OCEAN's 99

A GamingWorks üzleti szimulációja

ISMERŐSEK ÖNNEK IS AZ ALÁBBI KIHÍVÁSOK?

- Teljeskörű biztonságtudatosság
- Lehetőségek és kockázatok egyensúlya
- Hatékony kibervédelmi stratégia tervezése

Kibervédelem - Ellenállóképesség

Mi történik manapság a kibervédelem világában?

A nemzetközi Kibervédelmi Szövetség által kiadott jelentés szerint a cégek többsége nem rendelkezik megfelelő biztonság-tudatossággal és kibervédelmi ismerettel, egyúttal rávilágít a sürgetőbb informá-cióátadás és oktatás szükségességére is.

Az ISACA 2015-ös kiberbiztonsági státuszjelentéséből kiderül az is, hogy a cégek mindössze 38%-a vallja magát felkészültnek egy kifinomult számítógépes támadás kivédésére. Nem meglepetés tehát, hogy a vállalatok többségénél a "BIZTONSÁG" témaköre az informatikai vezetők egyik kulcsfontosságú problémája.

Az Axelos 'Resilia' néven megjelenő legújabb képzése komoly előrelépés a kibervédelmi oktatás és tanúsítás területén. Mindezek ellenére azonban, hiába a tudásba és készségebe történő befektetés, még mindig az emberek viselkedése és magatartása jelenti a legnagyobb kockázatot. A Cisco legfrissebb kibervédelmi jelentései azt mutatják, hogy a támadók a szerverek és operációs rendszerek kompromittálása helyett egyre jobban a felhasználói viselkedés kihasználására helyezik a hangsúlyt.

Az Ocean's 99 a legújabb üzleti szimulációs játékunk, melynek célja a kibervédelem tudatosságának és képzési program-jának támogatása, segítve a felhasználói hozzáállás és viselkedés megváltoztatását.

OCEAN's 99

Star of Africa

Jewish Bride

Bugatti 59

Az Ocean's 99-ről

"A Tokió Bank tulajdonosa úgy dönt, hogy három világhírű tárgyat állít ki a nagyközönség részére: a 'Star of Africa' gyémántot, a 'Jewish Bride' című festményt és egy 'Bugatti 59' típusú járművet. Ahhoz, hogy ez létrejöhessen, mindegyik tárgyat át kell szállítani a Tokió Múzeumba, ahol 4 hónapig lesznek a kiállítási darabok láthatóak. A kihívás tehát nem kevesebb, mint a tárgyak Tokióba szállítása, megfelelő biztonsággal és határidővel. Minden nap késéssel a bank és a múzeum komoly pénzügyi és presztízsveszteséget szenvedhet el. Ám nem árt az óvatosság sem, hiszen az Ocean's 99 bűnszervezet is nagyon nagy érdeklődést mutat a kiállítandó tárgyak iránt. Ráadásul emellett más, előre nem látható veszélyek is a aláásahatják az eredeti terveket."

Üdvözöljük az Ocean's 99 kibervédelmi üzleti szimulációban!

A szimuláció felépítése

Bevezetés

Először is bemutatásra kerülnek a szervezet konkrét tanulási célkitűzései. Ezt követően a csapattagok megismerik a tréning anyagait és a szerepköröket, annak érdekében, hogy azonosítani tudják feladataikat. A résztvevők mindegyikének konkrét szerepköre és felelőssége lesz a szimuláció során. A legfontosabb szerepkörök: Tokió Bank, Tokió Múzeum, biztonsági tiszt (CISO), projektmenedzser, IT támogatás, szállítmányozási menedzser, valamint a kiállítási tárgyak tulajdonosai Amsterdamból, Londonból és Las Vegasból.

Biztonságpolitika és kockázatértékelés

A csapat elsődlegesen meghatározza a szervezet biztonságpolitikáját. Közösen döntenek a stratégiáról, valamint egyeztetik a folyamatokat a szerepkörökkel és felelősségekkel. Utolsó lépésként meghatározzák a védendő, kulcsfontosságú vagyontárgyakat, eszközöket.

Ezt követően a csapat kockázatértékelést végez. Megvizsgálja a Tokiói Múzeum infrastruktúrájával, a projektmenedzserek folyamatkövető és a tárgyak helyzetét jelző rendszerével, valamint a tárgyak tulajdonosainak rendszereivel kapcsolatos fenyegetéseket és kockázatokat. A csapatnak korlátozott költségvetése van arra, hogy tanácsadást vegyen igénybe vagy teszteket hajtson végre a különböző rendszerek sebezhetőségének elemzésére. Ennek eredményeként a csapat dönthet úgy, hogy befektet fejlettebb rendszerekbe, szoftverbe, szabályozásba vagy eljárásokba.

A csapat megtervezi és jóváhagyja azon kibervédelmi támogatói folyamatokat, amelyek felhasználásra kerülnek a szimuláció során.

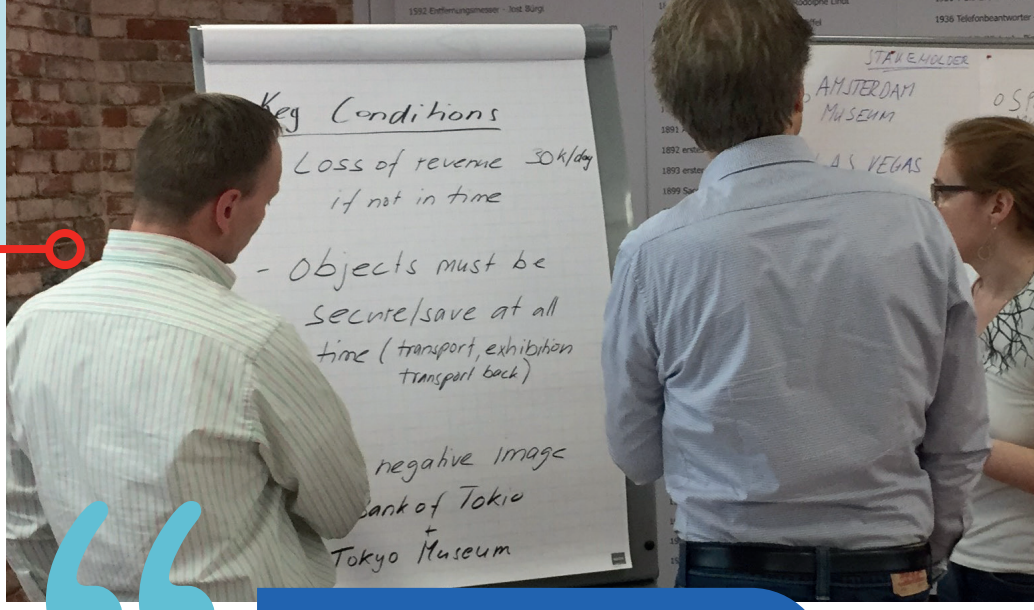
Tudatosság

A tervezés befejeztével a csapatnak fel kell készülnie a szimuláció következő fázisára. El kell dönteniük, hogy mi szerepeljen a tudatossági kampányban és hogyan legyen megszervezve annak terjesztése.

A műtárgyak mozgatása a múzeumból a helyi repülőtérre

Ez a szimuláció első fordulója, amelyben teszteljük a csapat által összeállított tervet. Cél a műtárgyak eljuttatása a helyi repülőtérre. Ebben a körben a csapat valós kibervédelmi eseményekkel szembesül majd, amelyeket egyrészt azonosítani, másrészt kezelni szükséges. Az események megoldására az IT támogatás számos lehetőséget kínál, egyes megoldások csúszáshoz vezethetnek, míg mások költségesek lehetnek. A csapatnak meg kell találnia a megfelelő egyensúlyt a projekt (a kiállítás időben történő megnyitása) és a biztonság között (minimalizálja a kockázatokat és a hatásokat).

A játék forgatókönyvei, eseményei és incidensei konkrét biztonsági jelentéseken és a leggyakoribb megállapításokon alapulnak, annak érdekében, hogy a szimuláció reális és releváns ismereteket adjon a résztvevőknek.



Kiértékelés és fejlesztés

Az első fordulót követően a csapattal megvitatjuk a tapasztalatokat. A 4P-re fogunk hagyatkozni. Példa ezen elemekre vonatkozóan:

» **EMBEREK:** a tudatosság, a szabályozás és eljárások megértése, valamint annak hatása, ha nem követjük azokat; kommunikáció, visszacsatolás a viselkedésre való összpontosításról; ismeretek és készségek a biztonsággal kapcsolatos tevékenységek elvégzéséhez

» **FOLYAMAT:** vajon a biztonságpolitika, a folyamatok és az eljárások valóban céljuknak megfelelőek voltak és használatra alkalmasak; az eljárások kapcsolódtak-e valamihez?

» **TERMÉK:** a biztonsági események és incidensek felderítésre és bejegyzésre kerültek? Fel lett-e bármilyen termék használva a detektálásra, megelőzésre vagy helyreállításra vonatkozóan?

» **PARTNER:** a partneri és beszállítói képességek mindegyike össze volt hangolva a végpontok között?

A aktuálisan kiértékelésre, átbeszélésre kerülő elemek és témák testreszabhatók, hogy megfeleljenek a szervezet sajátos kihívásainak és tanulási céljainak. A kiértékelést követően a csapat közösen elfogadja és végrehajtja a kibervédelmi képességekre vonatkozó fejlesztéseket.

A tárgyak reptérről történő átszállítása a múzeumba

Ez az utolsó forduló. A csapat az előzőekben elfogadott fejlesztések és ellenintézkedések végrehajtását követően az aktuális biztonsági szintjének megfelelő, újabb eseményekkel és incidensekkel szembesül majd. Ha minden rendben megy, remélhetőleg a kiállítás megnyitását ünnepelhetjük.

Lezárás és a tanulságok

A szimuláció a tanulságok levonásával és a napi munkavégzésre vonatkozó bevált gyakorlatokkal zárul.

> *A szimuláció szembesített bennünket azzal, hogy mekkora károkat okozhat ha egy szervezet megbízhatatlan információkra (OCEAN's 99 hekkelés folytán) alapozva hozza meg üzleti döntéseit.* - **CISO**

Miért szimuláció?

A legtöbb képzés elméleti és tudásalapú. Általánosságban elmondható, hogy a biztonsági incidensek legfőbb okozói az EMBEREK. Ez függ a hozzáállásuktól, viselkedésüktől, kommunikációjuktól vagy akár a folyamatokban és eljárásokban történő együttműködésüktől. Hiába találjuk ki a világ legjobb szabályozását, ha a felhasználó mindezt figyelmen kívül hagyva hazaviszi az érzékeny adatokat tartalmazó USB-kulcsot.

A szimuláció ideális eszköze az elméleti ismeretek gyakorlatba történő átültetésének, ugyanakkor a "hozzáállás" (megértés, beolvadás, betekintés) és "viselkedés" (a nemkívánatos felismerése és elkerülése, illetve a kívánt megismerése és megtapasztalása) elméletét egy interaktív csapatmunkában ötvözi. A 10-12 résztvevőből álló csapat *(gyakran különböző szervezeti egységek)* képviselőinek közösen kell megtervezniük, végrehajtaniuk és fejleszteniük a munkamódszereiket ebben a szimulált környezetben. A csapattagok láthatják és tapasztalhatják a teljes működési láncolatot és azok kölcsönös függőségeit.

Minden résztvevő saját tudással és tapasztalattal vesz részt a szimulációban. A tréning során közvetlen visszajelzést kap mindenki a tréning környezetéről és a meghozott döntésekről. A szimuláció több fordulóból áll, így a résztvevőknek folyamamatos fejlesztésre van lehetőségük, ezáltal ismerve meg a javító intézkedések szükségességét. Mivel a szimulált környezet és a tréning során előforduló események tényleges interakciót kívánnak, a képzés befejeztével ezen berögzült, konkrét ismeretekkel térhet haza a résztvevő, ezáltal sokkal gyorsabban elsajátítva a kibervédelmi tudnivalók gyakorlatát.

Célközönség

A szimuláció az alábbi 8-12 fős csoportok részére hasznosítható:

VEZETŐI TESTÜLETEK

A résztvevőkkel a biztonságpolitikai és kockázatértékelési gyakorlatot végrehajva elérhetővé válik a szervezet aktuális kibervédelmi állapotának megértése.

1½ óra

IT CSAPATOK

A teljes szimuláció során a résztvevők világos képet kapnak a kibervédelem vonatkozásában együttműködő, az informatikai szolgáltatásokkal és folyamatokkal kapcsolatos összes területről.

1 teljes nap

VÉGFELHASZNÁLÓK

A résztvevők megtapasztalhatják a kibertámadások, fenyegetések és tevékenységek következményeit, valamint a biztonságpolitikának megfelelő hozzáállás és viselkedés szükségességét.

2½ óra

Tanulási célok:

- Tudatában lesz, mennyire fontos a kibervédelem és a kiber-ellenállóképesség egy szervezet számára.
- Átfogóbb képet kap a saját szervezetét fenyegető veszélyekről, kockázatokról és gyengeségekről.
- Megérti a kibervédelem és kiber-ellenállóképesség lényegét, meghatározásait, szerepét, felelősségét és terminológiáját.
- Tudását és ismereteit felhasználva felmérheti a saját szervezetének kibervédelmi szempontból aktuális érettségi állapotát.
- Megismerheti, hogyan tudja megfelelően a kibervédelmi folyamatokat a saját szervezetében létrehozni és támogatni.
- Láthatóvá és tapasztalhatóvá válik ön és kollégái számára, hogy mennyire kritikus tényező a "hozzáállás" és "viselkedés" a kibervédelem területén.

Ismerősek Önnek is az említett célok?
Bővebb információért keresse partnerünket!

Vályi-Nagy Péter
üzleti szimulációs instruktor
+36-30-830-8174
valyinagy.peter@uzletiszimulaciok.info

version 3