МЕТОДЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ

Рекиш А.О., Шахно Н.В.
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
Шаталова В.В. – канд.техн.наук, доцент
Алексеев В.В. – канд.техн.наук, доцент

Аннотация- В статье рассматриваются основные методы социальной инженерии, а также способы противодействия данным методикам.

Социальная инженерия – метод получения необходимого доступа к информации, основанный на особенностях психологии людей. Основной целью социальной инженерии является получение доступа к конфиденциальной информации, паролям, банковским данным и другим защищенным системам.

Для того, чтобы обезопасить себя от воздействия социальной инженерии, необходимо понять, как она работает. На рисунке 1 представлены основные типы социальной инженерии.

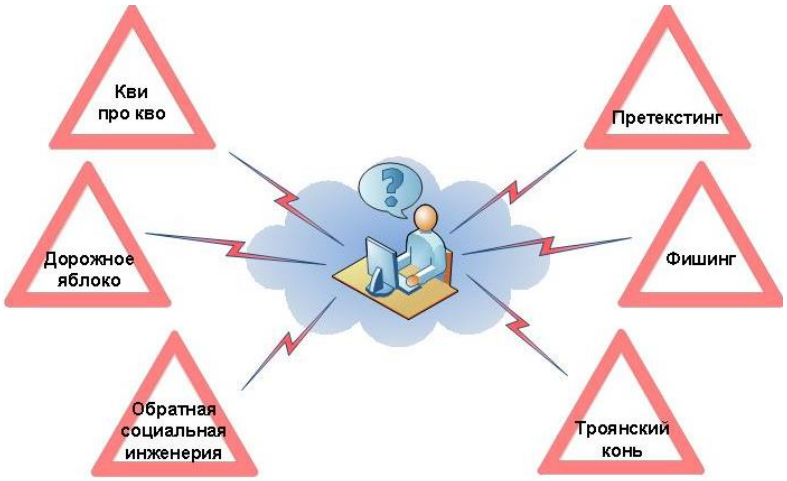

Рисунок 1 – Основные методы социальной инженерии

Претекстинг - это набор действий, отработанных по определенному, заранее составленному сценарию, в результате которого жертва может выдать какую-либо информацию или совершить определенное действие. Чаще всего данный вид атаки предполагает использование голосовых средств, таких как Skype, телефон и т.п.

Для использования этой техники злоумышленнику необходимо изначально иметь некоторые данные о жертве (имя сотрудника; должность; название проектов, с которыми он работает; дату рождения). Злоумышленник изначально использует реальные запросы с именем сотрудников компании и, после того как войдет в доверие, получает необходимую ему информацию.

Фишинг – техника интернет-мошенничества, направленная на получение конфиденциальной информации пользователей. Основным видом фишинговых атак является поддельное письмо, отправленное жертве по электронной почте, которое выглядит как официальное письмо от платежной системы или банка. В письме содержится форма для ввода персональных данных (пин-кодов, логина и пароля и т.п) или ссылка на web-страницу, где располагается такая форма. Причины доверия жертвы подобным страницам могут быть разные: блокировка аккаунта, поломка в системе, утеря данных и прочее.

Троянский конь – это техника основывается на любопытстве, страхе или других эмоциях пользователей. Злоумышленник отправляет письмо жертве посредством электронной почты, во вложении которого находится «обновление» антивируса, ключ к денежному выигрышу или компромат на сотрудника. На самом же деле во вложении находится вредоносная программа, которая после того, как пользователь запустит ее на своем компьютере, будет использоваться для сбора или изменение информации злоумышленником.

Кви про кво (услуга за услугу) – данная техника предполагает обращение злоумышленника к пользователю по электронной почте или корпоративному телефону. Злоумышленник может представиться, например, сотрудником технической поддержки и информировать о возникновении технических проблем на рабочем месте. Далее он сообщает о необходимости их устранения. В

процессе «решения» такой проблемы, злоумышленник подталкивает жертву на совершение действий, позволяющих атакующему выполнить определенные команды или установить необходимое программное обеспечение на компьютере жертвы.

Дорожное яблоко – этот метод представляет собой адаптацию троянского коня и состоит в использовании физических носителей (CD, флэш-накопителей). Злоумышленник обычно подбрасывает такой носитель в общедоступных местах на территории компании (парковки, столовые, рабочие места сотрудников, туалеты). Для того, чтобы у сотрудника возник интерес к данному носителю, злоумышленник может нанести на носитель логотип компании и какую-нибудь подпись. Например, «данные о продажах», «зарплата сотрудников», «отчет в налоговую» и другое.

Обратная социальная инженерия - данный вид атаки направлен на создание такой ситуации, при которой жертва вынуждена будет сама обратится к злоумышленнику за «помощью». Например, злоумышленник может выслать письмо с телефонами и контактами «службы поддержки» и через некоторое время создать обратимые неполадки в компьютере жертвы. Пользователь в таком случае позвонит или свяжется по электронной почте с злоумышленником сам, и в процессе «исправления» проблемы злоумышленник сможет получить необходимые ему данные.

Способы защиты от методов социальной инженерии. Основным способом защиты от методов социальной инженерии является обучение сотрудников. Все работники компании должны быть предупреждены об опасности раскрытия персональной информации и конфиденциальной информации компании, а также о способах предотвращения утечки данных. Кроме того, у каждого сотрудника компании, в зависимости от подразделения и должности, должны быть инструкции о том, как и на какие темы можно общаться с собеседником, какую информацию можно предоставлять для службы технической поддержки, как и что должен сообщить сотрудник компании для получения той или иной информации от другого сотрудника.

Всем сотрудникам в день приема на работу должно быть разъяснено то, что те логины и пароли, которые им выдали, нельзя использовать в других целях (на web-сайтах, для личной почты и т.п), передавать третьим лицам или другим сотрудникам компании, которые не имеют на это право. Например, очень часто, уходя в отпуск, сотрудник может передать свои авторизационные данные своему коллеге для того, чтобы тот смог выполнить некоторую работу или посмотреть определенные данные в момент его отсутствия.

Необходимо проводить вступительные и регулярные обучения сотрудников компании, направленные на повышения знаний по информационной безопасности.

Проведение таких инструктажей позволит сотрудникам компании иметь актуальные данные о существующих методах социальной инженерии, а также не забывать основные правила по информационной безопасности.

Обязательным является наличие регламентов по безопасности, а также инструкций, к которым пользователь должен всегда иметь доступ. В инструкциях должны быть описаны действия сотрудников при возникновении той или иной ситуации.

Например, в регламенте можно прописать, что необходимо делать и куда обращаться при попытке третьего лица запросить конфиденциальную информацию или учетные данные сотрудников. Такие действия позволят вычислить злоумышленника и не допустить утечку информации.

На компьютерах сотрудников всегда должно быть актуальное антивирусное программное обеспечение.

На компьютерах сотрудников также необходимо установить брандмауэр.

В корпоративной сети компании необходимо использовать системы обнаружения и предотвращения атак.

Также необходимо использовать системы предотвращения утечек конфиденциальной информации. Все это позволит снизить риск возникновения фитиновых атак.

Все сотрудники должны быть проинструктированы, как вести себя с посетителями.

Необходимы четкие правила для установления личности посетителя и его сопровождения. Посетителей всегда должен сопровождать кто-то из сотрудников компании. Если сотрудник встречает неизвестного ему посетителя, он должен в корректной форме поинтересоваться, с какой целью посетитель находится в данном помещении и где его сопровождение. При необходимости сотрудник должен сообщить о неизвестном посетители в службу безопасности.

Исходя из всего перечисленного, можно сделать вывод: основной способ защиты от социальной инженерии – это обучение сотрудников. Необходимо знать и помнить, что незнание не освобождает от ответственности. Каждый пользователь системы должен знать об опасности раскрытия конфиденциальной информации и знать способы, которые помогут предотвратить утечку.

Список использованных источников:

1. Методы социальной инженерии. [Электронный ресурс]. //Портал компании A1QA. – Режим доступа: https://www.a1qa.ru/blog/sotsialnaya-inzheneriya-ili-ataki-na-chelovecheskiy-faktor/.

2. Способы защиты от методов социальной инженерии. [Электронный ресурс] .– Режим доступа: https://efsol.ru/articles/social-engineering.html.