Как противодействовать социальной инженерии?

SYNESIS
STRATUS

#whoami

CISSP, OSCP, CCNA Cyber Ops

Суть проблемы

Компании строят свою защиту против технических векторов атак часто забывая о людях

С точки зрения атакующего

Социальная инженерия является последним и, зачастую, самым эффективным инструментом проникновения

Основа противодействия

В основе противодействия стоит осведомленность

Программа повышения осведомленности об атаках - обязательная часть политики безопасности.

Чтобы знать как защищаться, нужно знать как нападают

Фишинг

- Открытие документа с макросом
- Запуск исполняемого файла
- Эксплуатация уязвимостей браузера, pdf-ридера и т.п.
- Переход по ссылке и ввод своих данных в поддельную форму аутентификации.

Чтобы знать как защищаться, нужно знать как нападают

Вишинг (звонки)

- Я из технической поддержки банка/оператора связи/клуба и т.д., необходимо изменить ваши учетные данные….
- Вас беспокоит участковый, проверка ваших данных...
- Мы из торговой сети, вы стали участником рекламной игры, нужны ваши данные...

Чтобы знать как защищаться, нужно знать как нападают

Tailgating или Piggybacking

- Несанкционированный проход злоумышленника вместе с законным пользователем через пропускной пункт.

Road Apple (“находки”)

- Распространение “зараженных” носителей информации (флешки, диски, и т.д.) как бесплатных “потерянных” вещей на парковке, в офисном здании, кафе возле офиса и т.д.

Основа воздействия атакующего

- Осведомленность атакующего (ФИО сотрудников, понимание процессов, используемые технологии);
- Уверенность атакующего (наглость);
- Неопытность сотрудника (ссылки атакующего на “псевдо” поручения и начальников “звоню по поручению..”);
- Эксплуатация человеческих слабостей и эмоций (лень, страх, жадность, сочувствие, увлечения);
- Подтарапливание;
- Информационная перегрузка.

Как противодействовать

- Корпоративная культура и ответственность (Security is everyone's responsibility)
- Рабочая программа повышения осведомленности об атаках
- Следование лучшим практикам и принципам (принцип наименьших привилегий, принцип многоуровневой защиты, необходимого доступа) при проектировании безопасности IT
- Физическая/логическая изоляция подразделений
- Penetration Tests and Red Team Exercises (тесты на проникновения и наступательные операции)

Спасибо за внимание!