Ръководство за упражнение на маса (TTX) за обучение по цифрова безопасност

Цел и въведение

Това ръководство е предназначено да придружава набор от 11 сценария за упражнения на маса (TTX), насочени към цифровата сигурност, които могат да се използват за подобряване на обучението по цифрова сигурност. Настоящото ръководство е предназначено за използване от всеки, който желае да разработи и използва TTX като метод за обучение по цифрова безопасност. В това ръководство ще намерите кратки обяснения за това какво е TTX, защо TTX могат да бъдат ценно допълнение към обученията по цифрова безопасност и как човек може да разработи, планира и улесни TTX.

11-те сценария, включени в това ръководство, са разработени съвместно с журналисти от Централна и Югоизточна Европа в рамките на проекта на Internews Journalist Security Fellowship (JSF) и са използвани в обучения, проведени от стипендианти на JSF в региона. Тези примерни TTX, включително някои с версии, локализирани на езиците на Централна и Югоизточна Европа и преведени на арабски и испански език, са достъпни на линка тук.

Това ръководство е разработено специално с оглед на цифровата безопасност за журналисти и редакции, но може да бъде полезно за планиране на TTX и за други целеви аудитории.

Какво представлява TTX? Защо TTX са ценни?

Упражнението на маса е метод на обучение по сценарий, който често е под формата на интерактивна дискусия. TTX предоставят възможност на участниците в обучението да прилагат новопридобити знания и умения, като участват в измислена ситуация (наричана сценарий или сцена на TTX), която се доближава до реална такава. Сценариите на TTX могат да разглеждат широк спектър от ситуации в областта на сигурността, като например нахлуване в офис, изтичане на данни, случай на деанонимизиране или чувствително разследване. Докато по-традиционните методи за обучение могат да се съсредоточат върху предаването на определени технически умения и знания, TTX може да помогне за:

- Осигуряване на участниците на място с нисък риск, където да се упражняват и подготвят на това как да реагират на проблеми със сигурността, с които могат да се сблъскат.

- Стимулиране на критична дискусия по въпросите на цифровата сигурност и как най-добре да се подходи към тях в различен контекст и ситуации. Това може да бъде особено полезно за участниците в обучението, които редовно работят заедно, за да обмислят съвместния си или организационен подход към безопасността.

- Оценяване на това доколко дадено лице или организация са подготвени да се справят с проблемите на сигурността, с които се сблъскват.

Смисълът на TTX е да се установят пропуските в знанията, силните страни и ограниченията на отделните лица, организации и общности. Успешният TTX отива отвъд инструментите и основните практики, като също така подчертава какви процедури или политики може да липсват или трябва да бъдат подобрени.

TTX са най-ефективни, когато се използват като добавки за подобряване на други методи на обучение. Това е така, защото целта на TTX не е основно да се предадат нови умения и знания, а да се внушат и затвърдят наученото чрез практика, базирана на сценарии, обсъждане и оценка.

Компоненти на документите за сценария на TTX

Всяка от 11-те сцени на TTX е базирана на образа на Сара, който сме описали в това ръководство. Освен това всяка сцена включва следните компоненти:

- **Цел - Основната цел на сценария TTX.**
- **Цели на обучението - Възможности за общи цели на обучението, върху които да се съсредоточите по време на TTX. Лекторите вероятно ще имат полза от това да изберат само няколко цели на обучението, върху които да се съсредоточат.**
- **Умения/поведения за обучение преди или след TTX - варианти за конкретни и специфични умения и поведенчески промени, които TTX да възпита у участниците в обучението. Лектрите биха имали полза от това да изберат само няколко умения и поведения, върху които да се съсредоточат, като те трябва да съответстват на избраните цели и задачи на обучението.**
- **Сценарий - Това е действителният сценарий на TTX. Той включва следното:**
    - **Въвеждаща информация и контекстуална информация в началото**
    - **Допълнителна информация за контекста, предоставена по време на сценария**
    - **Въпроси и препоръки за участниците, които да обсъдят и да отговорят на тях. Те са отбелязани с буквата Q, последвана от номер (напр. Q1, Q2, Q3 и т.н.).**
        - **Под въпросите и подканите са посочени някои възможни отговори. Те не трябва да се споделят с участниците по време на TTX. Предназначени са да помогнат на фасилитатора.**

- **Някои сценарии включват инжекции (ще бъдат обозначени като "Инжекция"). Инжекцията е част от нова информация или ново развитие, вмъкнато от фасилитатора в сценария на ТТХ в определени моменти, за да придвижи сценария напред или да добави сложност. Инжекцията може да промени разказа на ТТХ и да изисква действие или отговор от участниците.**

Приложения - Някои сценарии (например Сценарий 3: Тормоз и деанонимизиране) включват и приложения, които често се използват за инжекции по време на сценария.

Разработване на сценарий за ТТХ

В рамките на проекта JSF бяха разработени единадесет сценария за ТТХ (виж тук). Всеки може да ги промени, така че да отговарят по-добре на нуждите за обучение на неговата общност. Може също така да създаде свои собствени от нулата. Ако обмисляте да преработите някой от ТТХ сценариите или да създадете свой собствен, помислете за следното

Целите на обучението трябва да бъдат определени в началото на фазата на проектиране, да се допълват взаимно, да следват логичен ред по отношение на обучението, да бъдат подредени по важност и да бъдат свързани с общата цел на ТТХ. За да опростите процеса на обучение и да улесните измерването на успеха, свържете целите на обучението с конкретни умения или поведения, върху които участниците трябва да се съсредоточат по време на ТТХ. В идеалния случай ще определите тези цели на обучението и конкретните умения въз основа на потребностите и нивата на умения на участниците. Възможно е вече да ги знаете, ако работите с общност, която ви е позната. Като алтернатива може да се наложи да извършите първоначална оценка на потребностите (може би чрез интервюта за ключова информация или предварително проучване), за да съберете тази информация, ако сте по-малко запознати с участниците.

Сценарият трябва да е възможно най-близък до реалния живот, но като цяло не трябва да съдържа имена на реални хора или организации. Съсредоточете се върху реални ситуации, предизвикателства и преживявания. В редки случаи може да е подходящо да се използват реални места, но трябва да се вземат предвид рисковете за сигурността и потенциалните ограничения от това. Изброяването на реални местоположения може например да означава, че хората ще отделят твърде много време за запомняне или проучване на подробности за тях и ще се съсредоточат по-малко върху сценария.

По отношение на сложността сценарият не трябва да засенчва или да отвлича вниманието от обучението. Изборите могат да помогнат на участниците да разберат въздействието, което техните решения ще окажат, но не забравяйте, че добавянето на сложност и избори затруднява изграждането на ТТХ и също така ще направи цялото упражнение много по-дълго.

Можете също така да използвате времето като елемент на дизайна по време на сценария, като задавате време на събитията, които се случват по време на ТТХ, задавате въпроси, обвързани с времето, или използвате ретроспекции или погледи в бъдещето. Във всеки

случай трябва да сте наясно с използването на времето в началото на сценария и да поддържате яснотата по време на цялата сцена.

В зависимост от нивото на уменията на фасилитатора и участниците, можете да обмислите включването на технически елементи в рамките на TTX. Това може да означава, че от участниците се изисква да използват конкретен инструмент, софтуер или процес, за да преминат през сценария. Ако включите технически елемент, предвидете допълнително време за изпълнение на тези задачи и винаги имайте резервен план в случай на технически проблеми или направете техническия компонент незадължителен, за да се приспособите към различните нива на умения.

Можете също така да използвате “инжекции” в рамките на TTX. Те могат да бъдат големи или малки и да зависят от участниците или да са независими от тях. Обикновено “инжекциите” се използват в по-дълги сценарии предвид необходимото време. Те се добавят от лектора и времето е от ключово значение. За успешното интегриране на “инжекция” в сценария са необходими ресурси на фасилитатора както преди, така и по време на фасилитирането на TTX. Използването на инжекции трябва да бъде съобразено с необходимостта от постигане на предварително определените цели на обучението..

Планиране на TTX

Преди да започнете да планирате TTX, помислете за целевата си аудитория и как това ще се отрази на целите на обучението. Дали се обръщате към журналисти, мениджъри на редакции, хора, занимаващи се със сигурност? Всеки един от тях ще работи с много различна информация и ще отговаря за различни решения. Алтернативно, някои TTX целенасочено работят с много по-широка структура - например цяла редакция - за да разберат по-добре как хората в нея общуват и вземат решения. Възможно е да работите с участници, които имат много различни нива на умения, знания и опит в областта на цифровата сигурност. Отделете известно време, за да модифицирате TTX, така че да отговаря най-добре на техните специфични нужди.

След като определите целевата си аудитория, планирайте целите на обучението и обмислете конкретни умения или поведения, които ще обучавате. Избирането на конкретни умения преди обучението е от съществено значение, за да ви помогне да определите обхвата на фокуса си като обучител, да поставите осезаеми цели за обучение на участниците и ще ви помогне да определите критерий за измерване на ефективността на обучението. Вижте списък с примерни умения в подраздела във всеки документ на TTX, озаглавен "Умения/поведения, по които да се обучавате преди или след TTX". Може да е изкушаващо да се обхванат възможно най-много цели на обучението в рамките на един TTX, но е по-ефективно да се проведе по-ограничено обучение, което обхваща конкретни цели на обучението. Не забравяйте, че аудиторията ви разполага с ограничено време и внимание.

Определете колко време ще ви е необходимо за TTX. Понякога правителствени агенции или корпорации организират TTX, които продължават няколко дни, но вашата аудитория може да е много по-притисната откъм време. Трябва да се вземат предвид работата, грижите и

другите ангажименти на участниците. Обикновено TTX с 4-6 въпроса или инжекции може да отнеме около 1 до 1,5 часа. Това също много зависи от големината на вашата група. По-големите групи обикновено се нуждаят от повече време, за да завършат TTX. Също така ще трябва да предвидите време за обобщаване и за преглед на целите на обучението и конкретните умения или поведения, които бихте искали участниците да приложат след сцената. Възможно е участниците да се нуждаят от допълнително обучение или последващи действия, за да могат успешно да приложат конкретните умения или поведения.

Помислете за пространството, с което разполагате за дейността. Ако се провежда лично, идеално е да улесните TTX в пространство, което позволява работа в екип. Стая с маси и удобни столове вероятно е по-подходяща за TTX, отколкото лекционна зала. Може също така да се наложи да се уверите, че има качествен Wi-Fi или други технологични приспособления, като например проектор. При възможност трябва да се даде приоритет и на достъпността на пространството (напр. достъп за инвалидни колички, тоалетни, включващи представители на двата пола, удобен транспорт и т.н.).

Вземете решение дали ще има няколко роли на лектори какви ще бъдат те. Може да е най-целесъобразно един фасилитатор да ръководи TTX, а други да помагат в конкретни стаи за почивка или подзадачи. Фасилитаторите може също така да пожелаят да репетират предварително провеждането на някои елементи.

Определете ресурсите, които ще са ви необходими за TTX. Може да пожелаете да създадете слайд-пакет, информационни материали или друг вид презентационни материали, за да покажете фона на сцената, въпросите/проблемите и/или инжекциите. Важно е също така да вземете предвид материалите, от които участниците може да се нуждаят за водене на бележки.

Провеждане на TTX

Провеждането на TTX се различава от провеждането на традиционно обучение или повишаване на квалификацията в областта на цифровата сигурност. При традиционното обучение по цифрова сигурност обучителите са склонни да говорят много и от тях се очаква да споделят знанията си с участниците. При обучението TTX обаче по-голямата част от говоренето и работата се извършва сред самите участници, тъй като те обсъждат сценария и вземат решения. Фасилитаторът на TTX играе ролята на водещ на процеса, като следи за гладкото протичане на TTX и постигането на целите му. Фасилитаторът на TTX представя упражнението, контекста и предисторията; отговаря на някои основни въпроси; и добавя инжекции. Други препоръки за провеждането на TTX включват:

- Уверете се, че сте добре запознати с TTX.
- Не забравяйте каква е целта и учебните задачи на TTX и насочвайте дискусиите така, че участниците да могат да постигнат тези цели.
- Обяснете ясно ролите и очакванията в началото и по време на TTX.
- Следете внимателно часовника и се уверете, че уважавате и използвате максимално времето, с което разполагате с участниците.

- Уверете се, че пространството е безопасно и гостоприемно и че много хора могат да почувстват, че техните гледни точки са чути и взети предвид.
- Когато участникът спомене добра практика, подчертайте я! Това може да повиши увереността и да насърчи по-нататъшното участие.
- Ако не знаете отговора на даден въпрос, не се страхувайте да го кажете и се ангажирайте да го проследите след TTX. Използвайте пространствата на общността, като например Mattermost на Team CommUNITY, за да получите отговори на въпроси, които може да не успеете да разберете сами.
- Ако е възможно, събирайте обратна връзка по време на обучението и бъдете готови да направите малки корекции. Ако планирате да организирате няколко итерации на TTX, можете също така да съберете обратна връзка в края на сесията, за да разберете по-добре как можете да се подобрите занапред.
- Ако TTX започне да се движи в посока, различна от първоначално планираната, това е нормално! Бъдете гъвкави, но се уверете, че в крайна сметка той е насочен към резултатите от обучението.

Ако желаете да получите по-подробни указания, по-долу са предложени инструкции стъпка по стъпка, които да подпомогнат провеждането.

1. Представете себе си (и всички други обучители), обяснете ролята си и опишете общата цел на TTX (например: днес ще разгледаме как една редакция може да реагира на инцидент, свързан със сигурността). Това е идеалният момент да определите и някои основни правила на групата.
2. След това опишете по-подробно какво ще се случи по време на TTX. Обяснете, че целта е да се симулира измислена ситуация, която се доближава до реалния живот, за да се разберат по-добре нашите реакции и тези на по-широката ни общност.
3. В зависимост от размера и състава на групата, може да пожелаете да разделите участниците на групи.
4. Представете на участниците сценатрия, като включите всякаква предистория, която може да е необходима.
5. Разкажете сцената, подкана по подкана, докато участниците се движат през TTX. Бъдете на разположение за въпроси и за помощ при отстраняване на проблеми, ако участниците се затруднят.
6. Осигурете инжекции при необходимост.
7. Насърчавайте участниците да се включат и да отговорят на подканите. Помолете ги да си водят бележки, когато това е уместно или полезно. Използвайте предварително подготвените си отговори, за да помогнете, ако участниците се затрудняват или се нуждаят от примери, за да започнат.
8. След като участниците завършат TTX, ги подканете да обсъдят основните си изводи от преживяването и мнението си за TTX като метод на обучение. Това е чудесен момент да запишете обратната връзка и да обмислите включването на подобрения за бъдещи обучения.

9. След приключване на ТТХ проверете дали има заключителни материали, последващи действия или обобщения, които трябва да бъдат споделени с участниците.

Приложение 1: Предистория на Сара (личност от ТТХ)

Създадохме един-единствен човек - Сара, на който да базираме преживяванията в примерните сценарии на ТТХ. Това ни помогна както да добавим чувство за последователност към ТТХ, така и да дадем добра отправна точка на журналистите да мислят за заплахите и по-широкия контекст. По-долу сме включили нашето представяне на Сара, което фасилитаторите могат да използват, за да създадат обстановката и да предоставят информация, преди да стартират един от нашите примерни ТТХ сценарии.

Сара е 41-годишна журналистка. В продължение на няколко години е работила за различни местни и международни новинарски организации в родната си страна и в съседни държави.

Миналата година Сара започна работа в разследваща новинарска организация, наречена "Free Press Now", в родната си страна, която често отразява различни политически въпроси. Сред тях са съмнения за нарушения на човешките права от страна на действащото правителство, корумпирани държавни служители и правителствени политики, които затрудняват живота на етническите малцинства в страната.

Благодарение на своите правдиви и надеждни репортажи Free Press Now се превърна в надежден и популярен източник на информация за местното население.

След националните избори преди 5 месеца новото правителство започна да ограничава свободата на печата, а миналата седмица властите нахлуха в домовете на трима известни журналисти в столицата. Неотдавна беше претърсен и домът на Сара, въпреки че извършилите обиска взеха само няколко тефтера.

Сценарии 1: Липсващо устройство

Created by Journalist Security Fellowship participants

Цел

Да помогне на участниците да планират и реагират в ситуация, в която едно или повече от техните устройства, които могат да съдържат чувствителна информация, изчезне.

Задачи на обучението

1. Да бъдат посочени подходи за осигуряване на защитена комуникация между журналистите и техните информатори/източници.
2. Да бъде повишена информираността относно рисковете от загуба на устройство като телефон или компютър.
3. Да бъдат разбрани добрите практики за защита и сигурност на устройствата.
4. Да бъдат споделени добри подходи при назначаване и освобождаване на персонал от организацията, особено във връзка със сигурността на устройствата.

Умения/поведения за обучение преди или след TTX

1. Инсталиране, настройка и използване на Signal (или друго приложение за сигурни съобщения)
2. Настройване и използване на алтернативено криптирано от край до край чат приложение (като WhatsApp или Facebook Messenger Secret Chat)
3. Инсталиране, настройка и използване на Mailvelope (или друг вариант за криптиране на електронна поща)
4. Криптиране на мобилно устройство (задаване на парола)
5. Задаване на пароли за отделни приложения в мобилното устройство
6. Създаване и криптиране на резервни копия на данни на мобилни устройства (чрез облачни услуги или външен твърд диск)

Сценарии

Неизвестен до момента източник се свързва със Сара чрез Facebook Messenger, заявявайки че разполага с чувствителна информация, която иска да сподели с нея. Файлът, който източникът иска да сподели, съдържа информация, касаеща финансите на настоящия министър на отбраната.

В желанието си да запази източника в безопасност Сара иска да го убеди да прехвърли информацията чрез чат приложение, което е криптирано от край до край.

B1 - Как Сара да обясни концепцията за криптиране от край до край, за да убеди източника си че то е важно?

- Никой - дори компанията, която оперира с месинджъра - няма да има достъп до съдържанието на съобщението. Съдържанието на съобщението няма да се съхранява некриптирано на сървърите на компанията.
- Правоприлагащите органи нямат достъп до файла от доставчика на услугата за разговори.
- Ако нападателят успее да хакне акаунта, използван за изпращане на съобщението, той няма да може да получи достъп и до съдържанието на съобщенията (освен ако няма некриптирани резервни копия).

B2 - Какви форми на цифрова комуникация трябва да обмисли Сара, за да гарантира сигурността на комуникацията си с този източник?

- Защита на приложенията за обмяна на съобщения
- Шифрована електронна поща

Източникът се радва, че Сара е загрижена за сигурността на разговорите им, но все още не е сигурен кой метод да избере. Той моли Сара за съвет относно приложенията за обмяна на съобщения като Signal, Telegram и Facebook Messenger, както и относно електронна поща.

Въпрос 3 (по избор) - От гледна точка на цифровата сигурност кои фактори трябва да бъдат взети предвид при избора и използването на различни приложения за обмяна на съобщения?

- Телефонни номера: повечето криптирани месинджъри от типа "от край до край" изискват телефонни номера, а на много места телефонните номера трябва да бъдат регистрирани, така че правителството да знае кой човек стои зад даден телефонен номер. Това означава, че ако правителството някога прегледа телефона на Сара или на източника, ще може да разбере, че те са изпращали съобщения, дори ако са използвали псевдоними или изчезващи съобщения (единственото смекчаване би било да се изтрият имената от контактите, месинджърите и в идеалния случай да се изтрие телефонът).
- Приложения за тайни разговори: Facebook Messenger и Telegram предлагат два режима, от които само единият е криптиран от край до край. Този режим обикновено се нарича таен чат или нещо подобно, въпреки че често е скрит в настройките.
- Изчезващи съобщения: почти всеки съвременен месинджър има функция за изчезване на съобщения, макар че при някои тя е достъпна само в режим на таен чат
- По възможност настройване на опцията “изтриване на разговорите”: Това е доста просто, но е важно да се знае, че някои месинджъри само архивират, а не изтриват чатове.

- Информираност относно екранните снимки: всеки злонамерен участник в разговора може просто да направи снимка на екрана или - ако функциите на месинджъра не позволяват това - просто да направи снимка на екрана на телефона си.
- Удостоверяване с два елемента (2FA) / Двуфакторна проверка (2FV): атакуващият може да завладее акаунт в Messenger, като завладее телефонния номер, използван за регистрация на акаунта, и изпрати отново SMS за проверка до него. Това му позволява да се представи за собственика на акаунта, въпреки че обикновено не дава достъп до историята на съобщенията. Повечето месинджъри вече имат възможност да изискват допълнителна парола в допълнение към SMS кода: това означава, че дори ако нападателят успее да превземе телефонния номер, той не може лесно да получи достъп до акаунта.
- Добри пароли или пароли за влизане в самото устройство (телефон)

B4 (избор) - От гледна точка на цифровата сигурност кои фактори трябва да бъдат взети предвид при комуникация по имейл?

- Източникът трябва да създаде нов имейл адрес, за да комуникира със Сара.
- Новият имейл трябва да има силна и уникална парола и надеждно двуфакторно удостоверяване.
- Източникът трябва също така да следи за фишинг атаки и да използва технологии, които биха могли да помогнат за смекчаването им, като например физически ключове за сигурност или автоматично попълване от мениджъра на пароли.
- В идеалния случай източникът и Сара трябва да комуникират чрез PGP, например с помощта на Mailvelope. Това означава, че дори акаунтите им да бъдат компрометирани по някакъв начин, нападателят няма да може да прочете съдържанието на съобщенията им без техния PGP ключ.

Източникът сигурно изпраща файла на Сара и тя го преглежда на мобилния си телефон. Тя е щастлива, че разполага с тази информация, и излиза с приятелите си, за да празнува. Докато е на парти, тя губи телефона си и разбира, че в него има много проста парола (1111).

B5 - Какво може да се случи с телефона на Сара и информацията в него?

- Всеки, който намери телефона, може да получи достъп до поверителната информация, ако разбере къде се намира тя.
- Всеки, който намери телефона, може да изпрати съобщение до контактите на Сара и да се представи за нея.
- Всеки, който прегледа информацията в телефона, може да застраши самоличността и безопасността на контактите на Сара или да събере информация, която да бъде използвана за социално инженерство.
- Сара може сериозно да загуби доверието към себе си като журналист.

B6 - Какво може да направи Сара сега, за да ограничи въздействието върху цифровата си сигурност?

- Тя може да изтрие информацията от телефона си от разстояние, ако е настроила тази функция.
- Тя може да влезе в акаунтите си за електронна поща и социални медии на другите си устройства, да промени паролата и, ако е възможно, да щракне върху връзката "Излизане от всички влезли устройства".

B7 - Какви са плюсовете и минусите на това да каже на източника, че е загубила телефона си?

- Дискусия без определени верни отговори.

Добри новини! Приятел на Сара, който празнувал с нея е намерил телефона в палтото си. Той ѝ се обадил и на следващия ден върнал телефона на Сара.

B8 - Сега, когато Сара си е върнала телефона, какви стъпки може да предприеме по отношение на цифровата защита на устройството си, в случай че в бъдеще го загуби отново?

- Предимства и недостатъци на използването на биометрични данни.
- Използвайте по-дълги пароли и пароли за отключване на телефона. Избягвайте отключването с шаблони (например такива, които свързват точки), тъй като те могат лесно да бъдат идентифицирани от човек, който гледа, от камера или от петна по екрана.
- Използване на парола за различни приложения в телефона.
- Създаване на приложения, които могат да проследяват, откриват и изтриват устройства от разстояние.

B9 - От гледна точка на организацията, как би изглеждал един добър процес на обучение на нов служител за защита на устройствата му, като мобилни телефони и компютри?

- Организацията трябва да се увери, че всички нейни служители, независимо от длъжността им, преминават през процес на обучение и разбират неговото значение.
- Организацията трябва ясно да посочи очакванията си към персонала по отношение на спазването на практиките за цифрова сигурност.
- Организацията трябва да определи стъпките, които трябва да бъдат предприети, когато сигурността може да бъде компрометирана (например при кражба на телефон или разбиване на парола).
- Организацията трябва да осигури поддръжка от специалист по ИТ на всички служители, които имат нужда от такава.

Сценарии 2: Оперативна сигурност

създаден от сътрудници на JSF

Цел

Да помогне на участниците да придобият високо ниво на осведоменост и да научат добри практики в областта на цифровата сигурност в своята организация, сред колегите си и/или сред журналистите на свободна практика.

Задачи на обучението

1. Да бъде разбрана, на теория, концепцията за цифрова сигурност като непрекъснат процес, а не като крайна цел.
2. Говорене, преподаване и убеждаване на другите за значението на цифровата сигурност.
3. Да бъдат обсъдени, на практика, възможностите за предаване на информация за сигурността чрез мобилно устройство.
4. Да бъдат осигурени добри практики относно боравенето с файлове.
5. Да бъде повишена информираността за настройките на профилите на компютрите, свързани в мрежа.
6. Да бъде разбрано значението на процеса анализ на риска.

Умения/поведения, които да тренирате преди или след TTX

1. Настройване и поддържане на разрешения за работа в платформи за колаборация между участниците (например като Google drive)
2. (ако това е възможно, доколкото някои от тези функционалности са възможни само в комерсиални платформи) Преглед на логовете за достъп в колаборативните платформи като Google drive
3. Създаване и използване на двуфакторно удостоверяване, в идеалния случай с физически ключове за сигурност или подобни механизми, устойчиви на фишинг.
4. Добри политики за пароли (използване на уникални пароли, използване на дълги пароли, използване на фрази) и мениджъри на пароли
5. Криптиране на документи (с помощта на Mailvelope и др.)
6. Инсталиране, настройка и използване на Signal (или друго приложение за сигурни съобщения)
    a. Използване на усъвършенствани функции в приложението за сигурни съобщения (напр. изтриване на съобщения по време)
7. Инсталиране, настройка и използване на Mailvelope (или друг вариант за криптиране на електронна поща)

8. Безопасна работа с файлове и документи от чувствителни източници

Сценарии

Сара сформира екип от журналисти, които да разследват корупцията в обществените поръчки по време на Covid-19, провеждани от Министерството на здравеопазването. Не всички журналисти в екипа имат еднакво ниво на цифрови умения/знания и практики за сигурност. Сара знае, че един от членовете на екипа ѝ има пропуски при защитата на файлове.

B1 - Как Сара би могла да насърчи колегите си да подобрят своя подход към цифровата сигурност? Какво трябва да направи Сара, за да гарантира правилното прилагане практиките за цифрова сигурност, когато организира екип за сътрудничество?

- Обяснете защо е важно да имате добра цифрова безопасност: това може да включва разказ за това как лошата цифрова безопасност може значително да попречи на кариерата на журналиста, как източниците и колегите вероятно ще ви имат по-голямо доверие, ако имате добра цифрова безопасност, и за необходимостта да защитаваме хората около нас.
- Обсъдете какви устройства използват, как защитават потребителските си профили, как съхраняват и обменят файлове, как осъществяват достъп до мрежата на компанията (дали използват собствени устройства, или работят на устройства, осигурено от компанията), как влизат в мрежата на компанията (безжично или по кабел), използват ли удостоверяване с два елемента за защита на потребителските профили и каква е дисциплината им по отношение на паролите (дали преизползват пароли, дали използват инструменти за управление на пароли).
- Вземете решение как екипът да обменя информация, съхранява файлове и получава достъп до тях. Смисълът на втората стъпка е да се гарантира, че всички спазват един и същ протокол, свързан с посочените по-горе дейности.
- Обмислете възможността за обучение на екипа с помощта на новосъздадените протоколи. След като определи правилата, екипът трябва да проведе „суха“ тренировка, при която на практика да изпробва новите начини на предаване на информацията и да установи дали в процеса има пропуски, които да бъдат отстранени.

B2 - Как Сара и нейният екип ще съхраняват и споделят аудио файлове и документи, изпратени от техните източници?

- Ограничете броя на лицата, които имат достъп до различни файлове и папки, използвайте внимателно настройките за споделяне в места като Google Drive
- Не насърчавайте хората да изнасят файлове и документи извън работната среда (USB ключове, прикачени файлове към имейли...), което може да разшири платформата за атаки и да увеличи риска от изтичане на информация/хакване.

- Помолете екипа да използва само служебни компютри за достъп до работни файлове.
- Ограничете това, какво може да бъде инсталирано на служебните компютри, и гарантирайте, че те винаги имат силни пароли и актуален софтуер.

B3 - Как Сара и нейният екип ще осигурят сигурна обмяна на информация между тях?

Като въведе целия екип в една и съща платформа и се увери, че всички се чувстват комфортно с нейното използване, Сара може да помогне на екипа си да установи безопасен и сигурен начин на обмяна на информация между тях.

Вземете предвид:

- Прехвърляне на повечето разговори в Сигнал с изчезващи съобщения и копиране на съобщенията, които трябва да бъдат архивирани
- Шифроване от край до край за електронна поща
- Създаване на строги правила за сигурност на акаунта (уникална парола, 2FA) за имейл

Две седмици преди публикуването на доклада Сара получава телефонно обаждане от главния правителствен източник в разследването. Сара познава добре източника и му вярва. По време на разговора източникът просто казва: „Правителството знае - имало е изтичане на информация“ и затваря.

B4 - От гледна точка на цифровата сигурност, кои са първите стъпки, които Сара трябва да предприеме в отговор на евентуално изтичане на информация?

- Да помоли всички в екипа си да сменят паролите си, в случай че някой нападател получи паролата за някой от акаунтите им.
- Да обърне внимание на факта, че правителството не е трябвало непременно да нахлува в редакцията ѝ. Възможно е да е разбрало за изтичането, например като е проучило кои държавни служители какво печатат.
- Да направи малко разследване в редакцията: да провери дали всички са спазвали протоколите, кой е имал достъп до файловете и изтеклата информация и какво точно е изтекло. Чрез използването на контрол на достъпа и контрол на версиите можете да имате по-лесен начин за проследяване на достъпа до отделните части от информацията, върху които работите.
- Да помисли дали ще трябва да ускори публикуването.

Сара научава, че изтичането на информация е дошло от член на организацията. Дизайнер е имал достъп до споделения Google Drive на организацията (въпреки че не е работил по доклада). Сара научава за това, като проверява контрола на достъпа до Google Drive и разбира, че екипът от дизайнери е имал достъп до всичко в мрежата поради естеството на работата си. Нещо повече: дизайнер случайно е споделил документ с техен клиент на

свободна практика, който е работил за правителството, вместо с приятел от редакцията, който е имал същата фамилия.

B5 - Какво Сара би трябвало да направи в тази ситуация, което не е направила?

- Сара трябва да създаде защитени протоколи, които да се прилагат само за нейния разследващ екип. Тя трябва да гарантира, че има ясна политика за достъп и че тя се спазва на практика.
- Екипът трябва да работи с дизайнерите по такъв начин, че те да разполагат с информация само при необходимост: не трябва да им се предоставят никакви тайни или чувствителни детайли, освен ако това не е абсолютно необходимо за публикацията.
- Сара също така трябва да разглежда сигурността и неприкосновеността на личния живот като процес, а не като състояние; това е нещо, което трябва постоянно да се усъвършенства.

Сценарий 3: Тормоз и деанонимизиране

създаден от сътрудници на JSF

Цел

Да помогне на участниците да осмислят как най-добре да се подготвят и реагират при деанонимизиране и тормоз онлайн.

Задачи на обучението

1. Да бъдат определени методи и мерки за смекчаване на последиците при журналисти, които са жертва на тормоз в социалните медии и деанонимизиране.
2. Да бъдат разбрани начините за събиране на информация от социалните медии и как тя може да бъде използвана срещу журналисти и служители в редакциите.
3. Да бъде проучена връзката между пола и тормоза и последиците от нея върху сигурността.
4. Да бъдат обсъдени съображенията за това как медията може да установи процедури и практики за защита на персонала и подизпълнителите, които са обект на тормоз и деанонимизиране.
5. Да бъдат обмислени планове за непредвидени ситуации за журналисти, които нямат подкрепата на редакцията (напр. на свободна практика, външен персонал).
6. Разказване на истории за сигурността и убеждаване на другите, как можем да говорим с хора, които традиционно не се сблъскват с тормоз, че това е сериозен проблем, който изисква координирани организационни действия и подкрепа.
7. Организационна сигурност: определяне на политики в организациите, намиране на начини, по които организациите могат най-добре да подкрепят журналисти, които са изправени пред атаки за тормоз.[1]

Умения/поведения за трениране преди или след TTX

1. Управление и актуализиране на настройките за поверителност на основните социални медийни платформи.
2. Използване на инструменти за безопасност на основните социални медийни платформи, като докладване и блокиране. Това включва както разбирането как да се използват такива механизми, така и какво точно правят.
3. Настройване и използване на двуфакторно удостоверяване, в идеалния случай с физически “ключове” за сигурност или подобни механизми, устойчиви на фишинг.

[1]В повечето обучения това е цел на обучението. Ако водите сесия с медийни мениджъри или други лица, вземащи решения, и е възможно да се измерят организационните резултати, бихте могли да го направите и като умение.

Сценарий

Сара работи върху нов материал за етническите малцинства в страната си и за това как политиката на правителството води до все по-голяма маргинализация на тези групи. През последните няколко седмици Сара забелязва рязък скок на коментарите в социалните мрежи в профилите си, от които споделя и работата си. Започва да получава и омразни и унизителни коментари от различни тролове, насочени директно към нея.

B1 - Какви са стъпките, които Сара може да предприеме, за да блокира и докладва хората, които правят тези коментари?

- Може да използва вградените възможности за блокиране и докладване, каквито притежават повечето платформи за социални медии.
- Може да се обърне към големите компании за социални медии (директно или чрез своята организация), за да съобщи за мащабния тормоз, насочен срещу нея.
- Да деактивира публикациите и отговорите в нейния профил.
- Да бъде по-внимателна в избора на това кой може да я намери в социалните медии.
- Да избере да не бъде тагвана в социалните медии.

Полагането на усилия от нейна страна за блокиране и докладване на някои от основните подстрекатели дразни групата тролове, което води до увеличаване на омразното съдържание срещу Сара. В някои коментари се намеква и за заплахи и насилие срещу нея, пряко или косвено.

B2 - Какви са начините, по които Сара би могла да разследва агресията срещу себе си, за да определи дали тя е част от по-голяма, по-координирана кампания, или е нещо органично.

- Тя може сама да разследва ситуацията или да помоли колегите си за помощ.
- Тя може да провери дали всички тролове използват абсолютно същия език, ключови думи или хаштагове. Ако го правят, това вероятно ще означава, че е координирана кампания.
- Зависи от платформата. В Instagram има обширни опции за преглед на информация за конкретни акаунти – кога е създаден, колко хора го използват, колко често е сменял името си и т.н.
- Проверете дали е усилено от някаква медия.
- Да провери най-честото време, в което се публикува

Тя разказва на колегите си за коментарите, но повечето мъже от екипа, включително редакторът ѝ, ѝ казват да не се притеснява и че проблемът ще изчезне от само себе си. Тя е стресирана, чувства, че екипът ѝ не я изслушва и не разбира проблема.

B3 - Вместо да кажат на Сара да не се притеснява, какви са начините, по които екипът и организацията ѝ могат да я подкрепят, особено по отношение на нейното присъствие в мрежата и цифрова сигурност?

- Да помогнат в извършване на пълна оценка на ситуацията.
- Да прегледат заедно със Сара практиките ѝ за цифрова сигурност и мерките за безопасност, които използва, и да ѝ помогнат да ги подобри, ако е необходимо.
- Да получи идеи и споделен опит от другите служители в организацията.
- Позволете на хората, на които имате доверие, да управляват вашия акаунт или да го преглеждат, така че да не сте изложени директно на тези думи и заплахи, но все пак да имате присъствие
- Организацията може да помогне в търсенето на модели в тормоза
- Да се проследи как тормозът преминава през публикациите на организацията, а не само през тези на Сара.
- Случая да бъде предаден на екипа по сигурността и да помогнете с разследването.

Един ден част от личните снимки на Сара са пуснати в интернет от един от подстрекателите. Снимките, които тя е публикувала в социалните мрежи преди години, са лични и в някои случаи съдържат чувствителна информация.

Включване - Споделете между 1 и 4 снимки с участниците. (Снимките могат да бъдат намерени в приложението към този документ). Примерните снимки включват:

- Сара и кучето ѝ се разхождат пред къщата ѝ
- Сара пуши цигара с марихуана
- Сара и група от най-близките ѝ приятели на почивка
- Сара работи в редакцията

Обсъдете с участниците защо всяка от тези снимки може да е чувствителна.

B4 - Какви са начините някой да е получил достъп до онлайн информацията на Сара, например стари публикации в социалните мрежи?

- Приятелите на Сара са публикували снимки с лоши настройки за поверителност
- Акаунтите на Сара са били разбити
- Някой от контактите на Сара в социалните медии може да е запазил снимките, за да ги сподели по-късно
- Снимките на Сара в социалните медии може да са били индексирани от търсачка

B5 - Какви стъпки може да предприеме Сара, за да предотврати изтичането на допълнителна лична информация в интернет?

- Да изтрие стари снимки

- Да закрие профили
- Да заключи профили
- Да качи нови снимки, които не разкриват много информация за нея
- Да получи доклади от социалните медии, който обобщават данните, с които разполагат за нея.
- Да докладва снимките, които са публикувани наскоро/ докладва акаунтите, които са ги публикували
- Да продължи да публикува служебно съдържание, дори ако публикува по-малко лично съдържание. Ако се откажете от интернет, троловете ще са победили.
- Да направи екранна снимка на публикациите, да ги документира колкото е възможно повече. Да запише онлайн псевдонимите на троловете.

B6 - Какви стъпки би могла да предприеме Сара и организацията ѝ, за да предотвратят събирането и изтичането на тази информация, особено по отношение на цифровата сигурност?

- създайте група от близки приятели, които са единствените, които виждат лични снимки и лични публикации в социалните медии
- изобщо не публикувайте чувствителна информация (като снимката с джойнта)
- не публикувайте снимки, които разкриват лична информация като местоположение
- отворете бизнес акаунти, така че да има онлайн присъствие, което не е свързано с личния ѝ живот
- силна парола и 2FA политики за акаунти в социални медии

Приложение 1: Примерни снимки

Сценарии 4: Властите влизат в редакция

създаден от сътрудници на JSF

Цел

Да помогне на участниците как да отговорят на теория и на практика на навлизането на властите в тяхната редакция.

Задачи на обучението

1. Да осигури резервни планове за комуникация и техническа подготовка, в случай че достъпът до редакцията или личното устройство вече не е възможен.
2. Да бъдат разбрани най - добрите практики за защита на цифрови устройства в редакция или организация.
3. Да бъдат идентифицирани начините за защита на различни файлове на цифрово устройство, като компютър или мобилен телефон.
4. Да бъде изготвен план за действие при компрометиране на информация в случай на влизане и претърсване на редакцията от властите.
5. Да бъдат изучени концепциите за анализ на риска и предварително планиране от физически лица и организации.

Умения/поведения за упражняване преди или след TTX

1. Използване на инструмент като VeraCrypt или подобен за криптиране на данни на твърди дискове и външни устройства
2. Изграждане на модел на заплахите, по-специално по отношение на справянето с властите и нахлуване в офиса: как да оцените рисковете, да се подготвите за такъв и да направите равносметка след него
3. Организационна и общностна сигурност, по-специално как да работите с редактори, мениджъри и адвокати по време на ситуации с висок стрес и как да определите кой въпрос към кой човек се отнаса
4. Използване на настройки в рамките на Microsoft Office и Google Drive, за да видите кои файлове са били достъпни наскоро и кога
5. (За напреднали) Ако организацията има достъп през премиум абонамент за Google Drive или O365, как да организираме достъпност и работа с такава регистрация
6. Преглеждане на хронологията на търсене и достъп до файлове на основните уеб браузъри и операционни системи

Сценарий

Сара работи в редакция, заедно с още около 20 души. Сутринта в понеделник е натоварена - 15 журналисти и други служители работят в редакцията, а други петима работят от разстояние. Около 10:00 ч., в редакцията пристигат около 50 полицаи. Те разполагат със заповед, която показват на главния редактор, след което влизат със сила, като същевременно изискват всички журналисти и служители да напуснат незабавно.

Сара и колегите ѝ се срещат отвън и обсъждат начините, по които да продължат да поддържат работата на медията си по безопасен и сигурен начин.

B1 - Кои са приоритетите в ситуация като тази?

- Да се свържат с адвокат, за да се консултират за следващи стъпки, които трябва да предприемат
- Да се свържат с колегите си, които работят дистанционно
- Да проверят кой е успял да вземе мобилния си телефон и кои са оставени в редакцията

B2 - Кои са начините, по които Сара и нейните колеги могат да общуват сигурно през това време?

- Да си създадат групов чат в WhatsApp/Signal
- Може би е добра идея да общуват чрез лични, а не служебни номера. В противен случай, чатът може да се синхронизира с устройствата, които са все още в офиса

B3 - Как Сара и колегите ѝ трябва да управляват онлайн профилите на организацията, като уеб страници и профили в социалните мрежи?

- Да променят незабавно паролите си
- Ако е възможно да излезат дистанционно от устройствата, които са все още в офиса, но първо се консултират с адвокати, така че това да не се счита за подправяне на доказателства (в зависимост от местоположението/юрисдикцията)
- Да се консултират с адвокати преди да публикуват информация за полицейското нахлуване

Сара си спомня, че на излизане от редакцията е видяла как полицията прибира компютри, устройства и документи в чанти. Сара е успяла да вземе телефона си, но лаптопът ѝ е останал в редакцията. Групата бързо преценява каква информация може да получи полицията.

B4 - Как би трябвало да бъдат защитени устройствата в редакцията?

- Компютрите - заключени със силни пароли
- Заключването на екрана да се случва след кратък период от време
- Криптиране на USB устройства и външни твърди дискове

По време на разговора им извън офиса, главният редактор се сеща, че е забравил да заключи компютъра си, при напускане на работното място.

Два часа по-късно полицията напуска редакцията и позволява на журналистите да се върнат на работните си места. Служителите се събират, за да преценят до каква информация полицията е имала достъп, както и да обсъдят заплахи от подобен характер, които могат да се случат в бъдеще.

B5 - По какъв начин редакцията може веднага да оцени резултата от нахлуването на властите?

- Да проверят какви хартиени документи, ако има такива, са били отнети или пренаредени (ако документите са били пренаредени, това означава, че полицията може да ги е снимала)
- Компютрите обикновено имат търсене/достъп до файлове/хронология на браузъра, да прегледат и това. Могат да видят последните файлове в Microsoft Word и хронологията в браузърите, ако използват Google Документи. Ако браузинг историята е изтрита, това би означавало, че някой може да се е опитал да изтрие знаци за "влизане" в устройство
- Малко вероятно е зловреден софтуер да е бил инсталиран по време на нахлуването, но ако се притесняват за това, трябва да се консултират с професионалист, специализиран в криминалистиката на зловреден софтуер

B6 - Как организацията може да си гарантира, че не е изложена на допълнителен риск след нахлуването на полицията?

- Да променят паролите за всеки случай
- Да говорят с адвокат за това, какво право за достъп е имала или не полицията по време на акцията
- Ако са използвали кодови имена или псевдоними за своите изследвания, да ги сменят

Няколко седмици по-късно главният редактор свиква всички служители на събрание. Целта е да се определят подобни бъдещи заплахи, пред които редакцията може да бъде изправена.

B7 - По отношение на анализа на риска и дигиталната сигурност, как отделните лица и организации идентифицират заплахите, с които могат да се сблъскат?

- Задават стандартните въпроси при изграждане на модела на заплахите: с каква информация разполагат противниците им, кой би се интересувал от достъп до нея и какви биха били последствията, ако противниците им успеят
- Когато изброяват противници, да помислят, както за мотива (какво биха искали да направят и защо), така и за възможностите (какво всъщност са способни да направят, какви технически, правни, организационни и финансови средства имат?)

Сценарии 5: Властите влизат в дома на журналист

създаден от сътрудници на JSF

Цел

Да предостави на журналистите теоретични и технически умения за осигуряване на възможно най-добрата дигитална сигурност в домашна среда.

Задачи на обучението

1. Разбиране как да бъдат защитени цифровите устройства у дома.
2. Приложение на предпазни мерки за хартиени носители на информация.
3. Иницииране на отдалечено изтриване на файлове - положителни и негативни страни.
4. Ограничаване на достъпа до информация, която е била компрометирана.
5. Подготовка на дома на журналиста, в случай на нахлуване на властите.
6. Участниците да помислят за сигурността на организацията и общността, по-специално как да работят с редактори, мениджъри и адвокати по време на ситуации на висок стрес и да определят кой въпрос към кого да адресират.

Умения/поведения за упражняване преди или след TTX

1. Използване на инструмент като VeraCrypt или подобен за криптиране на данни на твърди дискове и външни устройства
2. Изграждане на модел на заплахите, по-специално по отношение на справянето с властите в случай на нахлуване в дома: как да бъдат оценени рисковете, да се подготвите за такъв и да направите разбор след него
3. Активиране на инструменти като Find My на Apple или Android/Samsung Find, които могат да се използват за дистанционно заключване или изтриване на устройства
4. Използване на настройки за Microsoft Office и Google Drive, за да се види кои файлове са били достъпни наскоро и кога
5. (За напреднали) Ако организацията има достъп през премиум абонамент за Google Drive или O365, как да организираме достъпност и работа с такава регистрация
6. Преглеждане на хронологията на търсене и достъп до файлове на основните уеб браузъри и операционни системи

Сценарий

След националните избори преди 5 месеца новото правителство започва да насочва властите към ограничаване на свободата на печата и властите нахлуват в домовете на

трима известни журналисти в столицата. В отговор на това, Сара и няколко нейни колеги се събират и обсъждат начини да защитят себе си и информацията си, при подобен сценарий.

B1 - Кои са нещата, които журналистът трябва да обмисли, когато взима решение да съхранява информация в дома си?

- Да държи устройствата на безопасно място в дома си
- Да кодира и защити с парола всички устройства
- Да не включва информация за източник в документите си
- Да поддържа списък на това каква информация къде се съхранява (този списък също трябва да бъде защитен!)
- Нецифрова информация: да има предвид физическите копия
- Да има възможност да не съхранява нищо у дома си
- Да спазва местните закони, както и политиката на организацията
- Да бъде наясно с правните последици от съхраняването на чувствителна информация у дома си, вместо на работното място.
- Да бъде наясно кой има достъп до дома и устройствата му?

B2 (по избор) - Кои са добрите практики при съхраняването на хартиени текстови документи у дома?

- Помислете за унищожаване на нещата, които не са необходими
- Не съхранявайте всички бележки на едно място - по-малко леснодостъпна информация
- Скрийте хартиените носители на информация
- Сейф, ключалка и ключ, играйте на сигурно!
- Какъв вид чувствителна информация би могло да се съхранява у дома?
- Използвайте акроними, съкращения, които имат смисъл само за вас

B3 - Какви мерки могат да бъдат предприети за възможно най-добрата защита на електронни устройства (компютри, твърди дискове, USB памети и др.)

- Шифроване
- Защита с парола
- Резервни копия, пазени отдалечено
- Помислете за сигурността на по-старите устройства, особено тези, които вече не се използват

Днес Сара излиза от дома си в 09:00 ч., за да пие кафе и да напазарува. Когато се връща час по-късно, вратата на апартамента ѝ е отворена. Сара влиза и открива двама мъже, които претърсват бюрото и спалнята ѝ. Единият от тях чете хартиените ѝ бележници, а другият държи чантата с лаптопа ѝ вътре. Сара вижда, че USB паметите и външните твърди дискове липсват от бюрото. Двамата мъже са цивилни, но тя предполага, че по някакъв начин работят за правителството.

Избор 1 - Сара разговаря за кратко с двамата мъже и успява да напусне дома си безопасно. Тя отива до дома на приятел наблизо.

B4 (по избор) - Знаейки, че част от нейната информация, особено от хартиения ѝ бележник, е била компрометирана, кого Сара трябва да информира за инцидента?

- Да уведоми главния редактор и юристите на медията
- Преди да се свърже с източници, които може да са споменати в бележника, да говори първо с редактора си и колеги в редакцията, както и с персонала по IT сигурността (ако източниците са споменати само с псевдоним, но получат обаждане на следващия ден, това може да позволи на службите да достигнат до източника чрез псевдонима му). Може да е разумно да не се свързва с източниците си веднага.

B5 - Какво би могла да направи Сара, за да предотврати достъп до цифровата си информация, докато двамата мъже са все още в апартамента ѝ?

- Да направи всичко възможно да спазва местното законодателство
- Да настоява властите също да спазват местното законодателство (т.е. да имат заповед, свидетели и т.н.)
- Да използва техники за преговори
- Да разбере кои са те и дали имат правомощия
- Да прецени ситуацията с оглед на личната си безопасност
- Да потърси правен съвет, да се обади в редакцията
- Да предостави фалшиви профили и документи (изисква предварителна подготовка)
- Да отклони вниманието

Избор 2 - Сара не може да напусне апартамента си. Двамата мъже я подканят да седне и изискват от нея да предостави паролите за компютъра си и USB паметите си. Те я заплашват, че ще я отведат в полицейския участък, ако не предостави тази информация. Сара иска заповед за арест, но те не предоставят такава.

B6 - Знаейки, че на компютъра си има чувствителна информация, включително идентификацията на поверителни източници, какви възможности има Сара в тази ситуация?

- Да оцени заплахите и да приоритизира проблемите по важност
- Да излезе от компютъра си чрез отдалечен достъп и да изтрие профили с чувствителна информация
- Да определи каква част от наличната информация е била съхранявана в дома ѝ
- Да обмисли положителните и отрицателните страни на това да информира колегите си и източниците си, че може да са в опасност. Това решение може да бъде взето заедно с редакционния екип.
- Възможност за отдалечено изтриване на файлове

B7 - Сара има приложение за отдалечено изтриване на файлове, което е настроено на компютъра ѝ. Какво трябва да вземе предвид, преди да изтрие файловете от компютъра си?

- Възможно е да възникне правен проблем - възпрепятстване на правосъдието
- Последици
- Ако Сара няма доказателства, че хората са от правоприлагащите органи, но изглеждат като стандартни нарушители или от недържавни сили за сигурност, това също променя правния пейзаж и възможните заплахи

B8 (по избор) - Знаейки, че част от нейната информация е била компрометирана, кого трябва да информира Сара за инцидента? От значение ли е редът, в който тя информира хората?

- Главният редактор
- Екипът по сигурността/IT на редакцията
- Евентуално да се свърже с източниците си
- Ако е журналист на свободна практика, да сподели за ситуацията на други журналисти на свободна практика.

Сара в крайна сметка отказва да предостави паролата за устройствата си. След като претърсват апартамента ѝ още 10 минути, двамата мъже си тръгват с компютъра, USB паметите и хартиените ѝ бележници.

Сега Сара отново има достъп до апартамента си. Тя вижда, че единият от двата ѝ компютъра е оставен заедно с една от USB паметите ѝ. Всичките ѝ хартиени бележници са взети.

B9 - Какво трябва да направи Сара сега, за да е сигурна, че информацията и сигурността ѝ няма да бъдат допълнително застрашени от действията на двамата мъже, които са били в апартамента ѝ?

- Мъжете може да са инсталирали зловреден софтуер на устройствата на Сара; може би е добра идея да изпрати тези устройства на специалист по цифрова криминалистика
- Апартаментът може да се подслушва
- Да поиска ресурси от организацията
- Да говори със своите колеги, съветници по сигурността и правните въпроси, дали има смисъл от гледна точка на безопасността и сигурността, да се говори публично за нападението или не

B10 (по избор) - Освен аспектите на дигиталната сигурност в този сценарий, какви други предпазни мерки и реакции би могла да предприеме Сара, за да запази себе си и информацията си в безопасност?

- Да научете малко повече за това как работят силите за сигурност в страната, дали има групи, които се опитват да сплашат журналисти, които не са свързани със силите за сигурност

- Да се подготви с помощта на адвокати и редактори как е най-добре да се реагира при нахлуване на власите в дома
- Да не съхранява чувствителна информация у дома си, ако има вероятност за претърсване на дома

In partnership with

LOCALIZATION LAB