

## Подготовка

1

Установить контакты, выработать процедуры, собрать информацию для оптимизации временных затрат во время инцидента.

### Контакты

■ Внутренние: безопасность, команда реагирования на инциденты, юристы, и т.д.

■ Внешние: правоохранительные органы, детективы.

Убедиться в наличии возможностей для сбора данных посредством привлечения дополнительных контактов, знакомых с данной проблематикой.

### Информационная работа

Убедиться в достаточном уровне осведомленности сотрудников по проблематике данного типа инцидентов. Повышение уровня осведомленности возможно посредством проведения специальных информационных программ и семинаров.

Формализовать процесс реагирования с подробным распределением ролей ответственным лицам и командам.

## Обнаружение

2

Зафиксировать инцидент, определить затрагиваемые интересы, привлечь компетентные стороны.

■ Уведомить причастных лиц.

■ Сохранять любую информацию, имеющую отношение к инциденту. Сохранять всю переписку, записывать любую поступающую информацию, держать журнал входящих контактов. Например “телефонный звонок” / “номер звонящего” / “время разговора” / “суть переданной информации”.

■ Постараться получить как можно больше информации о злоумышленниках (имена, номера телефонов, геолокализация, электронные средства связи, психологический портрет, особенности речи, шумы на заднем фоне, и т.п.).

■ Оговорить возможные варианты действий с командой реагирования и юристами.

■ В случае вовлечения в инцидент важной внутренней информации, проверить на наличие соответствующих резервных копий; если произошла утечка информации – узнать каким образом.

■ Уведомить руководство о зафиксированной попытке шантажа и отчитаться по принятым мерам реагирования на инцидент в соответствии с ранее определенным процессом.

## Сдерживание

3

### Минимизировать риски от инцидента

Определить варианты реагирования на требования и последствия каждого из вариантов. Каковы возможные последствия игнорирования, положительного и отрицательного ответов.

### Наиболее распространенными вариантами угроз являются:

■ Атака на отказ в обслуживании (DDoS).

■ Публичное раскрытие конфиденциальных финансовых данных.

■ Раскрытие конфиденциальных данных о сотрудниках, клиентах или заказчиках предприятия.

■ Блокировка доступа к данным со стороны предприятия или его сотрудников посредством их удаления или использования специализированных информационных технологий, таких как, например, ransomware.

■ Осуществление массовых рассылок от лица шантажируемой компании.

### Проверка

■ Проверить имели ли место быть подобные случаи шантажа в прошлом. Существует ли опыт работы по схожим инцидентам у других компаний.

■ Тщательно проверить и проанализировать все найденные технические сведения для последующего использования в расследовании;

■ Проверить возможность причастности к инциденту:

■ Конкуренты

■ Идеологически мотивированные группы

■ Бывшие сотрудники

■ Постараться определить злоумышленников исходя из собранной информации.

■ Определить каким образом злоумышленник получил доступ к объекту шантажа.

## Сдерживание

3

Проинформировать компетентные органы.

В зависимости от ситуации, постараться выиграть время, затянув переговоры:

■ **Потребовать доказательства серьезности намерений шантажирующей стороны или наличия у нее интересующих вас данных.**

■ **Запросить дополнительное время для выполнения требований злоумышленников.**

## Устранение

4

**Принять меры по устранению угрозы.**

В случае, если объект шантажа попал в руки злоумышленников в следствие уязвимости в периметре технической структуры предприятия, немедленно устранить уязвимость.

■ После получения достаточного количества информации прервать дальнейшие активные контакты с вымогателями, предварительно обеспечив постоянный контроль за поступающей информацией. Дальнейшие шаги предпринимать по ситуации – в соответствии с глобальным планом реагирования на инцидент.

■ Не предпринимать никаких шагов в одиночку; вовлекать в процесс причастные департаменты.

**Помнить, что, один раз согласившись выполнить требования злоумышленников, вы открываете широкие возможности для последующих попыток шантажа.**

## Восстановление

5

**Восстановить нормальную работу системы.**

Уведомить руководство о предпринятых шагах и достигнутых результатах в рамках реагирования на инцидент.

## После инцидента

6

**Задokumentировать детали инцидента, обсудить извлеченные уроки, оптимизировать процессы защиты.**

Проинформируйте правоохранительные органы даже если вы не желаете возбуждать уголовное или административное дело по факту инцидента: другие юридические и физические лица могут быть также подвержены шантажу. Проинформировать об инциденте иерархию и дочерние структуры для совместного анализа ситуации и принятия четкой позиции в случае нападения на другие структуры группы.

### Отчет

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

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

### Капитализация опыта

Формализовать и задokumentировать опыт, накопленный в результате управления инцидентом с целью увеличения эффективности будущих действий.

## Incident Response Methodology

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

IRM #8

### Шантаж

Руководящие принципы реагирования на попытки шантажа

Автор IRM: CERT SG  
Версия IRM: 1.3 (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:** подготовиться 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.