План действий на случай инцидента, связанного с риском утечки данных.

Как подготовиться и что делать, если...

КОНСТАНТИН ТИТКОВ

07.04.2025

О чем пойдет речь?

- Взаимосвязь инцидентов ИБ
- Роли участников при ликвидации инцидента ИБ
- Профилактика для снижения вероятности утечки
- Превентивные меры для минимизации последствий
- Мероприятия по подготовке к реагированию (специфика)
- Типовые шаги по реагированию на инцидент ИБ
- Дополнительные шаги в случае выявления утечки
- Рекомендации по разработке отчета о реагировании в случае утечки

NB: Настоящие рекомендации предназначены для команд ИТ и ИБ СМБ (SMB) и разработаны в целях быстрого и эффективного реагирования на инцидент с привлечением внешней экспертной организации, и не адресованы экспертам DFIR (Digital Forensic and Incident Response) или SOC (Security Operations Center) крупных и крупнейших компаний, т.к. предполагается, что такие эксперты профессионалы в своем деле и руководствуются в своей работе промышленными тематическими рекомендациями и стандартами, малая часть из которых упоминается в настоящем докладе.

Взаимосвязь инцидентов ИБ

- Утечка не приходит одна
- Дефейс
- Wipe / шифрование
- Атака на партнеров
- Шпионаж
- ~~Майнинг~~

Платить ли выкуп?

Как это вообще могло произойти?

- VPN, RDP, SSH, OWA, Jira, Confluence, Gitlab, Sharepoint и т.д. - неисправленная уязвимость или подбор пароля
- Фишинг
- WEB-приложение - уязвимость
- Компрометация доверительных отношений
- Атака на цепочку поставок
- Внутренний нарушитель
- И так далее…

Пятница и праздники

- Инцидент – это финал в цепочке событий, последний шаг
- Немедленно, быстро и эффективно (даже ночью)
- Готовность к инциденту
- Рассчитывайте на свои наработки и на дежурных сотрудников
- Возможность привлечь помощь – бесценна!

(и дешевле простоя в работе)

Роли участников при ликвидации инцидента ИБ

- Координатор работ
- ЛПР
- ИБ
- ИТ
- Юрист
- PR/Маркетинг
- HR

В случае утечки ПДн, дополнительно, ответственные за:

- обработку ПДн
- обеспечение безопасности ПДн

Профилактика для снижения вероятности утечки

- Учет допущенных лиц и управление доступом
- СЗИ для мониторинга и контроля действий со стороны внешнего нарушителя
- СЗИ для защиты от утечек информации со стороны внутреннего нарушителя
- Обработка ПДн и другой чувствительной информации в выделенном сегменте сети (комплекс стандартов PCI SSC говорит нам о том же)
- Шифрование, обезличивание, удаление, минимизация реквизитного состава и количества ПДн
- Обучение работников «цифровой гигиене» (security awareness)
- Контроль уязвимостей (VM, испытания, аудит, пен-тест, red-team, Bug Bounty)
- Парольные политики и аутентификация
- Физическая безопасность

Превентивные меры для минимизации последствий утечки

- Проведение оценки вреда, который может быть причинен субъектам ПДн
- Разработка сценариев и планов по реагированию на события, связанные с утечкой
- Определение методов выявления области компрометации данных
- Определение методов оценки последствий инцидента, порядка определения и применения мер для минимизации последствий
- Определение порядка и сроков оповещения должностных лиц и выполнения мероприятий
- Создание и испытания плана обеспечения непрерывности бизнеса
- Разработка и описание процесса создания резервных копий АС и данных, обеспечения их безопасного хранения, тестирования механизма восстановления данных из резервных копий
- Определение ответственных лиц на каждом из этапов

Реализация мероприятий для смягчения ответственности

Одновременное выполнение всех 3-х условий до момента вынесения постановления:

- ежегодные расходы оператора ПДн на мероприятия по ИБ, осуществленные в рамках лицензируемой деятельности, в течение 3 календарных лет, предшествующих году совершения правонарушения, составляли не менее 0,1 % годового совокупного размера суммы выручки, полученной от реализации всех товаров (работ, услуг), либо размера собственных средств (капитала) кредитной организации.
- документально подтвержден факт проведения в течение 12 месяцев, предшествующих моменту выявления правонарушения, аудита выполнения оператором ПДн требований к защите ПДн.
- отсутствуют обстоятельства, отягчающие административную ответственность (продолжение противоправного поведения несмотря на требование уполномоченных лиц о его прекращении, повторное совершение административного правонарушения в сфере ПДн и защиты информации).

Мероприятия по подготовке к реагированию (специфика)

- 24 часа с момента обнаружения утечки ПДн - уведомить об инциденте Роскомнадзор.
- 72 часов с момента обнаружения - направить отчет о результатах внутреннего расследования.
- Субъект КИИ - 24 часа с момента обнаружения утечки ПДн - уведомить НКЦКИ в соответствии с форматами представления информации о компьютерных инцидентах в ГосСОПКА.
- Поднадзорным ЦБ РФ необходимо направить информацию об инциденте в АСОИ ФинЦЕРТ. При этом информирование НКЦКИ не требуется.
- Если утечка произошла в результате хакерской атаки, оператор ПДн обязан направить информацию в ГосСОПКА о компьютерном инциденте, повлекшим неправомерную передачу ПДн.
- GDPR.

Мероприятия по подготовке к реагированию (специфика)

- Определить порядок информирования, а также требования со стороны указанных государственных органов к форме и составу предоставляемых данных об инциденте.
- Утвердить основные и резервные каналы информирования.
- Проверить наличие доступа к личным кабинетам.
- Определить адреса, телефоны и иные контактные данные, режим работы офисов территориальных отделений соответствующих органов с учетом филиальной сети вашей организации.
- Определить круг лиц, ответственных за составление, согласование и направление отчетов и уведомлений в рамках взаимодействия с государственными органами.
- Определить порядок информирования субъектов персональных данных об утечке, а также размещения информации об утечке в открытых источниках (включая пресс-релизы), а также круг лиц, ответственных за составление, согласование и направление/публикацию информации.
- Разработать и согласовать заранее шаблоны пресс-релизов.

Если случился инцидент. Экстренно …

- Заблокировать доступ к ДБО в банках
- Не выключать и не перезагружать зараженные узлы, не переустанавливать ОС пострадавших систем
- Отключить (физически вынуть Ethernet кабель) от ЛВС серверы с резервными копиями и важными данными
- «Снапшоты» текущего состояния, если виртуальные
- Не подключать накопители информации с важной информацией, включая резервные копии, к потенциально скомпрометированным системам
- Проверить исходящий в сторону сети интернет сетевой трафик
- Рассмотреть целесообразность изоляции от сети интернет всей или части вашей сети
- Позаботиться о режиме работы персонала
- Кто главный? (лицо, обличенное полномочиями, и ответственный за коммуникации) + прочие участники реагирования.
- Коммуникации только ВНЕ пораженной инфраструктуры
- Провести DFIR (Digital Forensic and Incident Response / цифровая криминалистика и реагирование на инциденты)
- Сохранять экземпляры вредоносного ПО, но не загружать его на общедоступные ресурсы
- Обратиться в правоохранительные органы
- Необходимость привлечения подрядчиков на реагирование и на восстановление ИТ-инфраструктуры
- Информировать клиентов и партнеров об инциденте (или нет?)
- Заглушка о «техническом сбое» на сайт (или нет?)
- Поддержать сотрудников, которые задействованы в ликвидации инцидента

И как это все будет?

- установочная встреча
- анализ скомпрометированных узлов
- поиск способа входа в инфраструктуру, всех пораженных узлов, закладок (RAT)
- анализ HDD и/или снятие с них копий с использованием блокираторов записи и так далее
- У 2-х экспертов DFIR режим работы 24/7: 8 часов эксперт работает в одиночку, 8 вдвоем с напарником, 8 на отдых
- Принимающая сторона обеспечивает аналогичный режим работы сотрудников ИТ и ИБ для эффективного взаимодействия
- Нужно быстрее – нужно больше экспертов DFIR (лучше обсудить желаемые сроки работ до выезда экспертов, а также их ставки)

Что приготовить к прибытию экспертов

- Рабочие места для экспертов (стол/стул/свет/электропитание)
- Чат ВНЕ корпоративного мессенджера с участием необходимых лиц (руководители ИТ и ИБ, представитель менеджмента, юрист, специалист службы маркетинга/PR)

Критически важна конфиденциальность чата

- «Режим тишины» во внутренней сети, включая: почту и приглашения на собрания, ТКС/ВКС, корпоративные мессенджеры, личные мессенджеры, если в них был осуществлен вход в корпоративной сети
- Предусмотреть синхронный режим работы сотрудников ИТ и ИБ с режимом работы экспертов DFIR
- Отмена отпусков, командировок, увольнений
- Компенсации за переработки

Шаги IR (1/6) Этап 1: Подготовка к будущему инциденту

Реализация политики хранения логов:

- *Настройка ведения журналов (логов) с достаточной детализацией*
- *Обеспечение безопасного хранения журналов (логов)*
- *Настройка длительности хранения журналов (логов)*

Физический доступ к содержимому каждого диска (HDD) с данными в компании с обеспечением возможности:

- *Взять диск в руки*
- *Расшифровать диск (если он зашифрован самой компанией в целях безопасности)*

Возможность доставать артефакты:

- *Сетевой доступ ко всем узлам*
- *Административные права для доступа ко всем узлам*
- *Хранение реквизитов доступа (паролей) для административного доступа ко всем узлам безопасным с точки зрения уничтожения образом (например на бумаге в противопожарном сейфе)*

Резерв оборудования, вычислительных мощностей и дискового пространства для временного или постоянного развертывания ИТ-инфраструктуры или ее части без отключения зараженных (взломанных) узлов, потребляющих ресурсы

Обеспечение удаленного хранения резервных копий и данных (согласно правилу резервного копирования «3-2-1»)

Шаги IR (2/6)
Этап 2: Идентификация того, что инцидент произошел

Вам необходимо знание того, куда смотреть, чтобы понять, что инцидент начался
Например:

- Источники Threat Intelligence фидов с данными о возможной подготовке атаки на вашу компанию (регистрация фишинговых доменов, объявления о покупке или продаже доступа в вашу сеть и т.д.)
- SIEM/SOC
- MDR
- Централизованный (!) EDR/XDR
- Централизованный (!) AV
- …
- Система ИТ-мониторинга для контроля работоспособности и выявления отключения средств защиты
- …
- Экран зашифрованного компьютера (если вы не озаботились пунктами выше)
- Телеграмм-каналы с данными о взломах и утечках (вы одним из первых прочтете про свою компанию по пути на работу, пока в офисе еще никого нет, но все уже зашифровано или удалено…)

Шаг 3/6 IR Этап 3: Изоляция выявленного пораженного злоумышленниками ИТ-парка оборудования

- НЕ отключать электропитание!
- НЕ перезагружать!
- Отключать от ЛВС:
  - Виртуальные машины - на уровне системы управления виртуализацией отправить в “down” сетевой интерфейс (все сетевые интерфейсы ВМ)
  - Физические машины - вынуть сетевой провод из сетевой карты (RJ45 или оптику) Или вынуть провод на свиче. Или погасить порт на свиче
  - Wi-Fi - погасить сетевой интерфейс в ОС
  - Или погасить Wi-Fi точку доступа
  - Или на точке доступа заблокировать узел по MAC (в случае уверенности что злоумышленник не имеет доступа к узлу по другим интерфейсам + сменить пароль Wi-Fi на случай автоматической смены MAC зловредной программой)

Шаги IR (4/6) Этап 4. Зачистка

- Удалить троянов/закладок/web-шелов/RAT и т.д.
- Установить **обновления безопасности** для устранения уязвимостей, включая новейшие обновления (*могут закрывать еще не опубликованные, но уже известные злоумышленникам уязвимости*)
- Установить и настроить **средства защиты** (*которые, как правило, отключаются или “портятся” злоумышленниками*)
- **Сменить пароли.** Включая все системные УЗ. Включая в домене. И локальные. И в СУБД. И в VPN. И в прикладе. И ключи SSH/SSL тоже. И сертификаты web-сервисов. И пароли и ключи в ДБО вашего банка. И в интернет – сервисах и кабинетах. **Вообще ВСЕ пароли сменить.**
- **Kerberos** - необходимо **сменить пароль дважды**.

Шаги IR (5 и 6)

Этап 5. Восстановление

- Восстановление из резервных копий
- Включение ранее отключенных сетевых интерфейсов

Этап 6. Уроки

- Отчет об инциденте и реагировании
- Рекомендации для исключения повторения инцидента -> план работ
- Все работает!

Можно онлайн?

- Сотрудники ИТ и ИБ заказчика собирают улики, логи и т.д., и направляют результаты для анализа экспертам, после изучения материалов экспертами процесс повторяется
- Онлайн IR по ставкам экспертов может быть дешевле, чем оффлайн + не требуется учитывать время на дорогу и командировочные расходы
- Без слаженной, быстрой и экспертной работы на стороне заказчика DFIR может продлиться дольше и оказаться дороже, чем оффлайн

Дополнительные шаги в случае выявления утечки

Мероприятия 1-й очереди (выполнение в течение 24 часов с момента выявления утечки)

- Уведомить акционеров/СД/головную компанию
- Сформировать собственную позицию по инциденту (с привлечением специалистов по ИБ, юристов и иных экспертных служб организации)
- Принять решение о целесообразности обращения за помощью в правоохранительные органы и/или ко внешнему центру реагирования (экспертной компании в области DFIR)
- Провести необходимые мероприятия по реагированию и расследованию инцидента
- Уведомить об инциденте уполномоченные органы, подлежащие информированию
- Убедиться в получении уполномоченными органами уведомления

Дополнительные шаги в случае выявления утечки

Мероприятия 2-й очереди (выполнение в течение 72 часов с момента выявления утечки)

- Подготовить и согласовать отчет о ходе реагирования и расследования
- Уведомить о результатах расследования уполномоченные органы, подлежащие информированию
- Убедиться в получении уполномоченными органами уведомления

Дополнительные шаги в случае выявления утечки

Мероприятия 3-й очереди (срок не регламентирован)

- Актуализировать перечень процессов и ВНД
- Провести с контрагентами сверку оснований для обработки ПДн, их состава и способов передачи
- Определить наличие поручений на обработку ПДн, при которых ответственность несет лицо, поручающее обработку. Оповестить давших вашей компании поручения на обработку ПДн лиц, в случае если утечка затронула порученные вашей компании к обработке ПДн
- Проанализировать состав типов утекших данных, а также самих данных на предмет пересечения с выявленными ранее утечками (в том числе других организаций) с целью оценки состава и количества уникальных данных в утечке. При необходимости направить уточнения в государственные органы.
- Подготовить заключение и план работ по результатам анализа

Рекомендации по отчетности о реагировании на утечку

Отчет может состоять из следующих смысловых блоков:

- Вступительная часть - дата и время появления информации об утечке, состав заявленной злоумышленниками информации об утечке и фактически опубликованной ими информации
- Результаты расследования - обстоятельства и причины утечки, состав и объем утекших данных или данных, которые могли утечь, могут ли пострадать интересы субъектов ПДн в результате утечки в проекции на сервисы организации, удалось ли установить виновных и какие меры применены в их отношении
- Заключение по итогу проведения анализа утекших данных - оценка утекших данных на предмет их подлинности/фейковости, их уникальности с учетом сторонних утечек
- Принятые меры - тактические и стратегические меры с развернутым описанием

Отчет рекомендуется готовить полным и исчерпывающим

И это все? Нет, к сожалению…

- В ходе или после проведения DFIR и после согласования с юристами Вашей компании может быть принято решение осуществить обращение в правоохранительные органы. Для этого юрист пострадавшей компании уже в процессе DFIR готовит заявительные материалы. Можно обращаться в правоохранительные органы после получения отчета о DFIR, можно еще в процессе DFIR или даже до его начала - компания решает самостоятельно, отчет о DFIR может быть предоставлен в правоохранительные органы впоследствии, но крайне желательно до вынесения решения о возбуждении уголовного дела или об отказе от его возбуждения. Правоохранительные органы самостоятельно примут решение, возбуждать уголовное дело или нет, на основании представленной информации и собственных выводов. Поэтому, если компания хочет получить и представить в правоохранительные органы отчет экспертов DFIR для возбуждения уголовного дела, может быть целесообразно отложить подачу заявления в правоохранительные органы до получения отчета. С указанными материалами и доверенностью на представление интересов компании в правоохранительных органах юрист компании обращается, обычно, в РОВД/ОВД по месту регистрации компании (в случае компании федерального значения иногда может быть целесообразно обращение выше, например в ГУВД, или СК, или УБКП).
- При первом обращении юрист получит первую справку - талон-уведомление о том, что заявление принято. У талона будет уникальный в рамках даты номер (КУСП). Рекомендуем всегда обращаться в правоохранительные органы, в том числе потому, что без КУСП активный поиск злоумышленников с помощью отдельных мер может быть незаконен.
- В течение 30 дней после подачи заявления компания получит вторую справку о том, что следователь согласен с тем, что имело место преступление и возбуждено уголовное дело. Либо компания получит отказ (что довольно плохо для компании; причиной отказа может быть, например, не предоставление отчета об инциденте или иных необходимых доказательств, на основании которых можно возбудить уголовное дело и признать пострадавшую компанию потерпевшей стороной). Рассмотрим процесс взаимодействия со следствием немного подробнее.

И еще…

- Для возбуждения уголовного дела инцидент должен иметь признаки состава преступления, например:
  - Троян/шифровальщик/RAT - статья 273 УК РФ
  - Кража ПДн/логинов и паролей/фото - статья 272 УК.
  - DDOS - статья 274 УК.
  - Действия, направленные на неправомерное воздействие на критическую информационную инфраструктуру – статья 274.1 УК.
- Вы можете самостоятельно подготовить отчет о расследовании и реагировании для его направления в правоохранительные органы, но вам необходимо будет изложить в отчете все факты объективной стороны преступления, контрольные суммы файлов вредоносных программ, перечислить функциональные возможности выявленных вредоносных программ с указанием признаков, которые по вашему мнению можно отнести к вредоносному программному обеспечению (например такие как уничтожение или блокирование информации - см. ст. 273 УК РФ), необходимо быть готовым предоставить следствию сами вредоносные программы на флешке и так далее.
- Все, что указано в отчете, должно быть воспроизводимо, например должны быть указаны контрольные суммы, указание использованных программ с их версиями и так далее.
- Детальные требования к отчету (что должно в нем быть) можно найти в соответствующей методичке МВД, изданной МосУ МВД России имени В.Я. Кикотя.

И затем…

- В процессе рассмотрения заявления компании будет определен следователь, который будет вести дело. Следователь с постановлением на выемку обратится в компанию и предложит предоставить свидетельства инцидента в виде выемки, очно, под протокол и видеосъемку, после чего предоставленные свидетельства станут вещественными доказательствами в деле. Крайне важно, чтобы следователь после выемки признал пострадавшую компанию потерпевшей стороной и возбудил дело (пусть и против неустановленного пока круга лиц). В дальнейшем целесообразно чтобы данный вывод подтвердил суд. Для возмещения убытков целесообразно стремиться к тому, чтобы совершившие атаку лица были найдены и признаны виновными на основании вступившего в законную силу решения суда, а компания была признана потерпевшим в уголовном деле. Это позволит предъявить иск о возмещении причиненного преступлением вреда (ст. 42 Уголовно-процессуального кодекса РФ). При этом установление виновных в атаке лиц не снимает с компании и ее уполномоченных работников ответственность в случае нарушения ими правил защиты информации (например, правил эксплуатации критической информационной инфраструктуры).
- Пострадавшая компания может периодически обращаться к следователю с просьбой о доступе к уголовному делу (в отношении информации только своего юридического лица) для отслеживания прогресса.
- Дальнейшей задачей следствия является, если упростить, установить 3-е лицо (злоумышленника), подать его в розыск, задержать, направить дело в суд.
- Когда злоумышленник будет признан виновным потерпевшие смогут предъявить к нему претензии в суде.

А потом

В числе прочего **справка о признании компании потерпевшей** и о возбуждении уголовного дела **необходима для ряда государственных органов**, например для ФНС, если была утрачена или зашифрована бухгалтерия компании, так ФНС вполне может подать на компанию в суд за несвоевременное или неполное предоставление очередной бухгалтерской отчетности и соответствующая справка может помочь компании получить отсрочку в предоставлении отчетности.

Справка подтвердит в суде, что компания не сама удалила (скрывает) свою бухгалтерию

Это ещё не все проблемы… Утечка данных

- Вероятно, еще до шифрования данных украли изрядную долю информации. Определить это часто можно по журналам сетевых средств защиты или статистике исходящего трафика в сторону сети интернет.
- У вас могут попросить выкуп за ее удаление злоумышленниками, но нет гарантий, что они это сделают, а если вы не платили выкуп за расшифрованные данных - то нет гарантий вдвойне.
- Поэтому ваши данные скорее всего будут проданы всем, готовым за них заплатить
- В украденных у вас данных могут быть:
  - Ключи и пароли от личных кабинетов во внешних сервисах, включая госучреждения, сервисы партнеров и т.д.
  - Персональные данные сотрудников и клиентов
  - Информация о вашей экономической деятельности, договорах и т.д.
  - Интеллектуальная собственность: разработанный программный код и т.д.
- Сменить ключи и пароли от личных кабинетов во внешних сервисах сразу после завершения DFIR
- В сервисах проверить состав операций и пользователей - т.к. злоумышленники могут создать дополнительные аккаунты для доступа к вашим личным кабинетам

А потом еще…

- Через какое-то время после продажи ваших данных (или если на них не найдется покупатель) данные вполне могут быть опубликованы в открытом доступе частично или целиком
- Вы можете столкнуться с обращениями клиентов и партнеров, а также правоохранительных органов. Если вы ранее не уведомили все необходимые правоохранительные органы, например, Роскомнадзор об утечке персональных данных, вам необходимо будет выполнить соответствующие мероприятия в установленные законом срок.
- В будущем могут быть опубликованы новые части ранее украденных у вас данных и выданы за новую утечку - необходимо быть готовыми проанализировать такие данные, чтобы либо подтвердить, что это старая утечка, либо снова проводить DFIR либо Compromise Assessment (CA).

Я все понял. А можно пройти профилактический осмотр?

Что делать, если у вас есть подозрение, что вашу ИТ-инфраструктуру взломали и могут зашифровать и уничтожить, но этого еще не произошло.

Что может быть таким основанием?

- Ощущение некорректной работы ИТ-инфраструктуры, например, ввиду происходящих в ней с административными правами изменений, не санкционированных вами
- Наличие уязвимого ПО или сервисов на внешнем (интернет) периметре, которые вы не устраняете оперативно.
- Отчет о тесте на проникновение с успешной компрометацией вашей компании.
- И многое другое…

В данной ситуации целесообразно:

- провести CA (Comromise Assessment) – поиск следов взлома
- проверить безопасность, целостность и доступность ваших бэкапов (резервных копий данных)
- рассмотреть рекомендации со следующего слайда

Что может сделать владелец бизнеса?

- Довести рекомендации до ИТ и ИБ служб компании
- Убедиться, что никто не стесняется сказать, что он не может что-то выполнить или у него чего-то нет
- Убедиться, что все подготовительные шаги выполнены
- Привлечь при инциденте все возможные ресурсы и не терять время, по возможности – вернуть технический персонал из отпуска и т.д.
- Ни в коем случае не увольнять и не наказывать работников в ходе ликвидации последствий инцидента, наоборот – поддерживать!

Помните, что демотивированный сотрудник меньше всего будет заинтересован в реагировании на инцидент, а сотрудник, который допустил (по своей вине или нет), но исправил ситуацию, для вашей компании лучше и ценнее нового!

Константин Титков

tg: @ktitkov