Ghid de facilitare a exercițiului de tip TTX (tabletop exercise) pentru formarea în domeniul siguranței digitale

Scop și introducere

Acest ghid este destinat să însoțească un set de 11 scenarii TTX (tabletop exercises) axate pe siguranța digitală, care pot fi utilizate pentru a îmbunătăți formarea în domeniul securității digitale. Acest ghid este destinat pentru a fi utilizat de orice persoană care dorește să conceapă și să faciliteze exercițiile TTX ca metodă de formare în domeniul securității digitale. În cadrul acestui ghid, veți găsi explicații succinte despre ce este un TTX, de ce TTX-urile pot fi ajutoare valoroase pentru instruirea în domeniul securității digitale și cum se pot dezvolta, planifica și facilita TTX- urile.

Cele 11 scenarii incluse în acest ghid au fost elaborate împreună cu jurnaliști din Europa Centrală și de Sud-Est în cadrul proiectului Internews Journalist Security Fellowship (JSF) și au fost utilizate în cadrul unor cursuri de formare desfășurate de bursierii JSF în regiune. Aceste exemple de TTX- uri, inclusiv unele cu versiuni localizate în limbile din Europa Centrală și de Sud-Est și traduse în arabă și spaniolă, pot fi accesate la link-ul de aici.

Acest ghid a fost elaborat în special cu gândul la siguranța digitală pentru jurnaliști și redacții, dar poate fi util și pentru planificarea TTX-urilor pentru alte categorii de public țintă.

Ce este un TTX? De ce sunt utile TTX-urile?

Un exercițiu de tip TTX (tabletop exercise) este o metodă de formare bazată pe scenarii, care ia adesea forma unei discuții interactive. TTX-urile oferă participanților la trainungurile de formare posibilitatea de a aplica cunoștințele și competențele nou dobândite prin implicarea într-o situație fictivă (denumită scenariu TTX) care se apropie de o situație din viața reală. Scenariile TTX pot examina o gamă largă de situații de securitate, cum ar fi un raid la birou, o scurgere de date, un caz de doxxing sau o investigație sensibilă. În timp ce metodele de formare mai tradiționale se pot concentra pe transferul anumitor abilități și cunoștințe tehnice, un TTX poate ajuta la:

- Asigurarea un mediu cu risc scăzut pentru ca participanții la formare să exerseze pregătirea și răspunsul la problemele de securitate pe care le-ar putea întâlni.
- Stimularea discuțiilor critice despre subiectele de securitate digitală și a modului optim în care acestea să fie abordate în anumite situații. Aceasta ar putea fi în mod excepțioal util pentru antrenarea participanților care lucrează împreună în mod regulat pentru a lua în

considerare abordarea lor comună sau organizațională în privința securității.
- Evaluarea a cât de bine este echipat un individ sau o organizație pentru a face față problemelor de securitate cu care se confruntă. Scopul unui TTX este să identifice lacunele de cunoștințe, punctele forte și limitările individuale, organizaționale și comunitare.

Un TTX de succes merge dincolo de instrumente și practici de bază, subliniind totodată ca proceduri și politici pot lipsi sau trebuie îmbunătățite.

TTX-urile sunt cele mai eficiente atunci cțnd sunt folosite ca suplimente ca să îmbunătățească ale metode de training. Aceasta se întâmplă pentru că scopul principal al TTX-ului nu este să transfera noi îndemânări și cunoștințe, ci de a insufla și de a consolida conuștințe pe baza practicii bazată pe scenarii și a evaluării.

Componentele documentelor privind scenariul TTX

Fiecare dintre cele 11 scene TTX se bazează în mare parte pe persoana Sarei, pe care am descris-o în acest ghid. Fiecare scenă include, în plus, următoarele componente:

- Obiectiv - Obiectivul general al scenariului TTX.
- Obiective de învățare - Opțiuni pentru obiectivele generale de învățare asupra cărora să se concentreze în timpul TTX. Facilitatorii ar fi probabil avantajați dacă ar selecta doar câteva obiective de învățare pe care să se concentreze.
- Competențe/comportamente pe care să le formăm înainte sau după TTX - Opțiuni pentru abilități concrete și specifice și schimbări comportamentale pe care TTX să se concentreze pentru a le insufla participanților la formare. Facilitatorii ar avea de câștigat dacă ar selecta doar câteva abilități și comportamente asupra cărora să se concentreze, iar acestea ar trebui să se alinieze cu obiectivele și scopul de învățare selectate.
- Scenariu - Acesta este scenariul actual al TTX. Acesta include următoarele:
    - Informații introductive de fond și contextuale la început
    - Elemente suplimentare de context furnizate pe parcursul scenariului
    - Întrebări și sugestii pentru ca participanții să discute și să răspundă. Acestea sunt marcate prin litera Q urmată de un număr (de exemplu, Q1, Q2, Q3 etc.).
    - Sub întrebări și sugestii se află câteva răspunsuri posibile. Acestea nu trebuie comunicate participanților în timpul TTX. Acestea au rolul de a ajuta facilitatorul.
- Unele scenarii includ „injecții”(vor fi etichetate ca "Inject"). O injecție este o informație nouă sau o nouă evoluție inserată de către facilitator în scenariul TTX în anumite momente pentru a face să avanseze scenariul sau pentru a adăuga complexitate. O injecție poate schimba narațiunea TTX și poate solicita o acțiune sau un răspuns din partea participanților.

Anexe - Unele scenarii (de exemplu, Scenariul 3: Hărțuire și Doxxing) includ, de asemenea, anexe, de multe ori folosite pentru injecții în timpul scenariului.

Elaborarea unui scenariu TTX

Unsprezece scenarii TTX au fost dezvoltate în cadrul proiectului JSF (link aici). Oricine le poate modifica, astfel încât să se potrivească mai bine nevoilor de instruire ale comunității sale. De

asemenea, se pot crea propriile scenarii de la zero. Dacă vă gândiți să revizuiți unul dintre scenariile TTX sau să vă creați propriul scenariu, luați în considerare următoarele:

Obiectivele de învățare ar trebui să fie stabilite la începutul fazei de proiectare, să se completeze reciproc, să urmeze o ordine logică în ceea ce privește învățarea, să fie prioritizate în funcție de importanță și să se conecteze la obiectivul general al TTX. Pentru a simplifica procesul de formare și pentru a facilita măsurarea succesului, conectați obiectivele de învățare la abilități sau comportamente concrete asupra cărora participanții ar trebui să se concentreze în timpul TTX. În mod ideal, veți stabili aceste obiective de învățare și aceste competențe concrete pe baza nevoilor și a nivelurilor de competențe ale participanților dumneavoastră. Este posibil să le cunoașteți deja dacă lucrați cu o comunitate pe care o cunoașteți bine. Alternativ, este posibil să fie nevoie să efectuați o evaluare inițială a nevoilor (poate prin interviuri cu informatori cheie sau un sondaj prealabil) pentru a colecta aceste informații dacă sunteți mai puțin familiarizat cu participanții.

Scenariul trebuie să fie cât mai apropiat de viața reală, dar, în general, nu trebuie să numească persoane sau organizații reale. Concentrați-vă pe situații, provocări și experiențe reale. În cazuri rare, poate fi oportună utilizarea unor locații reale, dar trebuie să luați în considerare riscurile de securitate și potențialele limitări în acest sens. Enumerarea unor locații reale ar putea, de exemplu, să însemne că oamenii petrec prea mult timp pentru a reține sau a cerceta detalii despre acestea și să se concentreze mai puțin asupra scenariului.

În ceea ce privește complexitatea, scenariul nu trebuie să umbrească sau să distragă atenția de la învățare. Alegerile îi pot ajuta pe participanți să înțeleagă impactul pe care îl vor avea deciziile lor, dar nu uitați că adăugarea de complexitate și de alegeri îngreunează construirea unui TTX și, de asemenea, va face ca întregul exercițiu să fie mult mai lung.

De asemenea, puteți utiliza timpul ca element de proiectare în timpul scenariului dvs. prin atribuirea de momente evenimentelor care au loc în timpul TTX, prin punerea de întrebări legate de timp sau prin utilizarea de flashback-uri sau flashforwards. În orice caz, ar trebui să fiți clar cu privire la utilizarea timpului la începutul scenariului și să mențineți claritatea pe tot parcursul scenei.

În funcție de nivelul de calificare al facilitatorului și al participanților, puteți lua în considerare includerea unor elemente tehnice în cadrul TTX. Acest lucru ar putea însemna că participanților li se cere să utilizeze un anumit instrument, software sau proces pentru a parcurge scenariul. Dacă includeți un element tehnic, acordați timp suplimentar pentru a finaliza aceste sarcini și aveți întotdeauna un plan de rezervă în caz de probleme tehnice sau faceți componenta tehnică opțională pentru a vă adapta la diferite niveluri de competențe.

Poți folosi, de asemenea, „injecții”, în TTX-ul tău. Injecțiile pot fi mai mari sau mai mici și pot fi dependente de participanți sau independente de ei. La modul general, injecțiile sunt utilizate în în scenarii lungi, având în vedere timpul necesar. Injecțiile sunt livrate de către facilitator, iar momentul livrării este esențial. Ca să integrați cu succes o injecție într-o scenă, este necesar ca facilitatorul să aibă resurse atât înainte, cât și ăn cursul facilitării TTX-ului. Utilizarea injecțiilor ar trebui să se potrivească cu nevoile de a atinge obiectivele prestabilite de învățare.

Planificarea unui TTX

Înainte de a începe planificarea TTX-ului tău, ia-ți un moment pentru a te gândi la publicul țintă și cum aceasta va afecta obiectivele de învățare.

Vă adresați jurnaliștilor, directorilor de știri, oamenilor de la securitate? Fiecare dintre ei lucrează cu informații diferite și sunt responsabili pentru decizii diferite. Alternativ, unele TTX, în mod deliberat, lucrează cu entități mult mai largi - de exemplu o întreagă redacție - pentru a înțelege cum oamenii comunică și iau decizii. Ai putea juca cu participanți care au niveluri diferite de competență, cunoștințe și experiențe. Luați-vă timp să modificați TTX-ul astfel încât el să se adreseze cât mai bine nevoilor specifice.

Odată ce v-ați stabilit publicul țintă, planificați-vă obiectivele de învățare și luați în considerare abilitățile și comportamente specifice pe care le veți învăța. Selectarea abilităților specifice înainte de training este esențială pentru a vă ajuta în scopul dumneavoastră ca formator, pentru a stabili obiective tangibile de învățare și văva ajuta să stabiliți un punct de referință pentru a măsura cât de eficient este trainingul. Vedeți o listă de exemple de competențe sub fiecare subdocument TTX denumit „Abilități/Comportamente de instruit înainte sau după TTX". Ar putea fi tentant să acoperiți cât de multe obiective posibile într-un singur TTX, dar este mult mai eficient să țineți un training limitat care să acopere obiective de învățare specifice. Amintiți-vă că publicul dumneavoastră are timp și capacitate de atenție limitate.

Calculați cât de mult timp aveți nevoie pentru TTX. În timp ce uneori, agențiile guvernamentale sau corporațiile creează TTX-uti care se întind pe mai multe zile, publicul dumneavoastră ar putea fi mult mai presat de timp. Munca, îngrijirea sau alte angajamente de viață ale participanților dumneavoastră ar trebui luate în considerare. În mod obișnuit, un TTX care are 4-6 întrebări sau injecții va dura în jur de o oră, o oră și jumătate. Asta depinde foarte mult și de mărimea grupului. Grupurilor mari le ia mai mult ca să completeze un TTX. De asemenea, va trebui să luați în considerare și timpul pentru debrifing și să revizuiți obiectivele de învățare și abilitățile sau comportamentele concrete pe care ați dori ca participanții să le pună în aplicare după scenă. Este posibil ca participanții să aibă nevoie de formare suplimentară sau de monitorizare pentru a putea pune în aplicare cu succes abilitățile sau comportamentele concrete.

Luați în considerare spațiul pe care îl aveți la dispoziție pentru această activitate. Dacă se desfășoară personal, este ideal să facilitați TTX într-un spațiu care permite colaborarea. O cameră cu mese și scaune confortabile este probabil mai propice pentru un TTX decât o sală de curs. De asemenea, este posibil să fie nevoie să vă asigurați că există Wi-Fi de calitate sau alte facilități tehnologice, cum ar fi un proiector. Accesibilitatea spațiului ar trebui, de asemenea, să fie prioritară, dacă se poate (de exemplu, acces la scaune cu rotile, băi care să includă genul, opțiuni de transport convenabile etc.).

Decideți dacă vor exista mai multe roluri de facilitare și care vor fi acestea. Cel mai bine ar putea fi ca un facilitator să conducă TTX, iar ceilalți să ajute în cadrul divizării pe grupe de discuții sau al unor sarcini secundare. De asemenea, este posibil ca facilitatorii să dorească să repete anumite elemente înainte.

Stabiliți de ce resurse veți avea nevoie pentru TTX. Este posibil să doriți să creați un set de diapozitive, documente sau alte tipuri de materiale de prezentare pentru a le afișa pe parcursul trainingului, de asemenea, întrebările și/sau injecțiile. De asemenea, este important să luați în considerare materialele de care participanții ar putea avea nevoie pentru luarea de notițe.

Facilitarea unui TTX

Facilitarea unui TTX diferă de conducerea unei sesiuni tradiționale de formare sau de perfecționare în domeniul securității digitale. În cadrul formării tradiționale în domeniul securității digitale, formatorii au tendința de a vorbi mult și se așteaptă ca aceștia să își împărtășească cunoștințele cu participanții. Într-o formare TTX, însă, cea mai mare parte a discursului și a muncii se desfășoară între participanții înșiși, pe măsură ce aceștia discută scenariul și iau decizii.
Facilitatorul TTX joacă rolul de mediator al procesului, asigurându-se că TTX-ul se desfășoară fără probleme și că își îndeplinește obiectivele. Facilitatorul TTX introduce exercițiul, contextul și informațiile de background; răspunde la câteva întrebări de bază și adaugă injecții. Alte recomandări pentru facilitarea TTX includ:

- Asigurați-vă că sunteți foarte familiarizat cu TTX.
- Amintiți-vă care sunt scopul și obiectivele de învățare ale TTX și direcționați discuțiile astfel încât participanții să poată atinge aceste obiective.
- Comunicați clar rolurile și așteptările, atât la început, cât și pe parcursul TTX.
- Stați cu ochii pe ceas și asigurați-vă că respectați și maximizați timpul pe care îl aveți la dispoziție cu participanții.
- Asigurați-vă că spațiul este sigur și primitor și că multe persoane pot simți că părerile lor sunt ascultate și luate în considerare.
- Atunci când un participant menționează o bună practică, evidențiați-o! Acest lucru poate spori încrederea și poate încuraja participarea în continuare.
- Dacă nu știți răspunsul la o întrebare, nu vă fie teamă să spuneți acest lucru și angajați-vă să reveniți cu un răspuns după TTX. Folosiți resursele din comunitate cum ar fi instanța Team CommUNITY's Mattermos pentru a găsi răspunsuri la întrebările pe care nu le puteți afla singuri.
- Dacă este posibil, colectați feedback pe tot parcursul angajamentului și fiți gata să faceți micro-ajustări. Dacă intenționați să găzduiți mai multe sesiuni ale unui TTX, puteți, de asemenea, să colectați feedback la sfârșitul fiecăreia pentru a înțelege mai bine cum vă puteți îmbunătăți în continuare.
- Dacă TTX-ul începe să meargă într-o altă direcție decât cea intenționată inițial, este în regulă! Fiți flexibili, dar asigurați-vă că, în cele din urmă atinge scopurile învățării.

Dacă aveți nevoie de o îndrumare mai detaliată, mai jos sunt sugerate instrucțiuni pas cu pas pentru a vă ajuta la facilitare.

1. Prezentați-vă (și prezentați-i și pe ceilalți co-formatori), explicați rolul (rolurile) și descrieți obiectivul general al TTX-ului (de exemplu: astăzi, vom analiza modul în care o redacție de știri ar putea răspunde unui incident de securitate). Acesta este un moment ideal pentru a stabili, de asemenea, câteva reguli de bază ca grup.

2. În continuare, descrieți în detaliu ce se va întâmpla în timpul TTX-ului. Explicați că scopul este de a simula o situație fictivă care se apropie de viața reală pentru a înțelege mai bine reacțiile noastre și ale comunității noastre mai largi.
3. În funcție de mărimea și componența grupului, este posibil să doriți să împărțiți participanții în grupuri de lucru.
4. Prezentați participanților scena, inclusiv orice ampnunte de backgorund care pot fi necesare.
5. Narrați scena, pas cu pas, pe măsură ce participanții parcurg TTX-ul. Fiți disponibil pentru întrebări și pentru a ajuta la rezolvarea problemelor în cazul în care participanții se blochează.
6. Furnizați injecții după cum este necesar.
7. Încurajați participanții să se implice și să răspundă la solicitări. Rugați-i să ia notițe atunci când este relevant sau util. Utilizați răspunsurile pe care le-ați pregătit în prealabil pentru a ajuta participanții care au dificultăți sau au nevoie de exemple pentru a începe.
8. După ce participanții finalizează TTX-ul, invitați-i să discute principalele concluzii pe care le-au tras din această experiență și ce cred despre TTX ca metodă de formare. Acesta este un moment excelent pentru a înregistra feedback-ul și a lua în considerare încorporarea unor îmbunătățiri pentru viitoarele cursuri de formare.
9. Odată ce TTX s-a încheiat, verificați dacă există materiale, acțiuni de urmărire sau rezumate care ar trebui împărtășite cu participanții.

Anexa 1: Context despre Sara (un personaj TTX)

Am creat o singură persoană, Sara, pentru a ne baza pe experiențele din scenariile TTX de exemplu. Acest lucru ne-a ajutat atât să adăugăm un sentiment de coerență la TTX-uri, cât și să oferim jurnaliștilor un bun punct de plecare pentru a se gândi la amenințări și la contextul mai larg. Am inclus mai jos prezentarea Sarei, pe care facilitatorii o pot folosi pentru a pregăti scena și a oferi un context înainte de a lansa unul dintre scenariile TTX de exemplu.

Sara este o jurnalistă în vârstă de 41 de ani. Ea a lucrat pentru diverse organizații de știri locale și internaționale timp de mai mulți ani în țara sa natală și în țările vecine.

Anul trecut, Sara a început să lucreze cu o organizație de știri de investigație numită "Free Press Now" din țara sa natală, care relatează frecvent despre o serie de probleme politice. Printre acestea se numără suspiciuni de încălcare a drepturilor omului de către guvernul în exercițiu, funcționari guvernamentali corupți și politici guvernamentale care îngreunează viața minorităților etnice din țară.

Datorită reportajelor veridice și fiabile, Free Press Now a devenit o sursă de încredere și populară de informații pentru populația locală.

În urma alegerilor naționale de acum 5 luni, noul guvern aflat la putere a început să limiteze libertatea presei, iar săptămâna trecută autoritățile au percheziționat locuințele a trei jurnaliști importanți din capitală. Recent, casa Sarei a fost și ea percheziționată, deși cei care au efectuat o percheziție li au luat doar câteva caiete.

Scenariul 1: Dispozitiv pierdut

Scop

Să ajute participanții să planifice și să răspundă unei situații când unul sau mai multe dispozitive – care pot conține informații sensibile – dispar.

Obiective de învățare

- Identificarea unor abordări pentru a securiza comunicațiile dintre jurnalist și sursă.
- Conștientizarea riscurilor în situația pierderii dispozitivelor, cum ar fi telefonul mobil sau laptopul.
- Înțelegerea bunelor practici în domeniul protecției și securității.
- Împărtășirea bunelor practici, în special cu privire la securitatea dispozitivelor, cu organizația și echipa.

Aptitudini/comportamente care necesită antrenament

- Instalarea, configurarea și utilizarea Signal (sau o altă aplicație de mesagerie securizată)înainte sau după TTX
- Configurarea și utilizarea unei mesagerii alternative criptate end-to-end (cum ar fi WhatsApp sau Facebook Messenger Secret Chat).
- Instalarea, configurarea și utilizarea Mailvelope (sau o altă opțiune de criptare a e-mailurilor)
- Criptarea unui dispozitiv mobil (setarea unei parole)
- Setarea de parole pentru aplicațiile individuale sau dispozitivele mobile
- Efectuarea și criptarea copiilor de rezervă ale datelor de pe dispozitivele mobile (utilizând servicii cloud sau un hard disk extern).

Scenariu

O sursă necunoscută o contactează pe Sara prin intermediul Facebook Messenger, spunându-i că are informații confidențiale pentru ea. Documentele pe care vrea sa le dea Sarei conțin informații despre averea actualului ministru al apărării.

Dorind să păstreze confidențialitatea sursei, Sarei i-ar plăcea să îl convingă să îi transfere informația prin intermediul unei mesagerii criptate end-to-end.

1 - Cum poate Sara să explice conceptul de criptare pentru a convinge sursa de importanța acestuia?

- Nimeni - nici măcar compania care operează mesageria - nu are acces la conținutul mesajelor. Nici conținutul mesajelor nu va fi stocat necriptat pe serverele companiei.

- Forțele de ordine nu le pot accesa prin compania care furnizează serviciul de chat.
- Dacă un atacator reușește să spargă contul care a fost folosit pentru trimiterea mesajelor, el nu va putea nici să acceseze conținutul mesajelor (cu excepția cazului în care există o copie necriptată.)

2 - Ce fel de comunicare digitală va trebui Sara să folosească cu aceasta sursa pentru a asigura securizarea comunicațiilor?

- Mesaje cu criptare end-to-end și mesaje care dispar
- Emailuri criptate

Sursa este încântată că Sara se gândește la siguranța comunicației, dar încă nu este sigură ce metode să folosească. El o întreabă pe Sara despre aplicații de mesagerie cum ar fi: Signal, Telegram, Facebook Messenger și email.

3 - Din perspectiva securității digitale care ar fi factorii care ar putea fi considerați atunci cand selectezi și folosești diferite aplicații de mesagerie?

- Numerele de telefon: multe dintre serviciile de mesajele criptate end-to-end au nevoie de un număr de telefon și, în multe locuri, numerele de telefon au nevoie să fie înregistrate, așa că guvernul știe ce persoană se află în spatele fiecărui număr de telefon. Asta înseamnă că, dacă vreodată guvernul s-ar uita prin telefonul Sarei sau al sursei, și-ar putea da seama că ei au trimis mesajele, chiar dacă au folosit pseudonime sau mesaje care dispar (singura soluție de protecție ar putea fi ștergerea numelor din contacte, din mesagerie și, ideall, ștergerea telefonului).
- Chaturile secrete: Facebook Messenger și Telegram au două moduri de funcționare, doar unul este criptat end-to-end. Acest mod se numește, de obicei, chat secret sau ceva similar și este, în mod frecvent, ascuns undeva în setări.
- Mesaje care dispar după o perioadă de timp: aproape fiecare dintre mesageriile moderne are o funcție de dispariția mesajelor, deși, în cazul unora dintre ele, ea este disponibilă doar în chatul secret.
- Ștergerea chaturilor(a mesajelor din chat): acest lucru este destul de simplu, dar este important să țineți cont de faptul că unele mesagerii doar arhivează chaturile, în loc să le șteargă.
- Conștientizarea în privința capturilor de ecran: orice parte rău intenționată din conversație ar putea face o captură de ecran sau - dacă funcțiile mesagerului nu permit acest lucru - ar putea face pur și simplu o fotografie a ecranului telefonului său.
- Verificarea cu doi factori (2FV): un atacator ar putea prelua controlul unui cont de messenger prin preluarea numărului de telefon care a fost utilizat pentru înregistrarea contului și retrimiterea SMS-ului de verificare către acesta. Acest lucru îi permite să se dea drept proprietar al contului, deși, de obicei, nu oferă acces la istoricul mesajelor. Majoritatea mesagerilor au acum opțiunea de a solicita o parolă suplimentară în plus față

de codul SMS: acest lucru înseamnă că, chiar dacă un atacator reușește să preia numărul de telefon, nu poate obține cu ușurință acces la cont.
- Coduri de acces puternice sau fraze de acces puternice pentru a vă conecta la dispozitiv (telefon) în sine

4 - Din perspectiva securității digitale, care sunt câțiva factori pe care le considerați când comunicați prin email?

- Sursa ar trebui să creeze o nouă adresă de e-mail doar pentru a comunica cu Sara.
- Noul email ar trebui să aibă o parolă unică și puternică și o autentificare solidă cu doi factori.
- Sursa ar trebui, de asemenea, să fie atentă la atacurile de phishing și să utilizeze tehnologii care ar putea contribui la atenuarea acestora, cum ar fi cheile de securitate fizice sau completarea automată a managerului de parole.
- În mod ideal, sursa și Sara ar trebui să comunice prin PGP, de exemplu, folosind Mailvelope. Acest lucru înseamnă că, chiar dacă conturile lor ar fi cumva compromise, un atacator nu ar putea citi conținutul mesajelor lor fără cheia PGP.

Sursa îi trimite fișierul în siguranță Sarei, iar aceasta îl vizualizează pe telefonul mobil. Ea este fericită că are această informație și iese cu prietenii ei pentru a sărbători. În timp ce se afla la o petrecere, Sara își pierde telefonul și își dă seama că are o parolă foarte simplă (1111) pe el.

5 -Ce se poate întâmpla cu telefonul Sarei și cu informațiile de pe telefon?

- Oricine găsește telefonul poate accesa informațiile sensibile dacă își dă seama unde se află acesta
- Oricine găsește telefonul poate să trimită mesaje contactelor Sarei și să pretindă că este ea.
- Oricine se uită pe informațiile de pe telefon poate fie să pună în pericol siguranța și identitatea contactelor Sarei or să colecteze informații care pot fi folosite pentru inginerie socială.
- Sare își poate pierde în mod real credibilitatea ca jurnalist.

6 - Ce poate Sara sa facă acum pentru a limita impactul asupra securității digitale?

- Își poate șterge de la distanță telefonul dacă și-a setat aceasta funcționalitate.
- Poate sa se se logheze pe alte dispozitive de pe email și conturile de social media, să schimbe parola și, dacă e posibil, să dea click pe linkul „deconectați-vă de pe toate dispozitivele conectate".

7 - Ar trebui să-și avertizeze sursa că a pierdut telefonul? Care sunt argumentele pro și contra?

- Discuții fără un răspuns exact corect.

Veste bună! Un prieten al Sarei cu care a fost la petrecere a găsit telefonul în geaca lui. El o sună pe Sara și îi dă telefonul ziua următoare.

8 - Acum că Sara a primit telefonul înapoi, ce pași trebuie să facă ca să fie protejată în caz că își pierde telefonul din nou?

- Luați în considerare posibilitatea de a utiliza uneori deblocarea biometrică. Există avantaje (nimeni nu se poate uita peste umărul Sarei în timp ce introduce parola și nici nu va fi surprinsă de camerele de supraveghere) și dezavantaje (este mai ușor să o constrângi pe Sara să își deblocheze dispozitivul).
- Utilizați parole și fraze de deblocare a telefonului mai lungi. Evitați deblocările cu modele (cum ar fi cele care unesc puncte), deoarece acestea pot fi identificate cu ușurință de o persoană care se uită, de o cameră sau de petele de pe ecran.
- Blocați și aplicațiile (cum ar fi messenger) cu o parolă suplimentară, dacă Sara este îngrijorată că telefonul ei ar putea fi partajat/împrumutat uneori.
- Configurați aplicații care pot urmări, localiza și șterge de la distanță dispozitivele

9 - Din perspectivă organizațională, cum arată un proces de training pentru membrii noi din echipă pentru a le securiza dispozitivele precum telefonul și laptopul?

- Asigurați-vă că întreg personalul, indiferent de poziție, trece printr-un training și înțelege importanța securității digitale.
- Organizațiile ar trebui să enumere clar așteptările în ceea ce privește urmarea practicilor de securitate digitală.
- Identificați pașii de urmat atunci când securitatea ar putea fi compromisă (cum ar fi furtul unui telefon sau piratarea unei parole).
- Suportul IT ar trebui să fie acordat întregului personal care are nevoie de el.

Scenariul 2: Securitate operațională

Scop

Să ajute participanții să asigure un nivel ridicat de conștientizare a securității digitale și de bune practici în cadrul organizației lor, al colegilor de muncă și/sau al jurnaliștilor freelance.

Obiective de învățare

- Din punct de vedere teoretic, înțelegeți conceptul de siguranță digitală ca fiind un proces continuu și nu un obiectiv final.
- Să vorbiți, explicați și convingeți alte persoane despre importanța securității digitale.
- În mod practic, discutați opțiunile de comunicare sigure prin intermediul dispozitivului mobil.
- Asigurați cele mai bune practici în ceea ce privește manipularea securizată a fișierelor.
- Conștientizați setările conturilor pentru calculatoarele din rețea.
- Să înțelegeți importanța cartografierii amenințărilor (threat modeling).

Competențe/comportamente pe care să le antrenați înainte sau după TTX

- Configurarea și menținerea permisiunilor pe platformele de colaborare (de exemplu, Google Drive)
- (Dacă este posibil, deoarece unele dintre aceste funcționalități sunt disponibile numai pe conturile de nivel enterprise) Examinarea jurnalelor de acces pe platformele de colaborare, cum ar fi Google Drive.
- Configurarea și utilizarea autentificării cu doi factori, în mod ideal cu chei de securitate fizice sau mecanisme similare rezistente la phishing.
- Proceduri bune privind parolele (utilizarea de parole unice, utilizarea de parole lungi, utilizarea de fraze de acces) și manageri de parole.
- Criptarea documentelor (folosind Mailvelope, etc.)
- Instalarea, configurarea și utilizarea Signal (sau o altă aplicație de mesagerie sigură)
- Utilizarea funcțiilor avansate în cadrul aplicației de mesagerie sigură (de exemplu, ștergerea temporizată a mesajelor)
- Instalarea, configurarea și utilizarea Mailvelope (sau a unei alte opțiuni de criptare a e-mailurilor)
- Lucrul în siguranță cu fișiere și documente din surse sensibile

Scenariu

Sara formează o echipă de jurnaliști ca să investigheze cazuri de corupție din achizițiile publice efectuate de Ministerul Sănătății în timpul pandemiei Covid-19. Nu toți jurnaliștii din echipă au același nivel de competențe digitale/cunoștințe și practici de securitate. Sara știe că unul dintre membrii echipei sale nu se pricepe foarte bine la protecția fișierelor.

Î1 – Cum își poate încuraja Sara colegii să își îmbunătățească abordarea privind siguranța digitală? Ce ar trebui să facă Sara pentru a asigura practicile de securitate digitală atunci când organizează o echipă?

- Explicați de ce este important să aveți o bună siguranță digitală. Acest lucru ar putea include discuții despre modul în care siguranța digitală deficitară ar putea periclita în mod semnificativ cariera unui jurnalist, despre faptul că sursele și colegii vor avea mai multă încredere în dumneavoastră dacă practicați o bună siguranță digitală și despre necesitatea de a proteja persoanele din jurul nostru.
- Discutați despre ce dispozitive folosesc, cum își protejează conturile de utilizator, cum stochează și fac schimb de fișiere, cum accesează rețeaua (folosesc propriile dispozitive sau lucrează pe computerele redacției), cum se conectează la rețeaua internet (fără fir sau prin cablu), folosesc autentificarea cu doi factori pentru a securiza conturile de utilizator și dacă sunt disciplinați în materie de parole (dacă refolosesc parolele, dacă folosesc administratori de parole).
- Decideți modul în care echipa comunică, stochează fișierele și le accesează. Scopul celui de-al doilea pas este de a vă asigura că toată lumea urmează același protocol legat de activitățile menționate anterior.
- Luați în considerare trainingul echipei folosind protocoalele nou-înființate. După ce s-au stabilit regulile, echipa ar trebui să facă un exercițiu, să testeze efectiv noile modalități de comunicare și să vadă dacă există probleme care trebuie rezolvate.

Î2 – Cum vor stoca și partaja Sara și echipa ei fișierele audio și documentele obținute de la surse?

- Limitați cine are acces la diverse fișiere și foldere, utilizați cu atenție setările de partajare în aplicații precum Google Drive.
- Descurajați colegii să scoată fișiere și documente din mediul de lucru (chei USB, atașamente de e-mail...), aceste obiceiuri ar putea extinde platforma de atac și crește riscul de scurgeri/hack-uri.
- Cereți echipei să folosească întotdeauna doar calculatoarele de serviciu pentru a accesa fișierele de lucru.
- Limitați ceea ce poate fi instalat pe calculatoarele de serviciu, asigurați-vă că acestea au întotdeauna parole puternice și software actualizat.

Î3 – Cum vor asigura Sara și echipa ei siguranța comunicării?

Prin integrarea întregii echipe pe aceeași platformă și asigurându-se că toată lumea se simte confortabil cu utilizarea acesteia, Sara își poate ajuta echipa să stabilească un mod sigur și securizat de comunicare.

Luați în considerare:

- Mutarea majorității conversațiilor în Signal, cu dispariția mesajelor și copierea mesajelor care trebuie să fie arhivate
- Folosirea PGP-ului pe email
- Crearea unor reguli solide de securitate a contului (parolă unică, 2FA) pentru e-mail

Cu două săptămâni înainte de publicare, Sara primește un telefon de la principala sursă guvernamentală din această anchetă. Sara cunoaște bine sursa și are încredere în ea. În timpul apelului, sursa spune "guvernul știe – a existat o scurgere de informații" și închide.

Î4 – Din perspectiva securității digitale, care sunt primii pași pe care Sara ar trebui să îi facă pentru a răspunde la o posibilă scurgere de informații?

- Rugați-vă pe toți din echipă să își schimbe parolele, în cazul în care un atacator a obținut parola unuia dintre conturile lor.
- Luați în considerare faptul că guvernul nu trebuia neapărat să pătrundă în redacția ei; este posibil să fi aflat despre scurgerea de informații, de exemplu, investigând ce anume tipăreau unii angajați guvernamentali.
- Faceți o mică investigație în cadrul redacției: verificați dacă toată lumea a respectat protocoalele, cine a avut acces la fișiere și la informațiile care au fost divulgate și ce anume a fost divulgat în primul rând. Prin utilizarea controlului accesului și a versiunilor, urmări mai ușor accesul la datele individuale la care lucrați.
- Gândiți-vă dacă ar trebui să accelerați publicarea.

Sara află că scurgerea de informații a venit din interiorul organizației sale. Un designer a avut acces la Google Drive-ul comun al organizației (deși nu lucra la articol). Sara a aflat acest lucru verificând controlul accesului la Google Drive și realizând că din cauza naturii muncii lor, echipa de design avea acces la tot ce se afla în rețea. Un designer a partajat din greșeală un document cu un client freelance care lucra pentru guvern, și nu cu un prieten din redacție care avea același nume de familie.

Î5 – Ce ar fi putut să facă Sara în mod diferit în această situație?

- Sara ar trebui să stabilească protocoale sigure care să se aplice doar echipei sale de investigație. Ea ar trebui să se asigure că există un sistem clar de permisiuni și că acesta este respectat în practică.

- Echipa ar trebui să colaboreze cu designerii în așa fel încât aceștia să dispună de informații doar în funcție de necesități: nu ar trebui să aibă acces la detalii secrete sau sensibile decât dacă sunt absolut necesare din punct de vedere al publicării.
- Sara ar trebui, de asemenea, să privească securitatea și confidențialitatea ca pe un proces și nu ca pe o stare de fapt; este ceva asupra căruia trebuie să se revină în mod constant.

Scenariul 3: Hărțuire și Doxxing

Scop

Să ajute participanții să înțeleagă cum să se pregătească pentru a răspunde hărțuirii online.

Obiective de învățare

- Identificați metode și măsuri de atenuare pentru jurnaliștii care se confruntă cu hărțuire și doxxing pe rețelele sociale.
- Înțelegeți cum informațiile din social media pot fi colectate și folosite împotriva jurnaliștilor, redacției și a personalului.
- Explorați relația dintre gen și hărțuire și implicațiile sale de securitate.
- Discutați asupra modului în care o organizație media poate stabili proceduri și practici pentru a proteja personalul angajat și colaboratorii care sunt vizați de hărțuire și doxxing.
- Gândiți-vă la planuri de urgență pentru jurnaliștii care nu beneficiază de sprijin în redacție (de exemplu, liber profesioniști, freelanceri).
- Povestirea unor întâmplări legate de securitate. Cum puteți convinge persoane care nu se confruntă în mod tradițional cu hărțuirea că aceasta este o problemă majoră care necesită o acțiune și un sprijin organizațional coordonat.
- Securitatea organizațională: stabilirea de politici în cadrul organizațiilor, găsirea modalităților prin care organizațiile pot sprijini cel mai bine jurnaliștii care se confruntă cu atacuri de hărțuire.

Competențe/comportamente care trebuiesc antrenate înainte sau după TTX

- Gestionarea și actualizarea setărilor de confidențialitate pe principalele platforme de socializare.
- Utilizarea instrumentelor de siguranță de pe principalele platforme de socializare, cum ar fi raportarea și blocarea. Aceasta include atât înțelegerea modului de utilizare a acestor mecanisme, cât și a rolului lor exact.
- Configurarea și utilizarea autentificării cu doi factori, în mod ideal cu chei de securitate fizice sau mecanisme similare rezistente la phishing.

Scenariu

Sara lucrează la un nou articol despre minoritățile etnice din țara ei și despre modul în care politicile guvernamentale duc la o marginalizare sporită a acestor grupuri. În ultimele săptămâni, Sara a observat o creștere a volumului comentariilor de pe rețelele de socializare pe conturile ei, unde își împărtășește și munca. De asemenea, începe să primească comentarii pline de ură și derogatorii făcute de diferiți troli online care o vizează direct.

Q1 - Care sunt câțiva pași pe care îi poate lua Sara pentru a bloca și a raporta persoanele care fac aceste comentarii?

- Ea poate folosi funcțiile de blocare și raportare încorporate care se găsesc pe majoritatea platformelor de social media.
- Ea poate contacta companiile de social media (direct sau prin organizația sa) pentru a raporta hărțuirea pe scară largă.
- Poate dezactiva postările și răspunsurile de pe profilul ei.
- Poate fi mai selectivă cu privire la cine o poate găsi pe rețelele de socializare.
- Poate alege să nu poată fi etichetată pe platformele de social media.
- Efortul de a bloca și raporta unii dintre principalii instigatori online a enervat grupul de troli, ceea ce a dus la o creștere a conținutului instigator la ură împotriva Sarei. Unele comentarii conțin amenințări și violență la adresa ei, fie direct, fie indirect.

Q2 - Care sunt câteva modalități prin care Sara poate investiga această agresiune împotriva ei pentru a determina dacă face parte dintr-o campanie mai amplă, mai coordonată?

- Ea poate investiga situația, dar și să le ceară colegilor sprijin pentru investigații.
- Ea poate verifica dacă trolii folosesc același limbaj, cuvinte cheie sau hashtag-uri. Dacă da, este posibil să fie o campanie coordonată.
- Depinde de platformă. Pe Instagram, există numeroase opțiuni pentru a vedea informații despre anumite conturi - când a fost creat, câte persoane îl folosesc, de câte ori și-a schimbat numele etc.
- Verifică dacă este amplificat de o organizație media.
- Vezi cele mai frecvente ore de postare.

Ea le spune colegilor despre postări, dar cei mai mulți dintre membrii echipei de sex masculin, inclusiv editorul ei, îi spun să nu-și facă griji și că problema va dispărea de la sine. Este stresată, simte că echipa ei nu ascultă și nu înțelege problema.

Q3 - În loc să-i spună Sarei să nu-și facă griji, care sunt câteva modalități prin care echipa și organizația ei o pot sprijini pe Sara, în special în ceea ce privește prezența ei online și securitatea digitală?

- Ajutați la efectuarea unei evaluări complete a situației.
- Examinați împreună cu Sara practicile ei de securitate digitală și măsurile de siguranță. Ajutați-o să-și îmbunătățească situația.
- Exersați și împărtășiți experiența cu alții din organizație.
- Permiteți persoanelor în care aveți încredere să vă administreze contul sau să-l acceseze, astfel încât să nu fiți expus direct la acele cuvinte și amenințări, dar să puteți fi totuși prezent.
- Organizația poate ajuta la căutarea de tipare în hărțuiri.
- Urmăriți modul în care hărțuirea trece prin postările organizației și nu doar prin cele ale Sarei.
- Transmiteți aceste informații echipei de securitate și ajutați la investigație.

Într-o zi, fotografiile personale ale Sarei sunt publicate online de unul dintre troli. Fotografiile, pe care ea le-a postat pe rețelele de socializare în urmă cu ani, sunt personale și în unele cazuri includ informații sensibile.

Injectare - Partajați între 1 și 4 fotografii participanților. (Fotografiile pot fi găsite în anexa acestui document). Exemplele de fotografii includ:

Sara și câinele ei se plimbă în afara casei ei.

Sara fumează o țigară cu marijuana.

Sara și un grup de prieteni apropiați în vacanță.

Sara lucrează în redacție.

Discutați cu grupul de participanți de ce fiecare dintre aceste fotografii ar putea fi sensibilă.

Q4 - Care sunt câteva modalități prin care cineva ar fi putut accesa informațiile online ale Sarei, cum ar fi postările vechi de pe rețelele sociale?

- Prietenii lui Sara au postat fotografii cu setări de confidențialitate slabe.
- Conturile Sarei au fost sparte.
- Una dintre conexiunile de pe rețelele de socializare ale Sarei ar fi putut salva fotografiile pentru a le împărtăși mai târziu.
- Fotografiile din social media ale Sarei ar fi putut fi indexate de un motor de căutare.

Q5 - Ce pași poate lua Sara pentru a încerca să împiedice scurgerea de informații suplimentare despre ea online?

- Ștergerea fotografiilor vechi
- Ștergerea conturilor
- Blocarea conturilor
- Încărcarea unor fotografii noi, care conțin mai puține informații despre ea.
- Obținerea unui raport de la firma de social media cu toate datele pe care le au despre ea.
- Raportarea fotografiilor care au fost postate recent/raportarea conturilor care le-au postat.
- Continuarea postării unor conținuturi legate de muncă, chiar dacă postează mai puțin conținut personal. Dacă renunță la internet, trolii vor fi câștigat.
- Capturi de ecran cu postările, documentați cât mai mult posibil. Înregistrarea pseudonimelor online ale trolilor.

Q6 - Ce măsuri ar fi putut lua Sara și organizația ei pentru a preveni colectarea și scurgerea acestor informații online, în special în ceea ce privește securitatea digitală?

- Să creeze un grup de prieteni apropiați care sunt singurii care văd fotografiile și postările personale pe rețelele de socializare.
- Să nu posteze deloc informații sensibile (cum ar fi fotografia cu jointul).
- Să nu posteze fotografii care dezvăluie informații private, cum ar fi locația.
- Să își deschidă conturi de afaceri pentru a avea o prezență online care să nu aibă legătură cu viața personală.
- Să-și seteze parole puternice și 2FA pentru conturile de social media.

Anexa 1: Exemple de fotografii pentru injectare

Scenariul 4: Autoritățile intră în redacție

Scop

Să ajute participanții să aibă răspunsuri teoretice și practice la descinderea autorităților în redacțiile lor.

Obiective de învățare

- Asigurarea de planuri de comunicare de rezervă cu componentele tehnice în cazul în care accesul la dispozitivele redacției sau la cele personale nu mai este posibil.
- Înțelegerea bunelor practici când vine vorba de dispozitive de securitate digitală din înăuntrul redacției sau a organizației.
- Identificarea de metode de a securiza diferite fișiere pe dispozitive digitale cum ar fi computere sau telefoane mobile.
- Realizarea unui plan pentru informațiile compromise de percheziții autorităților în redacții.
- Explorarea conceptelor din jurul modelelor de amenințare, pregătirea individuală și a organizațiilor.

Abilități/comportamente pentru a vă antrena înainte sau după TTX

- Folosind un instrument precum Veracrypt sau similar cu Criptarea datelor pe hard disk -uri și unitățile externe
- Modelarea amenințărilor, în special în ceea ce privește tratarea autorităților și a raidurilor de birou: Cum să evaluezi riscurile, să te pregătești pentru unul și să te deplasezi după unul
- Securitatea organizațională și comunitară, în special cum să lucrați cu editori, manageri și avocați în situații de stres ridicat și să identificați ce întrebare să escaladeze la ce persoană
- Utilizarea setărilor din Microsoft Office și Google Drive pentru a vedea ce fișiere au fost accesate recent și când
- (Avansat) Dacă organizația are jurnale de acces minuțioase printr -o unitate Google premium sau abonament O365, accesând și lucrând cu astfel de jurnale
- Căutare prin istorii de acces la căutare și fișiere pe browserele web de frunte și sistemele de operare

Scenariu

Sara lucrează într-o redacție de aproximativ 20 de persoane. Este luni dimineață, 15 jurnaliști lucrând din redacție și alții 5 de la distanță.

La 10 dimineața, aproximativ 50 de ofițeri de poliție sosesc la redacție. Ei au un mandat pe care îl arată editorului și apoi intră cu forța, în același timp cerând jurnaliștilor și lucrătorilor să plece imediat.

Sara și colegii ei se întâlnesc afară și discută despre modul în care ar putea să mențină organizația lor să funcționeze într-un mod sigur și securizat.

Î1 - Care sunt unele priorități într -o situație de genul acesta?

- Luați legătura cu avocații pentru a consulta orice pași următori
- Contactați colegii care lucrează de la distanță
- Verificați cine are telefoanele mobile asupra lor și care au fost lăsate în urmă

Î2 - Milyen módon tudnak ez idő alatt Sára és kollégái biztonságos közösséget alkotni?

- Creati un chat de grup pe WhatsApp/Signal
- Ar putea fi o idee bună pentru a comunica prin numere personale, mai degrabă decât de lucru. În orice caz, chat -ul ar putea fi sincronizat cu dispozitivul care sunt încă la birou

Î3 - Cum ar putea Sara și colegii ei să folosească conturile online, ca cele ale website-ului sau conturile social media?

- Schimbati parolele imediat
- Dacă este posibil să vă deconectați de la distanță de pe dispozitivele care sunt încă la birou, faceți acest lucru, dar consultați -vă cu avocații mai întâi, astfel încât acest lucru nu este considerat modificarea probelor (ar putea depinde foarte mult de locație/jurisdicție)
- Consultați -vă cu avocații inaintea postari despre atacul poliției

Sara își amintește că, în timp ce ieșea din sala de știri, a văzut că poliția începe să pună computere, dispozitive și hârtii în pungi. Sara a putut să plece cu telefonul, dar laptopul a fost lăsat în sala de știri. Grupul de colegi evaluează rapid ce informații poate obține poliția?

Î4- Cum ar trebui asigurate dispozitivele din sala de știri?

- Calculatoarele blocate cu parole puternice
- Încuierea ecranului pornind după o perioadă scurtă de timp?
- USB key si harduri externe criptate

În timpul discuției lor în afara biroului, editorul dezvăluie că nu au reușit să -și blocheze computerul atunci când părăsesc biroul.

Poliția părăsește sala de știri două ore mai târziu, permițând jurnaliștilor să se întoarcă. Personalul se reunesc pentru a discuta despre informațiile posibile la care ar fi putut fi accesate de poliție, precum și pentru a discuta despre amenințări cu o natură similară care vor merge înainte.

Î5- Care sunt unele moduri în care o redactie de știri poate evalua imediat impactul unui atac de către autorități?

- Uită -te la ce fișiere de hârtie, dacă este cazul, au fost luate sau rearanjate (dacă fișierele ar fi rearanjate, înseamnă că poliția le -ar fi putut fotografia)
- Calculatoarele au, de obicei, un istoric de acces la căutare / fișier / browser, căutați și acest lucru. Puteți vedea fișiere recente în Microsoft Word și unele istorice în browsere dacă utilizați Google Docs. Dacă istoricul fișierelor a fost șters, asta înseamnă că cineva ar fi putut încerca să șteargă semne
- Este puțin probabil ca vreun malware să fi fost instalat în timpul atacului, dar dacă sunteți îngrijorat în acest sens, consultați -vă cu un profesionist specializat în malware criminalist

Î6 - Cum ar trebui organizația să se asigure că nu sunt în continuare în pericol de acest atac de către poliție?

- Schimbați parolele, doar în caz
- Discutați cu un avocat despre faptul ca a fost poliția și ce nu a fost permis să acceseze în timpul descinderii
- Dacă foloseau nume de cod sau pseudonime pentru cercetările lor, rotiți -le

Câteva săptămâni mai târziu, redactorul sef îi suna pe toți jurnaliștii și personalul administrativ. Vor să înțeleagă orice amenințări similare cu care s -ar putea confrunta redactia de știri în viitor.

Î7 - În ceea ce privește modelarea amenințărilor și securitatea digitală, cum identifică persoanele și organizațiile amenințărilor cu care s -ar putea confrunta?

- Puneți întrebările standard de modelare a amenințărilor: ce informații au, cine ar putea fi interesat să le acceseze și care ar fi consecințele dacă adversarii lor ar fi reușit
- Atunci când enumerați adversarii, gândiți -vă atât la motiv (ce le -ar plăcea să facă și de ce), cât și la capacități (ce sunt de fapt capabili să facă, ce mijloace tehnice, juridice, organizaționale și financiare au?)

Scenariul 5: Autoritățile intră în casa jurnalistului

Scop

Să furnizeze jurnaliștilor competențe teoretice și tehnice pentru a le asigura cea mai bună securitate digitală posibilă în mediul lor familial.

Obiective de învățare

- Să înțeleagă cum să securizeze dispozitivele digitale care se găsesc acasă.
- Să știe să aplice măsuri de protecție pentru agendele fizice.
- Să inițieze ștergerea fișierelor de la distanță. Avantaje și dezavantaje legate de acest lucru.
- Să limiteze accesul la informațiile care au fost compromise.
- Să se pregătească pentru descinderea autorităților în casa jurnalistului.
- Încurajați participanții să se gândească puțin la securitatea organizațională și comunitară, în special la modul de a lucra cu editorii, managerii și avocații în situații de stres ridicat și la identificarea întrebărilor pe care să le escaladeze către persoana potrivită.

Abilități/comportamente de antrenament înainte sau după TTX

- Utilizarea instrumentelor precum VeraCrypt sau alte soluții similare pentru criptarea datelor de pe hard disk-uri și unități externe este o metodă eficientă de a proteja informațiile sensibile împotriva accesului neautorizat.
- Modelul amenințărilor este procesul de identificare, analizare și evaluare a potențialelor amenințări la adresa unei organizații sau a unui sistem
- Instrumente de activare, cum ar fi Appl Find's sau Android/Samsung Find, care ar putea fi utilizate pentru a bloca de la distanță sau a șterge dispozitivele
- Utilizarea setărilor din Microsoft Office și Google Drive pentru a vedea ce fișiere au fost accesate recent și când
- (Avansat) Dacă organizația are jurnalele de acces minuțioase printr -o unitate Google premium sau O365
- Abonament, acceptând și lucrând cu astfel de jurnale
- Căutare prin istoricul de căutare și acces la fișiere pe browserele web populare și operarea sistemului

Scenariu

La cinci luni după alegerile generale, noul guvern a început să limiteze libertatea presei și să facă percheziții în casele a trei jurnaliști proeminenți din Capitală. Sara și câțiva colegi s-au întâlnit și au discutat despre modalități de a se proteja pe ei și informațiile pe care le dețin dacă s-ar afla într-o astfel de situație.

Î1 - Care sunt acele lucruri pe care un jurnalist trebuie să le ia în considerare atunci când decide să depoziteze informații în locuința lui?

- Depozitarea dispozitivelor într-un loc sigur
- Criptarea și protejarea cu parole a tuturor dispozitivelor
- Să nu includă informații despre surse în documente.
- Să aibă un inventar al informațiilor pe care le deține și unde sunt acestea depozitate (dar și această informație trebuie ținută într-un loc sigur!).
- Informații din afara sferei digitale: fii conștient de existența copiilor fizice.
- Da, este important să luați în considerare evitarea păstrării de materiale sensibile acasă, mai ales dacă există posibilitatea de percheziții în casă sau alte încălcări ale securității.
- Să respecte/cunoască legile locale și, de asemenea, regulile organizației din care face parte.
- Să fie conștienți de răspunderea legală a depozitării informațiilor sensibile în locuința personală și nu la birou.
- Cine are acces în locuința ta și la dispozitivele tale?

Î2 (opțională) - Care sunt bunele practici în legătură cu depozitarea agendelor în locuință?

- Ia în considerare să distrugi ceea ce nu ai nevoie.
- Nu ține toate notițele într-un singur loc - mai puține informații ușor de accesat.
- Ascunde agendele
- Puneți-le într-un seif, încuiați-l cu o cheie și păstrați-o în loc sigur.
- Care este nivelul de informații sensibile pe care le puteți depozita acasă?
- Folosiți acronime, abrevieri care înseamnă ceva doar pentru voi.

Î3 - Ce măsuri pot fi luate pentru a securiza cel mai bine dispozitivele electronice - (computere, harduri, stickuri USB)?

- Criptarea
- Protejarea prin parole
- Realizarea de copii offline
- Aruncarea în siguranță a dispozitivelor vechi, în special a celor care nu mai sunt utilizate, este importantă din mai multe motive.

Astăzi, Sara a plecat de acasă la 9 dimineața ca să ia o cafea și să facă cumpărături. Când s-a întors acasă, o oră mai târziu, ușa apartamentului era deschisă. Sara a intrat în apartamentul său unde a găsit doi bărbați care căutau prin biroul său și prin dormitor. Unul dintre bărbați citea în agenda sa în timp ce ținea o sacoșă cu calculatorul Sarei înăuntru. Sara a văzut că cheile USB de parole și hardurile externe de pe biroul său dispăruseră. Cei doi bărbați purtau haine civile, dar Sara presupune că ei lucrează pentru guvern.

Varianta 1 - Sara vorbește câteva minute cu cei doi bărbați și i se permite să plece de acasă în siguranță. Ea merge la o prietenă care locuiește în apropiere.

Î4 (opțională) - Știind că unele dintre informațiile ei, în special cele din agendă, au fost compromise, pe cine ar trebui Sara să informeze despre acest incident?

- Informați editorul și avocații redacției de știri.
- Înainte de a contacta orice surse care ar fi putut fi menționate în agenda, discută mai întâi cu editorul și întregul redacțional, precum și cu profesioniștii în securitate (dacă sursele au fost menționate doar sub un pseudonim, dar primesc un apel a doua zi, acest lucru ar putea permite serviciilor de securitate să le lege sursa de pseudonim). Ar fi înțelept să nu le abordezi inițial.

Î5 - Ce ar putea face Sara ca să prevină accesul pe viitor la informațiile sale digitale în timp ce cei doi bărbați sunt încă în apartamentul ei?

- Fă orice este posibil cu respectarea legislației locale.
- Insistă ca autoritățile să respecte legislația locală, de asemenea. (Să-ți dea voie să filmezi, să aduci martori, etc.)
- Tehnici de detensionare
- Aflați cine sunt și dacă au mandat de percheziție.
- Evaluează situația pentru propria siguranță digitală.
- Caută asistență legală, sună în redacție.
- Furnizarea de conturi și documente false (poate necesita o anumită pregătire).
- Deviază atenția

Varianta 2 - Sarei nu i se permite să părăsească apartamentul. Cei doi îi cer să le dea parolele de la calculator și de la stickurile USB. O amenință că o vor duce la poliție dacă nu le dă aceste informații. Sara le cere să-i arate un mandat, dar ei nu-i arată unul.

Î6 - Știind că are informații sensibile pe calculator, respectiv informații ce pot identifica o sursă confidențială, ce opțiuni are Sara?

- Să evalueze vulnerabilitățile și să prioritizeze cele mai importante lucruri.
- Să șteargă de la distanță conturile sensibile și să se deconecteze de la distanță.
- Să identifice toate informațiile deținute acasă.
- Luați în considerare care sunt avantajele și dezavantajele de a informa membrii echipei de proiect și sursele care ar putea fi în pericol. Poate e cazul să ia această decizie cu ajutor de la redacție.
- Există potențial pentru ștergerea fișierelor de la distanță.

Î7 - Sara a instalat de la distanță un program de ștergere a fișierelor de pe calculatorul ei. Ce trebuie să ia în considerare înainte de a șterge fișierele de pe computer?

- Ar putea fi o problemă juridică - obstrucționarea justiției sau distrugerea probelor
- Gândiți-vă la potențialele repercusiuni, dacă este posibil, discutați cu un avocat mai întâi.

- Dacă Shara nu are dovezi că persoanele sunt din forțele de ordine, dar par să fie intrusi standard sau dintr-o forță de securitate non-statală, atunci acest lucru schimbă de asemenea peisajul legal și de amenințare.

Î8 (opțional) - Știind că unele dintre informațiile ei au fost compromise, pe cine ar trebui Sara să informeze despre incident? Este importantă ordinea în care informează persoanele?

- Editorul redacției
- Echipa de securitate IT a redacției
- Echipa juridică a redacției de știri.
- Să ia în considerare contactarea surselor
- Dacă sunteți un freelancer, luați în considerare să împărtășiți experiența cu alți freelanceri.

În ultimă instanță, Sara refuză să dea parolele de la dispozitive. După ce au mai scotocit apartamentul timp de 10 minute, cei doi bărbați au părăsit locuința cu computerul Sarei, USB-ul de parole și agenda.

Sara are acces la apartamentul său din nou. Vede că unul dintre calculatoare a fost lăsat în locuință, împreună cu unul dintre USB-urile de parole. Toate agendele au fost ridicate.

Î9 - Ce ar trebui să facă Sara acum ca să se asigure că informațiile și elementele de securitate nu sunt și mai compromise de acțiunile celor doi bărbați în timp ce erau în apartament?

- Bărbații ar fi putut instala dispozitivele Sarei; ar fi o idee bună să trimiteți acele dispozitive unui specialist în investigații digitale.
- Luați în considerare că apartamentul ei ar putea fi ascultat.
- Shara sa-si intrebe organizatia ei ce fel de sprijin ar putea primi.
- Sa discute cu consilierii săi organizaționali, juridici și de securitate cu privire la faptul dacă are mai mult sens din punct de vedere al siguranței și securității să vorbească public despre raid sau nu.

Î10 (opțională) - În afară de aspectele de securitate digitală, ce alte măsuri de precauție ar fi trebuit Sara să ia ca să se protejeze pe ea și informațiile ei?

- Află mai multe despre modul în care funcționează forțele de securitate din țară, dacă există grupuri care încearcă să intimideze jurnaliștii care nu sunt asociate cu forțele de securitate.
- Pregătiți-vă cu avocații și editorii cu privire la modul în care să răspundeți cel mai bine la raidurile în casă.
- Nu păstrați informații sensibile acasă dacă există posibilități de percheziții în casă.