Zranitelnosti institucionálních repozitářů

Kovářová, Pavla
2011

MASARYKOVA UNIVERZITA

Zranitelnosti institucionálních repozitářů

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

Vymezení tématu

- Roste tlak na zpřístupnění dokumentů
- Potřeba přístupu bez ohledu na geografickou vzdálenost
- Řešením digitální (institucionální) repozitáře = oblast příspěvku
- Slabiny spojené s repozitáři spíš než s literaturou – nemá smysl omezení na šedou literaturu
- Pro uvedení do problematiky ukázky zranitelností z praxe, jejich možná řešení a odkazy na literaturu

Vymezení pojmů (Požár, 2005, s. 37-38)

- *„**Hrozba** (Threat) je skutečnost, událost, síla nebo osoby, jejichž působení (činnost) **může způsobit poškození**, zničení, ztrátu důvěry nebo hodnoty aktiva. (…)*
- ***Riziko** (Risk) je **pravděpodobnost**, s jakou bude daná hodnota aktiva zničena nebo poškozena působením konkrétní **hrozby**, která působí na slabou stránku této hodnoty. (…)*
- ***Útokem**, který nazýváme rovněž **bezpečnostní incident** rozumíme buďto úmyslné využitkování zranitelného místa, tj. využití zranitelného místa ke způsobení škod/ztrát na aktivech IS, nebo neúmyslné uskuteč-nění akce, jejímž výsledkem je škoda na aktivech. (…)*
- ***Zranitelnost** (Vulnerability) je nedostatek nebo **slabina** bezpečnost-ního systému, která může být zneužita hrozbou tak, že dojde k poškození nebo zničení hodnoty aktiv."*

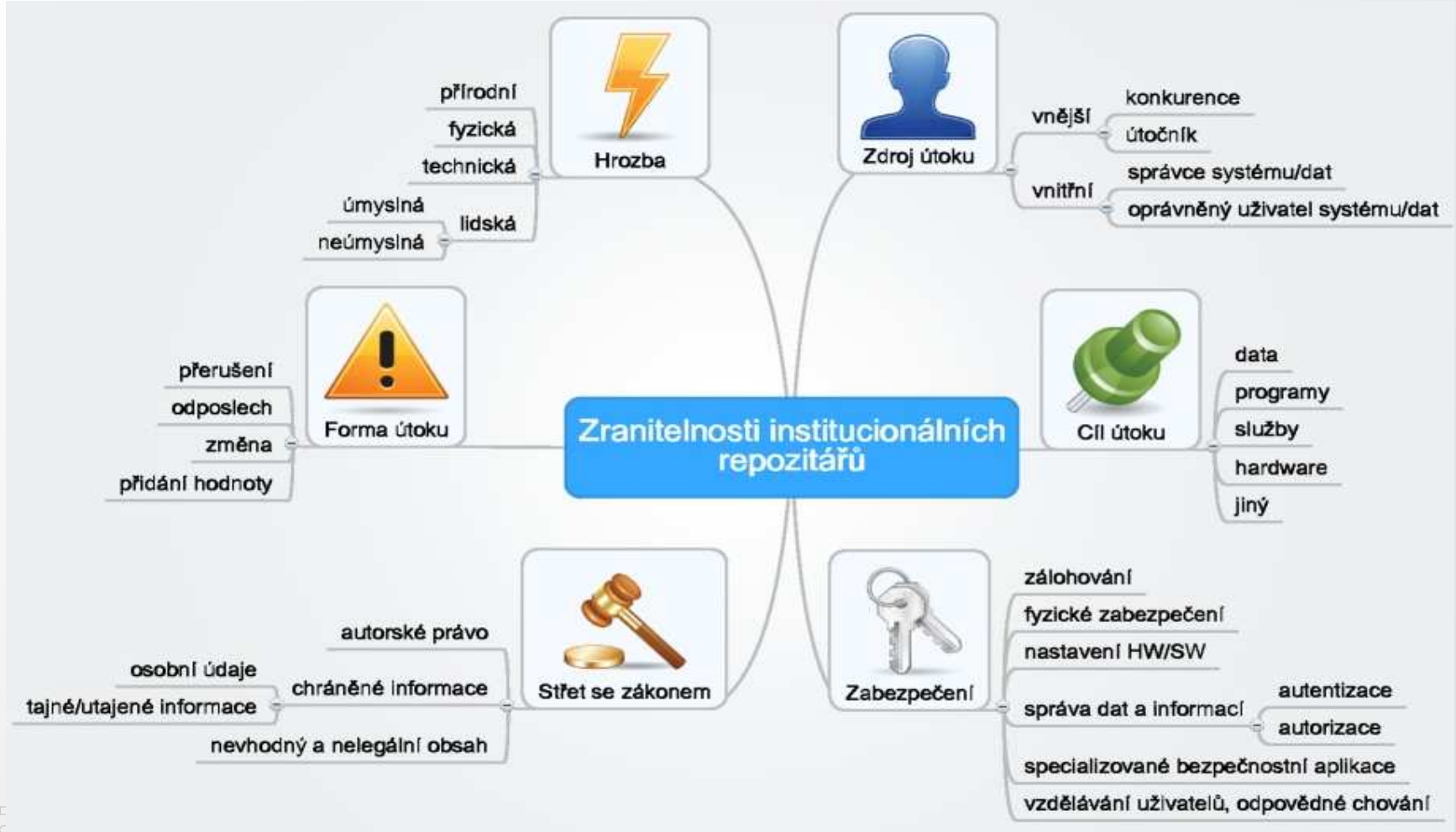
Zranitelnosti repozitářů

- Zabezpečení nikdy 100% – viz „neprolomitelná“ šifra
- Vznik zranitelností – chyba i úmysl, v technické, datové či lidské složce
- Pro omezení rizik jsou řešení, vhodnější je aplikovat než odepsat digitální repozitář

Risk management

- Ocenění rizik (Risk Assessment) "*proces vyhodnocení hrozeb, které působí na informační systém s cílem definovat úroveň rizika, kte-rému je systém vystaven. Cílem je zjištění, jsou-li bezpečnostní opatření dostatečná, aby snížila pravděpodobnost vzniku škody na přijatelnou úroveň.*" (Požár, 2005, s. 37)
- Efektivita -> ALE (Annual Loss Expectancy)
- Risk management součástí informačního auditu – viz NUŠL

Klasifikace hrozeb



Pomůcky zabezpečení

- ISO normy
  - ČSN ISO/IEC 27000 - 27002 - Systém řízení bezpečnosti informací,
  - ČSN ISO/IEC 15408 - Kritéria pro hodnocení bezpečnosti IT,
  - ČSN ISO/IEC TR 13335-1 - 13335-4 - Směrnice pro řízení bezpečnosti IT,
  - ISO/IEC TR 13335-5 - Guidelines for the management of IT Security, Management guidance on network security
- Hodnocení důvěryhodnosti systému
  - TCSEC - Trusted Computer System Evaluation Criteria, tzv. Orange Book
  - ITSEC - Information Technology Security Evaluation Criteria + evaluační manuál ITSEM
  - CTCPEC - Canadian Trusted Computer Product Evaluation Criteria
- Metodiky a softwarová řešení
  - CRAMM
  - Cobra
  - DRAMBORA

Příklad – narušení utajení (krádež dat konkurencí)

- Lidská hrozba úmyslná i ne (využití sociálního inženýrství), možný nátlak
- Fyzické prostředí či ICT (spyware)
- Primární zdroj konkurence, poslední kdokoli
- Odposlech dat, vč. chráněných informací
- Zabezpečení: správa dat/přístupu, bezpečnostní aplikace, fyzické prostředky, vzdělávání
- Problém nejen u digitálních repozitářů – musí respektovat informační politika

Příklad – narušení integrity

- Změna dat či přidání hodnoty k nim
- Poškozen uživatel (chybná data), správce (důvěryhodnost, příp. zákon – jakýkoli z uvedených)
- Lidská hrozba úmyslná (odkudkoli) i ne (vnitřní)
- Zabezpečení: zálohování, fyzické prostředky, ostatní jako prevence

Příklad – narušení dostupnosti (DoS)

- Forma přerušení
- Cíl program či služba
- Téměř výhradně lidská úmyslná hrozba, zdrojem konkurence
- Zabezpečení: těžké, hl. nastavení HW/SW a bezpečnostní aplikace
- Často jediné řešení počkat, až to přejde

Shrnutí

- Představení zranitelností digitálních institucionálních repozitářů s příklady
- Málo v odborné literatuře (spíš IS)
- Nastínění rizik i jejich omezení
- Všechno má slabiny – pokroku vstříc s digitálními důvěryhodnými repozitáři

DĚKUJI ZA POZORNOST.