Артемов О.Ю., Овчинников С.А.

Социальная инженерия как главная проблема обеспечения информационной безопасности

Аннотация: статья посвящена исследованию методов социальной инженерии с целью несанкционированного доступа к информации или системам ее хранения без использования технических средств с учетом человеческого фактора.

Ключевые слова: защита информации, когнитивный базис, коммерческая разведка, риск-менеджмент, социальная инженерия, человеческий фактор

Современный уровень технологий, интенсивное развитие научно-технической базы, регулярное выделение ряда направлений в новые науки, появление новых теорий и подходов, продолжающееся социально-экономическое развитие общества в условиях рынка, усиление коммерциализации и пр., ведут к появлению перепроизводства, жесткой конкуренции, расширению количества потребительских аудиторий в целях роста продаж и максимизации прибыли. Отсюда желание вернуть затраты на инновационные технологии, разработки и предшествующие им исследования. При этом сегодня немногие компании занимаются собственным производством, соблюдают честные правила торговли и используют «белые» схемы ведения финансового учета. Появилось немало организаций и независимых специалистов, которые в своей работе применяют методы и средства коммерческой разведки, а, следовательно, занимаются сами или заказывают «на стороне» сведения, получаемые посредством промышленного шпионажа. Как следствие, увеличивается стоимость и значимость информации, поскольку технологии по ее сбору и переработке занимают важное место в бизнес-процессах любой современной компании.

Повышается роль такой специальной функции управления, как риск-менеджмент, поскольку большее число фирм начинает учитывать риски, в связи с чем мы решили остановиться на социальной инженерии (СИ) в контексте защиты информации. Это относительно молодое направление, которое является составной частью социологии и претендует на совокупность тех

специфических знаний, которые направляют, приводят в порядок и оптимизируют процесс создания, модернизации и воспроизведения новых («искусственных») социальных реальностей.

Считается, что идеологом социальной инженерии является руководитель Центрального института труда в Москве А.К. Гастева. Новой науке, по замыслу ее создателя, следовало находиться на стыке социальных и естественных наук, что позволило бы из последних заимствовать точные экспериментальные методы и инструменты [1].

Объектом СИ является изучение человеческого фактора и его природы с целью последующего конструирования социальной среды в рамках той или иной области. В 1920-е и позже в 1950–60-е гг. под последней понималось отдельно взятое предприятие. Впоследствии рамки значительно расширяются и охватывают не только производственную сферу, но и общество в целом.

Считается, что сегодня социальная инженерия, главным образом, предназначена для манипулирования людьми. Как показывает опыт зарубежных стран, социальный инженер имеет дело не с рядовыми работниками организации, а с ее верхним эшелоном – администрацией. Работа же на управленческую элиту предполагает осуществление технократических воздействий на людей, то есть управление ими как техническими средствами.

С изменением направленности вектора содержании рассматриваемого нами термина, социальная инженерия в новых условиях трактуется, как метод несанкционированного доступа к информации или системам ее хранения без использования технических средств. Основной целью социальных инженеров является получение доступа к защищенным системам с целью кражи информации, паролей пользователей, данных о кредитных картах и тому подобное. Основным отличием от стандартной кибер-атаки является то обстоятельство, что в роли объекта ее атаки выбирается не вычислительная машина, а ее оператор. Метод основан на использовании слабостей человеческого фактора, в связи с чем считается потенциально очень разрушительным. У данного факта много объяснений, во-первых – нередко часть работников недостаточно обучена и им не хватает знаний, чтобы избежать такой атаки; во-вторых, большая часть компаний думает, прежде всего, о защите физического периметра от внешних угроз;

в-третьих, дешевизна нападения, в то время как результат достигается гораздо быстрее, чем если бы была использована иная технология.

Все техники социальной инженерии основаны на особенностях принятия решений людьми, называемых «когнитивным базисом», так как человек по своей социальной природе должен кому-либо доверять.

Рассмотрим некоторые из них. [2]

Претекстинг. Опирается на заранее составленный сценарий (претекст). В результате цель должна выдать нужную информацию или совершить определённое действие. Данный вид атак применяется обычно по телефону. Техника «взлома» включает в себя больше, чем просто ложь, и требует каких-либо предварительных исследований (например, персонализации – даты рождения, суммы последнего счёта и др.), с тем, чтобы обеспечить доверие со стороны адресата.

Фишинг. Основан на том, что злоумышленник посылает цели e-mail, подделанное под официальное письмо от банка или платёжной системы и требующее «проверки» той или иной информации. Такое письмо обычно содержит линк на фальшивую веб-страницу, имитирующую официальную с корпоративным логотипом и контентом, а также включает форму, в которую требуется ввести конфиденциальные данные (от адреса дома до пин-кода банковской карты).

Троянский конь. Его применение связано с любопытством либо алчностью потенциальной жертвы. Злоумышленник отправляет e-mail, содержащее во вложении заманчивый скрин-сейвер, важный апгрейд антивируса или даже свежий компромат на сотрудника. Данная техника остаётся эффективной, пока пользователи будут слепо кликать по любым вложениям.

Дорожное яблоко. Представляет собой адаптацию троянского коня и состоит в использовании физических носителей. Злоумышленник может подбросить инфицированный CD или флэш, в местах, где может быть легко найден (туалет, лифт, парковка). Носитель подделывается под официальный источник и сопровождается соответствующей подписью, призванной вызвать ответную реакцию. Человек по незнанию может его подобрать и вставить в компьютер, чтобы удовлетворить своё любопытство.

Quid pro quo. Подразумевает звонок злоумышленника в компанию по корпоративному телефону. В большинстве случаев он представляется сотрудником технической поддержки, опрашивающим, есть ли какие-нибудь проблемы. В процессе их «решения» он заставляет цель вводить команды, которые позволяют запустить или установить вредоносное программное обеспечение на ПК пользователя.

Сбор информации из открытых источников. Использование социальной инженерии требует умения собирать о человеке необходимую информацию. Основным способом ее получения сегодня стали социальные сети. Например, бразильский исследователь Нельсон Новаес Нето показал, что существует возможность стать другом любого пользователя «Facebook» в течение 24 часов, используя методы социальной инженерии. В ходе эксперимента исследователь выбрал жертву и создал фальшивый аккаунт человека из ее окружения – начальника с места работы. Сначала он отправлял запросы «на дружбу» друзьям друзей начальника жертвы, а затем и непосредственно его друзьям. Через 7,5 часов исследователь добился добавления в друзья от жертвы. Тем самым, исследователь получил доступ к личной информации пользователя, которой тот делился только со своими близкими знакомыми.

Как видно из приведенных примеров, самое слабое звено в автоматизированной информационной системе с точки зрения обеспечения ее безопасности – это человек, являющийся либо оператором данной системы, либо пользователем, либо выполняющим иные функции. Справедливость данного утверждения может быть подтверждена следующими аргументами: 1) деятельность человека не подчинена логике выполнения итераций вычислительного процесса: человек – не машина, работающая по заранее заложенной в него программе, поэтому сложность формирования адаптивного процесса защиты соизмерима со сложностью построения алгоритма функционирования человеческого мозга; 2) выполнение обязанностей оператора автоматизированной системы сопровождается наличием сторонних факторов, прямо или косвенно влияющих на соблюдение технологического процесса (причем указанные факторы носят вероятностный характер, не всегда

подчиненный определенному распределению); 3) любой человек обладает слабостями, используя которые можно внести изменения в технологический процесс обработки информации; 4) обилие всевозможных сервисов, их доступность, помноженные на стремление выделиться среди окружающих, заставляет совершать различные, не всегда обдуманные, поступки в информационном пространстве (в частности, в соцсетях).

Данные обстоятельства позволяют потенциальному злоумышленнику для достижения своих целей не искать уязвимости в программно-аппаратных средствах защиты информации, а всеми доступными методами, включая социальную инженерию, получать интересующие сведения от самих лиц, осуществляющих их обработку.

Специалисты по социальной инженерии часто цитируют высказывание великого Альберта Эйнштейна: «Можно быть уверенным только в двух вещах: существовании вселенной и человеческой глупости, и я не совсем уверен насчет первой». В этих двух строчках, по их мнению, состоит актуальность проблемы утечки конфиденциальных данных за счет использования методов социальной инженерии.

Обилие порталов, наводненных различными полезными сведениями по методам проникновения и взлому систем, позволяет любому желающему получить необходимые теоретические и практические знания по информационным технологиям, чтобы стать хакером. Современные «самоучки» и состоявшиеся специалисты объединяются в сообщества программистов, крекеров, кардеров и другие группы. По различным данным, возраст их участников от 13–14 до 35–38 лет включительно. Создаются специализированные открытые и закрытые интернет порталы, которые позволяют последним обмениваться материалами, опытом, наработками, брать на вооружение разные идеи и реализовывать их на практике, а также осуществлять координацию совместных проектов и набирать в свои команды новых рекрутов. Дополнительно через эти порталы, осуществляется взаимодействие с подобными им группами, территориально разбросанными по всему миру. Обращает на себя внимание и тот факт, что в последнее время многие из их членов начинают изучать психологию, методы гипноза и различного манипулирования.

Достаточно ознакомиться с отчетами антивирусных лабораторий или данными об убытках компаний и связанных с ними рисков, официально публикуемыми «IDC», «Garthner Group», «Computer Security Institute» и др., чтобы понять насколько эффективно происходит это обучение [3].

К сожалению, невозможно предсказать, какую атаку выберет атакующий, в какой период времени и кто будет жертвой. Однако возможно уменьшить ее вред, используя комплекс таких мероприятий, как: проведение проверочных мероприятий при приеме сотрудников на работу, включающих всестороннее изучение личностных качеств кандидатов, их окружения, области интересов и информации о прошлой трудовой деятельности; контроль входящей корреспонденции, поступающей в электронном виде в почтовые ящики персонала, независимо от уровня полномочий и привилегированности; проверка наличия служебной информации конфиденциального характера в открытых информационных сетях; регулярное проведение занятий с работниками по правилам работы с данными конфиденциального характера, а также обучение их навыкам противодействия методам социальной инженерии; контроль соблюдения технологии обработки информации на технических средствах компании; запись и последующий анализ телефонных переговоров персонала с использованием служебных средств связи; проведение воспитательной работы с целью повышения мотивации сотрудников, проведение периодических проверок их профпригодности в части обеспечения информационной безопасности.

Конечно, список методов защиты от социальной инженерии можно продолжать бесконечно, но это все равно не защитит от злоумышленников и мошенников всех мастей. К сожалению, типовых противодействий социальным инженерам не существует и не может существовать. Вот почему каждый новый инцидент требует индивидуального подхода и всестороннего рассмотрения.

Литература:

1. *Артемов О.Ю.* Социальная инженерия А.К. Гастева и ее развитие как науки о совместной трудовой деятельности людей

// В сб.: II Гастевские чтения. Межвузовская научно-практическая конференция. 22 октября 2019 г. – М., 2019.
2. Касперски К. Секретное оружие социальной инженерии [Электронный ресурс]. – Режим доступа: URL: http://citforum.ru/security/articles/soc_eng/ – Секретное оружие социальной инженерии. (Дата обращения: 19.10.2019).
3. *Дашко Д.А., Мешков В.И.* Социальная инженерия с точки зрения информационной безопасности / Д.А. Дашко, В.И. Мешков. – М., 2015.