

Оценка осведомленности персонала в вопросах информационной безопасности (социальная инженерия)

Процесс комплексной оценки осведомленности сотрудников компании в области информационной безопасности, а также эффективности применяемых средств защиты.



Оценка осведомленности персонала в вопросах информационной безопасности представляет собой практическую оценку путем рассылки писем с текстом, мотивирующим на:

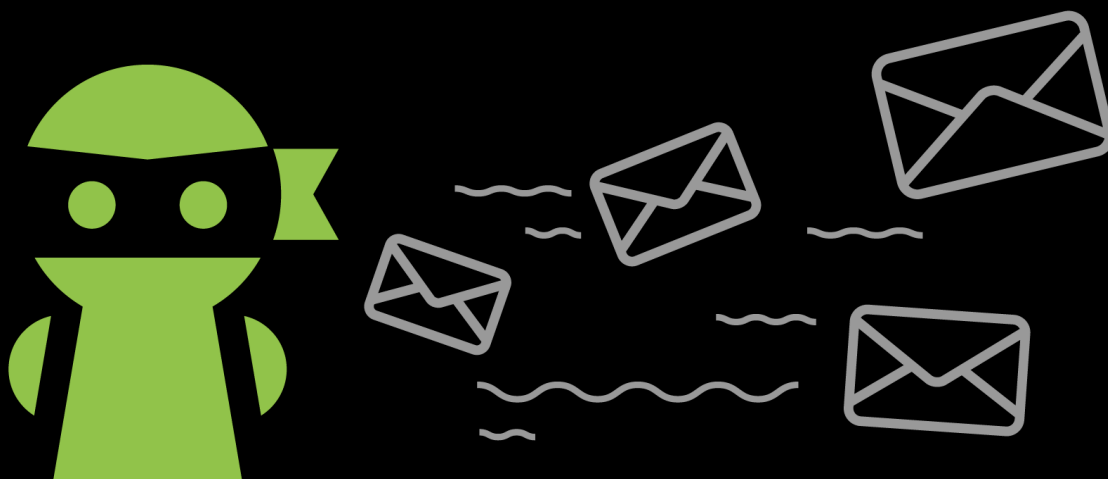
- переход по ссылкам
- ввод учетных данных
- запуск файлов



Анализ эффективности средств защиты

— процесс практической оценки эффективности, подразумевающий тестирование возможности обхода средств защиты.

Для выявления слабых мест защиты мы опираемся на лучшие мировые практики, рекомендации производителей и собственный опыт тестирований на проникновение и проектов по оценке защищенности.



Используемый нами подход включает:

- Сбор информации о сотрудниках в общедоступных источниках
- Разработку наиболее эффективного вектора социальной атаки и сценария ее реализации
- Подготовку полезной нагрузки с низким показателем обнаружения (реализуется исходя из выбранного вектора социальной атаки)
- Подготовку фишингового веб-сервиса в случае необходимости (реализуется исходя из выбранного вектора социальной атаки)
- Формирование массовой или целевой фишинговой рассылки (в зависимости от целей)
- Проведение теста на проникновение с использованием методик, основанных на социальной инженерии путем углубления атаки через эксплуатацию рабочей станции (для сценариев с вложением) либо путем использования учетных данных (для сценариев с фишинговым ресурсом)
- Анализ эффективности работы антиспам-защиты



Результаты

- Полученные учетные данные
- Перечень лиц, которые слабо осведомлены в вопросах фишинговых рассылок
- Высокоуровневая оценка эффективности антиспам-защиты на основе результатов рассылки
- Аналитика по результатам тестирования
- Отчетные документы по результатам проведения оценки осведомленности пользователей, включающие статистику и рекомендации по оптимизации программ осведомленности

Контакты



Денис Липов

Партнер,
управление рисками
dlipov@deloitte.ru

+7(495)787-06-00 (доб. 3071)



Юлия Гончарова

Старший менеджер,
управление рисками
ygoncharova@deloitte.ru

+7(495)787-06-00 (доб. 5086)



Софья Микова

Старший консультант,
управление рисками
smikova@deloitte.ru

+7(495)787-06-00 (доб. 1311)

Наименование «Делойт» относится к одному либо любому количеству юридических лиц, в том числе аффилированных, совместно входящих в «Делойт Туш Томацу Лимитед» (далее — «ДТТЛ»). Каждое из этих юридических лиц является самостоятельным и независимым. Компания «ДТТЛ» (также именуемая как «международная сеть «Делойт»») не предоставляет услуги клиентам напрямую. Более подробную информацию можно получить на сайте www.deloitte.com/about.

«Делойт» является ведущей международной сетью по оказанию услуг в области аудита, консалтинга, финансового консультирования, управления рисками и налогообложения, а также сопутствующих услуг. «Делойт» ведет свою деятельность в 150 странах, в число клиентов которой входят около 400 из 500 крупнейших компаний мира по версии журнала Fortune. Около 330 тысяч специалистов «Делойта» по всему миру привержены идеям достижения результатов, которыми мы можем гордиться. Более подробную информацию можно получить на сайте www.deloitte.com.

Настоящее сообщение содержит исключительно информацию общего характера. Ни компания «Делойт Туш Томацу Лимитед», ни входящие в нее юридические лица, ни их аффилированные лица не предоставляют посредством данного сообщения каких-либо консультаций или услуг профессионального характера. Прежде чем принять какое-либо решение или предпринять какие-либо действия, которые могут отразиться на вашем финансовом положении или состоянии дел, проконсультируйтесь с квалифицированным специалистом. Ни одно из юридических лиц, входящих в международную сеть «Делойт», не несет ответственности за какие-либо убытки, понесенные любым лицом, использующим настоящую публикацию.