Image not found or type unknown

Упражнение: «Жизненный цикл данных как способ понимания риска» [Углубленное упражнение]

Данное обучающее упражнение направлено на рассмотрение оценки рисков с точки зрения жизненного цикла данных. Активисты_ки, организации и движения работают с данными - от создания / сбора / сбора данных до публикации информации, основанной на данных.

Введение

Image not found or type unknown deepening_activ_circular_400px-with-text_russian.png

Картинка. Надпись на картинке: Углубленные Упражнения
Рисунок на картинке: зеленый круг. Сверху картины дерево и по всему кругу распущены корни

Данное обучающее упражнение направлено на рассмотрение оценки рисков с точки зрения жизненного цикла данных. Активисты_ки, организации и движения работают с данными - от создания / сбора / сбора данных до публикации информации, основанной на данных.

Существует два основных подхода к технике проведения данного мероприятия:

- **Общий семинар** проводится в рамках общего семинара по цифровой безопасности, участники_цы которого представляют различные организации и/или не принадлежат к каким-либо организациям.
- **Организационный семинар** предназначен для отдельных групп и их сотрудников_ц. Общий контекст для этого типа семинара заключается в том, что различные команды одной организации объединяются для оценки рисков, связанных с практикой и процессами работы с данными в их организации.

Цели обучения и общие темы, рассматриваемые в обоих подходах, одинаковы, но методологии и техники фасилитации должны быть скорректированы для двух различных сценариев семинаров.

Цели обучения

В процессе выполнения этого упражнения участники_цы смогут:

- понимать риски и аспекты безопасности на каждом этапе жизненного цикла данных;
- применять механизмы оценки рисков для обеспечения личной и/или организационной безопасности.

Для кого предназначено данное упражнение?

Это упражнение предназначено для отдельных активистов_к (в рамках общей оценки рисков или семинара по цифровой безопасности) или для группы (организации, сети, коллектива), проходящей процесс оценки рисков. Существуют две техники проведения, два подхода к этому упражнению, в зависимости от того, будет ли это общий семинар или занятие для отдельной группы.

Упражнение также может быть использовано в качестве диагностического для определения приоритетов, на каких практиках или инструментах следует сосредоточиться в оставшейся части семинара по цифровой безопасности.

Продолжительность

Зависит от количества участников_ц и размера группы. В целом, процесс может занять минимум четыре часа.

Ресурсы

- Бумага для флипчарта
- Маркеры
- Проектор для презентации жизненного цикла данных и направляющих вопросов, а также для совместного использования участниками_цами, если необходимо.

Техника проведения для общего семинара

(Этот материал предназначен для общего семинара по оценке рисков или цифровой безопасности, в котором участвуют активисты_ки из разных контекстов. Цели обучения остаются теми же, но некоторые тактики обучения и фасилитации будут отличаться от семинара для уже сформировавшейся группы людей.)

Первая фаза: что вы публикуете?

В этой части упражнения участникам_цам задается вопрос: «**Что вы публикуете в рамках своей работы в качестве активиста_ки?**»

Смысл здесь в том, чтобы начать с самой очевидной части жизненного цикла данных - обработанных данных, которые распространяются в виде информации. Это могут быть отчеты об исследованиях, статьи, сообщения в блогах, руководства, книги, веб-сайты, сообщения в социальных сетях и т. д.

Это можно сделать на пленарном обсуждении, в стиле "попкорн". Это когда ведущий_ая задает вопрос и просит участников_ц дать короткие и емкие ответы - как кукуруза, лопающаяся на сковороде!

Вторая фаза: презентация жизненного цикла данных и соображений по безопасности

Цель презентации - напомнить участникам_цам о цикле управления данными. Ключевые моменты презентации можно найти здесь (см.файлы основы-жизненного цикла данных-презентация.odp а также Презентация*)*.

Третья фаза: время рефлексии о жизненном цикле персональных данных

Сгруппируйте участников_ц в соответствии с тем, что они публикуют. Попросите их выбрать конкретный пример того, что они опубликовали (статья, исследовательский отчет, книга и т.д.), и попросите их сформировать группы на основе аналогичной работы.

Здесь у каждого_й из них будет время проследить жизненный цикл опубликованных данных, а затем у группы будет время поделиться своими рефлексиями.

Время на рефлексию должно составлять около 15 минут. Далее потребуется около 45 минут на обсуждение в группе.

Вопросы для индивидуальной рефлексии будут представлены в презентации.

При работе в группе все участники_цы группы по очереди расскажут о жизненном цикле данных своей опубликованной работы.

Четвертая фаза: обратная связь и соображения по безопасности

Вместо презентации групповых отчетов тренер_ка-фасилитатор_ка задает каждой группе вопросы, которые помогут выявить то, о чем шла речь в группах.

Ниже приведены вопросы, которые вы можете использовать для подведения итогов времени, проведенного в рефлексии и групповой дискуссии:

- Какие устройства хранения данных были наиболее распространены в группе? Какие из них использовал только один человек?
- Каковы были различия и сходства в доступе к хранилищу данных в вашей группе?
- Как насчет обработки данных? Какие инструменты использовались в вашей группе?
- Опубликовал ли кто-нибудь в группе что-то, что подвергло риску его или кого-то из его знакомых? Что именно?
- Задумывался ли кто-нибудь в группе о практике архивирования и удаления данных до сегодняшнего дня? Если да, то какова была практика в этой области?
- Возникали ли на каком-либо этапе жизненного цикла ваших данных проблемы с безопасностью и защитой? Каковы они?

Подведение итогов упражнения

По завершении групповых презентаций и обмена опытом тренер_ка-фасилитатор_ка может подвести итоги упражнения:

- Указать на ключевые моменты
- Спросить участников_ц об основных выводах, сделанных в ходе упражнения

- Спросить участников_ц об изменениях в практике управления данными, о которых они узнали в ходе мероприятия.

*Картинка с рисунком. На рисунке растения синего цвета

image-1605452256072.png

Техника проведения для организационного семинара

> Данный семинар предназначен для организаций и их сотрудников_ц.

Первая фаза: какая информация является общей для каждого отдела/ программы / команды организации?

Исходя из конфигурации и структуры организации, попросите каждый отдел или команду привести пример чего-то общего для них - внутри организации или за ее пределами.

- Вот примеры для стимулирования ответов:
- Для отделов коммуникаций - какие сводки вы публикуете?
- Для исследовательских команд - какие исследования вы проводите, о чем отчитываетесь?
- Для администраторов и финансистов - кто может ознакомиться с платежными ведомостями вашей организации? Как насчет финансовых отчетов?
- Для отделов кадров - как насчет оценки персонала?

Примечание по фасилитации: на этот вопрос гораздо легче отвечать командам, у которых есть цели, ориентированные на внешний мир, например, отделу по коммуникациям, или программе, которая публикует отчеты и исследования. В отношении более ориентированных на внутренний мир отделов, таких как финансово-административный или отдел кадров, тренеру_ке-фасилитатору_ке, возможно, придется потратить время на примеры того, какой информацией они обмениваются.

Цель этого этапа - заставить различные команды признать, что все они обмениваются информацией, как внутри организации, так и за ее пределами. Это важно, поскольку каждая команда должна быть в состоянии определить один или два вида информации, которыми они обмениваются при оценке риска в своей практике управления данными.

Вторая фаза: презентация жизненного цикла данных и соображений по безопасности

Цель презентации - напомнить участникам_цам о цикле управления данными. Ключевые моменты презентации можно найти здесь Презентация_Жизненный Цикл Данных

Третья фаза: групповая работа

В рамках команд попросите каждую группу определить один-два вида информации, которой они делятся/которую публикуют.

Чтобы расставить приоритеты, предложите командам подумать о том, какую информацию они больше всего хотят обезопасить, или о том, какая информация, которой они делятся, является конфиденциальной.

Затем, для каждого вида совместно используемой или публикуемой информации, попросите команды вернуться назад и отследить его жизненный цикл данных. Используйте приведенную ниже презентацию, чтобы задать ключевые вопросы о практике управления данными для каждого фрагмента опубликованных или совместно используемых данных.

В конце этого процесса каждая команда должна быть в состоянии поделиться с остальными результатами своих обсуждений.

В целом групповая работа займет около часа.

Четвертая фаза: презентации групп и рефлексия по поводу безопасности

В зависимости от размера организации и проделанной каждым отделом работы, дайте им время представить результаты обсуждения своим коллегам. Поощряйте каждую группу подумать о креативной презентации и ключевых моментах своих обсуждений. Им не обязательно делиться всем.

Призовите слушателей делать записи о том, что им рассказывают, поскольку после каждой презентации будет дано время для обмена комментариями и обратной связи.

В реалистичных условиях этот процесс займет около 10 минут на группу.

Роль тренера_ки-фасилитатора_ки здесь, помимо учета времени и управления обратной связью, заключается также в предоставлении обратной связи по каждой презентации. Сейчас самое время надеть шляпу практикующего специалиста по безопасности.

Некоторые области, о которых следует спросить:

- Если процесс сбора данных должен быть конфиденциальным, не лучше ли использовать более безопасные средства связи?
- Кто имеет доступ к устройству хранения данных в теории и в реальности? Если речь идет о физическом устройстве хранения данных, то где оно находится в офисе?
- Кто имеет доступ к исходным данным?

Как тренер_ка-фасилитатор_ка, вы также можете использовать эту возможность, чтобы поделиться некоторыми рекомендациями и предложениями по повышению безопасности практики управления данными в организации.

> **Примечание для фасилитатора_ки:** существует ресурс под названием Alternative Tools in Networking andCommunications («Альтернативные инструменты для нетворкинга и коммуникаций») в «FTX: перезагрузка безопасности», с которым вы

можете ознакомиться для проведения данного упражнения.

Пятая фаза: возвращение к группам: улучшение безопасности

После того, как все команды представили свои презентации, они возвращаются в свои группы для дальнейшего обсуждения и рефлексии по поводу того, как они могут лучше защитить свой процесс управления данными и собственно данные.

Цель каждой группы - спланировать методы повышения безопасности на всех этапах жизненного цикла данных.

К концу обсуждения каждая группа должна иметь некоторые планы по повышению безопасности своей работы с данными.

> **Примечание:** предполагается, что для этого группа прошла базовый тренинг по безопасности. Как вариант, тренер_ка-фасилитатор_ка может использовать четвертую фазу как возможность предоставить некоторые рекомендации по более безопасным альтернативным инструментам, опциям и процессам для практики управления данными группы.

Методические вопросы для обсуждения в группе

- Какие из данных, которыми вы управляете, являются общедоступными (о них может знать каждый), частными (о них может знать только организация), конфиденциальными (о них может знать только команда и определенные группы внутри организации) - и как ваша команда может гарантировать, что эти различные типы данных могут оставаться частными и конфиденциальными?
- Как ваша команда может обеспечить контроль над тем, кто имеет доступ к вашим данным?
- Какова политика содержания и удаления данных на платформах, которые вы используете для хранения и обработки данных в интернете?

- Как команда может практиковать более безопасные коммуникации, особенно в отношении частных и конфиденциальных данных и информации?
- Какие практики и процессы должна иметь команда, чтобы сохранить конфиденциальность и секретность данных?
- Что следует изменить в вашей практике управления данными, чтобы сделать ее более безопасной? Посмотрите на результаты предыдущей групповой работы и определите, что можно улучшить.
- Какие роли должны быть у каждого члена команды, чтобы управлять этими изменениями?

Шестая фаза: финальная презентация планов

На этом этапе каждой команде будет предоставлено время для представления способов, которыми они будут обеспечивать безопасность своей практики управления данными.

Это возможность для всей организации поделиться стратегиями и тактиками и поучиться друг у друга.

Подведение итогов упражнения

После завершения групповых презентаций и обмена мнениями тренер_ка-фасилитатор_ка может подвести итог упражнения:

- Указать на ключевые моменты
- Спросить участников_ц об основных выводах, сделанных в ходе упражнения
- Согласовать дальнейшие шаги по практической реализации планов.

Презентация

Существует еще один способ понять риски по возрастанию — это взглянуть на практику работы с данными в организации. Каждая организация имеет дело с данными, и каждое отделение внутри организации тоже.

Ниже приведены некоторые аспекты безопасности и защиты для каждого этапа жизненного цикла данных.

Создание / получение / сбор данных

- Какого рода данные собираются?
- Кто создает/получает/собирает данные?
- Подвергнет ли это людей риску? Кто подвергнется риску в случае обнародования этих данных?
- Насколько публичным / частным / конфиденциальным является процесс сбора данных?
- Какие инструменты вы используете для обеспечения безопасности процесса сбора данных?

Хранение данных

- Где хранятся данные?
- Кто имеет доступ к хранилищу данных?
- Какие методы / процессы / инструменты вы используете для обеспечения безопасности устройства хранения данных?
- Облачное хранилище в противовес физическому хранилищу или хранилищу на устройстве.

Обработка данных

- Кто обрабатывает данные?
- Будет ли анализ данных подвергать риску отдельных лиц или группы лиц?
- Какие инструменты используются для анализа данных?
- Кто имеет доступ к процессу/системе анализа данных?
- При переработке данных сохраняются ли вторичные копии данных в других местах?

Публикация/обмен информацией из обработанных данных

- Где публикуется информация / знания?
- Будет ли публикация информации подвергать людей риску?
- Кто является целевой аудиторией публикуемой информации?
- Есть ли у вас контроль над тем, как публикуется информация?

Архивирование

- Где архивируются данные и обработанная информация?
- Архивируются ли исходные данные или только обработанная информация?
- Кто имеет доступ к архиву?
- Каковы условия доступа к архиву?

Удаление

- Когда происходит уничтожение данных?
- Условия удаления?
- Как мы можем убедиться, что все копии удалены?

Примечание для фасилитатора_ки

Это упражнение - хороший способ узнать и оценить контекст цифровой безопасности, практику и процессы участников_ц. Хорошо бы сосредоточиться на этом аспекте, а не ожидать от этого упражнения выработки стратегий и тактик для повышения их цифровой безопасности.

В рамках организационного семинара вы, возможно, захотите обратить внимание на кадровые и административные команды / отделы. Во-первых, во многих организациях, как правило, именно у этих сотрудников_ц не было опыта участия в семинарах по цифровой безопасности, поэтому многие темы и вопросы могут быть для них новыми. Во-вторых, поскольку большая часть их работы является внутренней, они могут не воспринимать свои подразделения как ¨публикующие¨ что-либо. Однако во многих организациях эти

подразделения хранят и обрабатывают большое количество конфиденциальных данных (информация о персонале, зарплаты сотрудников, записи заседаний совета директоров, банковские реквизиты организации и т. д.) – поэтому важно указать на это в ходе семинара.

Обратите внимание и на физические устройства хранения данных. Если есть картотеки, где хранятся печатные копии документов, спросите, где они расположены, и кто имеет к ним физический доступ. Иногда существует тенденция слишком сильно концентрироваться на практике онлайн-хранилищ, упуская при этом возможность сделать более безопасной тактику физического хранения.

Дополнительное чтение (по желанию)

- FTX: перезагрузка безопасности: альтернативные инструменты для нетворкинга и коммуникаций - FTX Safety Reboot: Alternative Tools in Networking and Communications.
- FTX: перезагрузка безопасности, модуль мобильной безопасности
- Electronic Frontier Foundation's Surveillance Self-Defense – Хотя это руководство в основном рассчитано на американскую аудиторию, в нем есть полезные разделы, объясняющие концепции наблюдения и инструменты, используемые для их обхода.
- Front Line Defenders' Guide to Secure Group Chat and Conferencing Tools – полезное руководство по различным безопасным чат- и конференц-сервисам и инструментам, которые соответствуют критериям Frontline Defender о том, что делает приложение или сервис безопасным.
- Mozilla Foundation's Privacy Not Included website – в котором рассматриваются различные политики и практики конфиденциальности и безопасности различных сервисов, платформ и устройств на предмет их соответствия Mozilla´s Minimum Security Standards (минимальным стандартам безопасности Mozilla), которые включают шифрование, обновления безопасности и политики конфиденциальности.

*Картинка с рисунком. На рисунке растения красного цвета

image-1605451259399.png

Image not found or type unknown

Revision #7

Created 24 April 2023 17:49:57 by Kira

Updated 28 July 2023 14:51:15 by Kira