# Проверка осведомлённости сотрудников

«Человеческий фактор» — одна из самых распространённых угроз информационной безопасности. Злоумышленники успешно пользуются любопытством, жадностью и желанием развлечься обычных пользователей. Чтобы снизить риски эксплуатации человеческих ошибок применяются технические и административные методы защиты. Один из таких методов — повышение осведомлённости в области ИБ.

Мы проверяем уровень осведомлённости сотрудников заказчика в вопросах информационной безопасности, оцениваем эффективность инвестиций в защиту информации. Главное для заказчика такого исследования — не найти и публично покарать «виновного» невнимательного сотрудника, а выявить потенциально слабые места в защите и устранить эти недостатки.

Исследование может быть отдельным проектом или частью тестирования на проникновение.

Наши цели в рамках такого исследования отличаются от целей настоящих злоумышленников. Злоумышленники стараются заразить рабочие станции пользователей и развить атаку, попав во внутреннюю инфраструктуру организации, чтобы получить конфиденциальную информацию. Мы же пытаемся узнать, как вёл себя пользователь: открыл ли вложение или перешёл по ссылке.

## Семь этапов атаки

### Согласование со Службой ИБ

В первую очередь мы получаем разрешение на проведение работ. Со Службой информационной безопасности согласовываются сроки и методы проверок.

В некоторых случаях требуется добавить адреса «Перспективного мониторинга» в «белый список». Это нужно для моделирования ситуации, когда технические средства защиты не справились со своей задачей и не смогли заблокировать вредоносные вложения или ссылки.

### Планирование атаки

На этом этапе необходимо определить состав целевых групп, в отношении которых будет проводиться тестирование. Есть два подхода:

- заказчик сам определяет группы целей для рассылки;
- исследователи сами подбирают состав групп.

Первый подход является предпочтительным, благодаря ему можно наиболее полно решить задачи заказчика.

Если в исследуемой организации уже проводятся мероприятия, направленные на повышение осведомлённости сотрудников в вопросах ИБ, то мы формируем список проверок исходя из применяемых обучающих материалов.

С заказчиком также обсуждается, какой именно канал коммуникации будет использован для контакта с персоналом: корпоративная почта, социальные сети или что-то другое.

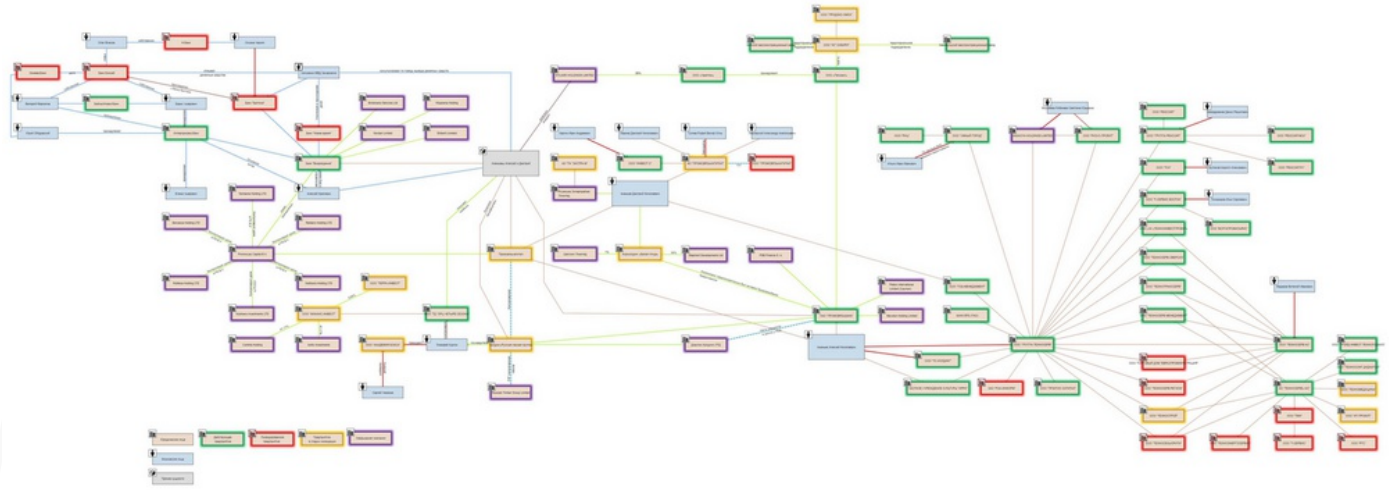
# Сбор информации о компании и сотрудниках из открытых источников

Успешная атака с использованием методов социальной инженерии всегда строится на доверии. А кому доверяют больше всего? Своим.

Чтобы стать «своим», исследователь «Перспективного мониторинга» изучает большой объём общедоступной информации:

- восстанавливает оргструктуру атакуемой организации;
- определяет руководителей и ключевых сотрудников, пытается найти сотрудников ИТ- и ИБ-подразделений, которым пользователи доверяют большое всего;
- получает максимальное число адресов электронной почты, восстанавливает шаблоны формирования адресов;
- получает список предполагаемых сотрудников;
- выявляет ключевых клиентов и партнёров.

Чем тщательнее собрана информация на этом этапе, тем больше шансов на успешную атаку. Заказчик также получит ответ на вопрос, какие данные о его сотрудниках можно найти в публичных источниках.



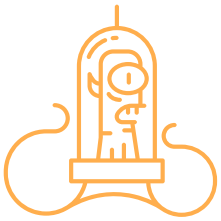
*Пример построения карты связей юридического лица*

Источниками информации могут быть:

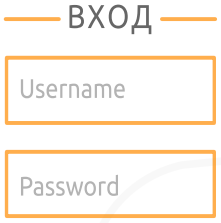
- собственные сайты организации;
- соцсети;
- блоги и форумы;
- сайты вакансий, сайты отзывов о работодателях;
- реестры информации о юридических лицах, судебных делах и решениях;
- площадки государственных и корпоративных закупок;
- конференции, митапы, вебинары.

## Подготовка «полезной нагрузки»

В рамках проверки осведомлённости мы используем три инструмента.



Первый инструмент — **вредоносное вложение** в сообщение или ссылка. Имитирует заражение вредоносным программным обеспечением. При таком варианте используются те же техники, что и в реальных атаках: мы пробуем проэксплуатировать известные уязвимости операционных систем, офисных пакетов, просмотрщиков pdf-файлов, браузеров — программ, которые чаще всего используются в любой организации.




Второй инструмент — **фишинг**. Имитирует кражу учётных данных пользователя. Мы создаём поддельные фишинговые сайты, регистрируем похожие на легитимные домены, чтобы заставить пользователя ввести свои реальные учётные данные.


Третий инструмент — **размещение USB-накопителей** рядом с офисом атакуемой организации. Имитирует доставку вредоносного ПО с помощью съёмных носителей. Согласно докладу на 37th IEEE Security and Privacy Symposium, 48% людей подключают найденные флешки. Это невероятно результативная атака.

## Контакт с жертвами

После разведки и подготовки инструментов атаки начинается непосредственно атака.

Основная задача исследователей «Перспективного мониторинга» на этом этапе — сделать так, чтобы как можно больше пользователей выполнили целевое действие (перешли по ссылке или открыли вложение), поэтому для каждой группы сотрудников будут свои темы писем и названия вложений.

### Все сотрудники

Приказ об увольнении

Повышение заработной платы

Внимание! Технические работы!!!

### Бухгалтеры

Отчёт

Акт выполенных работ

Акт сверки

Счёт на оплату

### Юристы

По делу №###

Досудебная претензия от ООО «Вашглавныйзаказчик»

| Продавцы | Пиарщики |
| --- | --- |
| Запрос предложений | Запрос по реальному информационному поводу |
| Конкурс на закупку | Интервью «Название отраслевого СМИ» |

Телефонный звонок сразу за отправкой сообщения поможет убедить жертву выполнить целевое действие.

*— Здравствуйте! Я менеджер по закупкам «Большого заказчика». Я десять минут назад послал вам запрос на коммерческое предложение. Получили? Нет?! Тогда давайте я вам продублирую ещё раз. Посмотрите, пожалуйста. Заранее спасибо. Всего доброго!*

## Заражение и эксплуатация

Для заражения мы используем известные уязвимости программного обеспечения, на которые уже существуют публично доступные эксплоиты — программный код, эксплуатирующий конкретную уязвимость. Мы модифицируем такой код, убираем из него действительно вредоносную часть, оставляя только механизм заражения конкретного компьютера пользователя, и добавляем инструменты сбора статистики. Благодаря такому подходу мы можем отследить и зафиксировать в отчёте каждый случай запуска нашего кода: кто, когда и при каких обстоятельствах мог бы подвергнуться реальному нападению.

Наш «троянский код» абсолютно безопасен: он не похищает конфиденциальную информацию, не уничтожает данные и полностью удаляется по завершении проверки.

Такой же подход применяется и при фишинговых атаках. Мы оперативно оповещаем администраторов безопасности о скомпрометированных учётных записях и просим сменить пароль пользователя.

## Подготовка отчёта

Благодаря встроенным в нашу «полезную нагрузку» механизмам, мы можем фиксировать следующие действия пользователя:

- переход по ссылке (злоумышленник мог заразить компьютер пользователя, эксплуатируя уязвимость в его операционной системе или браузере);
- скачивание чего-либо с подконтрольного нам сайта (злоумышленник мог заразить трояном);
- запуск нашего вложения в сообщении (злоумышленник мог заразить трояном);
- подключение съёмного носителя (злоумышленник мог заразить трояном);
- ввод данных в форму на подконтрольном нам ресурсе (фишинг).

Пентест считается успешным, если произошло хотя бы одно заражение или ввод реальных учётных данных.

Отчёт о проведённом исследовании будет содержать описание методов социальной инженерии, которые использовались во время проверки, оценку возможности проникнуть в информационную систему организации и рекомендации по повышению уровня защищённости.

Подробнее о всех услугах и продуктах компании на сайте amonitoring.ru

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ