Vodič za vođenje Tabletop Exercise (TTX) ili stolnih vježbi za obuku o digitalnoj sigurnosti

Svrha i uvod

Ovaj vodič je namijenjen da prati skup od 11 scenarija tabletop vježbi (TTX) usmjerenih na digitalnu sigurnost, koji se mogu koristiti za poboljšanje obuke o digitalnoj sigurnosti. Ovaj je vodič namijenjen svim osobama koje žele dizajnirati i provoditi TTX-ove kao metodu obuke o digitalnoj sigurnosti. Unutar ovog vodiča pronaći ćete kratka objašnjenja o tome što je TTX, zašto TTX-ovi mogu biti vrijedni dodaci obuci o digitalnoj sigurnosnoj i kako se mogu razviti, planirati i provoditi TTX-ovi.

Svih 11 scenarija uključenih u ovaj vodič razvijeno je zajedno s novinarima u srednjoj i jugoistočnoj Europi u sklopu projekta Internews Journalist Security Fellowship (JSF) i korišteni su u treninzima koje su provodili stipendisti JSF-a u regiji. Ovim oglednim TTX-ovima, uključujući neke s verzijama lokaliziranim na jezike srednje i jugoistočne Europe i prevedenim na arapski i španjolski, može se pristupiti putem ove poveznice.

Ovaj je vodič posebno razvijen imajući na umu digitalnu sigurnost za novinare i redakcije, ali može biti koristan i za planiranje TTX-ova za drugu ciljanu publiku.

Što je uopće TTX? Zašto su TTX-ovi vrijedni?

Tabletop exercise (TTX) ili stolna vježba je metoda obuke koja se temelji na scenariju i često ima oblik interaktivne rasprave. TTX-ovi pružaju priliku sudionicima obuke da primijene novostečena znanja i vještine uključivanjem u izmišljenu situaciju (koja se naziva TTX scenarij ili scena) koja je približna stvarnom životu. TTX scenariji mogu ispitati širok raspon sigurnosnih situacija kao što je racija u uredu, curenje podataka, slučaj doxxinga ili osjetljiva istraga. Dok se tradicionalnije metode obuke mogu usredotočiti na prijenos određenih tehničkih vještina i znanja, TTX može pomoći da:

- Omogućite prostor s niskim rizikom za sudionike obuke kako bi vježbali pripremu i odgovor na sigurnosne probleme s kojima bi se mogli susresti.
- Potaknete kritičku raspravu o pitanjima digitalne sigurnosti i kako im najbolje pristupiti u različitim kontekstima i situacijama. Ovo bi moglo biti posebno korisno za sudionike obuke koji redovito rade zajedno kako bi razmotrili njihov zajednički ili organizacijski pristup sigurnosti.
- Procijenite koliko je dobro pojedinac ili organizacija opremljena za rješavanje sigurnosnih

problema s kojima se susreću.

Svrha TTX-a je identificirati rupe u znanju, snagama i ograničenjima na individualnoj, organizacijskoj i razini zajednice. Uspješan TTX nadilazi alate i osnovne prakse, također naglašavajući koje procedure ili politike možda nedostaju ili ih je potrebno poboljšati.

TTX-ovi su najučinkovitiji kada se koriste kao dodaci za poboljšanje drugih metoda treninga. To je zato što cilj TTX-a nije primarno prenijeti nove vještine i znanja, već dodatno usaditi i učvrstiti naučeno kroz praksu temeljenu na scenariju, raspravu i procjenu.

Komponente dokumenata TTX scenarija

Svaka od 11 TTX scena bazirana je na personi Sari koju smo opisali u ovom vodiču. Svaka scena nadalje uključuje sljedeće komponente:

- Cilj - Sveobuhvatni cilj TTX scenarija.
- Ciljevi učenja – opcije za opće ciljeve učenja na koje se treba usredotočiti tijekom TTX-a. Voditelji bi vjerojatno imali koristi od odabira samo nekoliko ciljeva učenja na koje će se usredotočiti.
- Vještine/ponašanja za treniranje prije ili poslije TTX-a – Opcije za konkretne i specifične vještine i promjene ponašanja koje TTX treba usaditi sudionicima treninga. Voditeljima bi koristio odabir samo nekoliko vještina i ponašanja na koje će se usredotočiti, a oni bi trebali biti usklađeni s odabranim ciljevima učenja i sveobuhvatnim ciljem.
- Scenarij – ovo je zapravo TTX scenarij. Uključuje sljedeće:
    - Uvodne i kontekstualne informacije na početku
    - Dodatni dijelovi konteksta koji se nalaze u cijelom scenariju
    - Pitanja i upute za sudionike za raspravu i odgovore. Oni su označeni slovom P iza kojeg slijedi broj (npr. P1, P2, P3, itd.).
    - Ispod pitanja i uputa nalaze se neki mogući odgovori. Oni se ne bi trebali dijeliti sa sudionicima tijekom TTX-a. Namijenjeni su pomoći voditelju.
    - Neki scenariji uključuju umetke (bit će označeno kao "umetak"). Umetanje je dio nove informacije ili novi razvoj situacije koji je moderator ubacio u TTX scenarij u određeno vrijeme kako bi scenarij pomaknuo naprijed ili usložnio. Umetanje može promijeniti TTX narativ i može pozvati sudionike na akciju ili odgovor.
- Prilozi - Neki scenariji (npr. Scenarij 3: Uznemiravanje i Doxxing) također uključuju dodatke, koji se često koriste za umetanje tijekom scenarija.

Razvijanje TTX scenarija

Jedanaest scenarija TTX-a razvijeno je u okviru projekta JSF (poveznica). Svatko ih može modificirati kako bi bolje odgovarale potrebama obuke njihove zajednice. Također se može stvoriti vlastiti scenarij od nule. Ako razmišljate o revidiranju jednog od TTX scenarija ili izradi vlastitog, razmislite o sljedećem.

Ciljevi učenja trebali bi biti postavljeni na početku faze dizajna, nadopunjavati jedan drugoga, slijediti logičan redoslijed u smislu učenja, imati prioritet na temelju važnosti i povezati se s općim ciljem TTX-a. Kako biste pojednostavili proces obuke i olakšali mjerenje uspjeha, povežite svoje ciljeve učenja s konkretnim vještinama ili ponašanjem na koje bi se sudionici trebali usredotočiti tijekom TTX-a. U idealnom slučaju, postavit ćete ove ciljeve učenja i konkretne vještine na temelju

potreba i razina vještina vaših sudionika. Možda ih već znate ako radite sa zajednicom koja vam je poznata. Alternativno, možda ćete trebati provesti početnu procjenu potreba (možda kroz intervjue s ključnim informantima ili prethodnu anketu) kako biste prikupili ove informacije ako ste manje upoznati sa sudionicima.

Scenarij bi trebao biti što bliži stvarnom životu, ali općenito ne bi trebao imenovati stvarne ljude ili organizacije. Usredotočite se na stvarne situacije, izazove i iskustva. U rijetkim slučajevima može biti prikladno koristiti stvarne lokacije, ali trebali biste razmotriti sigurnosne rizike i potencijalna ograničenja toga. Navođenje stvarnih lokacija moglo bi, primjerice, značiti da ljudi troše previše vremena na prisjećanje ili istraživanje detalja o njima, a manje se usredotočuju na scenarij.

Što se tiče složenosti, scenarij ne bi trebao zasjeniti ili odvratiti pažnju od učenja. Izbori mogu pomoći sudionicima da razumiju utjecaj koje će njihove odluke imati, ali imajte na umu da dodavanje složenosti i izbora otežava izradu TTX-a, a također će cijelu vježbu učiniti mnogo duljom.

Također možete koristiti vrijeme kao element dizajna tijekom svog scenarija dodjeljivanjem vremena događajima koji se događaju tijekom TTX-a, postavljanjem vremenski ograničenih pitanja ili korištenjem flashbackova ili flashforwardsa. U svakom slučaju, trebali biste biti jasni u vezi s korištenjem vremena na početku scenarija i održavati jasnoću tijekom cijele scene.

Ovisno o razini vještine voditelja i sudionika, možete razmotriti uključivanje tehničkih elemenata u TTX. To bi moglo značiti da sudionici moraju koristiti određeni alat, softver ili proces za kretanje kroz scenarij. Ako uključite tehnički element, ostavite dodatno vrijeme za dovršetak ovih zadataka i uvijek imajte rezervni plan u slučaju tehničkih problema ili neka tehnička komponenta ne bude obvezna, kako bi se prilagodila različitim razinama vještina.

Također možete koristiti umetke unutar svog TTX-a. Umeci mogu biti veliki ili mali i mogu ovisiti o sudionicima ili neovisno o njima. Općenito, umeci se koriste u duljim scenarijima s obzirom na količinu potrebnog vremena. Umetke daje voditelj, a vrijeme je ključno. Za uspješnu integraciju umataka u scenu potrebni su resursi voditelja i prije i tijekom TTX facilitacije. Korištenje umetaka trebate uskladiti s potrebom za postizanjem unaprijed određenih ciljeva učenja.

Planiranje TTX-a

Prije nego počnete planirati svoj TTX, odvojite trenutak da razmislite o svojoj ciljanoj publici i kako će to utjecati na ciljeve učenja. Obraćate li se novinarima, voditeljima redakcija, ljudima koji se bave sigurnošću? Svaki od njih će raditi s vrlo različitim informacijama i biti odgovoran za različite odluke. Alternativno, neki TTX-ovi namjerno rade s puno širim entitetom - na primjer cijelom redakcijom - kako bi bolje razumjeli kako ljudi komuniciraju i donose odluke u njima. Možda radite sa sudionicima koji imaju vrlo različite razine vještina, znanja i iskustva u digitalnoj sigurnosti.
Odvojite malo vremena za izmjenu TTX-a tako da najbolje odgovara njihovim specifičnim potrebama.

Kada imate ciljnu publiku, isplanirajte svoje ciljeve učenja i razmislite o specifičnim vještinama ili ponašanjima o kojima ćete trenirati. Odabir konkretnih vještina prije vašeg treninga ključan je za pomoć u usmjeravanju vašeg fokusa kao trenera, postavljanje opipljivih ciljeva učenja za sudionike a pomoći će i u postavljanju mjerila za mjerenje je li trening bio učinkovit. Pogledajte

popis primjera vještina u pododjeljku unutar svakog TTX dokumenta pod naslovom “Vještine/ponašanja za trenirati prije ili poslije TTX-a”. Moglo bi biti primamljivo pokriti što više ciljeva učenja unutar jednog TTX-a, ali učinkovitije je održati obuku koja pokriva specifične ciljeve učenja. Zapamtite da vaša publika ima ograničeno vrijeme i raspon pažnje.

Odredite koliko će vam vremena trebati za TTX. Iako ponekad vladine agencije ili korporacije stvaraju TTX-ove koji se protežu na više dana, vaša bi publika mogla biti u manjku vremena. Treba uzeti u obzir posao, obitelj i druge životne obveze vaših sudionika. Tipično, za TTX koji ima 4-6 pitanja ili umetke može biti potrebno oko 1 do 1,5 sat da se dovrši. To također jako ovisi o veličini vaše grupe. Većim grupama će obično trebati više vremena da dovrše TTX. Također ćete morati uzeti u obzir vrijeme za ispitivanje i pregled ciljeva učenja i konkretnih vještina ili ponašanja koje biste željeli da sudionici primijene prateći scenu. Sudionicima može biti potrebna daljnja obuka ili praćenje kako bi mogli uspješno implementirati konkretne vještine ili ponašanja.

Razmotrite prostor koji imate na raspolaganju za aktivnost. Ako se provodi uživo, idealno je omogućiti TTX u prostoru koji omogućuje suradnju. Soba sa stolovima i udobnim stolicama vjerojatno je pogodnija za TTX nego dvorana za predavanja. Možda ćete također morati osigurati kvalitetan Wi-Fi ili drugu tehničku opremu, poput projektora. Pristupačnost prostora također bi trebala biti prioritet ako je moguća (npr. pristup invalidskim kolicima, spolno inkluzivni toaleti, prikladne mogućnosti prijevoza, itd.).

Odlučite hoće li postojati više uloga voditelja i koje će to biti. Najviše bi imalo smisla da jedan voditelj vodi TTX, a drugi pomažu u određenim situacijama kao što su sobe za podgrupe (breakout rooms) ili u pod zadacima. Voditelji bi također mogli htjeti prethodno uvježbati facilitiranje nekih elemenata.

Odredite koji će vam resursi biti potrebni za TTX. Možda ćete poželjeti izraditi dijapozitive, brošure ili drugu vrstu prezentacijskih materijala za prikaz pozadine scene, pitanja/upute i/ili umetke. Također je važno uzeti u obzir materijale koje sudionici mogu trebati za bilježenje.

Vođenje TTX-a

Vođenje TTX-a razlikuje se od vođenja tradicionalne obuke o digitalnoj sigurnosti ili sesije usavršavanja. U tradicionalnoj obuci o digitalnoj sigurnosti, treneri imaju tendenciju da govore puno i od njih se očekuje da podijele svoje znanje sa sudionicima. U TTX obuci, međutim, većina govora i rada odvija se među samim sudionicima, dok raspravljaju o scenariju i donose odluke. TTX voditelj ili facilitator igra ulogu nositelja procesa , osiguravajući da TTX teče glatko i ispunjava svoje ciljeve. Voditelj TTX-a predstavlja vježbu, kontekst i pozadinu; odgovara na neka osnovna pitanja; ubacuje umetke. Druge preporuke za vođenje TTX-a uključuju:

- Provjerite jeste li dobro upoznati s TTX-om.
- Upamtite koji su osnovni cilj i ciljevi učenja TTX-a i usmjerite rasprave tako da sudionici mogu postići te ciljeve.
- Jasno komunicirajte uloge i očekivanja na početku i tijekom TTX-a.
- Pažljivo pratite sat i pobrinite se da poštujete i maksimalno iskoristite vrijeme koje provodite sa sudionicima.

- Pobrinite se da je prostor siguran i gostoljubiv te da mnogi ljudi mogu osjetiti da se njihova stajališta čuju i uzimaju u obzir.
- Kada sudionik spomene dobru praksu, istaknite je! To može povećati samopouzdanje i potaknuti daljnje sudjelovanje.
- Ako ne znate odgovor na pitanje, nemojte se bojati to reći i obvežite se da ćete se vratiti na to pitanje nakon TTX-a. Iskoristite prostor zajednice kao što je Team CommUNITY's Mattermost instanca za pronalaženje odgovora na pitanja koja možda nećete moći sami shvatiti.
- Ako je moguće, prikupljajte povratne informacije tijekom događaja i budite spremni napraviti mikro prilagodbe. Ako planirate održati više ciklusa TTX-a, također možete prikupiti povratne informacije na kraju sesije kako biste bolje razumjeli kako se možete poboljšati u budućnosti.
- Ako TTX počne ići u drugom smjeru od prvobitno planiranog, to je u redu! Budite fleksibilni, ali pazite da se u konačnici odnosi na ishode učenja.

Ako želite detaljnije upute, u nastavku su predložene upute korak po korak za pomoć pri vođenju.

1. Predstavite se (i bilo koje druge kolege), objasnite svoju ulogu(e) i opišite sveobuhvatni cilj TTX-a (na primjer: danas ćemo pogledati kako bi redakcija mogla odgovoriti na sigurnosni incident). Ovo je idealno vrijeme da postavite neka osnovna pravila kao grupa.
2. Zatim detaljnije opišite što će se dogoditi tijekom TTX-a. Objasnite da je TTX namijenjen simulaciji izmišljene situacije koja je približna stvarnom životu kako bismo bolje razumjeli naše odgovore i odgovore naše šire zajednice.
3. Ovisno o veličini i sastavu grupe, možda ćete htjeti podijeliti sudionike u podgrupe (breakout groups).
4. Sudionicima predstavite uvod u scenu, uključujući pozadinsku priču koja može biti potrebna.
5. Ispričajte scenu, dio po dio, dok se sudionici kreću kroz TTX. Budite dostupni za pitanja i pomoć u rješavanju problema ako sudionici zapnu.
6. Dajte umetke po potrebi.
7. Potaknite sudionike da se uključe i odgovore na upite. Zamolite ih da vode bilješke gdje je relevantno ili korisno. Upotrijebite svoje unaprijed pripremljene odgovore kao pomoć ako sudionici imaju problema ili trebaju primjere za početak.

Nakon što sudionici dovrše TTX, potaknite ih da rasprave o svojim glavnim potezima iz iskustva i svojim razmišljanjima o TTX-ovima kao metodi obuke. Ovo je sjajno vrijeme za snimanje povratnih informacija i razmatranje uključivanja poboljšanja za buduće obuke.

Nakon što je TTX završen, provjerite postoje li završni materijali, nastavci ili sažeci koje bi trebalo podijeliti sa sudionicima.

Dodatak 1: Osnovne informacije o Sari (TTX osoba)

Stvorili smo jednu osobu, Saru, kako bismo temeljili iskustva u primjerima TTX scenarija. To nam je pomoglo da dodamo osjećaj dosljednosti TTX-ovima i damo dobru polaznu točku novinarima za razmišljanje o prijetnjama i širem kontekstu. U nastavku smo uključili naš uvod o Sari, koji voditelji

mogu koristiti za postavljanje scene i pružanje osnovnih informacija prije pokretanja jednog od naših primjera TTX scenarija.

Sara je 41-godišnja novinarka. Nekoliko je godina radila za razne lokalne i međunarodne novinske organizacije u svojoj zemlji i susjednim zemljama.

Prošle je godine Sara počela surađivati s istraživačkom novinskom organizacijom pod nazivom 'Free Press Now' u svojoj domovini koja često izvještava o nizu političkih tema. To uključuje sumnje u kršenje ljudskih prava od strane postojeće vlade, korumpiranih vladinih dužnosnika i vladine politike koje otežavaju život etničkim manjinama u zemlji.

Zbog njihovog istinitog i pouzdanog izvještavanja, Free Press Now postao je pouzdan i popularan izvor informacija za lokalno stanovništvo.

Nakon nacionalnih izbora prije 5 mjeseci, nova vlada je počela ograničavati slobodu medija, a prošlog su tjedna vlasti pretresle domove trojice istaknutih novinara u glavnom gradu. Nedavno je pretresena i Sarina kuća, no oni koji su izvršili pretres uzeli su samo nekoliko bilježnica.

Scenarij 1: Izgubljeni uređaj

Kreirali JSF stipendisti

Cilj

Pomoći sudionicima planirati i reagirati u situaciji kad nestane jedan ili više njihovih uređaja, koji mogu sadržavati osjetljive informacije.

Ciljevi učenja

- Identificirati pristupe kojima bi se osigurava sigurna komunikacija između novinara i njihovih izvora.
- Izgraditi svijest o rizicima gubitka uređaja poput mobitela ili računala.
- Razumjeti najbolju praksu oko zaštite i sigurnosti uređaja
- Podijeliti dobre načine pristupa onboardingu i offboardingu osoblja, posebice vezano uz sigurnost uređaja.

Vještine/ponašanja za treniranje prije ili poslije TTX

- Instaliranje, postavljanje i korištenje Signala (ili druge sigurne aplikacije za razmjenu poruka)
- Postavljanje i korištenje alternativne end-to-end enkriptirane aplikacije za dopisivanje (kao što je WhatsApp ili Facebook Messenger tajni chat)
- Instaliranje, postavljanje i korištenje Mailvelopea (ili druge opcije za enkripciju e-pošte)
- Enkripcija mobilnog uređaja (postavljanje lozinke)
- Postavljanje lozinki za pojedinačne aplikacije na mobilnom uređaju
- Izrada i enkripcija sigurnosnih kopija podataka na mobilnim uređajima (pomoću usluga u oblaku ili vanjskog hard diska)

Scenarij

Putem Facebook Messangera, Saru kontaktira izvor koji joj nije poznat od ranije, tvrdeći da ima osjetljive informacije koje želi podijeliti s njom. Datoteka koju želi podijeliti sadrži podatke o financijama trenutnog ministra obrane.

Želeći sačuvati izvor sigurnim, Sara bi ga željela nagovoriti da prenese informacije putem messengera koji je end-to-end enkriptiran.

P1 - Kako Sara može objasniti koncept end-to-end enkripcije kako bi uvjerila izvora da je to važno?

- Nitko – čak ni tvrtka koja upravlja messengerom – neće imati pristup sadržaju poruke. Sadržaj poruke također neće biti pohranjen nekriptiran na serverima tvrtke

- Policija nema pristup datoteki preko chat providera
- Ako napadač uspije hakirati račun koji je korišten za slanje poruke, neće moći pristupiti ni sadržaju poruka (osim ako nije bilo nekriptiranih sigurnosnih kopija)

P2 - Kako bi njihova komunikacija ubuduće bila sigurna, koje oblike digitalne komunikacije s ovim izvorom Sara treba razmotriti?

- Messengeri s end-to-end enkripcijom i nestajućim porukama
- Enkriptirana elektronička pošta

Izvoru je drago što je Sara fokusirana na sigurnost njihove komunikacije, ali još nije siguran koju metodu prioritizirati. Pitao je Saru za savjet o aplikacijama za dopisivanje poput Signala, Telegrama, Facebook Messengera, kao i o njegovoj e-pošti.

P3 (Izbor) - Iz perspektive digitalne sigurnosti, koje čimbenike treba razmotriti pri odabiru i korištenju različitih aplikacija za dopisivanje?

- Telefonski brojevi: većina end-to-end enkriptiranih messengera zahtijeva telefonske brojeve, a na mnogim mjestima (državama) telefonske brojeve je potrebno registrirati, tako da vlada zna koja osoba stoji iza kog telefonskog broja. To znači da bi, ako bi vlada ikada pregledala Sarin ili izvorov telefon, mogli shvatiti da su slali poruke, čak i ako su koristili pseudonime ili nestajuće poruke (jedino ublažavanje bilo bi brisanje imena iz kontakata, messengera i idealno očistiti telefon)
- Tajni chatovi: Facebook Messenger i Telegram nude dva načina, od kojih je samo jedan end-to-end enkriptiran. Ovaj način rada obično se naziva tajni chat ili slično i često je zakopan u postavkama
- Nestajuće poruke: gotovo svaki moderni messenger ima značajku nestajućih poruka, iako je u nekima dostupna samo u tajnom načinu chata
- Brisanje chatova: ovo je prilično jednostavno, ali važno je znati da neki messengeri samo arhiviraju, a ne brišu chatove
- Svijest o snimkama zaslona: svaka zlonamjerna strana u razgovoru mogla bi samo napraviti snimku zaslona ili – ako značajke messengera to ne dopuštaju – jednostavno fotografirati zaslon njihova telefona
- Dvofaktorska verifikacija (2FV): napadač bi mogao preuzeti račun messengera preuzimanjem telefonskog broja koji je korišten za registraciju računa i ponovnim slanjem SMS-a za potvrdu. To im omogućuje lažno predstavljanje kao vlasnika računa, iako obično ne daje pristup povijesti poruka. Većina messengera sada ima opciju zahtijevanja dodatne lozinke uz SMS kod: to znači da, čak i ako bi napadač uspio preuzeti telefonski broj, ne bi mogao lako pristupiti računu
- Jake lozinke ili lozinke-fraze za prijavu na sam uređaj (telefon).

P4 (Izbor) - Iz perspektive digitalne sigurnosti, koje čimbenike treba razmotriti u komunikaciji e-poštom?

- Izvor bi trebao napraviti novu adresu e-pošte samo za komunikaciju sa Sarom

- Nova e-pošta trebala bi imati jaku i jedinstvenu lozinku i čvrstu dvofaktorsku autentikaciju
- Izvor također treba paziti na phishing napade i koristiti tehnologije koje bi mogle pomoći u njihovom ublažavanju, kao što su fizički sigurnosni ključevi ili automatsko popunjavanje upravitelja zaporki
- U idealnom slučaju, izvor i Sara bi trebali komunicirati putem PGP-a, na primjer koristeći Mailvelope. To znači da, čak i ako su njihovi računi na neki način ugroženi, napadač i dalje ne bi mogao pročitati sadržaj njihovih poruka bez njihovog PGP ključa

Izvor na siguran način šalje datoteku Sari i ona ju pregledava na svom mobitelu. Sretna što je dobila informaciju, izlazi s prijateljima proslaviti. Dok je na zabavi, izgubi telefon i shvati da na njemu ima vrlo jednostavnu lozinku (1111).

P5 - Što se može dogoditi Sarinom mobitelu i informacijama koje se ondje nalaze?

- Svatko tko pronađe telefon može pristupiti osjetljivoj informaciji ako sazna gdje se nalazi
- Svatko tko pronađe telefon mogao bi poslati poruku Sarinim kontaktima i pretvarati se da je ona
- Svatko tko pregleda informacije na telefonu mogao bi ugroziti identitet i sigurnost Sarinih kontakata ili prikupiti informacije koje bi se mogle koristiti za društveni inženjering
- Sara bi mogla ozbiljno izgubiti svoj kredibilitet kao novinarka

P6 - Što Sara može napraviti kako bi ograničila utjecaj gubitka uređaja na njenu digitalnu sigurnost?

- Može daljinski obrisati svoj telefon ako je postavila tu funkciju
- Može se prijaviti na svoju e-poštu i račune društvenih mreža na svojim drugim uređajima, promijeniti lozinku i ako je moguće kliknuti "odjava sa svih prijavljenih uređaja"

P7 - Koje su prednosti i nedostaci otkrivanja izvoru da je izgubila mobitel?

- Rasprava bez točnih i preciznih odgovora.

Dobre vijesti! Sarin prijatelj koji je bio s njom na zabavi, je našao mobitel u svojoj jakni. Nazvao ju je i vratio joj mobitel sljedeći dan.

Q8 - Sada kada Sara opet ima svoj mobitel, što može napraviti da digitalno osigura svoj uređaj u slučaju da ga ponovno izgubi?

- Razmotriti korištenje biometrijskog otključavanja. To ima prednosti (nitko ne može gledati preko Sarinog ramena dok upisuje lozinku, a neće je snimiti ni CCTV kamere) i nedostataka (lakše je prisiliti Saru da otključa svoj uređaj).
- Koristiti duže lozinke i lozinke-fraze za otključavanje telefona. Izbjegavati otključavanje uzorkom (poput onih koje spajaju točkice), budući da ih lakše može otkriti osoba koja posmatra, kamerom ili mrljom na zaslonu.

- Također zaključati aplikacije (kao što su messengeri) s dodatnom lozinkom, ako je Sara zabrinuta da bi njezin telefon mogao biti dijeljen ponekad, odnosno da bi ga netko drugi mogao koristiti.
- Postavite aplikacije koje mogu pratiti, locirati i daljinski brisati uređaje.

P9 - Iz organizacijske perspektive, kako izgleda dobar proces onboardinga novog osoblja da osigura svoje uređaje, poput mobilnih telefona i računala?

- Pobrinuti se da svo osoblje, bez obzira na položaj, prođe kroz onboarding proces i da razumije njegovu važnost
- Organizacije bi trebale jasno navesti koja očekivanja imaju od osoblja vezano uz praksu digitalne sigurnosti organizacije.
- Identificirati korake koje treba poduzeti i ljude koje treba kontaktirati u slučaju kad bi sigurnost mogla biti ugrožena (primjerice mobitel je ukraden ili je lozinka hakirana)
- IT podrška treba biti pružena svim članovima koji ju trebaju.

Scenarij 2: Operativna sigurnost

Kreirali JSF stipendisti

Cilj

Pomoći sudionicima da osiguraju postojanje visoke razine svijesti o digitalnoj sigurnosti i najboljim praksama unutar njihove organizacije, među kolegama i/ili honorarnim novinarima.

Ciljeva učenja

- Teorijski - razumjeti koncept digitalne sigurnosti kao kontinuiranog procesa, a ne krajnji cilj.
- Razgovarati, podučavati i uvjeriti druge u važnost digitalne sigurnosti.
- Praktični - raspraviti o mogućnostima sigurnog komuniciranja kroz mobilne uređaje.
- Osigurati najbolje prakse za sigurno rukovanje datotekama.
- Postići svijest o postavkama računa za umrežena računala.
- Razumjeti važnost modeliranja prijetnji.

Vještine/ponašanja za treniranje prije ili poslije TTX

- Postavljanje i održavanje dopuštenja na suradničkim platformama (npr. Google disk)
- (Ako je moguće, budući da su neke od tih značajki dostupne samo na platformama poduzeća) Gledanje evidencije pristupa na platformama za suradnju kao što je Google disk
- Postavljanje i korištenje dvofaktorske autentikacije, idealno s fizičkim sigurnosnim ključevima ili sličnim mehanizmima otpornim na krađu identiteta
- Dobra pravila za lozinke (korištenje jedinstvenih lozinki, korištenje dugih lozinki, korištenje lozinki fraza - rečenica) i upravitelji lozinki
- Enkripcija dokumenata (korištenje Mailvelopea, itd.)
- Instaliranje, postavljanje i korištenje Signala (ili druge sigurne aplikacije za razmjenu poruka)
- Korištenje naprednih značajki unutar aplikacije za sigurnu razmjenu poruka (tj. vremenski određeno brisanje poruka)
- Instaliranje, postavljanje i korištenje Mailvelopea (ili druge opcije za enkripciju e-pošte)
- Siguran rad s datotekama i dokumentima iz osjetljivih izvora

Scenarij

Sara sastavlja tim novinara kako bi istražili korupciju u Ministarstvu zdravstva, povezanu s javnom nabavom tijekom pandemije koronavirusa. Novinari koji su u timu nemaju istu razinu digitalnih vještina niti znanja o digitalnoj sigurnosti i njenim praksama. Sara zna da jedan od članova njenog tima ima neuredne prakse u vezi sa zaštitom datoteka.

P1 - Kako Sara može potaknuti kolege da poboljšaju svoje pristupe digitalnoj sigurnosti? Što bi Sara trebala napraviti da osigura korištenje digitalnih sigurnosnih praksi kad organizira tim koji će međusobno surađivati?

- Objasniti zašto je važno imati dobru digitalnu sigurnost: to može uključivati razgovor o tome kako bi loša digitalna sigurnost mogla značajno ugroziti karijeru novinara, kako će vam izvori i kolege vjerojatnije vjerovati više ako imate dobru digitalnu sigurnost i potrebu zaštite ljudi oko vas.
- Razgovarati koje uređaje koriste, kako štite svoje korisničke račune, kako pohranjuju i razmjenjuju datoteke, kako pristupaju poslovnoj mreži (koriste li svoj uređaj ili rade na službenom računalu), kako se spajaju na mrežu (bežično ili žičano), koriste li dvofaktorsku autentikaciju kako bi osigurali svoje korisničke račune, i kakva im je disciplina lozinki (koriste li iste lozinke, koriste li upravitelj lozinki).
- Donijeti odluku o tome kako bi tim trebao komunicirati, pohranjivati datoteke i pristupati im. Ovo je kako bi se osiguralo da svi slijede isti protokol koji se odnosi na prethodno navedene aktivnosti.
- Razmotriti obuku tima koristeći novouspostavljene protokole. Nakon uvođenja pravila, tim bi trebao proći probu, stvarno testirajući nove načine komunikacije kako bi vidjeli postoje li poteškoće koje treba razriješiti.

P2 - Kako će Sara i njezin tim pohranjivati audio datoteke i dokumente koje dobiju od svojih izvora?

- Ograničiti tko ima pristup raznim datotekama i mapama, pažljivo koristite postavke dijeljenja na mjestima kao što je Google disk
- Obeshrabriti ljude da iznose datoteke i dokumente iz radnog okruženja (usb ključeve, privitke e-pošte...) što bi moglo povećati opseg napada i povećati rizik od curenja informacija/hakiranja.
- Zamoliti tim da za pristup radnim datotekama uvijek koriste samo radna računala
- Ograničiti što se može instalirati na radna računala, osigurati da uvijek imaju jake lozinke i ažuriran softver

P3: Kako će Sara i njezin tim osigurati sigurnu komunikaciju?

Uključivanjem cijelog tima na istu platformu, te osiguravanjem da se svi slažu s njezinim korištenjem, Sara može pomoći svom timu da uspostavi siguran način međusobne komunikacije.

Razmisliti o:

- Premještanju većine razgovora u Signal, s nestajućim porukama i kopiranjem poruka koje je potrebno arhivirati
- Korištenju PGP-a na e-pošti
- Stvaranje jakih sigurnosnih pravila zaštite računa za e-poštu (jedinstvena lozinka, 2FA)

Dva tjedna prije objave izvještaja, Sara dobiva telefonski poziv od glavnog izvora iz vlade u ovoj istrazi. Sara dobro poznaje izvor i vjeruje mu. Tijekom razgovora, izvor kaže: "Vlada zna, priča je procurila" i poklopi slušalicu.

P4 - Iz perspektive digitalne sigurnosti, koji su neki od prvih koraka koje bi Sara trebala učiniti po pitanju curenja podataka?

- Zamoliti sve unutar svog tima da promijene lozinke, za slučaj da je napadač dobio lozinku za neki od njihovih računa.
- Uzeti u obzir činjenicu da vlada nije nužno morala provaliti u njezinu redakciju; moguće je da su saznali za curenje tako što su, na primjer, istraživali koji vladini zaposlenici su i što su ispisivali na pisaču.
- Provesti malu istragu unutar redakcije: provjeriti jesu li svi slijedili protokole, tko je imao pristup datotekama i informaciji koja je procurila te što je točno procurilo. Korištenjem kontrole pristupa i kontrole verzija može se lakše pratiti pristup pojedinačnim dijelovima podataka na kojima se radi.
- Razmisliti treba li ubrzati objavljivanje.

Sara saznaje da je do curenja informacija došlo iz njezine organizacije. Dizajner je imao pristup dijeljenom Google disku organizacije. Sara je to saznala provjeravajući kontrolu pristupa Google disku, shvativši da dizajnerski tim ima pristup svemu na mreži zbog prirode svog posla i vidjevši da je dizajner slučajno podijelio dokument ss svojim freelance klientom koji je radio za vladu, umjesto s prijateljem u redakciji koji se isto preziva.

P5 - Što je Sara mogla drugačije napraviti u ovoj situaciji?

- Sara bi trebala uspostaviti sigurne protokole koji se odnose samo na njezin istraživački tim. Ona bi trebala osigurati da postoji jasan sustav dopuštenja i da se on poštuje u praksi.
- Tim bi trebao raditi s dizajnerima tako da im se pružaju samo neophodne informacije: ne smiju im se davati nikakve tajne ili osjetljive pojedinosti osim ako nisu apsolutno nužne za objavu.
- Sara bi također trebala razmatrati sigurnost i privatnost kao proces, a ne kao stanje; to je nešto što treba stalno ponavljati.

Scenarij 3: Uznemiravanje i doxxing

Kreirali JSF stipendisti

Cilj

Pomoći sudionicima da konceptualiziraju kako se najbolje pripremiti i odgovoriti na doxxing i online uznemiravanje.

Ciljevi učenja

- Identificirati metode i mitigacijske mjere za novinare koji se nose s uznemiravanjem na društvenim mrežama i doxxingom.
- Razumjeti kako se informacije na društvenim mrežama mogu prikupljati i koristiti protiv novinara i članova redakcije.
- Istražiti povezanost rodnog identiteta i uznemiravanja te sigurnosne implikacije tog odnosa
- Raspraviti o tome kako medijska organizacija može uspostaviti procedure i prakse za zaštitu zaposlenika i vanjskih suradnika koji su meta uznemiravanja i doxxinga.
- Razmotriti planove za nepredviđene situacije za novinare koji nemaju podršku redakcije (npr. honorarci, vanjski suradnici)
- Pričanje priče o sigurnosti i uvjeravanje drugih, kako možemo razgovarati s ljudima koji se tradicionalno ne suočavaju s uznemiravanjem, da je to veliki problem koji zahtijeva koordinirano organizacijsko djelovanje i podršku
- Organizacijska sigurnost: postavljanje politika unutar organizacija, pronalaženje načina na koje organizacije mogu najbolje podržati novinare koji su suočeni s napadima uznemiravanja[1]

Vještine/Ponašanja za trenirati prije ili poslije TTX-a

- Upravljanje i ažuriranje postavki privatnosti na glavnim platformama društvenih mreža
- Korištenje sigurnosnih alata na glavnim platformama društvenih mreža, kao što su prijavljivanje i blokiranje. To uključuje i razumijevanje kako koristiti takve mehanizme i što oni točno rade
- Postavljanje i korištenje dvofaktorske autentikacije, idealno s fizičkim sigurnosnim ključevima ili sličnim mehanizmima otpornima na phishing

[1] U većini treninga to bi bio cilj učenja. Ako vodite sesiju s medijskim menadžerima ili drugim donositeljima odluka i moguće je izmjeriti organizacijske rezultate, ovo također možete provjesti kao vještinu

Scenarij

Sara radi na novom prilogu o etničkim manjinama u svojoj zemlji i o tome kako vladine politike dovode do povećane marginalizacije tih skupina. Proteklih tjedana Sara vidi porast komentara na društvenim mrežama na svojim računima na kojima također dijeli svoj rad. Također je počela primati komentare pune mržnje i pogrdne komentare različitih online trolova upućene direktno njoj.

P1 - Koji su neki od koraka koje Sara može poduzeti da blokira i prijavi osobe koje ostavljaju ove komentare?

- Može koristiti ugrađene funkcije blokiranja i prijavljivanja koje se nalaze na većini društvenih mreža.
- Može kontaktirati velike društvene mreže (izravno ili preko svoje organizacije) kako bi prijavila uznemiravanje velikih razmjera.
- Onemogućiti objave i odgovore na svojem profilu
- Biti selektivnija oko toga tko je može pronaći na društvenim mrežama
- Odabrati da je se ne može označiti na društvenim mrežama
- Napori da se blokiraju i prijave neki od glavnih internetskih huškača su zasmetali skupinu trolova, što je dovelo do porasta sadržaja punih mržnje protiv Sare. Neki komentari sugeriraju prijetnje i nasilje prema njoj, bilo izravno ili neizravno.

P2 - Na koje načine Sara može istražiti ovu agresiju protiv nje kako bi utvrdila je li to dio veće, koordinirane kampanje ili nešto više organsko?

- Može sama istražiti situaciju, kao i zatražiti podršku od kolega za istragu
- Može provjeriti koriste li svi trolovi potpuno isti jezik, ključne riječi i hashtagove. Ukoliko to rade, vjerojatno se radi o koordiniranoj kampanji
- Ovisi o platformi. Na Instagramu postoje opsežne opcije za pregled informacija o određenim računima - kada je kreiran, koliko ga ljudi koristi, koliko često je mijenjao svoje ime i slično.
- Provjeriti je li pojačan nekim medijem
- Vidjeti najčešće vrijeme objavljivanja

Govori kolegama o objavama, no većina muškog dijela tima, uključujući i urednika, joj govori da se ne brine i da će problem nestati sam od sebe. Pod stresom je, osjeća da je njezin tim ne sluša ili ne razumije problem.

Q3 - Umjesto da kažu Sari da ne brine, na koje načine njezin tim i organizacija mogu podržati Saru, posebno u smislu njezine online prisutnosti i digitalne sigurnosti?

- Pomoći u provedbi potpune procjene situacije
- Revidirati zajedno sa Sarom njezine digitalne sigurnosne prakse i sigurnosne mjere koje su na snazi te pomoći poboljšati situaciju ako je potrebno.
- Podijeliti praktična iskustva drugih u organizaciji.

- Dopustiti osobama kojima vjeruju da upravljaju njihovim računom ili da ga pregledavaju tako da ne budu izravno izloženi tim riječima i prijetnjama, a i dalje mogu biti prisutni
- Organizacija može pomoći u traženju obrazaca uznemiravanja
- Pratiti kako se uznemiravanje odvija kroz objave organizacije, a ne samo Sarine
- Naglasiti to sigurnosnom timu i pomoći u istrazi

Jednog dana, jedan od trolova je objavio Sarine fotografije. Fotografije, koje je prije nekoliko godina objavila na društvenim mrežama, su osobne i u nekim slučajevima sadrže neke osjetljive informacije.

INJECT: Podziel się z uczestnikami od 1 do 4 zdjęć. Przykłady zdjęć:

Sara i jej pies spacerujący przed domem

Sara paląca papierosa z marihuaną

Sara i grupa jej najbliższych przyjaciół na wakacjach

Sara pracująca w swoim newsroomie

Przedyskutuj z grupą uczestników, dlaczego każde z tych zdjęć może być wrażliwe.

P4 – Na koje je načine netko mogao pristupiti Sarinim podacima na mreži, poput starih objava na društvenim mrežama?

- Sarini prijatelji su objavili fotografije sa slabim postavkama privatnosti
- U Sarine račune je provaljeno
- Jedan od Sarinih kontakata na društvenim mrežama je možda sačuvao fotografije kako bi ih podijelio kasnije
- Sarine fotografije na društvenim mrežama mogla je indeksirati tražilica

P5 – Koje korake Sara može poduzeti kako bi pokušala spriječiti daljnje curenje informacija o sebi na internetu?

- Izbrisati stare fotografije
- Izbrisati račune
- Zaključati račune
- Postaviti nove fotografije koje odaju malo informacija o njoj.
- Dobiti izvješće od društvene mreže koje sažima sve podatke koje imaju o njoj
- Prijaviti fotografije koje su nedavno objavljene/prijaviti račune koji su ih objavljivali
- Nastaviti objavljivati poslovni sadržaj čak i ako objavljuje manje osobnog sadržaja. Ode li s interneta, trolovi će pobjediti

- Uzeti snimku zaslona objava, dokumentirati ih što je više moguće. Zabilježiti online nadimke trolova

P6 – Koje su korake Sara I njena organizacija mogli poduzeti kako bi spriječili prikupljanje I curenje tih informacija na internetu, posebno u smislu digitalne sigurnosti?

- Stvoriti grupu bliskih prijatelja koji su jedini koji mogu vidjeti privatne fotografije i privatne objave na društvenim mrežama
- Uopće ne objavljivati osjetljive informacije (kao što je fotografija s jointom)
- Ne objavljivati fotografije koje otkrivaju privatne informacije kao što je lokacija
- Otvoriti poslovne račune kako bi imala online prisutnost koja nije vezana uz njen privatni život
- Jaka lozinka i 2FA politike za račune društevnih mreža

Dodatak 1: Primjeri fotografija

Scenarij 4: Ulazak organa vlasti u redakciju

Kreirali JSF stipendisti

Cilj

Pomoći sudionicima u teoretskom i praktičnom odgovoru na ulazak organa vlasti u njihovu redakciju

Ciljevi učenja

- Osigurati da su implementirani rezervni komunikacijski planovi i tehničke komponente u slučaju da pristup redakciji ili osobnom uređaju više nije moguć.
- Razumjeti najbolju praksu kad je u pitanju osiguranje digitalnih uređaja unutar redakcije ili organizacije.
- Identificirati načine za zaštitu različitih datoteka na digitalnom uređaju, poput računala ili mobitela.
- Planirati što sa kompromitiranim informacijama u slučaju racije na redakciju.
- Istražiti koncepte oko modeliranja prijetnji i pretplaniranja za individue i organizacije.

Vještine/Ponašanja za trenirati prije i poslije stolne vježbe

- Korištenje alata kao što je VeraCrypt ili sličnog za enkriptiranje podataka na tvrdim i vanjskim diskovima
- Modeliranje prijetnji, posebno u smislu suočavanja s vlastima i racija u uredima: kako procijeniti rizike, pripremiti se za jednu i preispitivanje nakon jedne
- Sigurnost organizacije i zajednice, posebno kako raditi s urednicima, menadžerima i odvjetnicima tijekom situacija visokog stresa i identificirati koje pitanje eskalirati kojoj osobi
- Korištenje postavki unutar Microsoft Officea i Google Drivea da se vidi kojim datotekama je nedavno pristupljeno i kada
- (Napredno) Ako organizacija ima temeljite pristupne logove putem premium Google Drivea ili O365 pretplate, pristupanje i rad s takvim logovima
- Pregledavanje povijesti pretraživanja i pristupa datotekama na vodećim web preglednicima i operativnim sustavima

Scenarij

Sara radi u redakciji od dvadesetak ljudi. Užurbani ponedjeljak je, 15 novinara i drugog osoblja radi iz redakcije, dok drugih 5 kolega radi udaljeno.

U 10 ujutro, otprilike 50 policijskih službenika dolazi u redakciju. Imaju nalog kojeg pokažu uredniku, zatim nasilno ulaze istovremeno zahtjevajući da svi novinari i osoblje napuste prostorije odmah.

Sara i njene kolege se okupljaju vani i raspravljaju o načinima kako nastaviti sa radom njihove medijske organizacije na siguran način.

P1 – Koji su neki od prioriteta u situaciji poput ove?

- Stupiti u kontakt s odvjetnikom radi savjetovanja o idućim koracima
- Kontaktirati kolege koji rade na daljinu
- Provjeriti tko ima mobitele kod sebe, a koji su ostavljeni

P2 – Koji su neki od načina na koje Sara i njezine kolege mogu komunicirati sigurno u ovo vrijeme?

- Kreirati grupni razgovor na WhatsAppu/Signalu
- Mogla bi biti dobra ideja komunicirati putem osobnih, a ne poslovnih brojeva. U suprotnom bi se razgovor mogao sinkronizrati s uređajima koji su još u uredu

P3 - Kako bi Sara i njezine kolege trebali koristiti organizacijske online račune, kao što su računi za internetske stranice i društvene mreže?

- Promijeniti šifre odmah
- Ukoliko je moguće na daljinu odjaviti se s uređaja koji su još u uredu, neka to učine, ali neka se prvo posavjetuju s odvjetnicima kako se to ne bi smatralo petljanjem s dokazima (može uvelike ovisiti o lokaciji/jurisdikciji)
- Neka se posavjetuju s odvjetnicima prije objave o policijskoj raciji

Sara se sjeća da je pri odlasku iz redakcije vidjela da je policija počela stavljati računala, uređaje, i papire u vreće. Sara je uspjela otići sa svojim mobitelom, ali je njen laptop ostao u redakciji. Grupa kolega brzo procjenjuje koje informacije policija može dobiti.

P4 - Kako su uređaji u redakciji trebali biti osigurani?

- Računala zaključana snažnim lozinkama
- Zaključavanje zaslona se pali nakon kratkog vremena
- Enkriptirani USB-i i vanjski diskovi

Tijekom rasprave izvan ureda urednik otkriva da je zaboravio zaključati svoje računalo prije izlaska iz ureda.

Policija napušta redakciju dva sata kasnije, dopuštajući novinarima da se vrate. Osoblje se okuplja kako bi raspravili kojim informacijama je policija mogla pristupiti, te kako bi raspravili slične prijetnje u budućnosti.

P5 – Koji su neki od načina na koje redakcija može odmah procijeniti učinak racije od strane vlasti?

- Neka pogledaju koje su datoteke, ukoliko postoje, oduzete ili preuređene (ako su datoteke preuređene, to znači da ih je policija možda uslikala)

- Računala obično imaju povijest pretraživanja/pristupa datotekama/posjećenih internetskih stranica, pregledajte i to. Možete vidjeti nedavno otvorene datoteke u Microsoft Wordu i povijest izmjena ako koriste Google Docs. Ako je povijest datoteka obrisana, to također znači da je netko možda pokušao izbrisati tragove
- Malo je vjerojatno da bi bilo kakav zlonamjerni softver bio instaliran tijekom racije, ali ako su zabrinuti zbog toga, neka se posavjetuju sa stručnjakom za forenziku zlonamjernih softvera

P6 – Kako bi organizacija trebala osigurati da ih ova racija policije ne izloži dodatnom riziku?

- Promijeniti lozinke, za svaki slučaj
- Razgovarati s odvjetnikom o tome čemu policija nije smjela pristupiti tijekom racije
- Ako su koristili kodna imena ili pseudonime u svojoj pretrazi, obrnite ih

Nekoliko tjedana kasnije, urednik redakcije saziva sve novinare i osoblje. Svi žele razumjeti sve slične prijetnje s kojima bi se redakcija mogla suočiti u budućnosti.

P7 - U smislu modeliranja prijetnji i digitalne sigurnosti, koga individue i organizacije identificiraju kao prijetnje s kojima se mogu suočiti?

- Neka postave standardna pitanja modeliranja prijetnji: koje informacije imaju, tko bi mogao biti zainteresiran da im pristupi i koje bi bile posljedice ako njihovi protivnici uspiju
- Kada nabrajaju protivnike, neka razmisle i o motivima (što bi htjeli učiniti i zašto) i o sposobnostima (što su zapravo sposobni učiniti, koja tehnička, pravna, organizacijska i financijska sredstva imaju?)

Scenarij 5: Organi vlasti ulaze u dom novinara

Kreirali JSF stipendisti

Cilj

Dati novinarima teoretske i tehničke vještine kako bi osigurali najbolju moguću digitalnu sigurnost u okruženju svog doma

Ciljevi učenja

- Razumjeti kako osigurati digitalne uređaje koji se nađu u domu
- Primjena sigurnosnih mjera na papirnate bilježnice
- Pokretanje daljinskog brisanja datoteka, te pozitivne i negativne strane toga.
- Ograničavanje pristupa informacijama koje su kompromitirane.
- Pripremanje za ulazak organa vlasti u dom novinara
- Poticanje sudionika da malo razmisle o organizacijskoj sigurnosti i sigurnosti zajednice, posebno o tome kako raditi s urednicima, menadžerima i odvjetnicima tijekom visokostresnih situacija i identificirati koja pitanja eskalirati kojoj osobi

Vještine/Ponašanja za trenirati prije ili poslije stolne vježbe

- Korištenje alata kao što je VeraCrypt ili neki sličan za enkriptiranje podataka na tvrdim i vanjskim diskovima
- Modeliranje prijetnji, posebno u smislu suočavanja s vlastima i kućnim racijama: kako procijeniti rizike, pripremiti se za jednu i preispitivanje nakon jedne
- Aktiviranje alata kao što je Apple-ov Find My ili Android-ov/Samsung-ov Find koji se mogu koristiti za daljinsko zaključavanje ili brisanje na uređajima
- Korištenje postavki unutar Microsoft Officea i Google Drivea da bismo vidjeli kojim je datotekama nedavno pristupljeno i zašto
- (Napredno) Ako organizacija ima temeljite pristupne logove putem premium Google Drivea ili O365 pretplate, pristupanje i rad s takvim logovima
- Pregledavanje povijesti pretraživanja i pristupa datotekama na popularnim web preglednicima i operativnim sustavima

Scenarij

Nakon nacionalnih izbora prije 5 mjeseci, nova vlada je počela naređivati organima vlasti da ograniče slobodu medija, te su oni pretresli domove trojici istaknutih novinara u glavnom gradu. Kao odgovor, Sara i nekoliko kolega okupili su se i razgovarali o načinima kako zaštiti sebe i svoje podatke ako se suoče sa sličnim scenarijem.

P1 - Koje bi stvari novinar trebao uzeti u obzir kad odlučuje pohranjivati informacije u svom domu?

- Čuvanje uređaja na sigurnom mjestu u domu
- Enkripcija i zaštita lozinkom na svim uređajima
- Ne držati informacije o izvoru na dokumentima
- Održavanje inventara o tome koje informacije se gdje čuvaju (čuvati i ovaj popis na sigurnom!)
- Podaci koji nisu digitalni: biti svjestan fizičkih kopija
- Uzeti u obzir da se, ukoliko je to moguće, ništa osjetljivo ne drži kod kuće
- Poštivanje lokalnih zakona kao i pravila organizacije
- Biti svjestan pravnih posljedica pohranjivanja osjetljivih informacija doma umjesto u uredu.
- Razmisliti tko ima pristup Vašem domu i uređajima?

P2 (opcionalno) - Koji su primjeri najbolje prakse za pohranjivanje papirnatih bilježnica u domu?

- Razmislite o uništavanju onoga što vam ne treba
- Ne držite sve bilješke na jednom mjestu – manje informacija kojima je lako pristupiti
- Sakrijte bilježnice
- Sef, lokot i ključ, osigurajte!
- Koja je razina osjetljivih informacija koju bi trebalo čuvati u domu?
- Koristite akronime, pseudonime i kratice koje samo vi razumijete

P3 - Koje mjere se mogu poduzeti kako bi se što bolje zaštitili elektronički uređaji (računala, diskovi, USB memorije itd.)?

- Enkripcija
- Zaštita lozinkom
- Čuvanje sigurnosnih kopija na drugom mjestu
- Razmotriti sigurno odlaganje starih uređaja, posebno onih koji se više ne koriste

Danas je Sara otišla od doma u 9 ujutro kako bi popila kavu i kupila namirnice. Kad se vratila nakon sat vremena, vrata njezina stana su bila otvorena. Sara je ušla u svoj stan i zatekla dva muškarca kako pretražuju njezin stol i spavaću sobu. Jedan od muškaraca je čitao Sarine bilježnice dok je drugi držao torbu u kojoj je bio Sarin laptop. Sara uočava da na njezinom stolu nedostaju USB-ovi i eksterni hard diskovi. Dvojica muškaraca nose civilnu odjeću, ali Sara pretpostavlja da na neki način rade za vladu.

Izbor 1 - Sara nakratko razgovara s dvojicom muškaraca i može sigurno napustiti svoj dom. Odšeće do obližnjeg prijatelja.

P4 (opcionalno) - Znajući da su neki od njenih podataka, posebno iz njene bilježnice, kompromitirani, koga bi Sara trebala obavijestiti o ovom incidentu?

- Informirati urednika i odvjetnika redakcije
- Prije nego što kontaktira bilo kojeg izvora koji se možda spominje u bilježnici, prvo neka razgovara s urednikom i ostatkom redakcije, također i sa stručnjacima za sigurnost (ako se izvori spominju samo pseudonimom, ali prime poziv idući dan, to može omogućiti sigurnosnim službama da povežu izvora sa pseudonimom). Može biti mudro ne zvati ih isprva

P5 - Što bi Sara mogla učiniti da dodatno spriječi pristup svojim digitalnim podacima dok su dvojica muškaraca još u njenom stanu?

- Učiniti sve što može u skladu s lokalnim zakonima
- Inzistirati da organi vlasti također poštuju lokalne zakone (npr. dopustiti snimanje, svjedočenje, itd.)
- Tehnike smirivanja situacije
- Otkriti tko su oni i imaju li ovlasti/nalog/dozvolu
- Procijeniti situaciju za osobnu sigurnost
- Potražiti pravni savjet, nazvati redakciju
- Dati lažne račune i dokumente (ovo može zahtjevati neku pripremu)
- Deflekcija (otklanjanje)

Izbor 2 - Sara ne može napustiti svoj stan. Dvojica muškaraca ju mole da sjedne, i zahtijevaju da im da lozinke za svoje računalo i USB memorije. Prijete joj da će ju odvesti u policijsku postaju ako im ne da te informacije. Sara traži nalog, ali ga oni ne daju.

P6 - Znajući da ima osjetljive informacije na svom računalu, uključujući identifikacije povjerljivih izvora, koje opcije Sara ima u ovoj situaciji?

- Procjena ranjivosti i prioritiziranje najbitnijih problema
- Udaljena odjava i udaljeno brisanje osjetljivih računa
- Identificiranje svih informacija pohranjenih u domu
- Razmotriti prednosti i mane obavještavanja članova tima i izvora koji bi mogli biti u opasnosti. Možda donijeti ovu odluku uz potportu redakcije.
- Potencijal za udaljeno brisanje datoteka

P7 - Sara ima podešen program za udaljeno brisanje datoteka na svom računalu. Što treba razmotriti prije nego obriše datoteke sa svog računala?

- Brisanje može biti pravno pitanje - ometanje pravde
- Razmisliti o potencijalnim posljedicama, ako je moguće, razgovarati prvo s odvjetnikom

- Ako Sara nema dokaze da su ti ljudi iz policijskih snaga, ali izgledaju kao standardni uljezi ili iz nedržavnih sigurnosnih snaga, onda to također mijenja pravni i prijeteći okvir

P8 (opcionalno) - Znajući da su neke njene informacije kompromitirane, kog bi Sara trebala obavijestiti o ovom incidentu? Je li bitan slijed kojim obavještava ljude?

- Urednik redakcije
- Sigurnosni/IT tim redakcije
- Razmotriti kontaktiranje izvora
- Ako je honorarni novinar, razmotriti dijeljenje situacije s drugim honorarcima.

Sara odbija dati lozinke za svoje uređaje. Nakon što provedu još 10 minuta pretražujući njezin stan, dvojica odlaze sa Sarinim računalom, USB-ovima i bilježnicom.

Sara sad opet ima pristup svom stanu. Vidi da je jedno od njena dva računala ostalo, skupa sa jednim USB-om. Sve bilježnice su odnesene iz stana.

P9 - Što bi Sara sad trebala učiniti kako bi osigurala da njezine informacije i sigurnost nisu daljnje ugroženi radnjama dvojice koji su bili u njezinom stanu?

- Možda su instalirali zlonamjerni softver na Sarine uređaje; mogla bi biti dobra ideja dati te uređaje stručnjaku za digitalnu forenziku
- Razmotriti da bi njen stan mogao biti ozvučen
- Pitati svoju organizaciju koju vrstu podrške može primiti od njih
- Razgovarati sa svojom organizacijom, savjetnicima za pravo i sigurnost o tome ima li smisla iz sigurnosne perspektive javno govoriti o raciji ili ne

P10 (opcionalno) - Osim aspekta digitalne sigurnosti ovog scenarija, koje druge mjere predstrožnosti i odgovora je Sara mogla poduzeti kako bi osigurala sebe i svoje informacije?

- Saznati malo više o tome kako snage sigurnosti djeluju u zemlji, postoje li skupine koje pokušavaju zastrašiti novinare koji nisu povezani sa snagama sigurnosti
- Pripremiti se s odvjetnicima i urednicima na to kako najbolje reagirati na racije u kući
- Ne držati osjetljive informacije kod kuće ako postoji mogućnost kućnih racija