Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Riešenie bezpečnostných incidentov

Jaroslav Janáček
Jún 2013

KPMG
cutting through complexity™

Bezpečnostný incident

- narušenie alebo bezprostredne hroziace narušenie bezpečnostnej politiky alebo iných požiadaviek na bezpečnosť
  - prienik útočníka do systému
  - znefunkčnenie služieb systému (napr. DDoS)
  - inštalácia škodlivého kódu
  - krádež počítača
  - ...

Spôsoby útokov

- priame napadnutie zraniteľnej služby
  - aplikácia, OS, ...
- nepriame napadnutie zraniteľného systému
  - s (nevedomou) pomocou interného používateľa
    - škodlivý kód, sociálne inžinierstvo
    - e-mail, web, ...
- zneužitie oprávnení
  - používatelia, administrátori, pomocný personál

Spôsoby útokov

- uhádnutie hesiel
  - slabé heslá
  - úplné preberanie
- násilné činy
  - vlámanie
  - krádež
  - vydieranie oprávnených používateľov

Riešenie bezpečnostných incidentov

- príprava
- detekcia incidentov
- obnova štandardnej prevádzky
- zhodnotenie

Príprava na riešenie bezp. incidentov

- cieľ:
  - naplniť predpoklady pre ďalšie fázy
- zdroje
  - ľudia
  - technika
  - dokumentácia
  - procesy v organizácii

Ľudia

- odborne a technicky zdatní
  - operačné systémy
  - siete, bezpečnostné prvky
  - nástroje na analýzu
    - komunikácie
    - stavu OS
    - logov
- kompetencie

Technika

- počítače
- externé disky
- káble, sieťové prvky (napr. hub)
- telefóny
- inštalačné médiá
- analytické nástroje

Dokumentácia

- topológia siete
- servery
  - prevádzkované služby
  - konfigurácia
- bezpečnostné prvky
- pracovné stanice
- kontakty

Procesy v organizácii

- snaha o predchádzanie incidentom
- zabezpečenie aktuálnosti
  - dokumentácie
  - kontaktov
- jasne definované
  - postupy pre nahlasovanie incidentov
  - práva, povinnosti a zodpovednosť pri ich riešení

Detekcia incidentov

- priebežný monitoring
  - logy, IDS, IPS, SIEM, ...
- nahlasovanie neštandardného správania
  - používatelia musia vedieť, že ho majú hlásiť, komu, ako
- analýza a korelácia hlásení
  - s cieľom odlíšiť plané poplachy od reálnych incidentov

Príznaky incidentu

- nefunkčnosť systému
- zmenený obsah web-u
- nezvyčajná sieťová aktivita
- nezvyčajná záťaž systému
- nezvyčajné záznamy v logoch
- zmenené správanie systému

Riešenie incidentu

- ciele:
  - minimalizovať škody
  - zistiť rozsah incidentu
  - čo najskôr obnoviť štandardnú prevádzku
  - zabrániť opakovaniu incidentu
  - zaistiť dôkazy pre ďalšiu analýzu a pre prípadné právne kroky
- nie všetky ciele sú v súlade
  - treba jasne stanoviť priority

Minimalizácia škôd

- pretrvávajúci incident => väčšie škody
  - napadnutie ďalších systémov
  - poškodzovanie mena organizácie
- izolovanie systému
- vypnutie systému
- izolovanie iných (kritickejších) systémov

Izolovanie systému

- zabráni rozšíreniu incidentu na ďalšie systémy
- ale môže byť napadnutým systémom vnímané ako signál k zahladeniu stôp
  - môže viesť k ďalšiemu poškodeniu dát v systéme
- izolovanie iných systémov
  - ochrana pred rozšírením incidentu na ne
  - potenciálne bez povšimnutia primárne napadnutého systému

Vypnutie systému

- zabráni rozšíreniu incidentu na ďalšie systémy
- ale môže znemožniť získanie cenných údajov pre ďalšiu analýzu
  - cenné údaje môžu byť len v „živom“ systéme v pamäti
  - v prípade virtualizácie prichádza do úvahy vytvorenie snapshot-u systému, ktorý môže byť neskôr analyzovaný

Zistenie rozsahu

- podobné systémy môžu mať rovnaké zraniteľnosti
- úspešný prienik do systému alebo inštalácia škodlivého kódu je často cestou k napadnutiu ďalších systémov
- výskyt incidentu je preto dôvodom na dôkladnejšiu analýzu stavu iných systémov

Obnova štandardnej prevádzky

- obnova systému zo zálohy
  - ideálne riešenie, ak je aplikovateľné
- reinštalácia systému
- snaha o priame odstránenie zmien v dôsledku incidentu
  - nemáme istotu, že boli odstránené naozaj všetky zmeny

Zabránenie opakovaniu

- aplikovanie „záplat“ na systémový a aplikačný softvér po obnove zo zálohy / reinštalácii
- zmena autentifikačných údajov
  - ktoré mohli byť získané útočníkom počas incidentu
  - nie len týkajúce sa napadnutého systému
  - ale aj také, ktoré napadnutým systémom prechádzali / mohli prechádzať
- revízia nastavení OS, firewallu, IPS

Zaistenie a analýza dôkazov

- zaistenie kópií napadnutého systému
  - disku, pamäte
- záznam sieťovej komunikácie
- analýza v laboratórnom prostredí
  - identifikácia útočníka
  - identifikácia spôsobu útoku

Zhodnotenie

- po vyriešení incidentu
- identifikácia a odstránenie nedostatkov v procese riešenia incidentov
- identifikácia a odstránenie nedostatkov v zabezpečení systému

Outsourcing vs. interné riešenie

- výhody outsourcingu
  - najmä menšie organizácie si nemôžu dovoliť kvalifikovaný tím ľudí na riešenie incidentov
- nevýhody
  - externý subjekt musí mať detailné znalosti o interných systémoch, fungovaní organizácie, ...
  - externý subjekt musí mať prístup k systémom (aj citlivým)
  - kompetencie pri rozhodovaní

Má nám kto pomôcť?

- CSIRT.SK
  - poskytuje upozornenia na aktuálne zraniteľnosti
  - vie poskytnúť pomoc pri riešení incidentu
  - ponúka možnosť centrálneho zberu a korelácie bezpečnostných udalostí
  - pripravuje systém zdieľania informácií medzi podobnými organizáciami
    - incidenty, zraniteľnosti, odporúčania

Otázky a diskusia

Ďakujem za pozornosť