Applied informatics

Fundamentals of security and data storage, protection of data in files and archives.

ZEMÁNEK, Z. – PLUSKAL,D. – SMETANA, B.

esf european social fund in the czech republic
EUROPEAN UNION
MINISTRY OF EDUCATION, YOUTH AND SPORTS
OP Education for Competitiveness
UNIVERSITY OF DEFENCE
INVESTMENTS IN EDUCATION DEVELOPMENT

Fundamentals of security and data storage, protection of data in files and archives.

1. Secure access to data on a PC.
2. Secure protection of data – assets and threats
3. Risk analysis – system penetration
4. Assignments

Aims of the lecture

1. Provide students with basic information about the secure access to the data on the PC
2. Clarify the importance of secure data protection - Assets and threats
3. Characterize the risk analysis of a PC - penetration into the system

esf european social fund in the czech republic
EUROPEAN UNION
MINISTRY OF EDUCATION, YOUTH AND SPORTS
OP Education for Competitiveness
UNIVERSITY OF DEFENCE
INVESTMENTS IN EDUCATION DEVELOPMENT

ICT Security

Secure access to data, information and ICT is a very general term. The actual security issues from the perspective of IS / IT are very extensive:

A. PC / system

B. Data transmission networks

C. Access to remote freely available data / resources

ICT Security

ICT Security covers:

1. Adherence to information security policy of organization by the employees.
2. Security Level of your computer against malicious software.
3. The issue of data stored outside the PC and transfer them.
4. Preventing theft of personal data by a hacker or abuse of our computer spam.
5. Protection against malware, the question of abuse of email, encryption ..
6. In the field of remote access, social networking is a question. Building new protective ethical mechanisms to protect accounts on social networking sites on the Internet.

Secure access to data on a PC

1. Users - employees

- Employees are often the weakest link in the chain of data security.
- Most errors are unintentional mistakes, but often also targeted effort to damage the company.
- "... For 78% of the companies the biggest threat are employees."
- Research Ogilvy Public Relations for GiTy Brno.

- ***The motivation may be:***
  - effort to sell the company a competitive advantage
  - dissatisfaction at work, responding to bullying annoyance of various forms of life in the workplace.

Secure access to data on a PC

2. *Protection of your computer*

E.g. Microsoft in its regular update on the second Tuesday of the month provides updates to fix critical vulnerabilities in Windows, Internet Explorer (IE)? Office and Exchange.

The total annual number of updates in recent years is roughly 20-30% higher than in previous years.

Secure access to data on a PC

Secure access to data is a very general term:

Security and safety within the protection of people and health

= The issue of crisis management information systems

= automated lines, safety breaks ....

Security of objects

= Protection of buildings and guarded areas with computer technology, ensuring fire protection, etc.

Information Security

= Focuses on information security in all forms and in entire life cycle (maintaining the credibility, integrity, availability of information).

Secure access to data on a PC

- Balance costs with security benefits
- Different types of attackers

Reasons to attack:

- Financial profit,
- Good feeling,
- Bad intentions,
- Negligence, …

Secure access to data on a PC

Autentication

- To verify identity of the user
- The aim is the identify verification
- *Typical authentication procedure is based on passwords*
  - Each secure system should authenticate its users.
  - User accounts are maintained in the system
  - Passwords are typically hashed (and NOT encrypted).

Secure access to data on a PC

Autorization

- *Verification of access rights*

Assets and threads

Assets represent basically everything I own. In the future assets will bring economic benefits (i.e., human resources, equipment, supplies, licenses, ...).

Threats and vulnerabilities increase the risk. We introduce countermeasures, based on security requirements.

For each asset, there can be a vulnerability, which can be carried forward by an attack, which we call a security incident..

Assets and threads

Tangible assets

1. ICT,
2. communication device,
3. medium,
4. other technical equipment,
5. Computer rooms and equipment.

Intangible assets

- ❑ data,
- ❑ Software,
- ❑ other.

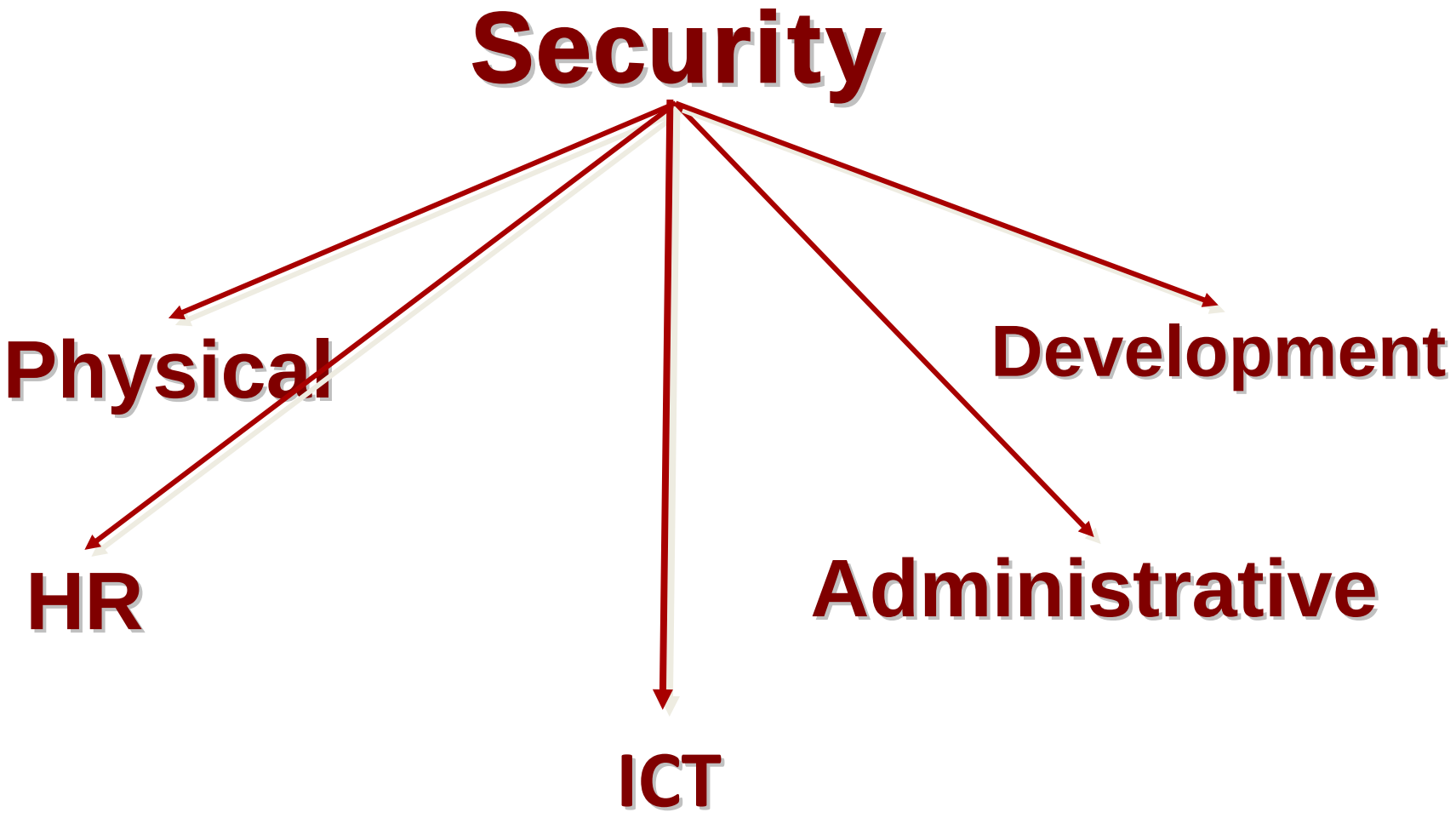
Assets and threads

- Natural and physical
  - natural disasters and accidents;
- Technical and technological
  - failure carriers and computers
  - disorders networks
  - disorders caused by programs;
- human
  - unintentional,
  - intentional

Countermeasures

Any activity, equipment, technology or other procedure to reduce the risk, interference effect of threats.

1. Types
    1. administrative nature,
    2. physical character,
    3. technical and technological nature.
2. objectives
    1. prevention
    2. correction,
    3. detection.


Security
Physical
Development
HR
Administrative
ICT

System penetration

The penetration can be done through each part of the system... formed and influenced by:

People - the biggest weakness of IS.

HW - depending on the kind and quality.

SW - depending on the kind and quality.

Method - methodology and organizational measures.

System penetration

Factors = causes or conditions that induce, facilitate or encourage the commission of crimes.

They have the character of intent, motive or motivation:

1. commit an offense,
2. cause irresponsibility, carelessness ...
3. unintentional torts.

System penetration

Factors:

- unregulated development of the information market,
- underestimating the protection and security of PC,
- low level of legal awareness of users
- frequent incompetence of law enforcement authorities in the field of information
- organization and professionalism of offenders...

Forms of penetration

Forms of penetration:

- violent assault on a data media
- use of human error in an individual who is the element of the system, thanks to the excessive security policy of the organization,
- breaking or getting input the password into the PC,
- introduction of the virus into the software for your own PC ...

System penetration

Countermeasures:

1. effective protection by the legal system,
2. effective protection by SW and HW equipment,
3. effective protection by organizational control activities,
4. effective protection by the internal rules of access,
5. effective protection by training of users.

System penetration

For these reasons, it is necessary to suppress or completely eliminate criminal factors enabling direct penetration of the perpetrators of the IS or affecting the motivation of the perpetrator.

Putting other factors initiates procedures, in criminal proceedings, cyber crime and reveals the hidden possibilities of protecting your own PC.

Assignments

1. In practice, implement basic information about the secure access to the data on the PC.
2. Clarify the importance of data protection - Assets and threats
3. To characterize the security analysis of PC – System penetration

Resources:

1. ČERNÝ, M. *Počítačová bezpečnost* [online]. 2010 [cit. 2013-12-20]. Dostupné z: *clanky.rvp.cz/wp-content/… /pocitacova_bezpecnost_prezentace.ppt*
2. ČERNÝ, M. *Systémy detekce a prevence průniku* [online]. 2010 [cit. 2013-12-20]. Diplomová práce. Brno: VUT, FEKT. Dostupné z: http://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=27248
3. Typy poškození dat. *Http://www.datahelp.cz* [online]. 2010 [cit. 2013-12-13]. Dostupné z: http://www.datahelp.cz/zachrana-dat/typy-poskozeni-dat/
4. COVEY, S. R. - MERRILL, A. R. - MERRILL, R. R. *To nejdůležitější na první místo*. 1. vyd. Praha: Management Press, 2009. 380 s. ISBN 978-80-7261-187-4.