СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

SOCIAL ENGINEERING AS A THREAT TO INFORMATION SECURITY

A. Sazonov
I. Vorobieva

Summary. Social engineering is the psychological manipulation of people based on the use of flaws in human logic, known as cognitive biases, in order to obtain confidential information. Social engineering (SI) has become a serious threat in virtual communities and is an effective means to attack information systems. SI is a potential threat to information security and should be considered on a par with its technological counterparts. However, much attention is paid to the implementation of technical security through antivirus, intrusion detection systems (IDS), intrusion prevention systems (IPS), firewalls, etc., completely ignoring the non-technical behavior. Since there is no hardware or software to protect an enterprise or individual from social engineering, it is essential to implement good practices.

Keywords: information security, social engineering, social hacker, confidential information.

Сазонов Алексей Иванович
К.т.н., доцент, МИРЭА — Российский Технологический Университет
sazonov@mirea.ru
Воробьева Ирина Алексеевна
МИРЭА — Российский Технологический Университет
Irina2803v@mail.ru

Аннотация. Социальная инженерия — это психологическое манипулирование людьми, основанное на использовании недостатков человеческой логики, известных как когнитивные предубеждения, с целью получения конфиденциальной информации. Социальная инженерия (СИ) стала серьезной угрозой в виртуальных сообществах и является эффективным средством для атаки на информационные системы. СИ представляет собой потенциальную угрозу информационной безопасности и должна рассматриваться наравне с ее технологическими аналогами. Тем не менее, большое внимание уделяется реализации технической безопасности с помощью антивирусов, систем обнаружения вторжений (IDS), систем предотвращения вторжений (IPS), брандмауэров и т.д., полностью игнорируя нетехническое поведение. Поскольку не существует ни аппаратного, ни программного обеспечения для защиты предприятия или отдельного лица от социальной инженерии, крайне важно внедрять надлежащую практику.

Ключевые слова: информационная безопасность, социальная инженерия, социальный хакер, конфиденциальная информация.

Социальная инженерия в контексте информационной безопасности — это категория атак, включающих целенаправленное воздействие на человека и манипулирование им в попытке получить информацию или спровоцировать определенное поведение, как правило, с помощью какой-либо формы обмана. СИ может проявляться в личных взаимодействиях, по телефону, в письмах, по электронной почте, через веб-сайты или людей. Она угрожает не только организациям, компаниям и правительствам, но и отдельным лицам.

Люди, использующие методы социальной инженерии для исследования и сбора данных в незаконных целях, называются социальными хакерами или социальными инженерами. Секрет действительно успешного социального инженера заключается в том, что он собирает информацию, не вызывая никаких подозрений относительно того, что он делает.

Атаки социальной инженерии могут быть широко классифицированы на две категории, а именно: технологический и человеческий обман. В технологическом подходе пользователь обманывается, полагая, что он взаимодействует с легитимным приложением или системой, тем самым разглашая конфиденциальную информацию и предоставляя доступ к информационным системам. В человеческом подходе атаки осуществляются с использованием предсказуемых человеческих реакций на психологические триггеры.

Несмотря на то, что каждая из атак социальной инженерии уникальна, можно выделить общую структуру для любой атаки, включающую в себя четыре этапа:

1. Исследование (Footprinting) — включает в себя сбор информации о цели. Целью может являться как отдельное частное лицо, так и сотрудник организации, через которого злоумышленник

стремится получить доступ к конфиденциальной информации данной организации. Сбор данных обычно осуществляется средствами OSINT (Open Source Intelligence) — разведка, основанная на общедоступных источниках, таких как: СМИ, сетевые сообщества (социальные сети, блоги и т.п.), базы данных операторов связи, регистраторы доменных имен и общественные данные (демография, показатели бюджетов и т.д.). Собранная информация используется на последующих этапах и имеет ключевое значение для успешного проведения атаки.

2. Развитие взаимопонимания и доверия (Establishing Trust). На данном этапе социальный хакер использует различные методы СИ, чтобы обеспечить доверие сотрудников атакуемой организации. Данные, собранные на первом этапе, такие как публичное имя, сведения о работодателе и сведения о компании, используются, чтобы укрепить достигнутые доверительные отношения.
3. Использование доверия (Psychological Manipulation). На этом этапе социальный инженер использует доверие, которое он приобрел на предыдущем этапе, чтобы извлечь как можно больше конфиденциальной информации об информационной системе организации или тонкостях работы персонала, чтобы в дальнейшем упростить проникновение в систему. Как только вся необходимая конфиденциальная информация будет собрана, социальный хакер переходит к непосредственному ее использованию.
4. Выход из системы (The Exit). Это завершающий этап всей операции, на котором атакующий удостоверяется, что никаких доказательств его визита не остается (реального или виртуального) и его действия не вызывают подозрений, которые могут привести к отслеживанию его реальной личности. При завершении атаки часто бывает, что киберпреступники создают для себя «точку возврата», позволяющую им вернуться в будущем.

Атаки социальной инженерии предполагают эксплуатацию различных слабостей человеческой психики с целью незаконного получения личной информации или несанкционированного доступа к компьютеру жертвы с целью установки вредоносного ПО. Основным отличием социальной инженерии является стремление обойти технические средства защиты, избрав главным вектором атаки человеческий фактор, а не компьютерную систему.

Рассмотрим наиболее распространенные виды атак:

- Фишинг (Fishing) включает в себя создание тщательно разработанных электронных писем, которые выглядят похожими на легитимные (Сбербанк, Госсуслуги, ГиБДД и пр.) и содержат в себе формы для ввода персональных данных (логин и пароль, данные платежных карт и т.д.) или ссылки на веб-сайты, где содержатся такие формы.
- Вишинг (Vishing) — это форма атаки социальной инженерии, в которой злоумышленник использует телефонный звонок, целью которого является извлечение личной или конфиденциальной информации от жертвы. Эти атаки обычно осуществляются подменой идентификатора вызывающего абонента с помощью технологии VoIP (Voice over IP). Так как это делает звонки похожими на исходящие из надежного источника, такого как банк или правоохранительные органы, это вынуждает жертв разглашать их конфиденциальную информацию (номера кредитных карт, пин-коды, номера счетов, пароли и т.д.).
- Смишинг (Smishing) — это комбинация SMS и фишинга, которая использует SMS-сообщения для обмана. Поддельные текстовые сообщения маскируются под угрозы или предложения из законных источников, таких как банки, магазины и т.д., чтобы заставить людей ввести свои личные данные и, в конечном итоге, стать жертвой.
- Кви про кво (Quid Pro Quo) — «услуга за услугу». Злоумышленники выдают себя за сотрудников технической поддержки, сообщают о неполадках на рабочем месте жертвы и предлагают свою помощь. В процессе устранения технических проблем атакующий вынуждает жертву устанавливать ПО, запускать различные команды или предоставлять удаленный доступ к компьютеру. Полагая, что сведения о сетевых учетных данных необходимы для решения проблемы, пользователи раскрывают их злоумышленнику, таким образом предоставляя ему полный доступ.
- Фарминг (Pharming) — основывается на том, как работает интернет-браузер — а именно, что последовательность букв, образующих интернет-адрес, должна быть преобразована в IP-адрес DNS-сервером для продолжения соединения. Эксплойт атакует этот процесс одним из двух способов. Во-первых, хакер может установить вирус на компьютер пользователя, который изменяет файл hosts компьютера, чтобы перенаправить трафик к поддельному веб-сайту. Во-вторых, хакер может вместо этого отравить DNS-сервер, заставляя пользователей непреднамеренно посещать поддельный сайт.
- Троянский конь (Trojan horse) — этот метод включает в себя отправку электронного письма с вложением. В прикрепленном файле может быть обновление для программы или офисный документ с встроенным вредоносным кодом.

- Дорожное яблоко (Road Apple) — эта техника основана на человеческом любопытстве и использовании физических носителей. Злоумышленник подбрасывает такой носитель в место, где он может быть легко обнаружен. Чтобы у сотрудника возник интерес, злоумышленник может нанести на носитель логотип компании или другую надпись. В результате распространяется вредоносное ПО, предустановленное на накопителе, и внутренняя сеть организации попадает под контроль хакера.
- Обратная социальная инженерия (Reverse Social Engineering) — это уникальный вид атаки, направленный на создание ситуации, при которой жертва вынуждена обратиться за помощью к злоумышленнику. Это включает в себя три этапа — саботаж, реклама и оказание помощи. Изначально злоумышленник создает поправимые неполадки на компьютере жертвы. Затем он рекламирует себя, представляясь сотрудником службы технической поддержки, способным решить возникшую проблему. Когда жертва обращается за помощью, злоумышленник для решения ранее созданных проблем может попросить пароль или установить определенное ПО.
- Плечевой серфинг (Shoulder Surfing) — означает наблюдение "из-за плеча" за тем, как кто-то использует свой компьютер. Этот метод позволяет злоумышленникам перехватывать конфиденциальную информацию и пароли, наблюдая за пользователем. Он может быть реализован физически или удаленно (с помощью камер или программного обеспечения).
- Разгребание мусора (Dumpster Diving) — включает в себя сбор конфиденциальных документов или выброшенного оборудования (CD/DVD/жесткие диски) из мусора компании или конкретного человека.
- Нападение вымогателей (Ransomware Attacks) — включает в себя установку вредоносного ПО, которое «удерживает компьютер пользователя в заложниках» до тех пор, пока не будет выплачен выкуп. Существует две распространенные формы вымогателей: Locker Ransomware (блокируется доступ к компьютеру пользователя или мобильному устройству) и Crypto Ransomware (шифруются ключевые файлы или данные).

Одной из самых сложных задач является защита от атак социальных инженеров, потому что они включают в себя человеческий фактор, который сам по себе довольно непредсказуем. Атаки социальной инженерии неизбежны, однако, есть некоторые меры, которые помогут свести влияние этих атак к минимуму и сделать организации менее уязвимыми. Рассмотрим основные способы защиты от социальных хакеров:

1. Никогда не разглашать какую-либо конфиденциальную информацию и сетевые учетные данные по электронной почте, телефону или лично любым посторонним лицам.
2. Не нажимать на любые подозрительные вложения, полученные по электронной почте, даже если они выглядят как легитимные.
3. При нажатии на ссылки, проверять наличие орфографических ошибок, символов и подозрительных поддоменов.
4. Всякий раз, при обнаружении, что какой-то файл загружается автоматически после нажатия ссылки или посещения веб-сайта, немедленно сообщать об этом системному администратору.
5. Системные администраторы должны постоянно следить за любой частной или конфиденциальной информацией, размещаемой пользователями на веб-сайтах компании по ошибке, и удалять их.
6. Необходимо блокировать возможность подключения внешних запоминающих устройств на компьютерах сотрудников для защиты от дорожного яблока.
7. Никому не предоставлять возможности входа в систему с учетной записью администратора, т.к. может быть получен доступ к любым данным на компьютере.
8. Использовать многофакторную аутентификацию для сотрудников.
9. Не устанавливать ПО из неизвестных источников.

Кроме перечисленных выше предложений есть другие дополнительные механизмы, которые могут быть полезны в удержании атакующих. Простые вещи, такие как постоянное обновление программного обеспечения, подходящие системы обнаружения вторжений (IDS), безопасная утилизация отходов (документов, носителей и т.п.), сложные пароли и т.д.

Обеспечение информационной безопасности должно осуществляться комплексно, сразу по нескольким направлениям. Необходимо разработать концепцию информационной безопасности и создать политику безопасности организации в целом, учитывая потенциальные угрозы и методы их предотвращения. Важно учитывать, что даже самая совершенная сетевая защита не смогла бы остановить атаку социальной инженерии из-за участия человеческого фактора. Поэтому угрозу со стороны СИ необходимо нивелировать, используя не только программно-аппаратные средства, а главным образом, используя корпоративную культуру осведомленности о безопасности, которая поможет сотрудникам регулярно выявлять и отражать атаки социальной инженерии. Обеспечение информационной безопасности должно быть направлено, прежде всего, на предотвращение рисков, а не на ликвидацию их последствий.

ЛИТЕРАТУРА

1. Granger S. Social engineering fundamentals Hacker Tactics, Part I, 2001–12–18. -Режим доступа: https://ru.scribd.com/doc/19676093/Social-Engineering-Fundamentals (дата обращения: 07.09.2019).
2. Kaspersky K., Hacker Disassembling Uncovered. Wayne: A-list Publishing, 2003. 584 p.
3. KasperskyLab Daily Режим доступа: https://blog.kaspersky.ru/socialnaya-inzheneriyaili-kak-vzlomat-cheloveka/2559/(Дата обращения: 07.09.2019)
4. Mitnick K., Simon W. L. The Art of Deception: Controlling the Human Element of Security. Indianapolis: Wiley Publishing, Inc., 2003. 335 p.
5. Schoeman, A.H.B., and B.V.W. Irwin. "Social Recruiting: a Next Generation Social Engineering Attack." Journal of Information Warfare, vol. 11, no. 3, 2012, pp. 17–24.
6. Воробьева И.А., Сазонов А. И. Информационная безопасность в промышленном сегменте. Перспективы науки. 2019. № 3 (114). С. 176–178.
7. Кузнецов М.В., Симдянов И. В. Социальная инженерия и социальные хакеры. -СПб.: БХВ-Петербург, 2014.

Журнал «Современная наука: актуальные проблемы теории и практики»

МИРЭА — Российский Технологический Университет