СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. АНАЛИЗ И МЕТОДЫ ЗАЩИТЫ

Тепляков С.П.[1], Тимохович А.С.[2]

[1]Тепляков Сергей Павлович – специалист,
направление: информационная безопасность телекоммуникационных систем;
[2]Тимохович Александр Степанович – кандидат педагогических наук, доцент,
кафедра безопасности информационных технологий,
Институт информатики и телекоммуникаций,
Сибирский государственный аэрокосмический университет им. академика М.Ф. Решетнева,
г. Красноярск

Аннотация: *в статье предложены способы обеспечения защиты информации от атак типа «социальная инженерия». Данные способы позволят повысить защищенность организации на всем протяжении ее жизнедеятельности.*
Ключевые слова: *Social Engineering, социальная инженерия, безопасность информации.*

В данное время все чаще злоумышленниками применяются методы социальной инженерии для обхода систем защиты, установленных в корпоративной сети, либо с целью выявления слабых мест в безопасности системы.

Социальная инженерия — совокупность приёмов, методов и технологий создания такого пространства, условий и обстоятельств, которые максимально эффективно приводят к конкретному необходимому результату, с использованием социологии и психологии.

В определенной форме люди использовали социальную инженерию с древних времен. Например, в Древнем Риме и Древней Греции очень уважали специально подготовленных риторов, способных убедить собеседника в его «неправоте». Эти люди участвовали в дипломатических переговорах и решали государственные проблемы. Позже социальную инженерию взяли на вооружение спецслужбы, такие как ЦРУ и КГБ, агенты которых с успехом выдавали себя за кого угодно и выведывали государственные тайны.

К началу 1970-х годов стали появляться телефонные хулиганы, нарушавшие покой разных компаний ради шутки. Но со временем кто-то сообразил, что, если использовать техничный подход, можно достаточно легко получать разную важную информацию. И уже к концу 70-х бывшие телефонные хулиганы превратились в профессиональных социальных инженеров (их стали называть синжерами), способных мастерски манипулировать людьми, по одной лишь интонации определяя их комплексы и страхи.

Использование методов социальной инженерии не требует больших денежных вложений, а также имеет огромное количество вариантов реализации, открывая большое поле действий злоумышленникам [2].

Также методы социальной инженерии не устаревают, в отличие от классических методов взлома. Как в защите, так и в атаке необходимо постоянно следить за новинками области, чтобы иметь возможность сделать что-либо.

Однако не все социальные инженеры — мошенники. Они могут вернуть доброе имя компании после атаки конкурентов или чёрного пиара. Психологические методы используют, например, чтобы получить данные анонимного комментатора и сподвигнуть его удалить нежелательный отзыв или клевету.

Социальные инженеры регистрируются на форумах, вступают в беседы с негативно настроенной аудиторией и техниками нейролингвистического программирования влияют на её мнение.

Для того, чтобы определить способы защиты от данного типа угроз, надо понимать, что и как может сделать киберпреступник.

Во-первых, войдя в переписку с человеком, можно войти в доверие и узнать информацию, которая пригодится для будущих атак. К примеру, номера телефонов, почты других сотрудников, конфигурацию сети, версию средств защиты и тому подобное [1].

Во-вторых, открыв зловредный файл, который не вызывает подозрений, к примеру «график работ», «долг по счету», «увольнение» может произойти заражение компьютера, благодаря чему у преступника появляется доступ к системе [1].

Иным способом атаки является «обратная социальная инженерия». Пример такой атаки – приходите в охраняемый периметр как уборщик, заменяете номер техподдержки в распечатке на стене на свой, а затем устраиваете мелкую неполадку. Уже через день вам звонит расстроенный пользователь, готовый поделиться всеми своими знаниями с компетентным специалистом. Ваша авторизация проблем не вызывает — ведь человек сам знает, кому и зачем он звонит.

Следуя следующим правилам, возможно устремить вероятность утечки конфиденциальных данных в следствии социальной инженерии к минимуму:

1) специалистами по информационной безопасности должны быть заблокированы для пересылки файлы, расширения которых используются для исполняемых, системных и других файлов. Проведены инструктажи с персоналом в целях повышения компьютерной грамотности [3];

2) при получении письма со вложением или ссылкой, внимательно проверить адрес отправителя, расширение письма и, при помощи антивирусного программного обеспечения, сам файл [3];

3) не вступать в общение со злоумышленником, так как в разговоре он может получить информацию, необходимую для атаки следующей жертвы [3].

Итогом работы можно заключить, что были представлены основные способы атак, при помощи социальной инженерии.

Также были сформулированы основные принципы по предупреждению атак данного типа и на основание этих принципов необходимо подготавливать персонал.

Список литературы

1. Социальная инженерия и социальные хакеры /. М.В. Кузнецов, И. В. Симдянов. СПб.: БХВ-Петербург, 2007.
2. Positive research. Сборник исследований по практической безопасности. [Электронный ресурс]. Режим доступа: https://www.ptsecurity.com/upload/ptru/analytics/Positive-Research-2017-rus.pdf/ (дата обращения: 03.06.2018).
3. Искусство обмана / Митник К., Саймон В. М: Издательский отдел ВМиК МГУ. Изд-во МАКС Пресс, 2006 г.