Hodnocení a klasifikace bezpečnosti informačních systémů

Petr Hanáček

Motto: *„The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn't stake my life on it."*

Gene Spafford

Motivace

V průběhu několika posledních desetiletí začaly hrát informační technologie (IT) a jejich konkrétní realizace, informační systémy (IS) velmi důležitou, často rozhodující roli téměř ve všech oblastech lidské společnosti. Důsledkem tohoto prudkého rozvoje IT je i to, že důležitým aspektem IT se stává **bezpečnost** IT.

Vzhledem k širokému uplatnění IT i v netechnických oblastech společnosti nestačí pouze vytvořit bezpečný IS. Uživatel IS potřebuje **věřit**, že používaný IS je bezpečný. Uživatel také potřebuje **měřítko** pro porovnání bezpečnosti IS, který hodlá zakoupit. Ačkoli by se uživatel mohl spolehnout na slovní tvrzení tvůrců a prodejců IS nebo by si mohl bezpečnost IS otestovat sám, jistě dá přednost výsledku nestranného hodnocení nezávislého orgánu. Takovéto hodnocení IS však vyžaduje objektivní, dobře definovaná kritéria a certifikační orgány, které zaručí, že hodnocení bylo řádně provedeno. Z výše uvedených důvodů se objevily snahy zavést nějaká kritéria bezpečnosti IS, která by splňovala následující požadavky:

- Kritéria by měla poskytnout uživateli měřítko pro vyjádření stupně důvěry, kterou může uživatel vložit do IS, který chce použít pro zpracování důležitých informací.
- Kritéria by měla poskytnout výrobcům IS vodítko, které prvky bezpečnosti má zabudovat do vytvářeného IS, aby tento IS splňoval požadovaný stupeň bezpečnosti.
- Kritéria by měla poskytnout základ pro hodnocení stupně bezpečnosti IS certifikačním orgánem.

Následující část příspěvku by měla poskytnout čtenáři přehled o nejrozšířenějších a nejpoužívanějších kritériích bezpečnosti IS. Vzhledem k rozdílnému vývoji kritérií ve světě je příspěvek rozdělen na dvě části – první část se zabývá vývojem v USA a část druhá se zabývá vývojem v evropských zemích.

Standardy bezpečnosti IS v USA

USA začaly s vývojem kritérií bezpečnosti IS v roce 1967, kdy byla sestavena pracovní skupina pod vedením ministerstva obrany (Department of Defense, DoD), která měla za úkol vypracovat pravidla bezpečnosti pro víceuživatelské počítačové systémy se vzdáleným přístupem. Výsledkem práce této skupiny byla zpráva 5200.28M, kterou DoD publikovalo v roce 1972. Tento dokument specifikoval bezpečnostní politiku, bezpečnostní požadavky a administrativní a technická bezpečnostní opatření v podmínkách DoD.

V roce 1977 byla započata na DoD systematická práce na vytváření bezpečnostních kritérií a byla založena pracovní skupina pod názvem DoD Computer Security Initiative. Ta byla transformována v roce 1981 ve výzkumné středisko DoD Computer Security Center. Toto středisko v roce 1983 publikovalo patrně nejznámější standard pro bezpečnost IS, DoD 5200.28 STD, známý pod jménem TCSEC nebo Orange Book.

Trusted Computer System Evaluation Criteria (TCSEC)

Publikace TCSEC je jednou ze série publikací DoD týkajících se bezpečností IS. Tato série je nazývána „Rainbow Series" a skládá se asi z 25 publikací. Nejznámější z této série jsou následující tři publikace:

- „Orange Book", neboli Trusted Computer Systems Evaluation Criteria (TCSEC), která definuje požadavky bezpečnosti pro počítačové informační systémy
- „Grey Book", neboli Trusted Database Interpretation, která definuje standardy bezpečnosti pro databázové aplikace
- „Raspbery Book", neboli Trusted Network Interpretation, která definuje standardy bezpečnosti pro počítačové sítě

Nejdůležitější z těchto publikací je publikace TCSEC a proto se jí budeme věnovat trochu podrobněji. Tato publikace byla poprvé zveřejněna v roce 1983 a upravena v roce 1985. Stala se prvním obecně dostupným dokumentem, který popisuje obecné bezpečnostní požadavky, které lze aplikovat na konkrétní část informačního systému (např. na operační systém). Informační systémy jsou podle stupně své bezpečnosti rozděleny do čtyř tříd bezpečnosti A, B, C a D. Třída D znamená nejmenší míru bezpečnosti, třída A znamená míru největší. Stručně lze tyto čtyři třídy charakterizovat takto: Třída D obsahuje IS s minimálními nebo žádnými prvky bezpečnosti. Třída

C obsahuje IS s volitelnou (nepovinné) definicí přístupových práv (sem spadá většina současných IS). Třída B obsahuje IS s povinnou definicí přístupových práv a s klasifikací dat podle stupně ochrany dat. Konečně třída A obsahuje IS jejichž prvky bezpečnosti splňují vše, co je požadováno ve třídě B a je proveden formální důkaz správnosti těchto prvků.

Třídy bezpečnosti A, B a C se dělí dále na podtřídy, které jsou dále číslovány (A1, B1, B2, B3, C1 a C2). Při klasifikaci IS se jména tříd A až C neužívají – užívá se vždy jméno podtřídy. V následujících odstavcích budou všechny podtřídy TCSEC popsány detailněji.

Třída D: Minimální nebo žádná ochrana

V této třídě nejsou na IS kladeny žádné požadavky z hlediska bezpečnosti. Tato třída je vyhrazena pro IS, které jsou hodnoceny z hlediska bezpečnosti, ale které nemohou být zařazeny do některé vyšší třídy.

Třída C1: Volitelná bezpečnostní ochrana

IS ve třídě C1 musí umožňovat volitelnou ochranu dat a volitelnou definici přístupových práv. Musí poskytovat možnost izolace jednotlivých uživatelů a jejich dat. Uživatel musí mít možnost chránit svá data před jinými uživateli. Systém musí nabízet ochranu dat před neúmyslným poškozením a před mírnějším úmyslným útokem. Pokud IS pracuje s klasifikovanými daty, předpokládá se, že všichni uživatelé pracují s daty stejného stupně utajení.

Třída C2: Řízený systém přístupových práv

Ve třídě C2 se požaduje všechno, co ve třídě C1. Volitelná definice přístupových práv musí umožňovat jemnější přidělení práv. Vyžaduje se jednoznačná identifikace a autorizace každého uživatele. Systém musí umožnit protokolování událostí významných z hlediska bezpečnosti. Vyžaduje se rušení obsahu objektů při jejich znovupoužití.

Třída B1: Povinná bezpečnostní ochrana

Systémy v této třídě musí splňovat všechny požadavky třídy C2. Musí existovat alespoň neformální definice bezpečnostní politiky IS. Systém musí zajišťovat povinnou definici přístupových práv pro všechny pojmenované objekty a subjekty. Data musí být klasifikována z hlediska bezpečnosti. Všechny informace exportované ze systému musí být rovněž klasifikovány.

Třída B2: Strukturovaná ochrana

Systémy v této třídě musí splňovat všechny požadavky třídy B1. Musí existovat formální definice bezpečnostní politiky IS. Povinná definice přístupových práv je rozšířena na všechny subjekty a objekty v systému. Musí být provedena analýza skrytých kanálů. IS musí být strukturován na části, které jsou kritické z hlediska bezpečnosti a na části, které kritické nejsou. Je zesílen autentizační mechanismus. Je zaveden pojem důvěryhodné zařízení. IS musí odolat všem běžným úmyslným útokům.

Třída B3: Bezpečnostní domény

V této třídě musí autorizaci zprostředkovávat referenční monitor. Referenční monitor musí být odolný proti fyzickému útoku a musí být dostatečně malý, aby mohl být podroben analýze a testování. Je zajištěno oddělení zodpovědnosti administrátorů. Protokolovací mechanismus dovoluje on–line detekci nebezpečných stavů. Je zajištěno bezpečné zotavení systému po poruše nebo po útoku. Systém musí odolat i silnému úmyslnému útoku.

Třída A1: Verifikovaný návrh

Na systém v této třídě jsou kladeny stejné funkční požadavky jako na systém ve třídě B3. Třída A1 však požaduje, aby bylo formálně dokázáno, že funkční požadavky jsou splněny. Musí existovat formální model bezpečnostní politiky a návrh IS musí být prováděn pomocí formální specifikace shora dolů.

Komerční snahy o kritéria bezpečnosti IS

Po zavedení TCSEC se ukázalo, že tato kritéria sice jsou velmi hodnotným výchozím bodem pro zavádění standardizace bezpečnosti IS, ale že nejsou dostatečná pro komerční aplikace. Bylo to způsobeno hlavně místem jejich vzniku ve vojenském prostředí. Proto se některé komerční společnosti rozhodly vytvořit svá vlastní kritéria bezpečnosti IS. Nejúspěšnější v tomto směru byla firma Bellcore a firma American Express Travel Related Services (TRS).

Firma Bellcore vytvořila dokument s názvem Bellcore Standard Operating Environment Security Requirements. Tento dokument nebyl koncipován příliš obecně a vycházel z TCSEC, z obecně používaných zásad bezpečnosti IS a ze zkušeností bezpečnostního oddělení firmy Bellcore.

Firma TRS vytvořila jako svůj bezpečnostní standard dokument pod názvem C2–Plus. Při jeho návrhu došla k závěru, že standard TCSEC sice splňuje většinu požadavků potřebných v komerčním sektoru, ale pro jeho praktické prosazení je třeba provést několik úprav. Za hlavní nedostatek považovala to, že třída bezpečnosti C2 (jako třída, jejíž realizace byla momentálním cílem) neobsahuje některé rysy, které jsou buďto zavedeny

až ve třídách vyšších nebo nejsou v dokumentu TCSEC zachyceny vůbec. Dokument C2-Plus se vlastně zabýval pouze definicí rozšířených, komerčně zaměřených požadavků pro třídu C2. Dokument C2-Plus byl pouze firemním standardem firmy TRS, ale později se stal základem mezinárodního standardu Commercial International Security Requirements (CISR), který vytvořila organizace International Information Integrity Institute (I-4). Tento dokument byl publikován v roce 1992.

Minimum Security Functionality Requirements (MSFR)

Dokument MSFR byl vytvořen v lednu 1992 pracovní skupinou, která se zabývala také přípravou dokumentu FC (viz dále). Při vytváření dokumentu se předpokládalo, že hlavní myšlenky MSFR budou zabudovány po nezbytných úpravách i do dokumentu FC. Cílem zveřejnění těchto myšlenek v dokumentu MSFR bylo jednak umožnit dřívější používání těchto kritérií (vydání dokumentu FC bylo tehdy v nedohlednu) a jednak seznámit veřejnost se směrem vývoje připravovaného dokumentu FC a získat připomínky potenciálních uživatelů dokumentu FC.

Cílem pracovní skupiny MSFR bylo vytvořit třídu požadavků, která by nahradila třídu bezpečnosti C2 TCSEC. Tato nová třída je orientována směrem k IS, které nezpracovávají klasifikované druhy informace (na rozdíl od vojenských IS, které zpracovávají informace přísně klasifikované podle stupně utajení) ve státních a komerčních organizacích. Třída se také orientuje více na specifika IS postavených na bázi víceuživatelských operačních systémů. MSFR je na rozdíl od TCSEC C2 modernizován, poskytuje podrobnější a detailnější popis požadovaných bezpečnostních opatření a také podrobnější instrukce pro tvůrce IS. Je zajištěna i kompatibilita s jinými standardy. Informační systém, který vyhovuje MSFR, také splňuje třídu C2 kritérií TCSEC a třídu E2 evropských kritérií ITSEC (viz odstavec o ITSEC).

Federal Criteria for Information Technology Security (FC)

Kritéria bezpečnosti IS pod názvem FC jsou společným dílem organizací National Institute of Standards and Technology (NIST) a National Security Agency (NSA). Projekt FC není zatím zcela dokončen. V prosinci 1992 byla zveřejněna první draft verze dokumentu FC a definitivní verze dokumentu se neočekává dříve než za rok. Motivace pro vznik dokumentu FC byla dvojí. Prvním důvodem je potřeba nahradit dokument TCSEC, který v dnešní době už přestává vyhovovat. Druhým důvodem je snaha harmonizovat kritéria bezpečnosti IS v mezinárodním měřítku. Právě předložení draft verze dokumentu FC pro diskusi světové veřejnosti by mělo tuto harmonizaci usnadnit. Dokument FC se skládá ze dvou částí. První část definuje pojmy a stupnice kritérií pro jednotlivé funkce a cíle bezpečnosti IS. Jako příklad použití definovaných pojmů je uvedena definice sedmi tříd bezpečnosti T1 až T7 a korespondence těchto tříd s třídami TCSEC. Díl druhý obsahuje všeobecně přijaté bezpečnostní profily, které by měly uživateli pomoci nalézt produkt, který vyhovuje jeho bezpečnostním požadavkům.

Evropské standardy bezpečnosti IS

Z evropských standardů pro hodnocení bezpečnosti IS stojí za zmínku kritéria britská a německá. Britská kritéria bezpečnosti IS vyšla v roce 1989 pod názvem UK Systems Security Confidence Levels. Tato kritéria definují šest hodnotících tříd L1 až L6. Mimo to kritéria definují ještě tzv. **požadavkový jazyk**, pomocí něhož lze popsat bezpečnostní vlastnosti produktu pomocí poloformální notace. Tento požadavkový jazyk byl pak převzat evropskými kritérii ITSEC.

Německá kritéria bezpečnosti IS vyšla rovněž v roce 1989 pod názvem IT-Sicherheitskriterien: Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik. Kritéria definují osm tříd kvality Q0 až Q7 a deset tříd funkčnosti F1 až F10. Hodnocený produkt je pak označen dvojicí (**Třída funkčnosti, Třída kvality**). Mezi IT-Sicherheitskriterien a TCSEC existuje jednosměrná korespondence, to znamená, že každou třídu TCSEC je možno vyjádřit pomocí IT-Sicherheitskriterien ale nikoli naopak.

Britská a německá kritéria hodnocení bezpečnosti IS (spolu s kritérii francouzskými a nizozemskými) byla základem pro vytvoření společných evropských kritérií ITSEC. Těmto kritériím je věnován následující odstavec.

Information Technology Security Evaluation Criteria (ITSEC)

Kritéria pro hodnocení bezpečnosti IT ITSEC, ve slangu nazývaná „Superman Book" byla vytvořena v roce 1990. Tato kritéria byla vytvořena jako harmonizovaná verze národních kritérií přijatých ve Francii, Německu, Anglii 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.

V terminologii ITSEC je předmět nebo systém, který bude hodnocen, nazýván **hodnocený předmět**. Strana, která nabízí předmět hodnocení, je nazývána **sponzor**. Sponzor musí předložit k posouzení produkt nebo systém spolu se zdokumentovanou specifikací svého bezpečnostního cíle, potenciálních hrozeb a příslušných protiopatření a mechanismů. Hodnotitel má povinnost otestovat hodnocený předmět a porovnat výsledky s bezpečnostním cílem, specifikovaným sponzorem. Podle výsledků hodnocení pak hodnotitel vydá certifikát.

ITSEC specifikuje sedm tříd správnosti E0 až E6 a v příloze definuje dalších deset tříd funkčnosti F. Třídy správnosti vycházejí ze čtyř základních skupin kritérií: proces vývoje IS, prostředí vývoje IS, provozní dokumentace IS a provozní prostředí IS. Pět tříd funkčnosti F-C1, F-C2, F-B1, F-B2 a F-B3 odpovídají stejnojmenným třídám kritérií TCSEC. Zbylých pět tříd funkčnosti je orientováno aplikačně. Korespondence mezi třídami ITSEC A TCSEC vypadá následovně:

ITSEC		TCSEC
	E0	D
F–C1	E1	C1
F–C2	E2	C2
F–B1	E3	B1
F–B2	E4	B2
F–B3	E5	B3
F–B3	E6	A1

Na rozdíl od TCSEC, která vznikala pro vojenské prostředí a orientovala se zejména na důvěrnost informace je TCSEC koncipován mnohem obecněji a pokrývá částečně i požadavky integrity a dostupnosti informace. Oproti TCSEC definuje ITSEC navíc způsob dokumentace hodnoceného předmětu, způsob definování bezpečnostního cíle a způsob provádění hodnocení. ITSEC také definuje **požadavkový jazyk**, což je doporučená poloformální notace pro standardní zápis požadavků bezpečnosti IS.

Závěr

Kritéria a standardy pro hodnocení bezpečnosti IS jsou cenným nástrojem pro možnost charakterizovat objektivně IS jako bezpečný. Význam těchto standardů nespočívá jen v nastavení laťky výrobcům a prodejcům IS, ale také jako návod pro vývoj produktů IT s možnou diferenciací výroby. Standardy a kritéria také mohou sloužit na straně kupujících pro výběr výrobků a dávají kupujícímu možnost ověřit si prohlášení prodávajícího o bezpečnosti prodávaného výrobku cestou nezávislého ohodnocení.

V České republice zatím nejsou standardizována žádná kritéria bezpečnosti IS. Je však pravděpodobné, že u nás budou používána kritéria ITSEC nebo kritéria jim velmi podobná. V tomto roce se očekává, že bude vydán český překlad kritérií ITSEC pod záštitou Národního informačního střediska.

Literatura

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

[2] Bernstein, K., Fischer, S.:
Risk Analysis of „Trusted Computer Systems", in Computer Security and Information Integrity, Elsevier Science Publisher B.V (North–Holland) IFIP, 1991

[3] Information Technology Security Evaluation Criteria (ITSEC), Office for Official Publications of the European Communities, Luxembourg 1991, ISBN 92–826–3004–8 [4] DoD Trusted Computer System Evaluation Criteria, CSC–STD–011–83, Department of Defense Computer Security Center, Fort Meade, August 1983

[5] 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

[6] IT–Sicherheitskriterien: Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT), Zentralstelle für Sicherheit in der Informationstechnik, Bonn, ISBN 3–88784–192–1

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