Ing. Oldřich Pekárek, CSc.

Bezpečnostní politika ve vojenských informačních systémech

Přestože od konce studené války poklesla hrozba vzniku velkých válek vedených masovými armádami, je svět dále a intenzivněji destabilizován hrozbou ozbrojeného násilí. Tato hrozba ohrožuje především společnost a tím i následně samotnou existenci států. Jen za minulý rok bylo ve světě napočítáno sedmdesát jedna konfliktů, které měly charakter ozbrojeného válečného střetu, byť i omezeného, lokálního rozsahu (údaj nadace Národní výbor obrany, USA).

Ze statistiky plyne, že neustále klesá podíl konfliktů mezi státy a roste počet etnicky, nábožensky a skupinově motivovaných střetů, které vyúsťují v masový a bezohledný teror proti obyvatelstvu a nesou s sebou nebezpečí zhroucení státu, resp. jeho demokratického systému. Nebezpečí se ještě násobí častým přechodem vycvičených vojáků - profesionálů a odborníků do služeb agresivních organizací a skupin, nebo států, které podporují mezinárodní terorismus. Přičteme-li k této situaci namnoze zřejmou absenci racionálního myšlení vůdců těchto terorizujících sil, jejich ztrátu pudu sebezáchovy, ignoranci možných následků jejich činnosti, jakož i neschopnost zvládnout rozpoutané vražedné zlo, je nutno, za těchto změněných okolností, přehodnotit i priority vojenských a společensky významných informačních systémů a jimi zpracovávaným citlivým informacím.

Vždyť právě existence informačních systémů, jejich přesná a rychlá funkce, včetně jejich schopnosti udržet důvěrnost citlivých informací, je jednou z podmínek fungování státní výkonné moci a řízení obranných reakcí.

Proto jsou a budou informační systémy častým cílem útoků destabilizačních sil.

Útoky na informační systémy rozumíme celou škálu forem, které začínají u pokusů o získání citlivých utajovaných informací (porušení důvěrnosti informací), pozměňování informací (porušení jejich integrity), až po ničení informací v systému a jeho násilné vyřazení z činnosti.

Dřívější bipolární uspořádání světa diktovalo bezpečnostní politiku pro informační systémy plně v souladu s tehdejším nazíráním na možnost vzniku vojenského konfliktu jako důsledku této bipolarity. Z toho vyplývá, že nejzávažnější hrozby pro informační systémy byly spatřovány téměř výhradně v úsilí rozvědek potenciálního protivníka o získání kontroly nad citlivými informačními toky a v případě otevřeného konfliktu pak ve snaze o destrukci celého informačního systému.

Z hlediska současného poznání se utváří celé spektrum možných hrozeb pro informační systémy, s nejrůznějšími motivacemi, kde závažnost jednotlivých hrozeb se v závislosti na okolnostech může výrazně měnit.

Jmenujme alespoň ty nejzávažnější:

▲ zpravodajské služby států s prioritním zaměřením na průmyslovou, politickou a vojenskou špionáž, s cíli zabezpečit jak politické, tak i ekonomické zájmy svých vlád;

▲ zpravodajské služby, které pracují pro velké firmy s orientací na získání a udržení odbytišť, zakázek a technologického know-how;

▲ teroristické organizace a extremistické skupiny (národní i mezinárodní), často podporované některými totalitními státy;

▲ kvalifikovaná kriminalita namířená především proti finančním, správním a bezpečnostním institucím a jejich informačním systémům;

▲ rutinní „hackeři", studenti a zvídaví lidé s odborným vzděláním v oblasti informatiky, kteří často bez zřejmé motivace pronikají do informačních systémů a rozrušují jejich integritu. To platí zvláště pro informační systémy propojené se sítí INTERNET;

▲ tvůrci a zaváděči počítačových virů, kteří narušují informační systémy rovněž většinou bez zřejmého motivu.

Pozn.: *Uvedené členění hrozeb je v souladu se současným názorem odpovědných míst NATO.*

Za těchto změněných podmínek je **nutno nově definovat i bezpečnostní politiku pro informační systémy Armády ČR.**

Bezpečnostní politika informačního systému

Nejprve obecně definujme bezpečnostní politiku informačního systému [4]:

Bezpečnostní politika informačního systému vyjadřuje bezpečnostní cíle, včetně všech použitých způsobů a nástrojů k jejich dosažení. Základním cílem je pak prokazatelné dosažení požadované úrovně bezpečnosti.

Z definice plyne, že bezpečnostní politikou informačního systému rozumíme naprosto konkrétní dokument.

Obecným východiskem pro stanovení systémově bezpečnostní politiky je bezpečnostní politika státu (obecná bezpečnostní politika) v oblasti ochrany citlivých informací, kterou tvoří soubor zákonů a z nich především o zákon č. 102/1971 Sb., o ochraně státního tajemství, s příslušnými novelami a provádějícími předpisy. S touto problematikou rovněž souvisí zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech.

Tak jako je tomu v jiných zemích, lze očekávat i v ČR další precizování bezpečnostní politiky státu směrem k ochraně informací a s tím i zdokonalování legislativních ustanovení.

V AČR pak tvoří základ bezpečnostní politiky soubor předpisů, rozkazů, procedur a metodik vydaných k ochraně utajovaných skutečností.

I přes zřejmé zaostávání úrovně legislativní podpory prosazování bezpečnosti v informačních systémech je jakákoli bezradnost a pasivita v tomto ohledu zbytečná. Zaostávání legislativy a procedurálních pravidel za rychlým rozvojem informatiky je celkem logické. S obdobným stavem zápolí více či méně všechny moderní státy. Snad nejlepší radu představuje citát prof. G. Gilmore z Yaleovy univerzity: **„Když zahodíte knihu s předpisy, nezbude vám nic než odpovědnost."**

Dodejme jen, že tento pocit odpovědnosti, spojený s dobrou profesionální kvalifikací, dokáže mnoho.

V každém případě je pro stanovení a prosazování odpovídající bezpečnostní politiky rozhodující znalost jejích cílů a metod, analytické myšlení, expertní zkušenost a v neposlední řadě i finanční možnosti. Je třeba počítat s tím, že náklady na bezpečnost

budou vždy nad hranicí 10 % celkových pořizovacích nákladů instalovaného informačního systému a tento podíl bude mít rostoucí trend. Doporučuje se proto zachovat si i nezbytnou dávku pragmatismu pro reálný odhad aktuálnosti jednotlivých hrozeb, ceny vlastních informací a ekonomické přiměřenosti při budování bezpečnostních informačních systémů. Je žádoucí formulovat bezpečnostní politiku informačního systému tak, aby tato byla maximálně účinná a transparentní, aby realizací bezpečnostních mechanismů nesnižovala a nekomplikovala jeho užitné vlastnosti.

Je nezbytné prosadit, aby systémová bezpečnostní politika všech stupňů byla popsána výkonným dokumentem s jasným metodickým a požadovaným obsahem a byla oproštěna od formálního balastu. Systémová bezpečnostní politika je prvním dokumentem, který zpracovává bezpečnostní architekt na počátku projekčních prací [4] a který je schvalován formou oponentního řízení. Požaduje se, aby dokument systémové bezpečnostní politiky vždy zahrnoval a konkrétně odpovídal na následující otázky:

- cíle informačního systému a cíle bezpečnostní politiky. V tomto smyslu dokument specifikuje začlenění informačního systému do struktur řízení a velení, specifikuje jeho strukturu, definuje hlavní informační toky, typ a stupeň utajení (klasifikaci) informací; cíle a nástroje bezpečnostní politiky pak určuje jako reakci na výsledek analýzy hrozeb,
- hrozby, jimiž má systém především čelit, včetně možných souvislostí (např. mezinárodních nebo regionálních, zájem rozvědek, rozkrádání atp.); jde především o takové hrozby, které vnáší do informačního systému rizika kompromitace, modifikace, destrukce a zneužití jak utajovaných informací, tak i vlastního informačního systému,
- specifikace požadovaných bezpečnostních služeb systému jednotlivým subjektům řízení a velení, s ohledem na minimalizaci rizika ztrát způsobených účinkem reálných hrozeb, způsob obnovy činnosti systému,
- mechanismy a vazby předávání informací oprávněným subjektům, jejich evidenci, označování a prokazování oprávnění,
- bezpečnostní zásady personální politiky pro osoby, které přicházejí do styku s informačním systémem na různých úrovních, pořízení seznamů subjektů (osob, orgánů) s odpovídajícími stupni osobního oprávnění k přístupu k utajovaným informacím příslušné klasifikace, zabezpečení personálního prověření; stanovení odborných a kvalifikačních předpokladů osob, způsoby jejich proškolování jak na počátku jejich vstupu do systému, tak i průběžně,
- právní a jiné bezpečnostní normativy, kterým má systém vyhovovat, odkazy na přijaté standardy, požadovanou třídu bezpečnosti posle přijatých (uznávaných) standardů atd. [1, 2],
- dokumenty, které obsahují nadřízenou bezpečnostní politiku,
- vazby na bezpečnostní politiku podřízených a spolupracujících informačních systémů,
- určení orgánů odpovědných za prosazování jednotlivých zásad bezpečnostní politiky, za vedení a využívání revizních záznamů (auditu), jakož i za kontinuitu dohledu, postupy řešení incidentních situací,
- specifikace finančního a materiálního krytí činností, které prosazují bezpečnost.

Dokument Bezpečnostní politika systému musí být vždy doplněn tabulkami a seznamy, v kterých případech i vývojovými diagramy a nákresy v rozsahu, který odpovídá velikosti a složitosti systému.

Jedině po schválení systémové bezpečnostní politiky lze přistoupit k dalším projektovým pracím.

Vzájemná souvislost aktiv informačního systému, hrozeb a jeho bezpečnostní politiky

Do procesu analýzy bezpečnosti informačního systému vstupují podle **obr. 1** následující základní problémové množiny:

A aktiva informačního systému, která jsou více či méně vystavena působení hrozeb a je možné je rozdělit do následujících kategorií:
- (hardware) přístrojové komponenty systému, např. procesorové jednotky, paměti, periferní zařízení, šifro a autentizační zařízení, síťové podsystémy, přenosové prostředí, centra a uzly, kabeláže budov, napájecí zdroje včetně záložních atp.,
- (software) operační systémy, programové aplikace, datové báze, autentizační, auditové a klíčové informace atd.,
- stavební lokality a jiné objekty, které souvisejí s činností informačního systému, logistické zabezpečení, sklady médií atp.;

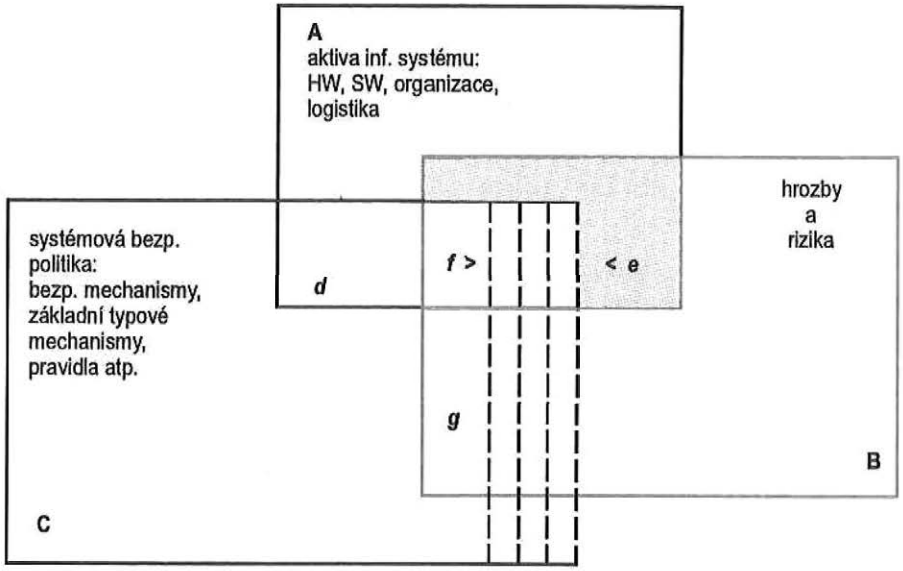
B hrozby, které tvoří hrozby vnější a hrozby vnitřní:
- vnější hrozby představují jednak různé formy fyzického útoku na systém nebo jeho části, jednak i přírodní živelní pohromy, elektrické výboje, havárie atp. Proti těmto hrozbám sám informační systém nedisponuje účinnou obranou, a tak tyto musí být eliminovány bezpečnostními mechanismy, které vycházejí z fyzické, procedurální a personální bezpečnosti,
- vnitřní hrozby jsou takové hrozby, proti kterým má informační systém své obranné prostředky, které spočívají v jeho bezpečnostních funkcích. Tyto funkce jsou kombinací přístrojových a programových nástrojů. Vnitřní hrozby jsou zpravidla charakterizovány jako skrytý útok protivníka s cílem získat citlivé informace nebo porušit jejich integritu, zkomplikovat jejich dostupnost anebo ve zvoleném čase, informační systém zevnitř rozvrátit;

C bezpečnostní politika, která je v tomto případě reprezentována souborem bezpečnostních mechanismů informačního systému, fyzické ochrany, personálních a procedurálních protiopatření.

Bezpečnost se analyzuje

Při budování bezpečnostních informačních systémů je třeba vzít v úvahu trvale působící rozpory téměř filozofické povahy, které dnes negativně ovlivňují řešení otázek informační bezpečnosti. Z nich vyjmenujme alespoň ty nejzávažnější:

- rozvíjející se telekomunikace a informatika jako celek zvyšující stupeň obtížnosti při nalézání odpovídajících bezpečnostních technologií; technické, kryptografické a programové prostředky ochrany rychle morálně stárnou,



Poznámka:
Jednotlivé množiny A, B, C vytvářejí interakční průniky, které charakterizují několik kategorií problémů bezpečnosti:

$f = A \cap B \cap C$ (1)

představuje soubor aktiv systému, která jsou ohrožena definovanými hrozbami nad přípustnou míru rizika, ale která jsou na základě požadavků systémové bezpečnostní politiky odpovídajícím způsobem chráněna,

$e = (A \cap B) \setminus f$ (2)

představuje soubor hrozeb, které nejsou kryty bezpečnostními mechanismy, a rizika plynoucí z tohoto ohrožení jsou tzv. zbytková rizika (reziduální risk),

$g = (B \cap C) \setminus f$ (3)

představuje soubor hrozeb, pro něž sice má bezpečnostní politika odpovídající obrany, ale tyto hrozby neohrožují nijak chráněná aktiva informačního systému,

$d = (A \cap C) \setminus f$ (4)

představuje soubor aktiv, pro něž jsou k dispozici bezpečnostní mechanismy, ale tato aktiva nejsou v daném systému ohrožena,

Vertikální posunutí mezi množinami A a B vylučuje ideální případ, kdy by se reziduální rizika rovnala nule.

Obr. 1: Interakce mezi aktivy informačního systému, bezpečnostní politikou a hrozbami

- ochrana informací se stává obecně známou technickou disciplínou, což je v obecné rovině pozitivním jevem, ale ve svém důsledku má negativní dopad na prolomitelnost bezpečnostních systémů; užívané metody a mechanismy bezpečnosti jsou známy podstatně širšímu okruhu technické veřejnosti, než tomu bylo dříve,
- uživatelé informačních systémů zpravidla požadují maximální bezpečnost s minimálními vynaloženými prostředky, cena bezpečnosti roste, zatímco úroveň ochran je značně limitována rozpočtovými možnostmi.

Za těchto podmínek je jediným rozumným východiskem velmi pečlivá identifikace hrozeb a rizik pro budovaný informační systém, jejíž výsledek je pak podkladem pro optimální rozhodnutí o volbě bezpečnostních mechanismů jak z hlediska požadované účinnosti, tak i z hlediska vynaložených nákladů.

Proces analýzy obecně zahrnuje:

- inventarizaci a ohodnocení aktiv informačního systému,
- identifikaci hrozeb a slabin informačního systému,
- hodnocení rizik a následků.

V této souvislosti je na místě připomenout nezbytnost „ocenění dat" jako hodnoty, která vstupuje do analytických úvah. V současné době se při oceňování dat uplatňují různé názory, mající svůj původ v hlavních činnostech uživatelů informačních systémů. Budou se tedy lišit kritéria a priority při oceňování dat v bankovním systému od systémů státní správy a ty pak od systémů armádních atp.

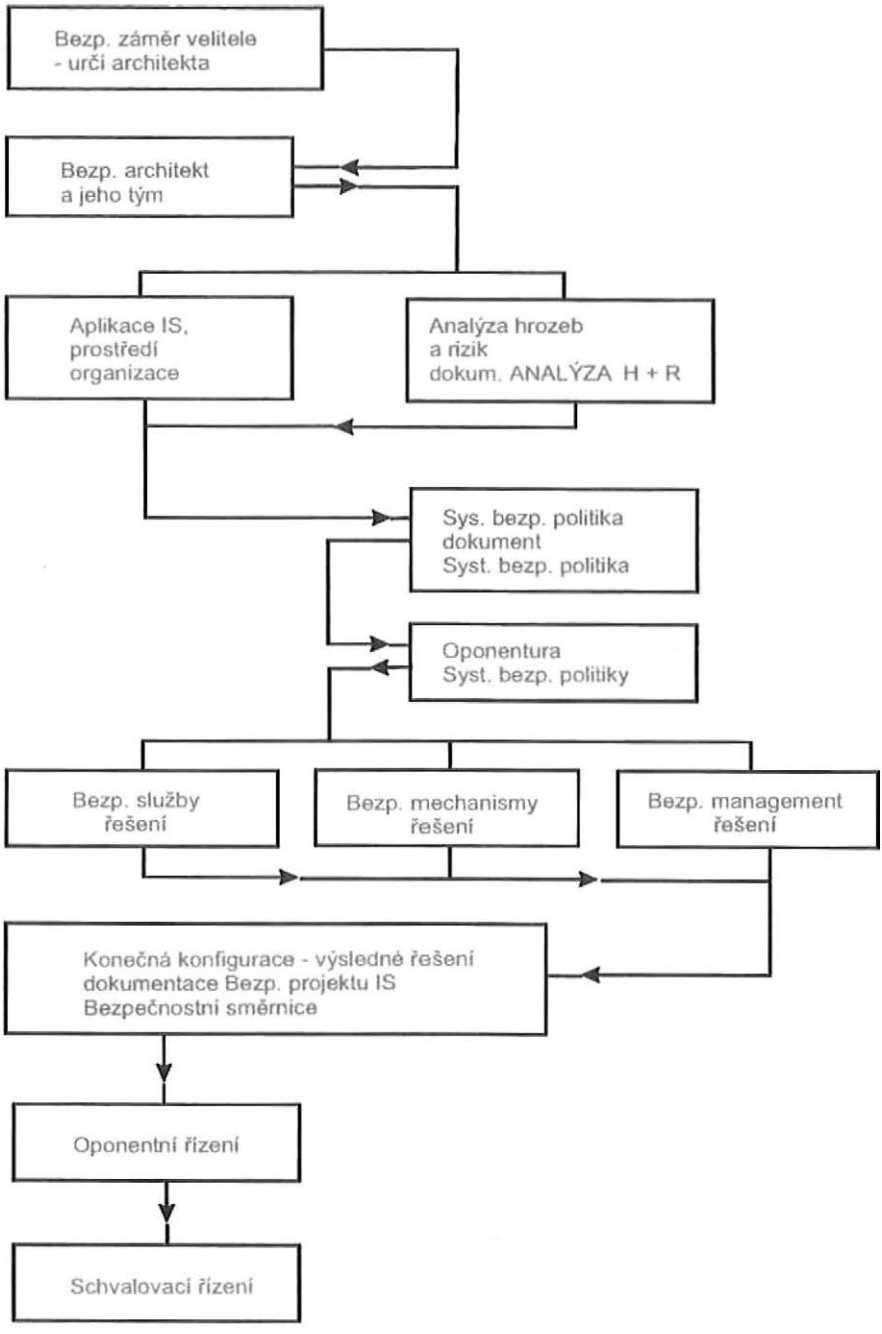
Možná sestava hodnotících atributů dat a jejich seřazení podle priorit, se zřetelem na vojenské informace systémy typu C^4I, může být následující:

1. Citlivost dat (vyjádřená většinou stupněm utajení).
2. Kritická dostupnost (data musí být dostupná v definovaných časových relacích, v řadě operací se tyto blíží práci v reálném čase).
3. Zničitelnost dat.
4. Obnovitelnost dat.
5. Množství (objem) dat.
6. Kvalita.

Za povšimnutí stojí, že uvedené uspořádání zdůrazňuje kromě citlivosti informací i jejich vysokou operabilitu a odolnost. Uvedený „žebříček priorit" se může v průběhu operací měnit, kdy se může dostat např. dostupnost i před citlivost a nastupuje pak nový doplňkový proces nepřetržitého oceňování rizik.

Vyspělé státy spolu s producenty informačních systémů vedla snaha po srovnatelnosti bezpečnostních vlastností jednotlivých produktů informační techniky ke sjednocení kritérií bezpečnostní analýzy, která nakonec vyústila do dvou obecně uznávaných dokumentů, a to:

TCSEC - *Trusted Computer System Evaluation Criteria* (Kritéria hodnocení bezpečnosti počítačových systémů; tzv. Oranžová kniha vydaná DoD USA),



Obr. 2: Postup projektování bezpečnosti informačního systému

ITSEC - *Information Technology Security Evaluation Criteria* (Kritéria hodnocení bezpečnosti informačních technologií, což představuje modernější evropskou verzi TCSEC).

Vedle klasického, ale i časově a finančně náročného, přístupu k analýze bezpečnosti podle výše uvedených dokumentů se stále větší míře uplatňují velmi efektivní metody analýzy, které jsou založeny na expertním principu (známé jsou systémy CRAMM, DEFENDER aj.), jejichž výklad však není předmětem tohoto článku.

Bezpečnost se projektuje

Postup projektování bezpečnosti informačního systému odpovídá vývojovému diagramu na **obr. 2.** Z diagramu je patrno, že bezpečnostní architekt, resp. jeho tým, vypracovává postupně systémovou bezpečnostní politiku, vlastní bezpečnostní projekt a bezpečnostní směrnice. Důležitými etapami jsou oponentní řízení, na jejichž základě je možno průběh prací účinně ovlivnit.

Jedním ze zásadních doporučení pro architekta je maximální využívání již dříve ověřených a certifikovaných produktů z množiny schválených základních typových mechanismů (ZTM) a až po vyčerpání této možnosti je možno se pouštět na cestu vlastního vývoje, konstrukcí a systémů. Rovněž je třeba si uvědomit, že při okamžité nedostupnosti kybernetických (technických) ochranných prostředků je vždy možno sáhnout po organizačních, administrativních personálních a fyzických protiopatřeních, která mohou namnoze pomoci účinně kompenzovat hrozby nebo alespoň snížit rizika ztrát.

Co říci závěrem?

Potřeba chránit informace se stala i informatizovaném světě obecnou nutností a nikdo se dnes o ní neodvažuje nahlas pochybovat. Zkušenosti z praxe však ukazují, že všude tam, kde bezpečnost vyžaduje více pozornosti, investičních prostředků, odpovědnosti a sebekázně uživatelů systémů, dochází k jejímu vědomému opomíjení, zvyšuje se nebezpečí kompromitace a zvyšují se i rizika ztrát.

Je nutno si uvědomit, že ochrana citlivých informací je jednou ze základních podmínek účinného rozhodovacího procesu státní administrativy. Pro armádu pak platí tato podmínka o to více.

Literatura:

[1] **TCSEC** - Trusted Computer System Evaluation Criteria. DoD USA.

[2] **ITSEC** - Information Technology' Security Evaluation Criteria. The commision of the European communities (90); český překlad vydalo MH ČR r. 1993.

[3] **Pužman, J.:** Datové sítě a služby. ČVUT, r. 1994, Praha.

[4] **Pekárek, O.:** Zásady projektování bezpečnosti ve vojenských informačních systémech, VA Brno, r. 1996.