Hannibal pred bránami! Alebo už za...?

Ján Kromel

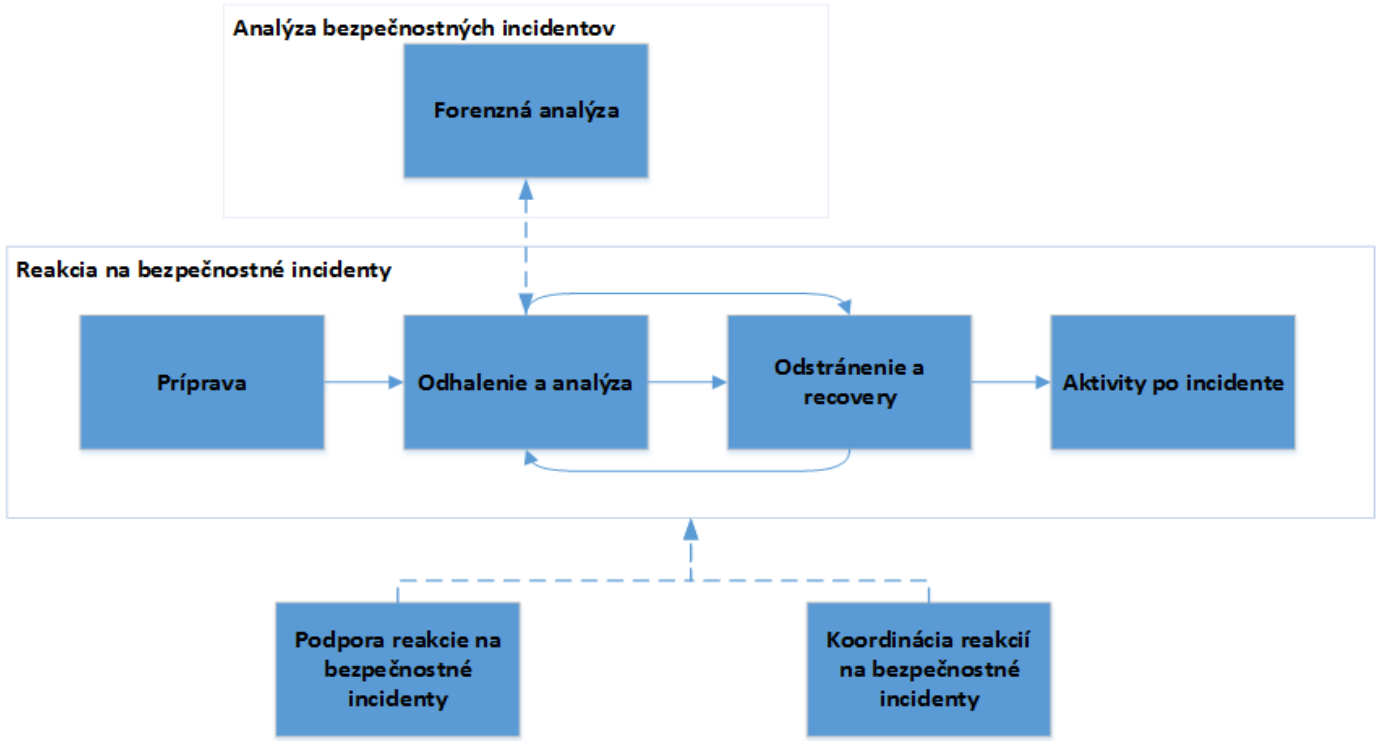
LYNX – niečo málo o nás...

- Založená v roku 1991
- Sídlo v Košiciach, od roku 1995 pobočka v Bratislave
- V súčasnosti vyše 100 zamestnancov
- Certifikácia NBÚ na prácu s utajovanými skutočnosťami
- Vypracovanie analýzy rizík, BCM a projekty ochrany osobných údajov/GDPR
- Súčasné trendy – zameranie na penetračné testy, komplexnú ochranu, manažment rizík, forenznú analýzu a strojové učenie
- Člen Združenia bezpečnostného a obranného priemyslu Slovenskej republiky (ZBOP) kde vedieme stálu komisiu o kybernetickej bezpečnosti

“Klasická” forenzná analýza

- Zaužívaný pohľad na forenznú analýzu
  - ✓ Súčasť procesu riešenia incidentov

Forenzná analýza = post-mortem



Proaktívna forenzná... Čo to...? ☺

- Viac pohľadov, ale v kontexte dnešnej prezentácie:

  Kontinuálny zber, uchovávanie a analýza údajov s „**predpokladom, že incident už nastal**“ (ideálne bez prerušenia činnosti)

- Vybrané príklady využitia
  - ✓ „Vyšetrenie“ anomálií (chyba vždy nemusí predstavovať „IBA chybu“)
    - ✓ Nárasty (aj sporadické) požiadaviek na hw zdroje, napr. CPU
    - ✓ Anomálne reštarty
  - ✓ Analýza existujúcich údajov
    - ✓ „Behaviorálna“ analýza aktivít používateľa – aktivity o ktorých netušíme ☹
    - ✓ Analýza súborového systému na identifikáciu odstránených súborov
    - ✓ Identifikácia neautorizovaného sw spúšťaného napr. z USB zariadení
    - ✓ Analýza sieťovej prevádzky
    - ✓ Analýza aktivít systémových účtov
    - ✓ ...
- Nepodceňovať ani incidenty s „nízkou“ dôležitosťou, resp. s nízkym dopadom
- Spoliehanie sa **IBA** na signatúry, prednastavené use-cases alebo výrobcom deklarované mechanizmy poskytuje falošný pocit bezpečia a teda „**Dôveruj, ale preveruj!**”

Ako na to?

- Príprava/úprava prostredia pre zber a uchovávanie údajov ako napr.:
  - ✓ Zabezpečenie centralizovaného logovania, uchovávania záznamov (vrátane logovania jadra operačného systému, powershellu a súborového systému) (samozrejme následná analýza ☺)
  - ✓ Profilovanie a tvorba „baseline“
  - ✓ Design infraštruktúry s ohľadom na potreby forenznej analýzy (napr. „forenzne priateľské“ súborové systémy ☺)
  - ✓ Implementácia IDS (ale spoliehať sa iba na samotné riešenie nestačí)
- Zabezpečenie personálnych zdrojov...
- Automatizovaná / semiautomatizovaná / manuálna analýza
- „Čerešnička na torte“ - honeypody
  - ✓ „Aktívny“ pohľad na záujem o prostredie z pohľadu útočníkov
  - ✓ Štúdium správania sa útočníkov
  - ✓ Prenos informácií na overenie aktuálnej bezpečnosti prostredia

Príklady benefitov...

- Zabezpečenie preliminárnych a „volatílnych“ dôkazov
- Odhalenie vektorov útoku, ktoré sú „pod radarom“ v súčasnosti aplikovaných mechanizmov, napr. APT, interný útočník
- Kontinuálne zvyšovanie bezpečnosti prostredia na základe úprav existujúcich nastavení a procesov po výsledkoch z analýzy
- Pravidelné testovanie procesu riešenia bezpečnostných incidentov
- Zdokonaľovanie sa v metódach forenznej analýzy
- Optimalizácia času forenznej analýzy v rámci procesu riešenia incidentov

Ťažko na cvičisku, ľahko na bojisku...

Na záver...?

Namiesto mlátenia prázdnej slamy a rekapitulácie už povedaného:

„Ak poznáš nepriateľa i seba samého, nebudeš porazený. Ak nepoznáš nepriateľa, ale poznáš sám seba, máš 50% šancu na víťazstvo. Ak nepoznáš sám seba, ani nepriateľa, prehráš.“

Sun Tzu

Ďakujem za pozornosť

jan.kromel@lynx.sk