Ай-ТИ Фреш

АНАЛИТИЧЕСКИЙ РАЗБОР

Безопасность RDP и удалённого доступа в малом офисе

Почему открытый удалённый доступ — главная дверь для шифровальщиков и как её закрыть

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Бухгалтер работает из дома в 1С, подрядчик подключается к серверу «на минутку» — удобно. Пока однажды все файлы не оказываются зашифрованы, а на экране — требование выкупа. Открытый в интернет удалённый доступ находят не хакеры-одиночки, а автоматические сканеры, круглосуточно перебирающие адреса и пароли. Вопрос не «заметят ли ваш сервер», а «когда».

Почему это важно бизнесу

- Боты сканируют весь интернет по порту 3389 непрерывно: открытый RDP находят за часы, а не за месяцы
- Малый бизнес — удобная мишень: деньги и данные есть, а выделенного ИБ-специалиста обычно нет
- Атака шифровальщика — это не только выкуп, но и недели простоя: без 1С и почты работа компании встаёт
- С 30.05.2025 утечка персональных данных грозит штрафом до 15 млн ₽, повторная — до 3% годовой выручки

СТАТИСТИКА

Проблема в цифрах

90%

инцидентов, разобранных Sophos IR за 2023 год, включали злоупотребление протоколом RDP

Источник: Sophos Active Adversary Report, 2024

65%

случаев — первичное проникновение через внешние сервисы удалённого доступа (RDP и подобные)

Источник: Sophos Active Adversary Report, 2024

500+

атак шифровальщиков на российские компании за 2024 год — в 1,5 раза больше, чем в 2023

Источник: F6, «Киберугрозы в России и СНГ 2024/25»

24 дня

средний простой бизнеса после атаки шифровальщика

Источник: Varonis (по данным Statista), 2024

до 5 млн ₽

запрос выкупа за расшифровку данных у малого бизнеса в России в 2024 году

Источник: F6, «Киберугрозы в России и СНГ 2024/25»

до 15 млн ₽

штраф за крупную утечку персональных данных (свыше 100 тыс. человек); повторная — до 3% выручки

Источник: КоАП РФ с 30.05.2025 (КонсультантПлюс)

КЕЙС 1 ИЗ 3

Госпиталь заплатил выкуп из-за учётки подрядчика

Ситуация

Hancock Health — региональный госпиталь (Индиана, США)

Как развивались события

1. Злоумышленники получили логин и пароль подрядчика, обслуживавшего оборудование госпиталя
2. Через легальный канал удалённого доступа вошли на сервер резервной площадки и запустили шифровальщик SamSam
3. За ночь зашифровано более 1 400 файлов; медицинские системы встали, персонал перешёл на бумажный учёт
4. Резервные копии оказались повреждены — восстановиться без ключа расшифровки было невозможно
5. Руководство заплатило выкуп 4 BTC (около 55 тыс. долларов), работа восстановлена через несколько дней

ПОСЛЕДСТВИЯ

Несколько дней работы госпиталя на бумаге в разгар эпидемии гриппа, выкуп около 55 тыс. долларов плюс расходы на расследование и усиление защиты. Группировка SamSam в те же годы массово ломала организации именно через открытый и слабо защищённый RDP.

ГЛАВНАЯ ОШИБКА / ВЫВОД

Удалённый доступ подрядчика без второго фактора и контроля — та же открытая дверь, что и ваш собственный. А резервные копии, доступные из основной сети, погибают вместе с данными.

Источник: Healthcare IT News; заявление CEO Hancock Health, 2018

КЕЙС 2 ИЗ 3

СДЭК: 11 дней без выдачи посылок по всей стране

Ситуация

СДЭК — курьерская служба, тысячи пунктов выдачи по России

Как развивались события

1. 26 мая 2024 года сайт и приложение перестали работать; приём и выдача посылок остановились по всей стране
2. Группировка Head Mare заявила, что зашифровала серверы компании и уничтожила резервные копии
3. Несколько дней компания не могла ни выдавать, ни отправлять заказы; к 29 мая сервисы восстановлены лишь частично
4. Полное восстановление работы — только к 6 июня, примерно через 11 дней после начала атаки

ПОСЛЕДСТВИЯ

По оценкам СМИ, в пунктах выдачи застряло от 1,5 до 3 млн отправлений. Прямые потери выручки, претензии и неустойки контрагентов за срыв сроков, репутационный удар. Точную сумму ущерба компания не раскрыла.

ГЛАВНАЯ ОШИБКА / ВЫВОД

Если резервные копии доступны из той же инфраструктуры, атакующий уничтожает их первым делом. Без офлайн-копии и сегментации доступа даже крупная компания встаёт на недели.

Источник: Ведомости, РБК, Известия, 2024

КЕЙС 3 ИЗ 3

Одна VPN-учётка без 2FA остановила топливопровод

Ситуация

Colonial Pipeline — оператор крупнейшего топливопровода США

Как развивались события

1. Пароль от старой VPN-учётки сотрудника оказался в утечке; второй фактор для входа не требовался
2. Злоумышленники вошли через удалённый доступ и развернули шифровальщик DarkSide в корпоративной сети
3. Компания на 6 дней остановила трубопровод — дефицит топлива на Восточном побережье, режим ЧС в ряде штатов
4. Выплачен выкуп 4,4 млн долларов; часть суммы позже вернуло ФБР

ПОСЛЕДСТВИЯ

6 дней остановки критической инфраструктуры, выкуп 4,4 млн долларов, топливный ажиотаж и разбирательство в Сенате США. Всё началось с одной забытой учётной записи удалённого доступа без двухфакторной аутентификации.

ГЛАВНАЯ ОШИБКА / ВЫВОД

Неучтённые «спящие» учётки удалённого доступа опаснее слабых паролей: о них никто не помнит, их никто не блокирует. Инвентаризация учёток и обязательная 2FA закрыли бы этот вектор.

Источник: Показания CEO Colonial Pipeline в Сенате США; Reuters, 2021

КАК ДЕЛАТЬ НЕ НАДО

Типовые ошибки

- ✕ **Порт 3389 открыт напрямую в интернет**
  Ботнеты сканируют этот порт круглосуточно. Открытый RDP находят за часы и сразу начинают подбор паролей по огромным словарям.

- ✕ **Вход по паролю без второго фактора**
  Украденный или подобранный пароль — это сразу полный доступ. С двухфакторной аутентификацией известный взломщику пароль не даёт войти.

- ✕ **Учётка Administrator для удалёнки**
  Стандартные имена (admin, administrator, rdp) перебирают в первую очередь. Взлом такой учётки — сразу максимальные права.

- ✕ **Нет блокировки после неудачных попыток**
  Без политики блокировки перебор идёт со скоростью тысяч паролей в час. С блокировкой «5 попыток / 15 минут» брутфорс нерентабелен.

- ✕ **Сервер без обновлений безопасности**
  Уязвимости уровня BlueKeep (CVE-2019-0708) позволяют захватить сервер вообще без пароля. Непропатченные серверы встречаются до сих пор.

- ✕ **Бэкапы в той же сети, что и сервер**
  Шифровальщик и оператор атаки первым делом ищут и уничтожают резервные копии. Доступная по сети копия — не защита.

- ✕ **Доступ подрядчиков без контроля**
  Учётки внешних специалистов живут годами после окончания работ. Именно так взломали Hancock Health и многих других.

- ✕ **Журналы входов никто не читает**
  Сотни событий 4625 (неудачный вход) в час — это атака в реальном времени. Без мониторинга её замечают уже после шифрования.

РЕКОМЕНДАЦИИ И ПРАКТИКИ

Как правильно

МИНИМУМ

- Закрыть порт 3389 из интернета, доступ — только по белому списку IP
- Включить NLA и установить все обновления безопасности Windows
- Политика блокировки: 5 неудачных попыток — блок на 15 минут
- Пароли от 12 символов; отдельная учётка вместо Administrator

НОРМАЛЬНО

- VPN или RD Gateway: наружу только 443-й порт, RDP скрыт внутри сети
- Мониторинг неудачных входов (событие 4625) с оповещением админа
- Геоблокировка: доступ к удалённым сервисам только из нужных стран
- Резервные копии по схеме 3-2-1 с офлайн-экземпляром вне офисной сети

ХОРОШО

- Двухфакторная аутентификация для всех удалённых подключений
- Сегментация: каждому пользователю — доступ только к своим ресурсам
- Учётки подрядчиков: срок действия, журналирование, отключение после работ
- Регулярный внешний аудит периметра и тест восстановления из бэкапа

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- ☐ Знаете ли вы, виден ли порт 3389 вашего сервера из интернета прямо сейчас?
- ☐ Включена ли двухфакторная аутентификация для всех, кто подключается к сети удалённо?
- ☐ Блокируется ли учётная запись после нескольких неудачных попыток входа?
- ☐ Подключаются ли сотрудники через VPN или RD Gateway, а не по прямому проброску RDP?
- ☐ Есть ли у вас резервная копия, физически недоступная из основной сети?
- ☐ Просматривает ли кто-то журналы неудачных входов хотя бы раз в неделю?
- ☐ Знаете ли вы все учётные записи подрядчиков с удалённым доступом и сроки их действия?
- ☐ Установлены ли на сервере обновления безопасности за последние 30 дней?
- ☐ Проверяли ли вы реальное восстановление из резервной копии за последние полгода?
- ☐ Есть ли план действий на случай шифрования сервера: кого звать, что отключать первым?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Аудит периметра: проверим, какие порты и сервисы вашей сети видны из интернета, и выдадим отчёт
- Внедрение защищённого доступа: RD Gateway или VPN, двухфакторная аутентификация, белые списки IP
- Резервное копирование с офлайн-копией и регулярной проверкой восстановления
- Мониторинг атак на вход в реальном времени: события Windows, оповещения, Zabbix
- Сопровождение: обновления, контроль учёток подрядчиков, проверки в рамках абонентского обслуживания

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

НА ЧЁМ ОСНОВАН РАЗБОР

Источники

01 Sophos Active Adversary Report (RDP в 90% инцидентов) (sophos.com — 2024)

02 Computer Weekly: RDP abused in over 90% of cyber attacks (computerweekly.com — 2024)

03 F6: главные киберугрозы 2025 — шифровальщики в России и СНГ (f6.ru — 2025)

04 Ведомости: причиной сбоя СДЭК мог стать вирус-шифровальщик (vedomosti.ru — 2024)

05 РБК: СДЭК о застрявших из-за сбоя посылках (rbc.ru — 2024)

06 Kaspersky: рост брутфорс-атак на RDP (Bruteforce.Generic.RDP) (kaspersky.com — 2020)

07 Healthcare IT News: Hancock Health заплатил выкуп за расшифровку (healthcareitnews.com — 2018)

08 CISA: advisory по SamSam Ransomware (AA18-337A) (cisa.gov — 2018)

09 Reuters: слушания по взлому Colonial Pipeline в Сенате США (reuters.com — 2021)

10 Positive Technologies: прогноз роста атак на российские компании (ptsecurity.com — 2025)

11 КонсультантПлюс: новые штрафы за утечки персональных данных (consultant.ru — 2025)

12 Varonis: Ransomware Statistics (средний простой 24 дня) (varonis.com — 2024)

Все данные пересказаны по открытым источникам; точность на дату публикации разбора.