УДК 65.012.8

студент А.А. Полосухин
ГВУЗ «Национальный горный университет»

МЕТОДЫ ЗАЩИТЫ СОТРУДНИКОВ ОТ АТАК, ОСНОВАННЫХ НА СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

В данных тезисах рассматривается понятие социальной инженерии. Основные направления атак, а также методы защиты от них.

Социальная инженерия (Социотехника) – это один из способов, который злоумышленники используют для получения доступа к компьютерам. Атаки, основанные на социотехнике, обычно проводятся с целью тайно установить программы-шпионы (или другие вредоносные программы) или обманным путем узнать пароли, важные личные или финансовые сведения.

Атаки, основанные на методах социотехники, можно разделить на пять основных направлений. [2]

- Сетевые атаки.
- Телефонные атаки.
- Поиск информации в мусоре.
- Персональные подходы.
- Обратная социотехника.

Сетевые угрозы

Сотрудникам компаний часто приходится использовать и обрабатывать электронные данные и запросы, полученные из внутренних и внешних источников. Благодаря этому злоумышленники могут налаживать отношения с сотрудниками компаний через Интернет, оставаясь при этом анонимными. Зачастую такие атаки предотвращаются использованием качественного антивирусного ПО. К сетевым атакам относят: так называемый Фишинг при котором злоумышленник выдает свои письма за письма реально существующих людей или компаний. Всплывающие приложения диалоговые окна предлагающие загрузить патчи для ПО например, или перейти на сайт злоумышленника. Атаки через службы мгновенного обмена сообщениями.

Угрозы связанные с использованием телефона

Телефонная связь обеспечивает уникальные возможности для проведения социотехнических атак. Это очень привычное и в то же время обезличенное средство общения, поскольку жертва не может видеть злоумышленника. Коммуникационные функции, поддерживаемые большинством компьютерных систем, могут также сделать привлекательной мишенью корпоративные телефонные станции. Объектами атак, кроме обычных пользователей, могут быть корпоративные телефонные станции, служба поддержки.

Угрозы связанные с утилизацией мусора

Несанкционированный анализ мусора часто позволяет злоумышленникам получить ценную информацию. Бумажные отходы компании могут содержать сведения, которые злоумышленник может использовать напрямую или которые облегчают ему проведение дальнейших атак.

Персональные подходы

В ходе, которых злоумышленник общается с жертвой личной, либо виртуально либо напрямую. Злоумышленник использует различные стратегии такие как – запугивание, убеждение, вызов доверия, предложение помощи.

Обратная социотехника

Более сложные методы в ходе которых ничего не подозревающая жертва сама рассказывает необходимую информацию злоумышленнику который в такой ситуации выступает в роли авторитета в технической или социальной сфере. Обычно злоумышленник, использующий методы социотехники, создает проблемную ситуацию, предлагает решение и оказывает помощь, когда его об этом просят. Рассмотрим следующий простой сценарий.

Атаки на основе социотехники могут нести разный ущерб от снижения работоспособности компании до финансовых потерь и урона репутации компании.

Социотехника и политики безопасности

Руководящие органы компании и представители ее ИТ-подразделения должны разработать эффективную политику безопасности и помочь реализовать ее в корпоративной среде. Иногда в политике безопасности основное внимание уделяется техническим средствам защиты, помогающим бороться с техническими же угрозами, примерами которых могут служить вирусы и черви. Средства защиты от социотехнических угроз должны помогать отражать социотехнические атаки на сотрудников компании.

Реализация мер защиты от угроз, основанных на методах социотехники

После того, как политика безопасности задокументирована и утверждена, нужно проинформировать о ней сотрудников и разъяснить им важность ее соблюдения. Технические средства защиты можно внедрить и без участия сотрудников, но при реализации мер защиты от социотехнических атак без поддержки сотрудников обойтись не удастся. Чтобы облегчить реализацию этих мер, нужно разработать для службы поддержки протоколы реагирования на инциденты.

Информирование

Осведомленный персонал будет более эффективно отражать атаки на основе социальной инженерии. Для этого должны проводится различные тренинги, кроме того сотрудники должны четко следовать политике безопасности. Прежде всего у сотрудников должна присутствовать такая черта характера как здоровый скептицизм.

Перечень литературы:

1. Максим Кузнецов, Игорь Симдянов. Социальная инженерия и социальные хакеры. БХВ-Петербург, 2007 г.

2. http://technet.microsoft.com/ru-ru/library/cc875841.aspx#ECAA