АТОМФЛОТ
РОСАТОМ

«Деструктивные методы социальной инженерии как фактор угрозы информационной безопасности»

Притуляк Виктор Константинович

Ведущий специалист отдела информационной безопасности

Социальная инженерия (в информационной безопасности)

АТОМФЛОТ
РОСАТОМ

Социальная инженерия - психологическое манипулирование людьми с целью принуждения их к совершению определенных действий или для получения несанкционированного доступа к конфиденциальной информации.

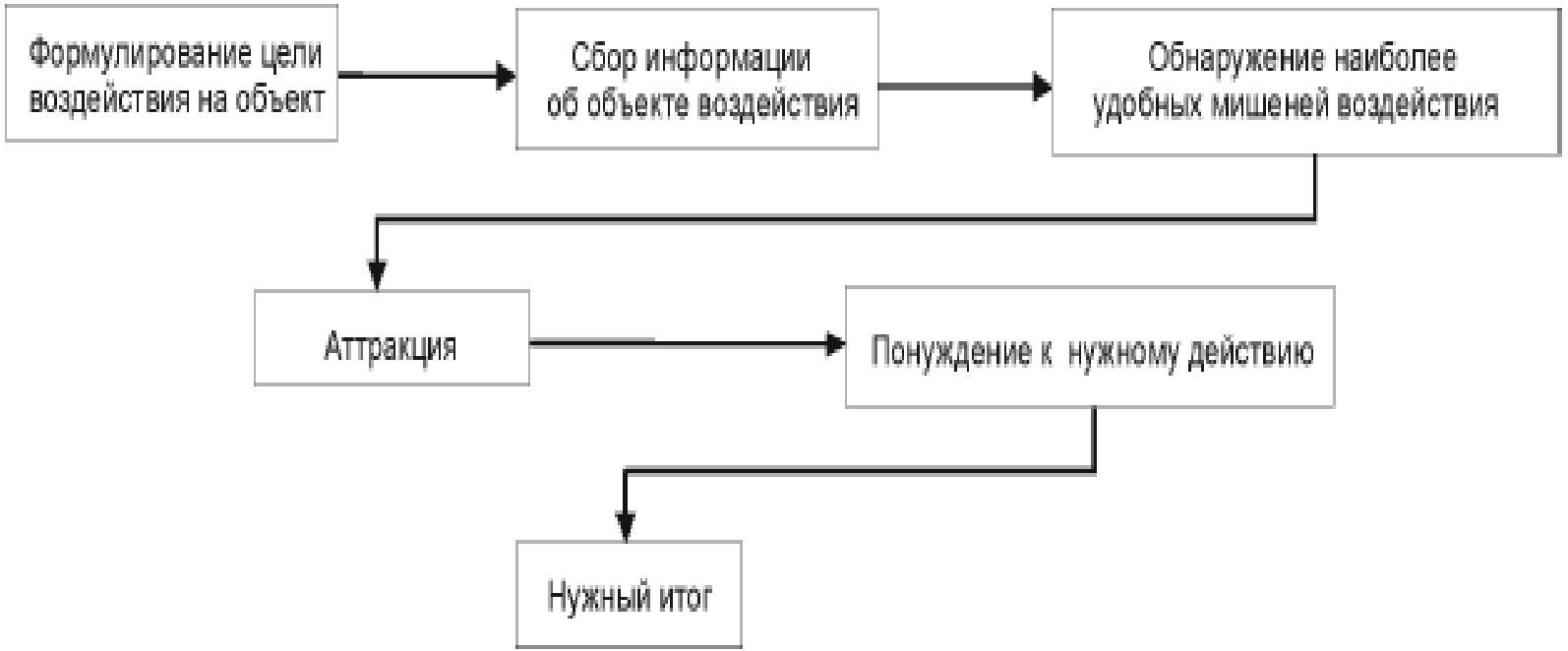
По данным из разных источников от 60% до 80% процентов всех инцидентов информационной безопасности происходит с участием сотрудника предприятия, и лишь около половины из них – из-за непреднамеренных ошибок сотрудников.

Самое слабое звено защиты любой системы – люди. Социальная инженерия пытается использовать присущие людям слабости в целях получения конфиденциальной информации и последующего доступа в систему. Особенностью социальной инженерии является стремление злоумышленников обойти все технические средства защиты, избрав основным вектором атаки человека, а не техническую систему. Злоумышленники часто прибегают к социальной инженерии, так как при помощи нее зачастую значительно проще (дешевле) добиться желаемого результата. Как пример – значительно проще убедить человека перевести деньги мошенникам, чем взломать систему безопасности банка.

Задачи привлечения методов социальной инженерии для информационных воздействий

АТОМФЛОТ
РОСАТОМ

Обобщенная схема атаки при помощи социальной инженерии



Основные техники социальной инженерии

Фишинг – вид интернет-мошенничества, целью которого является получения доступа к конфиденциальным данным пользователей – логинам и паролям. На сегодняшний день это самая распространенная схема социальной инженерии. Наиболее типичным пример фишинговой атаки - сообщение, полученное по электронной почте и подделанное под официальное письмо – от банка, гос. органов и т.п. – требующее проверки определенной информации или совершения определенных действий по разным причинам, от технических (произошел сбой, потерлась информация и т.п.) до человеческого фактора («я случайно удалила ваши данные»). Такие письма часто содержат ссылку на поддельную веб-страницу, в точности похожую на официальную и содержащую форму, требующую ввести конфиденциальную информацию.

Основные техники социальной инженерии

АТОМФЛОТ
РОСАТОМ

Популярные фишинговые схемы:

Поддельные ссылки – создается сайт (или адрес электронной почты) похожий на оригинальный, и расположенный по похожему адресу, но имеющий почти незаметные отличия, такие как замена l и i, добавление новых символов (gossuslugi.ru), или же в другом домене (gosuslugi.com).

Использование известных брендов – в таких схемах используют поддельные сообщения электронной почты, веб-сайты или телефонные звонки «от лица» представителя известных компаний. В сообщениях могут например поздравления с победой в конкурсе, требования срочно сменить учетные данные и пароль. Подобные схемы могут быть так же реализованы от лица службы технической поддержки.

Основные техники социальной инженерии

АТОМФЛОТ
РОСАТОМ

Популярные фишинговые схемы:

Ложное программное обеспечение – вас просят установить новое программное обеспечение, например антивирус, ПО для доступа к сайту, для сдачи отчетности и т.п. При этом вредоносное ПО может как быть вирусным, так и копировать и передавать информацию злоумышленнику.

Телефонный фишинг – эта техника основана на использовании системы предварительно записанных голосовых сообщений с целью воссоздать «официальные звонки», например банковские.

Основные техники социальной инженерии

АТОМФЛОТ
РОСАТОМ

Претекстинг – атака, в которой злоумышленник представляется другим человеком и по заранее подготовленному сценарию получает доступ к конфиденциальной информации или к системе. Эта атака подразумевает должную предварительную подготовку и сбор данных. Пример: во время отсутствия директора филиала секретарю позвонили на личный мобильный номер, представились сотрудником службы безопасности центрального офиса, действующим по поручению начальника СБ (назвал ФИО). Злоумышленник сказал что у центрального офиса есть основания подозревать что директор филиала не чист на руку и попросил секретаря зайти на компьютер директора филиала, скопировать его рабочие документы и направить ему на электронную почту. Звонок на личный номер и просьбу отправить запрашиваемую информацию не на корпоративную почту злоумышленник обосновал необходимостью проведения расследования в тайне. С учетом того что у секретаря был конфликт с директором филиала, она с радостью передала злоумышленнику запрашиваемую информацию. Т.е. злоумышленник предварительно выяснил личный номер секретаря, ФИО начальника СБ, то что в это время директор филиала отсутствует, что секретарь имеет доступ с определенными правами к компьютеру директора филиала и о конфликте участников, на чем и построил свою мошенническую схему.

Основные техники социальной инженерии

АТОМФЛОТ
РОСАТОМ

Quid pro quo (лат. «то за это) – данная техника предполагает обращение злоумышленника к пользователю по электронной почте или телефону. Злоумышленник может, например, представится сотрудником технической поддержки ресурса которым пользуется пользователь (торговая площадка, сервисы для сдачи отчетов и т.п.) и информировать о возникновении технических проблем на рабочем месте. Далее он сообщает о необходимости их устранения. В процессе «решения» проблемы, злоумышленник подталкивает жертву на совершение необходимых ему действий – установить требуемое ПО, предоставить удаленный доступ.

Основные техники социальной инженерии

АТОМФЛОТ
РОСАТОМ

Дорожное яблоко – некая адаптация всем известного троянского коня, состоит в использовании физических носителей. Злоумышленник подбрасывает «инфицированные» носители информации (диски, флэшки) в местах общего доступа, где эти носители могут быть найдены (туалеты, парковки, вестибюль и т.п.) или на рабочем месте атакуемого сотрудника. Носители могут оформляться как брендированные, или сопровождаться надписью, призванной вызвать любопытство («список премированных сотрудников», «зарплаты декабрь», «служебное расследование», и т.п.) или без них. Сотрудник из любопытства, думая что это его носитель или по незнанию вставляет носитель в свой компьютер, заражая его. Случай из личной практики: на лестничной клетке был обнаружен носитель ЭЦП. Носитель старый, номер стерся. Для того чтобы найти владельца, требовалось подключить носитель к компьютеру. Но подозревая «дорожное яблоко» подключено было к компьютеру не имеющему доступа к сети предприятия и не хранящему никакой информации. Предосторожность оказалась не лишней – на носителе был записан вирус.

Основные техники социальной инженерии

АТОМФЛОТ
РОСАТОМ

Обратная социальная инженерия – особенность данной техники в том, что инициатором контакта выступает сам атакуемый. Задача атакующего – создать у атакуемого такую ситуацию, из-за которой он сам обратится к атакующему, и убедить атакуемого что он и есть то самое легитимное лицо, способное помочь в возникшей ситуации. В процессе «решения проблемы» атакующий обеспечивает себе доступ к системе или информации в ней содержащейся. Например злоумышленник может выслать письмо с контактами «службы поддержки» ресурса которым пользуется жертва (торговая площадка, сервис для сдачи отчетов в государственные органы и т.п.) через некоторое время создать неполадки в работе с указанным ресурсом и дожидаться звонка жертвы. В таком случае, пользователь будет уверен в легитимности злоумышленника, и в процессе «исправления» проблемы злоумышленник сможет добиться желаемого.

Психологические аспекты социальной инженерии

АТОМФЛОТ
РОСАТОМ

Помимо сбора информации, подготовки сценария и технических средств атаки, злоумышленник пытается выявить особенности психики жертвы, на которую направлена атака. Эксплуатируются различные человеческие качества, как-то: лень, зависть, алчность, злость, доброта, доверчивость, трусость, тщеславие, любезность, отзывчивость и т.п. Каждый человек, потерявший бдительность, может стать жертвой социального инженера, если найти нужные рычаги воздействия.

Люди полностью уязвимы перед обманом, поскольку могут изменить отношение в сторону доверия к собеседнику, если манипулировать ими определенным образом. Человек судит людей по телефону точно так же, как и обычно – бессознательно, в спешке, во время первых секунд разговора: собеседник дружелюбный и общительный или чувствуется враждебность или давление, говорит ли он как образованный человек? Человеку свойственно предполагать, что вряд ли его обманут именно в этой конкретной ситуации, по крайней мере, пока нет причин предполагать обратное

Психологические аспекты социальной инженерии

АТОМФЛОТ
РОСАТОМ

Наверное самый известный социальный инженер, Кевин Митник, в своей книге «Искусство обмана» говорил «Будьте очаровательны, вежливы и просты – вот качества, необходимые для быстрой связи и доверия»

Обман — главное оружие социального инженера. Чтобы применить его эффективно, необходимо понимать, как люди принимают те или иные решения. Человеческий мозг – это сложный центр принятия решений. Систему принятия решений упрощая можно разбить на две составляющие: **разум** и **инстинкты**. Доминирование некоторых инстинктов подавляет возможности разума, что и делает человека уязвимым к методам социальной инженерии. Разум же активизируется в случае конфликта между инстинктами (например, между инстинктом самосохранения и альтруизмом в ситуации, когда человек решает оказать помощь попавшему в беду под угрозой для собственной жизни).

Психологические аспекты социальной инженерии

АТОМФЛОТ
РОСАТОМ

Разумную составляющую также можно условно разделить на логическую (аналитическую) и автоматическую. Именно аналитическая часть использует всю мощь человеческого мозга, когда человек объективно оценивает ситуацию, мыслит критически, оперируя всей доступной информацией, и принимает обоснованное решение. Этот способ мышления требует гораздо большего времени и энергии, чем автоматическое.

Автоматическое мышление значительно повышает продуктивность человека, так как позволяет выполнять большое количество операций за короткое время. Но в то же время оно может быть источником ошибок и порождает уязвимости к психологическим атакам. Так, чтобы завоевать доверие жертвы, атакующему зачастую достаточно убедительно представиться коллегой, используя характерную для сферы лексику и демонстрируя осведомленность в вопросе. Кстати, простые слова имеют большую силу убеждения, а вот сложные формулировки вынуждают слушателя подключать аналитическое мышление, что совсем не на руку злоумышленнику.

Психологические аспекты социальной инженерии

АТОМФЛОТ
РОСАТОМ

Стандартные методы социальной инженерии:

Использование авторитета - атакующий ссылается на поручение от топ-менеджмента. Жертва, услышав имена начальства, откидывает возможные подозрения и помогает выполнить поручение.

Игра на жалости - излюбленный прием социальных инженеров. Атакующий обращается за помощью, представившись новичком. Жертва может выполнить просьбу, вспомнив себя в первые трудовые дни.

Угроза - угрозой опять-таки может быть ссылка на авторитет начальства или упоминание о возможных негативных последствиях неподчинения (страх подавляет разум).

Психологические аспекты социальной инженерии

АТОМФЛОТ
РОСАТОМ

Стандартные методы социальной инженерии:

Симпатия - расположить к себе жертву — действенный прием для завоевания доверия. Социальный инженер общается вежливо, старается создать атмосферу неформального разговора. В разговоре может употреблять фразы: «мы работаем на благо нашего комьюнити…», «мы в одной команде…», «я замолвлю за вас слово» и т.д.

Чувство вины - основанные на чувстве вины манипуляции, испытывал на себе практически каждый человек. Злоумышленнику необходимо, чтобы невиновный в действительности почувствовал себя виноватым. Приведем пример в контексте обратной социальной инженерии. Социальный инженер отвечает на телефонный звонок и изображает, что звонящий причинил ему неудобства — авария, пролитый кофе и т.д. — но не заканчивает разговор, или обещает перезвонить. В результате звонивший испытывает чувство вины и с большей вероятностью выполняет просьбу атакующего

Методы противодействия

АТОМФЛОТ
РОСАТОМ

- Разработка продуманной политики классификации данных, учитывающей все типы данных, которые могут привести к получению злоумышленником чувствительной информации.
- Обеспечение защиты информации с помощью шифрования и разграничения доступа.
- Критичность мышления – проверяйте источник информации, ссылки, адреса электронной почты. Так же обнаружив в неожиданном месте носитель информации не вставляйте его в рабочий компьютер. Уясните твердо, что звонящий или посетитель не является тем, за кого он себя выдает только потому, что он знает имена некоторых людей в компании, корпоративные терминологию или процессы.
- Контроль информации размещаемой вами в открытых источниках.

Цифровая гигиена

АТОМФЛОТ
РОСАТОМ

- **Цифровая (сетевая) гигиена** — это концепция осознанных действий в интернете, направленная на защиту информации, предотвращение компьютерных атак и улучшение общего качества взаимодействия с технологиями.
- Соблюдение цифровой гигиены поможет не допустить нарушения безопасности информации в организации и кражи личных данных.

Цифровая гигиена.
Основные правила поведения в интернете

АТОМФЛОТ
РОСАТОМ

- Минимизируйте количество и «качество» оставляемой в открытых источниках информации.
- Используйте надежные пароли и периодически их меняйте. Для разных ресурсов используйте разные пароли. По возможности используйте многофакторную аутентификацию или одноразовые пароли (OTP).
- Используйте менеджеры паролей.
- Для разных задач используйте разные аккаунты.
- Удаляйте не нужные аккаунты.
- Ограничивайте доступ к приложениям.
- Используйте антивирусы и слушайте их «советы».

Спасибо за внимание