SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Modelování hrozeb

Hana Vystavělová

AEC, spol. s r.o.

Agenda

- Možné způsoby identifikace rizik
- Úskalí analýzy rizik
- Modelování hrozeb – metodiky
- Modelování hrozeb – ukázky
- Výhody a přínosy modelování hrozeb

Jak identifikovat rizika?

- Penetrační testy a audity
  - technické zranitelnosti a slabá místa
- Analýzy (současného stavu, audity bezpečnosti)
  - slabá místa, nedostatky, neshody (vůči normě, best practices)
- Analýza rizik IS
  - kvalitativní vs. kvantitativní přístup
  - detailní specifikace, číselné vyjádření
- Modelování hrozeb

Analýza rizik dle ISO/IEC 27005

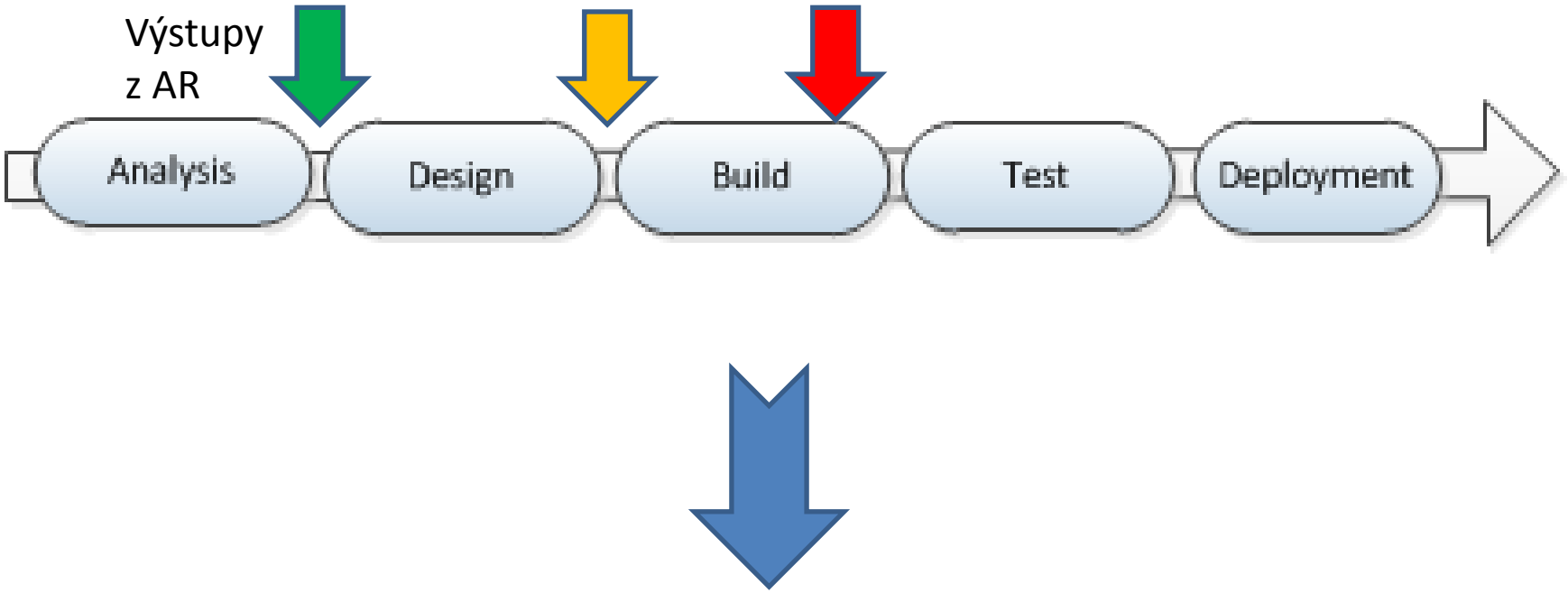
- Stanovení kontextu
- Identifikace a kategorizace aktiv
- Identifikace zranitelností
- Identifikace hrozeb
- Identifikace následků
- Identifikace stávajících opatření

Časté problémy spojené s AR

- málo detailní – obecná
  - jaká opatření a kde aplikovat?
- složitý výpočet rizika
  - co vše ovlivňuje míru rizika?
  - které veličiny snižovat?
- nesprávné pochopení (interpretace) výstupů
  - co mi tedy skutečně hrozí?
- obtížná uchopitelnost výsledků
  - výstupem je 50+ opatření, kde začít?

Časté problémy spojené s AR

- netriviální v rámci SDLC
  - dostupnost výstupů z AR v průběhu vývojového cyklu

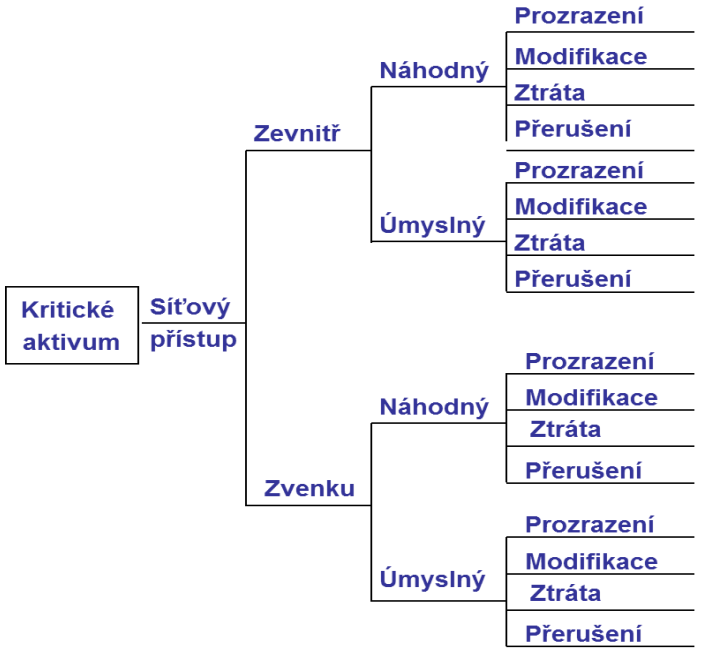


Možné řešení: modelování hrozeb

Cíle a metodiky modelování hrozeb

- Cíle:
  - identifikace a pochopení možných ohrožení aplikace nebo systému
  - které hrozby jsou reálné pro útok na aplikaci/systém?

- OCTAVE
- ISO/IEC 27002
- Microsoft
- OWASP



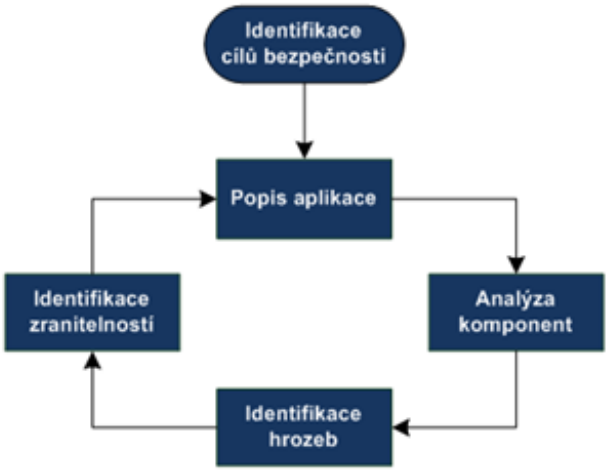
Vybrané ukázky

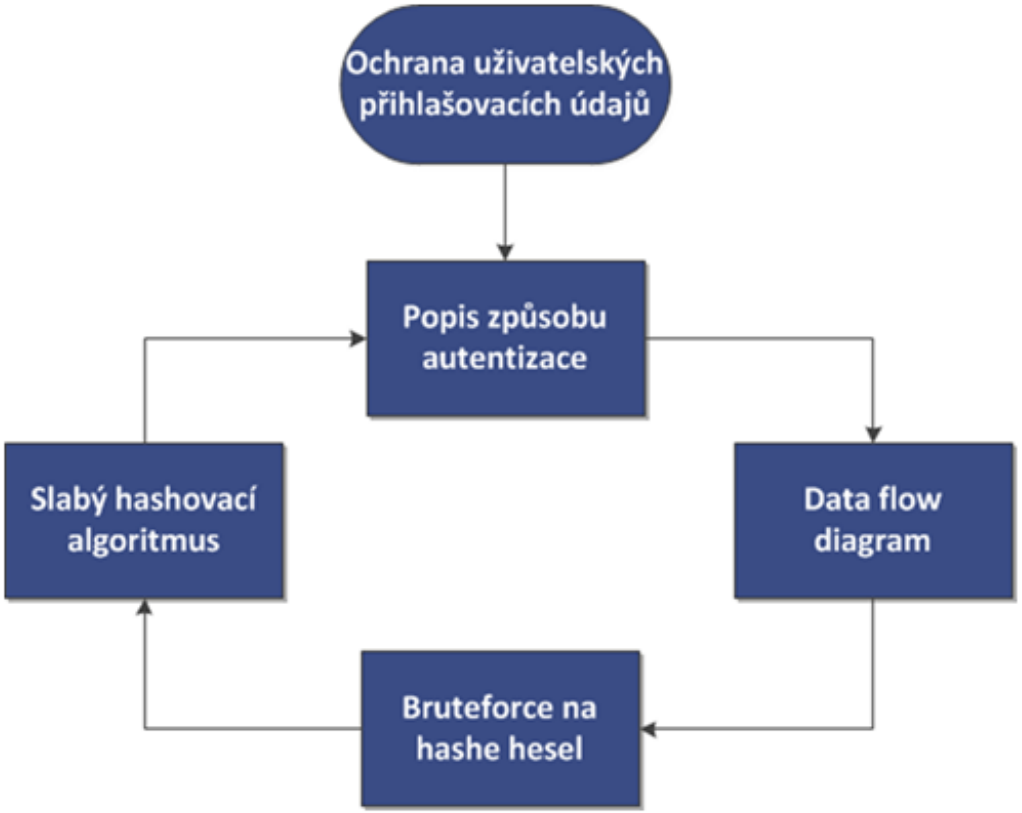
- Jednoduchý model zranitelnosti x hrozby

HROZBY/ZRANITELNOSTI	H	H	M	L	L	L	
	Proces obnovy je zdlouhavý a neodpovídá požadavkům na dostupnost	Neexistuje admininistrátorská VLAN	Systém logování událostí (log management) není dostatečný	TMOUT Is Missing for User ROOT	Neexistují provozní deníky	Nejsou prováděny zálohy konfigurcae	**Součet přes hrozby**
Únik informací z aplikace (uložených v databázi apod.)	1	2	3	2	1	1	**10**
Únik informací - odposlouchávání komunikace	1	2	3	1	1	1	**9**
Chyba integrity nebo ztráta informací uložených v aplikaci	3	2	3	2	2	2	**14**
Nedostupnost služeb nebo informací	3	3	3	2	3	3	**17**
Neautorizovaný přístup k aplikaci	1	2	3	2	1	1	**10**
Neautorizovaná změna informací v aplikaci	1	2	3	2	1	1	**10**
Únik citlivých informací o aplikaci (konfigurace, architektura, bezpečnostní opatření apod.)	1	1	2	2	1	1	**8**
Eskalace privilegií	1	1	2	3	1	1	**9**
Technická chyba HW	3	2	2	1	2	2	**12**
Poškození HW (vandalismus, požár, povodeň apod.)	2	1	1	1	1	1	**7**
Uživatelská chyba	1	1	2	1	1	1	**7**
Chyba administrátora	2	2	3	3	3	3	**16**
Chyba dodavatele aplikace, prostředí etc.)	2	2	3	2	2	2	**13**
Porušení legislativy (internal/externí) (osobní údaje, spam atd.)	2	2	3	2	2	2	**13**
Součet přes zranitelnosti	**24**	**25**	**36**	**26**	**22**	**22**	

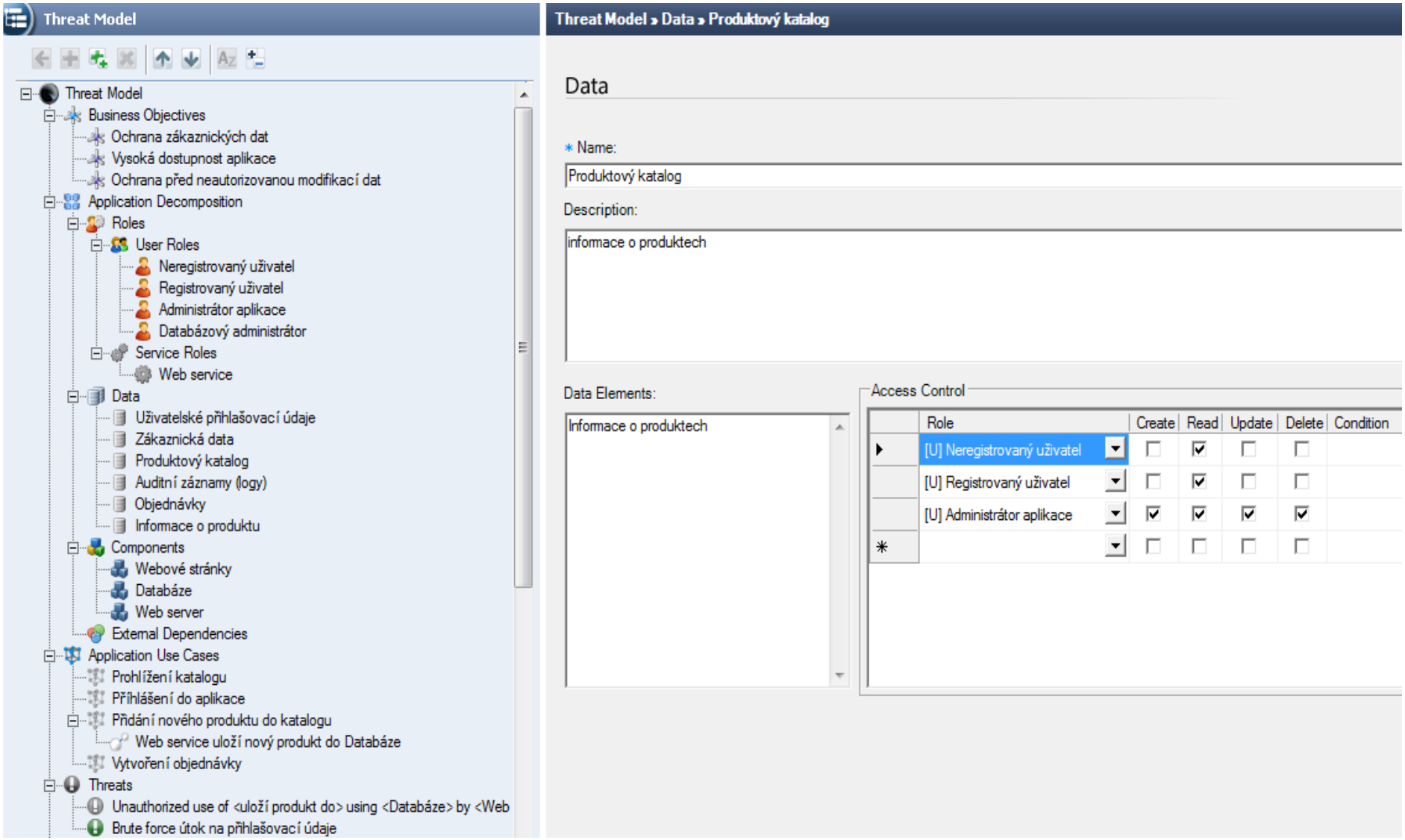
Vybrané ukázky

- Modelování hrozeb dle metodiky Microsoft

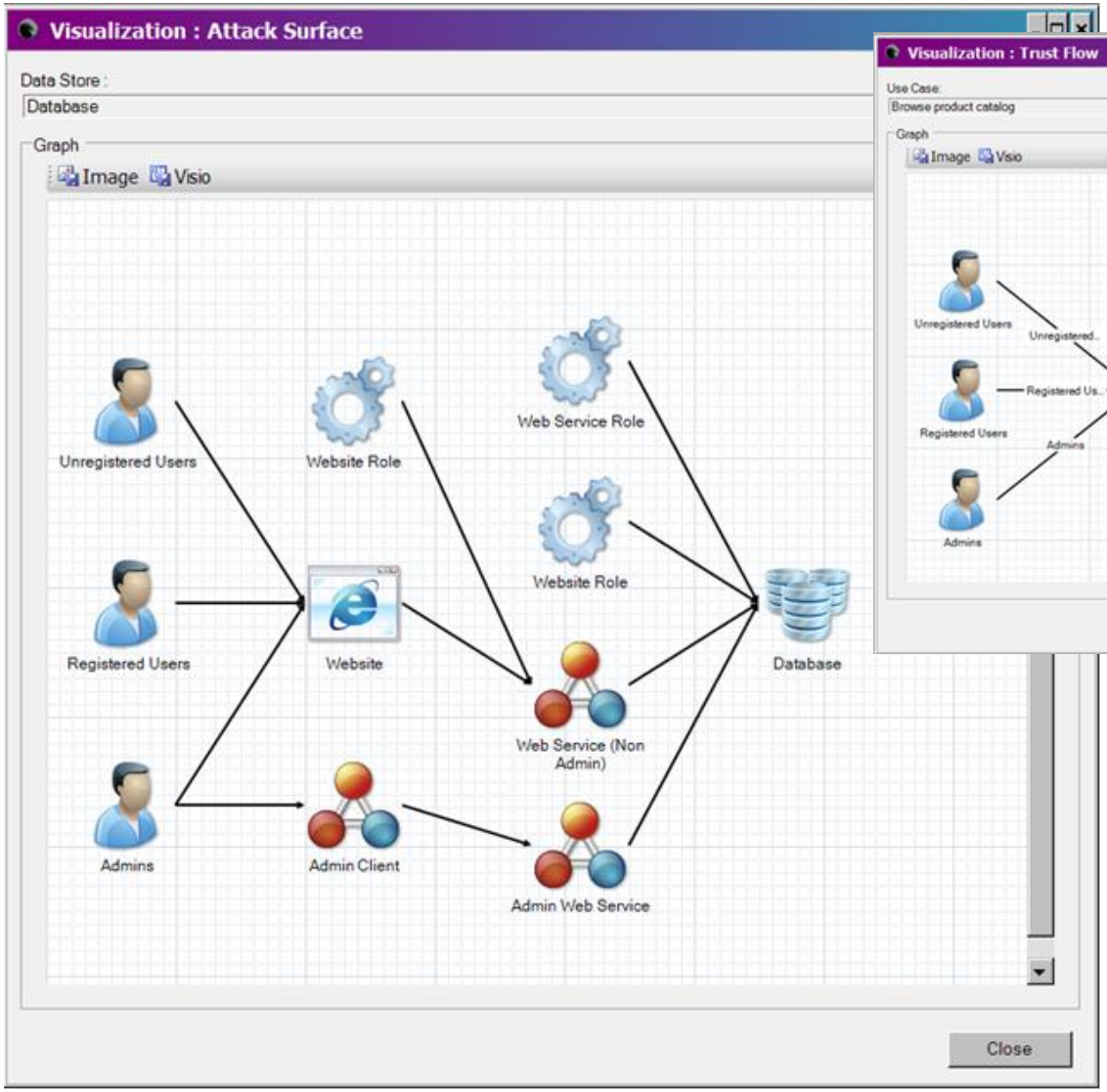


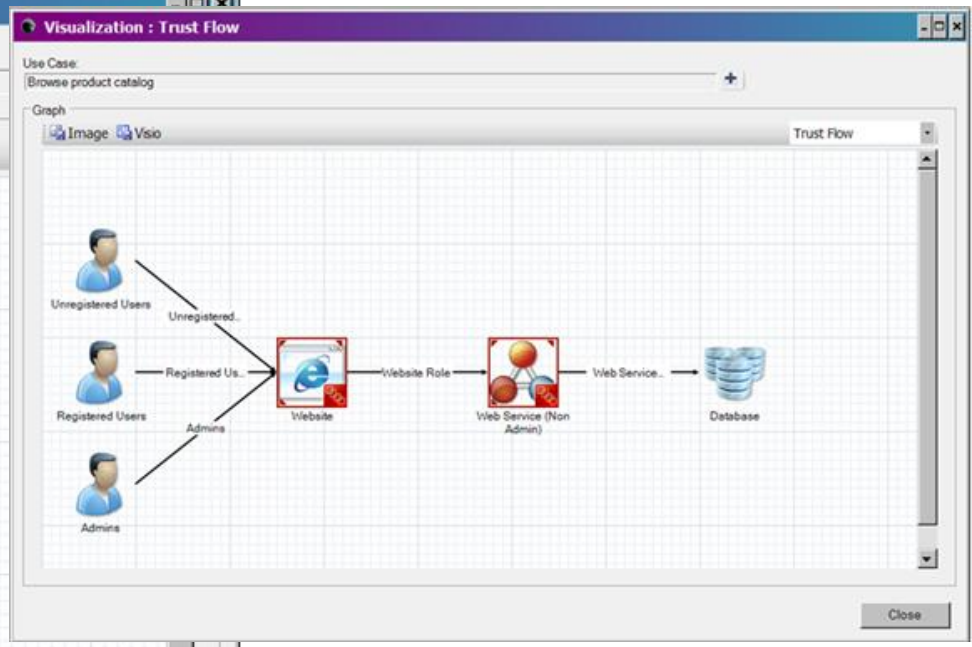


MS Threat Analysis and Modeling tool



Threat Analysis and Modeling tool





Zdroj: Microsoft Threat Analysis and Modeling Tool

Případová studie

- Model hrozeb pro aplikaci internetového bankovnictví
- Úvodní fáze:
  - sběr podkladů – dokumentace, interview, případně (penetrační) testy
  - specifikace systému, použité role
  - dekompozice aplikace (rozhraní s okolními systémy, datové toky, vstupní a výstupní body, použité technologie,…)
  - identifikace zranitelných míst

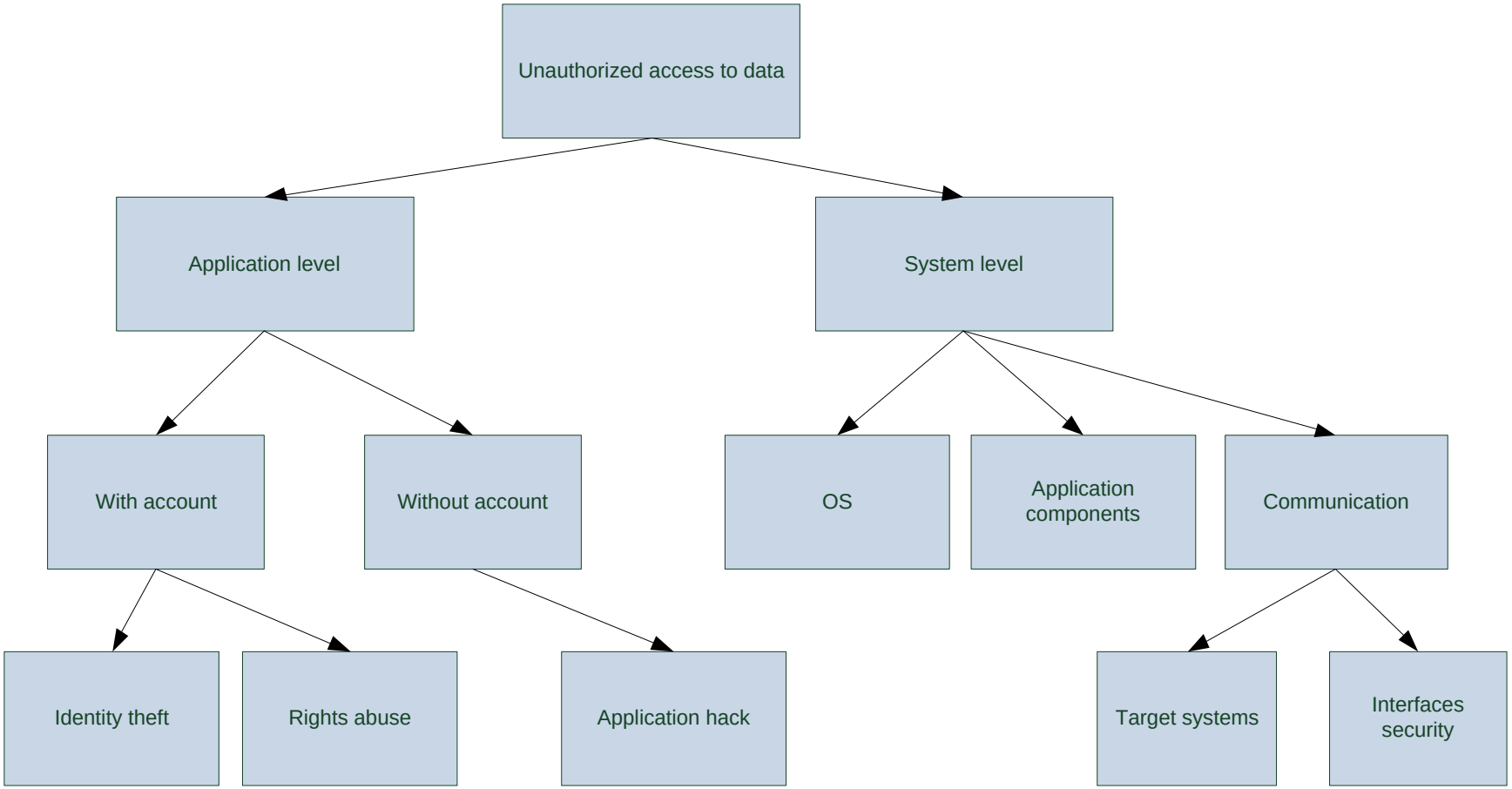
Případová studie

- Analýza útočníka

Attacker profile							
Group	Commitment		Resources				Resulting level
	Intensity	Time	Tech. personnel	Cyber knowledge	Vertical knowledge	Access	
Administrators	Medium	Months	15	Critical	Critical	Critical	**Critical**
Back Office	Medium	Months	40	Low	Critical	High	**High**
Security & Risk & Audit	Medium	Months	2	Critical	Critical	High	**High**
Legal & Compliance	Medium	Months	5	High	High	Medium	**Medium**
Developers	Medium	Months	5	High	Critical	Medium	**Medium**
Other employees	Medium	Months	100	Medium	Medium	Low	**Medium**
Former employees	High	Weeks	10	High	High	Low	**Medium**

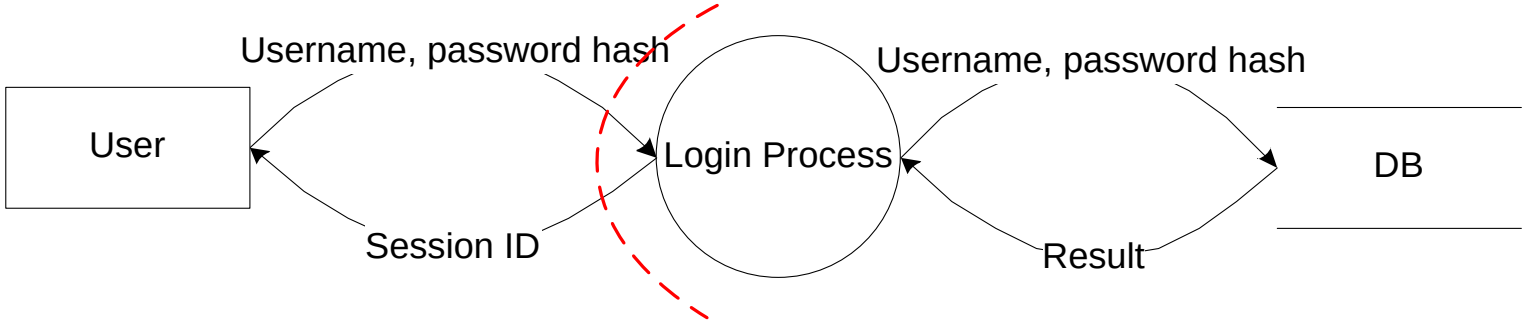
Případová studie

- Threat/attack tree



Případová studie

- Data flow diagrams



- Z hrozeb vyplývají oblasti pro další analýzu:
  - HTTPS konfigurace front-endového serveru
  - autentizace aplikace k databázi
  - zabezpečení komunikace s DB
  - politika hesel aplikace a její vynucování
  - politika hesel databáze
  - způsob uložení hesel v databázi
  - způsob auditování login procesu
  - síla hashovacího algoritmu

Možná úskalí modelování hrozeb

- Existuje více přístupů – na začátku je třeba dobře identifikovat potřeby
- Nedostatek informací/dokumentace pro detailní modelování
- Nesoučinnost dodavatele aplikace
- Provozní slepota
- Nedostatečné pochopení aplikace
- Správné uchopení výsledků odpovědnými osobami
- Pravidelná aktualizace modelu

Přínosy modelování hrozeb

- Modelování může být rychlé, jednoduché a přesto velmi účinné
- Efektivní při vývoji aplikace
- Nejsou analyzovány nepravděpodobné hrozby
- Jiný pohled než v případě code review a penetračních testů
- Umožňuje cíleně implementovat opatření
  - monitoring a ochrana informací (SIEM, DLP, …)
  - code review
  - zaměření penetračních testů

SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Hana Vystavělová

AEC, spol. s r.o.

hana.vystavelova@aec.cz