Подготовка 1

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

Контакты

- Заручится рабочими контактами в рамках технических отделов предприятия: отдел безопасности, отдел реагирования на инциденты, техническая поддержка и т.д.
- Заручиться контактами в юридическом отделе, отделе по связям с общественностью и отделе кадров.
- Заручиться внешними контактами, главным образом для использования в рамках разыскной деятельности, в т.ч. в правоохранительных органах.

Политика безопасности

- Удостоверьтесь в том, что факт ценности производственной информации представлен во внутренних правилах, процедурах, программах повышения уровня осведомленности сотрудников, тренингах и т.д.
- Дать четкое определение ценным информационным активам предприятия.
- Формализовать процесс эскалации инцидентов безопасности; распределить роли и назначить исполнителей.

Обнаружение 2

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

Утечка данных может произойти в любом месте информационного периметра. Причиной утечки может стать действие сотрудника, умышленно или неумышленно обошедшего периметр информационной безопасности предприятия.

Step 1: Обнаружить проблему

- **Процесс оповещения об инциденте**

Внутренняя информация может служить хорошим источником обнаружения: неформальные разговоры сотрудников, наблюдения отдела безопасности.

- **Мониторинг открытых источников информации**

Регулярный мониторинг результатов поисковых систем и открытых баз данных могут позволить своевременное обнаружение утечек информации.

- **Средства DLP (Data Loss Prevention)**

В случае существования средств DLP, использование может предоставить дополнительные возможности команде реагирования на инциденты ИБ.

Step 2: Подтвердить существование проблемы

Не осуществлять никаких шагов без письменного разрешения CISO или иного уполномоченного лица. Также, попросите юристов подготовить письменную форму согласия вовлеченного пользователя на проведение вами мероприятий.

- **E-Mail:**

Данные могли быть утечь посредством отсылки с рабочего адреса электронной почты сотрудника.

Проанализировать траффик электронных сообщений подозреваемого лица на предмет подозрительных. Не проводить поиска в сообщениях с грифом «Private». При необходимости, заручиться письменным согласием сотрудника на осуществление данных действий и осуществлять в его присутствии.

Проанализировать соответствующие логи.

Использовать спец средства для проверки удаленных пользователем файлов, истории посещенных сайтов и другого подозрительного контента.

Обнаружение 2

- **Веб контент**

Утечка могла быть осуществлена посредством вебмейла, форумов, сайтов-хранилищ и т.д. Проверить логи прокси сервера на предмет подозрительных подключений пользователя.
Проверить журналы браузеров на машине пользователя. Не ограничиваться браузерами по умолчанию – проверить все установленные. Если момент утечки запротоколирован, сверить действия пользователя на момент утечки.

- **Внешние носители информации**

Возможно использование флешек, CD/DVD-приводов, внешних HDD, мобильных терминалов, карт памяти и др. Информация о когда либо использованных внешних USB накопителях остается в реестре системы. Криминалистический анализ способен подтвердить подключение внешних устройств; данные по записи на них внутренней информации нуждаются в более скрупулёзной корреляции.

- **Локальные файлы**

Даже если ничего не обнаружено, всегда есть возможность найти следы доступа к локальным файлам на системе подозреваемого. Не проводить поиск информации в Private зоне пользователя. Действовать в строгом соответствии с местными законами, определяющими рамки подобных вмешательств.

- **Передача данных по сети**

Также возможна передача данных по: FTP, IM, P2P, Remote Access Tools. Постараться отследить подобные действия пользователя по доступным логам.
Данные также могут быть отправлены через VPN туннель или на SSH сервер. Эти действия также можно определить, исходя из анализа логов. Переданные данные не могут быть идентифицированы в этом случае.

- **Печатающие устройства**

Данные могут быть распечатаны через сетевые принтеры. В этом случае проверить следы очереди заданий по распечатке. Некоторые принтеры фиксируют задания непосредственно на внутреннем жестком диске; проверить их.

- **Вредоносный код**

Если никакой информации не обнаружено, рассмотрите версию о возможной компрометации системы пользователя вредоносным кодом и действуйте в соответствии с соответствующим IRM.

Прим: Даже при кажущемся избыточном кол-ве доказательств, всегда старайтесь найти дополнительные. Если данные были переданы с системы А на систему Б одним из описанных каналов еще не означает, что они не было переданы на систему В другим методом. Используйте специализированные средства компьютерной криминалистики. Обратитесь к специалистам в случае необходимости.

Сдерживание 3

Минимизировать эффект от инцидента.

Оповестить руководство, отдел связей с общественностью и юристов; удостоверьтесь в готовности управления инцидентом с их стороны.

В зависимости от вектора утечки, заблокируйте внешний адрес хостинга, отправной источник или получателя обнародованной информации. Данные действия должны включить весь периметр системы информации предприятия.

Понизить уровень доступа инсайдера или полностью заблокировать его. В случае подтверждения версии умышленной утечки, изъять логические и физические устройства авторизации инсайдера. Перед принятием любых шагов, проконсультироваться с юристами и отделом кадров. Также, см. IRM 12 – Insider Abuse.

Изолировать (выключить питание сети / аккумулятор переносного компьютера) систему пользователя для последующего анализа методами компьютерной криминалистики.

Устранение 4

Принять меры по устранению угрозы и предотвращению будущих инцидентов.

Если данные были отправлены на публичные сервера, попросить владельца / вебмастер / хостинг провайдера их удалить. Если удаление невозможно, проанализировать утекшие данные и подробно проинформировать руководство и отдел по связям с общественностью. Отслеживать распространение данных по третьим сайтам и соцсетям; следить за комментариями и реакцией пользователей.

Обеспечить отдел кадров и юристов достаточной информации для подачи жалобы или судопроизводства.

Восстановление 5

Вернуться к нормальному режиму работы

В случае компрометации или взлома системы, восстановить до нормального состояния.

Оповестить об инциденте всех сотрудников или некоторые отделы выборочно для поднятия уровня осведомленности о проблемах информационной безопасности.

Удалить официальное сообщение по возвращению к нормальному режиму работы.

После инцидента 6

Задокументировать детали инцидента, обсудить извлеченные уроки, оптимизировать процессы защиты.

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 / раннему обнаружения утечек информации.

SOCIETE GENERALE | CERT | SOCIETE GENERALE

Incident Response Methodology

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

IRM #11

Утечки информации

Реагирование на умышленные утечки данных

Автор IRM: CERT SG
Версия IRM: 1.2 (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.