ALF EXPERT TEAM

IT biztonsági incidensek kezelése

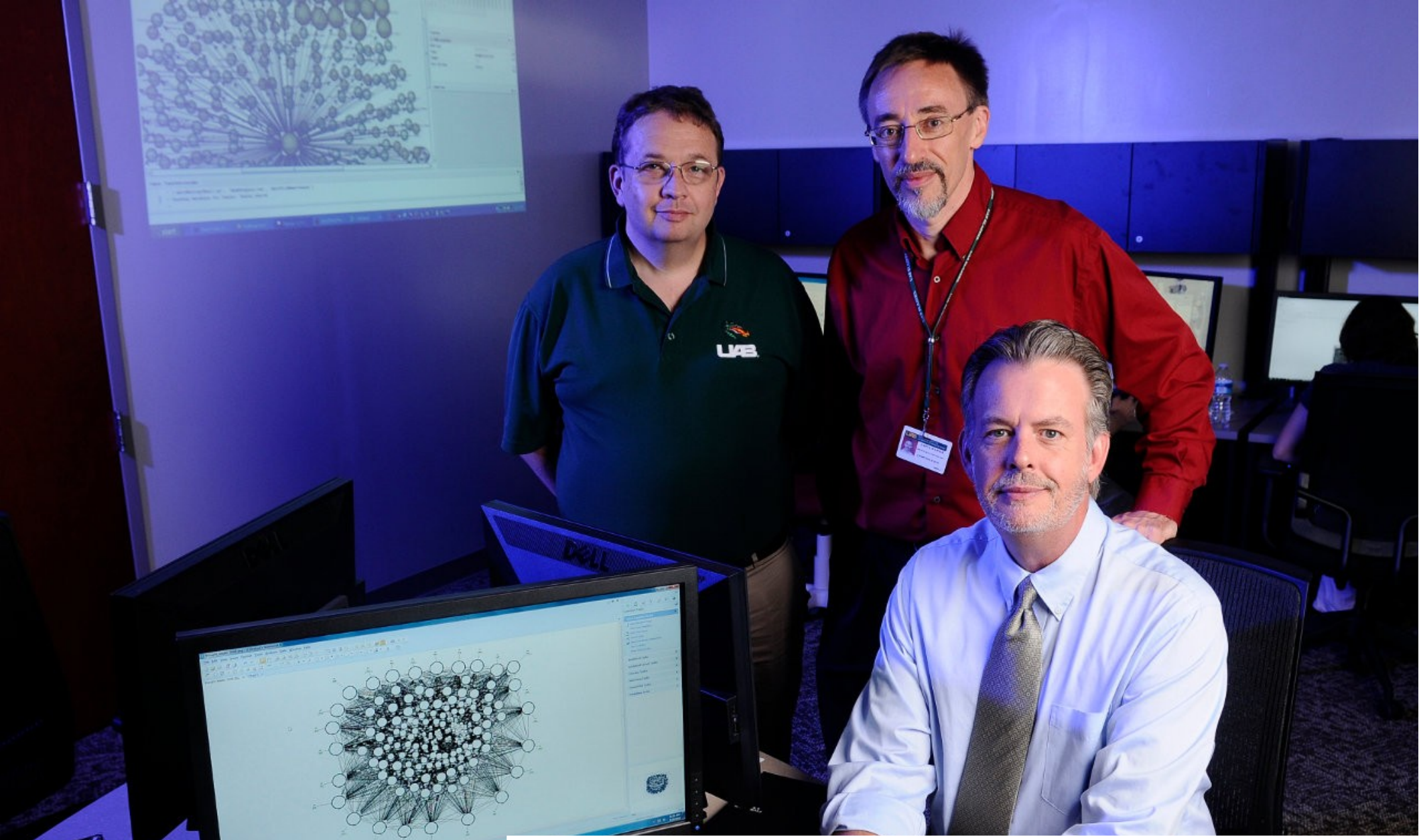
Mátó Péter <mato.peter@andrews.hu>

Betörtek a gépünkre.

Pánik!

A nyomozó csapat

Elvárások



A valóság

- Észre kell venni
- Meg kell állapítani,
  hogy mekkora a baj
- Elejét venni az esetleges
  újra behatolásnak
- Helyreállítani a rendszert

Elő-előkészületek

- cert.hu / cert.org tanulmányozása
- Különös tekintettel a
  Tanulmányok >
  Incidensek kezelése
  részre
- Wikipedia > Computer forensics

Előkészületek

- Telepítés után, még hálózat előtt archiválás
- Archiválás, rendszeres mentések
- Konfigok verziókezelőbe másik szerveren
- Helyi IDS, IPS
- Tűzfal, hálózati IDS, IPS
- Távoli naplózás
- Rendszeres napló elemzés (napi szinten!)
- DRP, Incidens kezelési terv

Helyi IDS-ek

- A helyi IDS-ek helyes használata
  - Rendszeres működés közbeni ellenőrzés
  - Tervezett leállítással egybekötött ellenőrzés
- Néhány helyi IDS szoftver
  - Open Source Tripwire
  - AIDE (Advanced Intrusion Detection Environment)
  - websitecds
  - saját megoldás (SHAn hash-ek tárolása, ellenőrzése)

Észlelés

- Szokatlan felhasználói azonosítók, jelszócserék
- Felhasználók szokatlan időpontban vagy helyről való belépése
- Szokatlan hálózati aktivitás (főleg bind)
- Szokatlan futó processzek
- Szokatlan időzített programok
- Gyanús (futtatható, ww) fájlok a rendszeren
- Gyanús naplóbejegyzések
- Rootkit ellenőrzők

Teendők

Ne ess pánikba!

További teendők

- Ne használjuk a gépet továbblépésre
- Független kommunikációs eszköz
  - Ha a számítógép rendszer kompromitálódott, akkor nem szabad számítógép alapú kommunikációt folytatni. Legalábbis azon a hálózaton.
- Diszkréció
  - Nem tudhatod, hogy ki a felelős
  - Csak a legfontosabbakat szabad bevonni
- Ha van incidens kezelési terv, akkor azt kell követni
- Ha nincs, akkor szakértőt kell hívni

Az első lépések

- Le kell húzni a gépet a hálózatról (vagy nem)
- Ki kell húzni a konnektorból (vagy nem)
- Teljes, bit szintű mentést kell készíteni

```
dcfldd if=/dev/sda
    of=/mnt/forensics_backup.dump bs=64M
```

- Ki kell deríteni, hogy hogyan jutottak be
  - Biztonsági hibás programokat keresve
  - IDS vizsgálattal
  - Naplók alapján

Hogy jönnek vissza?

- Megszerezték egy felhasználó jelszavát
- Új felhasználót hoztak létre
- Elindul egy támadó (szerver) program
- Időzítve elindul egy támadó program
- Módosítottak egy szerver konfigot
- Web alkalmazás módosítása
- DB módosítása (pl.: tárolt eljárások)
- Rendszeren lévő program lecserélése

Rejtőzködés

- Rootkit-ek, érzékelésük
  - Chkrootkit
  - rkhunter
  - OSSEC
- Rejtett könyvtárak
- Megváltozott fájlok (IDS segítségével)
- Más szerverek (helyi hálózaton vagy interneten)

Rejtett adatok felderítése

- Partícionálatlan, üres diszk területek
- EA mezők
- Ha látszólag valami nincs a diszken, attól még valójában rajta lehet
- Nem csak az elérhető fájlokban kell keresni
- Úgy kell tekinteni a diszkre, mintha nem lenne struktúrája

Hogy ne jöjjenek vissza

- Minden gépet meg kell vizsgálni
- Minden jelszót le kell cserélni
- Biztonsági rendszer felülvizsgálata, javítása
- Ha lehet, tiszta telepítés
- IDS adatok segítségével meg kell keresni, hogy melyik az utolsó hibátlan mentés
- Az adatokat tiszta mentésből kell visszaállítani
- Ha az újratelepítés nem opció, akkor a rendszert is mentésből

Elkerülés

- A nyilvános szolgáltatások legyenek hosting területen
- A nyilvános szolgáltatások legyenek DMZ-ben
- Csak azokat a szolgáltatásokat lehessen nyilvános hálózatról elérni, amit muszáj
- Csak csomagból frissülő szoftverek használata
- Támogatott rendszer használata (biztonsági frissítések)
- Rendszeres frissítés (ha lehet, automatikusan)
- Csak azok legyenek feltelepítve, aminek muszáj
- Szolgáltatások szétválasztása
- Hálózatok és szolgáltatások szétválasztása

Köszönöm a figyelmet!

Kérdések?