Education and training in Information security

Daniel Olejár
Comenius University, Bratislava

Agenda

- Information security
- Slovak National information security strategy and education in information security as a priority
- The categories of ICT users and what they need to know of information security
- The methodology of information security education
- The implementation
-

Information security

- Many human activities are now supported by Information and communication technologies (ICT)
- They cannot be conducted (in required scope and quality) without the use of ICT
- The human society heavily depends on its ICT
- ICT = the critical infrastructure of modern society and therefore must be adequately protected
- Information security (InfoSec) = the neccessary condition of the existence and of the future development of the information society
- A problem – information security:
  - Concerns all ICT systems
  - Must be flexible
  - Requires at least an elementary cooperation of all users
  - Is very expensive and sometimes restrictive
  - Requires (at least) small number of highly qualified experts
  -

The Slovak National information security strategy

- The protection of the national information and communication infrastructure requires a complex and highly coordinated approach
- Slovak government addopted The national information security strategy in 2008
- The strategy defined 8 priorities:
  - The coordination of InfoSec
  - The protection of the national critical information infrastructure
  - education and awareness in InfoSec
  - The protection of human rights and freedoms
  - The support of international cooperation
  - The use of standards and best practices
  - The legislative support of InfoSec
  - Research in InfoSec
  -
  -
-

1.

The human factor of InfoSec

- The main problem of The National InfoSec strategy implementation is the low security awarenes and the lack of qualified people
- The Strategy encountered this problem and formulated the education in InfoSec and the security awareness raising as its priority
- Consequently, in 2009 the proposal of InfoSec education system was prepared and approved by Slovak government
- Due to the political changes and the changes of priorities the implementation of the education system was postponed

Six principles of InfoSec education

- Information security is a multicisciplinary area
- Its scope is very large and its methods are developing
- It is difficult to define it from academic and educational points of view and use the standard educational methods
- Moreover, information security concers every user of ICT, but the needs of users are often very different

We encounter 6 basic principles wich must be employed in a system of InfoSec education

- Adequacy (need to know)
- Usefulness (applicability)
- Flexibility
- Guaranty of content and quality
- Sustainability
- Reproducibility

The categorization of InfoSec education addresees

- The criteria for classification of users: previous knowledge and current/future needs
- 5 basic categories
  - The layman
  - The manager
  - The informatician
  - The InfoSec expert
  - The researcher and the teacher

1. The layman

- The common user without systematic education in informatics
- He uses the ICT of his employer in his job and he use his own computer for his private purposes
- He is an unprivileged user of ICT in his job, but he has administrator privileges for his own computer
- The educational needs
  - Security awareness (basic notions, threats, vulnerabilities, risks, security controls, secure usage of ICT, the security requirements formulated in security policies and how to meet them)
  - Practical skills in the usage of ICT and their security mechanisms (login, logout, the usage of passwords, how to respond to warnings, security incidents, etc.)
  - The basic knowledge on and skills in the management of his own computer (configuration management, managing access rights, installing updates, creating backups)

2. The manager

- Manager
  - a laymen by qualification and by the usage of computers
  - a decision maker by his position in the organization
- Educational needs (basics)
  - The InfoSec management
  - The ICT Project management
  - The proceses of ICT systems operation
  - Personnel security
  - Business continuity planning
- He must understand the legislative requirements and to know how to meet them

3. The informatician

- We distinguish two subcategories of informaticians
  - Programmers and developers
  - Administrators
- The common educational requirements for informaticians
  - To understand basic concepts: threats, vulnerabilities, risks, security mechanisms, controls, assumptions and effects of security control implementation
  - To understand security requirements on ICT systems and to know possible ways how to satisfy them
  - The ability to propose, implement, maintain security mechanisms for/in a particular ICT system
  - The ability of cooperation with InfoSec experts
  -

The special educational needs of informaticians

- Developers and programmers
  - The security aspects during the whole life cycle of ICT system
  - Authentication, access control, auditing, sw. testing, cryptographic mechanisms implementation
- The administration of ICT systems
  - The security of operational environment (networks, operating systems, databases, applications, etc.)
  - The security of processes (system and data backups, security incident solving, business continuity planning, etc.)

4. The InfoSec professional

- InfoSec managers, auditors, specialists from CERTs, CSIRTs, developers of special sw (PKI systems), computer crime investigators, lawyers
- Common knowledge: ICT systems, threats, vulnerabilities, legal and other security requirements, risks, security controls, risk management, business continuity management, standards, certification and accreditation criteria and proceses, etc.
- Specialized knowledge – according to specialization

5. The teacher and the researcher

- They present from educational point of view the most problematic group
- the teachers of InfoSec need to know
  - the content
  - How to deliver the content to their „students“
- The content is specific for every target group and the pedagogical methods still must be developed
- Researchers are in general developing methods, solving (well defined and recognized) problems
- Standard academic research (cryptology)
- Who will deal with fundamental or practical problems?
- The problem of academic recognition and funding
- The preparation of teachers and researchers is an open problem

Body of knowledge (based on CBC)

The areas of InfoSec		laymen	Mana-gers	informaticians		experts
				Develo-pers	Admini-strators	
1	InfoSec management	A	B	B	B	C
2	Architecture, models and evaluation	–	A	B	B	B
3	Access control	A	A	B	B	C
4	Application security	A	A	C	C	B
5	Operation security	A	B	B	C	B
6	Physical security	–	A	A	B	B
7	Cryptography	A	A	B	B	B
8	Network, Internet and communication	A	A	B	B	C
9	Business continuity	A	A	B	C	C
10	Legislation and ethics	A	B	A	A	B

Methods of education (1)

- Responsible for the informatization of society, including InfoSec: The ministry of finance (MF)
- MF is preparing an educational project: creating the content, writing basic documents, testing the potential lectors and the auditorium
- How to spread the knowledge?
- Three basic models
  - School (include InfoSec topics into existing programs)
  - ECDL (prepare and add new InfoSec modul to existing ECDL moduls)
  - ISACA/(ISC)^2
- The proposed system combines all basic solutions
  - Expansion of basic and secondary school informatics curricula (MF+ME)
  - MF will issue the knowledge standards for the employees of public administration
  - MF+ME will create an acreditation body
  -

The methods of education – category informaticians and InfoSec specialists

- InfoSec specialists need knowledge and experience
- Four steps model:
  - Education (e.g. the university study of computer science)
  - Praxis (gaining experience and practical skills)
  - The qualification exam – testing the knowledge and the ability to use it (result = certification)
  - Continual education and maybe recertification
- The university curriculum of Information Security as a specialization of the accredited Computer science program
- Maybe compatible with the ISACA curriculum (and eventually accredited by ISACA)
- The InfoSec education of informaticians:
  - Postgradual
  - Selected topics (suitable for specialists, too)

Implementation

- The cornerstone of the education project is the university InfoSec program
- Does not depend on the ministry project
- In preparation (the deadline 2013)
- The education project is scheduled for 2 years
- Let´s see in 2014
-

Thank you

-