Útmutató Digitális Biztonság képzéshez Asztalnál végzett gyakorlatokkal (Tabletop Exercises - TTX)

Célok és bevezetés

Ez az útmutató 11 digitális biztonságra összpontosító asztali gyakorlatsor (TTX) forgatókönyvéhez tartalmaz segítséget. Az útmutatót bárki használhatja, aki szeretne TTX feladatsorokat tervezni, vagy TTX workhsopokat tartani a digitalis biztonságról. Ebben a kis útmutatóban rövid leírásokat találhattok arról, hogy mi is az a TTX, miért lehet hasznos a digitális biztonsag képzések során, és hogy tud valaki tervezni, továbbfejleszteni, és tartani TTX foglalkozásokat.

Azt a 11 forgatókönyvet, amit ez az útmutató tartalmaz, az Internews Journalist Security Fellowship (JSF) projektjében részt vevő közép- és délkelet-európai újságírókkal közösen fejlesztettük ki, akik a régióban tartott képzéseiken már használták is ezeket a közösen kidolgozott forgatókönyveket. Ezeket a minta TTX-eket, amelyek közül néhányat közép- és délkelet-európai országokra is lokalizáltunk, és lefordítottunk emellett arab és spanyol nyelvekre is, az itt található linken érhetitek el.

Ezt az útmutatót kifejezetten az újságírók és a hírszerkesztőségek részére tartott digitalis biztonsági képzésekhez hoztuk létre. De hasznos lehet más célközönség számára készült TTX-ek tervezésénél is.

Mi az a TTX? Miért értékesek a TTX-ek?

A TTX egy forgatókönyv-alapú képzési módszer. Amit a leggyakrabban interaktív beszélgetések formájában valósítunk meg. Ezzel pedig lehetőséget adunk a képzés résztvevőinek, hogy úgy tréningezzenek, hogy az újonnan megszerzett tudásukat és készségeiket alkalmazzák egy általunk kitalált szituációban (ezekre a szituációkra TTX-forgatókönyvekként vagy jelenetekként fogunk hivatkozni). A forgatókönyvek nagyon hasonlítanak azokra a valós szituációkra, amelyek a való életben is előfordulhatnak az újságírókkal. A TTX forgatókönyvek széles spektrumát lefedik az ujságírók biztonságával kapcsolatos lehetséges eseteknek: a szerkesztőségi házkutatásoktól kezdve az adatszivárogtatáson át a doxingig. Amíg a hagyományosabb képzési módszerek csupán bizonyos technikai készségek és ismeretek átadására összpontosíthatnak, a TTX a következőkben segíthet még:

- Az újságírók biztonságával kapcsolatos problémák kezelésének gyakorlása biztonságos környezetben.

- Kritikus viták ösztönzése a digitális biztonsági kérdésekről, és arról, hogyan lehet ezeket a legjobban megközelíteni különböző kontextusokban és helyzetekben. Ez különösen hasznos lehet azoknak a résztvevőknek, akik rendszeresen dolgoznak együtt. Számukra így alkalom adódik végiggondolni, hogy min lenne érdemes változtatniuk a biztonságuk érdekében.
- Felmérni, hogy az újsagíró, illetve a szerkesztőség mennyire készült fel arra, hogy megbírkózzon azokkal a biztonsági problémákkal, amikkel találkozhat.

A TTX lényege, hogy azonosítsa az egyéni, szervezeti és közösségi hiányosságokat a tudás, az erősségek és a korlátok terén. A sikeres TTX túlmutat az eszközökön és az alapvető gyakorlatokon, és rávilágít arra is, hogy mely eljárások vagy szabályzatok hiányozhatnak, vagy melyeket kell javítani.

A TTX-ek akkor a leghatékonyabbak, ha kiegészítőként használják azokat más tréningezési módszerek javítására. Ennek oka, hogy a TTX-ek célja nem az az elsősorban, hogy új készségeket és ismereteket adjon at. Hanem az, hogy még jobban elmélyítse a tanulást a forgatókönyv-alapú gyakorlatokon, megbeszéléseken és értékeléseken keresztül.

TTX-forgatókönyv-dokumentumok összetevői

A 11 TTX jelenet mindegyike többnyire Sára személyén alapul, amit felvázolunk ebben az útmutatóban. Emellett minden jelenet tartalmazza a következőeket:

- Cél – A TTX-forgatókönyv átfogó célja.
- Tanulási célok – Lehetőségek az általános tanulási célokra, amelyekre összpontosítani lehet a TTX során. A facilitátoroknak valószínűleg előnyös lenne, ha csak néhány tanulási célt választanának, amelyekre összpontosítanak.
- A TTX előtt vagy után edzendő készségek/viselkedések – Konkrét és specifikus készségek és viselkedésbeli változtatások lehetőségei a TTX segítségével. A facilitátorok számára előnyös, ha csak néhány készséget és viselkedést választanak ki, amelyekre összpontosítanak, és amelyek összhangban vannak a kiválasztott tanulási célokkal.
- Forgatókönyv — A következőket tartalmazza:
    - Bevezető háttértörténet, a történet megalapozása.
    - További információk, amelyek a történethez kapcsolódnak.
    - Kérdések és feladatok, amiket a résztvevők megvitathatnak, és megválaszolhatnak. A kérdéseket Q betűvel fogjuk jelölni, amit egy szám fog követni (pl. Q1, Q2, Q3 stb.).
    - A kérdések és feladatok alatt néhány lehetséges választ is feltüntettünk. Ezeket a válaszokat ne osszátok meg a résztvevőkkel a TTX foglalkozások alatt. Csupán a foglalkozást tartó személyeknek segítenek.
    - Néhany forgatókönyv tartalmaz Fordulatokat is, (Injects) amiket “Fordulat” felhívással fogunk jelezni. A fordulat ebben az esetben egy olyan új információ vagy esemény, amit a foglalkozást tartó személy ha szeretne, hozzáadhat a forgatókönyvhöz, hogy előre görgesse vagy komplexebbé tegye azt.

A TTX forgatókönyv kidolgozása

Tizenegy TTX-forgatókönyvet fejlesztettünk ki a JSF projekt keretében (amelyeket itt belinkeltünk). Ezeket bárki módosíthatja, így jobban illeszkedhetnek a közösségük képzési igényeihez. De bárki létrehozhatja a saját egyedi forgatókönyvét is. Ha saját TTX forgatókönyvet szeretnél létrehozni, vagy egy már meglévőt átalakítani, akkor a következőeket érdemes figyelembe venni:

A tanulási célokat a tervezési szakasz elején meg kell határozni. Ezeknek a tanulási céloknak ki kell egészíteniük egymást, és logikai sorrendet kell követniük a tanulást illetően, továbbá fontossági sorrendet kell felállítani közöttuk, illetve kapcsolódniuk kell a TTX fő céljához is. A képzési folyamat leegyszerűsítéséhez, és ahhoz, hogy a TTX sikerességét könnyebben lehessen mérni, majd kösd össze a tanulási céljaidat olyan konkrét készségekkel és viselkedésmódokkal, amelyekre a résztvevőknek a TTX során összpontosítaniuk kell. Ideális esetben ezeket a tanulási célokat és a konkrét készségeket a résztvevők szükségletei és készségszintjei alapján fogod meghatározni. Lehet az is, hogy már ismered ezeket, ha olyan közösséggel dolgozol, amelyet már jól ismersz. Alternatív megoldásként szükséged lehet kezdeti igényfelmérés elvégzésére is. Például interjúk vagy előzetes felmérés segítségével, hogy összegyűjtsd ezeket az információkat, ha kevésbé ismered a résztvevőket.

A forgatókönyvnek mindig a lehető legközelebb kell állnia a valós élethez, de nem szabad benne megnevezni valós személyeket vagy szervezeteket. Valós helyzetekre, kihívásokra és tapasztalatokra koncentrálj amikor készíted. Ritka esetekben helyénvaló lehet valós helyek használata, de figyelembe kell venned a biztonsági kockázatokat, és az ezzel járó kockázatokat is ezzel kapcsolatban. A valós helyek felsorolása azt jelentheti például, hogy az emberek túl sok időt töltenek azzal, hogy emlékezzenek vagy kutassanak rájuk vonatkozó részletekre, és kevésbé fognak összpontosítani a forgatókönyvre.

A bonyolultság szempontjából a forgatókönyv nem árnyékolhatja be a tanulást, és nem vonhatja el a figyelmet. A választási lehetőségek segíthetnek a résztvevőknek megérteni döntéseik hatását, de ne feledd, hogy a komplexitás és a választási lehetőségek növelése megnehezíti a TTX felépítését, és az egész gyakorlatot is sokkal hosszabbra növeli.

Az időt is használd tervezési elemként a forgatókönyv során. Például időket rendelhetsz a TTX során bekövetkező eseményekhez, és időhöz kötött kérdéseket tehetsz fel, vagy visszatekintéseket vagy előreugrásokat is használhatsz. Tisztáznod kell az idő felhasználási lehetőségeket és időkereteket a forgatókönyv elején, és fenntartani az átláthatóságot az egész jelenet soran.

Képzőként a résztvevők képzettségi szintjétől, és a saját képzettségi szintedtől függően fontolóra veheted technikai elemek beépítését is a TTX-be. Ez azonban azt jelentheti, hogy a résztvevőknek egy adott eszközt, szoftvert vagy folyamatot is használniuk kell a TTX workshop soran. Ha technikai elemet is hasznalni fogsz, akkor hagyj több időt ezeknek a feladatoknak a végrehajtására, és mindig legyen tartalék terved műszaki problémák esetére is, vagy tedd opcionálissá, hogy alkalmazkodhass a résztvevők különböző képzettségi szintjeihez.

A TTX-en belül használhatsz fordulatokat is, ahogy azt már korábban említettük. Ezek a fordulatok lehetnek nagyobbak vagy kisebbek is, és függhetnek a résztvevőktől, de akár lehetnek függetlenek is tőlük. A fordulatokat általában hosszabb forgatókönyvekben használják, figyelembe véve a rájuk szükséges időt. A fordulatokat a képző adja hozzá a történethez, és az időzítésük kulcsfontosságú. A fordulatok jelenetbe történő sikeres integrálásához szükség van a képző további erőforrásaira a TTX képzés előtt és közben is. Ráadásul a fordulatok használatát össze kell hangolni az előre meghatározott tanulási célokkal is.

TTX Tervezése

Mielőtt elkezdenéd a TTX tervezését, gondolj a célközönségedre, és arra, hogy a célközönséged jellege hogyan hathat a tanulási célkitűzések kialakítására. Például az újságírókat, a hírszerkesztőség vezetőit, vagy a biztonsági embereket szeretnéd megcélozni a TTX-szel? Ha belegondolsz, mindegyikük más-más információkkal dolgozik, és különböző döntésekért felelős. Alternatív megoldásként az egyes TTX-ek egy sokkal szélesebb entitást is megcélozhatnak – például egy egész szerkesztőséget –, így jobban megérthetik a résztvevők, hogyan kommunikálnak és hoznak döntéseket a többiek a szerkesztőségen belül. Ne feledd, lehet hogy olyan résztvevőkkel fogsz dolgozni, akik nagyon eltérő szintű digitális biztonsági készségekkel, ismeretekkel és tapasztalattal rendelkeznek. Szánj ezért egy kis időt a TTX szerkesztőségre szabására, hogy az a legjobban megfelelhessen a résztvevők szükségleteinek.

Ha már megvan a célközönséged, tervezd meg a tanulási célokat! Figyelembe véve azokat a konkrét készségeket és viselkedéseket, amelyeket szeretnél átadni, és erősíteni. A konkrét készségek kiválasztása alapvető fontosságú ahhoz is, hogy oktatóként fókuszálni tudj. Illetve kézzelfogható tanulási célokat tűzz ki a résztvevők számára. De segít meghatározni a referenciaértéket is a képzés hatékonyságának mérésére. Ne felejtsd el megnézni a mintakészségek listáját az egyes TTX-dokumentumok „TTX előtt vagy után edzendő készségek/viselkedések” alszakaszában. Bar csábító lehet, hogy egyetlen TTX-en belül a lehető legtöbb tanulási célt lefedd, de hatékonyabb egy kevesebb, konkrét tanulasi célt lefedő képzés megtartása. Ne feledd, hogy a közönség ideje és figyelme korlátozott!

Számítsd ki, hogy mennyi időre lesz szükséged a TTX-hez! Míg néha a kormányzati szervek vagy vállalatok több napig tartó TTX-eket hoznak létre, a te közönségednek valószínűleg nagyon kevés ideje lesz csak a TTX-edre. Figyelembe kell venned a résztvevők munkáját, és más, hétköznapi kötelezettségeit is. Vedd figyelembe, hogy általában egy 4-6 kérdést vagy fordulatot tartalmazó TTX kitöltése körülbelül 1-1,5 órát vehet igénybe. De ez nagyban függ a csoport méretétől is. Nagyobb csoportoknak általában tovább tart egy-egy TTX elvégzése. Számolnod kell a kiértékelésére, és a tanulási célok, illetve a konkrét, erősítendő készségek, viselkedési formák áttekintésére fordított idővel is. Ez utóbbit a TTX végén fogjátok elvégezni. A résztvevőknek további tanulásra vagy felzárkóztatásra is szükségük lehet az egyes készségek vagy viselkedések sikeres elsajátításához, ami további időt vehet igénybe.

Vedd figyelembe, hogy mekkora tér áll rendelkezésre a TTX elvégzéséhez. Ha személyesen tartod a TTX-et és nem online, akkor a legideálisabb a TTX megtartására egy olyan tér, amely lehetővé teszi az közös munkát. Egy asztalokkal és kényelmes székekkel felszerelt szoba például valószínűleg

sokkal alkalmasabb a TTX számára mint egy előadóterem. Előfordulhat az is, hogy neked kell gondoskodni a jó minőségi Wi-Fi-ről vagy más technikáról, például a projektorról is. A hely akadálymentesítésségét is figyelembe kell venni, ha lehetséges (pl. kerekesszékkel legyen megközelíthető, legyenek nemek szerinti fürdőszobák, kényelmes közlekedési lehetőségek stb.).

Döntsd el, hogy több képző tartja-e a tréninget. Ha igen, akkor mik lesznek a szerepek. A legcélravezetőbb, ha van egy képző, aki végig vezeti a TTX-et, egyfajta moderátorként, míg a többiek az egyes csoportoknak és alfeladatoknál segítenek. Képzőként néhány képzési részt érdemes néha előre elpróbálni, hogy kibukjanak a lehetséges problémák.

Határozd meg, milyen erőforrásokra lesz szükséged a TTX-hez. Előfordulhat, hogy létrehozol egy slide-ot, szóróanyagokat vagy más típusú prezentációs anyagokat, hogy élethűbbé és átláthatóbbá tedd a jelenetet, kérdéseket, feladatokat és fordulatokat. Fontos figyelembe venni azt is, hogy a résztvevőknek szüksége lehet papírra és íróeszközre is a jegyzeteléshez. Ne feledkezz meg az olyan technikai kiegészítőkről sem mint a projektor vagy wifi elérhetőség.

A TTX levezetése

A TTX lebonyolítása eltér egy hagyományos digitális biztonsági tréning vagy készségfejlesztési tanfolyam vezetésétől. Hiszen a hagyományos digitális biztonsági tréningeken az oktatók általában sokat beszélnek. Elvárják tőlük, hogy a technikai tudásukat megosszák a résztvevőkkel. Egy TTX tréningen azonban a legtöbb beszéd és munka a résztvevők részéről zajlik, miközben döntéseket hoznak, és helyzeteket értékelnek a forgatókönyv eljátszása során. A TTX képző a folyamat tovább görgető, mederben tartó szerepét tölti be, és gondoskodik arról is, hogy a TTX zökkenőmentesen menjen, és megfeleljen a kitűzött céloknak. A TTX képző elmondja a feladatot, a kontextust és a hátteret; válaszol néhány alapvető kérdésre; és fordulatokat ad a történethez. További ajánlásaink a TTX képzésekhez:

- Légy biztos abban, hogy nagyon alaposan ismered a TTX forgatókönyvét!
- Ne feledd, hogy mik a TTX-ed céljai! Irányítsd a beszélgetéseket úgy, hogy a résztvevők elérjék ezeket a célokat.
- Világosan kommunikáld a szerepeket és az elvárásokat a TTX elejétől a végéig.
- Tartsd a szemedet az óran! Győződj meg arról, hogy tiszteletben tartod és maximalizálod a résztvevők rendelkezésre alló idejét.
- Győződj meg arról, hogy a képzési tér biztonságos és barátságos. Egy olyan hely, ahol a résztvevők úgy érezhetik, hogy meghallgatják őket, és figyelembe veszik a nézőpontjukat.
- Ha egy résztvevő megemlít egy jó gyakorlatot, emeld ki! Ez növelheti az önbizalmat és ösztönözheti a további aktív részvételt.
- Ha nem tudod a választ egy kérdésre, ne félj megmondani, Vállald, hogy utánanézel a TTX után. Használd ki az olyan közösségi tereket is, mint például a Team CommUNITY Mattermost, hogy választ kapj azokra a kérdésekre, amelyeket esetleg nem tudsz egyedül megválaszolni.
- Ha lehetséges, gyűjts visszajelzéseket a foglalkozás során, és állj készen a mikromódosításokra. Ha azt tervezed, hogy egy TTX több fajta variációját fogod használni,

akkor a munkamenet végén gyűjthetsz visszajelzéseket, hogy jobban megértsd, hogyan javíthatsz még a TTX-en.

- Ha a TTX az eredeti szándéktól más irányba indul el, az is rendben van! Légy rugalmas, de ügyelj arra, hogy a tanulási célokat elérd.

Ha részletesebb útmutatásra van szükséged, az alábbiakban lépésről-lépésre segítünk neked ebben.

1. Mutatkozz be! (Mutasd be a többi társoktatót is). Magyarázd el a szerepeket, és írd le a TTX átfogó célját (például: ma azt fogjuk megvizsgálni, hogyan reagálhat egy hírszerkesztőség egy biztonsági incidensre). Ideális alkalom arra is, hogy csoportként felállítsatok néhány alapszabályt - a résztvevők javaslatai alapjan.
2. Ezután magyarazd el részletesebben, hogy mi fog történni a TTX alatt. Magyarázd el, hogy a TTX célja egy kitalált helyzet szimulálása, amely megközelíti a valós életet, azért, hogy jobban megértsük és javítani tudjuk a saját és a tágabb közösségünk reakcióit.
3. A csoport méretétől és összetételétől függően érdemes lehet a résztvevőket csoportokra osztani.
4. Mondd el a jelenet bevezetését a résztvevőknek, beleértve az esetlegesen szükséges háttértörténeteket is.
5. Olvasd, fel vagy mondd el a történetet, pontról pontra, ahogy a résztvevőket végigvezeted a TTX-en. Az egyes pontoknál tedd fel a kérdéseket a résztvevőknek. S adj meg nekik egy meghatározott időt a megvitatására. Légy elérhető kérdések esetén, és segíts a hibaelhárításban, ha a résztvevők elakadnának.
6. Tegyél bele fordulatokat a történetbe, hogyha úgy látod szükségét.
7. Bátorítsd a résztvevőket, hogy aktívan vegyenek részt a megbeszélésben, és válaszoljanak a kérdésekre! Kérd meg őket, hogy készítsenek jegyzeteket azokról a dolgokról, amiket relevánsnak vagy hasznosnak tartanak. Használj előre elkészített válaszokat, amik segíthetnek ha a résztvevők nehézségekbe ütköznek, vagy példákra van szükségük ahhoz, hogy neki kezdjenek a feladatnak.
8. Miután a résztvevők befejezték a TTX-et, kérd meg őket, hogy beszéljétek meg a tapasztalataikat és a véleményüket a TTX-ről, mint képzési módszerről. Ez egy nagyszerű alkalom a visszajelzések rögzítésére, és érdemes megfontolni a visszajelzések beépítését is fejlesztésként a jövőbeli képzésekhez.
9. A TTX befejezése után ellenőrizd, hogy vannak-e olyan anyagok, összefoglalók, amelyeket meg kell osztani a résztvevőkkel.

1. függelék: Sára háttere (TTX személy)

Létrehoztunk egy személyt, Sárát, akire felépítettük a TTX-szcenáriók forgatókönyvét és példait. Ez segített nekünk abban is, hogy a TTX-ekhez következetességet társítsunk, és jó kiindulópontot adjunk az újságíróknak a rájuk leselkedő esetleges fenyegetések és a tágabb összefüggések végig gondolásához. Az alábbiakban bemutatjuk Sárát. Ezt a bemutatást a képzők használhatják a helyszín megadására, és a történet hátterének a felrajzolására, mielőtt elkezdenék valamelyik TTX-forgatókönyvet.

Sára 41 éves újságíró. Több helyi és nemzetközi hírszerkesztőségnek dolgozott már a saját országában és az azt körülvevő szomszédos országokban több éven keresztül.

Sára tavaly kezdett dolgozni a „Free Press Now” nevű oknyomozó és tényfeltaró hírszerkesztőségnek a hazájában. Ez a szerkesztőség gyakran tudósít politikai eseményekről és történésekről. Ide tartoznak azok a feltételezett emberi jogi visszaélések, amiket az országa kormánya követhetett el, a korrupt kormányzati tisztviselők ügyei, és olyan kormányzati döntések és tevékenységek is, amelyek megnehezítik az országában élő etnikai kisebbségek életét.

A megbízható és igazsagos beszámolóinak köszönhetően a Free Press Now a helyi lakosság megbízható és népszerű információ forrásává vált.

5 hónappal az országos választások után a hatalmon lévő új kormány megkezdte a sajtószabadság korlátozását. A múlt héten a hatóságok három vezető újsagíró lakásában meglepetésszerű házkutatást tartottak. Nemrég Sára otthonában is tartottak házkutatást. Meglepő módon azok, akik a házkutatást végezték csak néhány jegyzetfüzetet vittek magukkal a házból.

1. forgatókönyv: Elveszett eszköz

A TTX forgatókönyveket a JSF ösztöndíjasai állították össze

Cél

Segíteni a résztvevőknek felkészülni egy olyan helyzetre, amelyben elvesztik egy vagy több eszközüket, ami akár érzékeny információt is tartalmazhat.

Tanulási célok

- Feltérképezni az újságírók és forrásaik közötti biztonságos kommunikáció formáit.
- Tudatosítani egy telefon vagy laptop elveszítésének kockázatait.
- Megismerni és megérteni az eszközök védelmének jó gyakorlatát
- Megosztani a szervezeti beléptetéssel és kiléptetéssel kapcsolatos jó gyakorlatot, elsősorban az eszközök biztonságával kapcsolatban.

Készségek / viselkedési formák gyakorlásra TTX előtt vagy után

- A Signal (vagy más biztonságos üzenetküldő alkalmazás) telepítése, beállítása és használata.
- Alternatív végpontok között titkosított üzenetküldő (például a WhatsApp vagy a Facebook Messenger Titkosított Chat) beállítása és használata.
- A Mailvelope (vagy egy másik opció az e-mailek titkosítására) telepítése, beállítása és használata.
- Egy mobileszköz titkosítása (jelszó beállítása)
- Jelszavak beállítása mobileszközön lévő egyes alkalmazásokhoz
- A mobileszközökön lévő adatok mentésének elvégzése és titkosítása (felhőszolgáltatások vagy külső meghajtó használatával).

Forgatókönyv

Egy korábban ismeretlen forrás kapcsolatba lép Sárával Facebook Messengeren, és azt állítja, hogy érzékeny információt szeretne vele megosztani. A fájl, amit meg szeretne osztani a védelmi miniszterről tartalmaz információt.

K1: Hogyan tudja Sára elmagyarázni a végpontok közötti titkosítás koncepcióját, hogy meggyőzze a forrást annak fontosságáról?

- Senki - még az üzenetküldőt üzemeltető vállalat - sem fér hozzá az üzenet tartalmához. Az üzenet tartalma nem kerül titkosítatlanul tárolásra a vállalat szerverein sem.
- A hatóságok nem tudják elérni a chat szolgáltatóból.
- Ha egy támadónak sikerül feltörni az üzenet küldésére használt fiókot, akkor sem fog tudni hozzáférni az üzenetek tartalmához (kivéve, ha ott titkosítatlan mentések vannak).

K2: Senki - még az üzenetküldőt üzemeltető vállalat - sem fér hozzá az üzenet tartalmához. Az üzenet tartalma nem kerül titkosítatlanul tárolásra a vállalat szerverein sem.

- A hatóságok nem tudják elérni a chat szolgáltatóból.
- Ha egy támadónak sikerül feltörni az üzenet küldésére használt fiókot, akkor sem fog tudni hozzáférni az üzenetek tartalmához (kivéve, ha ott titkosítatlan mentések vannak).

A forrás örül, hogy Sára biztonságossá szeretné tenni a kettejük közötti kommunikációt, viszont még mindig nem biztos benne, hogy melyik fajtáját részesítse előnyben. Sárához fordul tanácsért a Signallal, Telegrammal, Facebook Messengerrel és emailjével kapcsolatban

K3 (opcionális) - Milyen tényezőket érdemes figyelembe venni üzenetküldő alkalmazás választáskor a digitális biztonság szempontból?

- Telefonszámok: a legtöbb végpontok között titkosított üzenetküldőhöz telefonszámra van szükség, és sok helyen a telefonszámokat regisztrálni kell, így a kormány tudja, hogy melyik személy melyik telefonszám mögött áll. Ez azt jelenti, hogy ha a kormány valaha is átnézné Sára vagy a forrás telefonját, akkor rájönnének, hogy üzentek egymásnak, még akkor is, ha álneveket vagy eltűnő üzeneteket használtak (mérsékelné a helyzetetet, ha törölnék a neveket a névjegyekből, az üzenetküldőkből és ideális esetben a telefont is törölnék).
- Titkosított chatek: A Facebook Messenger és a Telegram kétféle módot kínál, amelyek közül csak az egyik titkosított a végpontok között. Ezt a módot általában titkosított chatnek vagy valami hasonlónak nevezik, bár gyakran el van rejtve a beállítások között.
- Eltűnő üzenetek: nagyjából minden modern üzenetküldő rendelkezik eltűnő üzenetek funkcióval, bár némelyikben ez csak a titkosított chat módban érhető el.
- Chatek törlése: ez elég célratörő, de fontos tudni, hogy egyes üzenetküldők csak archiválják, nem pedig törlik a chateket.
- Képernyőképekkel kapcsolatos tudatosság: a beszélgetés bármely rosszindulatú résztvevője egyszerűen készíthet képernyőképet, vagy - ha az üzenetküldő funkciói ezt nem teszik lehetővé - egyszerűen lefényképezheti a telefonja képernyőjét.
- Kétfaktoros azonosítás (2FA): egy támadó átveheti az üzenetküldő fiók irányítását a fiók regisztrálásához használt telefonszám megszerzésével és az ellenőrző SMS újbóli elküldésével. Ez lehetővé teszi számukra, hogy a fiók tulajdonosának adják ki magukat, bár jellemzően nem ad hozzáférést a korábbi üzenetekhez. A legtöbb üzenetküldő ma már lehetőséget biztosít arra, hogy az SMS-kódon kívül további jelszót is kérjen: ez azt jelenti, hogy még ha egy támadónak sikerül is megszereznie a telefonszámot, nem tud könnyen hozzáférni a fiókhoz.
- Erős jelszavak vagy jelszókódok magához a készülékhez (telefonhoz) való bejelentkezéshez

K4 (választás): Milyen tényezőket érdemes figyelembe venni digitális biztonság szempontjából az emailen történő kommunikáció során?

- A forrásnak egy új e-mail címet kell létrehoznia, csak a Sárával való kommunikációhoz

- Az új e-mail címnek erős és egyedi jelszóval és megbízható kétfaktoros azonosítással kell rendelkeznie.
- A forrásnak figyelnie kell az adathalász-támadásokra is és olyan technológiákat kell használnia, amelyek segítenek ezek mérséklésében, mint például a fizikai biztonsági kulcsok vagy a jelszókezelő automatikus kitöltő funkciója.
- Ideális esetben a forrásnak és Sárának PGP-n keresztül kellene kommunikálnia, például a Mailvelope használatával. Ez azt jelenti, hogy még ha a fiókjaikat valahogy fel is törné is, a támadó a PGP-kulcs nélkül nem tudná elolvasni az üzeneteik tartalmát.

A forrás egy biztonságos csatornán küldi el a fájlt Sárának, aki azt a telefonján nézi meg. Örül, hogy megvan az információ, és elmegy a barátaival ünnepelni. A buliban elhagyja a telefonját, és rájön, hogy egy nagyon egyszerű jelszóval (1111) védte csak le.

K5: Mi történhet Sára telefonjával és az információval ami rajta van?

- Bárki, aki megtalálja a telefont hozzáférhet az érzékeny információkhoz, ha rájön, hogy hol vannak azok.
- Bárki, aki megtalálja a telefont üzenetet küldhet Sára ismerőseinek és úgy tehet, mintha ő lenne Sára.
- Bárki, aki átnézi a telefonon lévő információkat, veszélyeztetheti Sára kapcsolatainak személyazonosságát és biztonságát, vagy olyan információkat gyűjthet, melyeket pszichológiai manipulációra használhat fel.
- Sára elveszítheti újságírói hitelességét.

K6: Mit tud Sára tenni most, hogy csökkentse ennek digitális biztonságára gyakorolt hatását?

- Távolról törölheti a telefonját, ha beállította ezt a funkciót.
- Bejelentkezhet a többi eszközén az e-mail és közösségi média fiókjaiba, megváltoztathatja azok jelszavait és ha lehetséges, rákattinthat a "kilépés minden bejelentkezett eszközről" linkre.

K7: Mik az előnyei és hátrányai annak, hogy elmondja a forrásának, hogy elveszítette a telefonját?

- Beszélgetés előre meghatározott helyes válaszok nélkül.

Jó hír! Sára egy barátja, aki a bulin volt vele megtalálja a kabátjában a telefont. Felhívta Sárát, és másnap visszaadta neki a telefont.

K8: Most, hogy Sára visszakapta a telefont, milyen lépéseket kell tennie, hogy biztonságban tudja az adatait, amennyiben a jövőben újra elveszítené a telefonját.

- Fontolja meg, hogy biometrikus feloldást használjon. Ennek vannak előnyei (senki nem lesheti ki Sára válla fölött, miközben beírja a jelszavát és a térfigyelő kamerák sem rögzítik) és hátrányai (könnyebb kényszeríteni Sárát, hogy feloldja a készülékét).

- Használjon hosszabb telefonfeloldó kódokat és jelszavakat. Kerülje a mintás feloldásokat (például a pontokat összekötő mintákat), mivel ezeket könnyen azonosíthatja egy megfigyelő személy, egy kamera vagy a képernyőn lévő foltok.
- Zárja le az alkalmazásokat (például az üzenetküldőket) egy további jelszóval is, ha Sára aggódik azon, hogy a telefonját néha mások is használják.
- Állítson be olyan alkalmazásokat, amelyek képesek a készüléket nyomon követni, lokalizálni és távolról törölni.

K9 - Szervezeti szemszögből hogy néz ki egy jó beléptető rendszer egy új munkatárs esetében annak érdekében, hogy az eszközei (pl telefon, számítógép) biztonságban legyenek?

- Biztosítani, hogy minden munkatárs végigmenjen egy beléptetésen, és ennek fontosságával mindenki tisztában legyen.
- Szervezetnek listázni kell az elvárásaikat a munkatársak felé a digitális biztonsági gyakorlatokkal kapcsolatosan.
- Feltérképezni a teendőket biztonság kompromittálódása esetére (pl. ha valakinek ellopják a telefonját, vagy feltörik egy jelszavát)
- IT támogatást kell biztosítani mindenkinek, akinek szüksége van rá.

2. forgatókönyv: Szervezeti biztonság

A TTX forgatókönyveket a JSF ösztöndíjasai állították össze

Cél

Segíteni a résztvevőknek abban, hogy szervezeteiknél, munkatársaiknál és/vagy szabadúszó újságíróknál a digitális biztonságtudatosság magas szintű legyen és a legjobb gyakorlatokat használják.

Tanulási célok

- A digitális biztonság koncepciójára elméletben folyamatos folyamatként, nem pedig végcélként kell tekinteni.
- Beszélni, tanítani és meggyőzni másokat a digitális biztonság fontosságáról.
- A biztonságos mobil eszközön történő kommunikáció lehetőségeinek megvitatása
- Annak biztosítása, hogy a fájlok biztonságos kezelésével a legjobb gyakorlatot követi.
- Tudatosság a hálózatra kötötti számítógépek fiókbeállításai kapcsán.
- A fenyegetés modellezés fontosságának megértése.

Készségek és viselkedési formák a TTX képzés előttre vagy utánra

- Hozzáférések beállítása és karbantartása kollaboratív platformokon (pl. Google Drive).
- (Amennyiben lehetséges, hiszen ezen szolgáltatások némelyike csak vállalati platformokon elérhető)
- Megnézni a naplófájlokat olyan kollaboratív platformokon, mint a Google Drive.
- Beállítani a kétfaktoros azonosítást, lehetőleg fizikai kulcsokkal, vagy más, adathalászat ellen védett módszerekkel
- Jó jelszó irányelvek (egyedi jelszavak használata, hosszú jelszavak, jelszó helyett mondatok vagy kifejezések) és jelszókezelő használata
- Dokumentumok titkosítása (pl. Mailvelope használatával)
- A Signal (vagy más biztonságos üzenetküldő alkalmazás) telepítése, beállítása és használata
- A, Haladó szintű beállítások az applikáción belül (pl. Eltűnő üzenetek)
- A Mailvelope telepítése, beállítása és használata (vagy más opció titkosított emailek küldésére)
- Biztonságosan bánni a forrásoktól származó fájlokkal és dokumentumokkal

Forgatókönyv

Sára egy újságíró csoportot állít össze, hogy az Egészségügyi Minisztérium által a Covid-19 során végzett közbeszerzésekkel kapcsolatos korrupciót vizsgálja. A csapatban nem minden újságíró

rendelkezik azonos szintű digitális készségekkel/biztonsági ismeretekkel és gyakorlatokkal. Sára tudja, hogy a csapat egyik tagja nagyon rosszul bánik a fájl védelemmel.

K1 - Hogyan ösztönözheti Sára a kollégáit arra, hogy javítsanak a digitális biztonsággal kapcsolatos megközelítésükön? Mit kell tennie Sárának a digitális biztonsági gyakorlatok használata érdekében, amikor egy együttműködő csapatot szervez?

- Magyarázza el, miért fontos jó digitális biztonsági intézkedésekkel rendelkezni. Beszéljen például arról, hogy a nem megfelelő digitális biztonsági intézkedések hogyan akadályozhatják egy újságíró karrierjét; hogy a források és a kollégák bizalmát könnyebb elnyerni, ha digitálisan biztonságban vagyunk, illetve, hogy milyen fontos védelmezni a környezetünkben lévőket.
- Vitassák meg, milyen eszközöket használnak, hogyan védik felhasználói fiókjaikat, hogyan tárolják és küldik/fogadják a fájlokat, hogyan férnek hozzá a munkahelyi hálózathoz (a saját eszközeiket használják, vagy a vállalat számítógépein dolgoznak), hogyan jelentkeznek be a munkahelyi hálózatba (vezeték nélkül vagy kábelen keresztül), használnak-e kétfaktoros azonosítást a felhasználói fiókok védelmére, és milyen a jelszó fegyelem (újra használják-e a jelszavakat, használnak-e jelszókezelőket).
- Döntsék el, hogyan kommunikáljon a csapat, hogyan tárolja a fájlokat és hogyan férjen hozzá a fájlokhoz. A második lépés lényege annak biztosítása, hogy mindenki ugyanazt a protokollt kövesse az előzőekben említett tevékenységekkel kapcsolatban.
- Fontolja meg a csapat képzését az újonnan létrehozott protokollok használatáról. A szabályok lefektetése után a csapatnak végig kell futnia egy szárazedzésen, ténylegesen tesztelve az új kommunikációs módokat, és megnézve, hogy vannak-e olyan problémák a folyamatban, amelyeket ki kell küszöbölni.

K2 - Hogyan fogja Sára és csapata tárolni és megosztani a különböző forrásokból származó hangfájlokat és dokumentumokat?

- Korlátozzák a hozzáférést a különböző fájlokhoz és mappákhoz, és használják a megosztási beállításokat körültekintően az olyan platformokon, mint a Google Drive.
- Kérjék meg a kollégákat, hogy ne vigyenek ki fájlokat és dokumentumokat a munkahelyről (USB-k, email csatolmányok stb.). Ezek növelhetik a támadási felületet és a szivárogtatás/feltörés rizikóját.
- Kérjék meg a csapatot, hogy csak munkával kapcsolatos fájlok eléréséhez használják a céges laptopjukat.
- Korlátozzák a céges laptopra letölthető programok körét, és biztosítsák, hogy mindig erős jelszavakkal és szoftver frissítésekkel rendelkeznek.

K3 (opcionális) - Milyen tényezőket érdemes figyelembe venni üzenetküldő alkalmazás választáskor a digitális biztonság szempontból?

Azzal, hogy az egész csapatot ugyanarra a platformra vezeti be, és meggyőződik arról, hogy mindenki elsajátította a használatát, Sára segíthet a csapatának abban, hogy biztonságos és védett kommunikációt alakítson ki egymás között.

Gondolkozzon el a következőkön:

- Helyezzék át a beszélgetések nagy részét Signalra, állítsanak be eltűnő üzeneteket, és másolják át azokat az üzeneteket, amelyeket archiválni szükséges.
- A PGP használata emailezéskor
- Hozzanak létre erős fiókbiztonságot az emailekhez (egyedi jelszavak, kétfaktoros azonosítás)

Két héttel a jelentésük közzététele előtt Sára telefonhívást kap fő kormányzati forrásától ezzel a vizsgálattal kapcsolatosan. Sára jól ismeri a forrást, és megbízik benne. A hívás során a forrás egyszerűen azt mondja: "A kormány tudja - volt egy szivárgás", és leteszi a telefont.

K4 - A digitális biztonság szempontjából melyek azok az első lépések, amelyeket a Sárának meg kell tennie egy esetleges információszivárgásra reagálva?

- Kérje meg a csapatát, hogy mindenki cserélje le jelszavait, arra az esetre, ha a támadó megszerezte volna a jelszót valamelyikük fiókjához.
- Vegye számba a lehetőséget, hogy a kormánynak nem kellett feltétlenül betörni a szerkesztősgébe. Tudomást szerezhettek a szivárogtatásról például úgy is, hogy kinyomozták, melyik kormányzati alkalmazott mit nyomtat.
- Végezzen egy kisebb vizsgálatot: ellenőrizze, hogy mindenki követte-e a protokollokat, kinek volt hozzáférése a kiszivárogtatott információhoz, és hogy egyáltalán mi szivrágott ki pontosan. A jogosultság kezeléssel és verzió követéssel könnyebben számontarthatják, hogy kinek milyen hozzáférése volt egyes információdarabkákhoz.
- Vegye fontolóra, hogy előbb publikálja az érintett anyagot.

Sára megtudja, hogy a szivárgás a szervezetén belülről érkezett. Egy tervezőnek hozzáférése volt a szervezet megosztott Google Drive-jához (annak ellenére, hogy nem dolgozott azon a feladaton). Sára ezt úgy tudta meg, hogy ellenőrizte a Google Drive hozzáférés-szabályozását, és rájött, hogy a tervezőcsapat a munka jellegéből adódóan mindenhez hozzáférhetett a hálózaton.

K5 - Mit tehetett volna Sára másképp ebben a helyzetben?

- Sárának biztonságos protokollokat kell létrehoznia a nyomozó csapata számára. Biztosítania kell a jogosultság rendszer tisztaságát, és hogy azt a gyakorlatban is betartsák.

- A csapat csak szükség szerinti alapon dolgozzon együtt a designerekkel. Ez azt jelenti, hogy semmilyen titkos információt ne kapjanak be egészen addig, amíg az nem feltétlenül szükséges a publikáláshoz.
- Sárának folyamatként érdemes felfognia a digitális biztonságot, nem pedig állapotként. A digitális biztonság olyasvalami, amit folyamatosan tovább kell fejleszteni.

3. forgatókönyv: Zaklatás és doxxolás

A TTX forgatókönyveket a JSF ösztöndíjasai állították össze

Cél

Segíteni a résztvevőknek abban, hogyan tudnak a legjobban felkészülni és reagálni a doxxingra és az online zaklatásra.

Tanulási célok

- Módszerek és enyhítő intézkedések meghatározása a közösségi médiában történő zaklatásban és doxxingban érintett újságírók számára.
- Az újságírók és szerkesztőségben dolgozók értsék meg, miképpen szerezhetik meg és használhatják fel ellenük a közösségi médiában megtalálható adataikat.
- A nemek és a zaklatás közötti kapcsolat, és annak biztonsági következményeinek megértése.
- Megbeszélni, milyen intézkedéseket és gyakorlatokat tud egy médiaszervezet hozni annak érdekében, hogy megvédje a doxxolásnak és zaklatásnak kitett dolgozóit és ügyfeleit.
- Megbeszélni a szerkesztőségi támogatással nem rendelkező dolgozók lehetőségeit (pl szabadúszók, külső munkatársak).
- Biztonságról szóló történetmesélés és mások meggyőzése: hogyan győzhetünk meg olyan embereket, akik hagyományosan nem szembesülnek zaklatással, arról, hogy ez egy súlyos probléma, amely összehangolt szervezeti intézkedéseket és támogatást igényel.
- Szervezeti biztonság: irányelvek megalkotása a szervezeten belül, módszerek megalkotása arra, hogyan tudják legjobban támogatni azokat a újságírókat, akik zaklatással szembesülnek.[1]

A TTX előtt vagy után gyakorolandó készségek/viselkedésmódok

- Az adatvédelmi beállítások kezelése és frissítése a főbb közösségi médiaplatformokon.
- A főbb közösségi médiaplatformok biztonsági eszközeinek használata, például a jelentés és a tiltás. Ez magába foglalja ezeknek a mechanizmusok használatának megértését, és azt, hogy pontosan milyen célt is szolgálnak.
- Kétfaktoros hitelesítés beállítása és használata, ideális esetben fizikai biztonsági kulcsokkal vagy hasonló, adathalászatnak ellenálló mechanizmusokkal.

Forgatókönyv

Sára egy új cikken dolgozik az országában élő kisebbségekről, és arról, milyen marginalizáló hatásai vannak rájuk a kormány intézkedéseinek. Az utóbbi hetekben Sára arra lett figyelmes, hogy

[1] A legtöbb képzésen ez egy tanulási cél lenne. Ha médiafelelősöknek vagy más döntéshozóknak tart foglalkozást, és lehetőség van a szervezeti eredmények mérésére, akkor ez készségként is megadható..

megnövekedett a kommentek száma a cikkei megosztására használt közösségi média felületeken. Egyre több gyűlöletteljes és megalázó kommentet kap különböző online trolloktól.

K1: Milyen lépéseket tud tenni Sára, hogy blokkolja és jelentse az ilyen kommenteket hagyó embereket?

- Használhatja a közösségi platformokon található “blokkolás és jelentés” funkciót.
- Fel tudja keresni a nagy közösségi média cégeket (személyesen, vagy akár a szervezetén keresztül is), hogy jelentse a nagyszabású zaklatást.
- Letilthatja a hozzászólásokat és válaszokat a profilján.
- Szűkítheti azt, hogy ki találhatja meg a közösségi platformon.
- Kiválaszthatja, hogy ne tudják mások megjelölni a közösségi médiában.

Działania w kierunku blokowania i zgłaszania podżegaczy zirytowało tylko grupę trolli. Skala nienawistnych treści skierowanych przeciw Sarze rozrosła się się. Niektóre komentarze zawierają również groźby.

K2 - Milyen módon tudja Sára kivizsgálni az ellene irányuló agressziót, hogy megállapítsa, egy nagyobb, összehangoltabb kampány része-e, vagy valami szervesebb dologról van-e szó.

- Saját maga is kivizsgálhatja a helyzetet, és kollégáitól is kérhet támogatást a nyomozásban.
- Ellenőrizheti, hogy a trollok mind pontosan ugyanazt a nyelvet, kulcsszavakat vagy hashtageket használják-e. Ha igen, akkor valószínűleg összehangolt akcióról van szó.
- Az adott platformtól függ. Az Instagramon széleskörű lehetőség van a fiókokra vonatkozó információk megtekintésére: mikor jött létre, hányan használják, milyen gyakran változtatta meg a nevét stb.
- Ellenőrizheti, hogy valamilyen médium felerősíti-e ezeket.
- Nézze meg a leggyakoribb posztolási időt.

Mesél a kollégáinak a posztokról, de a csapat férfi tagjainak többsége, köztük a szerkesztője is, azt mondja neki, hogy ne aggódjon, és hogy a probléma magától megoldódik. Ez stresszessé teszi, úgy érzi, hogy a csapata nem hallgatja meg, és nem érti meg a problémát.

K3 - Ahelyett, hogy azt mondaná Sárának, hogy ne aggódjon, milyen módon támogathatná a csapata és a szervezete Sárát, különösen az online jelenléte és a digitális biztonsága tekintetében?

- Segíthetnek a helyzet teljes körű felmérésében.
- Áttekinthetik Sárával az alkalmazott digitális biztonsági gyakorlatát és biztonsági intézkedéseit, és szükség esetén segíthetnek javítani a helyzeten.
- Gyakorlatot és megosztott tapasztalatokat szerezhet a szervezeten belül másoktól.
- Megengedheti, hogy olyan emberek kezeljék a fiókját, akikben megbízik, vagy átnézzék azt, hogy ne legyen közvetlenül kitéve ezeknek a szavaknak és fenyegetéseknek, de mégis jelen legyen.

- A szervezet segíthet mintákat keresni a zaklatásokban.
- Kövesse nyomon, hogy a zaklatás hogyan folyik az egész szervezet posztjain keresztül, nem csak Sára posztjain belül.
- Jelezze ezt a biztonsági csapatnak, és segítsen a nyomozásban.

Egy nap Sára személyes fotóit kiszivárogtatja az egyik troll az internetre. A fotók, amelyeket évekkel ezelőtt tett közzé a közösségi médiában, személyesek, és néhány esetben érzékeny információkat tartalmaznak.

Injektálás - 1-4 db fotó megosztása a résztvevőkkel. (A fényképek a dokumentum mellékletében találhatók). A példafényképek a következők:

Sára és a kutyája sétál a háza előtt

Sára marihuánát szív

Sára és a legközelebbi barátai nyaraláson

Sára a szerkesztőségben dolgozik

Vitassák meg a csoport résztvevőivel, hogy ezek a fotók miért lehetnek érzékenyek.

K4 - Milyen módon férhetett hozzá valaki Sára online adataihoz, például régi közösségi média-bejegyzésekhez?

- Sára barátai rossz adatvédelmi beállításokkal posztoltak fotókat.
- Sára fiókjait feltörték.
- Sára egyik közösségi média ismerőse talán elmentette a képeket, hogy később megoszthassa őket.
- Sára közösségi médiában megosztott fényképei indexelve lehetnek egy keresőmotor által.

K5 - Milyen lépéseket próbálhat meg Sára, hogy megelőzze további információk online kiszivárgását?

- Törölje le a régi fotókat.
- Törölje a fiókokat.
- Zárolja a fiókokat.
- Töltsön fel olyan fotókat, amelyek kevesebb információt árulnak el róla.
- Kérjen egy lekérdezést a szociális média szolgáltatótól, ami összefoglalja a náluk róla tárolt adatokat.
- Jelentse a közelmúltban közzétett fényképeket/jelentse a fényképeket közzétevő fiókokat.

- Folytassa a munkahelyi tartalmak közzétételét, még akkor is, ha kevesebb személyes tartalmat tesz közzé. Ha eltűnik az internetről, az azt jelenti, hogy a trollok győztek.
- Készítsen képernyőfotót a hozzászólásokról, dokumentálja őket, amennyire csak lehetséges. Jegyezze fel a trollok online álneveit.

K6 - Milyen lépéseket tehetett volna Sára és szervezete, hogy megelőzze a róluk szóló információk begyűjtését és online kiszivárogtatását, kifejezetten a digitális biztonság területén?

- uHozzanak létre egy olyan közeli baráti csoportot, akik kizárólagosan láthatják a személyes fotóikat és posztjaikat a közösségi oldalakon.
- Egyáltalán ne tegyen közzé érzékeny információkat (mint például a marihuánás fotó).
- Ne tegyenek közzé olyan fényképeket, amelyek személyes információkat, például a tartózkodási helyet mutatják.
- Nyisson üzleti felhasználói fiókot, hogy a magánéletétől független online jelenléte legyen.
- Erős jelszó- és 2FA irányelvek a közösségi média fiókokhoz.

Függelék 1: Szúrj be fénykép példákat

4. forgatókönyv: Hatóságok behatolnak a szerkesztőségbe

A TTX forgatókönyveket a JSF ösztöndíjasai állították össze

Cél

Segítség a résztvevőknek abban, hogy elméletben és gyakorlatban is reagálni tudjanak arra, ha a hatóságok behatolnak a szerkesztőségükbe.

Tanulási célok

- Biztosítson egy kommunikációs tervet és tartalék technikai elemeket arra az esetre, ha a szerkesztőséghez vagy a személyes eszközhöz való hozzáférés már nem lehetséges.
- Ismerje és értse meg a legjobb gyakorlatot a digitális eszközök biztosításával kapcsolatban egy szerkesztőségen vagy egy szervezeten belül.
- Azonosítsa a digitális eszközökön, például számítógépen vagy mobiltelefonon tárolt fájlok védelmének különböző módjait.
- Tervezze meg a veszélyeztetett információk védelmét, arra az esetre, ha a hatóságok behatolnak és rajtaütnek a szerkesztőségen.
- A veszély modellezéssel, valamint az egyének és szervezetek előzetes felkészülésével kapcsolatos fogalmak feltárása.

A TTX előtt vagy után gyakorolandó készségek/viselkedésmódok

- VeraCrypt, vagy ahhoz hasonló eszközök használata merevlemezeken tárolt adatok titkosítására.
- Veszély modellezés, elsősorban hatóságokkal és házkutatásokkal kapcsolatban: hogyan kell felmérni a kockázatokat, felkészülni egy esetleges házkutatásra, majd feldolgozni azt.
- Szervezeti és közösségi biztonság, különösen azzal kapcsolatban, hogy hogyan dolgozzunk együtt szerkesztőkkel, vezetőkkel és jogászokkal stresszhelyzetekben, és hogyan határozzuk meg, hogy melyik kérdést melyik személyhez kell továbbítani.
- Microsoft Office és Google Drive azon beállításainak ismerete, amivel megállapíthatjuk, milyen fájlokhoz fértek hozzá legutóbb
- (Haladó) Ha egy szervezetnek hozzáférése van részletes naplófájlokhoz (logok) egy prémium Google Drive vagy O365 előfizetésnek köszönhetően, akkor az ilyen naplókhoz való hozzáférés és az azokkal való munka.
- Keresési- és fájlhozzáférési előzmények áttekintése a legnépszerűbb böngészőkön és operációs rendszereken

Forgatókönyv

Sára egy körülbelül 20 fős szerkesztőségben dolgozik. Ez egy mozgalmas hétfő reggel, 15 újságíró és más munkatárs dolgozik a szerkesztőségben, valamint további 5 kolléga távolról dolgozik.

Délelőtt 10 órakor nagyjából 50 rendőr érkezik a szerkesztőségbe. Házkutatási parancsot mutatnak a szerkesztőnek, majd erőszakkal behatolnak a szerkesztőségbe, miközben azt követelik, hogy az összes újságíró és munkatárs azonnal távozzon.

Sára és kollégái odakint találkoznak, és megvitatják, hogyan tudnák biztonságos módon üzemeltetni médiaszervezetüket.

K1 - Mik a prioritások egy ilyen helyzetben?

- Keressenek fel egy ügyvédet, és egyeztessenek vele a következő lépésekről.
- Lépjenek kapcsolatba a távolról dolgozó kollégákkal
- Vegyék számba, hogy kinél van nála a mobiltelefonja, és ki hagyta hátra

K2 - Milyen módon tudnak ez idő alatt Sára és kollégái biztonságos közösséget alkotni?

- Csináljanak csoportbeszélgetést WhatsApp-on vagy Signal-on
- Lehet, hogy jobb ötlet a munkahelyi telefonszámok helyett a személyeseken kommunikálni.
- Ellenkező esetben a chat beszélgetés az irodában maradt eszközökre is szinkronizálódhat.

K3 - Hogyan kell Sárának és kollégáinak a szervezet online fiókjait, például a weboldalakat és a közösségi média fiókokat kezelniük?

- Változtassák meg a jelszavaikat azonnal
- Ha lehetséges távolról kilépni az irodában maradt eszközökről, lépjenek ki, de előtte egyeztessenek ügyvéddel, hogy ez nem minősül-e a bizonyíték meghamisításának.
- Egyeztessenek az ügyvédekkel mielőtt posztolnak a házkutatásról

Sára úgy emlékszik, hogy amikor elhagyta a szerkesztőséget, látta, hogy a rendőrök elkezdték zsákokba pakolni a számítógépeket, eszközöket és papírokat. Sára a telefonját el tudta hozni, de a laptopja a szerkesztőségben maradt. A kollégák csoportja gyorsan felmérte, milyen információkhoz juthat hozzá a rendőrség.

K4 - Hogyan legyenek biztosítva az eszközök a szerkesztőségben?

- A számítógépek erős jelszóval legyenek lezárva.
- A képernyő zárolódik egy rövid idő után?
- Titkosított USB kulcsok és merevlemezek

Egy irodán kívüli beszélgetés során kiderül, hogy az egyik szerkesztő elfelejtette zárolni a számítógépét mielőtt elhagyták az irodát.

A rendőrség két órával később hagyja el a szerkesztőséget, így az újságírók visszatérhetnek. A munkatársak összegyűlnek, hogy megvitassák, hogy mely információkhoz férhetett hozzá a rendőrség, és megvitatják a jövőbeni hasonló jellegű fenyegetéseket.

K5 - Milyen módokon tudja egy szerkesztőség azonnal felmérni egy házkutatás hatását?

- Nézzék meg, milyen papír alapú dokumentumokat vittek el, vagy rendeztek át (ha dokumentumok át vannak rendezve, az azt jelentheti, hogy a rendőrség fényképeket készített róluk)
- A számítógépeken általában megtalálhatóak a keresési-, fájlhozzáférési-, illetve böngészési előzmények, ezeken is érdemes végigmenni. A legutóbb megnyitott fájlok elérhetőek Microsoft Wordben, a böngészési előzményekben pedig a Google Docs hozzáférések. Ha a fájlelőzmények törölve lettek, az azt is jelentheti, hogy valaki megpróbálta elfedni a nyomokat.
- Nem valószínű, hogy rosszindulatú program telepítésre került, de ha emiatt aggódik valaki, konzultáljon erre szakosodott szakemberrel.

K6 - Hogyan biztosíthatja a szervezet, hogy a rendőrség rajtaütése ne jelentsen további kockázatot?

- Változtassák meg a jelszavakat a biztonság kedvéért
- Konzultáljanak egy jogásszal, hogy mihez férhetett hozzá jogosan a rendőrség, és mihez nem.
- Ha kódneveket vagy pszeudonimeket használtak a kutatásaikhoz, változtassák meg ezeket

Néhány héttel később a szerkesztőség szerkesztője összehívja az összes újságírót és munkatársat. Meg akarják érteni, hogy a szerkesztőséget a jövőben milyen hasonló fenyegetések érhetik.

K7 - A veszély modellezés és a digitális biztonság tekintetében az egyének és a szervezetek hogyan tudják azonosítani a veszélyeket, amikkel szemben állhatnak?

- Tegyük fel az általános veszély modellezés kérdéseinket: milyen információnk van, kinek állhat érdekében ehhez hozzáférni, és mik lennének a következményei, ha ellenségeink hozzáférnének?
- Amikor az ellenségeinket listázzuk, gondoljunk mind a cselekvési szándékokra (mit szeretnének csinálni és miért?), mind a képességekre (mik azok, amikre valóban képesek, milyen technikai, jogi, szervezeti és anyagi erőforrások állnak rendelkezésükre?)

5. forgatókönyv - Hatóságok behatolnak egy újságíró lakásába

A TTX forgatókönyveket a JSF ösztöndíjasai állították össze

Cél

Az újságíróknak elméleti és technikai ismereteket nyújtani ahhoz, hogy a lehető legjobb digitális biztonságot érhessék el otthoni környezetükben.

Tanulási célok

- Az otthoni digitális eszközök védelmének megértése
- Papír jegyzetfüzetekkel kapcsolatos biztonsági intézkedések alkalmazása
- A fájlok távoli törlésének kezdeményezése, valamint az ezzel kapcsolatos pozitívumok és negatívumok.
- A veszélyeztetett információkhoz való hozzáférés korlátozása.
- Felkészülés a hatóságok újságíró otthonába való behatolására.
- Rávenni a résztvevőket, hogy gondolkozzanak közösen a szervezeti és közösségi biztonságról. Különös figyelmet szentelve a szerkesztőkkel, a menedzserekkel, ügyvédekkel folytatott munkára stresszes helyzetekben. Illetve határozzák meg, hogy mely kérdéseknél és problémáknáll kiket vonjanak be az egyes folyamatokba.

A készségek, amelyeket meg kell tanítani a TTX előtt vagy után

- Egy olyan eszköz használatának az ismerete, amivel titkosítani lehet az adatokat hard drive-on, és külső meghajtókon. Például a VeraCrypt, vagy egy hozzá hasonló alkalmazás.
- Threat modelling, azaz veszélyeztetettségi modell felépítése, és annak módja. Különösen arra kiterjedően, hogy hogy kell bánni a hatóságokkal, illetve mi a teendő egy házkutatás során. Hogyan kell felkészülni a kockázatokra, hogyan kell kezelni azokat, és mit kell utána tenni, ha bekövetkeznek.
- Megtanítani az olyan eszközök használatát és bekapcsolását mint az Apple Find my…, vagy a Samsung find my..., amelyek az adathordozók távoli zárolását és törlését is lehetővé teszik.
- A Microsoft Office-ban és a Google Drive-ban azoknak a beállításoknak a megtanulása, amelyekkel látható, hogy mely fájlokhoz fértek hozzá az utóbbi időkben, és mikor.
- (Haladó) Hogyha a szervezetnek van hozzáférése prémium Google Drive vagy O365 előfizetésen keresztül a logokhoz (naplófájlokhoz), a logokkal való munka és a logok elérése.
- Átnézni a keresési és fájl elérési előzményeket a népszerű webböngészőkben és az operációs rendszerekben.

Forgatókönyv

Az 5 hónappal ezelőtti országos választásokat követően a hatalmon lévő új kormány elkezdte utasítani a hatóságokat a sajtószabadság korlátozására, és a hatóságok házkutatást tartottak három neves újságíró otthonában a fővárosban. Erre válaszul Sára és néhány kollégája összeült, hogy megvitassák, hogyan védhetik meg magukat és az információikat, ha hasonló helyzettel kellene szembenézniük.

K1 - Mi az a néhány dolog, amit egy újságírónak figyelembe kell vennie, amikor úgy dönt, hogy otthonában tárolja az információkat?

- Tárolja az eszközöket biztonságos helyen az otthonában
- Titkosítsa és lássa el jelszóvédelemmel minden eszközét.
- A dokumentumok ne tartalmazzanak szenzitív, érzékeny adatokat, például neveket.
- Vezessen leltárt arról, hogy az egyes információkat hol tárolja (de ezt is tartsa biztonságban).
- A nem digitális információk esetén figyeljen a fizikai másolatokra.
- Mindezek mellett lehetőleg semmilyen érzékeny vagy fontos dokumentumot ne tartson az otthonában az újságíró.
- Tartsa be a helyi törvényeket és a szervezeti irányelveket.
- Legyen tisztában azzal, hogy milyen jogi következményei lehetnek annak, ha az érzékeny adatokat az irodája helyett az otthonában tárolja.
- Gondolja végig, kinek van hozzáférése az otthonához és az eszközeihez?

K2 (opcionális) - Mi a legjobb gyakorlat a papír jegyzetek otthoni tárolására?

- Fontolja meg azoknak a papíroknak a megsemmisítését, amikre már nincs szüksége.
- Ne tartsa az összes jegyzetet egy helyen - kevesebb információhoz lehet így könnyen hozzáférni.
- Rejtse el a jegyzetfüzeteket
- Széf, zár és kulcs, hogy mindent biztonságban tartson!
- Gondolja végig, milyen szintű érzékeny információkat érdemes otthon tartani?
- Használjon rövidítéseket, álneveket, gyorsírást - olyan dolgokat, amelyeknek csak az ön számára van értelme.

K3 - Milyen intézkedéseket lehet tenni az elektronikus eszközök (számítógépek, merevlemezek, USB-stickek stb.) lehető legjobb védelme érdekében?

- Titkosítás
- Jelszóvédelem
- Az adatok külső helyszínre történő biztonsági mentése
- Memóriakártyák - nehéz biztonságosan törölni. Talán meg kellene semmisíteni őket
- A régebbi, különösen a már nem használt eszközök biztonságának mérlegelése.

Ma reggel 9 órakor Sára elindult otthonról, hogy igyon egy kávét és bevásároljon. Amikor egy órával később visszatért, a lakása ajtaja nyitva volt. Sára a lakásába lépve két férfit talált, akik az íróasztalát és a hálószobáját kutatták át. Az egyik férfi Sára jegyzetfüzeteit olvasgatta, míg a másik egy táskát tartott a kezében, amelyben Sára laptopja volt. Sára látta, hogy az íróasztalán lévő USB-kulcsok és külső merevlemezek hiányoznak. A két férfi civil ruhát visel, de Sára feltételezi, hogy valamilyen módon a kormánynak dolgoznak.

1. lehetőség - Sára röviden beszél a két férfival, és biztonságban el tudja hagyni az otthonát. Elsétál egy közeli barátjához.

K4 (választható) - Annak tudatában, hogy néhány információja, különösen a jegyzetfüzetéből származó információi veszélybe kerültek, kit kellene Sárának tájékoztatnia erről az esetről?

- Értesítse a szerkesztőjét és a szerkesztőség ügyvédeit.
- Mielőtt értesítené a forrását, amely benne lehetett a jegyzetfüzetében, először beszéljen a szerkesztőjével és a szerkesztőséggel, illetve biztonsági szakemberekkel. (Ha csak álnéven szerepelt a forrás, de másnap felhívom, elvezethetem hozzá a nyomozókat és ezzel felfedhetem a kilétét.) Ezért álnév esetében lehet hogy nem érdemes rögtön szólni neki.

K5 - Mit tehetne Sára, hogy megelőzze a digitális információihoz való hozzáférést, amíg a két férfi még a lakásában tartózkodik?

- Tegyen meg mindent a helyi törvények betartása érdekében
- Ragaszkodjon ahhoz, hogy a hatóságok is kövessék a helyi törvényeket (pl. Filmfelvétel készítés engedélyezése, tanú, stb.)
- De-eszkalációs technikák
- Tudja meg, hogy kik ők, és van-e megbízatásuk, felhatalmazásuk eljárni, és az mire vonatkozik.
- Értékelje a helyzetet a saját személyes biztonsága szempontjából
- Kérjen jogi tanácsot, hívja fel a szerkesztőséget
- Hamis beszámolók és dokumentumok bemutatása (előkészületet igényel).
- Elterelés

2. lehetőség - Sára nem tudja elhagyni a lakását. A két férfi megkéri, hogy foglaljon helyet és követelik, hogy adja meg a számítógépének és az USB-stickjeinek jelszavait. Megfenyegetik, hogy ha nem adja meg ezeket az információkat, akkor a rendőrségre viszik. Sára házkutatási parancsot kér, de ők ezt megtagadják.

K6 - Milyen lehetőségei vannak Sárának ebben a helyzetben, ha tudja, hogy bizalmas információkat tárol a számítógépén, beleértve a titkos források személyazonosságát?

- A sebezhetőségek felmérése és a legfontosabb kérdések előre sorolása.
- Távoli kijelentkezés és az érzékeny fiókok távoli törlése
- Az otthon tárolt összes információ azonosítása
- Mérlegelje a csapattagok és a veszélyben lévő források tájékoztatásának pozitív és negatív hatásait. Esetleg a szerkesztőség támogatásával hozza meg ezt a döntést.
- A fájlok távoli törlésének lehetőségei

K7 - Sára egy távoli fájltörlő programot állított be a számítógépén. Mit kell figyelembe vennie, mielőtt törli a számítógépes fájljait?

- Jogi problémája lehet - az igazságszolgáltatás akadályozása, vagy bizonyíték megsemmisítése miatt.

- Gondolja végig a lehetséges következményeket. Ha lehetséges, előbb konzultáljon egy ügyvéddel.
- Ha Sárának nincs bizonyítéka arra, hogy a “vendégei” rendőrök, és inkább gazfickóknak tűnnek, akkor ez a helyzet teljesen megváltoztatja a jogi és veszélyeztetettségi helyzetét a házkutatás során.

K8 (opcionális) - Tudva, hogy néhány adatát veszélybe sodorták, kit kellene Sárának tájékoztatnia erről az incidensről? Fontos, hogy milyen sorrendben tájékoztatja az embereket?

- A főszerkesztőt
- A szerkesztőség biztonsági/IT csapatát
- A szerkesztőség jogi csapatát
- Fontolja meg a forrásokkal való kapcsolatfelvételt
- Ha szabadúszó újságíró, fontolja meg a helyzet megosztását más szabadúszókkal.

Sára végül nem hajlandó megadni az eszközeihez tartozó jelszót. Miután még további 10 percig kutatták a lakását, a két férfi távozik Sára számítógépével, USB-kulcsaival és a jegyzetfüzetével.

Sára most már újra hozzáfér a lakásához. Látja, hogy a két számítógépe közül az egyiket és az egyik USB-kulcsát hátrahagyták, azonban az összes jegyzetét és jegyzetfüzetét elvitték a lakásból.

K9 - Mit kell most tennie Sárának, hogy az információi és a biztonsága ne kerüljön további veszélybe a két férfi tevékenysége miatt, amíg a lakásában tartózkodtak?

- A férfiak lehet, hogy malware-t, azaz rosszindulatú szoftvert telepítettek az eszközeire. Ezért érdemes az eszközeit egy digitális kriminalisztika szakértővel átvizsgáltatnia, mielőtt újra használja azokat. Lehetséges az is, hogy keyloggert tettek az eszközeire - amivel megszerezhetik a jelszavait.
- Figyelembe kell vennie, hogy a lakást lehallgathatják
- Kérdezze meg a szerkesztőségét vagy a szervezetet, akihez tartozik, hogy milyen segítséget és támogatást tudnak neki adni ebben a helyzetben.
- Beszéljen a szerkesztőségével vagy a civil szervezettel, akihez tartozik, a jogi és biztonsági szakértőkkel, hogy érdemes-e a nyilvánosság előtt, a közösségi csatornákon beszélni arról, hogy mi történt, vagy nem. (Ezt előre érdemes eldönteni, jogászok és biztonsági szakemberek bevonásával, hogy ilyenkor mi a szerkesztőség állaspontja, hogy például élőben közvetítik-e Facebookon vagy Youtube-on, hogy mi történik.)

K10 - A forgatókönyv digitális biztonsági szempontjain kívül milyen egyéb óvintézkedéseket és válaszlépéseket tehetett volna Sára annak érdekében, hogy biztonságban tartsa magát és az információit?

- Olvasson és kérdezzen utána, hogy működnek az országban, ahol van, a biztonsági erők, vannak-e olyan, nem a rendvédelmi erőkhöz tartozó csoportok, amelyek megpróbálják megfélemlíteni az újságírókat, és kik azok.
- Készüljön fel ügyvédekkel és a szerkesztőkkel arra, hogy mi a legjobb reakció és cselekedet egy az újságíró otthonába, vagy a szerkesztőségbe való behatolás, házkutatás során.
- Semmilyen szenzitív, érzékeny információt ne tároljon otthon. Akkor pedig különösen ne, ha esély van egy házkutatás bekövetkeztére.