MOSCOW FORENSICS DAY '25

КОНСТАНТИН ТИТКОВ

«КАК НЕ ДОВЕСТИ ДО ФОРЕНЗИКИ И ЧТО ДЕЛАТЬ, ЕСЛИ ЭТОГО НЕ ИЗБЕЖАТЬ»

MFD

Что делать, если всё зашифровано и украдено

Константин Титков

руководитель центра ИБ дочерних обществ, Газпромбанк
амбассадор Кибердома

09.2025

О чем пойдет речь?

- Что не так с типовым планом ОНиВД ИТ?
- Экстренные действия
- Кто и чем может помочь
- Этапы реагирования на инцидент
- Что делать после
- Если утечка ПДн
- Как подготовиться, чтобы было не ТАК больно

P.S. 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.

P.P.S. Рекомендации не могут быть абсолютно применимы для всех возможных случаев и не могут гарантировать идеального результата действий при реагировании на инцидент ИБ.

07.2025, по горячим следам успешных атак

Цель и дата инцидента	Инцидент официально	Последствия и восстановление
Производитель напитков и федеральная сеть магазинов, 14 июля	«… группа подверглась беспрецедентной кибератаке – масштабной и скоординированной акции, осуществленной хакерами…»	• Финансовые потери, потеря данных, репутационные потери, отток клиентов • Восстановление: порядка двух недель, полное восстановление – месяц
Крупная авиакомпания, 27 июля	«… в связи со сбоем в ИТ-инфраструктуре авиакомпания проводит вынужденную корректировку расписания полётов, в том числе путем частичной отмены рейсов…»	• Финансовые потери, потеря данных, репутационные потери, проверки со стороны регуляторов, возможна ответственность должностных лиц • Восстановление: несколько дней, часть функций недоступна
Федеральная сеть аптек, 29 июля	«Мы столкнулись с серьезным техническим сбоем вследствие хакерской атаки. В результате чего была нарушена работа аптек..»	• Финансовые потери, потеря данных, репутационные потери, отток клиентов • Восстановление: более двух недель
Следующая организация ***(дата уточняется…)***	**Будет раскрыто позднее**	**Оценка ожидается**

- Вероятны события уровня **ELE** (Extinction Level Event, событие уровня вымирания), когда деятельность организации невозможно или нецелесообразно восстанавливать: полная потеря важнейших производственных активов, включая их физическое уничтожение
- **Критически важно готовиться к устранению последствий атаки ещё до начала самой атаки**

Главная цель – как можно скорее восстановить работу

- Ограничиться только этой целью – ошибка!

При этом забывают:

- Выдворить злоумышленника
- Выяснить способ проникновения
- Предотвратить повторное проникновение
- Выявить все последствия атаки
- Минимизировать ущерб
  (клиенты, контрагенты, репутация, штрафы…)

- **«Мы поймали шифровальщика!»**
  – неверное утверждение

Есть план, да не тот

ИТ-инцидент: человеческая ошибка или технический сбой

- Восстановление за несколько часов (восстановление данных и отдельных элементов ИТ-инфраструктуры отработано и отточено)

ИБ-инцидент: целенаправленное сознательное вредоносное воздействие на все или любые элементы инфраструктуры и сотрудников, в любое время и адаптивно - с учетом ответных действий

- Восстановление за несколько дней / недель

Время уходит на:
- панику / бессмысленные действия
- принятие решения о реагировании
- реагирование на инцидент
- восстановление ИТ-инфраструктуры
- восстановление данных

Пятница и праздники

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

(и дешевле простоя в работе)

Рекомендаций нет – сделаем!

- **Константин Титков**, руководитель центра ИБ дочерних обществ, Газпромбанк; амбассадор Кибердома
- **Сергей Голованов**, главный эксперт, АО «Лаборатория Касперского»
- **Антон Величко**, руководитель Лаборатории цифровой криминалистики и исследования вредоносного кода, F6
- **Илья Зуев**, вице-президент по ИБ, МТС Банк
- **Коллеги**, которые задавали вопросы и делились опытом

Как это вообще могло произойти?

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

Платить ли выкуп?

Экстренно

- Проверить **операции в ДБО**
- **Не выключать** и не перезагружать
- Изолировать ценное / **бэкапы**, и их носители
- Снять «снапшоты»
- Изучить исходящий трафик
- Рассмотреть **сетевую изоляцию**
- Позаботиться о режиме работы **персонал**а
- **Поддержать** задействованных сотрудников
- **Кто главный**? И другие участники реагирования
- **Коммуникации** ВНЕ пораженной инфраструктуры
- Определить реалистичные **цели**
- Провести **DFIR**
- Обратиться в правоохранительные органы
- Привлечь ИТ-**подрядчик**ов
- Информировать **клиент**ов и партнеров
- «Заглушка» на **сайт**

Роли участников при ликвидации инцидента ИБ

- Принимающий решения
- Координатор работ
- ИБ
- ИТ
- Юрист
- PR/Маркетинг
- HR

В случае утечки ПДн также ответственные за:

- обработку ПДн
- обеспечение безопасности ПДн

Нужна помощь?

- Выбор компании (-ий), режима проведения, количества экспертов, даты/время
- Адрес, контакты, пропуска, парковка, гарантийные письма, NDA
- Установочная встреча
- Анализ скомпрометированных узлов, HDD (снятие копий для анализа)
- Поиск точек входа, всех пораженных узлов и закладок (RAT)
- Подготовка отчета
- *У 2-х экспертов DFIR режим работы 24/7: 8 часов эксперт работает один, 8 - вдвоем с напарником, 8 на отдых.*
  Обеспечьте аналогичный режим работы!

- *Нужно быстрее – нужно больше экспертов DFIR*
  Лучше обсудить сроки работ и ставки до выезда экспертов
- НКЦКИ (Национальный координационный центр по компьютерным инцидентам) https://www.cert.gov.ru/abuse/

Что приготовить?

- Рабочие места (стол/стул/свет/электропитание/кофемашина…)
- Чат ВНЕ корпоративного мессенджера с участием необходимых лиц (ИТ, ИБ, менеджмент, юрист, маркетинга/PR, …)
- «Режим тишины» во внутренней сети, почте, мессенджерах (если в них был осуществлен вход в корпоративной сети)
- Синхронный режим работы сотрудников ИТ/ИБ и экспертов DFIR
- Отмена отпусков, командировок, увольнений
- Компенсации за переработки

Критически важна конфиденциальность чата!

Этап 1: Подготовка к инциденту

- **Логи** – есть и в безопасности (состав, место, глубина)
- **Диски** – в доступности (найти, взять в руки, снять защиту)
- **Артефакты** – могут быть собраны (доступность, права, пароли)
- **Резервы** – достаточны и доступны
- **Бэкапы** – полные (данные + ПО) и в безопасности

  (и есть чем и на что их восстановить!)

Этап 2: Идентификация инцидента

- Threat Intelligence
- SOC/SIEM
- MDR
- EDR/XDR
- AV
- …
- Система ИТ-мониторинга (отключение средств защиты)
- …
- Экран зашифрованного компьютера (если не озаботились пунктами выше)
- Телеграмм/MAX-каналы… (если в отпуске)

Этап 3: Изоляция

- НЕ отключать электропитание!
- НЕ перезагружать!
- **НО** отключать от ЛВС:
- Виртуальные машины
- Физические машины
- Wi-Fi и иные интерфейсы

Этап 4. Зачистка

- Удаление троянов/закладок/web-шелов/RAT и т.д.
- Установка обновлений безопасности (для точек входа + новейшие)
- Восстановление средств защиты
- Смена паролей:
  - доменные и системные УЗ. Kerberos – x2
  - и локальные, в СУБД, VPN, прикладе…
  - и ключи SSH/SSL тоже.
  - и сертификаты web-сервисов.
  - и пароли/ключи в ДБО вашего банка.
  - и в интернет–сервисах и кабинетах.

  Вообще ВСЕ пароли сменить!
- Сверить перечень УЗ. Включая системные.

Этапы 5-6: Восстановление и уроки

- Восстановление из резервных копий
- Включение интерфейсов

- Отчет об инциденте и реагировании
- Рекомендации для НЕ повторения
- План работ

Это все долго?

Примерные оценки сроков:

- Шифровальщик еще не запущен? От 2-х часов.
- Анализ пары HDD – 1 день
- 100 - 200 узлов - 1 неделя работы 1-го эксперта
- 1000 - 2000 узлов - 2 недели для 2-х экспертов
- 50 000 - 150 000 узлов - 2 месяца работы сводных команд

Может онлайн?

Можно онлайн

- Можно онлайн, если умеете собирать логи, улики и т.д.
- Эксперты изучат данные и запросят недостающее
- Онлайн IR может быть дешевле по ставкам экспертов

+ нет расходов на дорогу и командировку!

- **НО**: без слаженной, быстрой и экспертной работы на стороне заказчика DFIR может продлиться дольше и оказаться даже дороже, чем оффлайн!

И это все? Нет, к сожалению…

- Обращение в правоохранительные органы
- Заявительные материалы
- Отчет о DFIR
- КУСП
- Выемка
- Возбуждение уголовного дела
- Справка о признании компании потерпевшей
- Взаимодействие с другими государственными органами

И это еще тоже не все

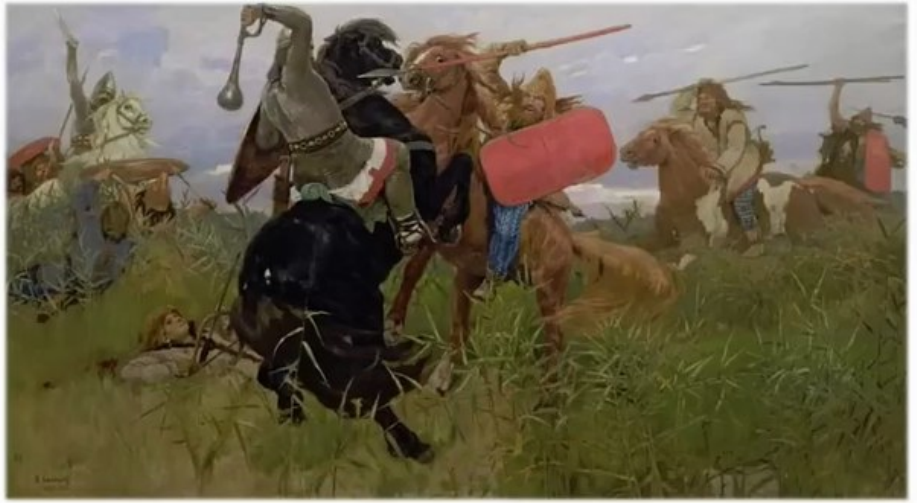
Кража информации и ПДн:

- выкуп за ее удаление
- продажа данных
- публикация данных

- Персональные данные сотрудников и клиентов
- Интеллектуальная собственность
- Условия договоров
- Ключи и пароли

В случае утечки ПДн

- Обращения клиентов, партнеров, правоохранительных органов.
- 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).



В случае утечки ПДн

Поэтому сейчас (и в будущем - каждый раз):

- 24 часа - уведомить Роскомнадзор
- 72 часов - отчет о результатах внутреннего расследования
- Субъект КИИ - в 24 часа уведомить НКЦКИ (формат ГосСОПКА)
- Поднадзорным ЦБ РФ - АСОИ ФинЦЕРТ
- GDPR (?)

Заранее для каждого информируемого

- порядок информирования и требования к форме и составу данных
- основные и резервные каналы информирования
- доступ к личным кабинетам
- учесть филиальную сеть вашей организации / группы / холдинга
- ответственные за составление, согласование и направление отчетов
- порядок информирования субъектов ПДн об утечке и размещения информации об утечке в открытых источниках
- ответственных за составление, согласование и публикацию информации
- согласовать заранее шаблоны пресс-релизов

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 и фактически опубликованной злоумышленниками 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 на предмет их подлинности/фейковости, уникальности с учетом сторонних утечек
- Принятые меры - тактические и стратегические меры с развернутым описанием

Желательно готовить исчерпывающий отчет!

Я все понял. А можно пройти профилактический осмотр?

Что делать, если у вас есть подозрение, что вашу ИТ-инфраструктуру взломали и могут зашифровать/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 инфраструктуры.
- И многое другое…

В данной ситуации целесообразно:

- провести CA (Comromise Assessment) – поиск следов взлома
- проверить безопасность, целостность и доступность ваших бэкапов (резервных копий данных)
- Подготовиться к будущему инциденту

Как подготовиться? CISO & CIO/CTO

- Разработать **план реагирования** в случае успешной кибератаки с самыми печальными последствиями
- Создать **резерв** оборудования, финансов и т.д
- Уделить особое внимание безопасности **бэкап**ов данных и самого ПО (“3-2-1”)
- **Защитить** систему резервного копирования
- **Учения** по реагированию
  + измерить время
- Заранее выбрать DFIR-**партнер**ов
- В случае подозрений на взлом
  - Comromise Assessment

Как подготовиться? CEO

- Довести **рекомендации** до ИТ и ИБ
- Проверить, что **все всё могут** и **у всех всё есть**, подготовительные шаги выполнены
- Оценить **время простоя** в при ИБ инциденте
- При инциденте привлечь все **ресурсы**
- **Поддерживать** работников в ходе ликвидации последствий инцидента, а не наказывать

Демотивированный сотрудник не заинтересован в реагировании на инцидент, а сотрудник, который допустил (по своей вине или нет), но исправил ситуацию, для вашей компании лучше и ценнее нового!

Рекомендации:
https://cyberdom.pro/recomendationbig

Памятка для CEO:
https://cyberdom.pro/recomendationceo

Благодарю за внимание!

Константин Титков