Internews
Local voices. Global change.

Journalist Security Fellowship

Udhëzues për lehtësimin e ushtrimeve të tavolinës (TTX) për trajnimin e sigurisë dixhitale

Qëllimi dhe Prezantimi

Ky udhëzues ka për qëllim të shoqërojë një grup prej 11 skenarësh ushtrimesh tavoline (TTX) të fokusuar në sigurinë dixhitale, të cilët mund të përdoren për të përmirësuar trajnimin e sigurisë dixhitale. Ky udhëzues synohet të përdoret nga çdo person që dëshiron të projektojë dhe lehtësojë TTX-të si një metodë trajnimi për sigurinë dixhitale. Brenda këtij udhëzuesi, do të gjeni shpjegime të shkurtra se çfarë është një TTX, pse TTX-të mund të jenë shtesa të vlefshme për trajnimet e sigurisë dixhitale dhe si mund të zhvillohen, planifikohen dhe lehtësohen TTX-të.

11 skenarët e përfshirë në këtë udhëzues u zhvilluan së bashku me gazetarët në Evropën Qendrore dhe Juglindore si pjesë e projektit Internews Journalist Security Fellowship (JSF) dhe u përdorën në trajnimet e kryera nga bashkëpunëtorët e JSF në rajon. Këto modele të ushtrimeve të tavolinës (TTX), duke përfshirë disa me versione të lokalizuara në gjuhët e Evropës Qendrore dhe Juglindore dhe të përkthyera në arabisht dhe spanjisht, mund të aksesohen në lidhjen këtu.

Ky udhëzues është zhvilluar posaçërisht duke pasur parasysh sigurinë dixhitale për gazetarët dhe redaksitë, por mund të jetë i dobishëm për planifikimin e TTX-ve edhe për audiencat e tjera të synuara.

Çfarë janë ushtrimet e tavolinës (TTX)? Pse janë të vlefshme?

Një ushtrim tavoline është një metodë trajnimi, e bazuar në një skenar, që shpesh merr formën e një diskutimi ndërveprues. TTX-të ofrojnë një mundësi për pjesëmarrësit e trajnimit që të aplikojnë njohuritë dhe aftësitë e fituara rishtazi duke u përfshirë në një situatë fiktive (referuar si një skenar ose skenë TTX) që përafrohet me atë të jetës reale. Skenarët TTX mund të ekzaminojnë një gamë të gjerë situatash sigurie si një bastisje në zyrë, një rrjedhje të dhënash, një rast të publikimit të të dhënave personale ose një hetim të ndjeshëm. Ndërsa metodat më tradicionale të trajnimit mund të fokusohen në transferimin e aftësive dhe njohurive të caktuara teknike, një TTX mund të ndihmojë në:

- Sigurimin e një hapësirë me rrezik të ulët për pjesëmarrësit e trajnimit që të praktikojnë përgatitjen dhe përgjigjen ndaj çështjeve të sigurisë që mund të hasin.

- Nxitjen e diskutime kritike rreth çështjeve të sigurisë dixhitale dhe si të qaseni më mirë në kontekste dhe situata të ndryshme. Kjo mund të jetë veçanërisht e dobishme për pjesëmarrësit e trajnimit që punojnë së bashku rregullisht për të marrë në konsideratë qasjen e tyre të përbashkët ose organizative ndaj sigurisë.

- Vlerësimin sa mirë është i pajisur një individ ose organizatë për t'u marrë me çështjet e sigurisë që hasin.

Qëllimi i një TTX është të identifikojë boshllëqet individuale, organizative dhe të komunitetit në njohuri, pikat e forta dhe kufizimet. Një TTX i suksesshëm shkon përtej mjeteve dhe praktikave bazë, duke theksuar gjithashtu se cilat procedura ose politika mund të mungojnë ose duhet të përmirësohen.

TTX-të janë më efektive kur përdoren si shtesa për të përmirësuar metodat e tjera të trajnimit. Kjo ndodh sepse qëllimi i TTX-ve nuk është kryesisht transferimi i aftësive dhe njohurive të reja, por futja dhe forcimi i mëtejshëm i mësimeve nëpërmjet praktikës, diskutimit dhe vlerësimit të bazuar në skenar.

Përbërësit e dokumenteve të skenarit të ushtrimit të tavolinës (TTX)
Secila nga 11 skenat TTX bazohet në personazhin e Sarës, të cilën e kemi përshkruar në këtë udhëzues. Për më tepër, çdo skenë përfshin komponentët e mëposhtëm:

- **Qëllimi** - Qëllimi kryesor i skenarit TTX.
- **Objektivat mësimorë** - Opsionet për objektivat e përgjithshme të të mësuarit për t'u fokusuar gjatë TTX. Lehtësuesit ka të ngjarë të përgjedhin vetëm disa prej objektivave të të mësuarit për t'u fokusuar.
- **Aftësitë/Sjelljet për të Trajnuar Para ose Pas TTX** – Opsione për aftësi konkrete dhe specifike dhe ndryshime në sjellje që TTX fokusohen gjatë trajnimit të pjesëmarrësve

Lehtësuesit do të përgjedhin të fokusohen vetëm në disa aftësi dhe sjellje dhe këto duhet të përafrohen me objektivat dhe qëllimin e zgjedhur të të mësuarit.

- **Skenari – Ky është skenari aktual TTX. Ai përfshin sa vijon:**
    - **Sfondi prezantues dhe informacioni kontekstual në fillim**
    - **Pjesë shtesë të kontekstit të ofruara gjatë gjithë skenarit**
    - **Pyetje dhe nxitje për pjesëmarrësit për të diskutuar dhe përgjigjur. Këto shënohen me shkronjën P të ndjekur nga një numër (p.sh., P1, P2, P3, etj.).**
        - **Nën pyetjet dhe kërkesat janë disa përgjigje të mundshme. Këto nuk duhet të ndahen me pjesëmarrësit gjatë TTX. Ato synojnë të ndihmojnë lehtësuesin.**
- **Disa skenarë përfshijnë injektime (do të etiketohen si "injektime"). Një injektim është një pjesë informacionit e re ose një zhvillim i ri i futur nga lehtësuesi në skenarin TTX në kohë specifike për ta çuar skenarin përpara ose për të shtuar kompleksitetin. Një injektim mund të ndryshojë narrativën e TTX dhe mund të kërkojë veprim ose përgjigje nga pjesëmarrësit.**

Anekset - Disa skenarë (p.sh., Skenari 3: Ngacmimi dhe Doksimi) përfshijnë gjithashtu anekse, shpesh të përdorura për injektime gjatë skenarit.

Zhvillimi i një skenari TTX

Njëmbëdhjetë skenarë TTX u zhvilluan nën projektin JSF (lidhur këtu). Çdokush mund t'i modifikojë këto, në mënyrë që të përshtaten më mirë me nevojat e trajnimit të komunitetit të tyre. Dikush gjithashtu mund të krijojë skenarët e vet nga e para. Nëse po mendoni të rishikoni një nga skenarët TTX ose të krijoni tuajin, merrni parasysh sa vijon.

Objektivat e mësimit duhet të vendosen në fillim të fazës së projektimit, të plotësojnë njëra-tjetrën, të ndjekin një rend logjik sa i përket të mësuarit, të prioritizohen në bazë të rëndësisë dhe të lidhen përsëri me qëllimin e përgjithshëm të TTX. Për të thjeshtuar procesin e trajnimit dhe për ta bërë më të lehtë matjen e suksesit, lidhni objektivat tuaja të të mësuarit me aftësitë ose sjelljet konkrete në të cilat pjesëmarrësit duhet të fokusohen gjatë TTX. Në mënyrë ideale, ju do t'i vendosni këto objektiva mësimore dhe aftësi konkrete bazuar në nevojat dhe nivelet e aftësive të pjesëmarrësve tuaj. Ju mund t'i njihni ato tashmë nëse jeni duke punuar me një komunitet me të cilin jeni njohur. Përndryshe, mund t'ju duhet të kryeni një vlerësim fillestar të nevojave (ndoshta përmes intervistave të informatorëve kryesorë ose një ankete paraprake) për të mbledhur këtë informacion nëse i njihni më pak pjesëmarrësit.

Skenari duhet të jetë sa më afër jetës reale, por në përgjithësi nuk duhet të emërojë njerëz ose organizata reale. Përqendrohuni në situata, sfida dhe përvoja reale. Në raste të rralla, mund të jetë e përshtatshme të përdorni vendndodhje reale, por duhet të merrni parasysh rreziqet e sigurisë dhe kufizimet e mundshme. Renditja e vendndodhjeve reale, për shembull, mund të nënkuptojë se njerëzit shpenzojnë shumë kohë për të kujtuar ose hulumtuar detaje rreth tyre dhe përqendrohen më pak tek skenari.

Për sa i përket kompleksitetit, skenari nuk duhet lërë në hije ose të shpërqendrojë nga mësimi. Zgjedhjet mund t'i ndihmojnë pjesëmarrësit të kuptojnë ndikimin që do të kenë vendimet e tyre, por mbani mend se shtimi i kompleksitetit dhe zgjedhjeve e bën më të vështirë ndërtimin e një TTX dhe gjithashtu do ta bëjë të gjithë ushtrimin shumë më të gjatë.

Gjithashtu mund të përdorni kohën si një element dizajni gjatë skenarit tuaj duke caktuar kohë për ngjarjet që ndodhin gjatë TTX, duke bërë pyetje të kufizuara në kohë ose duke përdorur kthime prapa ose prapa. Në çdo rast, duhet të jeni të qartë për përdorimin e kohës në fillim të skenarit dhe të ruani qartësinë në të gjatë gjithë skenarit.

Në varësi të nivelit të aftësive të moderatorit/lehtësuesit dhe pjesëmarrësve, ju mund të konsideroni përfshirjen e elementeve teknike brenda TTX. Kjo mund të nënkuptojë që pjesëmarrësve u kërkohet të përdorin një mjet, softuer ose proces specifik për të kaluar nëpër skenar. Nëse përfshini një element teknik, jepni kohë shtesë për të përfunduar këto detyra dhe kini gjithmonë një plan rezervë në rast të problemeve teknike ose bëjeni komponentin teknik opsional për të akomoduar nivele të ndryshme aftësish.

Gjithashtu mund të përdorni injektime brenda TTX tuaj. Injektimet mund të jenë të mëdha ose të vogla dhe mund të varen nga pjesëmarrësit ose të jenë të pavarura prej tyre. Në përgjithësi, injektimet përdoren në skenarë më të gjatë duke pasur parasysh sasinë e kohës që kërkohet. Injektimet jepen nga lehtësuesi dhe koha është vendimtare. Për të integruar me sukses një injektim në një skenar, kërkohen

burime lehtësuese si përpara ashtu edhe gjatë lehtësimit të TTX. Përdorimi i injektimeve duhet të përputhet me nevojën për të arritur objektivat e mësimit të paracaktuar.

Planifikimi i një ushtrimi tavoline (TTX)

Para se të filloni të planifikoni ushtrimet e tavolinës, mendoni **për audiencën tuaj të synuar** dhe se si kjo do të ndikojë në objektivat e të mësuarit. Po i drejtoheni gazetarëve, menaxherëve të redaksisë, njerëzve të sigurisë? Secili prej tyre do të punojë me informacione shumë të ndryshme dhe do të jetë përgjegjës për vendime të ndryshme. Nga ana tjetër, disa TTX funksionojnë qëllimisht për një entitet shumë më të gjerë - për shembull një redaksi e tërë - për të kuptuar më mirë se si njerëzit komunikojnë dhe marrin vendime në të. Mund të punoni me pjesëmarrës që kanë nivele shumë të ndryshme të aftësive, njohurive dhe përvojës së sigurisë dixhitale. Merrni pak kohë për të modifikuar TTX-të në mënyrë që të adresojë më së miri nevojat e tyre specifike.

Pasi të keni përcaktuar audiencën tuaj të synuar, **planifikoni objektivat e të mësuarit dhe merrni parasysh aftësitë ose sjelljet specifike, për të cilat do t'i trajnoni**. Përzgjedhja e aftësive konkrete përpara trajnimit është thelbësore për t'ju ndihmuar të shtrini fokusin tuaj si trajner, të vendosni objektiva të prekshme të të mësuarit për pjesëmarrësit dhe do të ndihmojë në vendosjen e një standardi për të matur nëse trajnimi ishte efektiv. Shihni një listë të aftësive të modelit te nënseksioni brenda çdo dokumenti TTX të titulluar "Aftësi/Sjellje për t'u trajnuar para ose pas TTX". Mund të jetë tunduese të mbulohen sa më shumë objektiva të të mësuarit brenda një TTX të vetëm, por është më efektive të mbahet një trajnim më i kufizuar që mbulon objektiva të veçanta të të mësuarit. Mos harroni se audienca juaj ka një hapësirë kohe dhe vëmendje të kufizuar.

Kuptoni se sa kohë do t'ju duhet për TTX. Ndërsa ndonjëherë agjencitë qeveritare ose korporatat krijojnë TTX që zgjasin shumë ditë, audienca juaj mund të jetë shumë më e kufizuar sa i përket kohës. Puna, kujdesi dhe angazhimet e tjera të jetës së pjesëmarrësve tuaj duhet të merren parasysh. Zakonisht, një TTX që ka 4-6 pyetje ose injeksione mund të marrë rreth 1 - 1.5 orë. Kjo gjithashtu varet shumë nga madhësia e grupit tuaj. Grupeve më të mëdha zakonisht do t'u duhet më shumë kohë për të përfunduar një TTX. Gjithashtu do t'ju duhet të merrni parasysh kohën për një përmbledhje dhe të rishikoni objektivat e të mësuarit dhe aftësitë ose sjelljet konkrete që dëshironi të zbatojnë pjesëmarrësit pas skenarit. Pjesëmarrësit mund të kenë nevojë për trajnime të mëtejshme ose ndjekje për të qenë në gjendje të zbatojnë me sukses aftësitë ose sjelljet konkrete.

Konsideroni hapësirën që keni në dispozicion për aktivitetin. Nëse zhvillohet personalisht, është ideale që ushtrimi të zhvillohet në një hapësirë e cila lejon bashkëpunim. Një dhomë me tavolina dhe karrige të rehatshme ka të ngjarë më të favorshme për një TTX sesa një sallë leksionesh. Gjithashtu duhet të siguroheni që të ketë Wi-Fi me cilësi ose pajisje të tjera teknologjike, si një projektor. Hapësira gjithashtu duhet të jetë e aksesueshme për të gjithë (p.sh., aksesi për karriget me rrota, banjat që përfshijnë gjininë, mundësitë e përshtatshme të transportit, etj.).

Vendosni nëse do të ketë disa trajnerë (lehtësues) dhe ç'role do të kenë ata. Mund të ketë më shumë kuptim që një lehtësues të drejtojë TTX-në dhe të tjerët të ndihmojnë në rastet kur do të ketë ndarje me grupe më vogla ose me detyra specifike. Lehtësuesit gjithashtu mund të praktikojnë më parë se si do t'i trajtojnë disa elementë.

Përcaktoni se çfarë burimesh do t'ju nevojiten për TTX. Mund të krijoni një prezantim, një fletëpalosje ose materiale të tjera për të shfaqur gjatë skenarit, pyetje/nxitje dhe/ose injektime. Gjithashtu është e rëndësishme t'u sigurohen pjesëmarrësve materiale për të marrë shënime.

Lehtësimi i ushtrimeve të tavolinës

Lehtësimi i një ushtrimi tavoline ndryshon nga drejtimi i një trajnimi tradicional të sigurisë dixhitale ose sesioni i përmirësimit të aftësive. Në trajnimin tradicional të sigurisë dixhitale, trajnerët priren të flasin shumë dhe pritet të ndajnë njohuritë e tyre me pjesëmarrësit. Ndërsa, në një trajnim TTX, shumica e të folurit dhe punës ndodh mes vetë pjesëmarrësve, pasi ata diskutojnë skenarin dhe marrin vendime. Lehtësuesi luan rolin e kujdesatarit të procesit, duke u siguruar që TTX të zhvillohet pa probleme dhe të përmbushë qëllimet e tij. Lehtësuesi prezanton ushtrimin, kontekstin dhe sfondin; u përgjigjet disa pyetjeve themelore; dhe shton injektime. Rekomandime të tjera për lehtësimin e TTX përfshijnë:

- Sigurohuni që të jeni të familjarizuar me ushtrimin TTX
- Mbani mend cilat janë qëllimet dhe objektivat e të mësuarit të ushtrimit dhe drejtoni diskutimet në mënyrë që pjesëmarrësit të arrinë ato qëllime.
- Njihini me rolet dhe pritshmëritë në mënyrë të qartë në fillim dhe gjatë TTX.
- Vëzhgoni me vëmendje orën dhe sigurohuni që po respektoni dhe maksimizoni kohën që keni me pjesëmarrësit.
- Sigurohuni që hapësira të jetë e sigurt dhe mikpritëse dhe që njerëzit të ndjejnë se këndvështrimet e tyre dëgjohen dhe merren parasysh.
- Kur një pjesëmarrës përmend një praktikë të mirë, theksoje atë! Kjo mund të rrisë besimin dhe të inkurajojë pjesëmarrjen e mëtejshme.
- Nëse nuk e dini përgjigjen e një pyetjeje, mos kini frikë ta thoni këtë dhe angazhohuni ta qartësoni këtë pas trajnimit. Përdorni hapësirat e komunitetit si për shembull Team CommUNITY's Mattermost, për të marrë përgjigje për pyetjet që mund të mos jeni në gjendje t'i kuptoni vetë.
- Nëse është e mundur, mblidhni komente gjatë zhvillimit të ushtrimit dhe jini gati për të bërë mikro-rregullime. Nëse planifikoni të përsërisni disa herë një ushtrim, mund të mblidhni gjithashtu reagime në fund të seancës për të kuptuar më mirë se si mund ta përmirësoni.
- Nëse ushtrimi shkon në një drejtim tjetër nga ai i synuar fillimisht, mos u shqetësoni! Tregohuni fleksibël, por sigurohuni që ushtrimi të adresojë përfundimisht rezultatet e të nxënit.

Nëse dëshironi udhëzime më të hollësishme, më poshtë sugjerohen udhëzime hap pas hapi që ju ndihmojnë gjatë procesit të lehtësimit.

1. Prezantoni veten (dhe çdo bashkëtrajner tjetër), shpjegoni rolin tuaj dhe përshkruani qëllimin e gjerë të TTX (për shembull: sot, ne do të shikojmë se si një redaksi mund t'i përgjigjet një incidenti sigurie). Ky është momenti për të vendosur gjithashtu disa rregulla bazë si grup.
2. Më pas, përshkruani më në detaje se çfarë do të ndodhë gjatë TTX. Shpjegoni se ka për qëllim të simulojë një situatë fiktive që përafrohet me jetën reale për të kuptuar më mirë përgjigjet tona dhe ato të komunitetit tonë më të gjerë.
3. Në varësi të madhësisë dhe përbërjes së grupit, mund t'i ndani pjesëmarrësit në grupe më të vogla.

4. Prezantojini skenarin pjesëmarrësve, duke përfshirë çdo histori në sfond që mund të jetë e nevojshme.
5. Tregoni skenarin, duke i nxitur të vijojnë ndërtimin e ushtrimit të tavolinës. Tregohuni të disponueshëm për pyetje dhe për të ndihmuar në zgjidhjen e problemeve nëse pjesëmarrësit ngecin.
6. Siguroni injektime sipas nevojës.
7. Inkurajoni pjesëmarrësit të angazhohen dhe t'u përgjigjen kërkesave. Kërkojuni atyre të mbajnë shënime aty ku janë të rëndësishme ose të dobishme. Përdorni përgjigjet tuaja të përgatitura paraprakisht për të ndihmuar nëse pjesëmarrësit janë në vështirësi ose kanë nevojë për shembuj për të filluar.
8. Pasi pjesëmarrësit të përfundojnë ushtrimin, nxitini ata të diskutojnë përfitimet e tyre kryesore nga përvoja dhe mendimet e tyre mbi TTX-të si një metodë trajnimi. Kjo është një kohë e mirë për të regjistruar komente dhe për të kuptuar se çfarë përmirësimesh mund të bëhen në trajnimet e ardhshme.
9. Pasi të përfundojë TTX, kontrolloni nëse ka materiale ose përmbledhje që duhet të ndahen me pjesëmarrësit.

Shtojca 1: Sfondi për Sarën (një person TTX)

Ne krijuam një person të vetëm, Sarën, për të ndërtuar skenarët e ushtrimeve të tavolinës. Kjo na ndihmojë t'i shtonim një ndjenjë qëndryeshmërie TTX-eve dhe t'u jepnim një pikënisje të mirë gazetarëve për të menduar për kërcënimet dhe kontekstin më të gjerë. Ne kemi përfshirë prezantimin tonë të Sarës më poshtë, të cilin lehtësuesit mund ta përdorin për të përshkruar skenarin dhe për të ofruar sfond përpara se të nisin një nga shembujt e skenarëve tanë TTX.

Sara është një gazetare 41-vjeçare. Ajo ka punuar për organizata të ndryshme lajmesh vendase dhe ndërkombëtare për disa vite në vendin e saj të lindjes dhe në vendet fqinje.

Vitin e kaluar, Sara filloi të punojë në vendin e saj me një organizatë investigative të lajmeve të quajtur 'Free Press Now', që raporton shpesh për një sërë çështjesh politike. Këto përfshijnë abuzime të dyshuara të të drejtave të njeriut nga qeveria në detyrë, zyrtarë të korruptuar qeveritarë dhe politika qeveritare që e bëjnë jetën më të vështirë për pakicat etnike në vend.

Për shkak të raportimit të tyre të vërtetë dhe të besueshëm, Free Press Now është bërë një burim informacioni i besueshëm dhe popullor për popullatën lokale.

Pas zgjedhjeve kombëtare 5 muaj më parë, qeveria e re në pushtet ka filluar të kufizojë liritë e shtypit dhe javën e kaluar autoritetet bastisën shtëpitë e tre gazetarëve të njohur në kryeqytet. Së fundmi u bastis edhe shtëpia e Sarës, ndonëse ata që kryen bastisjen morën vetëm disa blloqe shënimesh.

Tabletop Exercises
Skenari 1: Humbje Pajisjeje

Krijuar nga pjesëmarrësit e Fellowship-it të Sigurisë për Gazetarët

Synimi

Të ndihmohen pjesëmarrësit të planifikojnë dhe t'i përgjigjen situatës kur humbet një apo më tepër pajisje, të cilat mund të përmbajnë informacion të fshehtë.

Objektivat e të Nxënit

1. Të identifikohen qasje qw garantojnw komunikim të sigurt mes gazetarëve dhe individëve që janë burim informacioni.
2. Të shërbejë për të ndërgjegjësuar për rreziqet e humbjes së një pajisjeje të tillë, si celular apo kompjuter.
3. Të kuptohen praktikat më të mira për mbrojtjen dhe sigurinë e pajisjeve .
4. Të ndahen qasjet e mira sa i përket përfshirjes dhe largimit të personelit, sidomos në lidhje me sigurinë e pajisjeve.

Aftësi/Sjellje për t'u trajnuar para ose pas TTX (ushtrimeve të tavolinës)

1. Instalimi, konfigurimi dhe përdorimi i Signal (ose një tjetër aplikacioni mesazhesh të sigurt)
2. Vendosja dhe përdorimi i një aplikacioni mesazhesh alternativ, të enkriptuar nga skaji në skaj (siç është WhatsApp ose Facebook Messenger Secret Chat)
3. Instalimi, konfigurimi dhe përdorimi i Mailvelope (ose një opsion tjetër për enkriptimin e emaileve)
4. Enkriptimi/kodimi i një pajisjeje celulare (vendosja e një fjalëkalimi)
5. Vendosja e fjalëkalimeve për aplikacione individuale në pajisjen celulare
6. Ruajtja dhe kriptimi i kopjeve rezervë të të dhënave në pajisjet celulare (duke përdorur shërbime cloud ose hard disk të jashtëm)

Skenari

Një burim i panjohur më parë, kontakton Sarën përmes Facebook Messenger-it, ku i thotë se zotëron informacion të ndjeshëm, të cilin dëshiron ta ndajë me të. Skedari që dëshiron t'i japë, përmban informacion rreth financave të Ministrit aktual të Mbrojtjes..

Duke dashur ta mbajë burimin të sigurt, Sara do të donte ta bindte atë tw transferone informacionin përmes një aplikacioni mesazhesh që është i enkriptuar skaj më skaj.

> **P1- Si mund t'i shpjegojë Sara konceptin e enkriptimit skaj-më-skaj, që ta bindë burimin për rëndësinë e tij?**

- Askush, madje as kompania që ka aplikacionin e mesazheve, nuk do të ketë akses në përmbajtjen e mesazhit. Përmbajtja e mesazhit nuk do të ruhet e pakriptuar as në serverët e kompanisë
- Autoritetet ligjzbatuese nuk mund ta aksesojnë atë përmes kompanisë që ofron shërbimin e mesazheve.
- Nëse një sulmues arrin të hakojë llogarinë që është përdorur për të dërguar mesazhin, ai nuk do të mund të shohë përmbajtjen e mesazheve (përveç nëse ka pasur kopje rezervë të pakriptuara)

P2- Për të garantuar që komunikimi i tyre do të jetë i sigurt në të ardhmen, cilat forma të komunikimit dixhital duhet të përdorë Sara me këtë burim?

- Aplikacion mesazhesh me enkriptim skaj më skaj dhe mesazhe që zhduken
- Email i enkriptuar

Burimi është i kënaqur që Sara po përpiqet që komunikimi i tyre të jetë i sigurt, por ai ende nuk është i sigurt se cilës metodë duhet t'i japë përparësi. Ai i kërkon Sarës disa këshilla për aplikacionet e mesazheve si Signal, Telegram dhe Facebook Messenger, si dhe për emailin e tij.

P3 (Zgjedhje) - Nga perspektiva e sigurisë dixhitale, cilët janë disa faktorë që duhen marrë parasysh kur zgjidhni dhe përdorni aplikacione të ndryshme të mesazheve?

- Numrat e telefonit: shumica e aplikacioneve të mesazheve të enkriptuara nga skaji më skaj kërkojnë numra telefoni dhe në shumë vende numrat e telefonit duhet të regjistrohen, në mënyrë që qeveria të dijë se cili person qëndron pas secilit numër telefoni. Kjo do të thotë se, nëse qeveria do të shikonte ndonjëherë telefonin e Sarës ose të burimit të saj, mund të kuptonte se ato po i dërgonin mesazhe njëra-tjetrës, edhe nëse përdornin pseudonime ose mesazhe që zhdukeshin (i vetmi lehtësim do të ishte fshirja e emrave nga kontaktet, aplikacionet e mesazheve dhe në mënyrë ideale fshirja e emrava nga telefoni)
- Bisedat sekrete: Facebook Messenger dhe Telegram ofrojnë dy mënyra komunikimi, vetëm njëra prej të cilave është e koduar nga skaji në skaj. Kjo mënyrë zakonisht quhet një bisedë sekrete ose diçka e ngjashme, megjithëse shpesh fshihet tek cilësimet
- Mesazhe që zhduken: pothuajse çdo aplikacion mesazhesh modern ka një veçori të mesazheve që zhduken, megjithëse në disa prej tyre ai ofrohet vetëm në modalitetin e bisedës sekrete
- Fshirja e bisedave: kjo është mjaft e thjeshtë, por është e rëndësishme të dalloni se disa aplikacione mesazhesh vetëm arkivojnë bisedat, në vend që t'i fshijnë ato
- Ndërgjegjësimi rreth fotografimit të ekranit (sreenshots): çdo palë keqdashëse në bisedë mund të marrë thjesht një pamje nga ekrani ose—nëse veçoritë e aplikacionit të mesazheve nuk e lejojnë këtë—thjesht të bëjë një foto të ekranit të telefonit të tyre me një telefon tjetër
- Verifikimi me dy faktorë (2FV): një sulmues mund një llogari aplikacionit të mesazheve duke duke arritur të marrë në zotërim numrin e telefonit që është përdorur për regjistrimin e llogarisë dhe duke ridërguar SMS-në e verifikimit tek ajo. Kjo e lejon atë të hiqet si pronari i llogarisë, megjithëse zakonisht nuk i jep akses në historikun e mesazheve. Shumica e aplikacioneve të mesazheve tani kanë mundësinë të kërkojnë

një fjalëkalim shtesë përveç kodit SMS: kjo do të thotë se, edhe nëse një sulmues arrin të marrë numrin e telefonit, ai nuk mund të ketë lehtësisht akses në llogari.
- Fjalëkalime të forta ose fraza kalimi për të hyrë në vetë pajisjen (telefonin)

P4 (Zgjedhje) - Cilët janë disa faktorë për t'u marrë parasysh, nga këndvështrimi i sigurisë dixhitale, kur komunikojmë përmes email-it?

- Burimi duhet të krijojë një adresë të re emaili vetëm për të komunikuar me Sarën
- Emaili i ri duhet të ketë një fjalëkalim të fortë dhe unik dhe vërtetim të fortë me dy faktorë
- Burimi duhet gjithashtu të ketë kujdes nga sulmet përmes mesazheve karrem, si dhe të përdorë teknologji që mund të ndihmojnë në zbutjen e tyre, të tilla si çelësat e sigurisë fizike ose plotësim automatik të fjalëkalimeve
- Idealisht, burimi dhe Sara duhet të komunikojnë përmes PGP, për shembull duke përdorur Mailvelope. Kjo do të thotë se, edhe nëse llogaritë e tyre do të kompromentoheshin, sulmuesi ende nuk do të ishte në gjendje të lexonte përmbajtjen e mesazheve të tyre pa çelësin e tyre PGP

Burimi ia dërgon në mënyrë të sigurt skedarin Sarës dhe ajo e shikon atë në telefonin e saj celular. Ajo është e lumtur që ka këtë informacion dhe del me miqtë e saj për të festuar. Ndërsa është në një festë, ajo humbet telefonin e saj dhe kupton se ka vendosur një fjalëkalim shumë të thjeshtë (1111).

Q5 - Ç'mund t'i ndodhë telefonit të Sarës dhe informacionit brenda tij?

- Kushdo që e gjen telefonin mund ta aksesojë informacionin e fshehtë, nëse e kupton se ku ndodhet
- Kushdo që gjen telefonin mund t'u dërgojë mesazh kontakteve të Sarës dhe të hiqet sikur është ajo
- Kushdo që gjen informacionin në telefon ose mund të zbulojë identitetin dhe rrezikojë sigurinë e kontakteve të Sarës, ose mund të mbledhë informacione që mund të përdoren për inxhinieri sociale
- Sara mund të humbasë seriozisht kredibilitetin e saj si gazetare

Q6 - Ç'mund të bëjë tani Sara për të kufizuar ndikimin mbi sigurinë e vet dixhitale?

- Ajo mund të fshijë informacionet në telefonin e saj në distancë, nëse e ka vënë në punë këtë funksion.
- Ajo mund të hyjë në llogaritë e saj të postës elektronike dhe të mediave sociale nga pajisje të tjera, të ndryshojë fjalëkalimin dhe, nëse është e mundur, të klikojë lidhjen "dal nga të gjitha pajisjet e regjistruara".

Q7 - Cilat janë të mirat dhe të këqijat, nëse ithotë burimit se ajo humbi celularin?

- Diskutim pa përgjigje ekzaktësisht të sakta.

Lajme të mira! Një shok i Sarës, që ishte me të në festë, e gjeti telefonin në pallton e tij. I telefonoi dhe ia ktheu telefonin Sarës të nesërmen.

Q8 - Tani që Sara ka prapë telefonin, çfarë hapash mund të ndërmarrë, nga pikëpamja e sigurimit dixhital të pajisjes së vet, në rast se e humb prapë në të ardhmen?

- Të mbajë parasysh se mund të përdorë zhbllokimin biometrik ndonjëherë. Ka përparësi (askush nuk mund të shikojë mbi shpatullën e Sarës ndërsa ajo fut fjalëkalimin e saj dhe nuk do të kapet as nga kamerat), por dhe disavantazhe (është më e lehtë ta detyrojnë Sarën të zhbllokojë pajisjen e saj).
- Të përdorë fjalëkalime dhe fraza kalimi më të gjata për shkyçjen e telefonit. Të shmang shkyçjet përmes modeleve (të tilla si ato që lidhin pika), pasi ato mund të identifikohen lehtësisht nga një person që shikon, një aparat fotografik ose shenja e gishtit që mbetet në ekran.
- Të kyç aplikacionet (siç janë ato të mesazheve) me një fjalëkalim shtesë, nëse Sara shqetësohet se telefoni i saj mund të përdoret ndonjëherë nga të tjerë.
- Të shkarkojw dhe të përdorë aplikacione që mund të gjurmojnë, lokalizojnë dhe fshijnë në distancë pajisjet.

Q9 - Nga këndvështrimi i organizatës, si do të ishte një proces i mirë pranimi në punë i një anëtari të ri personeli, sa i përket sigurimit të pajisjeve, si celularë dhe kompjutera?

- Të garantohet që i gjithë stafi, pavarësisht nga pozicioni, të kalojë nëpër një proces pranimi dhe të kuptojë rëndësinë e tij
- Organizatat duhet të listojnë qartazi pritshmëritë nga personeli, në lidhje me ndjekjen e praktikave të sigurisë dixhitale të organizatës
- Të identifikohen hapat për t'u ndërmarrë, kur siguria mund të jetë kompromet uar (si p.sh, është vjedhur një telefon, ose është zbërthyer një fjalëkalim)
- Për këdo nga personali që ka nevojë, të jepet asistencë IT

Tabletop Exercises
Skenari 2: Siguria operacionale

Krijuar nga pjesëmarrësit e Fellowship-it të Sigurisë për Gazetarët

Synimi

Të ndihmohen pjesëmarrësit të arrijnë një shkallë të lartë ndërgjegjësimi rreth sigurisë dixhitale dhe të njohin praktikat më të mira brenda organizatës së tyre, kolegëve, dhe/ose gazetarëve në profesion të lirë.

Objektivat e të Nxënit

1. Nga pikëpamja teorike, të kuptohet koncepti i sigurisë dixhitale si një proces i vazhdueshëm, jo si një objektiv i një here
2. Të flasim, të mësojmë dhe të bindim për rëndësinë e sigurisë dixhitale
3. Nga pikëpamja praktike, të diskutohen mundësi për sigurinë e komunikimeve përmes pajisjes tuaj celulare
4. Të sigurohet njohja dhe përdorimi i praktikave më të mira lidhur me trajtimin e skedarëve
5. Të ndërgjegjësojmë lidhur me rregullime llogarish për kompjutera të lidhur në rrjet
6. Të kuptohet rëndësia e modelimit të kërcënimeve

Aftësi/Sjellje për t'u trajnuar para ose pas TTX (ushtrimeve të tavolinës)

1. Vendosja dhe mbajtja e lejeve në platformat bashkëpunuese (d.m.th., Google Drive)
2. (Nëse është e mundur, pasi disa nga këto veçori disponohen vetëm në platformat e ndërmarrjeve) Të shihen regjistrat e aksesit në platformat bashkëpunuese si Google Drive
3. Të vendoset dhe të dhe përdoret vërtetimi me dy faktorë, do të ishte ideale të përdoreshin çelësa fizikë të sigurisë ose mekanizma të ngjashëm rezistent ndaj mesazheve karrem (phishing)
4. Të ndiqen politika të mira të fjalëkalimeve (përdorimi i fjalëkalimeve unike, përdorimi i fjalëkalimeve të gjata, përdorimi i frazave të kalimit) dhe menaxherët e fjalëkalimeve
5. Të enkriptohen dokumentat (duke përdorur Mailvelope, etj)
6. Të instalohet, të konfigurohet dhe të përdoret Signal (ose një tjetër aplikacion mesazhesh i sigurtë)
    a. Të përdoren veçori të përparuara të aplikacionit të mesazheve (si fshirja e mesazheve pas një kohe të caktuar)
2. Të instalohet, të konfigurohet dhe të përdoret Mailvelope (ose një mënyrë tjetër për të enkriptuar emaile)
3. Të punohet në mënyrë të sigurt me skedarët dhe dokumenatat që vinë nga burime të ndjeshme

Skenar

Sara po krijon një ekip gazetarësh për hetimin e korrupsionit lidhur me prokurime publike bërë nga Ministria e Shëndetësisë gjatë Covid-19. Jo të gjithë gazetarët në ekip kanë të njëjtën shkallë aftësish dixhitale/dijesh dhe aftësish praktike për sigurinë. Sara e di se një nga anëtarët e ekipit është shumë dobët në mbrojtje skedarësh.

P1 - Si mund t'i nxisë Sara kolegët e vet të përmirësojnë qasjen ndaj sigurisë dixhitale? Ç'duhet të bëjë Sara për të garantuar praktika sigurie dixhitale, teksa organizon një ekip bashkëpunues?

- Të shpjegojë pse është e rëndësishme siguria dixhitale: kjo mund të përfshijë një shembull se si siguria e dobët dixhitale mund të pengojë ndjeshëm karrierën e një gazetari, se si burimet dhe kolegët kanë gjasa t'u besojnë më shumë nëse keni siguri të mirë dixhitale dhe nevojën për të mbrojtur njerëzit rreth nesh.
- Të diskutojë rreth pajisjeve që përdorin, si i mbrojnë llogaritë e tyre të përdoruesit, si i depozitojnë dhe shkëmbejnë kartelat, si hyjnë në rrjetin e vendit të punës (përdorin pajisje të tyre, apo punojnë në kompjutera të kpmpanisë përkatëse), si bëjnë hyrjen në rrjetin e vendit të punës (lidhje pa fije, apo me kabllo), a përdorin idnetifikimin me 2 faktorë për të siguruar llogaritë e përdoruesve dhe çfarë disipline zbatojnë për fjalëkalimet e tyre (a i ripërdorin fjalëkalimet, a përdorin menaxher fjalëkalimesh).
- Të vendosë se si duhet të komunikojë ekipi, si duhet të depozitojë dhe hyjë në skedarë. Thelbi i hapit të dytë është të garantohet se gjithkush ndjek të njëjtin protokoll lidhur me veprimtaritë e përmendura më herët.
- Të shohë mundësinë e trajnimit të ekipit për përdorimin e protokollëve të vendosur rishtas. Pas caktimit të rregullave, ekipi duhet të bëjë një provë, për të testuar aktualisht rrugët e reja të komunikimit dhe për të parë nëse ka ndonjë gjë në proces që çalon dhe që është e nevojshme të zgjidhet.

P2 - Si do të ruajnë dhe shpërndajnë skedarw audio dhe dokumente prej burimeve Sara dhe ekipi i saj?

- Të kufizojnë cilët kanë akses në skedarë dhe dosje të ndryshme, të përdorin cilësimet e ndarjes së materialeve me kujdes në vende si Google Drive
- Të shkurjajojnw stafin që të marrë skedarë dhe dokumenta jashtë ambjentit të punës (me usb, bashkëngjitur në emaile…), gjë që mund të gjerojnë platformën e sulmit dhe të rrisin rrezikun e rrjedhjeve/hakimeve.
- T'i kërkojë ekipit të përdorë kompjuterat e punës vetëm për të hapur skedarët e punës
- Të kufizojnë instalimet në komjuterat e punës, të sigurohen që ata të kenë gjithmonë fjalëkalime të forta dhe softuer të përditësuar

P3 - Si do të garantojë Sara dhe ekipi i saj se komunikojnë në mënyrë të sigurt?

Duke ndihmuar kalimin e tërë ekipit në të njëjtën platformë dhe duke siguruar që cilido të jetë i zoti në përdorimin e saj, Sara mund të ndihmojë ekipin e vet të vendosë një rrugë të sigurt komunikimi mes tyre.

Të shihet mundësia e:

- Të zhvendosen shumica e bisedave në Signal, me opsionin e mesazheve që zhduken dhe të kopjohen mesazhet që duhen arkivuar
- Të përdoret PGP në e-maile

- Të krijohet rregulla të forta sigurie për llogaritë e e-maileve (fjalëkalime unike, verifikim me 2 faktorë)

Dy javë para botimit të raportit të tyre, Sarës i vjen një telefonatë nga burimi kryesor qeveritar në këtë hetim. Sara e njeh mirë burimin dhe i beson atij. Gjatë telefonatës, burimi thjesht thotë “Qeveria ka dijeni - ka pasur rrjedhje të informaciont” dhe e mbyll telefonin.

P4 - Nga pikëpamja e sigurisë dixhitale, cilat janë disa nga hapat e parë që duhet të ndërmarrë Sara, si përgjigje ndaj një rrjedhje të mundshme informacioni?

- T’u kërkojë të gjithëve brenda ekipit të saj të ndryshojnë fjalëkalimet, në rast se një sulmues mund të ketë marrë fjalëkalimin e një prej llogarive të tyre.
- Të mbajë parasysh faktin se qeveria jo domosdoshmërisht ka nevojë të hyjë në redaksinë e lajmeve; është e mundur që ata ta kenë mësuar informacionin, për shembull, duke hetuar se cili punonjës i qeverisë po printonte çfarë.
- Të kryejë një hetim të vogël brenda redaksisë: të kontrollojë nëse të gjithë kanë ndikur protokollet, kush kishte akses në dosjet dhe informacionin që u zbulua dhe çfarë saktësisht u zbulua në radhë të parë. Nëpërmjet përdorimit të kontrollit të aksesit dhe kontrollit të variantit, ju mund të gjurmoni më kollaj aksesin në pjesët individuale të të dhënave, për të cilat po punoni.
- Të mendoj nëse duhet ta shpejtoj publikimin.

Sara mëson se rrjedhja erdhi që nga brenda organizatës së saj. Një grafist kishte akses te disku i përbashkët Google Drive i entit (pavarësisht se nuk po merrej me hetimin). Sara këtë e kuptoi duke parë regjistrin e kontrollit të aksesit të Google Drive dhe duke konstatuar se ekipi grafik kishte akses te gjthiçka në rrjet, për shkak të natyrës së punës së tyre, dhe duke parë që një grafist kishte ndarë rastësisht një dokument me një klientin e tyre, i cili punonte për qeverinë, në vend që ta ndante me dokumentin me një mik në redaksi që kishte të njëjtin mbiemër.

P5 - Ç’mund të kishte bërë ndryshe Sara në këtë situatë?

- Sara duhet të krijojë protokolle të sigurta që përdoren vetëm nga ekipi i saj investigues. Ajo duhet të sigurohet se ekziston një sistem i qartë i lejeve dhe se ai ndiqet në praktikë.
- Ekipi duhet të punojë me grafistët në mënyrë të tillë që ata të kenë informacion vetëm sipas nevojës: atyre nuk duhet t'u jepet asnjë detaj sekret ose i ndjeshëm përveç rasteve kur është absolutisht e nevojshme për publikimin.
- Sara gjithashtu duhet ta konsiderojë sigurinë dhe privatësinë si proces dhe jo si gjendjet; është diçka që duhet të përsëritet vazhdimisht.

Tabletop Exercises
Skenari 3: Ngacmim dhe cënim i imazhit

Krijuar nga pjesëmarrësit e Fellowship-it të Sigurisë për Gazetarët

Synimi

Të ndihmojmë pjesëmarrësit të konceptojnë se si të përgatiten më mirë dhe t'u përgjigjen përpjekjeve për cënimin e imazhit të tyre dhe ngacmimeve në internet.

Objektivat e të mësuarit

1. Të identifikohen metoda dhe masa zbutëse për gazetarë që ndeshen me ngacmime dhe cënim të imazhit në rrjetet sociale
2. Të kuptosh si mund të grumbullohet informacioni në rrjete sociale dhe të përdoret kundër gazetarëve dhe punonjësve të redaksisë
3. Të eksploroni marrëdhënien mes gjinisë dhe ngacmimeve, si dhe implikimet për sigurinë
4. Të diskutoni sesi një organizatë mediatike mund të ndërtojë procedura dhe praktika për të mbrojtur stafin dhe kontraktorët që janë në shënjestër për ngacmime dhe cënim të imazhit
5. Të konsideroni plane emergjente për gazetarët që nuk kanë mbështetje nga redaksia (për shembull, gazetarët e lirë dhe stafin e jashtëm)
6. Të tregoni histori rreth sigurisë dhe të bindni të tjerët, si mund të flasim me njerëzit që tradicionalisht nuk përballen me ngacmime se është një problem madhor që kërkon veprim dhe mbështetje të koordinuar organizative
7. Siguria organizative: vendosja e politikave brenda organizatave, gjetja e mënyrave në të cilat organizatat mund të mbështesin më së miri gazetarët që po përballen me sulme ngacmimi

Aftësi/Sjellje për t'u trajnuar para ose pas TTX

1. Menaxhimi dhe përditësimi i cilësimeve të privatësisë në platformat kryesore të mediave sociale
2. Përdorimi i mjeteve të sigurisë në platformat kryesore të mediave sociale, të tilla si raportimi dhe bllokimi. Kjo përfshin të kuptuarit se si të përdoren mekanizma të tillë dhe çfarë saktësisht bëjnë ata
3. Konfigurimi dhe përdorimi i verifikimit me dy faktorë, në mënyrë ideale me çelësa fizikë të sigurisë ose mekanizma të ngjashëm rezistent ndaj phishing

Skenari

Sara po punon për një artikull për minoritetet etnike në qytetin e saj dhe sesi politikat qeveritare po nxisin të rritet margjinalizimi në këto grupe. Para disa javësh, Sara spikati në rrjetin e saj social

komente ku ajo gjithashtu ndan edhe punën e saj. Edhe ajo ka filluar të marri komente urrejtje dhe poshtëruese që janë shkruar nga keqdashës të ndryshëm duke e shenjestruar atë direkt.

P1 - Cilat janë disa nga hapat që mund të marrë Sara për t'i bllokuar dhe raportuar personat që bëjnë këto komente?

- Ajo mund të përdorë funksionet për të bllokuar dhe raportua, që ofrohen nga shumica e platformave të medias sociale
- Ajo mund të kontaktojë kompanitë e rrjeteve sociale (personalisht ose përmes organizatës së saj) për të raportuar shkallën e lartë të ngacmimeve
- Të çaktivizojë postimet dhe përgjigjet në profilin e saj
- Të jetë më selektiv se kush mund ta gjejë atë në rrjetet sociale
- Të zgjedhë të mos etiketohet në mediat sociale

Të përpiqet të bllokojë dhe të raportojë disa nga nxitësit e mërzitur nga grupi i keqdashësëve, që drejtojnë grupin për të rritur gjuhën e urretjes kundër Sarës. Disa nga komentet gjithashtu sugjerojnë kërcenime dhe dhunë për atë, direkt ose tërthorazi.

P2 - Cilat janë disa nga mënyrat me të cilat Sara mund të hetojë këtë sulm kundër saj, për të përcaktuar nëse është pjesë e një fushate më të madhe, më të bashkërenduar, apo diçka më e organike?

- Ajo mund ta hetojë vetë gjendjen, si edhe t'u kërkojë kolegëve mbështetje në hetim
- Ajo mund të kontrollojë nëse trollët (keqdashësit) përdorin të njëjtën gjuhë, fjalë kyçe ose hashtags. Nëse e bëjnë këtë, ka të ngjarë të jetë një fushatë e koordinuar
- Varet nga platforma. Në Instagram, ka opsione të gjera për të parë informacione rreth llogarive specifike - kur është krijuar, sa njerëz e përdorin atë, sa shpesh e ka ndryshuar emrin, etj.
- Kontrolloni nëse është përforcuar nga ndonjë media
- Shihni kohën më të zakonshme të postimit

Ajo i tregon kolegëve të vetë për postimet, por shumica e anëtarëve meshkuj të ekipit, përfshirë redaktorin , i thonë të mos shqetësohet dhe se problemi do të zhduket vetvetiu. Ajo është e shqetësuar, ndjen se ekipi i saj nuk i kushton rëndësi dhe nuk e kupton problemin.

P3- Në vend që t'i thuhet Sarës të mos shqetësohet, cilat janë disa nga rrugët me të cilat ekipi dhe organizata mund ta përkrahin Sarën, sidomos për sa i përket pranisë së saj në internet dhe sigurisë digjitale?

- Të ndihmohet për një vlerësim të plotë të situatës
- Të rishikohet së bashku me Sarën praktikat e sigurisë digjitale dhe masat që janë marrë për të përmirësuar situatën nëse është e nevojshme.
- Të merren praktika dhe përvoja e përbashkët nga të tjerë brenda organizatës.
- Lejoni njerëzit që besoni të menaxhojnë llogarinë tuaj ose ta shikojnë atë në mënyrë që të mos ekspozoheni drejtpërdrejt ndaj atyre fjalëve dhe kërcënimeve, por të mund të keni ende një prani
- Organizata mund të ndihmojë në kërkimin e modeleve në ngacmimet
- Të gjurmohet sesi ngacmimi kalon nëpër postimet e organizatës dhe jo vetëm në ato të Sarës

- Të përshkallëzohet kjo tek ekipi i sigurisë dhe të ndihmojnë me hetimin

Një ditë, fotografitë personale të Vjollcës hidhen në internet nga njëri prej troll-ëve. Fotot, të cilat i kishte postuar në rrejtet sociale vite më parë, janë personale dhe, në disa raste, përfshijnë informacione të ndjeshme.

Injektim - Jepuni pjesëmarrësve 1 deri në 4 foto. (Fotot i gjeni te aneksi i këtij dokumenti). Në fotot shembull përfshihen:

- Sara dhe qeni i saj duke shëtitur jashtë shtëpisë
- Sara duke tymosur marihuanë
- Sara dhe një grup i miqve të saj më të ngushtë për pushime
- Sara duke punuar në redaksinë e vet

Diskutoni me grupin e pjesëmarrësve pse secila nga këto foto mund të jetë e ndjeshme.

P4 - Cilat janë disa mënyra se si dikush mund t'i ketë aksesuar informacionet E Sarës në internet, siç janë postimet e vjetra në mediat sociale?

- Miqtë e Sarës postuan foto me cilësime të dobëta të privatësisë
- Dikush ka hyrë në llogaritë e Sarës
- Një nga kontaktet e Sarës në mediat sociale mund t'i ketë ruajtur fotot për t'i ndarë më vonë
- Fotografitë e Sarës në rrjetet sociale mund të ishin gjetur nga një motor kërkimi

P5 - Ç'hapa mund të ndërmarrë Sara në përpjekje për të parandaluar rrjedhje të mëtejshme në internet të informacioneve të lidhura me të?

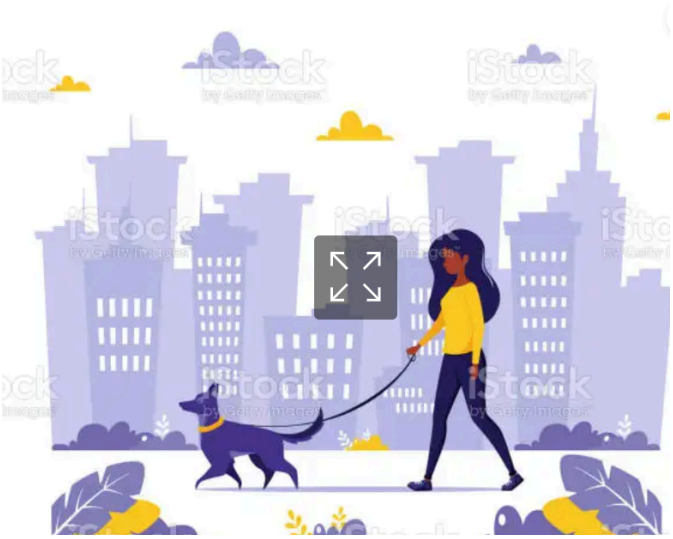
- Të fshijë foto të vjetra
- Të fshijë llogari
- Të kyçë llogari
- Të ngarkojë foto të reja, por që zbulojnë pak informacione rreth saj
- Të marrë një raport nga shoqëria e medias shoqërore që përmbledh krejt të dhënat që ata kanë rreth saj
- Të raportojë fotot që janë postuar së fundi/ të raportojë llogaritë, nga të cilat ato janë postuar
- Të vazhdojë të postojë përmbajtje pune, edhe nëse poston më pak përmbajtje personale. Nëse largoheni nga interneti, trollët do të kenë fituar
- Merrni një pamje (fotografi ekrani) të postimeve, dokumentojini ato sa më shumë që të jetë e mundur. Regjistroni pseudonimet në internet të trollëve

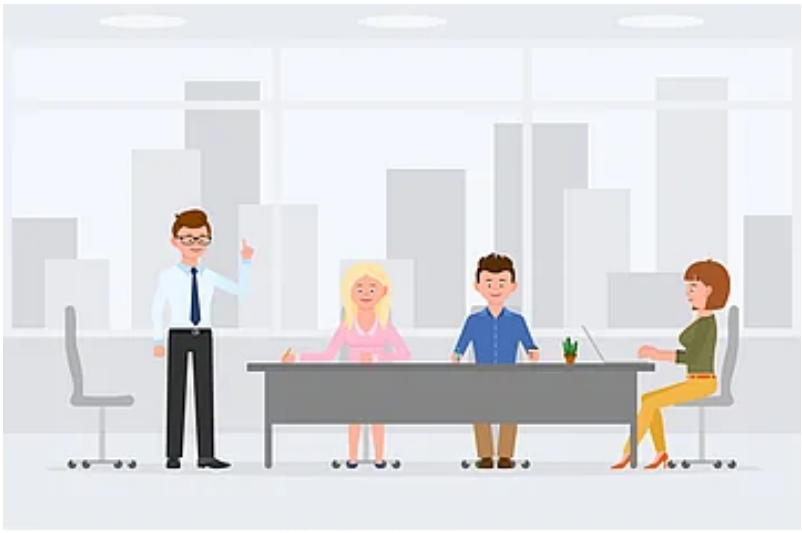
P6 - Ç'hapa mund të kishin ndërmarrë Sara dhe organizata e saj për të penguar mbledhjen e këtyre informacioneve dhe hedhjen e tyre në internet, veçanërisht nga pikëpamja e sigurisë dixhitale?

- Të krijonin një grup miqsh të ngushtë të cilët janë të vetmit që shohin foto personale dhe postime personale në mediat sociale
- Të mos postonin fare informacione të ndjeshme (si fotoja me lidhje)
- Të mos postonin foto që zbulojnë informacione private si vendndodhjen

- Të hapnin llogari biznesi në mënyrë që ajo të ketë një prani në internet që nuk ka lidhje me jetën e saj personale
- Të vendosin jalëkalim të fortë dhe politika 2FA (verifikim me dy hapa) për llogaritë e mediave sociale

Aneks 1: Injektoni Shembuj fotosh





© CanStockPhoto.com

Tabletop Exercises
Skenari 4: Autoritetet hyjnë në redaksi

Krijuar nga pjesëmarrësit e Fellowship-it të Sigurisë për Gazetarët

Synimi

Të ndihmohen pjesmarrësit të përgjigjen në teori dhe praktike ndaj hyrjes së autoriteteve në redaksinë e tyre

Objektivat e të mësuar

1. Të sigurohet një plan komunikimi rezervë dhe komponentët teknik të jenë gati në rast se nuk është i mundur aksesi nw redaksi apo në një pajisje personale
2. Të kuptohet praktika më e mirë, kur vjen puna për sigurimin e pajisjeve digjitale brenda një redaksie lajmesh, apo një organizate
3. Të identifikohen mënyra të tjera për të siguruar materiale të ndryshme në një pajisje digjiitale, si në një kompjuter, apo aparat celular
4. Të planifikoni për informacionin e komprometuar në përgjigje të autoriteteve që hyjnë dhe bastisin redaksinë
5. Të eksplorohen koncepte rreth modeleve të kërcënimeve dhe parapërgatitjejes, për individë dhe organizata

Aftësi/Sjellje për t'u trajnuar para oise pas TTX

1. Përdorimi i një mjeti të tillë si VeraCrypt ose i ngjashëm për të kriptuar të dhënat në hard drive dhe memorie të jashtme
2. Modelimi i kërcënimeve, veçanërisht në aspektin e trajtimit të autoriteteve dhe bastisjeve të zyrave: si të vlerësohen rreziqet, të përgatiten për një rast të tillë dhe të informohen pas një rasti të tillë
3. Siguria organizative dhe e komunitetit, konkretisht si të punohet me redaktorët, menaxherët dhe avokatët gjatë situatave me stres të lartë dhe të identifikohet se cilat pyetje duhet t'i bëhen cilit person
4. Përdorimi i cilësimeve brenda Microsoft Office dhe Google Drive për të parë se cilët skedarë janë aksesuar së fundi dhe kur
5. (I avancuar) Nëse organizata ka regjistra të plotë të aksesit përmes një abonimi premium Google Drive ose O365, duke hyrë dhe duke punuar me regjistra të tillë
6. Të kërkohet tek historia e kërkimit dhe aksesit të skedarëve në shfletuesit kryesorë të internetit dhe sistemet operative

Skenari

Sara punon në redaksinë e lajmeve, me gati 20 njerëz. Është një mëngjes i ngarkuar të hëne, me 15 gazetarë dhe staf tjetër që punojnë në redaksinë e lajmeve, me 5 kolegë të tjerë që punojnë në distancë. Në orën 10 paradite, mbërrijnë në redaksi gati 50 policë. Ata kanë një urdhër që ia tregojnë redaktorit dhe më pas futen me forcë, ndërsa në të njëjtën kohë kërkojnë që të gjithë gazetarët dhe stafi të largohen menjëherë.

Sara dhe kolegët e saj mblidhen jashtë dhe diskutojnë për mënyra se si ta mbajnë organizatën e tyre mediatike që të operojë të qetë dhe të sigurtë.

P1 - Cilat janë disa prioritete në një situatë si kjo?

- Kontaktoni me një avokat për të konsultuar çdo hap tjetër
- Kontaktoni kolegët që punojnë në distancë
- Kontrolloni se kush i ka celularët me vete dhe cilët kanë mbetur në redaksi

P2 - Cilat janë disa nga mënyrat me të cilat Sara dhe kolegët e saj mund të komunikojnë në mënyrë të sigurt gjatë kësaj kohe?

- Krijoni një bisedë në grup në WhatsApp/Signal
- Mund të jetë një ide e mirë për të komunikuar përmes numrave personalë dhe jo të punës. Përndryshe, biseda mund të sinkronizohet me pajisjet që janë ende në zyrë

P3 - Si duhet të menaxhojnë Sara dhe kolegët e saj llogaritë e organizatës në internet, si faqet e internetit dhe llogaritë e mediave sociale?

- Ndryshoni menjëherë fjalëkalimet
- Nëse është e mundur të dilni në distancë nga pajisjet që janë ende në zyrë, bëjeni këtë, por konsultohuni me avokatët fillimisht në mënyrë që kjo të mos konsiderohet ngacmim i provave (mund të varet shumë nga vendndodhja/juridiksioni)
- Konsultohuni me avokatët përpara se të postoni në lidhje me bastisjen e policisë

Sara kujton se teksa po dilte nga redaksia, pa policinë që nisi të vendoste kompjuterë, pajisje dhe letra në çanta. Sara mundi të largohej me telefonin e saj, por laptopi i saj mbeti në redaksi. Grupi i kolegëve vlerëson shpejt se çfarë informacioni mund të marrë policia.

P4 - Si duhen siguruar pajisjet në redaksinë e lajmeve?

- Kompjutera të kyçur me fjalëkalime të fortë
- Kyçje ekranësh, të aktivizuara pas një kohe të shkurtër
- Usb të enkriptuara dhe hard disk i jashtëm

Gjatë diskutimit mes tyre, jashtë zyrës, redaktori vë në dukje se kanë harruar të kyçin kompjuterat e tyre teksa dolën nga zyra.

Policia largohet nga redaksia pas dy orësh, duke lejuar gazetarët të rikthehen. Stafi u mblodh për të diskutuar për informacionet e mundshme që policia mund të ketë marrë, gjithashtu diskutuan kërcënimet e natyrës së ngjashme në vijim.

P5 - Cilat janë disa mënyra se si një redaksi mund të vlerësojë menjëherë ndikimin e një bastisjeje nga autoritetet?

- Shikoni se çfarë dosjesh letre, nëse ka, janë marrë ose janë riorganizuar (nëse dosjet janë riorganizuar, do të thotë se policia mund t'i ketë fotografuar)
- Kompjuterët zakonisht kanë një histori kërkimi / aksesi skedari / shfletuesi, shikoni edhe këtë. Ju mund të shihni skedarët e fundit në Microsoft Word dhe disa histori në shfletues nëse përdorni Google Docs. Nëse historiku i skedarëve është pastruar, kjo do të thotë gjithashtu se dikush mund të jetë përpjekur të fshijë shenjat
- Nuk ka gjasa që ndonjë malware të jetë instaluar gjatë bastisjes, por nëse jeni të shqetësuar për këtë, konsultohuni me një profesionist të specializuarë ligjor të malware

P6 - Si duhet të sigurojë organizata që ata të mos rrezikohen më tej nga kjo bastisje e policisë?

- Ndryshoni fjalëkalimet, për çdo rast
- Bisedoni me një avokat për atë se çfarë ishte policia dhe çfarë nuk lejohej të hynte gjatë bastisjes
- Nëse ata përdornin emra të koduar ose pseudonime për kërkimin e tyre, qarkullojini ato

Disa javë më vonë, redaktori i redaksisë thërret të gjithë gazetarët dhe stafin bashkë. Ata duan të kuptojnë çdo kërcënim të ngjashëm me të cilin mund të përballet redaksia në të ardhmen.

P7 - Për sa i përket modelit të kërcënimeve dhe sigurisë digjitale, si mund t’i identifikojnë individët dhe organizatat kërcënimet me të cilat mund të përballen?

- Bëni pyetjet standarde të modelimit të kërcënimit: çfarë informacioni kanë ata, kush mund të jetë i interesuar për t'i aksesuar ato dhe cilat do të ishin pasojat nëse kundërshtarët e tyre ia dilnin
- Kur renditni kundërshtarët, mendoni si për motivin (çfarë do të dëshironin të bënin dhe pse) ashtu edhe për aftësitë (çfarë janë në të vërtetë të aftë të bëjnë, çfarë mjetesh teknike, ligjore, organizative dhe financiare kanë?)

Tabletop Exercises
Skenari 5: Autoritetet hyjnë në banesën e gazetarit

Krijuar nga pjesëmarrësit e Fellowship-it të Sigurisë për Gazetarët

Synimi

T'u japë gazetarëve aftësitë teorike dhe teknike për të garantuar sigurinë digjitale më të mirë të mundshme në mjedisin e tyre shtëpiak

Objektiva e mësuar

1. Të kuptohet se si të sigurohen pajisje digjitale që gjenden në shtëpi
2. Të aplikohen masa mbrojtëse për blloqet e shënimeve
3. Të nisni fshirjen e skedarëve në distancë dhe të kuptoni anët pozitive dhe negative të këtij veprimi
4. Të kufizoni aksesin në informacionin që është kompromet uar
5. Të përgatiteni për rastin kur autoritetet hyjnë në shtëpinë e gazetarit
6. Bëjini pjesëmarrësit të mendojnë pak për sigurinë organizative dhe të komunitetit, veçanërisht se si të punojnë me redaktorët, menaxherët dhe avokatët gjatë situatave me stres të lartë dhe të identifikojnë se çfarë pyetje duhet t'i drejtohet cili person

Aftësi/Sjellje për t'u trajnuar para ose pas TTX

1. Përdorimi i një mjeti të tillë si VeraCrypt ose i ngjashëm me të për të kriptuar të dhënat në hard disk ose memorie të tjera të jashtme
2. Modelimi i kërcënimeve, veçanërisht në aspektin e përballjes me autoritetet dhe bastisjeve në shtëpi: si të vlerësohen rreziqet, të përgatiten për një të tillë dhe të informohen pasi janë përballur me një rrezik
3. Aktivizimi i mjeteve të tilla si Apple's Find My ose Android/Samsung Find të cilat mund të përdoren për të mbyllur ose fshirë pajisjet nga distanca
4. Përdorimi i cilësimeve brenda Microsoft Office dhe Google Drive për të parë se cilët skedarë janë aksesuar së fundi dhe kur
5. (I avancuar) Nëse organizata ka regjistra të plotë të aksesit përmes një abonimi premium Google Drive ose O365, duke hyrë dhe duke punuar me regjistra të tillë
6. Duke parë historitë e kërkimit dhe aksesit të skedarëve në shfletuesit dhe sistemet operative të njohura të internetit

Skenar

Pas zgjedhjeve kombëtare të mbajtura 5 muaj më parë, qeveria e re në pushtet ka nisur t'i drejtojë autoritetet të kufizojnë liritë e shtypit dhe autoritetet bastisën shtëpitë e tre gazetarëve të njohur në kryeqytet. Si përgjigje, Sara dhe disa kolegë u mblodhën dhe diskutuan mënyrat për të mbrojtur veten dhe informacionin e tyre nëse përballen me një skenar të ngjashëm.

P1 - Cilat janë disa gjëra që një gazetar duhet të marrë parasysh kur vendos të ruajë informacionin në shtëpinë e tij?

- Ruajtja e pajisjeve në shtëpi në një vend të sigurt
- Enkriptimi dhe mbrojtja me fjalëkalim në të gjitha pajisjet
- Mos përfshini informacionin e burimit në dokumente
- Mbani inventarin e informacionit ku ruhen (por mbajeni edhe këtë të sigurt!)
- Informacion jo dixhital: jini të vetëdijshëm për kopjet fizike
- Ekzizston mundësia për të mos mbajtur asgjë në shtëpi
- Ndiqni ligjet e vendit tuaj si dhe politikat e organizatës
- Jini të vetëdijshëm për pasojat ligjore të ruajtjes së informacionit të ndjeshëm në shtëpi në vend që ta ruani në zyrë
- Kush ka akses në shtëpinë dhe pajisjet tuaja?

P2 (opsionale) - Cilat janë disa praktika më të mira rreth ruajtjes së shënimeve në shtëpi?

- Merrni parasysh që të shkatërroni atë që nuk ju nevojitet
- Mos i mbani të gjitha shënimet në një vend – më pak informacion për t'u aksesuar lehtësisht
- Fshihni shënimet
- Kasafortë, kyç dhe çelës, mbaje të sigurt!
- Çfarë niveli të informacionit të ndjeshëm duhet të mbahen në shtëpi?
- Përdorimi i shkurtimeve, i fjalëve që kanë kuptim vetëm për ju

P3 - Çfarë masash mund të merren për të siguruar sa më mirë pajisjet elektronike (kompjuterë, harddisqe, USB, etj.)

- Enkriptim
- Mbrojtje me fjalëkalim
- Ruajte të dhënash larg vendit të punës
- Merrni parasysh asgjësimin e sigurt të pajisjeve të vjetra, veçanërisht ato që nuk përdoren më

Sot, Sara doli nga shtëpia në orën 9 të mëngjesit për të marrë një kafe dhe për të marrë ushqime. Kur u kthye një orë më vonë, dera e banesës së saj ishte e hapur. Sara hyri në banesën e saj ku gjeti dy burra që kontrollonin në tavolinën e saj dhe dhomën e gjumit. Njëri nga burrat po lexonte shënimet e Sarës, ndërsa tjetri mbante një çantë me laptopin e Sarës brenda. Sara pa që në tavolinë mungojnë çelësat USB dhe hard disqet e jashtme. Dy burrat janë të veshur me veshje civile, por Sara hamendësom se një farë mënyre ata punojnë për qeverinë.

Zgjedhja 1 - Sara flet shkurtimisht me dy burrat dhe mund të largohet e sigurt nga shtëpia e saj. Ajo shkon në shtëpinë e një shoku aty pranë.

P4 (opsionale) - Duke ditur që disa nga informacionet e saj, veçanërisht nga shënimet e saj , janë kompremetuar, kë duhet të informojë Sara për këtë incident?

- Të informojë redaktorin dhe avokatët e redaksisë
- Përpara se të kontaktojë ndonjë burim që mund të jetë përmendur në fletore, të bisedojë fillimisht me redaktorin dhe redaksinë e gjerë, si dhe me profesionistët e

sigurisë (nëse burimet janë përmendur vetëm me pseudonim, por ata marrin një telefonatë ditën tjetër, kjo mund të lejojë sigurinë shërbime për të lidhur burimin me pseudonimin). Mund të jetë e mençur të mos u afroheni atyre në fillim

P5 - Çfarë mund të bënte Sara për të parandaluar më tej aksesin në informacionin e saj digjital ndërsa dy burrat janë ende brenda banesës së saj?

- Të bëjë gjithçka që mundet për të zbatuar ligjet e vendit
- Të këmbëngul që autoritetet gjithashtu të zbatojnë ligjet e vendit (dmth, të lejojnë filmim, dëshmitarë, etj)
- Teknikat e de-përshkallëzimit (uljes së intensitetit të një reagimi)
- Të kuptojë se cilët janë ata dhe nëse kanë një mandat
- Vlerësoni situatën për sigurinë e saj personale
- Të kërkojë këshilla ligjore, të telefonojë redaksinë
- Të sigurojë llogari dhe dokumente false (mund të kërkojë përgatitje)
- Devijim

Zgjedhja 2 - Sara nuk mund të largohet nga banesa e saj. Dy burrat i kërkojnë asaj të ulet dhe kërkojnë që ajo të tregojë fjalëkalimet në kompjuterin e saj dhe USB-të. Ata e kërcënojnë se do ta çojnë në komisariat nëse nuk e jep këtë informacion. Sara kërkon nëse kanë një autorizim, por ata nuk e japin..

P6 - Duke ditur që ajo ka informacione të ndjeshme në kompjuterin e saj, duke përfshirë identifikimin e burimeve konfidenciale, çfarë opsionesh ka Sara në këtë situatë?

- Të vlerësoj dobësitë dhe të vendos prioritete
- Të mbyll llogaritë në distancë dhe të fshijë në distancë e llogaritë e ndjeshme
- Të idnetifikojë të gjithë informacionin e ruajtur, që ishte ruajtur në shtëpi
- Të marr parasysh anët pozitive dhe negative të informimit të anëtarëve të ekipit dhe burimeve që mund të jenë në rrezik. Ndoshta ta marr këtë vendim me mbështetjen e redaksisë
- Mundësia për fshirje të skedarëve në distancë

P7 - Sara ka një program për fshirjen e skedarëve në distancë të konfiguruar në kompjuterin e saj. Çfarë duhet të marrë parasysh para se të fshijë skedarët e saj të kompjuterit?

- Mund të jetë një çështje ligjore – pengim i drejtësisë
- Mendoni për pasojat e mundshme, nëse është e mundur, flisni fillimisht me një avokat
- Nëse Sara nuk ka prova që njerëzit janë nga forcat e rendit, por ata duken si ndërhyrës nga një forcë sigurie joshtetërore, atëherë kjo ndryshon edhe peizazhin ligjor dhe të kërcënimit.

P8 (opsionale) - Duke ditur që disa nga informacionet e saj janë kompromet uar, kë duhet të informojë Sara për këtë incident? A është e rëndësishme hierkia me të cilin ajo informon njerëzit?

- Redaktori i redaksisë
- Ekipi i sigurisë/IT i redaksisë së lajmeve
- Ekipi ligjor i redaksisë
- Merrni parasysh të kontaktoni burimet

- Nëse jeni gazetar i pavarur, merrni parasysh ta ndani situatën me profesionistë të tjerë të pavarur.

Sara në fund të fundit refuzon të japë fjalëkalimin për pajisjet e saj. Pasi kontrolluan apartamentin e saj për 10 minuta të tjera, dy burrat largohen me kompjuterin e Sarës, USB dhe shënimet e saj.

Sara tani ka sërish akses në banesën e saj. Ajo sheh që ata nuk kanë marrë një nga dy kompjuterët e saj dhe një nga çelësat USB. Ata kanë marrë të gjitha shënimet e saj.

P9 - Çfarë duhet të bëjë Sara tani për të siguruar që informacioni dhe siguria e saj të mos cenohet më tej nga veprimet e dy burrave gjatë kohës që ishin në banesën e saj?

- Burrat mund të kenë instaluar malware në pajisjet e Sarës,; mund të jetë një ide e mirë t'ia çojë ato pajisje një specialisti të “mjekësisë ligjore” dixhitale
- Apartamenti mund të përgjohet
- Të pyesë organizatën e saj se çfarë lloj mbështetjeje mund të marrë prej tyre
- Të flasë me këshilltarët në organizatën e saj, të sektorit ligjor dhe të sigurisë. Të vlerësohet nëse ka më shumë kuptim nga perspektiva e sigurisë të flitet publikisht për bastisjen apo jo

Q10 (opsionale) - Përveç aspekteve të sigurisë digjitale të këtij skenari, çfarë masash dhe reagimesh të tjera mund të kishte ndërmarrë Sara për të mbajtur veten dhe informacionin e saj të sigurt?

- Të mësojë pak më shumë se si funksionojnë forcat e sigurisë në vend, nëse ka grupe që përpiqen të frikësojnë gazetarët që nuk janë të lidhur me forcat e sigurisë
- Të përgatitet me avokatët dhe redaktorët se si t'i përgjigjen më së miri bastisjeve të shtëpive
- Të mos mbajë informacione të ndjeshme në shtëpi nëse ekziston mundësia e bastisjes së shtëpisë