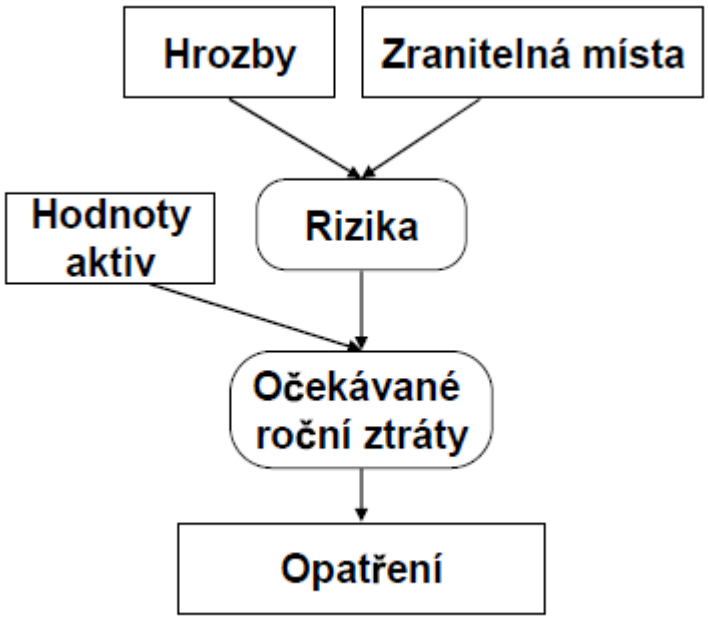
Analýza rizik

Z FITwiki

Obsah

Analýza rizik



Proces analýzy rizik

1. Identifikace aktiv
2. Stanovení zranitelných míst a hrozeb
3. Stanovení rizik
4. Výpočet očekávané roční ztráty (ALE)
5. Volba bezpečnostních opatření

Očekávaná roční ztráta (Annual Loss Expectations - ALE)

- je škodlivý efekt uskutečnění hrozby a využití zranitelného místa přepočtený na rok
- závisí na:
  - pravděpodobnosti výskytu bezpečnostního incidentu – P (např. jednotky výskytu za rok)
  - průměrné škodě vzniklé tímto incidentem – C.

- Riziko se vypočte jako R = P * C.

Námitky proti analýze rizik

- **Nepřesná** – odhady bývají nepřesné a výsledky různých metodologií se často liší
- **Vyvolává falešný dojem přesnosti** – Špatná interpretace výsledků není chybou metodologie ale chybou uživatele
- **Neměnnost** – uživatel často analýzu rizik provede jednou a nikdy ji neopakuje. Měla by se opakovat při každé změně vnějších okolností.
- **Nemá vědecký základ** – Většina metodologií má vědecký základ

1. Generace – Metody "checklist"

- Výběr z několika řešení na základě dotazníku

Předpoklady:

- Oblast možných řešení je silně omezena
- Každé z řešení je značně univerzální
- Vliv bezpečnostních opatření je vyjádřen jako snížení pravděpodobnosti výskytu hrozby nebo snížení vlivu hrozby

Určení míry zranitelnosti komponenty (VULAN)

- Oblast zranitelnosti
- Míra příležitosti útočníka a znalostí útočníka
- Čas potřebný pro útok
- Vybavení potřebné pro útok
- Výsledkem je zjištěná míra zranitelnosti komponenty

2. Generace – Mechanistické inženýrské metody

- Dělení složitých řešení na podúlohy a části
- Zobrazují problém do velkého množství částečných řešení
- Vývojové prostředky: Návrh shora dolů
- Zjišťují odděleně: aktiva, hrozby, zranitelné místa

Model analýzy rizik
: volbu alternativ bezpečnostních opatření může výrazně usnadnit automatizovaný přístup založený na vhodném modelu

Struktura modelu analýzy rizik

- model systému - struktury systému, aktiva
- model chování - hodnoty aktiv, hrozby, zranitelná místa

Postup

- vytváření struktury aktiv a seskupování
- ohodnocení zranitelných míst a hrozeb
- export modelu do expertního systému
- dotazník pro zjištění hrozeb
- práce s modelem
  - dotazování - uživatel klade systému dotazy a ten se snaží na základě aktuální báze znalostí odvodit správnou odpověď
  - prohlížení znalostí - umožňuje uživateli zobrazit bázi aktuálních znalostí
  - editace stávající báze znalostí

CRAMM (CCTA Risk Analysis and Management Method)

- obsahuje
  - Správa procesu analýzy rizik
  - Související dokumentace
  - Školení
  - Podpůrné softwarové nástroje
- Fáze
  - 1 - Aktiva
  - 2 - Hrozby, zranitelnost, rizika
  - 3 - Protiopatření

3. Generace - Logicko-transformační metody

- Vychází z toho, že model pro analýzu rizik musí znát nejenom strukturu systému ale i jeho funkčnost

4. Generace - Organizačně řízené metody

- Hledá se řešení i v netechnických oblastech

Kategorie: Státnice 2011 | Bezpečnost informačních systémů

- Stránka byla naposledy editována 19. 6. 2015 v 14:39.