístupu se nikde jinde skutečně neřeší. Většina principů je převzata z iniciativ ECMA. Mezi obvyklé metodiky politiky řízení přístupu se zahrnuje schéma řízení přístupu s bezpečnostními návěštími, které se obvykle používá pro podporu politiky řízené pravidly, schéma způsobilosti a schéma s přístupovými pravidly, které se obvykle používá pro podporu politiky řízené identitou. Politika řízená pravidly se obvykle používá jako administrativně vnucovaná politika, politika řízená identitou se obvykle používá jako uživatelem volená politika. Nemusí to být vždy absolutně pravda.
- ISO/IEC 10181-4 až 7, Části 4 až 7: Ostatní bezpečnostní soustavy
  Normou ISO/IEC 10181 jsou zaváděny čtyři další soustavy pokrývající nepopiratelnost, důvěrnost, integritu a bezpečnostní audit. Dosud není jasná jejich použitelnost a důležitost. Jejich použitelnost se charakterizuje v odborných kruzích jako poněkud diskutovatelná.

5.8 Vybrané ISO/IEC normy bezpečnostních mechanismů

Jen pro ilustraci trendů upozorníme na některé ISO/IEC normy bezpečnostních mechanismů jako doplněk popisu norem uvedených v souvislosti s výkladem OSI SA. Omezený prostor, který lze věnovat popisu normalizačního úsilí v oblasti bezpečnosti IT v této publikaci, nám více neumožňuje. Všechny zmíněné normy jsou produktem ISO/IEC JTC1/SC27, a to především WG2 z SC27.

- ISO/IEC 9979: Registr šifrovacích algoritmů
- ISO/IEC 10116: Režimy činnosti šifrovačů
- ISO/IEC 9797: Autentizační kódy zpráv (Message Authentication Codes - MACs)
- ISO/IEC 10118: Hašovací funkce
- ISO/IEC 9796: Digitální podpisy s obnovou zprávy
- ISO/IEC 14888: Digitální podpisy v dodatku zprávy
- ISO/IEC 13888: Mechanismy nepopiratelnosti
- ISO/IEC 15946: Kryptografie na bázi eliptických křivek
- ISO/IEC 9798: Norma autentizačního protokolu
- ISO/IEC 11770: Norma správy klíčů.

6. Hodnocení bezpečnosti

Cílem kapitoly je popsat filozofie, ze kterých vychází soudobé chápání bezpečnosti informačních technologií a jejího hodnocení mezinárodními normalizačními organizacemi, jmenovitě ISO/IEC. Porozumění těmto filozofiím umožní čtenáři porozumět jak normalizovaným principům hodnocení bezpečnosti produktů a systémů IT, které jsou určeny či zamýšleny k provozování ve třetím tisíciletí, tak i obecným principům jejich bezpečnosti.

6.1 Bezpečnost IT a kritéria bezpečnosti

Nacházíme se v éře, ve které ve stále větším počtu organizací lze považovat informace, uchovávané a zpracovávané informačními technologiemi, za zdroje kritické, tj. za zdroje, na kterých přímo závisí, zda daná organizace může plnit svoje poslání. Jednotlivci očekávají, že produkty nebo systémy IT zaručí adekvátní ochranu jejich soukromých (osobních) dat před neautorizovaným odhalením, neautorizovanou modifikací nebo před jejich ztrátou či dočasným znepřístupněním. Aby se tato ohrožení eliminovala, resp. aby se zajistilo zmírnění jejich vlivu, tj. aby se poskytla adekvátní ochrana, používá se soubor nástrojů (politiky, bezpečnostní funkce, bezpečnostní architektury) nazývaný bezpečnost IT.

Mají-li se používat IT bezpečně, je žádoucí mít k dispozici nějaký prostředek, který usnadní posouzení, zda daný produkt nebo systém IT je či není dostatečně bezpečný, resp. který usnadní vývoj produktů či systémů IT s bezpečností, která má předem zaručenou jistou *úroveň bezpečnosti*. V posledních dvou dekádách se postupně objevilo, používalo a používá několik takových nástrojů, vesměs nazývaných *kritéria bezpečnosti* (např. známá „oranžová kniha“ s kritérii amerického ministerstva obrany TCSEC nebo evropská „harmonizovaná“ kritéria ITSEC). V této kapitole se zabýváme hlavně výkladem kritérií bezpečnosti doporučovanými k používání jako základní metodický materiál pro hodnocení bezpečnostních vlastností produktů nebo systémů IT mezinárodní normou *ISO/IEC 15408*. Tato norma byla vydána teprve nedávno (v červnu r. 1999). Je výsledkem několikaleté mezinárodní iniciativy v rámci projektu pracovně nazývaném *Common Criteria for Information Technology Security Evaluation*. Z historických i pragmatických důvodů se proto v odborné veřejnosti i v uvedené normě pro tato kritéria i nadále používá označení *Common Criteria*, resp. zkratka *CC*.

6.2 Kritéria bezpečnosti ITSEC

Kritéria pro hodnocení bezpečnosti IT ITSEC (Information Technology Security Evaluation Criteria), ve slangu nazývaná "Superman Book", byla vytvořena v roce 1990. Byla vytvořena jako harmonizovaná verze národních kritérií přijatých ve Francii, Německu, Velké Británii a Nizozemí. Kritéria byla předložena v září 1990 v Bruselu k připomínkám a diskusi, které se zúčastnily i USA. Po úpravách byla vydána Úřadem pro oficiální publikace Evropského společenství v červnu 1991 jako prozatímní materiál k dvouletému ověření. Jako doporučení byla schválena v dubnu 1995.

V září 1993 byl Úřadem pro oficiální publikace Evropského společenství vydán prováděcí manuál ke kritériím ITSEC pod názvem Information Technology Security Evaluation Manual, zkráceně ITSEM. ITSEM je vypracován jako nadstavba nad kritérii ITSEC verze 1.2. Jeho účelem je popsat, jak má být hodnocen hodnocený předmět v souladu s požadavky kritérií ITSEC. ITSEM obsahuje harmonizovanou metodologii pro hodnocení bezpečnosti IS (zatímco ITSEC

obsahuje harmonizovaná kritéria pro hodnocení bezpečnosti IS) a tím vytváří komplementární dokument k dokumentu ITSEC.

6.2.1 Rozsah kritérií ITSEC

Kritéria ITSEC lze aplikovat jak na produkt IT, tak i na systém IT. Jako produkt IT se chápe kupovaný produkt, který je prodáván pultovým prodejem bez znalosti konkrétního provozního prostředí, o jehož provozním prostředí lze vyslovit pouze obecné předpoklady. Systém IT je zasazen do konkrétního reálného provozního prostředí.

Sponzor hodnocení, entita, která požadavek na hodnocení zadává, určuje požadavky na provoz a hrozby. Dílčí bezpečnostní cíle hodnoceného předmětu dále závisí i na legislativních a dalších omezujících podmínkách. Tím se stanovuje požadovaná bezpečnostní funkcionalita a třída míry zaručitelnosti bezpečnosti (jinými slovy – úroveň důvěryhodnosti záruky za bezpečnost). Všechny aspekty hodnoceného předmětu, které jsou relevantní pro hodnocení, specifikuje bezpečnostní cíl. Popisuje bezpečnostní funkcionalitu hodnoceného předmětu, možné předpokládané hrozby, dílčí bezpečnostní cíle a detailní informace o použitých bezpečnostních mechanismech. Bezpečnostní cíl může obsahovat:

- dílčí bezpečnostní cíle (uvedené v celkové nebo v systémové bezpečnostní politice)
- definici provozního prostředí
- bezpečnostní funkce
- zdůvodnění použití bezpečnostních funkcí
- požadované bezpečnostní mechanismy a stanovení jejich minimální síly
- požadovanou třídu míry zaručitelnosti bezpečnosti.

Pro každou požadovanou třídu míry zaručitelnosti bezpečnosti kritéria definují, které podklady musí sponzor hodnocení hodnotiteli dodat. Hodnotitel převážně pracuje s podklady dodanými sponzorem hodnocení. Předpokládá se, že sponzor hodnocení a hodnotitel úzce spolupracují. Výsledkem procesu hodnocení je výrok, zda hodnocený předmět svůj bezpečnostní cíl splňuje či nesplňuje.

V kritériích ITSEC jsou požadavky na míru zaručitelnosti bezpečnosti a na bezpečnostní funkčnost specifikovány odděleně. Oddělená existence těchto dvou skupin požadavků vlastně definuje charakter kritérií ITSEC – jde o kritéria, která jsou "dvojrozměrná", to znamená, že u každého produktu lze odděleně hodnotit funkčnost a míru zaručitelnosti bezpečnosti. Tento rys kritérií ITSEC je pravděpodobně nejvýznamnější výhodou těchto kritérií oproti kritériím "jednorozměrným", jako jsou například kritéria TCSEC. V kritériích TCSEC je definována pouze jedna lineární hierarchie tříd, která v sobě zahrnuje jak požadavky funkčnosti, tak i požadavky na míru zaručitelnosti bezpečnosti. Pokud si uživatel zvolí určitou třídu podle požadavků na funkčnost, musí se smířit i s požadavky na míru zaručitelnosti bezpečnosti, definovanými v této třídě, přestože tyto požadavky mohou být v některých případech neadekvátní požadavkům uživatele. Při použití kritérií ITSEC si může uživatel zvolit nezávisle téměř libovolnou kombinaci požadavků na funkčnost a míru zaručitelnosti bezpečnosti.

Stanovení konkrétní třídy míry zaručitelnosti za bezpečnost podle kritérií ITSEC ovlivňuje proces vývoje hodnoceného předmětu, prostředí, ve kterém byl vyvíjen, úroveň jeho dokumentace a prostředí jeho provozu, proces dodávky, údržby apod. Sedm možných tříd zaručitelnosti bezpečnosti hodnoceného předmětu podle kritérií ITSEC lze stručně charakterizovat takto:

- E0 – nedostatečná zaručitelnost bezpečnosti, hodnocení nelze provést
- E1 – musí být dodán bezpečnostní cíl a neformální popis hodnoceného předmětu a testování bezpečnostních funkcí musí indikovat, že hodnocený předmět splňuje bezpečnostní cíl
- E2 – navíc proti E1 se požaduje dostupnost neformálního popisu detailního návrhu hodnoceného předmětu a hodnotiteli se musí dodat důkazy testování; musí se provádět správa konfigurace a musí být zaveden proces dodávky hodnoceného předmětu
- E3 – navíc proti E2 se požaduje dostupnost detailního návrhu a zdrojové texty programů bezpečnostních funkcí
- E4 – bezpečnostní politika hodnoceného předmětu musí být vyjádřena formálním modelem, požaduje se semiformální popis architektury a detailního návrhu hodnoceného předmětu a provedení analýzy zranitelnosti na této úrovni
- E5 – musí se prokázat úzká souvislost mezi detailním návrhem a implementací na úrovni zdrojových textů programů a provedení analýzy zranitelnosti na této úrovni
- E6 – požaduje se formální popis bezpečnostní architektury hodnoceného předmětu konzistentní s formálním modelem bezpečnostní politiky; musí být jednoznačně prokazatelná souvislost výkonných (binárních) programů s jejich zdrojovými formami.

Pro komerční bezpečné produkty je typickou třídou zaručitelnosti bezpečnosti třída E3.

6.2.2 Proces hodnocení podle kritérií ITSEC

V následujících odstavcích stručně popíšeme proces hodnocení bezpečnosti systému nebo produktu IT podle metodiky kritérií ITSEC tak, jak je tento postup popsán v publikaci [ITSEM].

Procesu hodnocení se účastní čtyři subjekty: sponzor hodnocení, vývojář, hodnotící organizace a certifikační orgán.

Sponzor hodnocení je obvykle prodejce (v případě produktu) nebo uživatel či dodavatel (v případě systému), který si přeje demonstrovat, že hodnocený předmět splňuje specifikaci bezpečnosti. Sponzor iniciuje hodnocení produktu hodnotící organizací. Zajistí vypracování specifikace bezpečnosti a uzavírá kontrakt s hodnotící organizací. Pokud hodnocení dopadne úspěšně, sponzor obdrží od certifikačního orgánu certifikát bezpečnosti.

Názvem *vývojář* se obvykle označuje organizace, která vyrábí hodnocený předmět. Pokud vývojář není zároveň i sponzorem, musí spolupracovat se sponzorem hodnocení a musí spolupracovat i s hodnotící organizací.

Úkolem *hodnotící organizace* je provádět nezávislé hodnocení hodnoceného předmětu. Cílem je nalézt slabiny hodnoceného předmětu a určit, v jakém rozsahu jsou splněny požadavky, uvedené ve specifikaci bezpečnosti. Hodnocení musí být provedeno v souladu s dokumenty ITSEC a ITSEM a v souladu s národními normami země, kde se hodnocení provádí. Hodnotící organizace vypracovává zprávu o hodnocení, kterou předá certifikačnímu orgánu a sponzorovi.

Certifikační orgán je státní organizace, která jako jediná má oprávnění vydávat certifikát bezpečnosti informačního systému. Tento certifikát stvrzuje, že úroveň bezpečnosti hodnoceného předmětu odpovídá požadavkům, uvedeným ve specifikaci bezpečnosti a že hodnocený předmět dosáhl některé třídy míry zaručitelnosti bezpečnosti podle kritérií ITSEC. Certifikační orgán má dva úkoly:

- Vytváří hodnotící organizaci podmínky pro nestranné a objektivní hodnocení a kontroluje dodržení nestrannosti, objektivity a konzistence hodnocení.
- Vydává nestranné potvrzení (certifikát) bezpečnosti.

Hodnocení produktu (systému) se provádí ve třech fázích:

1. *Přípravná fáze*. V této fázi sponzor kontaktuje všechny účastníky hodnocení, uzavře s nimi kontrakty a zajistí vypracování specifikace bezpečnosti, kterou dá všem účastníkům. Hodnotící organizace provede odhad předpokládané úspěšnosti hodnocení a v kladném případě se ujme hodnocení.
2. *Vlastní hodnocení*. Během této fáze hodnotící organizace provádí vlastní hodnocení hodnoceného předmětu. Je vytvořen seznam slabých míst hodnoceného předmětu. Případné problémy jsou řešeny podle jejich charakteru buď v součinnosti s certifikačním orgánem, nebo v součinnosti se sponzorem hodnocení a s vývojářem. Během hodnocení je hodnotící organizací vypracována zpráva o hodnocení. Tato zpráva je pak předána sponzorovi hodnocení a certifikačnímu orgánu.
3. *Závěrečná fáze*. V této fázi certifikační orgán analyzuje výsledky hodnocení, uvedené ve zprávě o hodnocení a určí, zda byly splněny požadavky, uvedené ve specifikaci bezpečnosti. V kladném případě udělí hodnocenému předmětu certifikát a předá jej sponzorovi.

6.2.3 Kritické zhodnocení kritérií ITSEC

Je nutno konstatovat, že obsah dokumentu ITSEC neodpovídá zcela jeho názvu. Prvním důvodem je, že nejde zcela o "kritéria". O kritéria jde pouze v části, zabývající se mírou zaručitelnosti bezpečnosti, kde jsou definovány třídy míry zaručitelnosti E0 až E6. V části, zabývající se bezpečnostní funkčností, však jde spíše o návod, jak vypracovat kritéria, neboli jedná se spíše o "generická kritéria".

Dokument ITSEC nezahrnuje informační systémy s distribuovanou správou, to jest vzájemně propojené informační systémy s několika správci, jejichž zájmy mohou být rozdílné. Přestože jde o poměrně obtížnou a dosud nepříliš zpracovanou problematiku, bylo by vhodné, aby se jí dokument zabýval. Této problematiky se v dokumentu dotýká pouze odkaz na bezpečnostní mechanismy nepopiratelnosti, což však zdaleka nepostačuje. Na základě výše uvedených důvodů by tedy bylo vhodnější, kdyby se dokument ITSEC nazýval spíše "Generická kritéria pro hodnocení bezpečnosti hierarchicky spravovaných systémů IT".

6.2.3.1 Kritika definice integrity

Integrita je v materiálu ITSEC definována jako "prevence proti neautorizované modifikaci informace". Tato klasická definice je sice uváděna i v jiných materiálech, ale není právě šťastná. Její nevhodnost se ukazuje např. v prostředí distribuovaných informačních systémů. V těchto systémech při přenosu dat veřejnou datovou sítí zpravidla nelze zabránit neautorizované modifikaci informace bez použití velmi nákladných (a zpravidla prakticky nerealizovatelných) fyzických bezpečnostních opatření. Neautorizovanou modifikaci dat lze však detekovat (např. kryptografickými prostředky) a na základě této detekce lze přenos dat opakovat. Pokud při každém pokusu o přenos dat dojde k neautorizované modifikaci informace, je narušena dostupnost, nikoli integrita. Z tohoto důvodu by bylo lépe definovat, že integrita je "prevence proti neodhalené neautorizované modifikaci informace". Změnou definice integrity by se dosáhlo jednoznačnějšího rozhraní mezi integritou a dostupností.

Při zavedení výše uvedené změny v definici integrity je možno navíc dosáhnout korespondence pojmů integrita a dostupnost s dobře definovanými pojmy z oblasti dokazování programů. Pojem integrita bude pak odpovídat pojmu částečná správnost (partial correctness) a pojmy integrita a dostupnost společně budou odpovídat pojmu úplná správnost (total correctness).

6.2.3.2 Kritika generických záhlaví definujících bezpečnostní funkcionalitu

Generická záhlaví pro funkce prosazující bezpečnost nejsou vytvořena systematicky a jejich výčet není úplný. Zvláště schází duální funkce k některým funkcím, prosazujícím bezpečnost. K identifikaci a autentizaci schází duální funkce *anonymita* a *pseudonymita*. Totéž platí o auditu a jeho duální funkci *nemožnost sledování* (Freeness from observability).

Zařazení funkce *výměna dat* mezi ostatní funkce prosazující bezpečnost je opět nesystematické, neboť tato funkce je na zcela jiné úrovni než funkce ostatní. Navíc chybí k ní odpovídající funkce *ukládání dat*. Klasifikace bezpečnostních funkcí by měla být doplněna tak, aby bylo umožněno hodnocení informačních systémů, které požadují nebo zajišťují *anonymitu*, *pseudonymitu* a *nemožnost sledování.*

6.2.3.3 Kritika příkladů tříd funkčnosti

Deset příkladů tříd funkčnosti, uvedených jako příloha dokumentu ITSEC, je pro uživatele dokumentu velmi nedostatečným materiálem. Uživatel má sice možnost definovat si své vlastní třídy funkčnosti, avšak pouze málo uživatelů je schopno tuto činnost provádět. Navíc uvedených deset příkladů tříd funkčnosti budí ve čtenáři mylný dojem, že tyto příklady tvoří kompletní a konzistentní sadu, pokrývající všechny problémy bezpečnosti.

6.3 Kritéria bezpečnosti CC

Zavedení obecné kriteriální základny pro hodnocení bezpečnosti IT umožňuje, aby výsledky hodnocení měly význam pro širší auditorium.

6.3.1 Čeho se CC týkají a čeho se netýkají

CC umožňují porovnávat výsledky nezávisle prováděných hodnocení bezpečnosti. Tohoto cíle dosahují tím, že stanovují obecně platné sestavy požadavků na:

- *bezpečnostní funkce* produktů a systémů IT
- *míry zaručitelnosti bezpečnosti* udělované (připisované) při hodnocení těmto bezpečnostním funkcím.

Proces hodnocení bezpečnosti IT prokazuje úroveň důvěryhodnosti, s jakou bezpečnostní funkce produktu nebo systému IT splňují stanovené požadavky. Stanovuje míru zaručitelnosti bezpečnosti udělované těmto bezpečnostním funkcím.

Kritéria CC definují hierarchicky uspořádané *úrovně zaručitelnosti bezpečnosti*. Množiny požadavků na splnění jednotlivých mír zaručitelnosti bezpečnosti, a tím pádem i míry zaručitelnosti bezpečnosti, jsou uspořádané do hierarchické soustavy podle těchto úrovní.

Výsledkem hodnocení je výrok o prokázání úrovně důvěryhodnosti, s jakou bezpečnostní funkce produktu nebo systému IT a míry zaručitelnosti bezpečnosti udělené těmto bezpečnostním funkcím splňují zavedené požadavky. Výrok sděluje, kterou úroveň zaručitelnosti bezpečnost produkt nebo systém IT splňuje.

Zákazník si může z výsledků hodnocení vybíraného nebo i již pořízeného produktu nebo systému IT odvodit, zda daný produkt nebo systém IT je pro zamýšlenou aplikaci dostatečně bezpečný, zda jsou rizika plynoucí z jeho provozování v konkrétních podmínkách tolerovatelná.

CC jsou užitečnou příručkou také pro vývojáře produktů nebo systémů IT, které mají být vybaveny bezpečnostní funkcionalitou, a také pro dodavatele takto funkčně vybavených komerčních produktů a systémů IT.

Produktem nebo systémem IT se rozumí např. operační systém, počítačová síť, databázový (distribuovaný) systém nebo nějaký jiný aplikační systém. Produkt nebo systém IT může obsahovat jak softwarové, tak i firmwarové nebo i hardwarové komponenty. CC označují hodnocený produkt nebo systém IT jako *hodnocený předmět*[27].

CC jsou cíleně orientována především na ochranu informací před neautorizovaným odhalením, neautorizovanou modifikací a před ztrátou možnosti s nimi pracovat. Obecně se tato hlediska označují jako ochrana důvěrnosti, ochrana integrity a ochrana dostupnosti informací. CC jsou primárně orientována na hrozby, jejichž zdrojem jsou především aktivity lidí (úmyslné nebo neúmyslné).

CC lze aplikovat i na další hlediska bezpečnosti a do dalších oblastí IT, autoři CC však nevyslovují žádné prohlášení o kompetentnosti CC mimo výše zmíněné domény použitelnosti.

CC se např. nezabývají hodnocením administrativních bezpečnostních opatření (organizační řády, personální politika, nástroje fyzické a procedurální ochrany apod.), pokud se tato opatření bezprostředně netýkají bezpečnostních opatření IT. Pokud tato opatření mají vliv na schopnost čelit identifikovaným hrozbám, považují se za bezpečná. Problému elektromagnetického vyzařování se CC věnují spíše okrajově. CC dále nedefinují žádné legislativní a organizační rámce pro své uplatňování. Předpokládá se, že komunita, která se jimi bude chtít řídit, si taková prostředí, tzv. s*chémata hodnocení bezpečnosti IT*, ustanoví. Prostředí pro uplatnění CC stanovuje odpovědné autority, jurisdikci, požadavky na vlastnosti akreditačních autorit, požadavky na vlastnosti hodnotitele apod.

Konečně je třeba upozornit i na skutečnost, že CC se záměrně nezabývají oceňováním kryptografických algoritmů. Předpokládá se, že pokud bude tato oceňování nějaká komunita požadovat, potřebná a vhodná legislativní opatření si zavede.

6.3.2 Pro koho jsou CC určena

Na hodnocení bezpečnostních vlastností produktů nebo systémů IT podle CC mají zájem tři skupiny – zákazníci, vývojáři a hodnotitelé produktů a systémů IT. CC jsou strukturována tak, aby uspokojila potřeby všech tří skupin. Všechny tři skupiny jsou chápány jako jejich primární uživatelé.

- *Zákazníci*

  Mohou použít CC při výběru požadavků na bezpečnost IT, kterými vyjadřují potřeby své organizace. CC jsou psána tak, aby zajistila, že hodnocení splní potřeby zákazníků (to je prvotním záměrem procesu hodnocení a ospravedlněním jeho provádění). Výsledek hodnocení mohou zákazníci použít při rozhodování, zda hodnocený produkt nebo systém IT splňuje jejich bezpečnostní potřeby.

  Bezpečnostní potřeby vesměs vyplynou z provedení analýzy rizik a z politických rozhodnutí. Zákazníci mohou výsledky hodnocení použít také pro porovnání různých produktů nebo systémů. Tuto potřebu podporuje hierarchie požadavků zaručitelnosti bezpečnosti.

  CC nabízejí zákazníkům, zvláště pak skupinám zákazníků a komunitám se shodnými zájmy, implementačně nezávislé struktury, nazývané *profily ochran*, ve kterých mohou vyslovovat své speciální požadavky na bezpečnostní opatření produktu nebo sytému IT.

[27] *TOE*, Target of Evaluation. Pro lepší čtivost textu budeme používat opis „produkt nebo systém IT“ nebo zkratku HP (hodnocený předmět).

- *Vývojáři*

  Použijí CC jednak pro přípravu hodnocení a jednak jako pomocný nástroj při hodnocení vyvíjeného produktu nebo systému IT a také jako návod pro identifikaci požadavků na bezpečnost, kterým musí vyvíjený produkt nebo systém IT vyhovět. Metodologie hodnocení, případně doplněná smlouvou o vzájemném uznávání výsledků hodnocení, umožňuje použít CC někým jiným než vývojářem pro hodnocení produktů nebo systémů IT používaných vývojářem.

  Vývojář může pomocí nástrojů zavedených v CC připravit důkazový (dokladový) materiál pro vyslovení tvrzení, že vyvinutý produkt nebo systém IT hodnocenými přesně stanovenými bezpečnostními funkcemi a zárukami bezpečnosti vyhovuje svým identifikovaným požadavkům. CC nabízejí pro vyjádření těchto požadavků na konkrétní vývojový případ implementačně nezávislou strukturu nazývanou *bezpečnostní cíl*. Požadavky široké zákaznické základny může podporovat jeden nebo několik profilů ochran.

  CC popisují bezpečnostní funkce, které vývojář může zahrnout do produktu nebo systému IT. CC lze použít pro určení odpovědností a činností při přípravě důkazových materiálů, které jsou požadovány pro hodnocení produktu nebo systému IT. CC rovněž definují obsah a formu prezentace důkazů.

- *Hodnotitelé*

  Mohou CC použít pro formulování posouzení, jak produkty nebo systémy IT vyhovují svým bezpečnostním požadavkům. CC popisují množinu činností, které hodnotitel musí provést a bezpečnostní funkce, kterých se tyto činnosti týkají. CC ale nespecifikují postupy při takovém hodnocení, tj. nedefinují v jakém pořadí a s jak formátovanými výstupy se činnosti hodnotitele provádí[28].

Mimo výše uvedené tři hlavní zájmové skupiny, jsou CC užitečná i pro manažery systémů IT a pracovníky oddělení bezpečnosti při vypracovávání bezpečnostních politik, pro auditory bezpečnosti IT a pro akreditační úředníky.

6.3.3 Jak lze hodnocení podle CC uplatnit

Aby byly výsledky hodnocení vzájemně porovnatelné, musí se provádět v rámci nějakého autoritativního prostředí – *schématu hodnocení bezpečnosti IT*, které stanoví normy (standardy), monitoruje kvalitu hodnocení a vydává předpisy, kterým musí hodnotící zařízení a hodnotitelé vyhovovat.

CC žádné takové předpisové prostředí nestanovuje. Nicméně, aby se dosáhlo kýženého cíle, tj. vzájemného uznávání výsledků hodnocení, musí být předpisová prostředí různých hodnotících autorit konzistentní. Kontext hodnocení produktů a systémů IT je tedy dán jednak kritérii CC a jednak následujícími prvky (viz obr. 6.1).

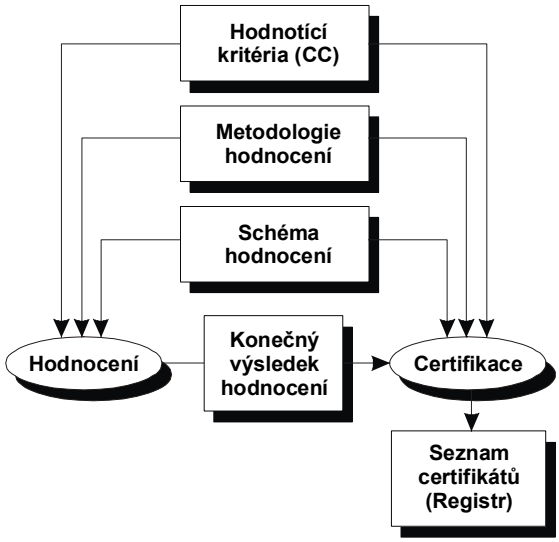
Jednotná obecná *metodologie hodnocení, která* sice přispívá k opakovatelnosti hodnocení a k objektivitě výsledků, ale sama o sobě není dostačující.

Mnohá hodnotící kritéria požadují použití expertních posudků, pro které je velmi obtížné dosáhnout konzistence. Aby se konzistentnost výsledků hodnocení zvýšila, měly by se konečné výsledky hodnocení podrobit *certifikačnímu procesu*. Certifikačním procesem se rozumí přezkoumávání výsledků hodnocení. Jedná se o prostředek pro zvýšení konzistence používání CC.

Certifikační proces končí vydáním konečného *certifikátu*, resp. schválení. Certifikát je normálně veřejně dostupný.

[28] Pro tento účel se připravuje norma, jejíž pracovní verze je známá pod *názvem Common Methodology for IT Security Evaluation, CME*.

Za schéma hodnocení bezpečnosti IT, metodologii hodnocení a certifikační proces včetně certifikátu jsou odpovědné autority hodnocení pověřené provozováním schémat a CC se jimi nezabývají.



Obr.6.1 Kontext hodnocení

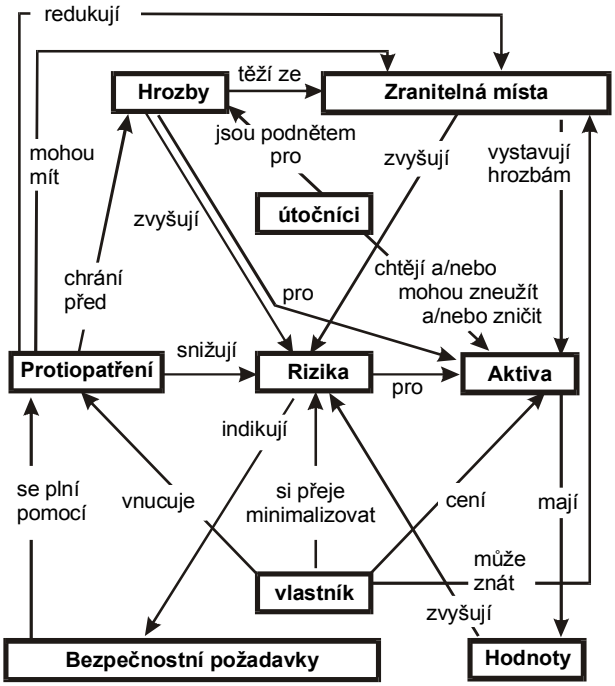
6.4 Model bezpečnosti CC

Základní pojmy z oblasti bezpečnosti a vztahy mezi nimi uvádí obr. 6.2. *Bezpečnost* se zabývá ochranou *aktiv* před *hrozbami*. Hrozby představují možnost neoprávněného využitkování aktiv. CC se zaměřují především na hrozby plynoucí z lidských zlomyslných nebo neúmyslných aktivit. Za chránění aktiva je odpovědný jeho vlastník, který aktivu přisuzuje hodnotu. Aktiva mohou mít hodnotu i pro skutečného nebo domnělého útočníka, který se proto snaží aktiva využitkovat způsobem, který odporuje zájmům vlastníka aktiva. Vlastník vnímá takové hrozby jako potenciální škodu, která snižuje hodnotu jeho aktiv.

Mezi základní typy hrozeb CC řadí ztrátu *důvěrnosti* (důvěrné aktivum se odhalí neoprávněnému příjemci), ztrátu *integrity* (aktivum je neoprávněně modifikováno) a ztrátu *dostupnosti* (způsobenou neoprávněným omezením přístupu k aktivu).

Vlastník aktiv analyzuje hrozby, kterým jsou jeho aktiva vystavena, vyhodnocuje, s jakými pravděpodobnostmi a s jakými typy útoků musí počítat, určuje *rizika*. Zná-li vlastník aktiva potenciální škodu a rizika, volí *bezpečnostní opatření*, kterými bude rizikům čelit a snižovat je na přijatelnou mez. Opatření se zavádějí tak, aby redukovala zranitelnost příslušného produktu nebo systému IT a aby se plnila bezpečnostní politika vlastníka aktiv. Zbytková rizika se vlastníci aktiv snaží minimalizovat dalšími omezeními, která nemusí být nutně z oblasti IT.

Vlastníci aktiv potřebují důvěřovat, že uplatněná bezpečnostní opatření adekvátně čelí hrozbám jejich aktiv, a to ještě dříve, než tato aktiva konkrétním hrozbám vystaví. Vlastníci aktiv nemusí být schopni sami posoudit všechna hlediska důvěryhodnosti přijatých bezpečnostních opatření a mohou si přijetí opatření nechat zhodnotit. Výstupem takového hodnocení je výrok, který charakterizuje, do jaké míry lze dát záruku za to, že přijatým bezpečnostním opatřením lze důvěřovat z hlediska kýžené minimalizace rizik. Hodnocení musí být objektivní a musí poskytovat opakovatelné výsledky, které lze v dalších hodnoceních citovat jako důkazový materiál.



Obr. 6.2 Základní bezpečnostní pojmy a vztahy mezi nimi

6.5 Pojetí bezpečnosti podle CC

Proces stanovení požadavků na bezpečnost produktu nebo systému IT musí bezpodmínečně vycházet z kontextu jeho použití a jeho obsahu. Bezpečný produkt nebo systém IT bývá provozován v nějakém prostředí, měl by vyhovovat nějakému profilu ochrany nebo bezpečnostnímu cíli.

6.5.1 Prostředí produktu nebo systému IT

Všechny relevantní zákonné a právní normy, bezpečnostní politiky organizace, zákazníci, odbornost a znalosti související se zabezpečovaným produktem nebo systémem IT vytvářejí *prostředí zabezpečovaného produktu nebo systému IT*. Toto prostředí definuje kontext, ve kterém se má produkt nebo systém IT používat. Do zabezpečovaného prostředí patří také hrozby pro bezpečnost IT, které v něm existují nebo by v něm mohly existovat.

Ten, kdo připravuje profil ochrany nebo bezpečnostní cíl související s jistým typem prostředí, musí brát do úvahy konkrétní typ fyzického prostředí, ve kterém se budou odpovídající produkty nebo systémy IT provozovat, známé principy fyzické a personální bezpečnosti, typy aktiv, která se mají chránit, a to jak přímých aktiv (soubory, databáze), tak i nepřímých, odvozených aktiv (certifikáty, autorizační pověření, vlastní implementaci IT) a účel, proč se mají produkty nebo systémy IT používat. Z hlediska potřeb pro definici profilů ochran a bezpečnostních cílů je nutné vypracovat:

- výčet předpokladů, které musí prostředí produktu nebo systému IT splnit, aby ho bylo možné považovat za bezpečné
- výčet hrozeb, které se považují v daném prostředí za relevantní (předpokládané metody útoku, zranitelná místa využitelná k útoku, ohrožená aktiva); ocenění bezpečnostních rizik by mělo vymezit pro každou hrozbu pravděpodobnost, se kterou se hrozba uplatní, pravděpodobnost úspěchu takového útoku a důsledky případných škod
- vyjádření bezpečnostních politik organizace, které bude možno v produktu nebo systému IT citovat a považovat je platné.

6.5.2 Bezpečnostní plán

Výsledek analýzy prostředí zabezpečovaného produktu nebo systému IT lze posléze použit pro definici *bezpečnostních plánů*, kterými se čelí identifikovaným hrozbám, které oslovují identifikované bezpečnostní politiky organizace a předpoklady. Bezpečnostní plány mají být konzistentní s definovanými provozními úmysly, se zamýšlenými účely produktu a se všemi znalostmi o fyzickém prostředí. Účelem vypracování bezpečnostního plánu je určit všechny bezpečnostní problémy a deklarovat, která bezpečnostní hlediska jsou dána přímo produktem nebo systémem IT a která jeho prostředím. Tato kategorizace je založena na procesu zahrnování konstrukčních úvah, bezpečnostních politik, ekonomických hledisek a rozhodnutí o přijatelnosti zbytkových rizik. Bezpečnostní plány pro dané prostředí by měly být implementovatelné pomocí IT, ale mohou se implementovat i netechnickými nebo i procedurálními (organizačními) prostředky. Na bezpečnostní plány se odkazuje při stanovování požadavků na bezpečnost IT.

6.5.3 Požadavky na bezpečnost IT

Požadavky na bezpečnost IT jsou konkretizací bezpečnostních plánů do množiny bezpečnostních požadavků na produkt nebo systém IT a na jeho prostředí. Produkt nebo systém IT může vyhovět svému bezpečnostnímu plánu, když jsou splněny požadavky na bezpečnost jeho prostředí. CC prezentují požadavky na bezpečnost IT ve dvou kategoriích. Stanovují se:

- *funkční požadavky*
  požadavky na bezpečnostní funkcionalitu
- *požadavky zaručitelnosti bezpečnosti*
  požadavky dané cílově požadovanou mírou zaručitelnosti bezpečnosti.

Požadavky na bezpečnostní funkcionalitu určují, která konkrétní bezpečnostní opatření (bezpečnostní funkce – identifikace, autentizace, bezpečnostní audit, nepopiratelnost původu apod.) se musí uplatnit, aby se podpořila bezpečnost produktu nebo systému IT.

Požadavky zaručitelnosti bezpečnosti mohou stanovovat sílu (odolnost) implementovaných bezpečnostních funkcí, požadované důkazy po hodnocení dodávané vývojářem, důkazy, které musí vypracovat třetí nezávislá strana (hodnotitel), rozsah, hloubku a přísnost hodnocení apod.

Záruka za splnění bezpečnostních plánů se odvozuje z dokázání oprávněnosti důvěry, že bezpečnostní funkce jsou implementovány správně a že implementované bezpečnostní funkce skutečně vyhovují daným bezpečnostním plánům.

6.5.4 Profil ochrany a bezpečnostní cíl

CC definují tři typy sestav požadavků na bezpečnost, jednu pomocnou a dvě cílové:

- *balík* (package)
  Je základní stavební jednotka pro skladbu jednotlivých požadavků do dílčích celků, na balík lze klást jak funkční požadavky, tak i požadavky zaručitelnosti bezpečnosti, z balíků se konstruují větší balíky, profily ochran, resp. bezpečnostní cíle.
- *profil ochrany* (protection profile)
  Umožňuje implementačně nezávisle stanovit požadovanou cílovou úroveň zaručitelnosti bezpečnosti a bezpečnostní funkcionalitu pro skupinu produktů nebo systémů IT, které budou plně vyhovovat dané množině bezpečnostních plánů;
  profily ochran se stanovují jako opakovaně použitelné a definují požadavky na produkt nebo systém IT, o kterých se ví, že jsou užitečné a potřebné pro splnění daných bezpečnostních plánů;
  profily ochran obsahují i logická zdůvodnění bezpečnostních plánů a bezpečnostních požadavků;
  profily ochran by mohly vypracovávat komunity uživatelů, vývojářů a jiných stran se společnými (příbuznými, shodnými) zájmy na bezpečnosti; na profily ochran se lze odkazovat při definování konkrétních bezpečnostních potřeb.
- *bezpečnostní cíl*
  Je určen pro vyjádření bezpečnostních požadavků na konkrétní produkt nebo systém IT;
  bezpečnostní cíl obsahuje množinu bezpečnostních požadavků, které lze zavést citováním některého profilu ochrany, případně přímým citováním odkazu na bezpečnostní komponentu nebo na komponentu zaručitelnosti za bezpečnost nebo explicitním vypracováním;
  bezpečnostní cíl dále obsahuje přehled specifikací produktu nebo systému IT, zadaných bezpečnostních požadavků a cílů a jejich logická zdůvodnění.

6.6 Bezpečnostní funkcionalita produktu/systému IT

Hlubší rozbor bezpečnostní funkcionality zaváděné v CC přesahuje rámec této kapitoly, který si klade za cíl seznámit čtenáře se základními filozofiemi a přístupy nově zaváděné normy ISO/IEC 15408. Systematickým rozborem bezpečnostních funkcí se zabývala kapitola 3. V pestrosti bezpečnostní funkcionality CC nepřinášejí žádné zásadní převratné změny proti chápání bezpečnostní funkcionality na konci 90. let. Omezíme se proto jen na orientační výčet bezpečnostní funkcionality považované v CC za standardní nástroje ochrany.

CC zavádějí bezpečnostní funkce v pojmech třída, rodina a komponenta. Každá *funkční třída* obsahuje (mimo definici své identity a popisu své struktury a účelu) alespoň jednu funkční rodinu, každá funkční rodina sestává z alespoň jedné funkční komponenty. Funkční komponenta je dále nedělitelný bezpečnostní element bezpečnostní funkcionality. Tak např. funkční třída *Identifikace a autentizace* sestává z funkčních rodin řešících dílčí bezpečnostní problémy typu *Definice atributů uživatelů*, *Specifikace tajemství*, *Autentizace uživatele*, *Identifikace uživatele* apod. Dále pak např. rodina *Autentizace uživatele* obsahuje pro plnění svého účelu komponenty (elementární bezpečnostní funkce) typu *Práce s časem*, *Jednorázová autentizace*, *Násobná autentizace* atd. Mezi standardní třídy bezpečnostních funkcí CC zahrnují bezpečnostní audit, komunikaci, kryptografickou podporu, ochranu dat uživatele, identifikaci a autentizaci, správu bezpečnosti, ochranu soukromí, ochranu bezpečnostní funkcionality, ochranu dostupnosti zdrojů, přístup k produktu nebo systému IT a důvěryhodné kanály a cesty.

6.7 Požadavky zaručitelnosti bezpečnosti

Cílem této kapitoly je popsat filozofii, ze které vychází přístup normy ISO/IEC 15408 k chápání zaručitelnosti bezpečnosti produktů a systémů IT.

6.7.1 Paradigma zaručitelnosti bezpečnosti IT

6.7.1.1 Základní filozofie zaručitelnosti bezpečnosti IT

Hrozby z hlediska bezpečnosti a z hlediska plnění požadavků daných bezpečnostní politikou organizace se mají vyslovovat jasně (tj. zřetelně a srozumitelně) a navrhovaná bezpečnostní opatření mají být z hlediska jejich zamýšleného účelu prokazatelně (tedy jasně, evidentně) dostatečná. Je nutné zavádět opatření, která snižují:

- pravděpodobnost existence zranitelných míst
- schopnost využití zranitelného místa (tj. záměrným využitkováním nebo neúmyslným podnětem)
- rozsah škod, které by mohly vzniknout využitím zranitelného místa.

Dále se mají zavádět opatření, která usnadňují:

- pozdější identifikaci zranitelných míst
- odstraňování škod, zmírňování následků a/nebo oznamování, že nějaké zranitelné místo bylo využitkováno nebo v něm neúmyslně vznikl podnět k jeho využití.

6.7.1.2 Role hodnocení

Zaručitelnost bezpečnosti jistého produktu nebo systému IT odvozuje z výsledků získaných hodnocením (tj. aktivním vyšetřováním) produktu nebo systému IT, který má být důvěryhodný. Hodnocení je tradiční prostředek pro poskytnutí záruky, je základem jak dokumentů dosud používaných hodnotících kritérií, tak i dokumentů ISO/IEC 15408. Norma ISO/IEC 15408 navrhuje provádět posuzování platnosti dokumentace a výsledného produktu nebo systému IT zkušenými hodnotiteli. Velký důraz se klade na rozsah, hloubku a přísnost hodnocení. Norma ISO/IEC 15408 nepopírá vynikající vlastnosti jiných nástrojů pro odvození zaručitelnosti bezpečnosti v IT, ani je nekomentuje. Ve výzkumu alternativních cest k získání zaručitelnosti bezpečnosti se pokračuje a norma ISO/IEC 15408 je strukturována tak, že nic nebrání tomu, aby je později akceptovala.

6.7.1.3 Ošetření zranitelných míst

Předpokládá se, že existují útočníci, kteří budou aktivně vyhledávat, jak využitkovat příležitosti k porušení bezpečnostních politik. Jejich motivací je snaha dostat se k nedovolenému výtěžku využitkováním aktiv. Útočníkem může být i ten, kdo provádí sice dobře myšlené, ale nicméně nebezpečné akce. Útočníci také mohou dávat podnět k využití zranitelných míst neúmyslně, a organizaci tak způsobovat újmu nechtěně.

Protože zpracovávání citlivých informací se nelze vyhnout a adekvátně důvěryhodné produkty a systémy IT dosud nejsou dostatečně dostupné, poruchy v IT jsou příčinou vysokých rizik. Je tudíž pravděpodobné, že prolomení bezpečnosti IT může vést k závažným ztrátám pro organizaci.

Prolomení bezpečnosti IT vzniká záměrným využitkováním zranitelných míst nebo neúmyslným podnětem k jejich využití v aplikaci IT provozované v nějakém reálném prostředí (obchodní činnosti apod.). Je proto žádoucí vykonat potřebné kroky s cílem prevence vzniku zranitelných míst v produktech a systémech IT. Zranitelná místa mají být v proveditelné míře:

- *odstraněna*
  tj. mají být vykonány aktivní kroky vedoucí k odhalení a k odstranění nebo k neutralizování všech využitelných zranitelných míst, nebo
- *minimalizována*
  tj. mají být vykonány aktivní kroky vedoucí k omezení potenciálního dopadu využití zranitelného místa na akceptovatelnou zbytkovou úroveň, nebo
- *monitorována*
  tj. mají být vykonány aktivní kroky vedoucí k zajištění, že jakýkoliv pokus o využití zbytkového zranitelného místa bude detekován, což umožní následně provést kroky minimalizující škodu.

6.7.1.4 Vznik zranitelných míst

Zranitelná místa vznikají jako důsledek selhání (opomenutí, zanedbání):

- ve specifikaci požadavků
  produkt nebo systém IT může plnit všechny funkce a vykazovat všechny rysy po něm požadované a přesto stále ještě obsahuje zranitelná místa, která ho činí z hlediska bezpečnosti nevhodným nebo neúčinným
- v konstrukci
  produkt nebo systém IT nesplňuje svoje specifikace a/nebo byla do něj zavlečena zranitelná místa v důsledku špatných konstrukčních standardů nebo nesprávných rozhodnutí (voleb) při jeho návrhu
- v provozu,
  produkt nebo systém IT byl sice správně zkonstruován podle správných specifikací, ale zranitelná místa do něj byla zavlečena v důsledku použití neadekvátních provozních řídicích nástrojů.

6.7.2 Zaručitelnost bezpečnosti IT podle CC

Zaručitelností bezpečnosti IT se rozumí důvody, příčiny, motivy a pohnutky opravňující důvěřovat, že produkt nebo systém IT splňuje své bezpečnostní plány. Zaručitelnost bezpečnosti IT lze odvodit z odkazů na takové zdroje, jako jsou nepodložená tvrzení, předchozí relevantní zkušenost nebo specifická zkušenost. Norma ISO/IEC 15408 ale odvozuje zaručitelnost bezpečnosti aktivním vyšetřováním. Aktivním vyšetřováním se rozumí hodnocení produktu nebo systému IT s cílem přesně určit jeho bezpečnostní vlastnosti.

6.7.2.1 Zaručitelnost bezpečnosti je odvozená z výsledků hodnocení

Tradičním prostředkem pro získání zaručitelnosti bezpečnosti je hodnocení a hodnocení je i základem přístupu k vyslovení zaručitelnosti bezpečnosti podle normy ISO/IEC 15408. Mezi hodnotící techniky lze zahrnout (bez nároku na úplnost výčtu):

- analýzu a kontrolu procesu (procesů) a procedury (procedur)
- kontrolu, že se proces(y) a procedura(y) používají
- analýzu korespondence mezi reprezentacemi návrhu hodnoceného předmětu (produktu nebo systému IT)
- analýzu reprezentace návrhu hodnoceného předmětu (produktu nebo systému IT) proti zadaným požadavkům
- ověřování (verifikace) důkazů
- analýzu dokumentů s návody, příruček
- analýzu vyvinutých testů funkcí a poskytnutých výsledků testů
- nezávislé testování funkcí (třetí stranou)
- analýzu zranitelných míst (včetně hypotéz o selháních)
- testování možností průniků.

6.7.2.2 Škálování zaručitelnosti bezpečnosti plynoucí z hodnocení

Filozofie normy ISO/IEC 15408 prosazuje dvě zásady:

- z vynaložení většího hodnotícího úsilí plyne důvěryhodnější zaručitelnost bezpečnosti
- cílem je vynakládat minimální hodnotící úsilí požadované pro poskytnutí nutné úrovně zaručitelnosti bezpečnosti.

Zvyšování úrovně hodnotícího úsilí se opírá o:

- *rozsah hodnocení*
  úsilí je větší, když se do hodnocení zahrnuje větší část produktu nebo systému IT
- *hloubku hodnocení*
  úsilí je větší, když je hodnocení rozvíjeno na jemnějších úrovních návrhu a na jemnějších implementačních detailech
- *přísnost hodnocení*
  úsilí je větší, když se hodnocení provádí strukturovanějším, formálnějším stylem.

6.7.2.3 Úrovně zaručitelnosti bezpečnosti podle CC

Kritéria, stanovená normou ISO/IEC 15408, definují vzrůstající škálu úrovní zaručitelnosti bezpečnosti. Jednotlivé úrovně definované na této škále jsou zavedeny tak, aby se dosáhlo vyrovnaného vztahu mezi *úrovní zaručitelnosti bezpečnosti* na straně jedné a cenou a realizovatelností požadovanou takovým stupněm zaručitelnosti na straně druhé.

Definice jednotlivých úrovní záruk za bezpečnost uvádějí, které požadavky zaručitelnosti bezpečnosti musí být splněny na jednotlivých úrovních.

Definovaných *úrovní zaručitelnosti bezpečnosti*, *EAL* (Evaluation Assurance Level), je sedm. Jsou uspořádané hierarchicky, každá úroveň musí splňovat jednak požadavky zaručitelnosti všech nižších úrovní a navíc požadavky definované na dané úrovni zaručitelnosti nově. Pro konkrétní aplikační prostředí se mohou jednotlivé úrovně zaručitelnosti bezpečnosti volitelně zesilovat.

6.7.3 Klasifikace požadavků zaručitelnosti bezpečnosti

Aby bylo možné používat nějakou taxonometrii při klasifikaci požadavků zaručitelnosti bezpečnosti, zavádějí se kategorie třída požadavků zaručitelnosti bezpečnosti (abstraktnější pohled) a rodina požadavků zaručitelnosti bezpečnosti (detailnější pohled).

6.7.3.1 Třída a rodina požadavků zaručitelnosti bezpečnosti

Nejobecněji chápaná sestava požadavků zaručitelnosti bezpečnosti pokrývá jistou problémovou oblast a nazývá se *třída*. Každá třída požadavků zaručitelnosti bezpečnosti sestává z jedné nebo několika *rodin*. Rodina požadavků zaručitelnosti bezpečnosti charakterizuje podmínky pro zaručitelnost bezpečnosti v některé dílčí problémové oblasti.

Definice třídy požadavků zaručitelnosti bezpečnosti třídu pojmenovává, popisuje záměr jejího zavedení a její strukturu. Definice rodiny požadavků zaručitelnosti bezpečnosti rovněž rodinu pojmenovává, dále pak uvádí obecné bezpečnostní cíle, které zavedení rodiny sleduje a popisuje její strukturu tvořenou z jednotlivých komponent zaručitelnosti bezpečnosti; v definici rodiny požadavků zaručitelnosti bezpečnosti se zavedení hierarchie komponent zdůvodňuje a vymezuje se rozsah, hloubka a přísnost jejich hodnocení.

6.7.3.2 Příklady tříd a rodin požadavků zaručitelnosti bezpečnosti

Jako příklady tříd požadavků zaručitelnosti bezpečnosti a jejich rodin lze uvést následující příklady tříd vymezené těmito problémovými oblastmi:

- správa konfigurace
  - automatizace správy konfigurace – definují se úrovně automatizace
  - schopnosti správy konfigurace – definují se charakteristiky systému správy
  - oblast správy konfigurace – uvádějí se položky produktu nebo systému IT řízené systémem správy konfigurace
- dodávka a provoz
  - dodávka – procedury použité pro udržování bezpečnosti během dodávky produktu nebo systému IT uživateli (počáteční i udržovací, záruka autenticity produktu nebo systému IT apod.)
  - instalace, generování a spuštění produktu nebo systému IT, nastavení jeho bezpečnostní funkcionality
- vývoj
  - specifikace bezpečnostní funkcionality
  - návrh na vysoké úrovni abstrakce – základní struktury bezpečnostní funkcionality, hlavní softwarové, hardwarové a firmwarové prvky
  - reprezentace implementace – zdrojové kódy, hardwarová schémata
  - návrh na nízké úrovni abstrakce (detailní návrh) – základ pro programování a konstrukci hardwaru
  - model bezpečnostní politiky – modely zvyšují záruku, že funkční specifikace odpovídá bezpečnostní politice
- dokumentace s návody
  - dokumentace správce
  - dokumentace uživatele

- podpora životního cyklu
  - bezpečnost vývoje – fyzické, procedurální, personální bezpečnostní opatření použitá ve vývojovém prostředí
  - oprava vad
  - konstrukční postupy použité při vývoji produktu nebo systému IT
  - vývojové nástroje a techniky
- testy
  - pokrytí – stanovení, které bezpečnostní funkce se testují
  - hloubka – detailnost, granularita, na které vývojář testoval produkt nebo systém IT
  - testy prováděné vývojářem
  - testy prováděné nezávislou autoritou (třetí stranou)
- oceňování zranitelnosti
  - analýza skrytých kanálů
  - analýza možnosti nesprávného použití – lze rozpoznat, že systém není bezpečně konfigurován a provozován
  - analýza síly bezpečnostních funkcí – např. analýza mechanismu hesel
  - analýza zranitelnosti – identifikace vad zavlečených při vývoji (úplnost bezpečnostní funkcionality, závislosti mezi bezpečnostními funkcemi), testování možností průniků

6.7.4 Specifikace požadavků zaručitelnosti bezpečnosti

Rodina požadavků zaručitelnosti bezpečnosti sestává z jedné nebo více *komponent*, každá komponenta podmínka sestává z jednoho nebo více *prvků*. Komponenty a prvky se používají pro specifikaci požadavků zaručitelnosti bezpečnosti v profilech ochrany[29] nebo v bezpečnostních cílech[30].

6.7.4.1 Komponenty a prvky zaručitelnosti bezpečnosti

Každá *komponenta zaručitelnosti bezpečnosti* je identifikována, kategorizována, registrována a odkazována pomocí své identifikace. Její definice dále uvádí přesně stanovené bezpečnostní cíle, záměry a detailní popis těchto cílů a záměrů, případné aplikační poznámky, které usnadňují jejich použití, a nakonec uvádí popis souvislostí mezi komponentami a definuje prvky tvořící danou komponentu rodiny požadavků. *Prvek zaručitelnosti bezpečnosti* představuje takový elementární bezpečnostní požadavek, který by po dalším dělení neposkytnul smysluplný hodnotitelný výsledek. Představuje tudíž nejmenší samostatný bezpečnostní požadavek. Každý prvek zaručitelnosti bezpečnosti se řadí do jedné ze tří skupin:

- *prvky vývojových akcí*
  činnosti, které má vývojář dělat a vymezení důkazových materiálů popsaných v následující skupině
- *důkazové prvky*
  požadované důkazy, popis co má důkaz demonstrovat, jakou informací má důkaz vyjádřit

[29] implementačně nezávislá soustava bezpečnostních požadavků na jistou kategorii produktů nebo systémů IT, která splňuje určité, přesně stanovené potřeby zákazníka

[30] množina bezpečnostních požadavků a specifikací používaná jako základ pro hodnocení/definování bezpečnosti produktu nebo systému IT

- *hodnotitelské akce*
  činnosti, které má provádět hodnotitel. Explicitně mezi takové akce patří potvrzení, že jsou splněny požadavky popsané pomocí důkazových prvků. Dále sem patří akce a analýzy, které by měl provádět hodnotitel jako dodatečná hodnocení k akcím, které již byly provedeny vývojářem. Pokud nejsou výsledky některých akcí vývojáře pokryty důkazovými prvky, musí odpovídající akce implicitně provést hodnotitel.

Akce vývojáře a důkazový materiál definují ty požadavky zaručitelnosti bezpečnosti, které jsou posléze použity pro vyjádření odpovědnosti vývojáře při prokazování zaručitelnosti v bezpečnostní funkcionalitě hodnoceného produktu nebo systému IT. Pokud vývojář tyto podmínky zaručitelnosti bezpečnosti splní, může mít vyšší důvěru v to, že jeho produkt nebo systém IT vyhovuje funkčním požadavkům a požadavkům zaručitelnosti bezpečnosti stanoveným profilem ochrany nebo bezpečnostním cílem.

Akce hodnotitele definují odpovědnost hodnotitele ve dvou rovinách. Hodnotitel jednak ověřuje a potvrzuje, že jsou splněny dané bezpečnostní cíle, resp. že hodnocený produkt nebo systém IT vyhovuje danému profilu ochrany, a jednak ověřuje, že hodnocený produkt nebo systém IT odpovídá stanoveným požadavkům na funkčnost a stanoveným požadavkům zaručitelnosti bezpečnosti. Když hodnotitel prokáže, že je správně implementován profil ochrany, resp., že jsou splněny bezpečnostní cíle a požadavky zaručitelnosti bezpečnosti, může poskytnout podklad pro oprávněnost důvěry v to, že hodnocený produkt nebo systém IT splňuje své bezpečnostní plány. Prvky vývojových akcí, důkazové prvky a požadavky stanovující explicitní akce hodnotitele identifikují úsilí hodnotitele, které má vynaložit při ověřování tvrzení o bezpečnosti, která jsou uvedena jako bezpečnostní cíle v hodnoceném produktu nebo systému IT.

Prvky zaručitelnosti bezpečnosti reprezentují požadavky, které se musí splnit. Vyjadřují se jasně, stručně a jednoznačně. Žádné složené věty, každá samostatná podmínka se vyjadřuje jako jeden prvek zaručitelnosti. Spíše než zkratkovitá symbolická vyjádření pomocí omezených množin rezervovaných pojmů se používá přirozeného jazyka.

6.8 Charakteristiky úrovní zaručitelnosti bezpečnosti

Závěrem uvádíme konkrétní základní charakteristiky jednotlivých úrovní zaručitelnosti bezpečnosti (EAL) podle normy ISO/IEC 15408.

6.8.1 EAL1, funkčně testovaný produkt nebo systém IT

6.8.1.1 Cíle EAL1

- Úroveň EAL1 je použitelná tam, kde se požaduje správný (bezchybný) provoz, ale hrozby nejsou posuzovány jako závažné. Je vhodná tehdy, když se požaduje získání nezávisle vyslovené záruky podporující tvrzení, že byla vynaložena patřičná snaha o ochranu např. personalistik a podobných informací.
- Úroveň EAL1 se odvozuje z hodnocení produktu nebo systému IT dostupného zákazníkovi. Hodnocení zahrnuje nezávislé testování, zda jsou splněny specifikace a zkoumání poskytnuté dokumentace s návody. Hodnocení na této úrovni by mohlo být úspěšně proveditelné bez spoluúčasti a bez pomoci vývojáře a mohlo by si vyžádat vynaložení minimálních nákladů.
- Při hodnocení produktu nebo systému IT úrovně EAL1 se poskytují důkazy, že jeho funkčnost je konzistentní s dokumentací a že poskytuje použitelnou ochranu proti identifikovaným hrozbám.

6.8.1.2 Záruky EAL1

- Úroveň EAL1 je základní úrovní zaručitelnosti bezpečnosti danou výsledky analýzy bezpečnostních funkcí pomocí specifikací funkcí a rozhraní a dokumentace s návody prováděnou s cílem porozumět bezpečnostnímu chování.
- Analýza se podporuje nezávislým testováním bezpečnostních funkcí.
- Ve srovnání s nehodnocenými produkty nebo systémy IT úroveň EAL1 představuje významně vyšší zaručitelnost bezpečnosti.
- Hodnocení na úrovni EAL1 se týká identifikace (čísla verze) produktu nebo systému IT, procedur instalace, generování a spuštění provozu, neformální specifikace funkcí, dokumentace správce a uživatele a provádí se nezávislé testování bezpečnostních funkcí.

6.8.2 EAL2, strukturálně testovaný produkt nebo systém IT

6.8.2.1 Cíle EAL2

- Na úrovni EAL2 se požaduje kooperace s vývojářem, pro hodnocení jsou od vývojáře požadovány informace o návrhu a výsledky testů. Po vývojáři se ovšem nemá požadovat více než odpovídá dobrým obchodním praktikám, hodnocení si tudíž neklade požadavky na podstatné zvýšení finančních a časových nákladů.
- Úroveň EAL2 je proto vhodnou úrovní pro podmínky, ve kterých vývojář nebo uživatel požadují malou až průměrnou úroveň nezávisle zaručované bezpečnosti a nepožaduje se dostupnost úplné vývojové dokumentace. Tato situace může odpovídat např. zabezpečování systémů podnikového účetnictví nebo případům, kdy je vývojář dostupný pouze omezeně.

6.8.2.2 Záruky EAL2 (rozšíření proti EAL1)

- Požaduje se provedení analýzy návrhu produktu nebo systému IT na vysoké úrovni.
- Analýza se navíc podporuje důkazy, poskytnutými vývojářem, získanými testováním bezpečnostních funkcí, výběrovým nezávislým potvrzením výsledků testů vývojáře, analýzou síly bezpečnostních funkcí a důkazy vývojářova hledání obvyklých zranitelných míst (všeobecně známých zranitelných míst).
- Požaduje se důkaz bezpečných procedur dodávek a konfigurační seznam hodnoceného produktu nebo systému IT.
- Úroveň EAL2 představuje významně vyšší zaručitelnost bezpečnosti než úroveň EAL1, poněvadž se po vývojáři požaduje, aby svůj produkt testoval a provedl analýzu zranitelných míst a provádí se nezávislé testování založené na detailnějších specifikacích hodnoceného produktu nebo systému IT.
- Hodnocení na úrovni EAL2 se proti úrovni EAL1 týká i konfiguračních položek správy konfigurace, procedur dodávek, popisu návrhu na vysoké úrovni, důkazů úplnosti testů bezpečnostní funkcionality, testování prováděného vývojářem i nezávislého testování třetí stranou, síly bezpečnostních funkcí a analýzy zranitelnosti provedené vývojářem.

6.8.3 EAL3, metodicky testovaný a kontrolovaný produkt nebo systém

6.8.3.1 Cíle EAL3

- Úroveň EAL3 umožňuje svědomitému vývojáři dosáhnout maximálně možnou zaručitelnost bezpečnosti odvozenou z průkazného používání bezpečnostního konstruování při návrhu produktu nebo systému IT, a to aniž by vývojář musel podstatně měnit své dobré vývojové praktiky.
- Úroveň EAL3 je vhodná pro podmínky, ve kterých vývojář nebo uživatel požadují průměrnou úroveň nezávisle zaručené bezpečnosti, důkladné vyšetření produktu nebo systému IT a vývoje a nechtějí provádět rozsáhlý reengineering.

6.8.3.2 Záruky EAL3 (rozšíření proti EAL2)

- Hodnotí se důkazy testování návrhu na vysoké úrovni. Požaduje se používání řídicích nástrojů ve vývojovém prostředí a správa konfigurace produktu nebo systému IT.
- Úroveň EAL3 představuje významně vyšší zaručitelnost bezpečnosti než úroveň EAL2, poněvadž se požaduje úplnější testování pokrytí bezpečnostních funkcí a mechanismů a/nebo procedur, které poskytují jistou důvěru v to, že produkt nebo systém IT nebyl nějak narušen během vývoje.
- Hodnocení na úrovni EAL3 se proti úrovni EAL2 týká i autorizačních nástrojů správy konfigurace a pokrytí správy konfigurace, návrhu prosazení bezpečnosti na vysoké úrovni, identifikace bezpečnostních opatření při vývoji, analýzy pokrytí funkcionality testy a testů návrhu na vysoké úrovni a zkoumání návodů z hlediska možné zranitelnosti plynoucí z neúplnosti nebo nedokonalosti dokumentace.

6.8.4 EAL4, metodicky navrhovaný, testovaný a přezkoumávaný produkt nebo systém IT

6.8.4.1 Cíle EAL4

- Úroveň EAL4 umožňuje svědomitému vývojáři dosáhnout maximálně možnou zaručitelnost bezpečnosti odvozenou z průkazně používaného bezpečnostního inženýrství založeného na dobrých komerčních vývojových praktikách, které, třebaže se požaduje vysoká přísnost, nepožadují mimořádně velké odborné znalosti, dovednosti a jiné zdroje. Úroveň EAL4 je nejvyšší úrovní zaručitelnosti bezpečnosti, která bude muset pravděpodobně být ekonomicky zabudovatelná do existujících výrobních postupů.
- Úroveň EAL4 je tudíž vhodná pro podmínky, ve kterých vývojář nebo uživatel požadují průměrnou až vysokou úroveň nezávisle zaručené bezpečnosti pro běžně prodávané zboží a jsou srozuměni s vynaložením dodatečných nákladů na specifické bezpečnostní konstruování.

6.8.4.2 Záruky EAL4 (rozšíření proti EAL3)

- Musí se provést analýza všech rozhraní a analýza podrobného (detailního) návrhu a implementace bezpečnostních funkcí. Požaduje se existence neformálního modelu bez-

pečnostní politiky produktu nebo systému IT. Provádí se nezávislá analýza zranitelnosti prokazující odolnost vůči útočníkům s malými možnostmi a schopnostmi.

- Správa konfigurace se analyzuje detailně, včetně jejích automatizačních prostředků.
- Úroveň EAL4 představuje významně vyšší zaručitelnost bezpečnosti než úroveň EAL3, poněvadž se požaduje hodnotit detailnější popis návrhu, implementace bezpečnostních funkcí a požadují se vylepšené mechanismy nebo procedury, které poskytují důvěru, že produkt nebo systém IT nebyl nějak narušen během vývoje nebo dodávky.
- Hodnocení na úrovni EAL4 se proti úrovni EAL3 týká i automatizace konfiguračních postupů, pokrytí vlastní konfigurace, podpory správy konfigurace, detekce modifikace během dodávky, úplné sestavy vnějších rozhraní, implementace bezpečnostní funkcionality, detailního návrhu, neformálního modelu bezpečnostní politiky, dobře definovaných vývojových nástrojů, analýzy správnosti analýzy zranitelnosti provedené vývojářem a provedení nezávislé analýzy zranitelných míst.

6.8.5 EAL5, semiformálně navrhovaný a testovaný produkt nebo systém IT

6.8.5.1 Cíle EAL5

- Úroveň EAL5 umožňuje svědomitému vývojáři dosáhnout maximálně možnou zaručitelnost bezpečnosti odvozenou z průkazně používaného bezpečnostního konstruování založeného na dokonalých komerčních vývojových praktikách podporovaných běžnou, nikoli extrémní aplikací speciálních bezpečnostních technik. Takový produkt nebo systém IT bude pravděpodobně navrhován a vyvíjen s apriorním záměrem dosažení úrovně zaručitelnosti bezpečnosti EAL5. Je pravděpodobné, že dodatečné náklady vynaložené na splnění podmínek zaručitelnosti bezpečnosti EAL5, při porovnání s použitím náročných vývojových postupů bez zahrnování specializovaných technik, nebudou velké.
- Úroveň EAL5 je tudíž vhodná pro podmínky, ve kterých vývojář nebo uživatel požadují vysokou úroveň nezávisle zaručené bezpečnosti pro speciálně plánovaný vyvíjený produkt nebo systém IT a požadují použití dokonalých vývojových nástrojů a nechtějí hradit neodůvodněně zvýšené náklady za použití speciálních bezpečnostních technik.

6.8.5.2 Záruky EAL5 (rozšíření proti EAL4)

- Hodnotí se úplná implementace, používá se formální model bezpečnostní politiky a semiformální prezentace specifikace bezpečnostních funkcí a návrhu vysoké úrovně a semiformálním způsobem se demonstruje jejich vzájemná korespondence. Produkt nebo systém IT musí být navržen jako modulární produkt nebo systém.
- Testy se provádějí na úrovni detailního návrhu a ověřuje se analýza skrytých kanálů, provedená vývojářem.
- Správa konfigurace produktu IT musí být z hlediska komponent produktu nebo systému IT úplná a vyčerpávající.
- Úroveň EAL5 představuje významně vyšší zaručitelnost bezpečnosti než úroveň EAL4, poněvadž se požaduje hodnocení semiformálních popisů návrhu, celé implementace bezpečnostních funkcí, požaduje se strukturovanější, a tudíž snadněji analyzovatelná architektura, analýza skrytých kanálů a požadují se vylepšené mechanismy a procedury,

které poskytují důvěru v to, že produkt nebo systém IT nebyl nějak narušen během vývoje nebo dodávky.

- Hodnocení na úrovni EAL5 se proti úrovni EAL4 týká i vývojových nástrojů správy konfigurace, používají se semiformální specifikace bezpečnostních funkcí a semiformální návrh na vyšší úrovni, hodnotí se implementace celé bezpečnostní funkcionality, na semiformální úrovni se hodnotí korespondence návrhu a implementace, používá se formální model bezpečnostní politiky, musí se používat implementační standardy a standardizovaný model celého životního cyklu, testování se provádí na úrovni detailního návrhu, požaduje se provedení analýzy skrytých kanálů a produkt nebo systém IT musí být odolný proti útokům střední síly.

6.8.6 EAL6, testovaný produkt nebo systém IT se semiformálně ověřovaným návrhem

6.8.6.1 Cíle EAL6

- Úroveň EAL6 umožňuje svědomitému vývojáři dosáhnout maximálně možnou zaručitelnost bezpečnosti odvozenou z prokázaného použití bezpečnostního konstruování a dokonalého vývojové prostředí. Cílem je mít možnost vytvářet vynikající produkty nebo systémy IT pro ochranu aktiv s vysokou hodnotou provozované ve vysoce rizikových prostředích.
- Úroveň EAL6 je tudíž vhodná pro vývoj bezpečných produktů nebo systémů IT, které se mají používat ve vysoce rizikových prostředích a kde hodnota chráněných aktiv ospravedlňuje dodatečné vyšší náklady.

6.8.6.2 Záruky EAL6 (rozšíření proti EAL5)

- Požaduje se strukturovaná prezentace implementace a detailního návrhu. Hodnocený předmět musí mít modulární, hierarchickou architekturu a vývojář musí provést systematickou analýzu skrytých kanálů.
- Vývojový proces musí mít strukturovaný charakter, správa konfigurace musí být úplná.
- Úroveň EAL6 představuje významně vyšší zaručitelnost bezpečnosti než úroveň EAL5, poněvadž se požadují mnohem více vyčerpávající analýzy, strukturovaná reprezentace implementace, propracovanější architektura (hierarchické vrstvy), nezávislá mnohem více vyčerpávající analýza zranitelnosti, systematická identifikace skrytých kanálů a náročnější správa konfigurace a řídicí nástroje pro vývoj. Produkt nebo systém IT s úrovní EAL6 musí být odolný vůči útokům vedeným s velkou silou.

6.8.7 EAL7, testovaný produkt nebo systém IT s formálně ověřovaným návrhem

6.8.7.1 Cíle EAL7

- Úroveň bezpečnosti EAL7 se používá pro vývoj bezpečných produktů nebo systémů IT určených pro provozování ve vysoce rizikových prostředích nebo kde vysoká hodnota aktiv ospravedlňuje vyšší náklady. Praktická použitelnost EAL7 je v současné době

omezena na produkty nebo systémy IT s úzce zaměřenou bezpečnostní funkcionalitou, kterou lze rozsáhle formálně analyzovat.

6.8.7.2 Záruky EAL7 (rozšíření proti EAL6)

- Požaduje se formální prezentace funkčních specifikací a návrhu vysoké úrovně, formálně musí být demonstrovatelná rovněž korespondence mezi návrhem vysoké úrovně a detailním návrhem, pokud je to možné. Návrh nesmí být složitý, musí se jednat o jednoduchý produkt nebo systém IT.
- Úroveň EAL7 představuje významně vyšší zaručitelnost bezpečnosti než úroveň EAL6, poněvadž se požaduje vyčerpávající analýza pomocí formálních prezentací, a dále formální prokázání korespondence návrhu vysoké úrovně a detailního návrhu a konečně rovněž vyčerpávající testování.

Rejstřík

A

B

C

D

E

F

H

C

I

J

K

M

N

O

P

R

S

T

U

V

W

Z

Odkazovaná literatura

[And72] Anderson, J. P.: Computer Security Technology Planning Study, ESD-TR-73-51, ESD/AFSC, US Air Force, Bedford, Mass., October 1972.

[BLP76] Bell, D. E. - LaPadula, L. J.: Secure Computer Systems: Unified Exposition and Multics Interpretation, Report MTR-2997 Rev. 1, MITRE Corporation, Bedford, Mass, 1976.

[FC] Federal Criteria for Information Technology Security, Volume I and II, US National Institute of Standards and Technology & National Security Agency, December 1992.

[FIPS140] FIPS PUB 140-1, Security Requirements for Cryptographic Modules, US DOC/NBS, 1994

[ITSEC] Information Technology Security Evaluation Criteria (ITSEC), Office for Official Publications of the European Communities, Luxembourg 1991, ISBN 92-826-3004-8.

[ITSEM] Information Technology Security Evaluation Manual (ITSEM), Office for Official Publications of the European Communities, Luxembourg 1994, ISBN 92-826-7087-2.

[MSFR] Minimum Security Functionality Requirements for Multi-User Operating Systems, Computer Security Division, Computer Systems Laboratory, US National Institute of Standards and Technology, Issue 1, January 28, 1992.

[MSR] Minimum Security Requirements for Multi-User Operating Systems, NISTIR-5153, Computer Security Division, Computer Systems Laboratory, US National Institute of Standards and Technology, March 1993.

[TCSEC] Trusted Computer Systems Evaluation Criteria, DOD 5200.28-STD, Department of Defense, United States of America, December 1985.

[ZSIEC] Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems, ISBN 3-88784-200-6, German Information Security Agency (Bundesamt für Sicherheit in der Informationstechnik), Federal Republic of Germany, January 1989.

[TRMITS] ISO/IEC JTC1/SC27 TR 13335: Guidelines for the Management of IT Security.

[TTP] ISO/IEC JTC1/SC27 N2138, PDTR 14516: Information technology - Security techniques - Guidelines on the use and management of Trusted Third Party Services. November 1998.