Informačná bezpečnosť globálny pohľad

Prednáška č. 3

Agenda

- Ochrana národného digitálneho priestoru
- Prevencia
  - Legislatíva
  - Vytváranie bezpečnostného povedomia
  - Budovanie know-how (normy, štandardy, best-practices)
  - Zavádzanie bezpečných systémov (certifikované systémy)
- Efektívna reakcia na bezpečnostné incidenty
  - CERT a CSIRT
  - Riadenie informačnej bezpečnosti (zavádzanie systémov riadenia informačnej bezpečnosti ISMS)
- Trvalo udržateľná úroveň

Ako zorganizovať spoľahlivú ochranu národného digitálneho priestoru?

- Zmena chápania informačnej bezpečnosti
  - od zaistenia izolovaných systémov ku ochrane celého priestoru
  - Od striktných požiadaviek k dynamickým riešeniam
  - Nielen špecialisti, ale všetci
  - Primeranosť ochrany (aspoň baseline všade)
  - Údržba a postupné zvyšovanie úrovne
- Integrácia čiastkových riešení do ucelených koncepcií
- USA, Nemecko, Austrália, Japonsko, Fínsko, Česká republika, EÚ

Základné oblasti

- Koncepcie sú rôzne, ale v podstate sa sústreďujú na tri oblasti
  - Prevencia
  - Efektívna reakcia na bezpečnostné incidenty
  - Trvalo udržateľná úroveň

Prevencia

- Cieľ: zabrániť vzniku bezpečnostných incidentov v (národnom) digitálnom priestore
- Ako
  - Legislatíva
  - Vytváranie bezpečnostného povedomia
  - Budovanie know-how (normy, štandardy, best-practices)
  - Zavádzanie bezpečných systémov (certifikované systémy)
  - Riadenie informačnej bezpečnosti (zavádzanie systémov riadenia informačnej bezpečnosti ISMS)
  - CERT a CSIRT

Legislatíva

- Dva prístupy
  - Informačná bezpečnosť zakomponovaná v jednotlivých zákonoch
  - Špeciálne zákony
- Uplatňujú sa oba prístupy
- „Obyčajné“ zákony
  - Trestný zákon, Trestný poriadok, Občiansky zákonník, Obchodný zákonník, Telekomunikačný zákon, Zákon o poskytovaní zdravotnej starostlivosti, Zákon o archívnictve a i
- Špeciálne zákony
  - Ochrana utajovaných skutočností
  - Ochrana osobných údajov
  - Elektronický podpis
  - Elektronický obchod

Legislatíva - Nemecko

- Federal Data Protection Act of December 20, 1990 (Bundesdatenschutzgesetz-BGBl.I 1990 S.2954), amended by law of September 14, 1994 (BGBl. I S. 2325), law of December 16, 1997 (BGBl. I S. 2325) and December 17, 1997 (BGBl. I S. 2325), last amendment 14.01.2003
- Act on Digital Signature (Gesetz zur digitalen Signatur) Federal Law Gazette (Bundesgesetzblatt) 1997 I 1872
- Act on the Protection of Personal Data used in Teleservices (Gesetz über den Datenschutz bei Telediensten). The Act was adopted on 22 July 1997 and entered into force on 1 August 1997.
- Act for the Establishment of the BSI (dated 17 December 1990, Federal Law Gazette I p. 2834 et seq.)
- Penal Code (1871) last amended 24.03.2005 (Strafgesetzbuch-StGB)
- Code of Criminal Procedure (1950) last amended 22.03.2005 (Strafprozessordnung-StPO)
- Telecommunications Act (2004) last amended 14.03.2005 (Telekommunikations-gesetz-TKG)
- Teleservices Act (1997) last amended 14.12.2001 (Gesetz für die Nutzungvon Telediensten-TDG)
- Unfair Competition Act (2004) (Gesetz gegen den unlauteren Wettbewerb-UWG)
- Protection of Minors in the Media Treaty (2004) (Jugendmedienschutz-Staatsvertrag-JMStV)

Legislatíva – USA (1)

- (Vybrané zákony a prezidentské smernice týkajúce sa informačnej bezpečnosti)
- The National Security Act of 1947, Pub. L. No. 235, 80 Cong., 61 Stat. 496 (July 26, 1947)
- the National Security Council Intelligence Directive (NSCID) No. 9 on 24 October 1952, ktorou bola založená NSA on 4 November 1952.
- Privacy Act of 1974, Public Law 93-579 93rd Congress, Title 54 .S.C Sec. 552a U.S. Code -CITE- 5 USC Sec. 552a 01/16/96
- Computer Security Act of 1987 Public Law 100-235 (H.R. 145) January 8, 1988
  - NIST poverený vypracovaním štandardov pre minimálnu úroveň bezpečnosti
  - Vyžaduje bezpečnostné politiky pre systémy pracujúce s citlivou informáciou
  - Povinné školenia pracovníkov pracujúcich s týmito systémami

- http://en.wikipedia.org/wiki/Category:Computer_law

Legislatíva – USA (2)

- Presidential Decision Directive/NSC – 29 on Security Policy Coordination (1994)
- Paperwork Reduction Act of 1995
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001
- Homeland Security Act of 2002
- The E-Government Act of 2002. (H.R. 2458/S. 803)
- The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899).
- Cyber Security Research and Development Act of 2002. PUBLIC LAW 107–305—NOV. 27, 2002
- Help America Vote Act of 2002

Legislatíva – USA (3)

- Cyber Security Research and Development Act of 2002

  A Department of Defense Joint Task Force concluded after a 1997 United States information warfare exercise that the results ‘‘clearly demonstrated our lack of preparation for a coordinated cyber and physical attack on our critical military and civilian infrastructure’’.
- Computer security technology and systems implementation lack—

  (A) sufficient long term research funding;

  (B) adequate coordination across Federal and State government agencies and among government, academia, and industry; and

  (C) sufficient numbers of outstanding researchers in the field.

Legislatíva – USA (4)

- Federal investment in computer and network security research and development must be significantly increased to—

  (A) improve vulnerability assessment and technological and systems solutions;

  (B) expand and improve the pool of information security professionals, including researchers, in the United States workforce; and

  (C) better coordinate information sharing and collaboration among industry, government, and academic research projects.

- http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ305.107.pdf

Legislatíva EÚ (1)

- Najdôležitejšie dokumenty Európskej únie pre oblasť informačnej bezpečnosti sú
- Council Directive 1991/250/EEC on the legal protection of computer programmes.
- Directive 1995/46/EC on personal data protection.
- Directive 1997/66/EC on data protection in the telecommunications sector.
- Directive 1999/93/EC on community framework for electronic signatures.
- Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)
- Regulation 2001/45/EC on personal protection in personal data processing by authorities and institutions.
- Council Directive 2001/264/EC on the protection of classified information.

Legislatíva EÚ (2)

- Directive 2002/58/EC on privacy and electronic communications.
- Directive 2002/58/EC on the processing of personal data and privacy protection.
- Regulation (EC) No 460/2004 of the European parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency)
- Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
- Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions On Fighting spam, spyware and malicious software
- Communication From The Commission To The European Parliament, The Council, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime

	Regulation	Directive	Decision	Resolution	Recommendation or Communication	Framework Decision	Directive Proposal	Regulation Proposal
Network and Information Security	Yes		Yes	Yes	Yes			
Attacks against Information Systems			Yes	Yes	Yes	Yes		
Corporate Governance / IT Governance		Yes			Yes		Yes	
Data Authentication and Security	Yes	Yes						Yes
Data Protection and Data Retention		Yes			Yes			
Provision of Electronic Communications Networks and Services	Yes	Yes			Yes			
Intellectual Property rights and Protection of Technical Mechanisms designed to prevent copying and counterfeiting	Yes	Yes						
Security and financial Services		Yes			Yes		Yes	

Legislatíva EÚ (4)

- ENISA ad hoc working group on regulatory aspects of network and information security (RANIS) *Inventory and assessment of EU regulatory activity on network and information security* (NIS) December 2006
- Právne a regulatívne prostredie NIS (sieťová a informačná bezpečnosť) je charakterizované
  - neúplnými a zavádzajúcimi zákonmi a reguláciami, ktoré tvoria ovzdušie neistoty pre implementáciu celoeurópskej NIS,
  - hoci sú zákony a regulácie dobre mienené a sú v zhode s dlhodobou víziou elektronickej fakturácie (e-billing), zavádzajú neprimeranú záťaž pre výrobcov, podnikateľov a obchodníkov,
  - je príliš veľa (otvorených) otázok okolo interoperability, najmä cezhraničnej NIS, hoci štandardy NIS sú dostupné a nejaký čas sa používajú.
- http://www.enisa.europa.eu/Pages/ENISA_Working_group_RANIS.htm

Council Directive 1991/250/EEC on the legal protection of computer programs

- **Article 1 Object of protection** 1. In accordance with the provisions of this Directive, Member States shall protect computer programs, by copyright, as literary works within the meaning of the Berne Convention for the Protection of Literary and Artistic Works. For the purposes of this Directive, the term 'computer programs` shall include their preparatory design material.
- 2. Protection in accordance with this Directive shall apply to the expression in any form of a computer program. Ideas and principles which underlie any element of a computer program, including those which underlie its interfaces, are not protected by copyright under this Directive.
- 3. A computer program shall be protected if it is original in the sense that it is the author's own intellectual creation. No other criteria shall be applied to determine its eligibility for protection.
- **Article 7 Special measures of protection** 1. (c) any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program.

Legislatíva SR (1)

- Zákon č. 483/2001 Z.z. o bankách a o zmene a doplnení niektorých zákonov a naň naväzujúce
- Metodické usmernenie Úseku bankového dohľadu NBS č. 7/2004 k overeniu bezpečnosti informačného systému banky a pobočky zahraničnej banky
- Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
- Výnos Ministerstva dopravy, pôšt a telekomunikácií SR č. 1706/M-2006 o štandardoch pre informačné systémy verejnej správy (obsahujúci aj bezpečnostné štandardy)
- Zákon č. 618/2003 Z.z. o autorskom práve a o právach súvisiacich s autorským právom
- Zákon č. 610/2003 Z.z. o elektronických komunikáciách v znení neskorších predpisov
- Zákon č. 211/2000 Z.z. o slobodnom prístupe k informáciám v znení neskorších predpisov
- Zákon č. 22/2004 Z. z. o elektronickom obchode

Legislatíva SR (2)

- ústavný zákon č. 254/2006 Z.z. o zriadení a činnosti výboru Národnej rady Slovenskej republiky na preskúmavanie rozhodnutí Národného bezpečnostného úradu
- Nariadenie vlády č. 216/2004 Z.z. ktorým sa ustanovujú oblasti utajovaných skutočností
- Zákon 300/2005 Z.z, z 20. mája 2005,Trestný zákon
- Zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov.
- Zákon č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov Uplne_znenie_428_2002.pdf
- Zákon č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov
- Zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov

Trestný zákon

- Pozrieme sa na trestný zákon
- Dva typy zmien:
  - Rozšírenie „tradičných“ trestných činov aj na oblasť digitálneho priestoru (počítače ako nástroj na páchanie tradičnej trestnej činnosti, ako je falšovanie dokumentov, peňazí a pod.)
  - Nová počítačová kriminalita (prieniky do systémov, odpočúvanie, elektromagnetické vyžarovanie)
- Odporúčam si pozrieť aj iné zákony, minimálne zákony o ochrane utajovaných skutočností, elektronickom podpise, ochrane osobných údajov a informačných systémoch verejnej správy.

Trestný zákon

§ 196
Porušovanie tajomstva prepravovaných správ

(1) Kto úmyselne poruší

a) listové tajomstvo vyzvedaním alebo otvorením uzavretého listu alebo inej písomnosti prepravovanej poštovým podnikom alebo iným obvyklým spôsobom,

b) tajomstvo informácie prenášanej prostredníctvom elektronickej komunikačnej služby, alebo

c) tajomstvo neverejného prenosu počítačových dát do počítačového systému, z neho alebo v jeho rámci, vrátane elektromagnetického vyžarovania z počítačového systému, prenášajúceho takéto počítačové dáta,

potrestá sa odňatím slobody až na tri roky.

Trestný zákon

§ 219
Neoprávnené vyrobenie a používanie elektronického platobného prostriedku a inej platobnej karty

(1) Kto neoprávnene vyrobí, pozmení, napodobní, falšuje alebo si obstará elektronický platobný prostriedok alebo inú platobnú kartu vrátane telefónnej karty alebo predmet spôsobilý plniť takú funkciu na účel použiť ho ako pravý alebo na taký účel ho prechováva, prepravuje, použije alebo poskytne inému, potrestá sa odňatím slobody na jeden rok až päť rokov.

(2) Kto neoprávnene vyrobí, prechováva, obstará si alebo inak zadováži alebo poskytne inému nástroj, počítačový program alebo iný prostriedok špeciálne prispôsobený na spáchanie činu uvedeného v odseku 1, potrestá sa odňatím slobody až na tri roky.

Trestný zákon

§ 226
Neoprávnené obohatenie

(1) Kto na škodu cudzieho majetku seba alebo iného obohatí tým, že neoprávneným zásahom do technického alebo programového vybavenia počítača, automatu alebo iného podobného prístroja alebo technického zariadenia slúžiaceho na automatizované uskutočňovanie predaja tovaru, zmenu alebo výber peňazí alebo na poskytovanie platených výkonov, služieb, informácií či iných plnení dosiahne, že tovar, služby alebo informácie získa bez požadovanej úhrady alebo peniaze získa neoprávnene, a spôsobí tým na cudzom majetku malú škodu, potrestá sa odňatím slobody až na dva roky.

Trestný zákon

§ 247
Poškodenie a zneužitie záznamu na nosiči informácií

(1) Kto v úmysle spôsobiť inému škodu alebo inú ujmu alebo zadovážiť sebe alebo inému neoprávnený prospech získa neoprávnený prístup do počítačového systému, k inému nosiču informácií alebo jeho časti a

a) jeho informácie neoprávnene použije,

b) také informácie neoprávnene zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu,

c) urobí zásah do technického alebo programového vybavenia počítača, alebo

d) vkladaním, prenášaním, poškodením, vymazaním, znížením kvality, pozmenením alebo potlačením počítačových dát marí funkčnosť počítačového systému alebo vytvára neautentické dáta s úmyslom, aby sa považovali za autentické alebo aby sa s nimi takto na právne účely nakladalo,potrestá sa odňatím slobody na šesť mesiacov až tri roky.

Trestný zákon

§ 283
Porušovanie autorského práva

(1) Kto neoprávnene zasiahne do zákonom chránených práv k dielu, umeleckému výkonu, zvukovému záznamu alebo zvukovo-obrazovému záznamu, rozhlasovému vysielaniu alebo televíznemu vysielaniu alebo databáze, potrestá sa odňatím slobody až na dva roky.

(2) Odňatím slobody na šesť mesiacov až tri roky sa páchateľ potrestá, ak spácha čin uvedený v odseku 1

a) a spôsobí ním väčšiu škodu,

b) závažnejším spôsobom konania,

c) z osobitného motívu, alebo

d) prostredníctvom počítačového systému.

Trestný zákon

§ 283
Porušovanie autorského práva

(3) Rovnako ako v odseku 1 sa potrestá, kto na účel spáchania činu uvedeného v odseku 1

a) neoprávnene sleduje prostredníctvom technických prostriedkov neverejný prenos počítačových dát do počítačového systému, z neho alebo v rámci počítačového systému, alebo

b) zaobstará alebo sprístupní počítačový program a iné zariadenia alebo počítačové heslo, prístupový kód alebo podobné údaje umožňujúce prístup do celého počítačového systému alebo do jeho časti.

(4) Odňatím slobody na jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 alebo 2 a spôsobí ním značnú škodu.

(5) Odňatím slobody na tri roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 alebo 2

a) a spôsobí ním škodu veľkého rozsahu, alebo

b) ako člen nebezpečného zoskupenia.

Trestný zákon

§ 376

Kto neoprávnene poruší tajomstvo listiny alebo inej písomnosti, zvukového záznamu, obrazového záznamu alebo iného záznamu, počítačových dát alebo iného dokumentu uchovávaného v súkromí iného tým, že ich zverejní alebo sprístupní tretej osobe alebo iným spôsobom použije a inému tým spôsobí vážnu ujmu na právach, potrestá sa odňatím slobody až na dva roky.

Legislatíva SR (3)

- Vyhlášky NBÚ upravujúce ochranu utajovaných skutočností
- Vyhláška NBÚ č. 314/2006 Z. z. z 23., ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 337/2004 Z. z., ktorou sa upravujú podrobnosti o certifikácii mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov a o ich používaní
- Vyhláška NBÚ č. 315/2006 Z. z., ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti
- Vyhláška NBÚ č. 325/2004 Z. z. o priemyselnej bezpečnosti
- Vyhláška NBÚ č. 331/2004 Z. z. o personálnej bezpečnosti a o skúške bezpečnostného zamestnanca
- Vyhláška NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti
- Vyhláška NBÚ č. 337/2004 Z. z., ktorou sa upravujú podrobnosti o certifikácii mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov a o ich používaní
- Vyhláška NBÚ č. 338/2004 Z. z. o administratívnej bezpečnosti
- Vyhláška NBÚ č. 339/2004 Z. z. o bezpečnosti technických prostriedkov
- Vvyhláška NBÚ č. 340/2004 Z. z., ktorou sa ustanovujú podrobnosti o šifrovej ochrane informácií

Vytváranie bezpečnostného povedomia

- Legislatíva tvorí rámec, potrebujeme aj vedieť ako napĺňať definované požiadavky
- Vzdelávanie v školách
- Školenia používateľov IKT (v organizáciách, ktoré majú implementovaný systém riadenia informačnej bezpečnosti)
- Masovokomunikačné prostriedky (osveta a propaganda)
- zavedenie programov zvyšovania bezpečnostného povedomia a kompetentnosti používateľov IKT so zvláštnymi nárokmi na informačnú bezpečnosť

Budovanie know-how

- individuálne (vzdelávanie)
- Využívanie cudzieho know-how
- OECD zásady
- Best practices
- Normy
- Štandardy
  - Oficiálne (národné a medzinárodné) (de iure)
  - Neoficiálne (de facto)

OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS

- **Awareness** Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.
- **Responsibility** All participants are responsible for the security of information systems and networks.
- **Response** Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.
- **Ethics** Participants should respect the legitimate interests of others.
- **Democracy** The security of information systems and networks should be compatible with essential values of a democratic society.
- **Risk assessment** Participants should conduct risk assessments.
- **Security design and implementation** Participants should incorporate security as an essential element of information systems and networks.
- **Security management** Participants should adopt a comprehensive approach to security management.
- **Reassessment** Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies,practices, measures and procedures.

Best practices

- Information Security Forum • Standard of Good Practice 2007
  - Security Management (enterprise-wide)
  - Critical Business Applications
  - Computer Installations
  - Networks
  - Systems Development
  - End User Environment

https://www.isfsecuritystandard.com/SOGP07/index.htm

Metodické materiály NIST

- A Guide to NIST Information Security Documents http://csrc.nist.gov/publications/CSD_DocsGuide.pdf
- http://csrc.nist.gov/publications/CSD_DocsGuide_Trifold.p

Metodiky BSI

- http://www.bsi.de/english/publications/bsi_standards/index
- **BSI-Standard 100-2: IT-Grundschutz Methodology**

Normy a štandardy

- Veľa štandardizačných organizácií
  - ISO,IEC, CEN, CENELEC, ETSI, NIST, BSI, DIN,...
  - Súkromné spoločnosti RSA Labs - PKCS
  - Profesné združenia IETF – RFC
  - Ad hoc iniciatívy (EESSI, UNCITRAL)

ISO/IEC

- **ISO/IEC JTC 1/SC 27: IT Security techniques**
- JTC 1/SC 27/WG 1 Information security management systems
  The convener can be reached through: BSI
- JTC 1/SC 27/WG 2 Cryptography and security mechanisms
  The convener can be reached through: JISC
- JTC 1/SC 27/WG 3 Security evaluation criteria
  The convener can be reached through: SIS
- JTC 1/SC 27/WG 4 Security controls and services
  The convener can be reached through: SPRING SG
- JTC 1/SC 27/WG 5 Identity management and privacy technologies
  The convener can be reached through: DIN

- http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm

Aktuálny zoznam bezpečnostných noriem ISO

- TK37_SK27_Standards.xls

Vybrané ISO štandardy

- Bezpečnostných ISO štandardov je veľa, pozri

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306

- Ktoré sú základné?
- Manažment informačnej bezpečnosti
- **ISO/IEC 27001:2005**
  Information technology -- Security techniques -- Information security management systems – Requirements
- **ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management**
- Hodnotenie bezpečnosti systémov
- **ISO/IEC 15408:2005**
  Information technology -- Security techniques -- Evaluation criteria for IT security

ISO/IEC 27001:2005 Information security management systems Requirements

ISO/IEC 27001:2005 covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations).

ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

ISO/IEC 27002:2005 Code of practice for information security management

- ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains best practices of control objectives and controls in the following areas of information security management:
- security policy;
- organization of information security;
- asset management;
- human resources security;
- physical and environmental security;
- communications and operations management;
- access control;
- information systems acquisition, development and maintenance;
- information security incident management;
- business continuity management;
- compliance.
- The control objectives and controls in ISO/IEC 27002:2005 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 27002:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.

ISO/IEC 15408-1:2005 Common Criteria

- ISO/IEC 15408-1:2005
  Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
- ISO/IEC FCD 15408-2 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements
- ISO/IEC 15408-3:2005 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements
- ISO/IEC CD TR 15446 Information technology -- Security techniques -- Guide for the production of Protection Profiles and Security Targets

Budovanie bezpečných systémov

- Bezpečnostná konfekcia (opakované riešenia)
- Certifikované komponenty
- Štandardné riešenia
- Zmysel – nie je potrebných toľko kvalifikovaných ľudí a dosiahne sa potrebná bezpečnostná úroveň vo väčšom rozsahu
- Viacero riešení (BSI, NIST)
- Pozrieme sa na Common Criteria

Efektívna odpoveď na riešenie bezpečnostných incidentov

- Bezpečnostný incident = udalosť narušujúca zásady bezpečnostnej politiky organizácie
- Preventívne opatrenia mali za cieľ zabrániť vzniku bezpečnostných incidentov, ale nemohli ich vylúčiť
- Ďalšia línia ochrany – efektívne riešenie bezpečnostných incidentov
- Ciele : minimalizovať dopad, urýchlene dosiahnuť návrat do normálneho stavu, zaistiť stopy, vyvodiť dôsledky
- Viaceré zo spomenutých úloh spadali tak do prevencie ako aj do riešenia bezpečnostných incidentov

CERT a CSIRT - história

- Morrisov červ 1988
- Stretnutie expertov – záver vytvoriť jeden kontaktný bod, v ktorom by sa sústreďovali informácie o bezpečnostných incidentoch
- krátko na to vznikol prvý CERT® (Computer Emergency Response Team), ktorého úlohou bolo poskytovať pomoc pri riešení bezpečnostných incidentov (na Internete).
- v Európe zaužíval širší pojem CSIRT (Computer Security and Incident Response Team)
- 1990 založená medzinárodná organizácia FIRST (Forum of Incident Response and Security Teams) združujúca v súčasnosti viac než 180 CSIRT a CERT tímov z celého sveta.
- Európa TF-CSIRT

Poslanie a úlohy CSIRT

- Analógia – hasičská stanica
- Pre verejnosť, alebo vybranú skupinu používateľov
- Úlohy
  - Riešenie akútnych problémov
  - Cvičenia, metodiky, školenia, posudzovanie úrovne ochrany konkrétnych systémov
  - Monitorovanie a varovné signály
  - Legislatíva a štandardy
  - Zaisťovanie stôp
  - Spolupráca s vyšetrovateľmi a políciou
  - Medzinárodná spolupráca

Základný rámec CSIRT

Základný rámec CSIRT-u sa dá neformálne vyjadriť odpoveďami na nasledujúce otázky

- čo bude CSIRT robiť (reaktívne, proaktívne služby)
- pre koho,
- v akom lokálnom prostredí.
- s kým bude spolupracovať ?

- *CERTS in Europe* v1.4 © European Network and Information Security Agency (ENISA), 2006 cert_inventory_v1_4.pdf
- Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, Mark Zajicek, *Handbook for Computer Security Incident Response Teams (CSIRTs)* First release: December 1998 2nd Edition: April 2003

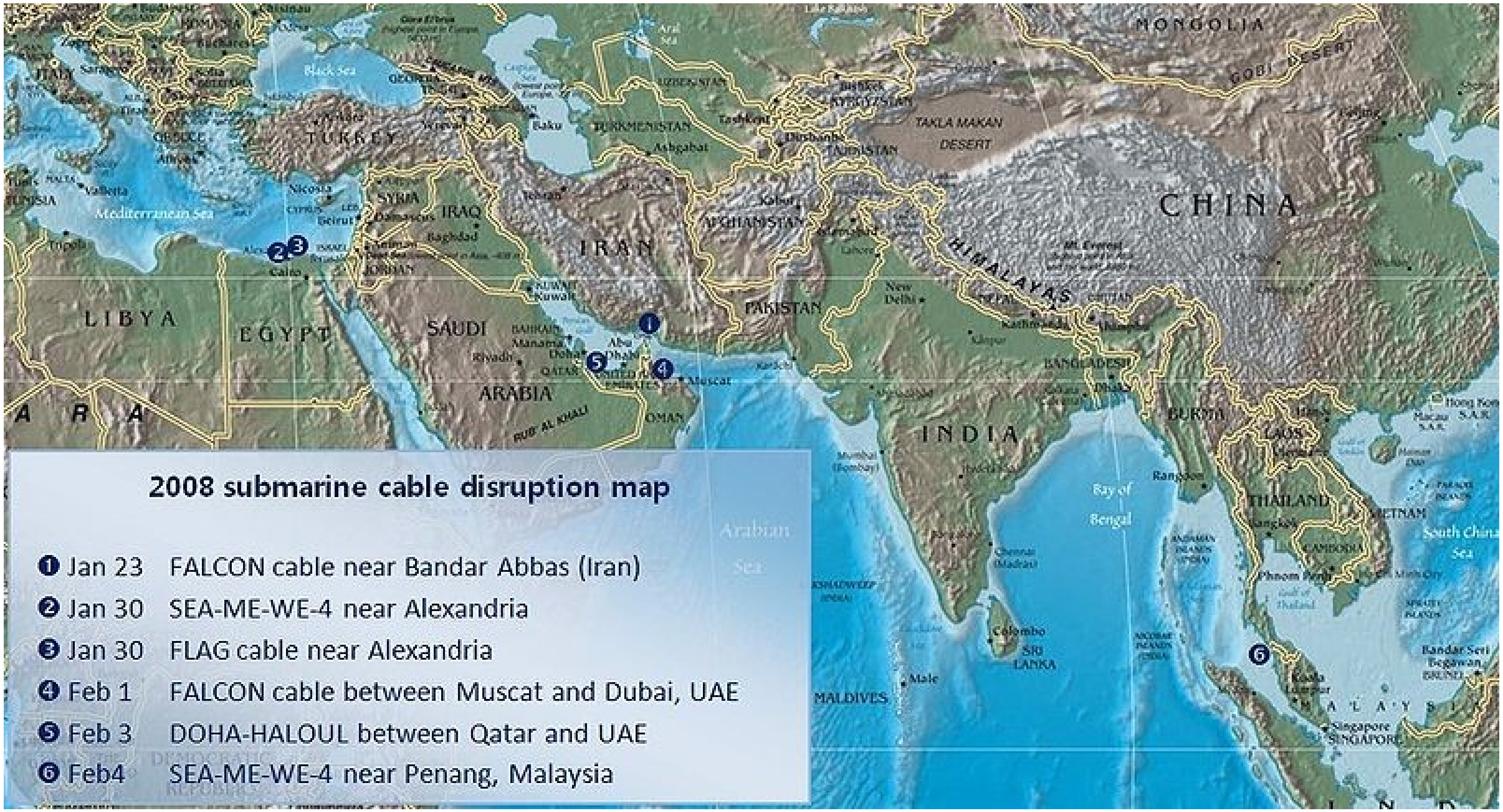
Systémy riadenia informačnej bezpečnosti

- Komplexnejšie (pozri ISO/IEC 27001) – budeme sa ním zaoberať neskôr
- Súčasťou je aj riešenie bezpečnostných incidentov
- Špeciálne
  - Business continuity planning
  - Disaster recovery

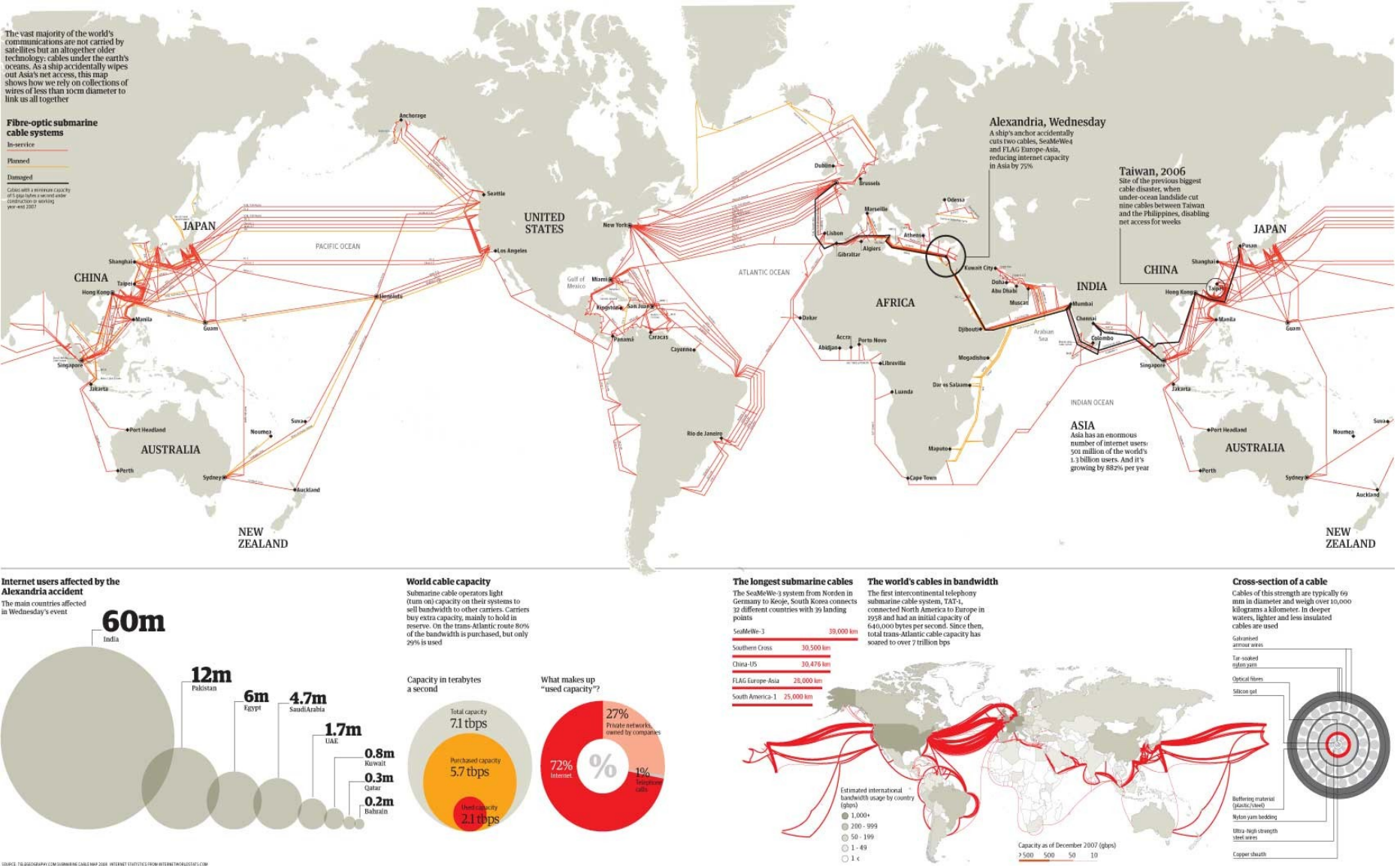
Kritická infraštruktúra

- IKT sú súčasťou kritickej infraštruktúry spoločnosti

  Revolutionary advancements in computing and communications technology have interconnected government, commercial, scientific, and educational infrastructures—including critical infrastructures for electric power, natural gas and petroleum production and distribution, telecommunications, transportation, water supply, banking and finance, and emergency and government services—in a vast, interdependent physical and electronic network.
- Terč potenciálnych útokov (posledný príklad – prerušenie podmorských káblov na Blízkom východe)
- http://en.wikipedia.org/wiki/2008_submarine_cable_disruption
- http://image.guardian.co.uk/sys-images/Technology/Pix/pictures/2008/02/01/SeaCableHi.jpg


2008 submarine cable disruption map
❶ Jan 23 FALCON cable near Bandar Abbas (Iran)
❷ Jan 30 SEA-ME-WE-4 near Alexandria
❸ Jan 30 FLAG cable near Alexandria
❹ Feb 1 FALCON cable between Muscat and Dubai, UAE
❺ Feb 3 DOHA-HALOUL between Qatar and UAE
❻ Feb4 SEA-ME-WE-4 near Penang, Malaysia
MONGOLIA
CHINA
IRAN
INDIA
PAKISTAN
LIBYA
EGYPT
SAUDI
ARABIA
TURKEY
IRAQ
SYRIA
HIMALAYAS
Mediterranean Sea
Black Sea
Bay of Bengal
Arabian Sea
THAILAND
MALDIVES

The internet's undersea world



Internet users affected by the Alexandria accident

The main countries affected in Wednesday's event

World cable capacity

Submarine cable operators light (turn on) capacity on their systems to sell bandwidth to other carriers. Carriers buy extra capacity, mainly to hold in reserve. On the trans-Atlantic route 80% of the bandwidth is purchased, but only 29% is used

Capacity in terabytes a second

What makes up "used capacity"?

The longest submarine cables

The SeaMeWe-3 system from Norden in Germany to Keoje, South Korea connects 32 different countries with 39 landing points

SeaMeWe-3	39,000 km
Southern Cross	30,500 km
China-US	30,476 km
FLAG Europe-Asia	28,000 km
South America-1	25,000 km

The world's cables in bandwidth

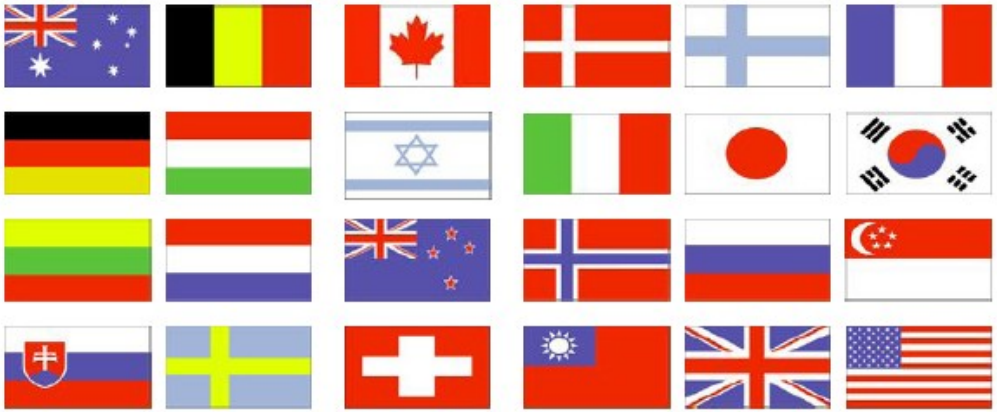
The first intercontinental telephony submarine cable system, TAT-1, connected North America to Europe in 1958 and had an initial capacity of 640,000 bytes per second. Since then, total trans-Atlantic cable capacity has soared to over 7 trillion bps

Cross-section of a cable

Cables of this strength are typically 69 mm in diameter and weigh over 10,000 kilograms a kilometer. In deeper waters, lighter and less insulated cables are used

GREEN

FOR GOVERNMENT USE ONLY



INTERNATIONAL CIIP DIRECTORY

Top ten security guidelines

1. assess the risks to your business
2. consider security first when planning building works
3. establish a security culture in your business
4. keep premises clear and tidy
5. control access points and use staff and visitor passes
6. install physical measures e.g. locks, alarms, CCTV, lighting etc
7. establish good mail handling procedures
8. recruit carefully, checking identities and following up references
9. take proper IT security precautions
10. test your business continuity plans regularly

http://www.cpni.gov.uk/About/topTen.aspx

Príklad: Bomb threat checklist

Bomb threat checklist

This checklist is designed to help staff to deal with a telephoned bomb threat effectively and to record the necessary information.

Photocopy this form or visit **www.mi5.gov.uk** to download the pdf and print it out.

Actions to be taken on receipt of a bomb threat:

- Switch on recorder/voicemail (if connected)
- Tell the caller which town/district you are answering from
- Record the exact wording of the threat:

_____

_____

_____

Ask the following questions:

- Where is the bomb right now? _____
- When is it going to explode? _____
- What does it look like? _____
- What kind of bomb is it? _____
- What will cause it to explode? _____
- Did you place the bomb? _____
- Why? _____
- What is your name? _____
- What is your address? _____
- What is your telephone number? _____

Record time call completed:

- Where automatic number reveal equipment is available, record number shown: _____
- Inform the Security Co-ordinator of name and telephone number of the person informed: _____
- Contact the police on 999. Time informed: _____

The following part should be completed once the caller has hung up and the Security Co-ordinator and the police have been informed.

- Time and date of call: _____
- Length of call: _____
- Number at which the call was received (i.e. your extension number): _____

About the caller

- Sex of caller: _____ Age: _____
- Nationality: _____

✓ Tick where appropriate

Language

- ☐ Well spoken
- ☐ Irrational
- ☐ Taped message
- ☐ Offensive
- ☐ Incoherent
- ☐ Message read by threat-maker

Caller's voice

- ☐ Calm
- ☐ Crying
- ☐ Clearing throat
- ☐ Angry
- ☐ Nasal
- ☐ Slurred
- ☐ Excited
- ☐ Stutter
- ☐ Disguised
- ☐ Slow
- ☐ Lisp
- ☐ Accent

Type of accent

_____

- ☐ Rapid
- ☐ Deep
- ☐ Hoarse
- ☐ Laughter
- ☐ Familiar

If so, whose voice did it sound like?

_____

_____

Background sounds

- ☐ Street noises
- ☐ House noises
- ☐ Animal noises
- ☐ Crockery
- ☐ Motor
- ☐ Clear
- ☐ Voice
- ☐ Static
- ☐ PA system
- ☐ Booth
- ☐ Music
- ☐ Factory machinery
- ☐ Office machinery
- ☐ Other (specify)

_____

_____

_____

Other remarks

_____

_____

_____

_____

_____

_____

_____

Signature: _____

Date: _____

Print name: _____

Trvale udržateľná úroveň

- Vzdelávanie
  - Používatelia
  - Informatici nešpecialisti
  - Špecialisti na InfoSec
  - Neinformatici InfoSec (právnici)
  - Výskumníci v InfoSec
- Výskum
- Medzinárodná spolupráca

Slovensko

- SR musí v oblasti informačnej bezpečnosti riešiť tie isté alebo podobné problémy, ako informačne najvyspelejšie krajiny, s výnimkou toho, že slovenská NIKI nie je pre medzinárodný terorizmus zatiaľ natoľko zaujímavá, ako IKI iných krajín,
- Na zaistenie svojej informačnej bezpečnosti má SR podstatne menšie zdroje ako informačne vyspelé krajiny
- Štát sa sústredil na zaistenie informačnej bezpečnosti vo vybraných oblastiach (utajované skutočnosti a osobné údaje); v ostatných oblastiach (informačnej bezpečnosti) sú aktivity štátu nedostatočné
- pripravujú sa rozsiahle (štátne) IKT projekty (e-Government, e-Health a i.) pri riešení ktorých treba zohľadňovať informačnú bezpečnosť už od fázy návrhu,

Čo chýba

- koncepcia informačnej bezpečnosti,
- legislatíva, normy a štandardy informačnej bezpečnosti,
- explicitné rozdelenie kompetencií za informačnú bezpečnosť,
- koordinácia rozličných aktivít v štátnej a súkromnej sfére,
- organizačné zabezpečenie informačnej bezpečnosti na úrovni štátu,
- odborné kapacity (know-how a ľudia),
- vlastný výskum v oblasti informačnej bezpečnosti,
- systematické budovanie bezpečnostného povedomia,
- medzinárodná spolupráca.

Perspektíva

- Vláda koncom augusta 2008 schválila Národnú stratégiu, ktorá by mala vytvoriť základný rámec
- rozumné využitie existujúcich zdrojov, využitie medzinárodnej spolupráce, spolupráca štát-súkromný sektor-akademické inštitúcie-IT firmy a občania môže priniesť výrazné zlepšenie.
- Aktuálne projekty
  - Návrh systému vzdelávania v informačnej bezpečnosti
  - Posudzovanie stavu informačnej bezpečnosti – metodika
  - Analýza štandardizačnej činnosti
  - CSIRT.SK

Bezpečnostné normy a štandardy

Prednáška č. 4

Hodnotenie bezpečnosti systémov

- Trocha histórie (USA)
- DoD projekt na zabezpečenie svojich počítačov už v roku 1977
- NIST (Brooks Act, 1965) stal inštitúciou zodpovednou za návrh a vývoj federálnych noriem stanovujúcich podmienky pre výber a používanie výpočtovej techniky
- Dve oblasti
  - návrh noriem pre počítačovú kryptografiu a
  - noriem pre vytváranie a hodnotenie zabezpečených počítačových systémov
- V r 1981 bola NSA poverená zaistením všetkých systémov v pôsobnosti Ministerstva obrany USA a vzniklo Computer Security Center, ktoré sa neskôr (1985) zmenilo na National Computer Security Center (NCSC), zabezpečujúce počítačové systémy federálnej vlády

The Brooks Act

Public Law 89-306 (Brooks Act), dated October 30, 1965
Public Law 89-306 89th Congress, H.R.4845
October 30, 1965
An Act 79 STAT. 1127

To provide for the economic and efficient purchase, lease, maintenance, operation, and utilization of automatic data processing equipment by Federal departments and agencies.

Hodnotenie bezpečnosti systémov 2

- CSC vypracovalo dokument Trusted Computer System Evaluation Criteria, známu ako Orange Book,
- Neskôr rainbow series
- V roku 1987 bol prijatý Computer Security Act, ktorým boli redukované právomoci NCSC na oblasť národných

  (klasifikovaných) systémov.
- Ostatné systémy NIST
- Koordinácia s NSA
- Federal Information Security Management Act (FISMA) v roku 2002

Národné a medzinárodné kritériá

- [TCSEC] Trusted Computer Systems Evaluation Criteria, US DoD 5200.28-STD, December 1985.
- Ďalšie národné kritériá (Kanadské) [CTCPEC] Canadian Trusted Computer Product Evaluation Criteria, Version 3.0, Canadian System Security Centre, Communications Security Establishment, Government of Canada, January 1993.
- [FC] Federal Criteria for Information Technology Security, Draft Version 1.0, (Volumes I and II), jointly published by the National Institute of Standards and Technology and the National Security Agency, US Government, January 1993.
- [ITSEC] Information Technology Security Evaluation Criteria, Version 1.2, Office for Official Publications of the European Communities, June 1991.

Common Criteria

- **Tvorcovia**
- *Canada: Communications Security Establishment*
- *- France: Service Central de la Sécurité des Systèmes d'Information*
- *- Germany: Bundesamt für Sicherheit in der Informationstechnik*
- *- Netherlands: Netherlands National Communications Security Agency*
- *- United Kingdom: Communications-Electronics Security Group*
- *- United States: National Institute of Standards and Technology*
- *- United States: National Security Agency*

Štruktúra

- Part 1: Introduction and General Model
- Part 2: Security Functional Requirements
- Part 3: Security Assurance Requirements

Cieľové skupiny CC

- **Používatelia**
  - Consumers can use the results of evaluations to help decide whether an evaluated product or system fulfils their security needs
  - Špecifikácia požiadaviek používateľov v podpobe PP
- **Vývojári**
  - The CC is intended to support developers in preparing for and assisting in the evaluation of their products or systems and in identifying security requirements to be satisfied by each of their products or systems.
- **Posudzovatelia**
  - The CC contains criteria to be used by evaluators when forming judgements about the conformance of TOEs to their security requirements.

Ako vyzerá evaluácia podľa CC?

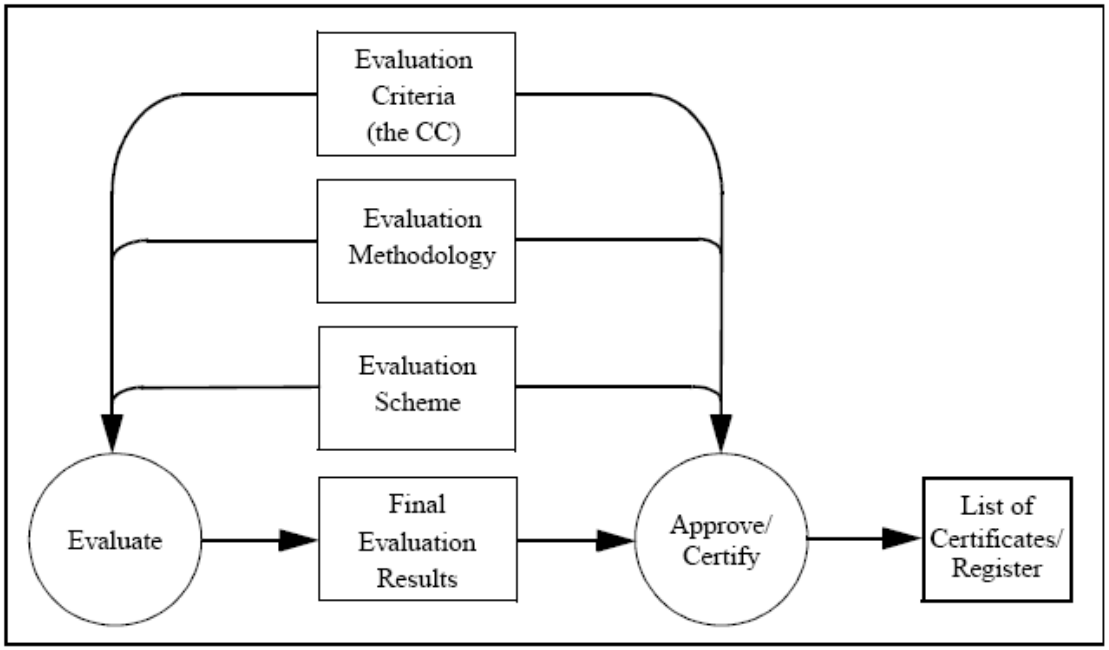


Figure 3.1 - Evaluation context

Vzťahy medzi základnými bezpečnostnými konceptami podľa CC

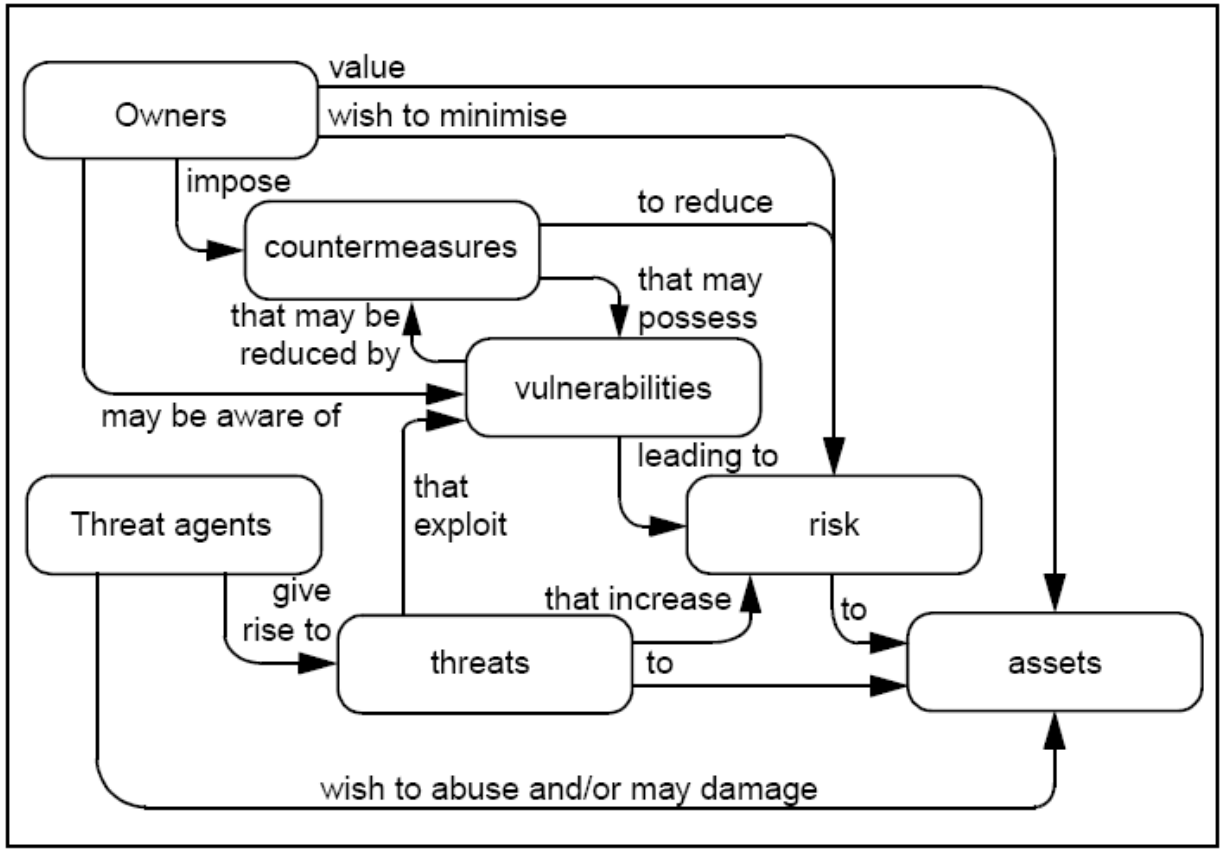


Figure 4.1 - Security concepts and relationships

Základné pojmy evaluácie systémov

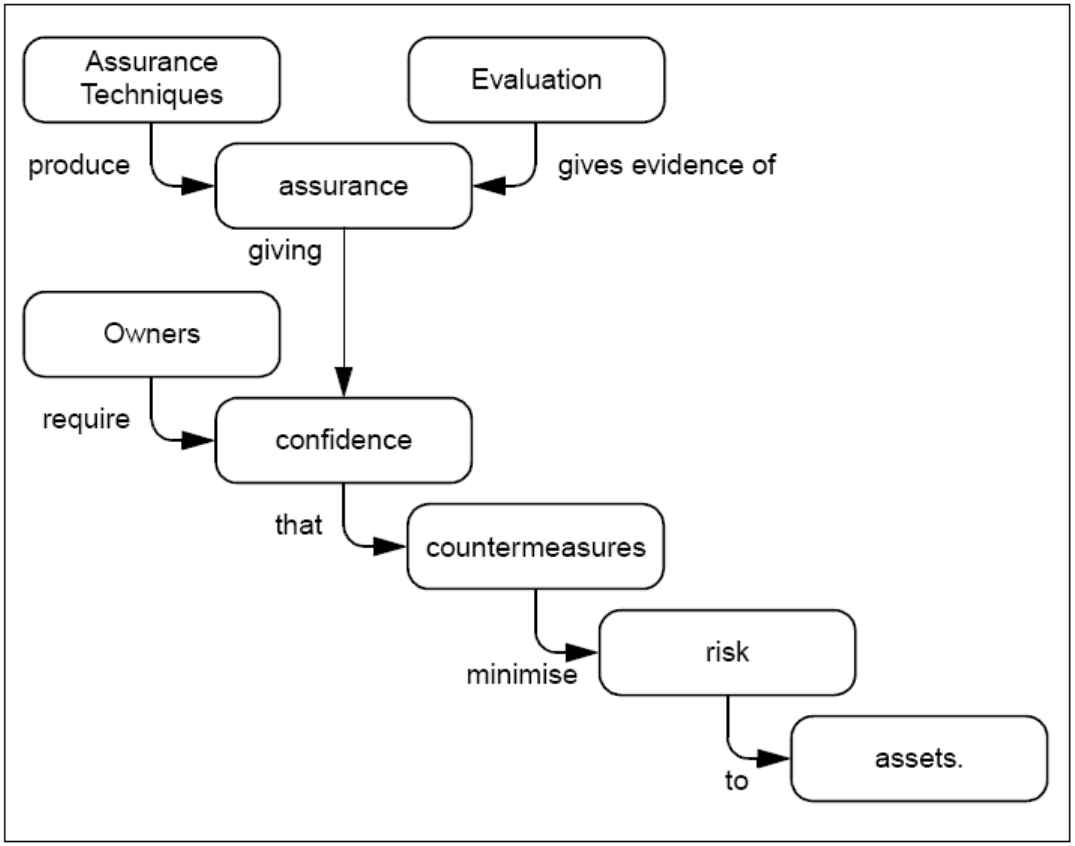


Figure 4.2 - Evaluation concepts and relationships

Vývoj bezpečného systému

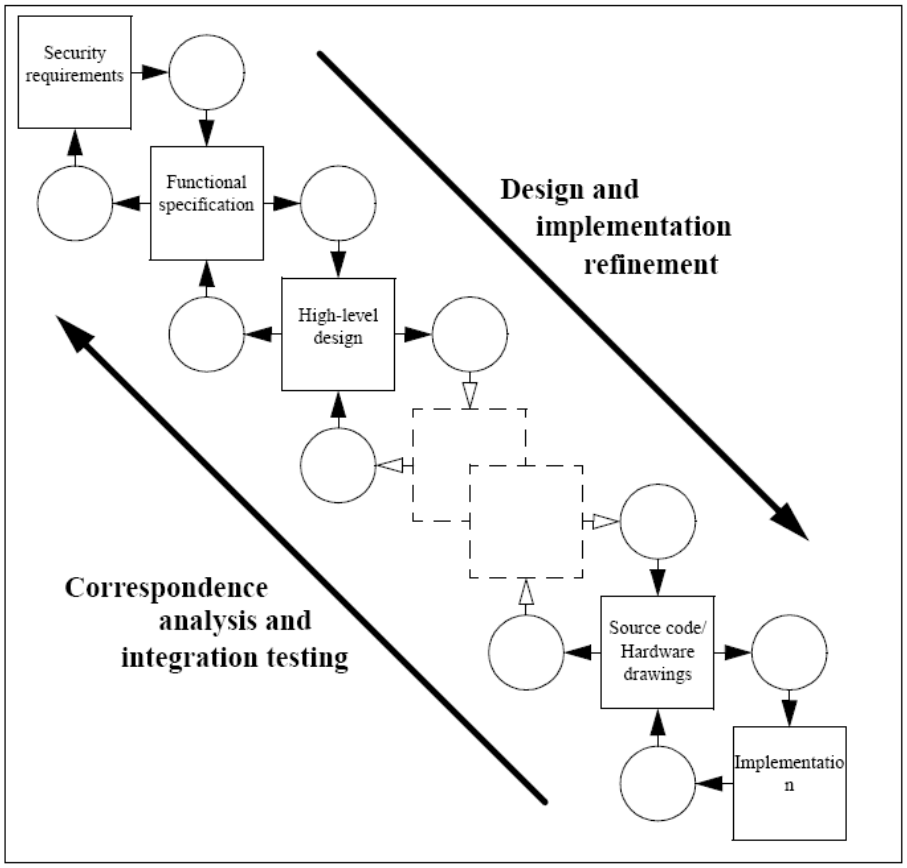
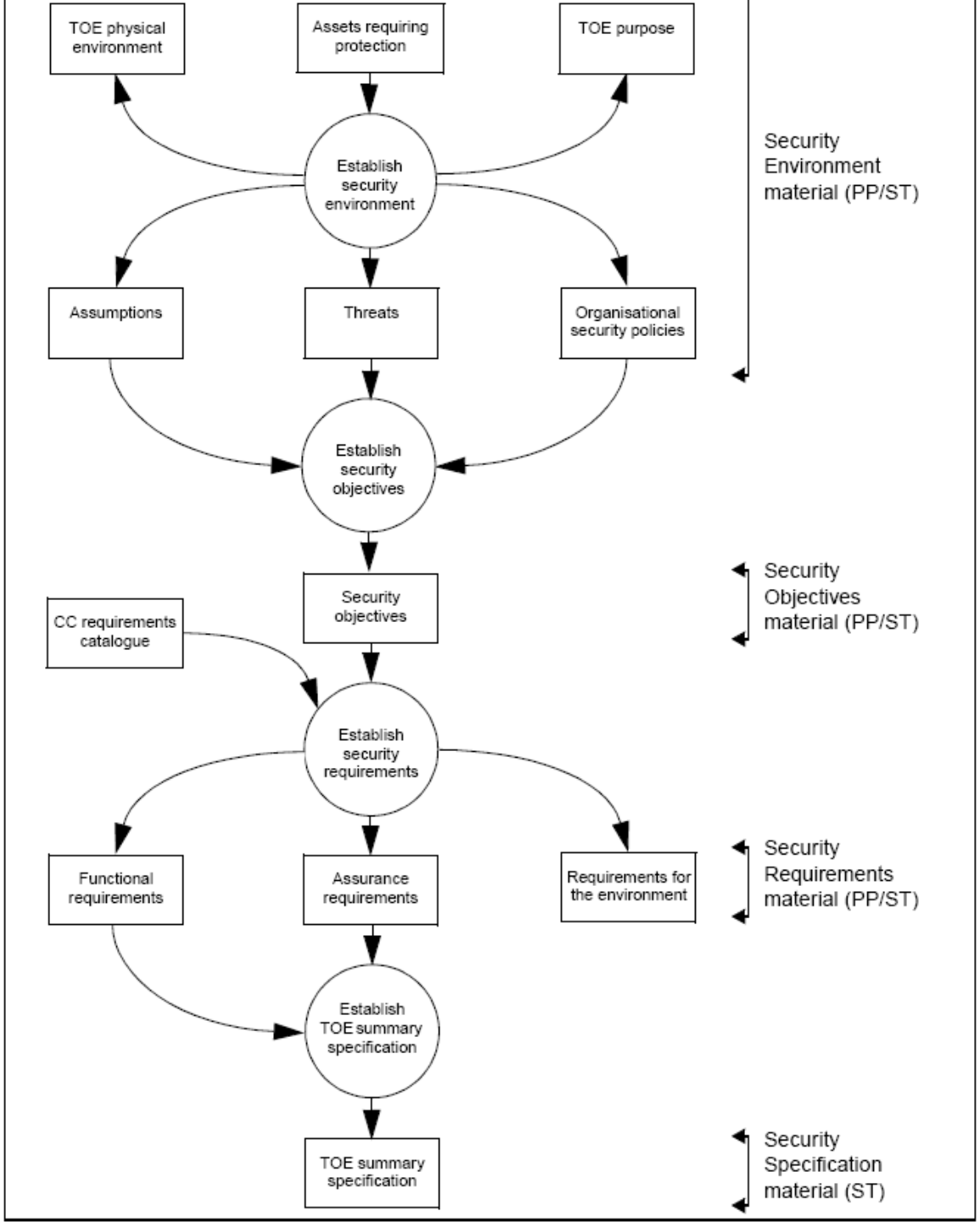


Figure 4.3 - TOE development model


TOE physical environment
Assets requiring protection
TOE purpose
Establish security environment
Security Environment material (PP/ST)
Assumptions
Threats
Organisational security policies
Establish security objectives
Security objectives
Security Objectives material (PP/ST)
CC requirements catalogue
Establish security requirements
Functional requirements
Assurance requirements
Requirements for the environment
Security Requirements material (PP/ST)
Establish TOE summary specification
TOE summary specification
Security Specification material (ST)

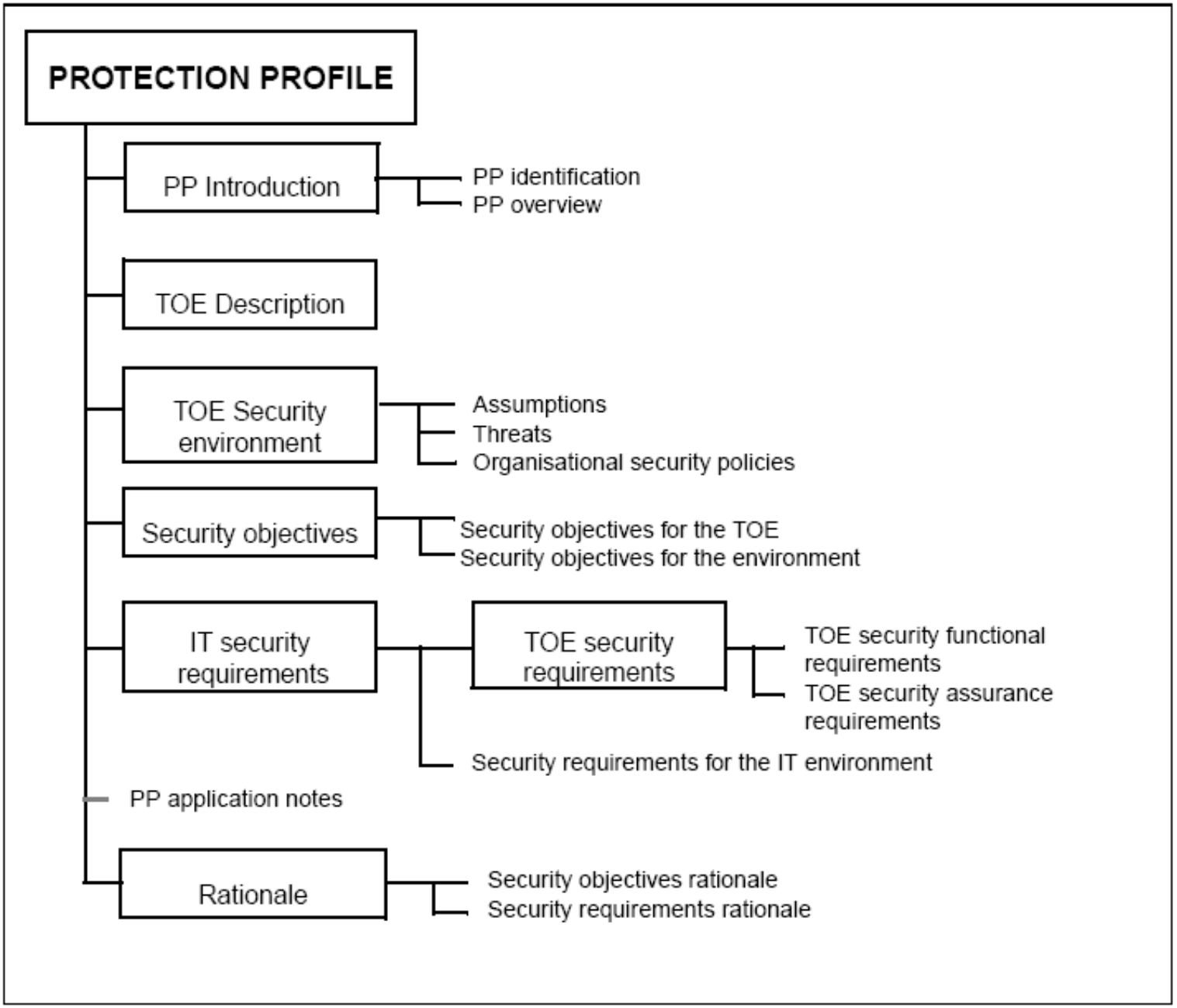
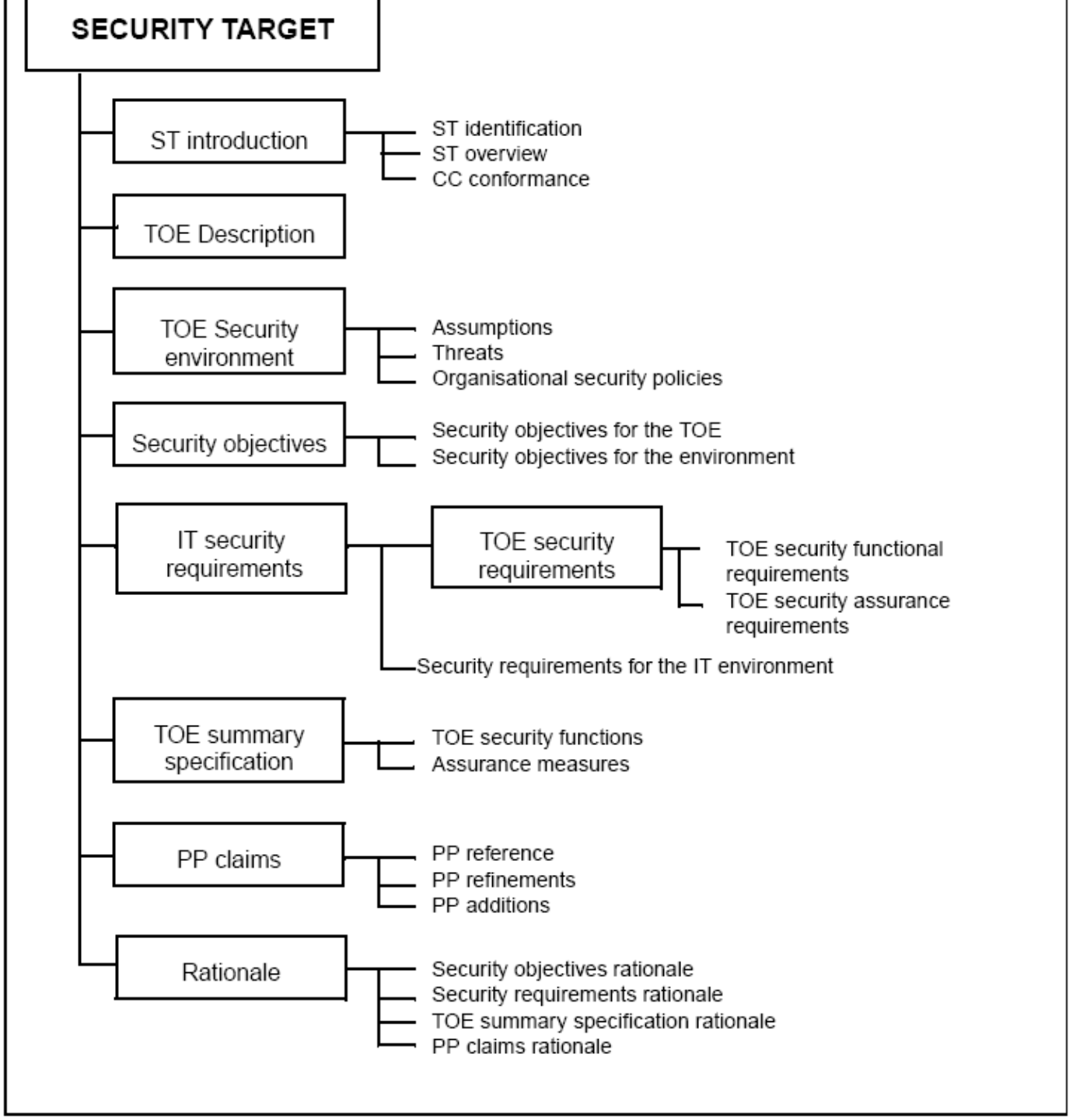


Figure B.1 - Protection Profile content


SECURITY TARGET
ST introduction
ST identification
ST overview
CC conformance
TOE Description
TOE Security environment
Assumptions
Threats
Organisational security policies
Security objectives
Security objectives for the TOE
Security objectives for the environment
IT security requirements
TOE security requirements
TOE security functional requirements
TOE security assurance requirements
Security requirements for the IT environment
TOE summary specification
TOE security functions
Assurance measures
PP claims
PP reference
PP refinements
PP additions
Rationale
Security objectives rationale
Security requirements rationale
TOE summary specification rationale
PP claims rationale

Funkcionálne bezpečnostné požiadavky

- Security audit (FAU)
- Communication (FCO)
- Cryptographic support (FCS)
- User data protection (FDP)
- Security management (FMT)
- Identification and authentication (FIA)
- Privacy (FPR)
- Protection of the TOE Security Functions (FPT)
- Resource utilisation (FRU)
- TOE access (FTA)
- Trusted path/channels (FTP)