Implementácia bezpečnostných opatrení pre zmiernenie rizík pri poskytovaní IaaS služieb v akademickom prostredí

Bc. Simona Husová
husova1@stud.uniza.sk
Vedúci: Mgr. Jana Uramová, PhD.

Aplikované sieťové inžinierstvo
Katedra Informačných Sietí, FRI UNIZA
Univerzitná 8215/1, 010 26, Žilina

Štandardy:

- ISO 27001
- ISO 27002
- ISO 27005
- Zákon o KB 69/2018

ANALÝZA A ZMIERŇOVANIE RIZÍK

KIS Bezpečnostná dokumentácia

- Aktuálny stav zabezpečenia KIS FRI UNIZA
- Komplexný dokument spísaný na základe ISO štandardov, GAP analýzy a interných dokumentov

KIS Postupy riešenia KBI

- Pravidlá pre klasifikáciu KBI, ich zistenie, hlásenie, eskaláciu, vyšetrovanie a reakciu na tieto incidenty
- Dokument spísaný na základe ISO štandardov a interných dokumentov

Oprávnenia a zodpovednosti administrátorov KIS CC

- Oficiálny dokument spísaný na základe RACI matice
  - R = responsible
  - A = accountable
  - C = consulted
  - I = informed

Inventarizačné nástroje

- automatický sken aktív, pre následný manažment rizík

Lansweeper

- Agent/Agentless
- Automatický sken aktív
  - Scanning Targets
  - Asset Radar
- Široká škála typov aktív
- Odhalenie zraniteľností (na základe SQL kódu pre report aktív)
- Import/Export aktív a reportov
- Odlíšenie skenovaných a manuálne pridaných aktív
- Skenovanie zaťaženia aktíva (CPU, memory, disk, network)
- Detailné informácie aktív (Windows 10 – typ aktíva , OS, výrobca, RAM, procesor, základná doska, grafika, zvukové a sieťové karty, úložisko, antivírus, nainštalovaný SW a jeho verzie, licenčné kľúče, história využívaných aplikácií)

Nástroje pre manažment rizík

- Aktíva, hrozby, zraniteľnosti
- Stanovenie rizika a jeho mitigácia

SimpleRisk
SIMPLE. EFFECTIVE. AFFORDABLE.

- User-friendly prostredie
- Žiadna preddefinovaná DB aktív
- Slabý zber informácií z automatického skenu aktív
- Hierarchické usporiadanie aktív
- Nerozlišuje zraniteľnosti a hrozby
- Viacero metód ohodnotenia rizík
- Import/Export ako platená doplnková služba

cases MONARC

- User-friendly prostredie
- Preddefinovaná DB aktív, rizík, zraniteľností
- Rozdelenie aktív na primárne a sekundárne
- AGPL 3.0 licencia
- Len 3 role používateľov
- Žiaden automatický zber aktív
- Možný import/export ale len v konkrétnej forme Monarcu
- Výpočet rizika na základe CIA triády a ROLFP
- Vypracované detailné dokumentácie ako pracovať s Monarcom