Przewodnik dla facylitatorów szkoleń z użyciem ćwiczeń scenariuszowych (TTX) z zakresu cyberbezpieczeństwa

Cel i wprowadzenie

Niniejszy przewodnik ma towarzyszyć zestawowi 11 scenariuszy TTX (tabletop exercise), skupiających się na zagadnieniu bezpieczeństwa cyfrowego, które mogą być wykorzystane do ulepszenia szkoleń z zakresu cyberbezpieczeństwa. Z tego przewodnika może korzystać każdy, kto chce zaplanować i przeprowadzić szkolenie z bezpieczeństwa cyfrowego z użyciem ćwiczeń scenariuszowych (TTX). W tym przewodniku znajdziesz krótkie wyjaśnienie, czym jest TTX, dlaczego TTX może być cennym uzupełnieniem szkoleń z zakresu bezpieczeństwa cyfrowego oraz jak można opracować, zaplanować i ułatwić prowadzenie szkoleń z użyciem ćwiczeń scenariuszowych.

11 scenariuszy, które towarzyszą temu przewodnikowi, zostało opracowanych wspólnie z dziennikarzami z Europy Środkowej i Południowo-Wschodniej w ramach projektu Internews Journalist Security Fellowship (JSF). Scenariusze zostały również wykorzystane w szkoleniach prowadzonych przez stypendystów JSF w tym regionie. Zawarte tu przykładowe ćwiczenia scenariuszowe, w tym niektóre przetłumaczone na języki używane w Europie Środkowej i Południowo-Wschodniej oraz na arabski i hiszpański, są dostępne pod tym linkiem.

Niniejszy przewodnik został opracowany z myślą o bezpieczeństwie cyfrowym dziennikarzy i redakcji, ale może być również przydatny do planowania szkoleń z użyciem TTX dla innych grup docelowych.

Czym w ogóle jest TTX? Dlaczego warto z niego skorzystać?

Ćwiczenia scenariuszowe metodą TTX to szkolenia oparte na scenariuszach, które często przybierają formę interaktywnej dyskusji. TTX zapewnia uczestnikom szkolenia możliwość zastosowania nowo nabytej wiedzy i umiejętności poprzez zaangażowanie się w fikcyjną sytuację (zwaną scenariuszem lub sceną TTX), która mogłaby się wydarzyć w rzeczywistości. Scenariusze TTX mogą dotyczyć szerokiego zakresu sytuacji związanych z bezpieczeństwem, takich jak nalot na biuro, wyciek danych, doxxing lub prowadzenie dziennikarskiego śledztwa. Podczas gdy bardziej tradycyjne metody szkoleniowe zazwyczaj koncentrują się na przekazywaniu pewnych umiejętności technicznych i wiedzy, TTX może pomóc w:

- Zapewnieniu uczestnikom szkolenia bezpiecznej przestrzeni, w której mogą ćwiczyć przygotowanie i reagowanie na niebezpieczne sytuacje, w których mogą się znaleźć.
- Pobudzaniu dyskusji na temat kwestii bezpieczeństwa cyfrowego i tego, jakie mogą być

najlepsze rozwiązania w danej sytuacji i kontekście. Może to być szczególnie pomocne dla uczestników szkolenia, którzy regularnie ze sobą współpracują, aby przeanalizować ich wspólne - lub na poziomie całej organizacji - podejście do bezpieczeństwa. Ocenie, w jakim stopniu dana osoba lub organizacja jest przygotowana do radzenia sobie z napotykanymi sytuacjami dotyczącymi bezpieczeństwa.

Celem TTX jest zidentyfikowanie braków w wiedzy, mocnych stron i ograniczeń indywidualnych osób, organizacji i społeczności. Udany TTX wykracza poza narzędzia i podstawowe praktyki, wypunktowując również procedury lub polityki, których może brakować lub które należy ulepszyć.

Ćwiczenia scenariuszowe są najbardziej skuteczne, gdy stosujemy je jako uzupełnienie innych metod szkoleniowych. Wynika to z faktu, że celem TTX nie jest tylko przekazywanie nowych umiejętności i wiedzy, ale ich dalsze wpajanie i utrwalanie poprzez praktykę opartą na scenariuszach, dyskusję i diagnozę.

Elementy scenariuszy TTX

Każdy z jedenastu scenariuszy TTX oparty jest na bohaterce Sarze, którą przedstawiamy w niniejszym przewodniku. Każdy scenariusz dodatkowo zawiera następujące elementy:

- Cel - nadrzędny cel scenariusza TTX
- Cele edukacyjne - propozycje ogólnych celów edukacyjnych, na których należy się skupić podczas ćwiczenia scenariuszowego. Facylitatorzy powinni skupić się tylko na kilku wybranych celach edukacyjnych.
- Umiejętności/praktyki do ćwiczenia przed lub po TTX - propozycje konkretnych i sprecyzowanych umiejętności i nabytych praktyk, które mają zostać zaszczepione w uczestnikach za pomocą ćwiczenia scenariuszowego. Facylitatorzy powinni skupić się tylko na kilku wybranych umiejętnościach i praktykach, które powinny iść w parze z wybranymi celami edukacyjnymi i celem nadrzędnym.
- Scenariusz - właściwy scenariusz TTX. Zawiera następujące elementy:
    - Wprowadzenie i kontekst do zaprezentowania na samym początku
    - Dodatkowe elementy tła wprowadzane przez całość scenariusza
    - Pytania i podpowiedzi dla uczestników. Są one oznaczone literą Q, po której następuje numer (np. Q1, Q2, Q3 itd.).
    - Pod pytaniami i podpowiedziami znajdują się możliwe odpowiedzi. Nie należy ich udostępniać uczestnikom podczas ćwiczeń scenariuszowych. Mają one pomóc facylitatorowi.
    - Niektóre scenariusze zawierają “wrzutki”. “Wrzutka” to nowa informacja lub nowe wydarzenie wprowadzone przez facylitatora do scenariusza TTX w określonych momentach, by popchnąć historię do przodu lub dodać mu kolejną warstwę. “Wrzutki” mogą zmienić narrację scenariusza TTX i wymagać działania lub reakcji ze strony uczestników szkolenia.
    - Załączniki - Niektóre scenariusze (np. scenariusz nr 3.: Nękanie i Doxxing) zawierają załączniki, często używane jako “wrzutki” do scenariusza.

Opracowanie scenariusza TTX

Jedenaście scenariuszy TTX powstało w ramach projektu JSF (tutaj link). Każdy może je modyfikować, by jak najlepiej odpowiadały na potrzeby szkoleniowe własnej społeczności. Każdy może również stworzyć swój własny scenariusz od podstaw. Jeśli zamierzasz przerobić jeden ze scenariuszy TTX lub napisać własny, rozważ poniższe rady.

Cele edukacyjne powinny być ustalone we wstępnej fazie tworzenia scenariusza, uzupełniać się wzajemnie, być zgodne z logiczną kolejnością uczenia się, uszeregowane według ważności i łączyć się z ogólnym celem TTX. Aby uprościć proces szkolenia i ułatwić ocenę postępu, połącz cele edukacyjne z konkretnymi umiejętnościami lub praktykami, na których uczestnicy powinni się skupić podczas TTX. Najlepiej byłoby, gdybyś ustalił cele edukacyjne i pożądane umiejętności w oparciu o potrzeby i poziom wiedzy uczestników szkolenia. Być może je już znasz, jeśli pracujesz z daną społecznością. W innym razie może być konieczne przeprowadzenie wstępnej oceny potrzeb (np. poprzez wywiady z kluczowymi informatorami lub wstępną ankietę) w celu zebrania tych informacji.

Scenariusz powinien być na tyle realistyczny na ile to możliwe, ale ogólnie nie należy korzystać z nazwisk prawdziwych osób czy nazw organizacji. Skup się na rzeczywistych sytuacjach, wyzwaniach i oczekiwaniach. W rzadkich przypadkach właściwym może okazać się użycie prawdziwych lokalizacji, ale wtedy powinieneś rozważyć możliwe zagrożenia i potencjalne ograniczenia związane z tą decyzją. Wylistowanie prawdziwych lokalizacji może na przykład sprawić, że uczestnicy będą bardziej skupieni na zapamiętaniu czy wyszukiwaniu informacji na temat tych miejsc zamiast na samym scenariuszu.

Jeśli chodzi o złożoność scenariusza, to nie powinien on przyćmić czy rozpraszać uczestników i pozwolić im skupić się na samej nauce. Możliwości wyboru mogą pomóc uczestnikom szkolenia zrozumieć wpływ ich decyzji, jednak pamiętaj, że dodawanie kolejnych elementów scenariusza może utrudnić przeprowadzenie ćwiczenia i sprawi, że będzie trwało znacznie dłużej.

Możesz również wykorzystać czas jako element scenariusza, przypisując daty i godziny do wydarzeń mających miejsce w scenariuszu, zadając pytania związane z konkretnym okresem lub wykorzystując retrospekcje. W każdym przypadku powinieneś mieć jasność co do tego, po co korzystasz z ram czasowych - zarówno na początku jak i przez całość trwania ćwiczenia.

W zależności od poziomu umiejętności facylitatora i uczestników, można rozważyć włączenie elementów technicznych do ćwiczenia scenariuszowego. Może to oznaczać, że uczestnicy będą musieli użyć określonego narzędzia, oprogramowania lub wykonać konkretne działanie, by przejść przez scenariusz. Jeśli zdecydujesz się na dodanie elementów technicznych, zapewnij dodatkowy czas na wykonanie tych zadań i zawsze miej plan awaryjny na wypadek problemów technicznych lub zdecyduj, by element techniczny był opcjonalny i daj możliwość dostosowania zadań do różnych poziomów umiejętności uczestników.

Możesz także użyć “wrzutek” w swoim TTX. “Wrzutki” mogą być małe lub duże, zależne bądź niezależne od uczestników szkolenia. “Wrzutki” na ogół są stosowane w dłuższych scenariuszach, uwzględniając ramy czasowe ćwiczenia. “Wrzutki” są zapewniane przez facylitatora i kluczowy

tutaj jest czas. By z powodzeniem włączyć “wrzutki” do scenariusza, niezbędne są materiały facylitatora, zarówno przed jak i w trakcie prowadzenia TTX. Twoje “wrzutki” powinny korespondować z celami edukacyjnymi, ustalonymi wcześniej.

Planowanie ćwiczeń scenariuszowych (TTX)

Zanim zaczniesz planować TTX, poświęć chwilę na zastanowienie się nad docelową grupą odbiorców i tym, jak wpłynie to na cele edukacyjne. Czy docierasz do dziennikarzy, kierowników newsroomów, pracowników ochrony? Każdy z nich będzie posiadał bardzo różne informacje i będzie odpowiedzialny za różne decyzje. Z drugiej strony, niektóre ćwiczenia scenariuszowe są skierowane do znacznie szerszych podmiotów - na przykład całego newsroomu - by lepiej zrozumieć, w jaki sposób ludzie komunikują się ze sobą i podejmują wspólne decyzje. Możesz pracować z uczestnikami, którzy mają bardzo różne poziomy umiejętności, wiedzę i doświadczenie w zakresie bezpieczeństwa cyfrowego. Poświęć trochę czasu na zmodyfikowanie TTX, żeby jak najlepiej odpowiadał ich konkretnym potrzebom.

Gdy masz już grupę docelową, zaplanuj cele edukacyjne i zastanów się nad konkretnymi umiejętnościami lub praktykami, nad którymi będziecie pracować. Wybór poszczególnych umiejętności przed szkoleniem jest niezbędny, by pomóc ci skupić się na roli trenera i ustalić konkretne cele edukacyjne dla uczestników, a także pomoże ustalić punkt odniesienia przy ocenie skuteczności szkolenia. Lista przykładowych umiejętności znajduje się w podrozdziale każdego dokumentu TTX zatytułowanym "Umiejętności/praktyki do przećwiczenia przed lub po TTX". Kuszące może być omówienie jak największej liczby celów edukacyjnych w ramach jednego TTX, ale skuteczniejsze jest przeprowadzenie bardziej zawężonego szkolenia, które obejmie tylko wybrane cele edukacyjne. Pamiętaj, że twoi odbiorcy mają ograniczony czas i uwagę.

Ustal, ile czasu będziesz potrzebować na przeprowadzenie TTX. Podczas gdy agencje rządowe lub korporacje czasami organizują wielodniowe ćwiczenia scenariuszowe, twoi uczestnicy mogą być znacznie bardziej ograniczeni czasowo. Należy wziąć pod uwagę ich pracę, opiekę i inne zobowiązania. Zazwyczaj TTX składający się z 4-6 pytań lub “wrzutek” może zająć około 1 do 1,5 godziny. Jest to również uzależnione od wielkości grupy. Większe grupy zazwyczaj potrzebują więcej czasu na ukończenie TTX. Konieczne będzie również uwzględnienie czasu na podsumowanie i przyjrzenie się celom edukacyjnym oraz konkretnym umiejętnościom lub praktykom które uczestnicy powinni wdrożyć po zakończeniu scenariusza. Uczestnicy mogą wymagać kolejnego szkolenia lub kontynuacji ćwiczenia, żeby móc z powodzeniem posiąść i wdrożyć pożądane umiejętności i praktyki.

Weź pod uwagę przestrzeń dostępną do przeprowadzenia ćwiczenia. Jeśli TTX odbywa się na żywo, najlepiej zorganizować go w przestrzeni umożliwiającej współpracę. Pokój ze stołami i wygodnymi krzesłami jest prawdopodobnie bardziej sprzyjający dla TTX niż sala wykładowa. Konieczne może być również zapewnienie wysokiej jakości Wi-Fi lub innych udogodnień technologicznych, takich jak projektor. Jeśli to możliwe, priorytetem powinna być również dostępność przestrzeni (np. dostęp dla wózków inwalidzkich, inkluzywne łazienki, dogodne opcje transportu itp.)

Zdecyduj, czy będzie kilkoro facylitatorów i jakie będą ich role. Najbardziej sensowne może być poprowadzenie TTX przez jednego facylitatora, podczas gdy pozostali będą pomagać poszczególnym podgrupom lub w pomniejszych zadaniach. Facylitatorzy mogą również chcieć przećwiczyć wcześniej facylitację niektórych elementów ćwiczenia.

Zdecyduj, jakie materiały będą potrzebne do przeprowadzenia TTX. Możesz chcieć utworzyć slajdy, ulotki informacyjne lub innego rodzaju materiały prezentacyjne by przedstawić/wyświetlić tło wydarzeń w scenariuszu, pytania/kroki i/lub "wrzutki". Ważne jest również, by wziąć pod uwagę materiały, których uczestnicy mogą potrzebować do sporządzania notatek.

Facylitowanie ćwiczeń scenariuszowych (TTX)

Prowadzenie TTX różni się od prowadzenia tradycyjnego szkolenia z zakresu bezpieczeństwa cyfrowego lub zajęć z podnoszenia kwalifikacji. W tradycyjnych szkoleniach z zakresu bezpieczeństwa cyfrowego trenerzy zwykle dużo mówią i oczekuje się, że podzielą się swoją wiedzą z uczestnikami. W szkoleniu TTX większość wypowiedzi i pracy odbywa się jednak wśród samych uczestników, którzy omawiają scenariusz i podejmują decyzje. Facylitator TTX odgrywa rolę osoby odpowiedzialnej za proces, upewniając się, że TTX przebiega sprawnie i spełnia swoje cele. Facylitator TTX wprowadza uczestników w ćwiczenie, kontekst i tło, odpowiada na podstawowe pytania i dodaje "wrzutki". Pozostałe rekomendacje dotyczące facylitacji TTX są następujące:

- Upewnij się, że jesteś dobrze zaznajomiony z ćwiczeniami scenariuszowymi.
- Pamiętaj o celu nadrzędnym oraz celach edukacyjnych TTX i kieruj dyskusję uczestników w taki sposób, by te cele osiągnąć.
- Na początku i w trakcie trwania TTX jasno komunikuj zadania i oczekiwania wobec uczestników.
- Pilnuj godziny i upewnij się, że maksymalnie wykorzystujesz czas z uczestnikami i nie marnujesz go.
- Upewnij się, że wasza przestrzeń jest bezpieczna i zachęcająca oraz pilnuj, by każdy czuł się wysłuchany i zauważony.
- Jeśli uczestnik zwróci uwagę na cenną praktykę - podkreśl to! Może to zwiększyć pewność siebie i zachęcić do aktywnego uczestnictwa w przyszłości.
- Jeśli nie znasz odpowiedzi na zadane pytanie, nie bój się do tego przyznać i obiecaj wrócić do tej kwestii po skończeniu TTX. Korzystaj z przestrzeni społecznościowych, takich jak platforma Mattermost Team CommUNITY, by uzyskać odpowiedzi na pytania, na które możesz nie być w stanie odpowiedzieć samodzielnie.
- Jeśli to możliwe, zbieraj informacje zwrotne przez cały czas trwania projektu i bądź gotowy do wprowadzania mikro-poprawek. Jeśli planujesz zorganizować wiele sesji z użyciem TTX, możesz również zebrać informacje zwrotne na koniec danej sesji, aby lepiej zrozumieć, w jaki sposób ulepszyć je w przyszłości.
- Jeśli TTX zacznie zmierzać w innym kierunku niż pierwotnie zakładałeś, nic się nie dzieje! Bądź elastyczny, ale upewnij się, że ostatecznie osiągacie zamierzone efekty.

Jeśli chcesz uzyskać bardziej szczegółowe wskazówki, poniżej znajdują się instrukcje krok po kroku, które pomogą ci w facylitacji.

1. Przedstaw się (i innych współprowadzących), wyjaśnij swoją rolę (wasze role) i opisz ogólny cel TTX (na przykład: dzisiaj przyjrzymy się, jak newsroom może zareagować na sytuację naruszającą bezpieczeństwo). Jest to też doskonały moment na ustalenie podstawowych zasad obowiązujących w grupie.
2. Następnie, opisz bardziej szczegółowo co będzie się działo w trakcie TTX. Wyjaśnij, że TTX to symulacja fikcyjnej, ale prawdopodobnej sytuacji, która ma nam pomóc lepiej zrozumieć, jakie decyzje i działania podejmujemy - jako jednostki i jako społeczność.
3. W zależności od wielkości i składu grupy, możesz podzielić uczestników na mniejsze grupy.
4. Przedstaw uczestnikom wprowadzenie do pierwszej sceny, w tym każdą informację dodatkową, która może okazać się niezbędna.
5. W miarę jak uczestnicy przechodzą przez scenariusz, przedstawiaj kolejne fragmenty, kawałek po kawałku. Odpowiadaj na pytania i pomagaj w rozwiązywaniu problemów, jeśli uczestnicy utkną gdzieś po drodze.
6. W odpowiednim momencie przedstawiaj uczestnikom “wrzutki”.
7. Zachęcaj uczestników do angażowania się i odpowiadania na pytania. Poproś ich o robienie notatek w chwilach, gdy może okazać się to przydatne. Skorzystaj z wcześniej przygotowanych odpowiedzi, by pomóc uczestnikom w razie trudności lub jeśli będą potrzebowali przykładów, żeby zacząć.

Po ukończeniu TTX przez uczestników, zachęć ich do podzielenia się głównymi wnioskami z doświadczenia i przemyśleniami na temat TTX jako metody szkoleniowej. To świetny moment na zebranie informacji zwrotnych i rozważenie, czy warto ulepszyć przyszłe szkolenia.

Po zakończeniu TTX sprawdź, czy są jakieś materiały podsumowujące, dalsze kroki lub streszczenia, które powinny zostać udostępnione uczestnikom.

Załącznik 1.: Informacje ogólne na temat Sary (bohaterki TTX)

Stworzyliśmy jedną bohaterkę, Sarę, by na jej przykładzie przedstawić sytuacje zawarte w scenariuszach TTX. Pomogło nam to stworzyć jeden, spójny punkt dla wszystkich scen TTX oraz zaoferować dziennikarzom dobry punkt wyjścia do myślenia o możliwych zagrożeniach i szerszym kontekście. Poniżej znajdziecie nasz opis Sary, który facylitatorzy mogą wykorzystać do przygotowania danej sceny i tła wydarzeń przed rozpoczęciem jednego z naszych przykładowych scenariuszy TTX.

Sara jest 41-letnią dziennikarką. Przez kilka lat pracowała dla różnych lokalnych i międzynarodowych redakcji w swoim kraju i krajach sąsiednich.

W zeszłym roku Sara rozpoczęła współpracę z organizacją dziennikarzy śledczych o nazwie "Free Press Now" (“Wolna Prasa Teraz”) działającą w jej kraju. Organizacja często podejmuje tematy związane z polityką. Publikuje między innymi doniesienia o przypadkach łamania praw człowieka przez obecny rząd, skorumpowanych urzędnikach państwowych i polityce rządu, która utrudnia życie mniejszościom etnicznym w kraju.

Dzięki rzetelnym i wiarygodnym relacjom, Free Press Now stała się zaufanym i popularnym źródłem informacji dla lokalnej społeczności.

Po wyborach, które odbyły się 5 miesięcy temu, nowy rząd zaczął ograniczać wolność prasy, a w zeszłym tygodniu władze dokonały nalotu na domy trzech znanych dziennikarzy w stolicy. Niedawno przeprowadzono również nalot na dom Sary, choć zabrano jej jedynie kilka notesów.

Scenariusz 1: Utrata urządzenia

Autorami dokumentu są stypendyści JSF

Cel

Pomóc uczestnikom zaplanować i zareagować na sytuację, w której jedno lub więcej ich urządzeń - mogących zawierać poufne informacje - zaginie.

Cele dydaktyczne

- Identyfikacja sposobów bezpiecznej komunikacji pomiędzy dziennikarzami a ich źródłami.
- Budowanie świadomości na temat ryzyka związanego z utratą urządzenia (telefon, komputer).
- Zrozumienie dobrych praktyk w zakresie ochrony i bezpieczeństwa urządzeń.
- Dzielenie się dobrymi praktykami w zakresie wdrażania (onboarding i offboarding) pracowników organizacji, zwłaszcza w odniesieniu do bezpieczeństwa urządzeń.

Scenariusz

Nieznany wcześniej informator (dalej: źródło) kontaktuje się z Sarą przez aplikację Messenger, twierdząc, że ma poufne informacje, którymi chce się z nią podzielić. Plik, który chce udostępnić, zawiera informacje o finansach obecnego Ministra Obrony Narodowej.

Pragnąc zapewnić źródłu bezpieczeństwo, Sara chciałaby przekonać go do przesłania informacji za pośrednictwem komunikatora szyfrowanego end-to-end (od końca do końca).

P1 - Jak Sara może wyjaśnić ideę szyfrowania end-to-end i przekonać źródło, że ważne jest, by z niego korzystać?

- Nikt - nawet firma zarządzająca komunikatorem - nie będzie miał dostępu do treści wiadomości. Treść wiadomości nie będzie również przechowywana w postaci niezaszyfrowanej na serwerach tej firmy
- Organy ścigania otrzymają do niej dostępu, jeśli wystąpią o to do firmy
- Jeśli atakującemu uda się zhakować konto, które zostało użyte do wysłania wiadomości, nie będzie on również w stanie uzyskać dostępu do treści wiadomości (chyba że istniały niezaszyfrowane kopie zapasowe)

P2 - Aby zapewnić bezpieczeństwo ich komunikacji w przyszłości, jakie formy komunikacji cyfrowej powinna rozważyć Sara w przypadku tego źródła?

- Komunikatory z szyfrowaniem end-to-end (od końca i do końca) i znikającymi wiadomościami
- Szyfrowany email

Źródło docenia, że Sara stara się zapewnić bezpieczeństwo ich komunikacji, ale nadal nie jest pewne, którą metodę uznać za najlepszą. Pyta Sarę o radę dotyczącą komunikatora, takiego jak Signal, Telegram i Facebook Messenger, a także o swoją skrzynkę mailową.

P3 (do wyboru) - Z punktu widzenia bezpieczeństwa cyfrowego, jakie czynniki należy wziąć pod uwagę wybierając i korzystając z komunikatorów?

- Numery telefonów: większość szyfrowanych komunikatorów end-to-end (od końca do końca) wymaga podania numerów telefonów, a te w wielu miejscach muszą być zarejestrowane, więc rząd wie, jaka osoba kryje się za danym numerem telefonu. Oznacza to, że gdyby rząd kiedykolwiek przejrzał telefon Sary lub źródła, mógłby dowiedzieć się, że to oni wysyłali wiadomości, nawet jeśli używali pseudonimów lub znikających wiadomości (jedynym sposobem ograniczenia dostępu do tych informacji byłoby usunięcie nazwisk z listy kontaktów, komunikatorów, a najlepiej wyczyszczenie telefonu).
- Tajne konwersacje: Facebook Messenger i Telegram oferują dwa tryby rozmowy, z których tylko jeden jest szyfrowany end-to-end (od końca do końca). Ten tryb jest zwykle nazywany tajną konwersacją lub czymś podobnym, choć często jest ukryty w ustawieniach
- Znikające wiadomości:prawie każdy współczesny komunikator ma funkcję znikających wiadomości, choć w niektórych jest ona dostępna tylko w trybie tajnej konwersacji
- Usunięcie konwersacji: jest to dość oczywiste, ale ważne, by pamiętać, że niektóre komunikatory tylko archiwizują, a nie usuwają konwersacji
- Świadomość dotycząca zrzutów ekranu: każda podejrzana osoba uczestnicząca w rozmowie może po prostu zrobić zrzut ekranu lub - jeśli funkcje komunikatora na to nie pozwalają - zwyczajnie sfotografować ekran swojego telefonu.
- Uwierzytelnianie dwuskładnikowe (2FA): atakujący może przejąć konto w komunikatorze poprzez przejęcie numeru telefonu, który został użyty do rejestracji konta i ponowne wysłanie na niego SMS-a weryfikacyjnego. Pozwala to na podszycie się pod właściciela konta, choć zazwyczaj nie daje dostępu do historii wiadomości. Większość komunikatorów ma obecnie opcję wymagania dodatkowego hasła oprócz kodu SMS: oznacza to, że nawet jeśli atakującemu udało się przejąć numer telefonu, nie będzie mógł on łatwo uzyskać dostępu do konta
- Silne hasła lub frazy używane do logowania się do samego urządzenia (telefonu)

P4 (do wyboru) - Z punktu widzenia bezpieczeństwa cyfrowego, jakie czynniki należy wziąć pod uwagę podczas komunikacji mejlowej?

- Źródło powinno utworzyć nowy adres email tylko do komunikacji z Sarą
- Nowa poczta e-mail powinna mieć silne i unikalne hasło oraz solidne uwierzytelnianie dwuskładnikowe

- Źródło powinno również zwracać uwagę na ataki phishingowe i korzystać z technologii, które mogą pomóc w ich uniknięciu, takich jak fizyczne klucze bezpieczeństwa lub automatyczne wypełnianie menedżera haseł
- Najlepiej byłoby, gdyby źródło i Sara komunikowały się za pośrednictwem PGP, na przykład za pomocą Mailvelope. Oznacza to, że nawet gdyby ich konta zostały w jakiś sposób naruszone, atakujący nadal nie byłby w stanie odczytać treści ich wiadomości bez klucza PGP

Źródło bezpiecznie wysyła plik do Sary, a ta wyświetla go na swoim telefonie komórkowym. Sara jest zadowolona z treści przekazanej informacji i wychodzi z przyjaciółmi świętować. Podczas imprezy gubi telefon i uświadamia sobie, że zabezpieczyła go bardzo prostym hasłem (1111).

P5 - Co może się stać z telefonem Sary i znajdującymi się w nim informacjami?

- Każdy, kto znajdzie ten telefon, może uzyskać dostęp do poufnych informacji, jeśli dowie się, gdzie się one znajdują
- Każdy, kto znajdzie ten telefon może napisać do kontaktów Sary i się pod nią podszywać
- Każdy, kto przegląda informacje w jej telefonie, może zagrozić tożsamości i bezpieczeństwu kontaktów Sary lub zebrać informacje, które mogą zostać wykorzystane do inżynierii społecznej
- Sara może całkowicie stracić wiarygodność jako dziennikarka

P6 - Co może teraz zrobić Sara, aby ograniczyć wpływ na swoje bezpieczeństwo cyfrowe?

- Może zdalnie wyczyścić swój telefon, jeśli skonfigurowała taką funkcję
- Może zalogować się do swoich kont e-mail i mediów społecznościowych na innych urządzeniach, zmienić hasło i, jeśli to możliwe, kliknąć link "wyloguj się ze wszystkich zalogowanych urządzeń"

P7 - Jakie są plusy i minusy, w przypadku kiedy Sara poinformuje źródło, że zgubiła telefon?

- Dyskusja, bez nacisku na konkretne poprawne odpowiedzi

Dobra wiadomość! Przyjaciel Sary, który był z nią na imprezie, znalazł telefon w swoim płaszczu. Zadzwonił do niej i zwrócił telefon Sarze następnego dnia.

P8 - Sara ma z powrotem swój telefon! Jakie może teraz podjąć kroki w kwestii cyfrowego zabezpieczenia urządzenia na wypadek, gdyby w przyszłości znów je zgubiła?

- Czasami warto rozważyć użycie odblokowania biometrycznego. Ma to swoje zalety (nikt nie może zaglądać Sarze przez ramię, gdy wprowadza swoje hasło, a także nie zostanie to zarejestrowane przez kamery CCTV) i wady (łatwiej jest zmusić Sarę do odblokowania urządzenia)
- Używaj dłuższych haseł lub fraz odblokowujących telefon. Unikaj odblokowywania wzorem (takich jak łączenie kropek), ponieważ mogą one zostać łatwo zidentyfikowane przez podglądającą osobę, kamerę lub poprzez smugi na ekranie

- Blokowanie aplikacji (takich jak komunikatory) dodatkowym hasłem, jeśli Sara obawia się, że jej telefon może być czasem udostępniany/przekazywany dalej
- Używanie aplikacji, które mogą śledzić, lokalizować i zdalnie czyścić urządzenia.

P9 - Jak z perspektywy organizacji wygląda właściwy proces wdrażania nowych pracowników w celu zabezpieczenia ich urządzeń (telefony komórkowe, komputery)?

- Dopilnowanie, aby wszyscy pracownicy, niezależnie od stanowiska, przeszli przez proces wdrożenia i rozumieli jego znaczenie
- Organizacje powinny jasno określić oczekiwania wobec pracowników w zakresie praktyk bezpieczeństwa cyfrowego organizacji
- Określenie kroków, które należy podjąć w przypadku, gdy bezpieczeństwo może zostać naruszone (np. skradziony telefon lub złamane hasło)
- Wsparcie IT powinno być udzielane wszystkim pracownikom, którzy go potrzebują

Scenariusz 2: Bezpieczeństwo operacyjne

Autorami dokumentu są stypendyści JSF

Cel

Wzmocnienie świadomości bezpieczeństwa cyfrowego i dobrych praktyk w redakcji, wśród os. współpracujących i/lub freelancerów.

Zakres zagadnień

- Teoria: Zrozumienie koncepcji bezpieczeństwa cyfrowego jako ciągłego procesu, a nie celu końcowego.
- Komunikacja, przekazywanie wiedzy i uwrażliwianie innych ludzi w zakresie tego, jak ważne jest bezpieczeństwo cyfrowe
- Praktyczne omówienie bezpiecznego komunikowania się za pomocą urządzeń mobilnych.
- Budowanie dobrych praktyk bezpiecznej wymiany plików
- Świadomość w kwestii konfiguracji komputerów podłączonych do sieci
- Zrozumienie zagadnienia modelowania zagrożeń (threat modelling)

Umiejętności i dobre praktyki do przećwiczenia przed lub po warsztacie TTX

- Wprowadzenie i stosowanie w codziennej pracy kontroli uprawnień dostępów do danych w chmurze (np. Google Drive)
- Przeglądanie historii logowania do wspólnych folderów w chmurze, np. Google Drive (jeśli to możliwe – czasami taka opcja dostępna jest tylko w modułach płatnych)
- Konfiguracja i używanie logowania dwuskładnikowego 2FA, najlepiej przy użyciu fizycznego klucza bezpieczeństwa lub innego rozwiązania skutecznie chroniącego przed phishingiem
- Dobre praktyki w zakresie tworzenia haseł (unikalne hasła; długie hasła; użycie tekstów szyfrujących; menadżer haseł)
- Szyfrowanie dokumentów (np. przy użyciu Mailvelope)
- Instalacja i konfiguracja aplikacji Signal (lub innej bezpiecznej aplikacji do wysyłania wiadomości)
- Używanie zaawansowanych opcji dostępnych w takiej apce (np. znikające wiadomości)
- Instalacja, konfiguracja i używanie Mailvelope (lub innego rozwiązania do szyfrowania wiadomości e-mail)
- Bezpieczna praca z plikami pochodzącymi z wrażliwych źródeł

Scenariusz

Sara zbiera zespół dziennikarski w celu prześwietlenia korupcji w Ministerstwie Zdrowia dot. zamówień publicznych podczas pandemii Covid-19.

Członkowie zespołu mają różny poziom umiejętności, wiedzy i poziom doświadczenia w zakresie bezpieczeństwa cyfrowego.

Sara wie, że jeden z członków jej zespołu bardzo słabo radzi sobie z ochroną plików.

P1 - Jak Sara może zachęcić kolegów i koleżanki do zadbania o bezpieczeństwo cyfrowe? Na co powinna zwrócić uwagę podczas organizowania pracy zespołu, by zapewnić bezpieczeństwo cyfrowe?

- Wytłumaczcie, dlaczego bezpieczeństwo cyfrowe jest ważne: można to zrobić dając przykłady na to, jak zaniedbania w bezpieczeństwie cyfrowym mogą zagrozić dziennikarce/dziennikarzowi i ich reputacji, jak bezpieczeństwo cyfrowe pozytywnie wpływa na zaufanie pomiędzy współpracownikami oraz na komfort w kontakcie z informatorami czy tłumacząc, jak istotna jest ochrona osób w naszym otoczeniu.
- Przedyskutujcie, jakich urządzeń używają, jak chronią swoje konta użytkownicy, jak przechowują i wymieniają pliki, jak uzyskują dostęp do sieci (czy używają własnych urządzeń czy może pracują na komputerach firmowych), jak logują się do sieci w pracy (bezprzewodowo czy przez kabel), czy używają dwuskładnikowego uwierzytelniania do zabezpieczenia kont użytkowników i jaka jest ich dyscyplina w zakresie haseł (czy wielokrotnie używają tych samych haseł, czy korzystają z menedżerów haseł)
- Zdecydujcie, w jaki sposób zespół powinien się komunikować, przechowywać pliki i uzyskiwać do nich dostęp. Jak można się upewnić, że wszyscy stosują taką samą procedurę?
- Rozważcie szkolenie zespołu z wykorzystaniem nowo ustalonych procedur. Po ustaleniu zasad, zespół powinien przeprowadzić próbę na sucho, testując nowe sposoby komunikacji i sprawdzając, czy w procesie nie wyłaniają się żadne problemy do zaadresowania.

P2 - Jak Sara i jej zespół przechowują i udostępniają pliki audio i dokumenty pozyskane od informatorów?

- Ograniczać dostęp do niektórych plików i folderów, używaj świadomie i ostrożnie opcji udostępniania np. w Google Drive
- Odradzić współpracownikom kopiowania wrażliwych plików na prywatne nośniki danych (pendrive, załącznik mejlowy) z uwagi na zwiększone ryzyko ataku hakerskiego lub wycieku.
- Doradzić współpracownikom, żeby używali służbowych komputerów jedynie w celu pracy nad służbowymi plikami i materiałami.
- Ograniczyć możliwość instalacji zewnętrznego oprogramowania na służbowych komputerach, regularnie sprawdzaj, czy są one wyposażone w odpowiednio mocne hasła i najnowsze aktualizacje systemowe.

P3 - W jaki sposób można zapewnić bezpieczeństwo komunikacji Sary i jej zespołu?

Upewniając się, że wszyscy korzystają z tych samych narzędzi i procedur, a także, że wszystkim one odpowiadają, Sara chce pomóc swojemu zespołowi w wybraniu bezpiecznego sposobu wewnętrznej komunikacji.

Rozważcie kwestie:

- Przeniesienie większości konwersacji do bezpiecznej apki, jak Signal, z włączonymi znikającymi wiadomościami, równocześnie archiwizując w innym miejscu informacje, które są niezbędne do dalszej pracy
- Używanie w komunikacji mejlowej szyfrowania kluczem PGP
- Stworzenie jasnych i dobrych zasad ochrony kont mejlowych (unikalne hasła, uwierzytelnianie dwuskładnikowe 2FA)

Dwa tygodnie przed publikacją tekstu Sara otrzymuje telefon od głównego informatora/ki ze strony rządowej w tym śledztwie. Sara dobrze zna tego informatora i ufa mu. W rozmowie telefonicznej informator mówi krótko: "Rząd wie - był przeciek" i rozłącza się.

P4 - Z punktu widzenia bezpieczeństwa cyfrowego, jakie pierwsze kroki powinna podjąć Sara w odpowiedzi na możliwy wyciek informacji?

- Poprosić wszystkich członków zespołu o zmianę haseł, na wypadek, gdyby haker zdobył hasło do jednego z ich kont.
- Rozważyć możliwość, że służby niekoniecznie dostały się fizycznie do newsroomu; możliwe, że o wycieku dowiedzieli się np. analizując konkretne wydruki dokonywane przez ich własnych pracowników
- Przeprowadzić małe śledztwo w redakcji; kto miał dostęp do pliku, z którego pochodziły informacje? Jaki konkretnie plik wyciekł? Przy użyciu kontroli dostępu i historii zmian w dość prosty sposób można prześledzić, kto po kolei korzystał z pliku z informacjami.
- Rozważyć przyspieszenie publikacji materiału.

Sara dowiaduje się, że wyciek nastąpił wewnątrz jej firmy. Osobą, która miała dostęp do wspólnego Dysku Google organizacji był redakcyjny grafik. Sara doszła do tego wniosku po sprawdzeniu zakresu dostępów do danych w redakcyjnej chmurze. Odkryła, że team graficzny miał, z racji specyfiki swojej pracy, dostęp do całości materiałów redakcji. Grafik, zamiast koledze z teamu, przypadkowo udostępnił plik jednemu ze swoich klientów, pracującemu dla rządu. Pomyłka wynikała z faktu, że mieli oni takie samo nazwisko.

P5 - Co Sara mogłaby zrobić inaczej w przeszłości, by zapobiec tej sytuacji?

- Sara powinna od początku traktować swoją firmę jako potencjalne źródło niebezpieczeństwa i wprowadzić bezpieczne procedury, które dotyczą tylko jej zespołu śledczego. Powinna upewnić się, czy w firmie istnieje jasny system przyznawania uprawnień dostępów i czy jest on przestrzegany w praktyce.

- Zespół powinien współpracować z grafikami w taki sposób, aby otrzymywali oni wyłącznie niezbędne informacje: nie należy podawać im żadnych poufnych lub wrażliwych informacji, chyba że jest to absolutnie konieczne w celach publikacji.
- Ponadto, Sara powinna traktować dbałość o bezpieczeństwo i prywatność jako proces, a nie jako stan; jest to coś, co powinno być stale udoskonalane.

Scenariusz 3: Uporczywe nękanie i doxxing

Autorami dokumentu są stypendyści JSF

Cel

Pomoc uczestnikom w zrozumieniu, jak najlepiej przygotować się i zareagować na doxxing i nękanie online.

Zakres zagadnień

- Zidentyfikowanie metod i środków łagodzenia konsekwencji doxxingu i nękania w mediach społecznościowych dla dziennikarzy i dziennikarek, których one spotykają.
- Zrozumienie, jak informacje z mediów społecznościowych mogą być zbierane i wykorzystywane przeciwko dziennikarzom i pracownikom redakcji.
- Zbadanie zależności między płcią a nękaniem oraz ich implikacji dla bezpieczeństwa.
- Dyskusja o redakcyjnych procedurach i praktykach mających na celu ochronę pracowników i współpracowników, którzy padli ofiarą nękania i doxxingu.
- Rozważenie planu działania w wypadku doxxingu i nękania, wspierającego dziennikarzy i dziennikarki, którzy nie mają wsparcia newsroomu (np. freelancerzy).
- Storytelling na temat cyberbezpieczeństwa, uwrażliwianie ludzi na to, jak można rozmawiać z osobami, które na co dzień nie spotykają się z nękaniem: uświadamianie, że jest to poważny problem, który wymaga skoordynowanych działań całego zespołu i indywidualnego wsparcia.
- Bezpieczeństwo firmy: ustalanie w organizacjach zasad i sposobów, w jakich mogą one najlepiej wspierać dziennikarzy, którzy są narażeni na cyberataki nękania.[1]

Umiejętności i dobre praktyki do przećwiczenia przed lub po warsztacie TTX

- Zarządzanie ustawieniami prywatności na głównych platformach mediów społecznościowych oraz aktualizowanie ich.
- Korzystanie z narzędzi na głównych platformach mediów społecznościowych, takich jak raportowanie i blokowanie użytkowników. Obejmuje to zarówno korzystanie z takich rozwiązań, jak i zrozumienie, jak dokładnie działają
- Konfiguracja i używanie logowania dwuskładnikowego 2FA, najlepiej przy użyciu fizycznego klucza bezpieczeństwa lub innego rozwiązania skutecznie chroniącego przed phishingiem

[1] W większości szkoleń byłby to cel kształcenia. Jeśli prowadzisz sesję z menedżerami mediów lub innymi decydentami i możliwe jest zmierzenie wyników na poziomie organizacji, możesz również wykorzystać to w ten sposób.

Scenariusz

Sara pracuje nad nowym materiałem o mniejszościach etnicznych w swoim kraju i tym, jak polityka rządu prowadzi do coraz większej marginalizacji tych grup. Sara w ciągu ostatnich tygodni na swoich kontach w mediach społecznościowych, gdzie również dzieli się swoją pracą, zauważyła większą ilość komentarzy. Zaczyna również otrzymywać nienawistne i obraźliwe wiadomości od internetowych trolli.

P1 - Jakie kroki może podjąć Sara, aby zablokować i zaraportować działania osób zamieszczających te komentarze?

- Może skorzystać z wbudowanych funkcji blokowania i zgłaszania dostępnych na większości platform mediów społecznościowych.
- Może skontaktować się z firmami odpowiadającymi za dane medium społecznościowe (bezpośrednio lub za pośrednictwem swojej redakcji), aby zgłosić nękanie odbywające się na dużą skalę.
- Wyłączyć dodawanie postów i odpowiedzi na jej profilu
- Być bardziej ostrożną ustawiając zakres, w którym można ją znaleźć w mediach społecznościowych.
- Zrezygnować z możliwości bycia tagowaną w mediach społecznościowych
- Działania w kierunku blokowania i zgłaszania podżegaczy zirytowało tylko grupę trolli. Skala nienawistnych treści skierowanych przeciw Sarze rozrosła się się. Niektóre komentarze zawierają również groźby.

P2 - Jak Sara może zbadać, czy przemoc jest częścią większej, skoordynowanej kampanii czy oddolnym działaniem?

- Może zbadać sytuację samodzielnie, ale też poprosić kolegów i koleżanki z redakcji o wsparcie w śledztwie.
- Może sprawdzić, czy wszystkie trolle używają dokładnie tego samego języka, słów kluczowych lub hashtagów. Jeśli tak, to prawdopodobnie jest to skoordynowana kampania
- Zależy od platformy: na Instagramie istnieje wiele opcji dostępu do informacji o konkretnych kontach - kiedy zostały utworzone, ile osób z nich korzysta, jak często zmieniały nazwę itp.
- Sprawdzić, czy przekaz jest wzmacniany przez jakiekolwiek media
- Przeanalizować najbardziej typowe pory dnia, w których dodawane są takie posty

Sara mówi swoim kolegom o postach, ale większość męskich członków zespołu, w tym jej redaktor, mówi jej, by się przesadnie nie martwiła i że problem sam zniknie. Sara jest zestresowana – czuje, że zespół jej nie słucha i nie rozumie jej problemu.

P3 - Zamiast mówić Sarze, żeby się nie martwiła, jak jej zespół i organizacja mogą ją wesprzeć – zwłaszcza w aspekcie jej obecności w sieci i bezpieczeństwa cyfrowego?

- Pomóc w przeprowadzeniu pełnej oceny sytuacji
- Wspólnie z Sarą przeanalizować praktyki dotyczące bezpieczeństwa cyfrowego i stosowane środki bezpieczeństwa oraz w razie potrzeby pomóc w poprawie sytuacji.
- Skonsultować praktyki i podobne doświadczenia innych osób w organizacji
- Pozwolić zaufanym osobom zarządzać Twoim kontem lub przeglądać je, aby nie była bezpośrednio narażona na groźby, ale nadal mógł być w nich obecna.
- Organizacja może pomóc w poszukiwaniu konkretnych schematów nękania
- Śledzić, w jaki sposób nękanie odbywa się za pośrednictwem postów organizacji, a nie tylko w wypadku Sary.
- Przekazać sprawę zespołowi ds. bezpieczeństwa i pomóc w dochodzeniu.

Pewnego dnia osobiste zdjęcia Sary wyciekają do sieci za sprawą jednego z trolli. Zdjęcia, które przed laty zamieściła w mediach społecznościowych, są osobiste i w niektórych przypadkach zawierają pewne wrażliwe informacje.

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 - W jaki sposób ktoś mógł uzyskać dostęp do informacji o Sarze, takich jak stare posty w mediach społecznościowych?

- Znajomi Sary opublikowali zdjęcia ze słabymi ustawieniami prywatności
- Ktoś włamał się na konto Sary
- Znajomy Sary z mediów społecznościowych mógł zapisać zdjęcia, aby udostępnić je później
- Zdjęcia Sary w mediach społecznościowych mogły zostać zindeksowane przez wyszukiwarkę

P5 - Jakie kroki może podjąć Sara, aby spróbować zapobiec wyciekowi dalszych informacji o niej w sieci?

- Usunąć stare zdjęcia
- Usunąć konta
- Zablokować konta
- Wrzucić nowe zdjęcia, które jednak zawierają niewiele informacji na jej temat
- Uzyskać raport od firmy prowadzącej dane medium społecznościowe, który podsumuje wszystkie dane, jakie o niej posiadają
- Zgłaszać zdjęcia, które zostały ostatnio opublikowane / zgłaszać konta, które je publikują.
- Kontynuować publikowanie treści związanych z pracą, nawet jeśli publikuje mniej osobiste treści. Jeśli znikniesz z internetu, trolle wygrają
- Robić zrzuty ekranu postów i dokumentować je tak dokładnie, jak to możliwe. Zapisywać aliasy online trolli

P6 - Jakie kroki mogła podjąć Sara i jej organizacja, aby zapobiec gromadzeniu i rozpowszechnianiu w internecie tych informacji, szczególnie w zakresie bezpieczeństwa cyfrowego?

- utworzyć grupę bliskich przyjaciół, którzy jako jedyni widzą osobiste zdjęcia i osobiste posty w mediach społecznościowych
- w ogóle nie publikować poufnych, prywatnych materiałów (takich jak zdjęcie z jointem)
- nie publikować zdjęć, które ujawniają prywatne informacje, takie jak lokalizacja
- otwierać konta służbowe, aby jej obecność w Internecie nie była związana z jej życiem osobistym
- silne hasła i zastosowanie 2FA dla kont w mediach społecznościowych

Aneks 1: INJECT - Przedstaw przykłady zdjęć

Scenariusz 4: Przeszukanie newsroomu

Autorami dokumentu są stypendyści JSF

Cel

Praktyczne i teoretyczne przygotowanie uczestniczek/ów na wypadek sytuacji przeszukania przez służby w ich redakcji

Cele dydaktyczne

- Pewność, że istnieją awaryjne plany komunikacji i przygotowanie techniczne na wypadek, gdyby dostęp do redakcyjnych lub osobistych urządzeń nie był już możliwy
- Dobre praktyki zabezpieczania cyfrowych urządzeń w redakcji lub organizacji
- Identyfikacja sposobów zabezpieczenia plików na urządzeniu cyfrowym (komputer, telefon komórkowy itp.).
- Plan na wypadek przejęcia informacji przez służby podczas przeszukania
- Rozważania nad modelowaniem zagrożeń i planowaniem na przyszłość wobec osób i organizacji

Umiejętności/zachowania do przećwiczenia przed i po TTX

- Używanie narzędzi do szyfrowania danych na dyskach twardych i zewnętrznych, np. VeraCrypt
- Modelowanie zagrożeń, w szczególności pod kątem zachowania wobec służb i przeszukania redakcji: jak ocenić ryzyko, przygotować się na nie i odprawić zespół po jego wystąpieniu
- Bezpieczeństwo organizacji i społeczności, w szczególności jak pracować z redaktorami, kierownictwem i prawnikami w napiętych sytuacjach oraz określić, jakie pytania kierować do kogo
- Określanie, z których plików korzystano ostatnio i kiedy to było – za pomocą ustawień Microsoft Office i Dysku Google
- (Zaawansowane) Jeśli organizacja dysponuje szczegółowym rejestrem dostępu (logami) za sprawą subskrypcji premium Dysku Google lub O365 – dostęp logów i praca z nimi
- Przeglądanie historii wyszukiwania i dostępu do plików w najpopularniejszych przeglądarkach internetowych i systemach operacyjnych

Scenariusz

Sara pracuje w newsowej redakcji liczącej ok. 20 osób. W poniedziałkowy poranek 15 osób na różnych stanowiskach pracuje w newsroomie, a jeszcze pięcioro pracuje zdalnie.

O 10 rano do redakcji przybywa około 50 funkcjonariuszy policji. Mają nakaz sądowy, który pokazują redaktorom, a następnie siłą wdzierają się do środka, jednocześnie żądając, aby wszyscy dziennikarze i pracownicy natychmiast opuścili redakcję.

Sara i jej koledzy spotykają się na zewnątrz i omawiają, jak zapewnić dalsze funkcjonowanie redakcji z zachowaniem bezpieczeństwa

P1 - Jakie są priorytety w takiej sytuacji?

- Konsultacja z prawnikiem, aby ustalić dalsze kroki
- Kontakt ze współpracownikami pracującymi zdalnie
- Ustalenie, kto ma przy sobie telefon komórkowy, a które z nich zostały w redakcji

P2 - W jaki sposób Sara i osoby, z którymi pracuje, mogą bezpiecznie komunikować się w tym czasie?

- Czat grupowy na WhatsAppie lub Signalu
- Być może lepiej komunikować się za pośrednictwem numerów prywatnych, a nie służbowych? W przeciwnym razie konwersacja może być zsynchronizowana z urządzeniami, które nadal znajdują się w biurze

P3 - W jaki sposób Sara i zespół redakcyjny powinni zabezpieczyć konta internetowe organizacji, takie jak strony www i profile w mediach społecznościowych?

- Natychmiastowa zmiana haseł
- Jeśli to możliwe, zdalne wylogowanie z urządzeń, które nadal znajdują się w redakcji – wymaga konsultacji z prawnikiem/czką, aby nie zostało to uznane za zacieranie śladów przestępstwa
- Konsultacja z prawnikiem/czką przed publikacją nt. nalotu

Sara pamięta, że wychodząc z newsroomu widziała, jak policja zaczyna wkładać do toreb komputery, inne urządzenia i dokumenty. Sarze udało się wyjść z telefonem, ale jej laptop został w newsroomie. Zespół szybko ocenia: jakie informacje może uzyskać policja?

P4 - W jaki sposób powinny były być zabezpieczone urządzenia w redakcji?

- Silne hasła w komputerach
- Blokady ekranu po krótkim czasie braku aktywności
- Zaszyfrowane pendrive'y i dyski zewnętrzne

W rozmowie na zewnątrz jedna z osób na stanowisku redaktora przyznaje, że zostawiła w redakcji odblokowany komputer

Policja opuszcza redakcję dwie godziny później, umożliwiając dziennikarzom powrót. Zespół spotyka się, aby omówić, do jakich informacji mogła uzyskać dostęp policja, a także porozmawiać o podobnych zagrożeniach w przyszłości.

P5 - Co może zrobić redakcja, aby natychmiast określić skutki nalotu?

- Określenie, jakie dokumenty, jeśli w ogóle, zostały zabrane lub przestawione (w tym drugim przypadku policja mogła je sfotografować).
- Komputery zwykle mają historię wyszukiwania / dostępu do plików / przeglądarki – warto ją przejrzeć. Możesz zobaczyć ostatnie pliki w Microsoft Word oraz część historii w przeglądarce, jeśli korzystasz z Dokumentów Google. Jeżeli historia plików została wyczyszczona, oznacza to, że ktoś mógł próbować wymazać ślady
- To mało prawdopodobne, by podczas nalotu zainstalowano jakiekolwiek złośliwe oprogramowanie (malware) – ale jeśli to was niepokoi, skonsultujcie się z profesjonalistą w zakresie kryminalistyki złośliwego oprogramowania

P6 - W jaki sposób organizacja może upewnić się, że następstwa tego nalotu nie doprowadzą do kolejnych zagrożeń?

- Zmiana haseł, na wszelki wypadek
- Konsultacja prawna – do czego policja miała legalny dostęp podczas przeszukania, a do czego nie?
- Jeśli redakcja używała pseudonimów wobec bohaterów czy informatorów – zmiana tychże

Kilka tygodni później redaktor/ka newsroomu wzywa zespół, aby wspólnie zastanowić się, jakie podobne zagrożenia mogą czyhać na nich w przyszłości.

P7 - W kontekście modelowania zagrożeń i bezpieczeństwa cyfrowego, jak organizacje i pojedyncze osoby mogą określać stojące przed nimi zagrożenia?

- Standardowe pytania dotyczące modelowania zagrożeń: jakie informacje posiada osoba/organizacji, kto może być zainteresowany ich uzyskaniem oraz jakie byłyby konsekwencje, gdyby adwersarzom się udało
- Określając adwersarzy, trzeba wziąć pod uwagę motywy (co chcieliby zrobić i dlaczego) oraz możliwości (co faktycznie są w stanie zrobić, jakimi środkami technicznymi, prawnymi, organizacyjnymi i finansowymi dysponują).

Scenariusz 5: Przeszukania domu dziennikarza/dziennikarki

Autorami dokumentu są stypendyści JSF

Cel

Dać osobom z mediów teoretyczne i techniczne umiejętności, by zapewnić jak najlepsze cyfrowe bezpieczeństwo ich domu

Cele dydaktyczne

- Wiedza jak zabezpieczyć urządzenia cyfrowe w domu
- Zabezpieczenie papierowych notatek
- Uruchomienie zdalnego kasowania plików – pozytywy i negatywy
- Ograniczanie dostępu do przejętych informacji
- Przygotowanie na wejście służb do domu dziennikarza/ki
- Zachęcenie uczestników/czek do przemyślenia bezpieczeństwa organizacji i społeczności. W szczególności: jak pracować z redaktorami, kierownictwem i prawnikami w napiętych sytuacjach oraz określić, jakie pytania kierować do kogo

Umiejętności/zachowania do przećwiczenia przed i po TTX

- Używanie narzędzi do szyfrowania danych na dyskach twardych i zewnętrznych, np. VeraCrypt
- Modelowanie zagrożeń, w szczególności pod kątem zachowania wobec służb i przeszukania mieszkania: jak ocenić ryzyko, przygotować się na nie i odprawić zespół po jego wystąpieniu
- Aktywowanie narzędzi, takich jak Apple Find My lub Android / Samsung Find, które mogą być używane do zdalnego blokowania lub wymazywania urządzeń
- Określanie, z których plików korzystano ostatnio i kiedy to było – za pomocą ustawień Microsoft Office i Dysku Google
- (Zaawansowane) Jeśli organizacja dysponuje szczegółowym rejestrem dostępu (logami) za sprawą subskrypcji premium Dysku Google lub O365 – dostęp logów i praca z nimi
- Przeglądanie historii wyszukiwania i dostępu do plików w najpopularniejszych przeglądarkach internetowych i systemach operacyjnych

Scenariusz

Po wyborach krajowych (pięć miesięcy temu) nowy rząd zaczął nakazywać służbom ograniczenie wolności prasy, a te dokonały przeszukań w domach trojga znanych dziennikarzy/ek w stolicy. Sara i kilkoro znajomych z pracy spotkało się, by omówić sposoby ochrony siebie i swoich informacji w podobnej sytuacji

P1 Na co powinni uważać dziennikarze, decydując się przechowywać informacje w swoim domu?

- Przechowanie w bezpiecznym miejscu
- Szyfrowanie i hasła we wszystkich urządzeniach
- Usuwanie informacji o informatorach z dokumentów
- Inwentarz, gdzie przechowywane są jakie dane (również zabezpieczony!)
- Nie tylko cyfrowe: pamiętać o fizycznych kopiach
- Możliwość nie trzymania czegokolwiek w domu
- Przestrzeganie krajowego prawa i reguł swojej organizacji
- Świadomość ram prawnych przechowywania wrażliwych danych w domu, a nie w redakcji
- Kto ma dostęp do twojego domu i urządzeń?

P2 (opcjonalne) – Jak trzymać papierowe notatki w domu?

- Rozważ zniszczenie tego, czego nie potrzebujesz
- Nie trzymaj notatek w jednym miejscu – mniej informacji łatwo dostępnych
- Ukryj notesy
- Sejf, kłódka, klucz - zabezpieczone!
- Poziom wrażliwości danych, które można trzymać w domu
- Skróty i skrótowce – mają sens tylko dla ciebie

P3 Jakie środki można podjąć, by jak najlepiej zabezpieczyć elektroniczne urządzenia (komputery, dyski, pendrive'y itd.)

- Szyfrowanie
- Zabezpieczenie hasłem
- Kopie zapasowe w innej lokalizacji
- Pod rozwagę: bezpieczne pozbycie się starszych urządzeń, szczególnie tych już nie w użyciu

Dziś Sara wyszła z domu o 9 rano, aby wypić kawę i zrobić zakupy. Kiedy wróciła godzinę później, drzwi do jej mieszkania były otwarte. Sara zastała w nim dwóch mężczyzn przeszukujących jej biurko i sypialnię. Jeden z mężczyzn czytał papierowe notesy Sary, podczas gdy drugi trzymał torbę z jej laptopem. Sara zauważyła, że na biurku brakuje pendrive'ów i zewnętrznych dysków twardych. Obaj mężczyźni mają na sobie cywilne ubrania, ale Sara zakłada, że w jakiś sposób pracują dla władz.

Wybór 1 – Sara krótko rozmawia z dwoma mężczyznami i udaje się jej bezpiecznie opuścić dom. Kieruje się do przyjaciela, który mieszka w pobliżu.

P4 (opcjonalnie) - Wiedząc, że niektóre z informacji, zwłaszcza z papierowego notatnika, zostały przechwycone, kogo Sara powinna poinformować o incydencie?

- Informacja dla redaktora/ki oraz redakcyjnego zespołu prawnego
- Przed kontaktem z informatorami, którzy mogli być wymienieni w notatniku, trzeba porozmawiać z redaktorem/ką i zespołem redakcyjnym, a także ze specjalistami ds. bezpieczeństwa (jeśli informatorzy są wymienieni tylko pod pseudonimem, ale następnego dnia się do nich zadzwoni, może to umożliwić służbom bezpieczeństwa powiązanie źródła z pseudonimem). Być może lepiej zaczekać w ich przypadku

P5 - Co może zrobić Sara, aby uniemożliwić dalszy dostęp do jej danych, gdy mężczyźni wciąż przebywają w jej mieszkaniu?

- Najważniejsze to przestrzegać prawa
- Domaganie się, by służby również przestrzegały prawa (np. pozwalały filmować, dobrać świadków itp.)
- Techniki deeskalacji
- Sprawdzenie, kim są mężczyźni i czy mają umocowanie prawne
- Określenie własnego bezpieczeństwa
- Pomoc prawna, telefon do redakcji
- Fałszywe konta i dokumenty (może wymagać przygotowania)
- Zbicie z tropu

Wybór 2 - Sara nie może opuścić mieszkania. Mężczyźni proszą, by usiadła i żądają podania haseł do komputera i pendrive'ów. Grożą, że jeśli nie poda tych informacji, zabiorą ją na posterunek policji. Sara prosi o pokazanie nakazu przeszukania, ale go nie otrzymuje

P6 - Wiedząc, że na jej komputerze znajdują się poufne informacje, w tym pozwalające na ustalenie tożsamości informatorów, jakie możliwości ma Sara w tej sytuacji?

- Ocena niebezpieczeństw i priorytetyzacja działań
- Zdalne wylogowanie i kasowanie poufnych kont
- Określenie wszystkich informacji przechowywanych w domu
- Rozważenie plusów i minusów poinformowania zespołu i zagrożonych informatorów. Być może lepiej podjąć decyzję ze wsparciem redakcji?
- Możliwości zdalnego usunięcia plików

P7 - Sara ma na swoim komputerze skonfigurowany program do zdalnego usuwania plików. Co powinna rozważyć przed usunięciem plików z komputera?

- Kwestia prawna – utrudnianie interwencji lub zacieranie śladów przestępstwa
- Potencjalne konsekwencje – jeśli to możliwie najpierw konsultacja prawna

- Jeśli Sara nie ma dowodów na to, że intruzi są z organów ścigania, ale wyglądają np. na firmę ochroniarską, to zmienia sytuację prawną i zagrożenia

P8 (opcjonalnie) - Wiedząc, że niektóre z informacji zostały przechwycone, kogo Sara powinna poinformować o incydencie? Czy kolejność, w jakiej informuje ludzi, jest ważna?

- Redaktor/ka
- Zespół bezpieczeństwa/IT redakcji
- Pod rozwagę: informatorzy
- Dla freelancerów, pod rozwagę: inni freelancerzy

Sara ostatecznie odmawia podania hasła do swoich urządzeń. Po kolejnych 10 minutach przeszukania, dwaj mężczyźni wychodzą z komputerem Sary, pendrive'ami i papierowym notatnikiem.

Sara znów ma dostęp do swojego mieszkania. Zauważa, że jeden z jej dwóch komputerów został pozostawiony wraz z jednym z pendrive'ów. Wszystkie jej papierowe notatniki zostały zabrane z mieszkania.

P9 - Co powinna teraz zrobić Sara, aby upewnić się, że jej informacje i bezpieczeństwo nie są dalej zagrożone przez mężczyzn, którzy byli w jej mieszkaniu?

- Mężczyźni mogli zainstalować złośliwe oprogramowanie na urządzeniach Sary; dobrym pomysłem może być wysłanie tych urządzeń do specjalisty ds. kryminalistyki cyfrowej
- Mieszkanie może być na podsłuchu
- Jakiego wsparcia może udzielić redakcja?
- Konsultacja w redakcji i z doradcami ds. bezpieczeństwa i prawa, czy z perspektywy bezpieczeństwa lepiej publicznie informować o nalocie, czy nie

Q10 (opcjonalnie) - Poza aspektami bezpieczeństwa cyfrowego, jakie inne środki ostrożności i reakcje mogła podjąć Sara, aby zapewnić bezpieczeństwo sobie i posiadanym informacjom?

- Dowiedz się nieco więcej o tym, jak działają państwowe służby; czy istnieją grupy, które próbują zastraszyć dziennikarzy niezwiązane z państwem?
- Przygotuj się z prawnikami i redaktorami, jak najlepiej reagować na przeszukania domu
- Nie przechowuj poufnych informacji w domu, jeśli istnieje ryzyko przeszukania