EGY ZSAROLÓVÍRUS ÁMOKFUTÁSA

Budai László – IT Biztonsági üzletág vezető

Nádor 30 éve RENDSZERHÁZ

ÉSZLELÉS

- Az egyik ügyfelünknél egy péntek reggeli napon a munkaállomások munkaképtelenek voltak.
- A felhasználók nem tudtak bejelentkezni.
- A helyzetfelmérés során megállapítást nyert, hogy a kiszolgálókat és munkaállomásokat egy titkosító vírus támadás érte, tette használhatatlanná.

KÁROK FELMÉRÉSE

- Antivirus megoldás gyártójának mérnökeinek felkérése a fájlok visszaállításának vizsgálatára
- Működésképtelen rendszerek felmérése (kiszolgálók, mentőszerverek)
- Megsemmisült adatok felmérése
- Munkaállomások felmérése
- Hálózati forgalom vizsgálata – szolgáltató bevonása
- Résztvevő területek: MS mérnökök, mentő megoldás vizsgázott mérnökei, IT biztonsági tanácsadók, Adatvédelmi tisztviselő

TÁMADÁSI VEKTOR FELÁLLÍTÁSA

- Sérülékeny szerveren futó szolgáltatás leáll a támadást követő 6. percben
- Mentőmegoldás leáll a zsarolóvírus aktivizálódását követő 15. percben Elsődleges és másodlagos mentőegységeken lévő adatok törlésre kerültek.
- Hypervisor-ok konfig állományai kerültek titkosításra
- DC, Exchange, Fizikai backup szerver, DC2, Sharepoint szerverek egymás után leálltak
- Zabbix, Mantis
- **A támadás az aktivizálódás előtt 2 nappal történt**

JELENTÉSI KÖTELEZETTSÉGEK

- Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet - NBSZ NKI
  - Hány számítógépet ért a támadás?
  - Történt-e adatvesztés illetve rendelkeznek-e a helyreállításhoz szükséges biztonsági mentéssel?
  - Amennyiben nem, mekkora az adatvesztés mértéke?
  - Milyen adatokat érintett az adatvesztés (pl.: XLS, DOC stb.)?
  - Milyen új kiterjesztést helyezett el a vírus a kódolt file-okon?
  - Van-e információjuk róla, hogy a támadás milyen módon történt (pl.: nyitott RDP port használata)?
  - Történt-e esetleges adatszivárgás az eset kapcsán?

JELENTÉSI KÖTELEZETTSÉGEK

- Nemzeti Adatvédelmi és Információszabadság Hatóság – NAIH
  - Hatósági űrlap kitöltése, szakaszos bejelentés
  - 72 órás határidő betartása

- Szervezet vezetőjének gyakori tájékoztatása

HELYREÁLLÍTÁS MEGTERVEZÉSE

- Rendelkezésre álló offline mentés vizsgálata. (3 héttel korábbi állapot)
- Kiszolgálók és alapszolgáltatást biztosító rendszerek visszaállítása ideiglenes környezetbe (hétfő reggeltől – szerda délutánig, majd a sharepoint és a többi rendszer
- Munkaállomások vírusellenőrzés és fájl átvizsgálást követően kerültek bekapcsolásra.

HIBÁK LEVONÁSA – FEJLESZTÉSI JAVASLATOK

- Mentési eljárások átalakítása – offline mentés
- Hálózati szegmentáció – kiszolgálók, munkaállomások, wifi, wifi guest
- Vírusvédelmi megoldásnál EDR funkció bevezetése
- Karbantartási eljárások átalakítása – frissítések telepítési lépéseinek
- Lokális adminisztrátori jelszavak feltérképezése, és megvonásuk

KÖSZÖNÖM A FIGYELMET

Budai László – IT Biztonsági üzletág vezető

Email: budai.laszlo@nador.hu
Telefon: +36 20 483 9237