Чек-лист:

5 ШАГОВ ДЛЯ УСТРАНЕНИЯ ПОСЛЕДСТВИЙ УТЕЧКИ

Госдума приняла законопроект о поправках в ФЗ-152 «О персональных данных» – все операторы ПДн должны будут сообщать о кибератаках и утечках в ГосСОПКА и Роскомнадзор в течение 24 часов, за 72 часа – представлять результаты внутреннего расследования. Собрали памятку с инструкцией, как действовать при инциденте и правильно отчитаться регулятору.

SEARCHINFORM
INFORMATION SECURITY

1 Соберите рабочую группу

Распределите задачи, которые необходимо закрыть при утечке информации, между разными отделами.

Как?

- ИТ- и ИБ-отделы: отвечают за быстрое купирование утечки, оценку ее масштабов, расследование, а также уведомление регулятора.
- Бизнес-подразделение, руководство и PR-отдел: сообщают клиентам об утечке.
- PR-отдел: занимается отработкой негатива в СМИ и соцсетях.
- Юристы: проводят оценку юридических рисков и нивелируют их.

Зачем?

В экстренной ситуации ответственные отделы помогут быстро предотвратить последствия утечки для компании.

2 Уведомите регулятора

Всем следует сообщать об утечке ПДн в Роскомнадзор. Также по приказу ФСБ №282, субъекты КИИ должны отчитываться об инцидентах перед НКЦКИ, финансовые организации ещё и перед ЦБ.

Как?

- Об утечке персональных данных нужно сообщить в Роскомнадзор через форму в «Общественной приемной», в ней следует выбрать тему жалобы (данные в общем доступе, обработка данных против нашей воли и т.п.) и отправить форму.
- О кибератаках и сбоях нужно отчитаться в НКЦКИ: в ГосСОПКА, по интернету, почте, факсом или формы электронной обратной связи. Удобно, если сообщить о кибератаке в ГосСОПКА можно прямо из консоли защитного ПО.
- Регуляторам нужно передавать технические сведения об инциденте: категорию и тип события, дату и время выявления, состояние работ по реагированию, оценку последствий и др. Полный список можно найти на сайте.

Зачем?

При игнорировании этих правил субъекты КИИ могут попасть под административную или уголовную ответственность, в зависимости от критичности инцидента. Операторы ПДн в скором времени также столкнутся с серьезным наказанием за сокрытие инцидентов, в том числе в виде оборотного штрафа.

Это важно сделать в течение 24 часов с момента обнаружения инцидента!

3 Проведите расследование

Как?

- Оцените масштаб утекших данных – сколько строк утекло, насколько критичная информация оказалась в открытом доступе.
- Определите канал, по которому могла произойти утечка: почта, внешние носители, социальные сети, облака и др.
- Найдите виновных – это был внутренний инсайдер или внешний нарушитель, а может данные утекли не из вашей компании, а, например, от контрагента или у госведомства.
- Установите обстоятельства – была ли это спланированная утечка или случайная.
- Соберите доказательства – опросите свидетелей, выгрузите данные из DLP, DCAP или SIEM (скриншоты рабочего стола, архив переписки, аудит операций в файловой системе и т.д.) и др.

Зачем?

Расследование нужно не только для того, чтобы отчитаться или передать материалы в суд. Оно поможет увидеть болевые точки в копании и «вылечить» их, благодаря чему вы сможете предотвратить утечку в будущем.

В течение 72 часов передайте регулятору результаты внутреннего расследования: сообщите о виновных, причинах и вреде от инцидента.

4 Предупредите клиентов

Составьте простое и понятное письмо с объяснениями и извинениями, без профессиональных ИБ-терминов.

Как?

- Расскажите клиентам, что произошло и в каких масштабах.
- Объясните, какие меры вы сейчас предпринимаете для расследования утечки и как вы планируете усилить защиту.
- Не скрывайте масштабов инцидента и сообщите, что за утечкой могут последовать активные действия мошенников – фишинг, социальная инженерия или взлом.
- Дайте несколько рекомендаций для снижения рисков: сменить пароли, ввести двухфакторную аутентификацию, поменять привязанную почту и т.д.
- Предложите компенсацию: бонусы, скидки или подарки. Не стоит делать такую компенсацию большой, важнее скорее психологический момент.
- Передайте информацию об утечке в СМИ. Следует придерживаться такой позиции: «Мы допустили ошибку, однако в настоящее время работаем над тем, чтобы устранить последствия и не оступаться так впредь».

Зачем?

Разослав клиентам предупреждение об утечке, вы дадите им возможность защитить себя постфактум. Например, поменять пароль. А еще так будет больше шансов сохранить репутацию: вы успеете объяснить ситуацию до того, как информация появится в СМИ.

5 Устройте профилактику

Как?

- Обучайте сотрудников ИБ-грамотности. Важно освещать темы фишинга, парольной политики, правила блокировки ПК и др.
- Наведите порядок в ИТ-инфраструктуре: ограничьте доступ к важным документам, разберитесь, в каких сетевых папках они должны лежать, настройте двухфакторную аутентификацию для доступа к критичным сервисам, используйте зашифрованные каналы передачи данных и др.
- Настройте защиту: в DCAP на обнаружение ПДн, в DLP на контроль пересылки таких файлов, в SIEM – на нежелательный доступ к местам их хранения. Используйте проактивную защиту – блокировки.
- Вводите ответственность за разглашение конфиденциальной информации и слив данных.

Зачем?

Профилактика снизит риски, что инцидент повторится. Это не единоразовая акция, подобные меры должны быть постоянными.

«СёрчИнформ» – ведущий российский разработчик средств информационной безопасности. Входит в НП «Руссофт». Его клиенты – более 3000 компаний по всей России и еще 20+ странах мира. Сегодня в активе команды – продукты и услуги для комплексной защиты от внутренних угроз на всех уровнях корпоративных информационных систем:

«СёрчИнформ КИБ»

система класса DLP, защищает от утечек информации, корпоративного мошенничества и других инцидентов безопасности, связанных с человеческим фактором. В 2017 году включена в «магический квадрант» лучших DLP-систем мира по версии Gartner.

«СёрчИнформ FileAuditor»

DCAP-решение (data-centric audit and protection) проводит автоматизированный аудит хранилищ информации, находит нарушения прав доступа и отслеживает изменения в критичных данных.

«СёрчИнформ SIEM»

система сбора и анализа событий безопасности в режиме реального времени, выявления ИБ-инцидентов и реагирования на них.

«Аутсорсинг DLP»

услуга, когда с защитными решениями работает профессиональный ИБ-аналитик вне штата. Мы ведем мониторинг и расследуем инциденты – компания получает результат.

Подробнее о защите персональных данных с помощью DLP, SIEM, DCAP читайте в «Практике и аналитике» на сайте searchinform.ru.

SEARCHINFORM
INFORMATION SECURITY