Kibergyakorlatok megvalósítási tapasztalatai

Korvin András Gábor

OTP Bank Nyrt.
Kibervédelmi Központ
osztályvezető

Andras.Gabor.Korvin@otpbank.hu

A gyakorlat témájának a kiválasztása

- A begyakoroltatni kívánt tevékenységet célszerű előre meghatározni és amennyiben lehetséges az éves tervezésben szerepeltetni, szervezeti egység szintjén – a szükséges szakértelem, technika és személyi állomány biztosításának az érdekében.
- A gyakorlat témájával összefüggésben minden érdekelt felet célszerű előre azonosítani – (pl. phishing, insider threat, IoT/célhardver, ransomware, 3rd party/supply chain/vendor, fizikai veszélyhelyzetek, komplex szituációs gyakorlatok/active threat).
- A kibertámadás következményeként fellépő fizikailag is manifesztálódó krízishelyzetek esetében szükséges azt tisztázni, hogy a gyakorlat során ezen következmények felszámolása is részét képezi-e a feladatvégrehajtásnak.
- Szükséges a gyakoroltatni kívánt főbb szervezeti funkciókat előre meghatározni – pl. tervezés, koordináció, menedzsment, kommunikáció, jog, compliance, hatósági kapcsolattartás, kritikus infrastruktúra védelme, üzemeltetés, ügyfélérintettség - panaszkezelés, stb.

A gyakorlat végrehajtásának biztosítása

- **Infrastrukturális feltételek - Hány funkcionális csoport vesz részt? Melyik csoportnak szükséges szeparált elhelyezés/hálózat, dokumentáció/virtuális war room, hangszigetelt fizikai war room stb.**
- **A gyakorlat dokumentációjának és sablonjainak előkészítése - pl.: jegyzőkönyv, üdvözlő levél, levelezési sablonok, jelentések sablonjai, stb.**
- **Kulcsszereplők belső telefonkönyvének összeállítása – nem csak a résztvevőké, hanem minden szóba jöhető szakértelemé vagy vezetési szinté is, amelyeket meg kell tudni szólítani.**
- **Támogatási feladatok azonosítás és dedikálása – pl. catering, jegyzőkönyvvezető, hálózati / AV támogatás, stb.**
- **A végrehajtás helyszíneinek bejárása – pl. ülőalkalmatosságok, asztalok, monitor, stb.**
- **Az igénybevételre tervezett állomány eligazítása 24-36 órával annak kezdete előtt és annak vezetői biztosítása, hogy a gyakorlat időtartama alatt ne kerüljenek más feladatba bevonásra.**

A gyakorlat végrehajtásának biztosítása

Az élet nem áll meg …

… ezért a gyakorlat időtartamára mindig gondoskodjunk független, a gyakorlatba nem bevont állományról és vezetésről a valós életben jelentkező incidenskezelési feladatok biztosításának az érdekében.

Ha és amennyiben lehetséges, gondoskodjunk párhuzamos kommunikációs csatornákról és szeparált fizikai elhelyezésről.

Gyakorlat közben

- **Önálló, a gyakorlattól függetlenített jegyzőkönyvvezető – a feladatok végrehajtásában nem érintett és a gyakorlatban nem animált résztvevőt célszerű választani – akinek a feladata az összes résztvevő minden tevékenységének és levelezésének, stb. összegyűjtése és időrend szerint jegyzőkönyvezése.**
- **A döntések meghozatalának időpontja legyen transzparens, hogy a szakállományt összefogó csoportok tudják, hogy mennyi idejük van egy adott döntés szakmai előkészítésére – a döntés lehet „most” (pl. emberélet veszélybe kerülése), lehet „majd” (pl. vezetői testület elé kell felterjeszteni és nincsen mód soron kívüli egyszemélyi döntésre), illetve lehet adott időpont is.**
- **Kis dolognak tűnhet, de … a mosdó, dohányzóhely és az ebédlő a lehető legközelebb legyen, minimalizálva a ki-, és beléptetést és az információszivárgást (pl. ebéd vagy dohányzás közbeni „na mi van” jellegű kérdések kapcsán).**

TAFE

- A tapasztalatfeldolgozás (After-Action Report/Improvement Plan) célja a felkészültségi szint felmérése, a gyakorlatban külön értékelhető elemek, mozzanatok, szaktevékenységek, stb. értékelése – az éles feladatvégrehajtásra való képességszint felmérése céljából.
- A TAFE célja nem a gyakorlat sikerességének a meghatározása, hanem az, hogy felmérjük, hogy szervezetünk képességein mit kell még javítanunk.
- A különböző gyakorlatokat célszerű azonos szempontrendszer és értékelési módszertan segítségével mérni, hogy azok alkalmasak legyenek a trendanalízisre is szervezeten belül.
- A gyakorlat céljait egyesével kell külön-külön értékelni, kiemelve az erősségeket és a fejlesztendő területeket.
- A gyakorlatban résztvevő különböző szervezeti egységek résztvevői közötti kommunikációt és együttműködést külön célszerű értékelni.

After-Action Close

- **Célszerű a felsővezetésnek előterjeszteni egy köszönőlevél javaslatot, a részt vevő Kollégák munkájának a megköszönésére.**
- **A TAFE érdekében a belső, közös értékelést minél előbb végre kell hajtani, hogy még élénk legyen a részt vevők emlékezete és ezekre támaszkodva tudjunk javítani a folyamatainkon.**
- **Meg kell teremteni annak a lehetőségét, hogy a gyakorlatot végrehajtó csoport vezetőjét is értékelhesse a beosztott állomány, mert máskülönben nem képesek felszínre kerülni az incidenskezelés vezetőjének hibái, tévedései, stb.**

Closing

Köszönöm a figyelmet !!!

Kérdések ?