Социальная инженерия

Социальная инженерия-

манипулирование человеком или группой людей с целью взлома систем безопасности и похищения важной информации.

(В отл. от социального программирования, которое применяется не только для взлома, но и для других целей: обуздания толпы, победы на выборах и т.д. и реализуется без использования ЭВМ).

Человек понимается как часть

ая
ы-
с
анием
кого
eople
н из
тов
XI века.

Роль человеческого фактора в защите информации.

- Взлом систем защиты информации от несанкционированного доступа, систем охранной сигнализации и т. д. в 80% случаев происходят из-за человеческого фактора.

Психологические предпосылки (схема Шейнова В.П.)

- Формирование цели воздействия на объект;
- Сбор информации об объекте воздействия;
- Обнаружение наиболее удобных мишеней воздействия;
- Аттракция (от лат. attralure- привлекать, притягивать)- создание нужных условий для воздействия на объект;
- Понуждение к нужному действию;
- Нужный итог.

(Обратная социальная инженерия- создание условий, при которых объект сам просит вас придти).

- Проблема «уборщицы»
- Выставки и презентации

Проблема- наказание за кражу БД предприятия- практически никакой. В судах практически нет обращений от организаций, у которых крадут информацию.

- **Правило 1.** Ни один из сотрудников предприятия не должен знать больше, чем ему полагается знать по должности *(подавляющее большинство людей не может хранить секреты).*

- **Правило 2.** В трудовом контракте обязательно должен быть пункт об ответственности сотрудника, вплоть до уголовной.

Области применения социальной инженерии

- Финансовые махинации *(Наташа+Илья=…)*
- Конкурентная разведка

  – Информация о маркетинговых планах организации *(выставки, интервью с ключевыми лицами и т.д.)- см. правила 1 и 2.*
  – Воровство клиентских баз данных - *правила 1 и 2* + *доступ в офис и к серверам.*
  – Информация о наиболее перспективных сотрудниках
  – Информация об организации с целью последующего уничтожения конкурента

Области применения социальной инженерии

- Фишинг и другие способы кражи паролей с целью доступа к персональным банковским данным частных лиц *(Защита: генерация одноразовых паролей, использование USB устройств, мобильное подтверждение, хэширование паролей…)*
- Фарминг – изменение адресов так, чтобы страницы, которые посещает пользователь были не оригинальными, а фишинг- страницами.
- Общая дестабилизация работы организации
- Рейдерские атаки (методы социального инжиниринга применяются на первом этапе – сбора информации).

Настройка «человеческого брандмауэра»-

постоянная работа.

«Безопасность – это процесс».

Защита информации должна быть системной.