

Цуркан О.В.

Институт проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины

ОСОБЕННОСТИ ПРИМЕНЕНИЯ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ НА ЭТАПЕ АУДИТА СБОРА И АНАЛИЗА ИНФОРМАЦИИ С ВНЕШНЕЙ СРЕДЫ.

The features of application of methods of the social engineering are considered on the stage of audit of collection and analysis of information from an external environment.

Аудит сбора и анализа информации с внешней среды является важной и необходимой частью подготовки к проведению всевозможных атак на исследуемую информационную систему. Под этапом ориентированом на сбор информации подразумевают этап социальной инженерии (СИ). Учитывая высокую вероятность человеческого фактора, на данном этапе успешно применяются технологии социальной инженерии, составляющими компонентами которой являются: технический и социальный методы исследования информации. Для успешного выполнения планируемых действий аудита социоинженер проводит свою работу согласовано с системным администратором. В конструктивные действиям социоинженера входят: изучение и анализ содержательной стороны информационной системы, поиск уязвимостей, систематизирование сведений, разработка схемы действий.

Применение методов социальной инженерии направленных на пользователей информационной системы организации, позволяет оценить уровень квалификации пользователей в области обеспечения информационной безопасности (ИБ) и вероятность реализации атак, выполняемых нетехническими способами.

Входящими данными для социоинженера при попытке получения нужных данных о информационной системе может быть найденная в публичных источниках, контактная информация, фамилии и должности служащих, и т.д. Из собранной информации нужно выбрать, выделить такие уязвимые места, лазейки в организационной структуре, которые наиболее подвергаются атакам социальной инженерии, для дальнейшего их применения в своих целях.

Методы социальной инженерии опираются на:

- особенности, управляющие человеческим сознанием;
- аудиторию или поле деятельности злоумышленника;
- некомпетентность аудитории в определенных терминах и предметных областях в сфере ИБ;

– неустойчивости психологических свойств личности, которые характеризуют поведенческие стереотипы. Их можно использовать для осторожного манипулирования (выражаются через основные потребности, слабости, пристрастия, желания, идеалы).

Большинство социоинженеров действует по идентичным или близким шаблонам, поэтому, изучение приемов их "работы" позволяет выделить такие уровни взаимодействий с объектом влияния: доминирование, манипуляция, соперничество, партнерство, содружество.

Все методы социальной инженерии можно разделить на две группы:

1. **Удаленная социальная инженерия** реализуется средствами современных телекоммуникаций с использованием:

1.1. «Телефона».

Благодаря телефонии, социоинженер может оставаться анонимным и в то же время иметь прямую связь с целевым объектом. Последнее важно потому, что непосредственный контакт не дает собеседнику времени обдумать положение и взвесить все за и против. Решать нужно немедленно, причем под натиском социоинженера. Так как в телефонном разговоре происходит процесс обмена только звуковой информацией, большую роль в принятии решений играет интонация и голос собеседника. Данные характеристики подбираются в соответствии с моделью поведения социоинженера для получения информации о объекте воздействия, например:

а) **начальник** – человек, привыкший отдавать команды, ценящий свое время, добивающийся поставленных целей. Манера разговора жесткая, нетерпеливая. Полная уверенность в себе и легкое (или полное) пренебрежение к рядовым служащим. Своим тоном показывает, что проблема, с которой обратился – мелкая неувязка, которую нужно решить как можно скорее. Никаких просьб – только требования и указания. В ответ на недоверчивые или проверяющие реплики – допустимы негодование и запугивание собеседника.

б) **секретарь** – девушка (в большинстве случаев) с приятным голосом. Задача – выполнить конкретное поручение шефа, не отвлекаясь на условности. Она осведомлена о начальнике и некоторых его делах, между прочим, роняет достоверные факты (или недостоверные, которые нельзя проверить). Характер разговора – мягкий, с легким эротическим подтекстом (если собеседник – мужчина). Реакция на нежелание сотрудничать – бурное огорчение, жалоба, что начальство накажет.

в) **техслужащий** – сотрудник организации, который характеризуется снисходительным, но дружелюбным отношением к клиентам. Цель проста – устранить неполадку и избавить обе стороны от головной боли. Подчеркнутая специфическими терминами компетентность. На отказ сотрудничать – реакция удивления, так как сотрудничество в первую очередь выгодно для клиента. Никаких уговоров – просто дать

понять, что без его участия проблема только усугубится. Допустимо запугивание тяжелыми последствиями.

д) **пользователь** – работник, выполняющий свои обязанности и напуганный неожиданной проблемой. Четко выраженный мотив поскорее решить все проблемы и вернуться к своей рутинной работе. Отсутствие представления о характере проблемы, заинтересованность только в ее устранении. Характер общения – показать всю безнадежность своего положения и готовность отдаться в руки специалиста.

1.2. Глобальной сети Интернет.

Наиболее распространенными способами реализации методов СИ с помощью Интернет являются:

- a) проведение СИ посредством электронной переписки;
- b) проведение СИ через системы обмена сообщениями (ICQ, QIP, Skype, Miranda и др.);
- c) СИ на форумах, чатах, блогах.

В данных случаях успешная реализация СИ обусловлена правильностью разработки сценария общения.

2. Личный контакт. Наиболее трудоемкий и опасный метод социальной инженерии. Кроме выше перечисленных требований к сценарию общения и модели поведения, социоинженер должен уделить должное внимание своей внешности и манерам «живого» общения. Для правильного визуального восприятия, необходимо правильно подобрать:

- a) цвета в одежде и обуви;
- b) манеры и жесты при разговоре;
- c) положение в пространстве относительно собеседника.

Так же при применении методов социальной инженерии необходимо характеризовать собеседника. По голосу или же по внешности, следует определить какую слабость собеседника стоит использовать для достижения поставленной цели. К основным слабостям человека, эксплуатация которых в связке с правильно подобранной моделью поведения и сценарием разговора позволяет достичь ожидаемого результата, относятся:

- a) доверчивость;
- b) страх;
- c) жадность;
- d) отзывчивость;
- e) превосходство;
- f) милосердие.

Основными побудителями воздействия на объект СИ выступают: чувство достоинства индивида, его стремление к успеху, материальная выгода, получение удовольствия, комфорт, желание быть здоровым, наличие благополучной семьи.

Использование приемов скрытого и прямого манипулирования человеком дают возможность социоинженеру узнавать и в дальнейшем использовать полезную информацию в своих корыстных целях.

Практическое применение методов СИ, показывает, что почти в 100 % случаях достижение поставленной цели увенчивается успехом. Как следствие этого утверждения, возникает необходимость не просто предотвращения, выявления, учета, нейтрализации первопричин использования методов СИ, а и, во-первых, применения технологий безопасности в комбинации с требованиями политики информационной безопасности, во-вторых, установления правил поведения сотрудников, регламентированных должностными инструкциями, в-третьих, проведения тренинговых занятий направленных на повышение стойкости стереотипов сотрудников организации.

1. *Кузнецов М.В., Симдянов И.В.* Социальная инженерия и социальные хакеры. – СПб.: БХВ-Петербург, 2007. – 368 с.: ил.
2. *Жечко Т.М.* Как оценить человека за полчаса. – СПб.: Питер, 2008. – 160 с.: ил.
3. *Денис Ферри.* Секреты супер хакера.