Сергей Мартынов

Социальная инженерия и информационная безопасность

9 февраля 2018, Москва

ACFE
Association of Certified Fraud Examiners

Association of Certified Fraud Examiners

Ассоциация сертифицированных специалистов по расследованию хищений

70 000 членов по всему миру

ACFE Russia

Профессиональные методики противодействия мошенничеству и защиты бизнеса

Мартынов Сергей Александрович

Президент российского отделения ACFE,
MSc in Criminal Justice,
CFE, CISA, CIA, CRMA
Профессиональный бухгалтер

Главная угроза информационной безопасности компании

Как Вы думаете, кто является наибольшей угрозой информационной безопасности Вашей компании? Варианты ответа:

- Зловредный хакер, нанятый конкурентами?
- Системный администратор, который не меняет пароли по умолчанию?
- Фирма-разработчик дырявых файерволов и не работающих DLP-решений?
- Мария Ивановна, старший бухгалтер отдела расчетов?

Первым этапом большинства кибератак является получение доступа к системе методами социальной инженерии

Что такое социальная инженерия?

- Это скрытое управление (манипуляция) действиями человека помимо его воли, без применения физического насилия или технических средств, на основе использования законов психофизиологических реакций, социальных навыков поведения, с целью заставить его выполнить определенные действия, не осознавая, что эти действия могут не соответствовать его интересам.

В чем разница между соц инженерией и:

- манипуляцией; - мошенничеством; -троллингом?

Какие инструменты используются в СИ?

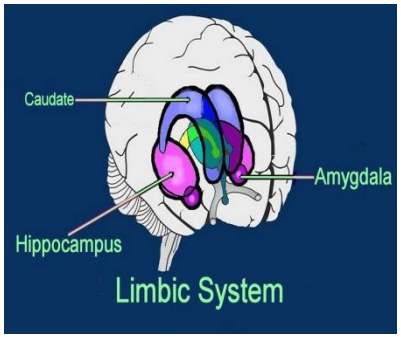
1. - Базовые физиологические реакции (страх, гнев, любопытство, жалость к себе, и так далее)
2. - Выученные социальные навыки: вежливость, помощь слабым, уважение к старшим, т.д.
3. - Социальные потребности человека («пирамида Маслоу»)
4. - Типология личности

1

Базовые физиологические эмоции

Они не могут полностью контролироваться человеком

- Страх, ужас
- Любопытство, интерес
- Радость (удовольствие)
- Удивление
- Гнев, ярость, азарт (охотничий)
- Горе, печаль, грусть, депрессия
- Отвращение, презрение



Примеры: «Смотри - вон птичка полетела»

«Налетай, торопись...»

1 Базовые физиологические эмоции

Задача социального инженера - помочь объекту атаки отключить критическое мышление. Для этого прежде всего надо спровоцировать его базовые эмоции.

Чем выше уровень эмоции, тем больше реакция определяется автономной нервной системой, теряется способность критически оценивать ситуацию

Реакция испуга

Реакции автономной нервной системы:

- Реакция человека на сильное эмоциональное воздействие: (опасность, стресс, нечто неожиданное):
- Первая реакция = Замереть (Freeze)
- Вторая реакция = Спрятаться (Hide) или Напасть (Fight) или Убежать (Flight)

Какую эмоцию выбрать для атаки? Это зависит от типа личности человека - объекта атаки

Пример: базовая реакция: азарт, гнев, ярость («Охота»):

1

Будем использовать эмоциональную реакцию азарта в погоне за добычей:

- Схема: Спровоцировать объект атаки принять задачу догнать цель (обещанием вознаграждения)
- Создать ощущение, что цель вот-вот будет достигнута.
- Отодвигать приманку, как при игре с кошкой, пока у атакуемого азарт преследования не блокирует способность критически мыслить.
- Предлагаем объекту выполнить действие, которое он бы никогда не сделал, подумав.

Шаг 1. Вы хотите прочитать эту статью? Её можно бесплатно скачать здесь.

Шаг 2. А теперь надо только зарегистрироваться, ввести свой мэйл и имя.

Шаг 3. Осталось совсем немного: книга в формате нашего ридера, который нужно скачать и установить, чтобы читать.

«Переполнение буфера»

Метод информационной перегрузки сознания. Человек мыслит примерно в 30 раз быстрее, чем говорит. Если говорить, используя многозначные слова и обороты речи, сложные конструкции предложений, то слушатель не будет успевать обдумывать все варианты смысла речи, чтобы принимать какие-либо решения.

Через некоторое время у слушателя наступает «переполнение входного буфера» (human buffer overflow). Он входит в состояние «потери сознательной реакции» и выполняет команды оператора.

Цыганский гипноз:

- «все о тебе знаю», «тебя ждет несчастье», «тебя ждет опасность в дороге», «сегодня нельзя ехать», «кто-то болеет». Параллельно –дезориентирующее шумовое и осязательное воздействие.

Эриксоновский гипноз:

- в текст историй все время вплетаются суггестивные команды или поведенческие установки, в которых увязает сознание слушателя. Более того, применяется «перекрывание реальностей», когда одна история вплетается в другую, третья во вторую и т.д.

Социальные навыки

Человек приобретает социальные навыки в процессе жизни, начиная обучаться с первых дней жизни.

Примеры социальных навыков:

- уважать старших;
- быть вежливым;
- помогать слабым;
- слушаться начальство ...

Авторитет:

2

- Лучшая линия поведения, чтобы выжить, если ты не можешь стать вожаком стаи - признать авторитет того, кто сильнее, и подчиниться ему.
- К тому же подчинение авторитету освобождает от необходимости думать своей головой - а это просто бесценно.

Авторитетом для бухгалтера является системный администратор или вообще любой сотрудник из службы ИТ-поддержки - ведь по мановению его руки компьютер может умереть или ожить снова. Поэтому указания ИТ, СБ (или людей, которые на них похожи, выполняются с отключенным мозгом)

Почему социальная инженерия -это абсолютное оружие?

- Человек не может жить в обществе, не выполняя множество социальных правил, не подчиняясь социальным законам поведения.
- Чтобы стать неуязвимым для социальной инженерии, человек должен отказаться от всех социальных навыков - не помогать, не знакомиться, не разговаривать - такой человек станет асоциальным и будет отвергнут обществом.

Что такое профессиональная деформация?

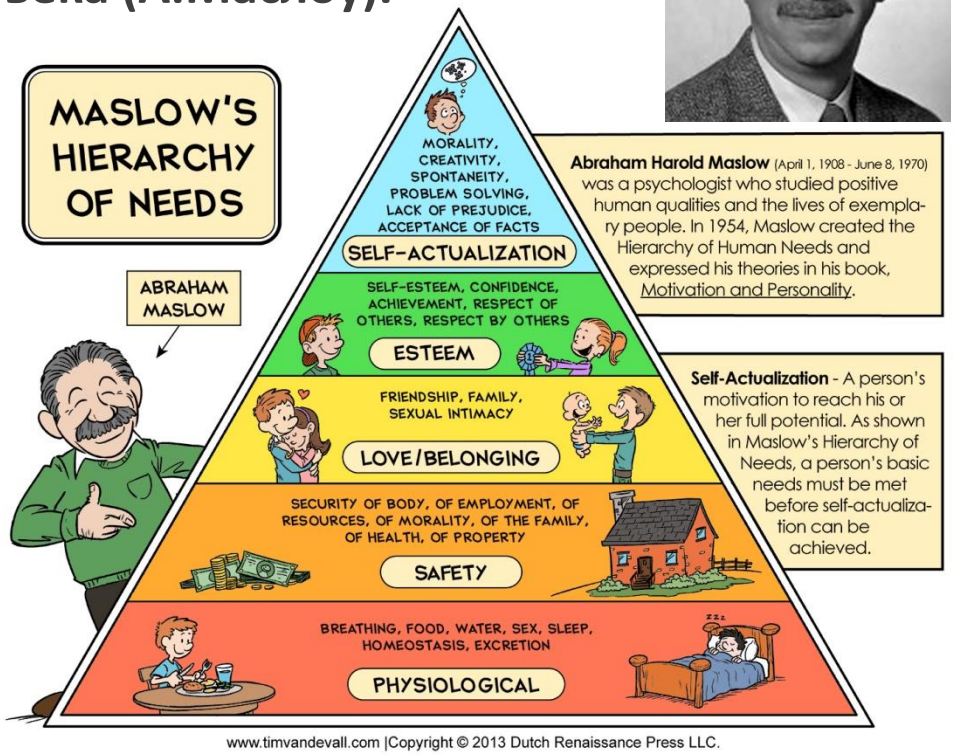
3 Социальные потребности человека

Теория иерархии потребностей человека (А.Маслоу).

Социальные потребности человека:

- **Потребность в принадлежности к сильной социальной группе (защите)**
- **Потребность в общественном признании, уважении со стороны социума**

Социальный голод не слабее физического!



Типология личности:

- Количество типологий личности превышает количество психологов.
- «Диагностическое и статистическое руководство Американской психиатрической ассоциации» DSM-IV
- Тест Д. Олдхэма (John M. Oldham) и Луи Морриса (Lois B. Morris)
- 14 типов личности

Пример: «Добросовестный тип личности»

- Люди добросовестного типа личности – высоких моральных принципов, они очень обязательны, не позволяют себе отдохнуть до тех пор, пока работа не выполнена и не выполнена правильно. Они преданны своим семьям, своему делу, своим начальникам. Упорный труд для них – норма.

Тип личности определяет способ контакта (что можно и нельзя говорить)

Разработка социальной атаки

1. Исходные данные:

   Цель атаки: загрузка вредоносного ПО, выполнение неправильных действий, предоставление доступа к компьютеру по сети, предоставление физического доступа в помещение, разглашение информации, получение социального доказательства (рекомендации).

2. Выбор объекта атаки:

   - Получение списка всех людей, имеющих доступ к необходимым ресурсам: помещениям, компьютерам, информации и т.д. или могущих быть агентом влияния на таких людей.

   - Составление списка 3-5 наиболее подходящих в качестве объекта атаки людей.

   - Сбор о каждом из них персональной информации:
     - в социальных сетях;
     - от соседей, сослуживцев, других источников, (видео и фото)

Разработка социальной атаки

3. Выбор схемы атаки:

- Оценка типа личности;
- Выбор базовых эмоций для воздействия на объект атаки
- Выбор социальной потребности объекта для использования в атаки

Разработка схемы атаки:

- тип базовой эмоции для блокирования критического мышления;
- тип аргументации к социальным потребностям объекта;
- определение способа побуждения к действию на основе типа личности объекта.

4. Техническая подготовка и репетиция атаки

- Уничтожение доказательств атаки
- Маскировка личности и целей атаки

Разработка схемы атаки: пример

- Особенности личности (добросовестный тип)
- С ним лучше всего сочетается реакция типа «беспокойство»
- К этой паре хорошо подходит прием игры в авторитет

- **Итак, волшебный треугольник атаки сложился**
- Получение указания от начальника, которое приводит человека в состояние стресса и отключает его критическое восприятие;
- Далее следует приказ открыть дверь, сообщить пароль или передать документ

- Внезапно возникает необходимость срочно поехать в командировку; составить новую справку; обработать – вам будет установлен новый код доступа; цейтнот; гипс снимают, клиент уезжает… Электронное письмо от руководителя. Обнаружена ошибка в вашем отчете. Необходимо срочно подготовить незначащий документ. За ним придет некто… кого вы не знаете. Он принесет вам необходимую информацию.

Вопросы?

MS Business Security Consulting Oy

«Истина рождается как ересь, а умирает как предрассудок».

Инжиниринг систем безопасности бизнеса

martynovsa@mac.com