NEMZETI KIBERVÉDELMI INTÉZET

WWW.NKI.GOV.HU

HunEX 2019 Gyakorlat

NEMZETI
KIBERVÉDELMI INTÉZET

MARSI TAMÁS

A GYAKORLAT CÉLJA

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

KERETTÖRTÉNET

- Kiberbűnözés, életszerű forgatókönyv
- Célzott támadás, mindenki támadás áldozata

RÉSZTVEVŐK

(TERVEZET)

Állami Egészségügyi Ellátó Központ

Budapesti Közlekedési Központ Zrt.

E.ON Hungária Zrt.

ELMŰ-ÉMÁSZ Energiaszolgáltató Zrt.

Fővárosi Vízművek Zrt.

GIRO Elszámolásforgalmi Zrt.

Magyar Államkincstár

Magyar Fejlesztési Bank Zrt.

Magyar Közút Nonprofit Zrt.

Magyar Posta Zrt.

Magyar Telekom Nyrt.

MÁV Zrt.

Nemzeti Infokommunikációs Szolgáltató Zrt.

Nemzeti Közművek Zrt.

Nemzeti Útdíjfizetési Szolgáltató Zrt.

OTP Bank Zrt.

Telenor Magyarország Zrt.

Nemzeti Kibervédelmi Intézet (CSIRT-GFT, SOC)

GYAKORLAT INFRASTRUKTÚRÁJA

- Intézmények valós infrastruktúráját **semmiféle támadás** nem fogja érni
- A szervezetek **incidenskezelő csapat**ként vesznek részt
  - A cél az incidenskelezési nem az üzemeltetési képesség gyakorlása
- Kapcsolat az **infrastruktúrával NINCS**
  - Technikai adat – virtuális gép átadása történik
- **Hírportál**
- **Egyéb szereplők**

VIRTUÁLIS GÉP

- Gépigény (futtatva):
  - Kb. 130 GB adat (tömörítve (kb. 10 GB) kerül átadásra)
  - Virtuális gép futtatásra alkalmas eszköz
  - Kb. 6-8 GB szabad memória
  - OVA formátum
  - Virtualbox ismeri
  - Statikusan és dinamikusan is vizsgálható
  - Gyakorlat előtti napokban elérhető lesz

NKI SZEREPEI

- **Technikai részletek (különböző forrásokból)**
- **Sajtó**
  - Sajtómegkeresések
  - Hírek közzététele
- **Irányító hatóság**
- **NAIH**
- **CEO**
- **REST OF THE WORLD**
  - A gyakorlatban nem szereplő intézményeket helyettesíti
- **Játékszervezés**
  - Felügyeli a játék menetét
  - Kiküldi a játékszervezéssel kapcsolatos technikai információkat

RÉSZTVEVŐK FELADATA I.

- **Előzetes feladat:** kommunikációs csatornák tisztázása
  - Résztvevők adatai (név, telefonszám, email cím)
- **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)

RÉSZTVEVŐK FELADATA II.

- **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
- Ha valaki kérdez, arra válaszolni!

RÉSZTVEVŐK FELADATA III.

- Technikai feladat
  - A chain összeállítása
  - Az incidensek felderítése
  - Vezetői tájékoztatók készítése
  - CTF
  - Technikai adatok kinyerése
  - Megoldások a weboldalon keresztül küldhetőek be

RÉSZTVEVŐK CSAPATA

- 1 fő **gyakorlatért felelős vezető** (a gyakorlat szemszögéből játszik vezető szerepet, a szervezet belső hierarchiája szerint nem kell vezetőnek lennie)
  - Csapat koordinációjáért felelős
  - A sajtómegkeresés elsődleges címzettje
- 2 fő **incidenskivizsgáló csapattag**
  - Technikai incidensek kezelése
  - Fenyegetésmenedzsment
  - Kapcsolattartás
- Javasolt 1 fő „sajtószóvivő”
- A feladatok megoldásába bevont emberek száma nincs limitálva

GYAKORLAT LEFOLYÁSA

- Gyakorlat hetében **COMCHECK**
  - Sikertelen COMCHECK esetén ismétlés
- A gyakorlat tervezett napja: 2019.12.05 (csütörtök)
  - Kezdete (STARTEX): ~ 8:30
  - Vége (ENDEX): ~ 14:30
  - Feladatok (injectek) száma
    - Technikai: 8-10 db
    - Media: 8-10 db
    - Egyéb: 3-5 db
  - Ütemezés: kb. fél óránként újabb inject
  - A feladatok készen vannak
- Értékelés: 2020. januárban (írásban)

ELJÁRÁSREND - SOP

- Szereplők feladatai
- Kommunikáció módja
- Kommunikációs csatornák
- Kommunikáció szabályai
- Gyakorlat előtti héten átküldésre kerül minden partnernek

ADATKÉRÉS

- Cél: belső telefonkönyv
- Kör
  - Vezető
  - Incidenskezelők
  - Sajtósok
  - Egykapus kontakt
  - Sajtó kontakt
- Adatok
  - Telefonszám
  - E-mail cím
  - Publikus-e?

Köszönöm a figyelmet!

NEMZETI
KIBERVÉDELMI INTÉZET