УДК 366.636.2

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

студент В. С. МОКЕРОВ, канд. техн. наук, доц. Е. С. БЕЛОУСОВА

(Белорусский государственный университет информатики и радиоэлектроники, Минск)

Автором статьи описан личный опыт обнаружения социальной инженерии при использовании социальных сетей. В статье представлены примеры различные типы атак, описаны их особенности применения, способы и методы противодействия им. Были исследованы последствия реализации данных угроз и их влияние на концепцию национальной безопасности.

Ключевые слова: *социальная инженерия, социальные сети, фишинг, методы зашиты.*

Социальная инженерия в контексте информационной безопасности – психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации [1].

Сайты социальных сетей – платформа обменом сообщениями и представления информации для широкой аудитории (процесс, называемый "публикацией"). Несмотря на то, что в Интернет пространстве существуют тысячи веб-сайтов социальных сетей, по данным Amazon.com по состоянию на 1 сентября 2021 года наиболее посещаемыми социальными сетями считались следующие веб-сайты: Facebook.com (23,17% пользователей Интернета); Blogger.com, (9,25%); MySpace.com (4,45%). Кроме того, необходимо упомянуть еще одну общеизвестную социальную сеть Twitter. Сайты социальных сетей содержат идентифицирующую личность информацию. Таким образом, личная информация пользователей, отображаемая на сайтах социальных сетей, может быть использована в качестве средства социальной инженерии не только против определенного пользователя, но и против информационной безопасности любой организации, с которой это лицо связано. "Захват учетной записи" происходит, когда злоумышленник нарушает установленные меры безопасности, чтобы получить несанкционированный доступ к соответствующей консоли владельца учетной записи; процесс, который можно назвать "взломом". Учетная запись может быть "подделана" злоумышленником, создающим достоверную онлайн-личность. Соединение сотрудника организации, прошедшего процесс авторизации, может быть перехвачено, также возможен подбор идентификационных параметров для аутентификации, в результате чего нарушитель получает доступ к учетным записям пользователя социальной сети.

Если онлайн-идентификация подделана, это увеличивает риск определенного уровня воздействия угроз. Из-за угроз, которые могут скомпрометированы социальными сетями, организации должны разработать и внедрить политику безопасности, которая помогает предотвратить раскрытие любой информации о сети организации, инфраструктуре или информационной безопасности через контент, записанный на веб-сайте социальной сети [2].

На фоне стремительного развития информационных технологий, также стремительно развиваются новые способы нарушений конфиденциальности, целостности и доступности информации. Атаки социальной инженерии направлены не на технологический характер, а психологический. Несмотря на использование цифровых инструментов для нацеливания на компьютерные ресурсы, принцип действия таких угроз мало чем отличается от традиционного мошенничества.

К примеру действия злоумышленников, нацеленные на доверие пожилых людей, с целью их манипуляции и провоцирования помощи родственникам. Что демонстрирует схожесть этих атак со своими цифровыми аналогами, а именно манипуляция слабостям, воздействие на человеческую психологию посредством страха, чувством срочности, вынужденными быстрыми решениями. Иногда выбирается другой вектор воздействия, основанный на предложении вознаграждения.

Хотя в некоторых случаях социальная инженерия может быть не только прямой атакой, она часто используется для создания основы для более сложных атак. Во многих случаях злоумышленники собирают персональные данные для совершения социальной инженирии. Существует несколько типов атак социальной инженерии.

Фишинг, вишинг, смишинг основаны на взаимодействии злоумышленника с жертвой по электронной почте, по телефону или SMS для извлечения конфиденциальной информации. Атаки отличаются изощренностью: от легко узнаваемых мошеннических сообщений до электронных писем, которые едва можно отличить от реальной сделки.

Фишинг с использованием “копья” – аналогично описанному выше, но вместо того, чтобы использовать широкую сеть в надежде на результаты, злоумышленники будут тщательно нацеливаться на высокопоставленных лиц, используя информацию, которой делятся в социальных сетях, или даже информацию, собранную через скомпрометированные учетные записи компаний с более низким уровнем доступа. Скрытый фишинг чрезвычайно трудно обнаружить, что подчеркивает важность обучения руководителей распознавать такие атаки [2].

Baiting тесно связан с фишингом, использует человеческую жадность (финансовые трудности), чтобы вынудить людей расстаться с конфиденциальной информацией для аутентификации. Некоторые имитированные атаки на основе **baiting** вызывают провоцируют агрессивную реакцию жертвы, в результате чего ее легко можно обмануть обещанием вознаграждения, бонусов, подарков.

Использование предлога угрозы вредоносного ПО основано на программах-вымогателях. При угрозе вредоносного ПО злоумышленники заявляют, что система пользователя заражена вредоносным ПО, и предлагают удалить его за определенную плату.

На основе выше сказанного, можно утверждать, что «предлог» используется злоумышленниками с целью создания некомфортной ситуации для жертвы, чтобы и обманом заставить ее предоставить персональную информацию, данные аутентификации и т.д.

Water-holing – тип атаки, которая использует уровень доверия пользователей к определенным веб-сайтам, особенно к профессиональным сообществам, например, к Stack Exchange. Пользователи могут чувствовать себя более комфортно, переходя по ссылке, предоставленной на таком сайте, чем где-либо в Интернете, что позволяет злоумышленникам устанавливать вредоносное ПО на свои устройства или компрометировать данные для входа [3].

Для обеспечения безопасности рекомендовано следовать следующим принципам:

1. Соблюдать бдительность, с подозрением относиться к электронным письмам от неизвестных отправителей, особенно когда они отображают тег внешнего отправителя в бизнес-среде.

2. Проверять данные отправителя, внимательно изучить адрес электронной почты, с которого было получено сообщение. Обязательно следить за незначительными изменениями в правописании, которые можно легко пропустить.

3. Проверять ссылки. Если навести курсор мыши на ссылку в письме, не нажимая на нее, можно увидеть адрес, который также можно проверить. Если есть подозрения, что сообщение от используемой службы (например, Microsoft, Google) легитимно, необходимо открыть страницу поставщиков услуг вручную, войти в систему и проверить уведомления.

4. Избегать автоматической загрузки вложений электронной почты, которые могут представлять собой не только угрозу безопасности при их отправке, а также содержать множество форм вредоносных программ для заражения целевых устройств. Не рекомендуется загружать вложения от неизвестных отправителей.

5. Необходимо помнить, что существует возможность компрометации учетных записей сотрудников, поэтому рекомендуется использовать другие каналы связи для получения подтверждения легитимности полученного письма.

6. Строго соблюдать требования политики безопасности. У большинства организаций есть четкие регламенты действий предотвращения угроз, а также ответственные лица, которым необходимо сообщить о потенциальных угрозах [4].

Исследую данную проблему, необходимо выделить что зачастую последствия социальной инженерии приводят к финансовым проблемам как частных,

так и юридических лиц [5]. Существует возможность реализации угроз социальной инженерии критически важным объектам, в следствии чего будет нанесен существенный ущерб национальной безопасности [6].

ЛИТЕРАТУРА

1. Светлана Собалева. Социальная инженерия. [Электронный ресурс] – Опубл. 06.0.2019 – Режим доступа: https://stekspb.ru/blog/socialnaya-inzheneriya. – Дата доступа: 18.10.2022.
2. Сайты социальных сетей как источник информации [Электронный ресурс] – Режим доступа: https://alexa.com/. – Дата доступа: 19.10.2022.
3. Определение фишинг, использование для доступа к информации. [Электронный ресурс]. – Режим доступа: https://www.phishing.org/what-is-phishing. – Дата доступа: 19.10.2022.
4. Использование различных типов атак для достижения цели. [Электронный ресурс] – Режим доступа: https://www.securityinfowatch.com/cybersecurity/article/21203580/social-engineering-cyberattacks-and-how-theyre-impacting-businesses. – Дата доступа: 18.10.2022.
5. Методы и способы защиты от социальной инженерии. [Электронный ресурс] – Режим доступа: https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack. – Дата доступа: 20.10.2022.
6. Влияние социальной инженерии на бизнес и экономику. [Электронный ресурс] – Режим доступа: https://www.securityinfowatch.com/cybersecurity/article/21203580/social-engineering-cyberattacks-and-how-theyre-impacting-businesses. – Дата доступа: 20.10.2022.
7. Концепция национальной безопасности Республики Беларусь [Электронный ресурс] – Режим доступа: https://pravo.by/document/?guid=3871&p0=P31000575. – Дата доступа: 20.10.2022.