УДК 004.056
DOI: 10.33764/2618-981X-2019-6-2-33-38

ТИПОВОЙ АЛГОРИТМ ВОЗДЕЙСТВИЯ В СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Роман Олегович Максименко
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант, тел. (913)063-99-52, e-mail: max_roma96@inbox.ru

Полина Александровна Звягинцева
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, ст. преподаватель кафедры информационной безопасности, тел. (383)343-91-11, e-mail: polina11-03@mail.ru

Описываются понятия и цели социальной инженерии. В статье приведен общий подход к атаке с использованием социальной инженерии. Описаны основные области применения социальной инженерии. Рассмотрены цели применения социальной инженерии в области конкурентной разведки. Сформулирован типовой алгоритм взаимодействия в социальной инженерии. Рассматривается понятие аттракции. Типовой алгоритм взаимодействия включает в себя формирование цели воздействия, сбор информации об объекте, создание нужных условий для воздействия на объект, принуждение к нужному действию.

Ключевые слова: социальная инженерия, атака, типовой алгоритм, аттракция, информационная безопасность, конфиденциальная информация, сбор информации, угрозы.

TYPICAL IMPACT ALGORITHM IN SOCIAL ENGINEERING

Roman O. Maksimenko
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, phone: (913)063-99-52, e-mail: max_roma96@inbox.ru

Polina A. Zviagintseva
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Senior Lecturer, Department of Information Security, phone: (383)343-91-11, e-mail: polina11-03@mail.ru

Concepts and goals of social engineering are described. The article presents a general approach to attack using social engineering. The main application areas of social engineering are described. Objectives of social engineering application in the field of competitive intelligence are considered. Typical interaction algorithm in social engineering is formulated. The concept of attraction is considered. The typical interaction algorithm includes the formation of the goal of exposure, collection of information about the object, creation of necessary conditions for impact on the object, coercion to desired action.

Key words: social engineering, attack, typical algorithm, attraction, information security, confidential information, information gathering, threats.

Введение

Цифровые технологии изменили наши представления о безопасности и конфиденциальности. Полагаясь на разработчиков, создающих инструменты, которые помогают предотвратить большое количество уязвимостей сети, мы

забываем о том, что самым большим врагом безопасности остается сам человек, точнее, допускаемые им ошибки. Именно эти ошибки использует социальная инженерия, чтобы завладеть ценными данными, причем преступники получают эту информацию с нашего же согласия.

Самое слабое звено защиты любой системы – пользователи. Социальная инженерия пытается использовать присущие людям слабости, например, торопливость, алчность, альтруизм или страх перед официальным учреждением, в целях получения конфиденциальной информации и последующего доступа в систему.

Социальная инженерия представляет собой вид атаки, которая опирается на взаимодействие людей и часто сопровождается манипулированием этими людьми в нарушение нормальной процедуры безопасности и является обычной практикой в целях получения доступа к системам, сетям или получения финансовой выгоды.

Социальная инженерия применяется с целью побудить человека выполнить конкретные действия, которые без определенного влияния он никогда бы не стал выполнять, например, передача конфиденциальной информации третьим лицам. Социальная инженерия основывается на факте – человек самое слабое звено системы безопасности, в частности, информационной. Исходя из этого, в случае, если получение конфиденциальной информации, используя технические и физические способы добычи информации, становится слишком дорогостоящим, то гораздо легче и менее ресурсоемко воспользоваться методами социальной инженерии для достижения цели.

Социальная инженерия применяется:

- для сбора сведений о цели;
- получения конфиденциальной информации;
- прямого доступа к системе;
- получения данных, которые иначе достать невозможно.

В сфере информационной безопасности термин «социальная инженерия» используется для описания науки и искусства психологической манипуляции. По статистике [1–4], 55 % убытков, связанных с нарушениями информационной безопасности, возникают по вине сотрудников, подвергшихся влиянию социальных инженеров.

Особенности атак на человеческий фактор:

- не требуют значительных затрат;
- не требуют специальных знаний;
- могут продолжаться на протяжении длительного срока;
- сложно отслеживаются.

Человек, зачастую, намного более уязвим, чем система. Именно поэтому социальная инженерия направлена на получение информации при помощи человека, особенно в тех случаях, когда невозможно получить доступ к системе (например, компьютер с конфиденциальной информацией не имеет доступа в локальную сеть).

Общий подход к атаке:

- сбор информации о жертве (зачастую через социальные сети);
- установление доверительных отношений;
- эксплуатация;
- сокрытие следов пребывания.

Общий принцип всех атак – введение жертвы в заблуждение. Для этого могут использоваться различные тактики, направленные на эмоции, слабости или иные особенности личности:

Основные области применения социальной инженерии

Область применения социальной инженерии не ограничивается телефонными звонками жертвам с целью получения какой-либо конфиденциальной информации посредством выдачи себя за другое лицо. Область применения социальной инженерии гораздо шире.

Можно выделить следующие области применения социальной инженерии:

- общая дестабилизация работы организации с целью снижения ее влияния и возможностью последующего полного разрушения организации;
- финансовые махинации в организациях;
- фишинг и другие способы кражи паролей с целью доступа к внутренним системам;
- проникновение в сеть организации для дестабилизации работы основных узлов сети с какой-либо целью;
- конкурентная разведка.

В области конкурентной разведки можно также выделить следующие цели:

- воровство клиентских баз данных;
- получение общей информации об организации, ее сильных и слабых сторонах, с целью последующего деструктивного воздействия на организацию тем или иным способом;
- получение информации о наиболее перспективных сотрудниках с целью их дальнейшего «переманивания» в свою организацию;
- получение информации о маркетинговых планах [1–3].

Типовой алгоритм взаимодействия в социальной инженерии

Типовой алгоритм воздействия в социальной инженерии включает в себя:

- формулирование цели воздействия на тот или иной объект;
- сбор информации об объекте, с целью обнаружения наиболее удобных мишеней воздействия;
- на основе собранной информации реализуется этап, который психологи называют аттракцией, подразумевая под этим термином создание нужных условий для воздействия на объект;
- принуждение к нужному для социального инженера действию.

На рисунке представлена схема алгоритма взаимодействия в социальной инженерии.

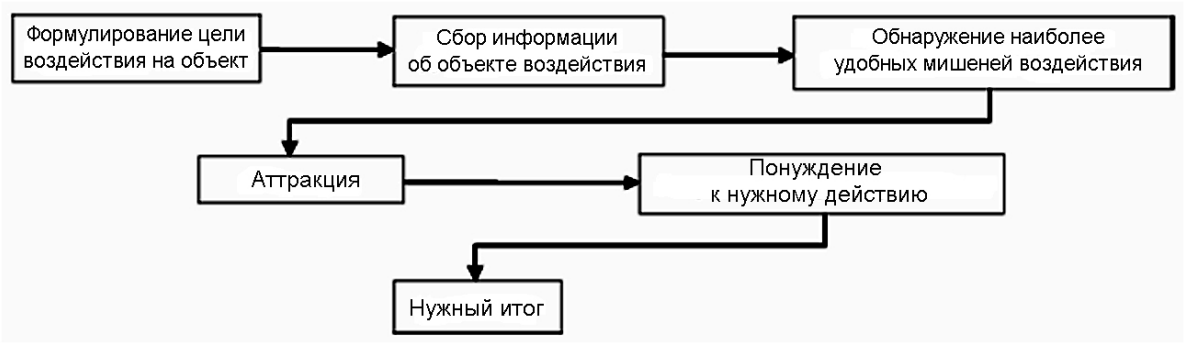

Схема алгоритма взаимодействия в социальной инженерии

Как уже было сказано ранее, основной целью социальной инженерии является получение доступа к конфиденциальной информации, паролям, банковским данным и другим защищенным системам. То есть следует сформулировать, что необходимо получить от объекта атаки, для дальнейшего построения вектора атаки.

На этапе сбора информации основными источниками являются общедоступная информация и социальные сети. Социальная сеть представляет собой интернет-ресурс, предназначенный для обмена текстовыми сообщениями, медиаресурсами (фото-, аудио-, видеоинформация) и другими видами информации.

Желание поделиться своей радостью (знаменательные даты, события), успехами, а зачастую и обычное хвастовство заставляет человека отключить разумную часть своего сознания и не контролировать содержание выдаваемой им собственноручно информации при общении в социальных сетях. Анализ представленной человеком информации в социальных сетях позволяет злоумышленнику, часто без особого труда, составить его морально-психологический портрет, узнать об увлечениях, семейном положении, обычаях, запланированных мероприятиях. Полученная в результате сбора и обработки информация из социальных сетей является исходной в проведении атак рассмотренными в статье методами [4–6].

Значительным достижением для социального инженера будет получение необходимой ему информации через социальные сети. В этом случае, как правило, дальнейшее изучение человека, тем более применение других методов социальной инженерии, вообще не требуется.

Аттракция – это создание нужных условий для воздействия на объект. Аттракция означает «притяжение» одного человека к другому. Она включает в себя:

- привлечение и удержание внимания;
- привлечение определенного интереса;
- расположение к собеседнику;
- уважение партнера.

Аттракция представляет собой притяжение личностей в физическом смысле, в некотором роде, тенденция к объединению. Аттракция включается такую форму восприятия индивидуумом другого индивидуума, которая основывается на формировании эмоционально устойчивого положительного чувства друг к другу.

Принуждение объекта воздействия к выполнению необходимых для социального инженера действий достигается успешным выполнением предыдущих этапов. Если объект воздействия относится к социальному инженеру достаточно лояльно, то не возникает трудностей заставить объект выполнять необходимые действия. Но в ряде случаев, бывает, что жертва достаточно подготовлена и психологически устойчива, в таком случае социальный инженер может прибегнуть к более агрессивным способам воздействия на жертву, например, прямой подкуп, психологическое давление и так далее [7–10].

Заключение

Получение несанкционированного доступа к информации с помощью применения социальной инженерии составляет около 70 % от всех атак [10]. Это связано, в первую очередь, с человеческим фактором и сотрудниками, которые не соблюдают политику безопасности, принятую в организации. Можно сделать вывод, что социальная инженерия – это достаточно мощный инструмент в руках злоумышленника, и защита от данного вида атак является одним из главных компонентов построения комплексной защиты. Социальная инженерия является быстрым и простым путем получения конфиденциальной информации и достаточно сложным в обнаружении. Защититься от данного вида атак невозможно, используя только технические или физические средства защиты. Необходимо проводить регулярное обучение сотрудников, проверять соблюдение выполнения принятой политики безопасности и проводить регулярный аудит безопасности, включающий в себя проверку персонала на устойчивость к атакам социальной инженерии.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Основные виды атак социальной инженерии / Ананьин Е. В., Кожевникова И. С., Лысенко А. В., Никишова А. В., Мартынова Л. Е., Назарова К. Е., Попков С. М., Белозерова А. А. // Молодой ученый. – 2017. – №1. – С. 15–17.

2. Гафарова Я. К., Герасимов В. В., Гарипов И. М. Социальная инженерия // Научное сообщество студентов: Междисциплинарные исследования: сб. ст. по мат. LI междунар. студ. науч.-практ. конф., 2018, № 16 (51). – С. 22–27.

3. Кузнецов М. В. Социальная инженерия и социальное хакерство. – СПб. : БХВ-Петербург, 2007. – 368 с.

4. Краткое введение в социальную инженерию [Электронный ресурс]. – Режим доступа: https://habr.com/post/83415/ (дата обращения: 17.02.2019).

5. Fagone, Jason. «The Serial Swatter». New York Times. Retrieved 25 November 2015. – 32 с.

6. Christopher Hadnagy, Paul Ekman. Unmasking the Social Engineer: The Human Element of Security. – San-Francisco: Wiley, 2014. – 256 с.

7. Peter Kim. The Hacker Playbook: Practical Guide To Penetration Testing. – New York: Kindle Edition, 2014. – 149 с.

8. Kevin D. Mitnick, The Art of Intrusion. The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers. – John Wiley & Sons Limited, 2008. – 261 с.

9. Кевин Д. Митник. Призрак в Сети. Мемуары величайшего хакера / Кевин Д. Митник, Уильям Л. Саймон. – М. : Эксмо, 2012. – 321 с.

10. Christopher Hadnagy. Social Engineering. The Art of Human Hacking. – John Wiley & Sons Limited. 2014. – 358 с.