СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК ОДИН ИЗ ОСНОВНЫХ И СЛОЖНЫХ В ОБНАРУЖЕНИИ МЕТОДОВ АТАКИ НА ОБЪЕКТЫ ИНФОРМАТИЗАЦИИ НА ПРЕДПРИЯТИЯ

SOCIAL ENGINEERING AS ONE OF THE MAIN AND DIFFICULT TO DETECT METHODS OF ATTACK ON OBJECTS OF INFORMATIZATION IN ENTERPRISES

УДК 004.056.53

DOI: 10.24411/2658-4964-2021-10339

Курдюков Дмитрий Станиславович, студент, 2 курс, магистр, кафедра КБ-1 «Защита информации», Институт комплексной безопасности и специального приборостроения, РТУ МИРЭА, Россия, г.Москва

Kurdiukov Dmitry Stanislavovich, student, 2 course, magistrature, department CS-1 «Data protection», Institute for Integrated Security and Special Instrument Engineering, RTU MIREA.

Аннотация: В данной статье будет рассмотрена социальная инженерия как один из наиболее эффективных методов атаки на предприятия и их объекты информатизации. В настоящее время на рынке существует бесчисленное множество различного программного обеспечения, а также специализированного оборудования, направленного на обеспечение безопасности информационных систем, а также их персонала. Однако главным недостатком любой системы защиты являются ее пользователи, не ознакомленные или сознательно игнорирующие простейшие правила корпоративной безопасности.

Annotation: In this article, social engineering will be considered as one of the most effective methods of attacking enterprises and their objects of informatization.

Currently, there are countless different software on the market, as well as specialized equipment aimed at ensuring the security of information systems and their personnel. However, the main drawback of any security system is its users who are not familiar with or knowingly ignoring the simplest corporate security rules.

Ключевые слова: информационная безопасность, социальная инженерия, защита информации, предприятия.

Key words: information security, social engineering, information protection, enterprises.

Введение

Социальная инженерия - вид атак, направленных на получения доступа к личным данным или объектам информатизации основанный на манипуляции человеческой психологией. Основной часть социальной инженерии направлена на получения доступа к паролям и учетным записям пользователей на различных ресурсах начиная от социальных сетей заканчивая банковскими аккаунтами или учетными записями в корпоративных сетях.

Виды атак методом социальной инженерии

Социальная инженерия - представляет собой один из немногих методов атак основанный не на технических средствах, однако прекрасно гармонирующий с ними. Многими людьми достаточно легко манипулировать, заставляя их выполнять действия злоумышленников.

В целом действия криминальных группировок средне-низкого уровня за 2019-2021г прослеживается достаточно четко, по информации RT-Solar злоумышленники все чаще используют методы социальной инженерии для проникновения в компанию, однако они были не единственными: 72% - фишинг, 20% - атаки на веб приложение, 3% - компрометация данных, 3% - прочие атаки (Таблица - 1).

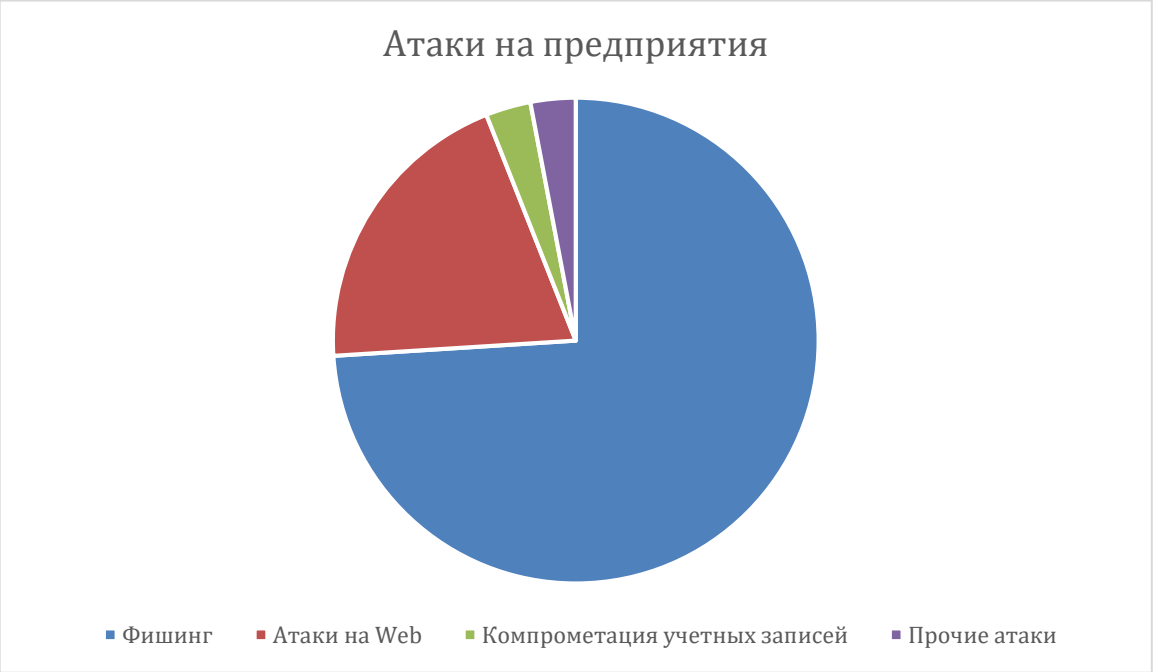

Таблица 1 – статистика атак на предприятия

Большинство современных компаний тратят огромные деньги на закупку и разработку защитных мер и средств, но в то же время работники могут предоставить весь спектр информации для проникновения в систему необходимые злоумышленнику, что избавляет его от необходимости прямого взлома системы.

Социальную инженерию можно поделить на две основные категории:

- Методы, основанные на технологиях: представляющие собой различные сайты обманки и поддельное по, основная цель подобного заставить пользователя поверить, что он взаимодействует с реальной информационной системой и вынудить его предоставить персональные данные.
- Методы, основанные на человеческой психологии: представляющие собой манипуляцию особенностями человеческой психологии связанные с интересом к новой информации или жаждой наживы.

Однако чаще всего эти категории тесно переплетаются между собой и социальную инженерию проще классифицировать по методам атаки.

В качестве основных атак методом социальной инженерии можно выделить следующие:

Фишинг - одна из основных техник мошенничества в интернете направленная на получение данных авторизации пользователей. К самому распространенному методу фишинговой атаки можно отнести поддельные письма, отправляемые жертвам по электронной почте. Подобные письма выглядят как официальные письма от платежных систем банков или других организаций, которым пользователь потенциально доверяет. В подобных письмах могут содержаться формы ввода персональных данных или ссылки на различные web ресурсы имитирующие официальные страницы. Зачастую подобные поддельные письма невозможно с 1го взгляда отличить от их оригинального исполнения, но тем не менее при чуть более внимательном изучении становиться ясно что с ними что-то не так.

Основной причиной доверия у пользователей к подобным письмам может послужить не грамотность в области безопасности или какие-либо технические проблемы в системах с которыми потенциальная жертва могла столкнуться.

Кви про кво (услуга за услугу) - данная техника предполагает собой прямой контакт злоумышленника с жертвой по телефону или электронной почте. Злоумышленник может может представиться , как работник службы технической поддержки и проводить опрос на на наличие технических неполадок на рабочем месте пользователя или системе, либо сообщить о их наличии. Далее злоумышленник сообщает о необходимости устранения найденных неполадок, и в процессе решения подобных проблем подталкивает жертву на совершение действий позволяющий злоумышленнику руками жертвы установить необходимое программное обеспечение или выполнить необходимые команды на компьютере жертвы.

Обратная инженерия - вид атаки схожий с кви про кво. Данный вид атаки направлен на создание ситуаций, в которых жертва сама вынуждена связаться с атакующим. Как пример данная атака может быть реализована следующим образом: Злоумышленник высылает по электронной почте письмо, содержащее контакты вымышленной службы поддержки, и через некоторое время спровоцировать технические проблемы на рабочем месте жертвы. Жертва,

столкнувшись с неполадками с высокой долей вероятности сама свяжется с злоумышленником в надежде получить помощь и зачастую будет готова выполнять инструкции по телефону. Последствием такой технической помощи могут быть практические любые последствие, доверчивая жертва в связи с технической неграмотностью может и не заподозрить что инструкции получаемые с другого конца провода могут привести к ужасным последствиям.

Претекстинг - данная атака чаще всего представляет собой звонки с использованием программного обеспечения для видеоконференций или обычного телефона. Для успешной реализации данной атаки необходима предварительная разведка, злоумышленнику необходимо знать как можно больше данных о своей жертве таких как (имя, дату рождения, названия проектов над которыми она работает, название отделов, а также имена начальников и других сотрудников отдела). Оперируя данной информацией, злоумышленник входит в доверие к потенциальной жертве и вынуждает жертву поделиться какой-либо информацией, интересующей атакующего.

Троянский конь - данная техника целиком основывается на любопытстве пользователей. Атака методом троянского коня схожа с фишингом и также подразумевает отправку жертве сообщения с вирусным вложением или ссылкой на него и каким-либо заманчивым сообщением его открыть. Это может быть уведомление о выигрыше лотереи или предложение обновить антивирус. Доверчивый пользователь может запустить это приложение тем самым предоставив злоумышленнику доступ к своей системе.

Атака на водопое - основываясь не на заражении как можно большего количества машин, а на повышении вероятности заражения. Атакующий пользуется доверием жертв к самым часто посещаемым сайтам и в случае присутствия на них уязвимостей производит модификацию сайта добавляя различные эксплойты, которые впоследствии будут выполнены на компьютерах пользователей для установки вредоносного программного обеспечения.

Дорожное яблоко - один из наиболее проблемных методов для различных организаций, имеющих какие-либо общедоступные помещения, такие как

столовые, парковки или туалеты. Атака подразумевает собой использование физических носителей, в частности флеш накопителей. Злоумышленник подбрасывает накопитель с вредоносным по в подобные места, а для стимуляции интереса может нанести на флеш накопитель какие-либо пометки в виде логотипов компаний или различных подписей.

Реализация атак методом социальной инженерии по этапам

Действия хакеров можно условно разделить на этапы:

- Проведение первичной разведки:

В течении последних 10 лет активное развитие получают социальные сети и различные мессенджеры плотно вошли в обиход большого числа людей чем и пользуются злоумышленники. Подавляющее большинство работников крупных компаний являются активными пользователями мессенджеров и социальных сетей. Многие из них публикуют фотографии и различные записи, которые выглядят мало информативными, однако могут послужить ключом для запуска и реализации успешной атаки. В качестве подобной информации могут выступать: фотографии, различная информация о пользователях, геоданные.

По отдельности подобные данные могут и не представлять особой опасности, однако сгруппировав их злоумышленник сможет получить четкое представление о делах интересующего его человека.

Современная сеть интернет устроена таким образом что из нее практически невозможно удалить информацию, вся попадающая в нее информация очень быстро распространяется между людьми и сайтами, а также проходит резервное копирование. Также опасность представляют программы-черви, активно распространяемые в них, подобные программы создают заманивающие публикации от имени зараженных пользователей.

- Развитие доверительных отношений

После окончания первичной разведки и получения инсайдерской информации обычно пытаются наладить контакт с лицом, имеющим доступ к полезным ресурсам. Целью подобных действий служит манипуляция над психологической склонностью человека доверять более авторитетным лицам.

Злоумышленник может выдать себя за авторитетное лицом в какой-либо сфере интересной жертве, и пользуясь этим попытаться получить пароли пользователя и доступ к его сессиям.

- Использование и эксплуатация отношений

На данном этапе злоумышленник ставит перед собой целью закрепить авторитет перед жертвой. И по средствам манипуляции привести ее в выгодное ему эмоциональное состояние. Подобную манипуляцию можно использовать для:

Получения персональной информации или доступа в закрытые помещения;

Для манипуляции другими лицами;

Представления социального инженера другим членам организации как доверенного и авторитетного лица.

- Реализация атаки

На последнем этапе происходит непосредственная реализация внезапной атаки. Хорошо реализованной атакой считается та, что оставляет у жертвы ощущение правильно совершенных действий, подобное дает окно для реализации последующих атак.

Рекомендации по противодействию

Поскольку атаки социальной инженерии как никогда актуальны, были разработаны четкие инструкции для персонала по противодействию ей:

1. Никогда не верьте на слово в телефонных или VoIP звонках. Даже если вам звонят по внутреннему телефону и представляется сотрудником тех. Поддержки или каким-либо другим сотрудником. Необходимо проверять каждый номер с базой номеров организации правда ли это человек является тем кем представился.

2. Никогда никому не сообщайте или присылайте свой пароль ни под каким предлогом, даже если это прямое требование начальника или от этого зависит выполнение важной задачи. Вы должны четко осознавать все риски, связанные с утечкой корпоративных данных.

3. Никогда не используйте на рабочем устройстве личные или не знакомые носители информации, если вы принесли с собой или нашли незнакомое

устройство или носитель информации отнесите его в IT отдел где его совместно с вами проверят на наличие угроз и откроют на изолированном устройстве, в случае подтверждении безопасности устройства вам будет выдано разрешение на его использование или поиск потерявшего его лица.

4. Всегда проверяйте отправителей электронных писем и ни в коем случае не открывайте их если они пришли с незнакомого вам адреса. Подобные письма могут иметь зазывающие заголовки или интересные вам вложения, ни в коем случае не открывайте их в них могут быть вирусы. Сообщите о подобном письме IT отделу и службе безопасности.

5. Вы должны использовать уникальные пароли в разных системах. Пароли должны быть действительно уникальны поскольку поскольку если пароли частично совпадают сильно повышается шанс того, что злоумышленники смогут подобрать пароль, если же вам сложно запоминать пароли используйте менеджеры паролей. Однако используйте разные менеджеры и мастер пароли для рабочих и нерабочих целей.

6. Никогда не открывайте двери незнакомым людям, каждый посетитель должен быть в сопровождении официально представленного к нему сотрудника.

7. Никогда не открывайте двери даже знакомым людям. Даже знакомые вам сотрудники могут представлять опасность, поскольку они могут быть на данный момент уволены и в целях мести планировать инсайдерскую атаку. В случае же если вы или кто-либо другой забыли пропуск в своем кабинете, необходимо связаться с начальником или службой безопасности для разрешения данной ситуации.

Заключение

В данной статье была рассмотрена социальная инженерия как один из основных и наиболее опасных методов атаки на информационные системы.

Были рассмотрены виды атак методом социальной инженерии, а также этапы реализации атаки, на основании которых стало возможно проработать рекомендации для рядового персонала соблюдение которых позволит в разы

снизить шансы на проникновение в систему и позволит службе безопасности сконцентрировать свое внимание на более технически сложных источниках угроз.

Литература

1. Искусство обмана. Социальная инженерия в мошеннических схемах // Хэднеги Кристофер: Альпина Паблишер,2020.
2. В.Г. Грибунин, В.В. Чудовский. Комплексная система защиты информации на предприятии: учеб. пособие для студ. высш. учеб. заведений // – М.: Издательский центр «Академия», 2009.
3. Общий ресурс компании EFSOL. Статья - Социальная инженерия как не стать жертвой. [Электронный ресурс]. URL:https://efsol.ru/articles/social-engineering.html - (дата обращения: 04.2020)
4. Общий ресурс habr.com. Статья - Социальная инженерия как метод атаки. [Электронный ресурс]. URL:https://habr.com/ru/post/348496/ - (дата обращения: 04.2020)
5. Общий ресурс habr.com. Статья - Исследование атак со стороны профессиональных кибергруппировок: смотрим статистику техник и тактики. [Электронный ресурс]. URL:https://habr.com/ru/company/solarsecurity/blog/530674/ - (дата обращения: 04.2020)
6. В.Г. Грибунин, В.В. Чудовский. Комплексная система защиты информации на предприятии: учеб. пособие для студ. высш. учеб. заведений // М.: Издательский центр «Академия», 2009.

Literature

1. The art of deception. Social engineering in fraudulent schemes // Hadnegie Christopher: Alpina Publisher, 2020.
2. V.G. Gribunin, V.V. Chudovsky. Integrated information security system at the enterprise: textbook. manual for stud. higher. study. institutions // - M.: Publishing Center "Academy", 2009.

3. General resource of the EFSOL company. Article - Social engineering how not to become a victim. [Electronic resource]. URL: https: //efsol.ru/articles/social-engineering.html - (date accessed: 04.2020)
4. The general resource habr.com. Article - Social engineering as a method of attack. [Electronic resource]. URL: https: //habr.com/ru/post/348496/ - (date accessed: 04.2020)
5. General resource habr.com. Article - Investigation of attacks from professional cyber groups: we look at the statistics of techniques and tactics. [Electronic resource]. URL: https: //habr.com/ru/company/solarsecurity/blog/530674/ - (date accessed: 04.2020)
6. V.G. Gribunin, V.V. Chudovsky. Integrated information security system at the enterprise: textbook. manual for stud. higher. study. institutions // M .: Publishing Center "Academy", 2009.