



Kibervédelmi gyakorlat
Eljárásrend
2019.

Célja

A gyakorlat eljárásrendjének célja, a játék során alkalmazandó szerepkörök pontos tisztázása, a lehetséges kommunikációs csatornák azonosítása, valamint a gyakorlatban alkalmazandó kommunikáció módjának és szabályainak leírása, hatékonyabbá tétele.

Az eljárásrend a HunEX 2019 gyakorlatban részt vevő személyek (játékba bevont szervezetek és személyek valamint a szervezők) számára készült, annak érdekében, hogy a gyakorlatot egyértelmű szabályrendszer mentén tudják megvalósítani.

Szereplők

- **Játékos:** A gyakorlatban megkeresés alapján részt vevő szervezet kijelölt munkatársai, akiknek feladatuk az injectek alapján a gyakorlat megvalósítása, a gyakorlatban szereplő incidensek kezelése, sajtó megkeresések megválaszolása, valamint kapcsolattartás a gyakorlat szervezőjével és a részt vevő többi szervezettel. A játékosok által ellátandó szerepkörök:
 - gyakorlatért felelős vezető játékos: (a gyakorlat szemszögéből játszik vezető szerepet, a szervezet belső hierarchiája szerint nem kell vezetőnek lennie), aki a csapat koordinációjáért felelős, és a sajtómegkeresés elsődleges címzettje is.
 - incidenskivizsgáló játékos: a technikai incidensek kezelésével és a fenyegetésmenedzsmenttel foglalkoznak, tartják a kapcsolatot az üzemeltetéssel, egy szervezetnek kettő ilyen játékost kell delegálnia, de a játékba bevont (szervezeten belüli vagy kívüli) szereplők száma nincs korlátozva.
 - sajtókapcsolatért felelős játékos: opcionálisan kijelölhető szerepkör, a sajtómegkeresések címzettje lehet.
 - fontos kiemelni, hogy jelen gyakorlat során a résztvevők az infrastruktúrát nem birtokolják, közvetlenül nem érik el, tehát kizárólag a szervezet incidenskezelési és kommunikációs képessége kerül előtérbe, az üzemeltetéssel a játékosoknak nem kell foglalkoznia.
 - a Nemzeti Kibervédelmi Intézet CSIRT-GFT és SOC szakterületei is játékosként vesznek részt a gyakorlaton

NKI szervezési szerepkörei (a szervezők)

- **Monitor:** Megtervezi és lebonyolítja a gyakorlatot, felügyeli a gyakorlat menetét, kiküldi a játékszervezéssel kapcsolatos technikai információkat. A Nemzeti Kibervédelmi Intézet kijelölt munkatársai töltik be ezt a szerepkört.
- **Sajtó:** az elkészült „Gyakorlott Sajtó” hírportálon a gyakorlat erre delegált munkatársai közzéteszik a különböző, gyakorlat kerettörténetével kapcsolatos híreket, sérülékenység-információkat, valamint közvetlen sajtómegkereséseket intéznek (e-

mailben és telefonon) a szervezetek játékosai felé. A Nemzeti Kibervédelmi Intézet kijelölt munkatársai töltik be ezt a szerepkört.

- **Technikai segítségnyújtó szereplők:** több egymástól független forrásból, változatos helyekről érkező technikai segítség és megoldás közvetlenül a játékosokhoz. A Nemzeti Kibervédelmi Intézet kijelölt munkatársai töltik be ezt a szerepkört.
- **Felsővezetés:** Megjeleníti a játékos szervezet felsővezetését, döntés-előkészítést kezdeményezhet, jelentéseket, riportokat kérhet be. A Nemzeti Kibervédelmi Intézet kijelölt munkatársai töltik be ezt a szerepkört.
- **Irányító és adatvédelmi hatóság:** Megjeleníti a játékos szervezet irányító hatóságát, jelentéseket, riportokat, adatokat kérhet be. A Nemzeti Kibervédelmi Intézet kijelölt munkatársai töltik be ezt a szerepkört.
- **REST OF THE WORLD:** A szerepkör ellátója az összes, a gyakorlatban nem szereplő intézményt helyettesíti. Ha a gyakorlat résztvevőinek egy olyan partnerrel kell kapcsolatot létesíteni, aki egyébként nem vesz részt a játékban, akkor ezt az elérhetőséget kell megszólítani. A Nemzeti Kibervédelmi Intézet kijelölt munkatársai töltik be ezt a szerepkört.

Kommunikációs csatornák

A gyakorlat végzésének helyszíne, a szervezetek alaprendeltetés szerinti munkavégzésének helyszíne. A gyakorlat nem előbb kezdődik, mint 8:00 és nem tart tovább, mint 16:30.

A gyakorlat nyelve elsődlegesen magyar. Amennyiben a játékos belső nyelve az angol, a felsővezetés irányába így is kommunikálhat.

A gyakorlat során használt kommunikáció e-mailes és telefonos megnyilvánulási formára korlátozódik. Alternatív, bilaterális kommunikációs csatornák használata megengedett.

A gyakorlat hivatalosan a játékszervezés által e-mailben, minden résztvevőnek küldött úgynevezett „STARTEX” üzenettel veszi kezdetét és az „ENDEX” üzenettel fejeződik be.

A játékosok a gyakorlat során kizárólag a HunEX 2019 kontaktgyűjteményben szereplő e-mail címeken és telefonszámokon folytathatnak kommunikációt.

Minden kommunikáció (az írásbeli és a szóbeli is) a játékosok és szervezők között egyaránt az „EXERCISE EXERCISE EXERCISE” jelzéssel kezdődik és végződik a játék során, a következők szerint:

- **E-mail:** A játék részét képező injectek jelentős része e-mailesen keresztül kerül kiküldésre a játékosoknak. A gyakorlat keretén belül érkező e-mailek mindig az „EXERCISE EXERCISE EXERCISE” jelzések kezdődnek és végződnek. Az e-mailek tárgyát minden üzenetnél a „[HunEX2019]” előtaggal kell kezdeni, ezzel is támogatva a gyakorlat elkülönítését, valamint ezáltal könnyedén lehet az előtagra szabályt létrehozni.

- **Telefon:** A játék részét képező kommunikációs típusú injectek egy részét telefonos megkeresés útján juttatjuk el a játékosokhoz. A gyakorlat részét képező telefonos megkeresések az „EXERCISE EXERCISE EXERCISE” kijelentéssel kezdődnek és végződnek.
- **Kommunikációs portál:** A gyakorlatra létrehozott zárt rendszerben működő portál ahol fórumok segítségével kommunikálhatnak formálisan a játékosok.
- **Hírportál:** A „Gyakorlott Sajtó” a gyakorlatra létrehozott zárt rendszerben működő portál, amely az aznapi híreket és a gyakorlat részét képező híreket, valamint a gyakorlat kerettörténetét tartalmazza. Az „EXERCISE EXERCISE EXERCISE” felirat itt is megjelenik, de fontos kiemelni, hogy a jelölés nem a cikkekre, hanem a portálra vonatkozik, így a portálon megjelenő összes tartalom közül a játékosoknak kell kiszűrni a gyakorlat eseményeinek, valamint a kerettörténet releváns információit.

Kommunikáció szabályai

A gyakorlat során a játékosok a jelenleg hatályos jogszabályok, valamint saját szervezeti eljárásrendjük szerint járnak el.

Jelen eljárásrend, ezen szabályokhoz képest fogalmaz meg további figyelembe veendő szabályokat és szerepköröket, annak érdekében, hogy a gyakorlat során figyelemmel tudjuk követni a hatályos szabályok megvalósulását, működését és hatékonyságát.

- A játékosok feladata a bejelentések fogadása, jelzések monitorozása, valamint a reaktív incidenskezelés.
- Az incidenskivizsgáló szerepkörben lévő játékosok a saját szervezeti eljárásrendjüknek megfelelően tájékoztatják a gyakorlatért felelős vezető játékost az őket ért incidensekről, valamint vezetői döntéseket készítenek elő, terjesztenek fel számára.
 - Az incidenskezelést, az üzemeltetéssel való kapcsolattartást, valamint az ellenintézkedések megfogalmazását minden játékos a saját szervezetében érvényben lévő eljárásrend és szabályok alapján látja el.
- A gyakorlat során a játékosok a hatályos jogszabályoknak megfelelően az incidenseket haladéktalanul bejelentik az illetékes (játékosként megjelenő) eseménykezelő központnak, a gyakorlatban szereplő elérhetőségeken. A játékszervezésnek küldött tájékoztatás nem minősül bejelentésnek.

A játékosok a saját szervezeti szabályaikban foglaltaknak megfelelően kapcsolatba léphetnek más játékosokkal (pl. azonos szektor szereplőivel, akik szintén érintettek lehetnek az incidensben) a telefonkönyvben szereplő elérhetőségeken. A telefonkönyv elérhető lesz a kommunikációs portálon és minden résztvevő számára e-mailben előzetesen megküldésre kerül.

- Abban az esetben, ha a belső eljárásrendjük szerint a gyakorlatban nem résztvevő szervezetekkel vagy személyekkel kellene kapcsolatba lépni, kommunikálni (Pl: riasztások kiadása ügyfeleknek, vagy a szervezet kollégáinak tájékoztatása egy incidensről, a hírekben megjelent információk valóságáról, esetleg egy szolgáltatás nem működéséről), akkor azt a Rest of the World játékos (NKI) felé kell megvalósítani. Ennek köszönhetően az eljárásrendben szereplő előírásokat a játékosok maradéktalanul végre tudják hajtani, a gyakorlatban nem résztvevő, arról nem tudó személyek bevonása nélkül.
- A játékosok folyamatosan monitorozzák a sajtóportált a gyakorlat alatt.
 - A játékosok a hírportálon megjelenő híreket, az e-mailes és telefonos sajtó megkereséseket saját belső szervezeti eljárásrendjüknek megfelelően kezelik, válaszokat fogalmazznak meg.
- A játékosok folyamatosan kapcsolatot tartanak a gyakorlat szervezőivel, annak érdekében, hogy a szervezők a gyakorlat menetét és az eljárásrendben foglalt szabályok megvalósulását ellenőrizni tudják.
 - Ennek módja, hogy a játékosok minden a gyakorlat részét képező e-mailes (játékos-játékos közötti, játékos-üzemeltető közötti, játékos-eseménykezelő központ közötti, játékos – rest of the world közötti) kommunikációban, másolatban (CC) megjelenítik a gyakorlatszervezőket. Emellett a játék közben és végén lévő telefonos konferencián aktívan részt vesznek, az esetleges bilaterális telefonbeszélgetésekről, azok tartalmáról mindkét résztvevő tájékoztatja a gyakorlatszervezést.
- Ha a játékos valamilyen oknál fogva nem vesz részt tovább a gyakorlatban, akkor azt haladéktalanul jelezze a gyakorlat szervezőinek.

Traffic Light Protocol

A gyakorlat ideje alatt TLP használata szükséges az információmegosztás során.

TLP:RED

Vörös: csak a címzett olvashatja. Például egy találkozó esetén az elhangzott információ csak a jelenlévőkre tartozik. A legtöbb esetben a vörös jelzésű információ szóban, személyesen hangzik el.

TLP:AMBER

Borostyánsárga: korlátozott megosztás. A borostyánsárgával jelölt információk megoszthatóak az adott szervezeten belül, de csak azokkal, akiknek szükséges tudniuk róla.

TLP:GREEN

Zöld: közösségen belül terjeszthető. A zölddel jelölt információk bizonyos közösségen belül terjeszthetők. Nincs közzétéve teljesen nyilvánosan (például az Interneten). Ezek általában olyan hasznos információk, amelyek megoszthatóak partner szervezetekkel egy közösségen belül.

TLP:WHITE

Fehér: korlátok nélkül, nyilvánosan terjeszthető. Szerzői szabályokat betartva a fehérrel jelölt információk szabadon, korlátok nélkül terjeszthetőek