HunEx 2022 gyakorlat

2023.01.19.

A gyakorlat célja

- Incidenskezelési képességek gyakorlása
- Felkészülés egy komolyabb incidensre
- Kommunikációs csatornák tesztelése
- Kapcsolatok kialakítása, elmélyítése
- Belső eljárásrendek begyakorlása
- Sajtóval való kapcsolattartás gyakorlása
- Egyéb szereplőkkel való kapcsolattartás

Kerettörténet – a kezdet

- Minden résztvevő vállalat globális kibertámadás áldozatává válik (versenytársak, külföldiek is)
- Belső rendszereket, felhőszolgáltatásokat támadtak
- Nem működik a netbankolás, tranzaktálás, kártyás műveletek (ATM, POS, online)
- Pánikhangulat alakul ki a polgárok körében
- Elfogy a készpénz, boltok rohamozása, fizikai összetűzések

Kerettörtének – a támadás

- Salzonymus anarchista csoport támad, vezetőjük Salzenberg
- Egy komplex és újszerű wipert töltöttek fel a hálózatokba
- Alapos, több éves tervezés előzte meg a támadást
- Cél: monetáris rendszer eltörlése
  ⟶ só lesz az új fizetőeszköz
  - sóval behintett föld
  - Bírák könyve 9:45
  - Karthagó eleste

Kerettörtének – a támadás

Kerettörténet – a megoldás

- Egy sikeresen leválasztott gépen kell keresni a nyomokat (átadott VM)
- Több szálon a nyomozás (bankok, bankszövetség, hatóságok), kommunikáció és információ megosztás kiemelten fontos
- Elrejtett flagek a nyomok -> ezek dekódolása vezet el a bűnbanda rejtekhelyéhez
- A nap végén közös együttműködéssel elfogják a hatóságok Salzenberget

Gyakorlat infrastruktúrája

- Intézmények valós infrastruktúráját **semmiféle támadás** nem érte
- A szervezetek **incidenskezelő csapatként** vettek részt
- A cél az incidenskelezési és **NEM** az üzemeltetési képesség gyakorlása volt
- Kapcsolat az **infrastruktúrával NINCS**
- Technikai adat az infrától elkülönültén működik
- **Hírportál**
- **Közösségi oldal**

Résztvevők csapata

- Gyakorlatért felelős vezető (a gyakorlat szemszögéből vezető szerepben, a szervezet belső hierarchiája szerint nem feltétlen vezető) – 1 fő
  - Csapat koordinációjáért felelős
  - A sajtómegkeresés elsődleges címzettje
- Incidenskivizsgáló csapattag – 2 fő
  - Technikai incidensek kezelése
  - Fenyegetésmenedzsment
  - Kapcsolattartás
- „Sajtószóvivő” – 1 fő
- „Jogász” – 1 fő
- A feladatok megoldásába bevont emberek száma nem volt limitálva

A részvevők feladata I. rész

- **Bejelentések fogadása**
- **Fenyegetettség menedzsment**, a sajtó folyamatos monitorozása
- **Reaktív incidenskezelés**
  - Log elemzés
  - Káros kód elemzés
  - Összefüggések vizsgálata
- **Kapcsolattartás** a játékosokkal és a szereplőkkel
- **Ellenintézkedések** kidolgozása, megküldése (dedikált csatornára)

A részvevők feladata II. rész

- **Elemző csapat koordinálása** a szervezet belső eljárásrendje szerint
- **Vezetői döntések** előkészítése, végrehajtása a szervezet belső eljárásrendje szerint
- **Sajtómegkeresések kezelése**
  - Fogadása
  - Válaszok írása
  - A szervezet belső eljárásrendje szerinti kezelése
- **Kapcsolattartás** a külső partnerekkel (többek között az illetékes eseménykezelő központtal) a jogszabályi környezetnek megfelelően a gyakorlat eljárásrendjében foglaltak betartásával

A jövő

- Soha ne legyen szükség ezekre a tapasztalatokra!
- De ha mégis, akkor legyen az **eljárás gördülékeny, szakszerű, szabályoknak és normáknak megfelelő**!
- Mindenkit ösztönzünk a későbbi gyakorlatokon való részvételre
  - kollektív
  - ágazati
- Képességek és hiányosságok felmérése és javítása

Köszönöm a figyelmet!

Szász Péter