УДК 304.444 DOI: 10.18698/2541-8009-2019-06-494

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ: ВЧЕРА, СЕГОДНЯ, ЗАВТРА

К.А. Балакин balakinka@student.bmstu.ru
SPIN-код: 6184-5181

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Одной из наиболее актуальных тем в современном мире является проблема защиты информации. Существует превеликое множество способов хищения данных пользователя. В данной статье рассмотрены основные этапы истории формирования такого явления современности, как социальная инженерия. Проанализированы основные ее техники и способы защиты о них. Показано, что современная информационно-коммуникативная среда и технический прогресс являются безграничными источниками, порождающими новые виды и техники социального взлома. Описан потенциальный сценарий дальнейшего развития данной науки, обусловленного переходом от индустриального к информационному строю общества.

Ключевые слова

Социальная инженерия, защита информации, личная информация, человеческий фактор, схема воздействия, технологии социальной инженерии, техники социальной инженерии, безопасность пользователя

Поступила в редакцию 05.06.2019

Введение. Сегодня понятие социальной инженерии, впервые примененное американским социологом Роско Паундом в своем прямом значении, настолько обширно, что едва ли можно дать одно наиболее четкое определение. То, что раньше называлось одним словом «инженерия», сегодня является социальным конструированием, проектированием, а также одновременно анализом с использованием социальных конструктов. Однако из всего множества определений можно выделить одно, наиболее четко описывающее суть данного понятия в контексте информационной безопасности: Социальная инженерия — совокупность подходов прикладных социальных наук, приемов и технологий, ориентированных на создание организационных структур для регулирования и управления действиями человека. Это созидательная функция социологии и методология практики управления, сформированная на базе психологии вариативности принятия решений людьми и теоретических оснований социальной организации общества [1].

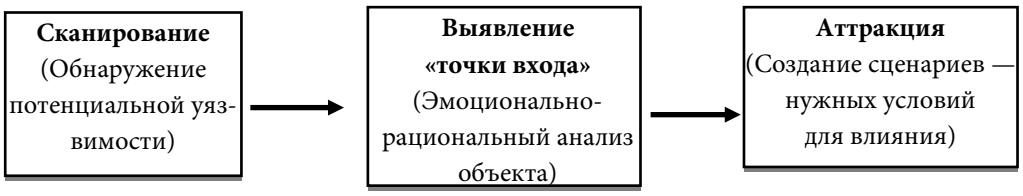
Несмотря на то что социальная инженерия как самостоятельная отрасль формирующегося научного знания сформировалась лишь в прошлом веке, люди пользуются ее методами с древних времен. Так, в IV в. до н. э. на острове Сицилия начало развиваться ораторское искусство, получившее распространение в Афинах уже в V в. до н. э. [2]. Основными направлениями стали: политическое красноречие, прославленное именем Фемистокла; судебное красноречие; торжественное красноречие (здесь был особенно искусен Горгий).

Риторы (профессиональные ораторы), выступая от имени менее разговорчивых представителей власти, вели важные для страны переговоры и, мастерски подмешивая в свои слова лесть, выгодные аргументы и, конечно же, ложь, убеждали оппонента в его неправоте, чем в корне устраняли несогласия сторон, предотвращая потенциальные конфликты.

Неудивительно, что такой действенный способ манипуляции никуда не исчез, а наоборот, стремительно развивался вместе с человечеством. Схемы обмана становились все изощреннее и запутаннее. Однако они все еще требовали физического присутствия злоумышленника, что существенно повышало риск быть пойманным. Так продолжалось до тех пор, пока в 1876 г. Александр Белл не изобрел телефон.

Начало 1970-х годов в США — период расцвета так называемого фрикинга (англ. *phreaking*, слияние слов *phone* и *freak*) [1]. Появились телефонные хулиганы, которые поначалу просто забавлялись, звоня ничего не подозревающим операторам телефонных компаний и шутя на тему их компетентности. Нескольких лет такого «озорства» было достаточно для того, чтобы повысить уровень мастерства мошенников настолько, что он позволял им получить практически любую конфиденциальную информацию, доступную работнику компании.

Появление компьютеров и развитие сети Интернет побудило многих фрикеров освоить и эту принципиально новую область [3]. Так появились «сетевые мошенники», или просто хакеры. В настоящее время понятия «социальная инженерия» и «социальные хакеры» синонимичны. Интенсивное развитие социальной инженерии лишь порождает ее новые виды и расширяет арсенал методик, которые, в свою очередь, основаны на уникальности когнитивного базиса человека. В общем виде схема воздействия имеет вид, показанный на рисунке.



Основная схема воздействия на жертву в социальной инженерии

В настоящее время выделяют шесть основных техник [4].

1. **Фишинг** (англ. *fishing* — рыбалка) — пожалуй, самый распространенный метод обмана в сети. Жертва получает фальсифицированное письмо, содержащее ссылку на какой-либо сайт, не вызывающий явных подозрений. Перейдя по ней, пользователь, сам того не понимая, выкладывает свои логины и пароли злоумышленникам. Также нередки случаи, когда данные похищаются с помощью QR-кодов и других «прямых» ссылок. Техника фишинга основана на том, что человек склонен верить в надежность именитых брендов, связывая их с авторитетностью [5].

2. **Претекстинг** (англ. *Pretexting* — заранее составленный сценарий). Этот вид атак осуществляется обычно с помощью онлайн-мессенджеров или просто по телефону. Данный метод требует от синжера (социального инженера) предварительной подготовки — сбора информации, как правило, из открытых источников (социальные сети, базы данных операторов связи и т. п), для обеспечения определенного уровня доверия цели. В результате жертва, проникнувшись к злоумышленнику, сообщает конфиденциальную информацию и/или совершает определенное действие, несущее угрозу безопасности компании.

3. **Кви про кво** (лат. *Quid pro quo* — то за это). Обычно используется в значении «услуга за услугу». Чаще всего злоумышленник звонит в компанию, представляясь сотрудником технической поддержки. В процессе разговора он узнает о наличии каких-либо проблем. В случае если они есть, мошенник по телефону помогает сотруднику компании «решить» их, в процессе чего последний собственноручно вводит команды, запускающие вредоносное программное обеспечение.

4. **Троянская программа** — это техника, основой которой является банальное любопытство. Этот тип программного обеспечения создан для несанкционированного удаленного проникновения на компьютер пользователя. Злоумышленник отправляет электронное письмо, содержащее, например, муляж важного обновления антивируса, представленного в виде ссылки, после перехода по которой в устройство проникает троян. В отличие от обычного вируса, он не имеет функции размножения и дальнейшего распространения по сети. Однако троян открывает дверь для проникновения других вирусов. По своему действию он напоминает принцип троянского коня, подаренного греками непокорившимся защитникам города Трои.

5. **Дорожное яблоко** — это методика, в основе которой лежат те же принципы, что и у «Троянского коня». Разница лишь в использовании зараженных физических носителей (flash-диски, CD-диски и т. д.), подделываемых под официальные и подбрасываемых работнику компании. Статистика показывает, что данный метод является самым успешным, когда речь идет об атаке на крупную компанию [6].

6. **Обратная социальная инженерия** — это вид атаки, при которой злоумышленником создается такой сценарий, в котором жертва сама будет вынуждена обратиться к нему за помощью. Например, никто в здравом уме не сообщит пароль от социальной сети незнакомому человеку. Однако звонок в 8 утра в воскресенье от «сотрудника технической поддержки» по поводу устранения важных неполадок может развязать пользователю язык.

Люди, применяющие техники социальной инженерии в тех или иных целях, также могут быть разделены на классы в соответствии с ущербом, полученным в результате их деятельности [4, 7].

1. **Хакеры.** Как известно, «любая система небезопасна, пока в ней присутствует человек». Хакеры, охотясь за какой-либо информацией, зачастую применяют техники социального взлома, ведь современные информационные сети надежно защищены от угроз извне, в отличие от рядовых сотрудников.

2. **Воры личной информации.** Данный вид социальных инженеров использует такую информацию, как, например, имя человека, номер банковского счета или дату рождения без ведома владельца. Чаще всего эти данные собираются для гораздо большего преступления.

3. **Коммерческие социальные инженеры.** В данный класс входят люди, которые с помощью социальной инженерии выуживают деньги из людей, в основном по телефону и в Интернете.

4. **Пентестеры** — это люди, которые в учебных целях проводят санкционированные атаки на информационную систему компании для выявления потенциальных уязвимостей. Они не используют полученную информацию для личной выгоды, а лишь указывают на ошибки в системе безопасности [7].

В целом можно выделить общие моменты в технологиях, используемых современными социальными инженерами. Социальные атаки базируются на доверчивости, слепом подчинении авторитетам, лени пользователей и их малограмотности в области безопасности. Защита от подобного рода действий — дело непростое, ведь зачастую сам факт обмана выявляется много позже или не выявляется вообще. Цели социальных хакеров мало чем отличаются от целей любых других злоумышленников. Во всех случаях охота ведется на аккаунты, банковские счета, компрометирующую информацию, или ИТ-ресурсы компании-жертвы.

Сейчас шаблоны атак, которые используют злоумышленники, тщательно изучаются специалистами в области информационной безопасности. На их основе создаются специальные методики защиты от потенциальных угроз. Эксперты выделяют три вида средств противодействия методам социальной инженерии [1, 3, 4, 6]: административный, антропогенный и технический.

1. **Административный.** Все работники компании независимо от занимаемой должности обязаны понимать ценность информации, с которой им приходится работать. Ключевым фактором здесь является постоянное обучение сотрудников. От опасности извне защититься реально, а от опасности изнутри — практически невозможно. С целью повышения уровня безопасности проводятся специальные тренинги, постоянно контролируется уровень знаний и, конечно же, совершаются внутренние диверсии с использованием всех возможных техник социальной ин рии, которые позволяют определить уровень подготовленности сотрудников в реальных условиях. Как правило, это звонки и электронные письма различного содержания, сервисы общения и социальные сети. Тестирование позволяет не только блокировать доступ нарушителя, но и проверить честность сотрудников и их реакцию на попытки нарушения.

2. **Антропогенный.** К средствам данного вида защиты относят:

– привлечение внимания людей к вопросам безопасности с помощью объявлений, баннеров социальной рекламы и т. п.;

– осознание пользователями всей серьезности проблемы и принятие политики безопасности системы;

– изучение и внедрение необходимых методов и действий для повышения защиты информационного обеспечения.

Однако антропогенная защита является наиболее пассивным и бесполезным средством противодействия. Большинство людей просто игнорируют предупреждения независимо от формы их представления.

3. **Технический** [8]. Противодействие потенциальной угрозе взлома можно осуществить двумя способами:

1) помешать получить конфиденциальную информацию. К данному способу можно отнести:

– ограничение прав сотрудника в системе — запрет на доступ к «нежелательным» web-сайтам и использование съемных носителей;

– использование системы обнаружения и предотвращения атак в корпоративной сети компании;

– наличие обязательных регламентов безопасности, а также инструкций, находящихся в постоянном доступе сотрудников и содержащих в себе порядок действий при возникновении различных угроз безопасности;

– четкое разграничение информации, получаемой каждым сотрудником, для исключения возможности получения всего пакета сведений при «взломе» одного человека;

2) помешать воспользоваться полученной информацией. К данному способу относятся:

– привязка аутентификационных данных к ip, серийным номерам и электронным подписям;

– авторизация по системе Captcha;

– использование двухфакторной аутентификации.

Данные средства полностью блокируют возможность автоматизации процесса взлома, что приводит к нарушению равновесия между ценностью информации и работой, необходимой для ее получения. Время, потраченное хакером на взлом, не оправдывает данных, полученных в результате. Подобные действия помогут уберечь практически всех сотрудников от большинства техник социальной инженерии, описанных ранее.

Заключение. Социальная инженерия всегда существовала и будет существовать, ведь наличие человеческого фактора делает любую, даже самую защищенную систему уязвимой. Говоря о возможном будущем этой науки, необходимо принимать во внимание тот факт, что новые информационно-коммуникативные технологии — от Интернета до распределенных баз данных — совершенно иначе структурируют общество [4, с. 30–44]. Прогресс заставляет иерархические структуры, выработанные на протяжении всей истории человечества, отходить на второй план, уступая место сетевым. Устройство социального мира меняет формат, становясь все более гибким и динамичным. Общество индустриальное неизбежно станет обществом информационным, а двухполюсное логоцентрическое, линейное мышление человека постепенно перейдет в трехполюсное-нелинейное. Это неизбежно станет причиной появления новых видов мошенничества, в основе которых лежат иной взгляд на мир и технологии, доныне не-

известные. Эти процессы также требуют разработки принципиально нового аппарата, способного обеспечить должный уровень безопасности простого пользователя [9].

Литература

[1] Митник К., Саймон В. Искусство обмана. М., АйТи, 2004.
[2] Ораторское искусство в античности. Ораторы Древней Греции. Ораторы Древнего Рима. *myfilology.ru: веб-сайт*. URL: https://myfilology.ru/147/oratorskoe-iskusstvo-v-antichnosti-oratory-drevnej-greczii-oratory-drevnego-rima/ (дата обращения: 15.05.2019).
[3] Security Through Education: веб-сайт. URL: https://www.social-engineer.org (дата обращения: 15.05.2019).
[4] Социальная инженерия, или как «взломать» человека. *Kaspersky.ru: веб-сайт*. URL: https://www.kaspersky.ru/blog/socialnaya-inzheneriya-ili-kak-vzlomat-cheloveka/2559/ (дата обращения: 15.05.2019).
[5] ГОСТ Р 56205-2014. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели. М., Стандартинформ, 2014.
[6] Краткое введение в социальную инженерию. *habr.com: веб-сайт*. URL: https://habr.com/ru/post/83415/ (дата обращения: 15.05.2019).
[7] Freeman L.C. The development of social network analysis. BookSurge, 2004.
[8] Тестирование корпоративной информационной системы на проникновение. *sp123.ru: веб-сайт*. URL: https://sp123.ru/services/testirovanie-vashey-korporativnoy-informatsionnoy-sistemy/ (дата обращения: 15.05.2019).
[9] Тихонов А.В. Материалы круглого стола «Социология управления: вчера, сегодня, завтра». *Социологические исследования*, 2018, № 2, с. 105–110.

Балакин Константин Андреевич — студент кафедры «Защита информации», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Оплетина Надежда Витальевна, кандидат социологических наук, доцент кафедры «Социология и культурология», МГТУ им. Н.Э. Баумана.

SOCIAL ENGINEERING: YESTERDAY, TODAY, TOMORROW

K.A. Balakin
balakinka@student.bmstu.ru
SPIN-code: 6184-5181

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

In this paper, the author shows a topic within the context of the everyday world is an issue of information security. There are many ways of user's data theft. The present paper describes the main stages of the history of the formation such phenomenon of modernity as social engineering, and analyzed its main techniques and protective devices. The author showed that modern information and communication environment and technical progress are unlimited sources, generating new types and techniques of social hacking. In addition, the potential scenario of the further development of this science, due to the transition system of society is described.

Keywords

Social engineering, information security, personal information, human factor, impact scheme, social engineering technologies, social engineering techniques, user safety

Received 05.06.2019

References

[1] Mitnick javascript: void(0)K.D., Simon javascript: void(0)W.L., Wozniak S. The art of deception: controlling the human element of security. Wiley, 2003. (Russ. ed.: Iskusstvo obmana. Mowcow, AyTi Publ., 2004.)

[2] Oratorskoe iskusstvo v antichnosti. Oratory Drevney Gretsii. Oratory Drevnego Rima [The art of rhetoric in ancient world. Orators of Ancient Greece. Orators of Ancient Rome]. *myfilology.ru: website* (in Russ.). URL: https://myfilology.ru/147/oratorskoe-iskusstvo-v-antichnosti-oratory-drevnej-greczii-oratory-drevnego-rima/ (accessed: 15.05.2019).

[3] Security Through Education: website. URL: https://www.social-engineer.org (accessed: 15.05.2019).

[4] Sotsial'naya inzheneriya, ili kak "vzlomat'" cheloveka [Social engineering or how to "hack" a person]. *Kaspersky.ru: website* (in Russ.). URL: https://www.kaspersky.ru/blog/socialnaya-inzheneriya-ili-kak-vzlomat-cheloveka/2559/ (accessed: 15.05.2019).

[5] GOST R 56205-2014. Seti kommunikatsionnye promyshlennye. Zashchishchennost' (kiberbezopasnost') seti i sistemy. Chast' 1-1. Terminologiya, kontseptual'nye polozheniya i modeli [State standard R 56205-2014. Industrial communication networks. Network and system security. Part 1-1. Terminology, concepts and models]. Moscow, Standartinform Publ., 2014 (in Russ.).

[6] Kratkoe vvedenie v sotsial'nuyu inzheneriyu [Brief introduction into social engineering]. *habr.com: website* (in Russ.). URL: https://habr.com/ru/post/83415/ (accessed: 15.05.2019).

[7] Freeman L.C. The development of social network analysis. BookSurge, 2004.

[8] Testirovanie korporativnoy informatsionnoy sistemy na proniknovenie [Hacking test of corporative information system]. *sp123.ru: website* (in Russ.).

URL: https://sp123.ru/services/testirovanie-vashey-korporativnoy-informatsionnoy-sistemy/ (accessed: 15.05.2019).

[9] Tikhonov A.V. Sociology of governance and administration: yesterday, today, tomorrow. *Sotsiologicheskie issledovaniya*, 2018, no. 2, pp. 105–110 (in Russ.).

Balakin K.A. — Student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific adviser — Opletina N.V., Cand. Sc. (Sociol.), Assoc. Professor, Department of Sociology and Culturology, Bauman Moscow State Technical University, Moscow, Russian Federation.