Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Безопасный удалённый доступ: шлюз, NLA и жизнь без 3389

Что происходит с открытым портом, как устроен RD Gateway и какие слои защиты действительно работают

Август 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Порт 3389, открытый в интернет, находят за часы — массовое сканирование адресного пространства идёт непрерывно. Публичный RDP остаётся одним из основных путей проникновения шифровальщиков в компании малого и среднего размера.

Почему это важно бизнесу

- Успешный подбор пароля означает доступ ко всей учётной системе компании
- Перебор извне блокирует реальных сотрудников и выглядит как «глючит сеть»
- Каждая попытка входа нагружает контроллер домена
- История RDP знает уязвимости, позволявшие выполнить код без аутентификации
- Смена порта на нестандартный не защищает: полное сканирование адреса занимает минуты

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

41 800

неудачных попыток входа за сутки на сервере клиента с проброшенным портом

Практика ITfresh, 2026

340

адресов-источников перебора в том же инциденте

Практика ITfresh, 2026

3 года

столько проблема существовала, воспринимаясь как «глючит сеть»

Практика ITfresh, 2026

11

событий 4625 за сутки после закрытия проброса и настройки шлюза

Практика ITfresh, 2026

4625

идентификатор события неудачного входа, по которому строится мониторинг

Microsoft Learn

РЕАЛИЗАЦИЯ 1 ИЗ 2

Утренние блокировки, которые считали проблемой сети

Что настраиваем

Аренда складской техники, 19 PM

Как мы это делаем

1. Обратились с тем, что «утром половина не может войти»
2. Внутренний ИТ дважды перезагружал контроллер домена
3. Событий 4625 за сутки — 41 800 с 340 адресов
4. Перебирались реальные имена сотрудников: формат совпадал с почтой на сайте
5. Политика блокировала запись после пяти попыток — к приходу человека она уже была заблокирована

РЕЗУЛЬТАТ

Три года ежедневной потери первых рабочих часов и полное отсутствие понимания причины

КЛЮЧЕВОЙ НЮАНС

За один день: подняли шлюз, закрыли проброс, включили NLA, отсекли лишнюю географию — 41 800 событий превратились в 11

Практика ITfresh

РЕАЛИЗАЦИЯ 2 ИЗ 2

NLA выключили ради двух старых устройств

Что настраиваем

Компания со складскими тонкими клиентами

Как мы это делаем

1. NLA была отключена «для совместимости»
2. Причиной были два тонких клиента 2011 года выпуска
3. Сервер принимал сеанс до проверки учётных данных
4. Поверхность атаки оставалась широкой годами
5. Замена двух устройств стоила меньше, чем последствия инцидента

РЕЗУЛЬТАТ

Годы работы с ослабленной защитой ради двух единиц устаревшего оборудования

КЛЮЧЕВОЙ НЮАНС

Обновить клиента почти всегда дешевле, чем ослаблять сервер

Практика ITfresh

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Проброс 3389 в интернет**
  Находится за часы. Основной вектор для шифровальщиков в малом бизнесе.
- ✕ **Смена порта как мера защиты**
  Снижает фоновый шум, не защищает от целенаправленного поиска.
- ✕ **NLA отключена ради совместимости**
  Сервер поднимает сеанс до проверки учётных данных.
- ✕ **Слишком агрессивная политика блокировки**
  Перебор извне превращается в отказ в обслуживании для своих.
- ✕ **CAP и RAP настроены на «всех пользователей домена»**
  Смысл разграничения теряется.
- ✕ **Нет второго фактора и нет ограничения по географии**
  Единственная преграда — пароль.
- ✕ **Пользователи с правами локального администратора**
  Успешный вход превращается из неприятности в катастрофу.
- ✕ **Обновления безопасности не ставятся**
  Известные уязвимости остаются открытыми годами.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Порт 3389 не проброшен наружу ни для одного сервера
- Внешний доступ только через RD Gateway или VPN
- NLA включена на всех узлах сеансов

НОРМАЛЬНО

- Политики CAP и RAP ограничивают доступ конкретными группами
- Сертификат шлюза действителен, автопродление проверено
- Политика блокировки задана и не создаёт отказа в обслуживании
- На периметре отсечены географические диапазоны, откуда не работают сотрудники

ХОРОШО

- Настроен второй фактор либо доступ только из доверенной сети
- Мониторинг событий 4625 с порогом по фактическому фону
- У обычных пользователей нет прав локального администратора
- Обновления безопасности на узлах и шлюзе ставятся регулярно

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Порт 3389 закрыт снаружи для всех серверов
- [ ] Внешние подключения идут через шлюз или VPN
- [ ] NLA включена, уровень безопасности — SSL/TLS
- [ ] Сертификат шлюза действителен, автопродление проверено
- [ ] CAP и RAP ограничены конкретными группами, а не всем доменом
- [ ] Настроен второй фактор либо доступ ограничен доверенной сетью
- [ ] Политика блокировки не превращается в отказ в обслуживании
- [ ] Мониторинг событий 4625 настроен с порогом по фактическому фону

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).

- Развернём ферму RDS: роли, коллекции, сертификаты, лицензирование, режим стока для обслуживания
- Закроем удалённый доступ шлюзом и NLA, уберём проброс 3389 из интернета
- Настроим профили так, чтобы вход занимал секунды, а не минуты
- Разберёмся с печатью и периферией: Easy Print, изоляция драйверов, токены ЭЦП
- Рассчитаем мощности под ваш профиль нагрузки и скажем, когда пора добавлять узел

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

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Microsoft Learn — Remote Desktop Services: планирование (learn.microsoft.com — 2026)

02 Microsoft Learn — Лицензирование клиентского доступа RDS (learn.microsoft.com — 2026)

03 Microsoft Learn — RD Gateway: политики CAP и RAP (learn.microsoft.com — 2026)

04 Microsoft Learn — FSLogix: контейнеры профилей (learn.microsoft.com — 2026)

05 Microsoft Learn — Счётчики RemoteFX и качество сеанса (learn.microsoft.com — 2026)

06 Microsoft Learn — Изоляция драйверов печати (learn.microsoft.com — 2026)

07 Практика ITfresh: терминальные фермы для офисов до 50 PM (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.