Nemzeti Média- és Hírközlési Hatóság

Az incidens mint lehetőség

Hogyan fordíthatunk előnyünkre egy felhasználói ballépést?

EIVOK 77

Barczi Tamás

A mi világunk

- Kis csapat, nagy szakterület
  - Támogató társosztályok
  - Jó kommunikáció
  - Sok oldalú kollégák

Egy eset bemutatása az operáció perspektívájából

- Hogy néz ki az incidens belső nézetből?
- Hogyan érinti a felhasználók munkáját?
- Mit tanulunk belőle?

Az incidenskezelés lépései

- Előkészületek
- Észlelés
- Analízis
- Elszigetelés
- Felszámolás
- Helyreállítás
- Tanulságok levonása

Előkészületek

- OSINT
- Publikusan elérhető adatok, leak DB-k
- Robosztus IT védelmi infrastruktúra
- Rendszer hardening, baselineok
- Felhasználók képzése
- Monitoring
- Folyamatok kialakítása és revíziója

Észlelés

- Nyitva tartjuk a szemünk
  - Monitoring
  - Felhasználói bejelentések
  - Partneri bejelentések
- Ebben az esetben NKI észlelte a kiszivárgott felhasználói adatokat

Analízis

- Részben a következő fázissal párhuzamosan
- Érintett szolgáltatások, szerverek és komponensek meghatározása
- Az érintett felhasználói fiókok vizsgálata
- Az információk továbbítása a társosztályok és a vezetés felé

Elszigetelés

- Amikor megfelelő mennyiségű információ áll rendelkezésre, elkezdjük az érintett szolgáltatások funkcióinak korlátozását, esetleg teljes leállítását
- Tűzfalszabályok módosítása, felhasználói fiókok felfüggesztése, eszközök leválasztása a hálózatról

Le és felszámolás

- Az incidens elszigetelése után az incidens okának megszüntetése
- Felhasználói adatok megváltoztatása, fiókok helyreállítása
- Biztonságos konfigurációk aktualizálása
- Patchek és hotfixek telepítése
- Tűzfalszabályok, vírusdefiníciós adatbázisok frissítése, felülvizsgálata

Helyreállítás

- A rendszerek vizsgálata és a fenyegetés felszámolása után a rendszerek rendes üzemelésének visszaállítása következik a társosztályok segítségével
- Mentésből visszaállás
- További biztonsági vizsgálatok
- Hypercare
- Egy teljes és végleges helyreállításhoz az előbbi fázisokon sokszor több alkalommal is végig kell menni

Tanulságok levonása

- A hat fázis után a munka gyümölcse:
  - Incidens összefoglalása, jelentések
  - Ajánlások megfogalmazása
  - Irányelvek, folyamatok és erőforrások fejlesztése

Esetünk konkrét kérdései

- Miért voltak kint a felhasználói belépési adataink a darkweben?
- Történt-e adatszivárgás?
- Miért nem mi vettük észre?
- Milyen folyamatbeli hiányosságaink voltak?

Mi változott? Hogyan lett ebből stratégiai előny?

- Felhasználói adatok felülvizsgálata
- Felhasználók oktatása a biztonságos jelszókezelésről
- Rendszerek felülvizsgálata
- Folyamatfejlesztési javaslatok
- Új technológiai beszerzések
- Új képességek létesítése

Nemzeti Média- és Hírközlési Hatóság

Köszönöm megtisztelő figyelmüket!