Zranitelnosti institucionálních repozitářů

Kovářová, Pavla
2011

MASARYK UNIVERSITY

Vulnerabilities of Institutional Repositories

- Mgr. Pavla Kovářová
- KISK FF MU, ÚISK FF UK
- kovarovap@gmail.com

Definition of Topic

- An increasing pressure to make documents public
- A need to access them irrespective of the geographical distance
- With solution being digital (institutional) repositories = the topic of the paper
- Weak spots connected with repositories rather then with literature – limitation to grey literature makes no sense
- After introduction of the topic, real life examples of vulnerabilities, their possible solutions and references to literature

Definition of Threats (Požár, 2005, p. 37-38)

- *„The **Threat** is a circumstance, occurrence, force or persons, the operation (activity) of which **may cause a damage**, loss, loss of confidence or value of an asset. (…)*
- *The **Risk** is a **probability**, with which the value of an asset will be destroyed or damaged by the operation of a particular **threat** working against the weakness of this value. (…)*
- *The **Attack**, which we also call a **security incident**, means either an intentional use of the weak spot that making use of the weak spot to cause damage/loss of IS assets, or unintentional action result in the damage to the assets. (…)*
- *The **Vulnerability** is a deficiency or a **weak spot** of the security system that can be used by the threat resulting in the damage or loss of the assets."*

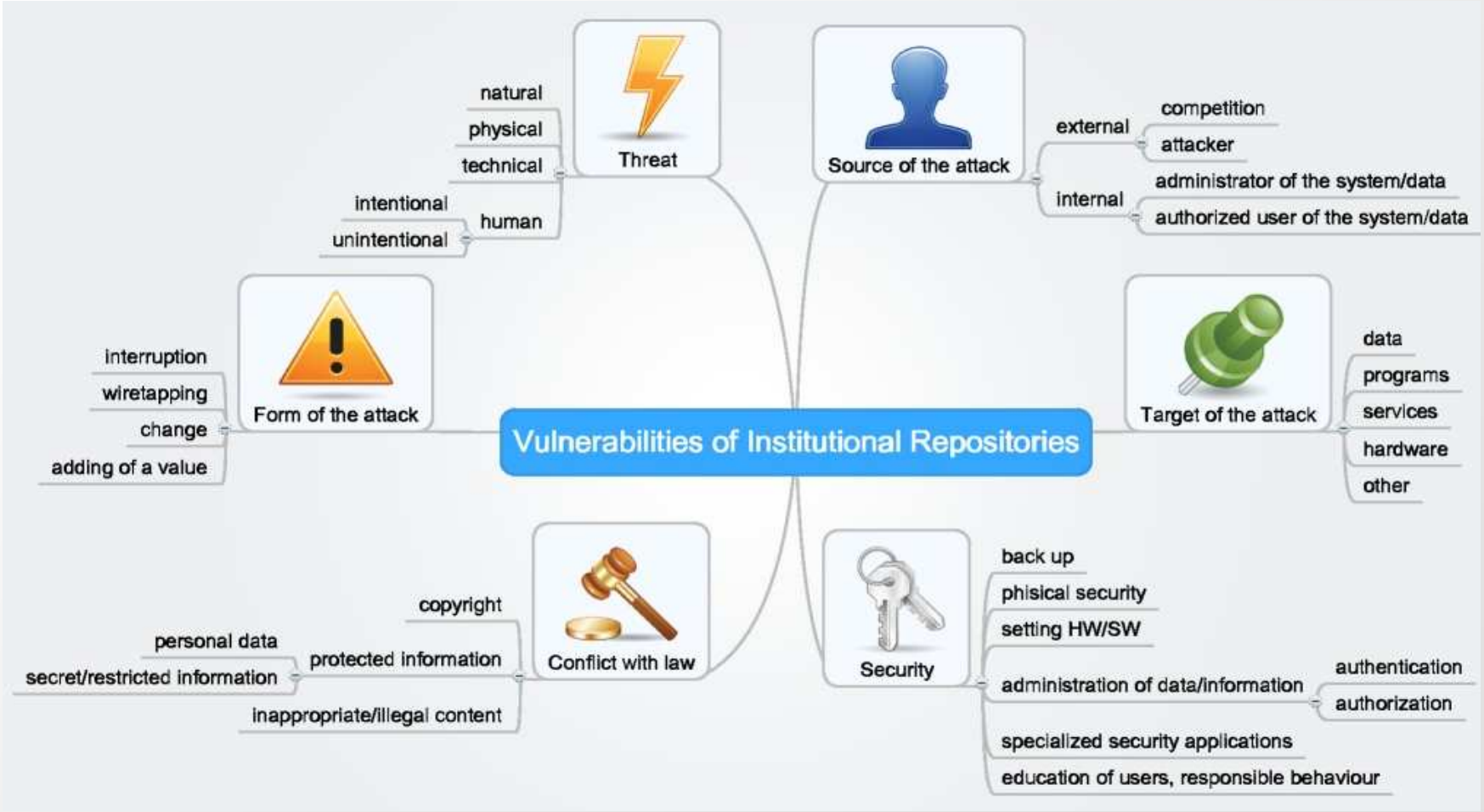
Vulnerabilities of Institutional Repositories

- Never 100% security – please see „unbreakable" code
- Ocurence of vulnerabilities– error or intention in technical, data or human element
- There are solutions to limit risks, it is more appropriate to apply them then to write the repository off

Risk Management

- Risk Assessment "*a process of assessing the threats working against the information system with an aim to define the level of risk, to which the system is exposed. The purpose is to establish whether the security measures in place are sufficient to reduce the probability of the occurrence of the damage to an acceptable level.*" (Požár, 2005, s. 37)
- Effectiveness -> ALE (Annual Loss Expectancy)
- Risk management as a part of information audit – please see NUŠL

Threat Classification



Security Tools

- ISO standards
  - ČSN ISO/IEC 27000 - 27002 – System for information security management,
  - ČSN ISO/IEC 15408 – Criteria for IT security assesment,
  - ČSN ISO/IEC TR 13335-1 - 13335-4 – Guideline for management of IT Security,
  - ISO/IEC TR 13335-5 - Guidelines for the management of IT Security, Management guidance on network security
- Assesment of system credibility
  - TCSEC - Trusted Computer System Evaluation Criteria, so called Orange Book
  - ITSEC - Information Technology Security Evaluation Criteria + evaluative manual ITSEM
  - CTCPEC - Canadian Trusted Computer Product Evaluation Criteria
- Methodologies and software solutions
  - CRAMM
  - Cobra
  - DRAMBORA

Example – Violation of Secrecy (Theft of Data by Competition)

- Both intentional and unintentional human threat (the use of social engineering), possible coercion
- Physical environment or ICT (spyware)
- Primary source – competion or any person
- Data wiretapping, including proprietary information
- Security: data/access management, security applications, physical devices, education
- Problem not only with digital repositories – must respect information policy

Example – Integrity Violation

- Data alteration or adding values to them
- User harmed (wrong data), administrator (credibility, or by law – or by any of the above)
- Intentional (from anywhere) and unintentional (internal) human threat
- Security: back-ups, physical devices, and other as prevention

Example– Availability Violation (DoS)

- Form of suspension
- Program or service is targeted
- Almost exclusively an intentional human threat, competion is the source
- Security: difficult, mainly setting of HW/SW and security apps
- Often we can only wait when it is over

Summary

- Introduction of digital institutional repositories with examples
- Few references in professional literature (more often IS)
- Outline of risk and their limitations
- Weak spots are everywhere – advancement through credible digital repositories

THANK YOU FOR YOUR ATTENTION.