Informačná bezpečnosť (5)

Informačná bezpečnosť na globálnej úrovni (povedomie,know-how, štandardy)

Obsah

- Budovanie bezpečnostného povedomia
- Budovanie know-how
  - Guidelines
  - Best practices
  - Normy a štandardy
- Prehľad bezpečnostných noriem

1.2. Vytváranie bezpečnostného povedomia

- Legislatíva tvorí rámec, ale 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

1.3. Budovanie know-how

- Jednotlivé oblasti nie sú disjunktné (výskum aj vzdelávanie patria aj do oblastí prevencie aj trvalo udržateľnej úrovne)
- Výskum (vlastný a sledovateľský)
- Transfer a využívanie cudzieho know-how
- individuálne a organizované vzdelávanie nešpecialistov
- Hotové riešenia
  - OECD zásady (filozofické princípy)
  - Best practices (riešenie pre konkrétne situácie)
- Štandardy (normy)
  - Oficiálne (národné a medzinárodné) (de iure)
  - Neoficiálne (de facto)

OECD (1)

- Dlhodobo sa zaoberá informačnou bezpečnosťou
- OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS = filozofický základ viacerých bezpečnostných štandardov
- Aj iné oblasti
  - C(2012)7 – Recommendation of the Council on International Mobile Roaming Services
  - C(2011)155 – Recommendation of the Council on the Protection of Children Online
  - C(2011)154 – Recommendation of the Council on Principles for Internet Policy Making
  - C(2010)61 – Recommendation of the Council on Information and Communication Technologies and the Environment
  - C(2008)36 – Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information

OECD (2)

- C(2007)68 – Recommendation of the Council on Electronic Authentication
- C(2007)67 – Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy
- C(2006)57 – Recommendation of the Council on Cross-Border Co-operation in the Enforcement of Laws against Spam
- C(2003)259 – Recommendation of the Council on Broadband Development
- C(2002)131/FINAL – Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security
- C(97)62/FINAL – Recommendation of the Council concerning Guidelines for Cryptography Policy
- C(80)58/FINAL – Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

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 *)

- Návody na riešenie štandardných problémov
- Nie sú teoreticky zdôvodnené, nevyžadujú profesionálne znalosti
- Koncový používateľ laik a vzdelaný laik
- 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

- Dobrá úroveň, dostupné, pokrytie širokého okruhu problémov, ale vychádzajúce z amerických podmienok = metodické dokumenty NIST, najmä SP 800
- Prehľad dokumentov NIST: A Guide to NIST Information Security Documents http://csrc.nist.gov/publications/CSD_DocsGuide.pdf
- http://csrc.nist.gov/publications/CSD_DocsGuide_Trifold.pdf

Metodiky BSI

- podobný systematický prístup ako NIST má aj Spolkový úrad pre informačnú bezpečnosť
- Menší počet štandardov
- Do pozornosti
- BSI-Standard 100-2: IT-Grundschutz Methodology
- http://www.bsi.de/english/publications/bsi_standards/index.htm

Normy a štandardy

- Terminologicky standard=norma, v SR štandard je (aj) právny dokument (napr. bezpečnostné štandardy ISVS, vydané MF SR)
- My budeme používať pojmy štandardy a normy ako synonymá
- Veľa štandardizačných organizácií
  - ISO,IEC, CEN, CENELEC, ETSI, NIST, BSI, DIN,...
  - Súkromné spoločnosti RSA Labs – PKCS
  - IETF – RFC
  - Ad hoc iniciatívy (EESSI, UNCITRAL)
- Oficiálne normy a štandardy de-facto
- Dobrý štandard = koncentrované know-how, môže byť veľmi užitočný
- Najprv prehľad, neskôr sa k vybraným štandardom vrátime

ISO/IEC

- Najdôležitejšia medzinárodná štandardizačná organizácia
- Informačná bezpečnosť spadá do kompetencie podvýboru ISO/IEC JTC 1/SC 27: IT Security techniques
- Ten sa delí na 5 pracovných skupín

JTC 1/SC 27/WG 1 Information security management systems
JTC 1/SC 27/WG 2 Cryptography and security mechanisms
JTC 1/SC 27/WG 3 Security evaluation criteria
JTC 1/SC 27/WG 4 Security controls and services
JTC 1/SC 27/WG 5 Identity management and privacy technologies

Ktoré spravujú cca 80 štandardov (väčšinou si ich treba kúpiť, ale dajú sa čítať prezenčne v knižnici SÚTN)

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

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

- alebo diplomovú prácu M.Královiča
- Ktoré sú základné?
- Manažment informačnej bezpečnosti 27xxx (dobrý prehľad na http://en.wikipedia.org/wiki/ISO/IEC_27000-series)
- Hodnotenie bezpečnosti systémov

Manažment informačnej bezpečnosti, vydané štandardy

- ISO/IEC 27000 — Information security management systems — Overview and vocabulary [1]
- ISO/IEC 27001 — Information security management systems — Requirements
- ISO/IEC 27002 — Code of practice for information security management
- ISO/IEC 27003 — Information security management system implementation guidance
- ISO/IEC 27004 — Information security management — Measurement
- ISO/IEC 27005 — Information security risk management
- ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27011 — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27031 — Guidelines for information and communications technology readiness for business continuity
- ISO/IEC 27033-1 — Network security overview and concepts
- ISO/IEC 27035 — Security incident management
- ISO 27799 — Information security management in health using ISO/IEC 27002

Manažment informačnej bezpečnosti (pripravované štandardy)

- ISO/IEC 27007 — Guidelines for information security management systems auditing (focused on the management system)
- ISO/IEC 27008 — Guidance for auditors on ISMS controls (focused on the information security controls)
- ISO/IEC 27013 — Guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001
- ISO/IEC 27014 — Information security governance framework
- ISO/IEC 27015 — Information security management guidelines for the finance and insurance sectors
- ISO/IEC 27032 — Guideline for cybersecurity (essentially, 'being a good neighbor' on the Internet)
- ISO/IEC 27033 — IT network security, a multi-part standard based on ISO/IEC 18028:2006 (part 1 is published already)
- ISO/IEC 27034 — Guideline for application security
- ISO/IEC 27036 — Guidelines for security of outsourcing
- ISO/IEC 27037 — Guidelines for identification, collection and/or acquisition and preservation of digital evidence

ISO/IEC 27001:2013 Information security management systems Requirements

ISO/IEC 27001:2013 covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations).

ISO/IEC 27001:2013 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 27002:2013 Code of practice for information security management *)

5. Information Security Policies
6. Organization of Information Security
7. Human Resource Security
8. Asset Management
9. Access Control
10. Cryptography
11. Physical and environmental security
12. Operation Security- procedures and responsibilities, Protection from malware, Backup, Logging and monitoring, Control of operational software, Technical vulnerability management and Information systems audit coordination
13. Communication security - Network security management and Information transfer
14. System acquisition, development and maintenance - Security requirements of information systems, Security in development and support processes and Test data
15. Supplier relationships - Information security in supplier relationships and Supplier service delivery management
16. Information security incident management - Management of information security incidents and improvements
17. Information security aspects of business continuity management - Information security continuity and Redundancies
18. Compliance - Compliance with legal and contractual requirements and Information security reviews

Certifikácia systémov: ISO/IEC 15408-1:2005 Common Criteria *)

- Najrozsiahlejší štandard
- 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

1.4. Budovanie bezpečných systémov

- Štandardy = teória, bezpečné systémy = aplikácia teórie
- Motivácia:
  - spoľahlivý systém sa dá ťažko budovať z nespoľahlivých častí
  - Veľký systém sa ťažko analyzuje a optimalizuje (aj z bezpečnostného hľadiska)
- 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 neskôr na Common Criteria