Подготовка 1

Установить контакты, выработать процедуры, собрать необходимую информацию для оптимизации временных затрат в момент инцидента.

- Улучшить уровни осведомленности пользователей и политики безопасности компании

Не сообщать никакой личной или профессиональной информации (логины, пароли, id, пользовательскую информацию, адреса, номера телефонов, занимаемую позицию, ИНН и т.д.) посторонним лицам.

Цель использования методов социальной инженерии – получение незаконного доступа к информации сотрудников, секретам предприятия, клиентским или пользовательским данным.

В случае обнаружения, необходимо сообщить о всех подозрительных событиях вашему руководителю или начальнику отдела безопасности.

- Формализовать процесс переадресации подозрительный входящих звонков на специально организованную «Красную линию».

«Красная линия» должна быть обозначена как «Социальная инженерия», «Мошеннические звонки» или «Подозрительные звонки». Сотрудники должны быть в состоянии легко идентифицировать номер «Красной линии» посредством корпоративного телефонного справочника. «Красная линия» должна быть специально оборудована для записи поступающих звонков.

- Подготовиться к ведению диалога со злоумышленниками с целью выявления природы собираемой информации, целей атаки и идентификации атакующей стороны.

- Сверить ваши действия с юридическим отделом для проверки легальности ваших намерений в соответствии с местным законодательством.

Обнаружение 2

Обнаружить инцидент, определить затрагиваемый периметр, привлечь к решению компетентные стороны.

- **Телефонный звонок:** попытка выведать конфиденциальную информацию по телефону.

- Если звонящий запрашивает информацию, входящую в область интересов конкурентов, ответить отказом и следовать фазе «Сдерживание».

- Если звонящий позиционирует себя в качестве сотрудника компании, однако его номер не определяется или замаскирован, предложить перезвонить ему по внутрикорпоративному номеру. Если звонящий отказывается, далее следовать в соответствии с фазой «Сдерживание».

Злоумышленники могут прибегнуть в нескольким техникам «развязывания» языка жертвам, таким как страх, любопытство, сочувствие, и т.д. Не разглашайте информацию не под каким видом.

Внимательно выслушайте суть запросов звонящих и попросите их контактные данные для того, чтобы связаться ними «после уточнения информации по их запросам». В течение всего диалога, делайте заметки и сохраняйте спокойствие, даже если злоумышленники кричат или угрожают вам – атакующие пытаются играть на человеческих слабостях.

Если есть возможность вовлечь звонящих в двусторонний диалог, постарайтесь уточнить:

- имя звонящего;
- акцент, особенности речи;
- использование профессионального сленга, знания атакуемой организации;
- фоновые шумы.

- **E-mail:** получение неавторизованных запросов на разглашение конфиденциальной информации.

- Если запрашиваемая информация входит в область интересов конкурентов перейти к фазе фазе «Сдерживание».

- Если контактирующая сторона использует корпоративный имэйл, задавая при этом нехарактерные или странные вопросы, попросить пояснений, после чего ответь на сообщение, поставив в копию руководителя звонящего (найти в справочнике).

- Уведомить руководство об атаке методами социальной инженерии Оно может иметь лучшее понимание о возможных целях атаки.

Сдерживание 3

Минимизировать эффект от атаки

До перехода к данной фазе вы должны удостовериться в том, что имеете дело именно с социальной инженерией.

Действия сотрудников

- **Телефонный звонок**

- Если звонящий требует от вас контактов разыскиваемого лица следуйте рекомендациям ниже:
  - Воспользоваться корпоративным справочником
  - Найти номер «Красной линии»
  - Передать звонящему
  - Немедленно связаться с вашей CERT/CSIRT командой, передать суть инцидента и характер запрашиваемой злоумышленниками информации.

- Если звонящий оказывает слишком сильное давление и не дает время для нахождения номера «Красной линии», сослаться на срочное собрание и попросить перезвонить позже

- Если звонящий требует перевода линии на нужного ему сотрудника компании:
  - Поставить звонящего в режим ожидания, позвоните с вашей CERT/CSIRT командой и изложите суть инцидента.
  - Перевести звонящего на телефон вашей CERT/CSIRT командой (не выдавать номер команды злоумышленнику).

- **E-mail**

- Переадресовать сообщение вместе со служебными заголовками отделу безопасности/CERT/CSIRT (приложение в .msg, .eml) для расследования, профайлинга и геолокализации злоумышленника.

Сдерживание 3

Действия CERT / CSIRT / Отдела безопасности

- **Телефонный звонок**

Возобновить разговор со злоумышленником, используя следующие методы:

- выдать себя за искомого сотрудника;
- затянуть разговор в ожидании ошибки со стороны звонящего;
- объяснить звонящему, что использование методов социальной инженерии запрещено законом и может караться соответствующим образом; объясните звонящему, что, в случае продолжения попыток с его стороны, передадите его дело в юридический отдел для оформления официальной жалобы.
- Если, в течение атаки, номер «Красной линии» стал известен атакующей стороны, рассмотрите возможность замены его на другой с изменением записи в справочнике .

- **E-mail**

Собрать как можно больше информации по идентифицированному адресу:

- Проанализировать служебные заголовки и геолокализовать злоумышленника
- Осуществить поиск владельца email в Интернете и социальных сетях
- Проанализировать различные схемы атак методами социальной инженерии для лучшего понимания угрозы.

Устранение 4

Принять меры для ликвидации угрозы и предотвращения будущих инцидентов.

Способы работы по данному типу инцидентов:

- Оповестить / подать жалобу в правоохранительные органы.
- Обсудить инцидент и обменяться опытом с доверенными внешними контактами.
- Пригрозить злоумышленнику применением юридических методов воздействия.

Восстановление 5

Вернуться к нормальному режиму работы

Проинформировать руководство об инциденте; оповестить о принятых решениях, совершенных действиях и их результатах.

После инцидента 6

Проинформировать центральное руководство, филиалы и партнеров для внедрения дополнительных мер безопасности на местах.

Отчет

Написать отчет об инциденте; сделать отчет доступным причастным лицам. Раскрыть следующие темы:

- Причины инцидента
- Действия и сроки
- Верные действия
- Неверные действия
- Стоимость инцидента

Капитализация опыта

Используя накопленный опыт, оптимизировать меры по предотвращению утечек информации путем социальной инженерии.

SOCIETE GENERALE | CERT | SOCIETE GENERALE

Incident Response Methodology

cert.sg@socgen.com / cert.societegenerale.com / @certsg

IRM #10

Социальная инженерия

Реагирование на использование методов социальной инженерии

Автор IRM: CERT SG
Версия IRM: 1.1 (RU)

Об IRM

Данная методология по реагированию на инциденты ИБ является кратким руководством, предназначенным вниманию специалистов, работающих над проблемами безопасности:

- Системные администраторы
- Члены Security Operation Centers
- Начальники и представители отделов ИБ
- Представители CERT/CSIRT/IRT

Распространение IRM возможно в рамках SG Group.

В случае обнаружения признаков инцидента, следуйте рекомендациям IRM, делайте заметки, не поддавайтесь панике и немедленно оповестите свой CERT.

Фазы управления инцидентами ИБ

Шесть фаз управления инцидентами ИБ:

- **Подготовка**: подготовится к управлению инцидентом
- **Обнаружение**: идентифицировать проблему
- **Сдерживание**: ограничить негативный эффект
- **Устранение**: ликвидировать угрозу
- **Восстановление**: восстановить до нормального
- **После инцидента**: формализация и совершенствование процесса управления инцидентом

IRM предоставляет детальную информацию по каждой из фаз.