- бизнеса): сб. научных трудов 15-й междунар. науч.-практ. конф. (Москва, 3-4 февраля 2015 г.) / под ред. Чистова Д.В. – М.: ООО «IC-Публишинг», 2015. – Ч. 1. – С. 7-20.
5. Загорная Т.О. Повышение эффективности функционирования социально-ориентированных рынков через механизм партнерства / Т.О. Загорная, Ю.А. Кобзева // Стратегия устойчивого развития в антикризисном управлении экономическими системами. 2016. №2. С. 262–267.
  6. Кадочников С.М. Система высшего профессионального образования и развитие человеческого капитала в российской экономике: необходимость реформ / С.М. Кадочников // Доклады школы экономического анализа. 2015. №4. URL: <http://conf-expert.urfu.ru/blind/2015/docs/>.
  7. Каплан Р.С., Нортон Д.П. Сбалансированная система показателей. От стратегии к действию / пер. с англ. М.: ЗАО «Олимп-Бизнес», 2003.
  8. Морозова И.А., Мысин М.Н., Грязнов С.А. Концепция развития образовательных учреждений (в рамках модернизации системы российского образования) // Материалы междунар. научно-практ. конф. "21 век: фундаментальная наука и технологии" (г. Москва, 24-25 декабря 2012 г.)
  9. Морозова И.А., Мысин М.Н. О необходимости формирования инновационных подходов в рамках модернизации системы образования // Экономика и менеджмент систем управления. 2013. №4.
  10. Официальный сайт Министерства образования и науки Российской Федерации: <http://минобрнауки.рф/>

Самойлова А.А.

Методы социальной инженерии

*Южно - Уральский Государственный университет
(Россия, Челябинск)*

doi: 10.18411/lj-11-2019-48

idsp: ljjournal-11-2019-48

Аннотация

В данной статье рассматриваются 5 способов несанкционированного получения конфиденциальной информации и способы защиты от взлома.

Ключевые слова: социальная инженерия; фишинг; троянский конь; претекстинг; кви про кво; несанкционированный проход.

Abstract

The article considers the 5 methods of illegal getting confidential information and ways to protect against hacking.

Keywords: social engineering; fishing; trojan horse; pretexting; qui pro quo; tailgating

Введение. Для обозначения психологических техник получения важной информации, в интернете используют понятие социальная инженерия. Данный метод заключается в использовании слабостей человеческого фактора, таких как торопливость, невнимательность, альтруизм, алчность или страх перед официальным учреждением, с целью незаконного получения личной информации (персональных или финансовых данных) или несанкционированного доступа к компьютеру жертвы с целью установки на него вредоносного ПО. Как известно, человек, т.е. пользователь ПК в нашем случае, – это самое слабое звено защиты, намного уязвимее, чем сама система. Поскольку с помощью данного метода гораздо проще получить учетные данные, нежели путем взлома системы безопасности, злоумышленники прибегают именно к подобной практике.

Актуальность темы исследования заключается в том, что в современных условиях становится все менее возможным сохранить какие-либо данные конфиденциальными. По данным InfoWatch, мировой объем утечек информации в 2017 г. увеличился более чем в четыре раза [1]. Поскольку сейчас все больше данных хранится в сети Интернет, то обеспечение безопасности личных данных особенно важно.

Целью работы является изучение основных и самых популярных техник социальной инженерии.

Задачами исследования являются изучение основных типов социальной инженерии и методов защиты от них.

Общим принципом всех атак является введение жертвы в заблуждение. Для этого могут использоваться различные тактики, направленные на эмоции, слабости или иные особенности личности:

- Неопытность
- Страх перед начальством
- Жадность и желание быстрых результатов
- Сочувствие и жалость
- Любовь
- Лень

Много результатов обычно дает и анализ социальных сетей: ВК, Twitter, Facebook, «Одноклассники», Tumblr, LinkedIn и прочие. Все они позволяют указать место рождения, место жительства, место работы/учебы и т.д., по которым и будет совершен поиск. Существует множество средств для анализа информации из социальных сетей, например, `linkedin_profiles.py`, `corpint` или `aleph data`.

Также не стоит забывать и Instagram, где возможен поиск по геолокации. Если известно, например, где расположена компания, то можно посмотреть фотографии, которые делают сотрудники на своем рабочем месте. Например, попадают кадры с экранами мониторов, а на них — внутренние номера и почтовые адреса, иконки программ, которые весьма облегчают взлом информации.

Для того, чтобы обезопасить себя от воздействия социальной инженерии, следует понимать, как это работает. Рассмотрим основные типы социальной инженерии [2].

Фишинг

Фишинг-атаки — это самый популярный вид мошенничества в социальной инженерии. Целью фишинга является незаконное получение конфиденциальных данных пользователей (логина и пароля). Для атаки пользователей злоумышленники используют электронную почту, предварительно собрав из открытых источников список работников компании и их имейл-адреса. После сбора адресов хакеры переходят к подготовке письма с полезной нагрузкой.

Полезная нагрузка, как правило, может быть двух типов:

1. Поддельная страница корпоративного ресурса, которая используется для кражи паролей пользователей корпоративной сети.
2. Вредоносный офисный документ.

Для создания поддельной страницы злоумышленники копируют HTML- и JavaScript-код оригинального корпоративного ресурса и добавляют изменения, которые позволяют получать пароль и логин, вводимые пользователями.

В офисные файлы, как правило, добавляют вредоносный код, который выполняется при открытии. Для добавления кода используют стандартную функцию Microsoft Office — создание макросов. Запущенный документ скачивает исполняемый файл, который заражает рабочую машину пользователя и предоставляет взломщикам удаленный доступ для кражи информации.

Троянский конь

Эта техника использует такие качества потенциальной жертвы, как любопытство и алчность. Социальный инженер отправляет e-mail с бесплатным видео или обновлением антивируса во вложении. Жертва сохраняет вложенные файлы, которые на самом деле являются троянскими программами. Такая техника останется

эффективной до тех пор, пока пользователи продолжают бездумно сохранять или открывать любые вложения.

Помимо вложений злоумышленники могут использовать USB-устройства (накопители и другую периферию).

В таком случае, злоумышленники подбрасывают жертве цифровые носители (например, флешки) в публичных местах, на стоянке или у входа в здание. На флэш-накопитель записывается программа, осуществляющая кражу конфиденциальных данных или сети при ее открытии. Вредоносное ПО находится внутри Excel, Word или PDF файлов, обычно помещаемых на такие носители, а сами файлы именуются надписями, которые привлекают внимание, такими как: «Строго конфиденциально», «Прайс-лист», «Бухгалтерская отчетность» и т.д.

Претекстинг

Претекстинг – это атака, проводимая по заранее подготовленному сценарию. Такие атаки направлены на развитие чувства доверия жертвы к злоумышленнику. Атаки обычно осуществляются по телефону. Этот метод зачастую не требует предварительной подготовки и поиска данных о жертве. Для получения информации, обычно, входят в доверие, используются небольшие запросы и упоминаются имена реальных людей в организации, представляются третьим лицом или сообщают, что кто-то нуждается в помощи, которая, как правило, не вызывает подозрений. Как только доверительная связь установлена, злоумышленник может попросить что-то более глобальное и с наибольшим успехом.

Кви про кво

При использовании этого вида атаки злоумышленники обещают жертве выгоду в обмен на факты. Например, злоумышленник звонит в компанию, представляется сотрудником технической поддержки и предлагает установить «необходимое» программное обеспечение. После того, как получено согласие на установку программ, нарушитель получает доступ к системе и ко всем данным, хранящимся в ней.

Tailgating

Tailgating или piggybacking подразумевает несанкционированный проход злоумышленника вместе с законным пользователем через пропускной пункт. Такой способ невозможно применять в компаниях, где сотрудникам необходимо использовать пропуски для входа на территорию предприятия.

Очевидно, что социальная инженерия может нанести огромный ущерб любой организации. Именно поэтому необходимо принимать все возможные меры, для предотвращения атак на человеческий фактор.

Рекомендации по защите от атак социальной инженерии

Рекомендуется соблюдать следующие правила защиты, чтобы не стать очередной жертвой злоумышленников:

- использовать разные пароли для доступа к внешним и корпоративным ресурсам;
- не открывать письма, полученные из ненадежных источников;
- блокировать компьютер, когда покидаете рабочее место;
- установить антивирус;
- ознакомиться с политикой конфиденциальности вашей компании;
- проинструктировать всех сотрудников, как вести себя с клиентами и что следует делать при обнаружении незаконного проникновения;
- обсуждать по телефону и в личном разговоре только необходимую информацию;
- необходимо удалять все конфиденциальные документы с портативных устройств.

Заключение. Технические средства контроля могут и должны быть использованы для предотвращения нежелательных утечек информации с помощью

методов социальной инженерии. В первую очередь, фишинг-атаки контентно-центрированы и использование стандартных систем предотвращения утечек информации может оказать огромную услугу в раннем обнаружении и блокировке подобных попыток изменения чувствительных данных. Средства контроля съемных носителей и внешних устройств могут защитить интеллектуальную собственность организации только в том случае, если кто-то из ее сотрудников стал случайной жертвой подброшенного устройства с интересным содержимым.

Однако, самым эффективным методом будет программа обучения вопросам информационной безопасности. Сотрудники должны иметь в виду, что электронная почта компании предназначена для ведения бизнеса, тем самым ограничивая возможное попадание адресов электронной почты пользователей в Интернет. Сотрудники также должны быть внимательны при работе с вложениями из неизвестных источников. Организации также должны иметь формальную политику для использования социальных сетей, запрещающую или ограничивающую информацию, которую сотрудники могут размещать на своих личных страницах. Сайты социальных сетей представляют собой отличный инструмент для использования социального инжиниринга. Приведенные в порядок данные о компании, размещенные сотрудниками на сайтах социальных сетей, будут способствовать повышению уровня общей информационной безопасности компании.

***

1. Ведомости // <https://www.vedomosti.ru/finance/blogs/2018/09/25/781952-izbezhat-utechki-personalnoi/> [Электронный ресурс]. – Дата обращения 12.05.2018.
2. Социальная инженерия. Основные типы социальной инженерии // <https://efsol.ru/articles/social-engineering.html/> [Электронный ресурс]. – Дата обращения 12.05.2018.
3. Методы социальной инженерии или атаки на человеческий фактор // <https://www.a1qa.ru/blog/sotsialnaya-inzheneriya-ili-ataki-na-chelovecheskiy-faktor/> [Электронный ресурс]. – Дата обращения 12.05.2018.

Семенова А.Н., Аджиев Н.Д., Чочиева А.Н.

Сравнение современных методов детектирования объектов на изображении

СКГА

(Россия, Черкесск)

doi: 10.18411/lj-11-2019-49

idsp: ljournal-11-2019-49

Аннотация

В современном мире системы видеонаблюдения становятся важной частью инфраструктуры городов и предприятий. Под системой видеонаблюдения понимается комплекс программных и аппаратных средств получения и анализа видео для помощи в принятии решения человеком. В настоящее время в большинстве случаев системы видеонаблюдения используются для видеофиксации событий с целью последующего анализа и разбора человеком-оператором, например, после возникновения какой-либо внештатной ситуации. Текущий уровень развития алгоритмов компьютерного зрения позволяет автоматизировать получение ответов на эти вопросы для ряда важных практических сценариев. Достижения в решении задач выделения автомобилей на дороге и их идентификации по номерному знаку позволили создать систему автоматической фиксации нарушений правил дорожного движения, принуждающую водителей им следовать. В последние несколько лет были разработаны эффективные алгоритмы выделения лиц людей в видео и идентификации человека по изображению лица.

Ключевые слова: алгоритмы, объекты, модель, методы, нейронные сети