Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Защита сервера офиса от взлома: наш инженерный чек-лист 2026

Как мы закрываем периметр, учётки, сеть и бэкапы офисного сервера — от WireGuard до Veeam

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Любой сервер с белым IP непрерывно сканируют боты: подбор паролей к RDP и SSH идёт тысячами попыток в сутки. Один угаданный пароль — и компания получает зашифрованные базы 1С, простой на 5–15 дней и восстановление за миллионы. Разбираем наш типовой проект защиты офисного сервера: от drop-all на периметре до бэкапов, которые шифровальщик не сможет удалить.

Почему это важно бизнесу

- Простой сервера 1С останавливает продажи, отгрузки и зарплату: каждый день — прямые убытки плюс штрафы за сорванную отчётность
- Восстановление после шифровальщика без пригодных бэкапов в разы дороже всего проекта защиты и не гарантирует возврата данных
- Утечка клиентской базы через незаблокированные учётки уволенных — потеря клиентов и риски по 152-ФЗ
- Контрагенты и страховые всё чаще требуют подтверждённый контур ИБ: без него срываются контракты и аудиты

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

7.x

RouterOS на периметре: WireGuard-сервер штатно с ветки 7.x, держим релиз long-term, конфиг вер…

по докам MikroTik

0 портов

Управляющих сервисов наружу: RDP, SSH, Winbox, SQL из WAN недоступны вовсе — только через VPN

наш стандарт

5/15 мин

Порог Account Lockout Policy: 5 неверных паролей — блокировка учётки на 15 минут, подбор по RD…

по докам Microsoft

v13

Veeam Backup & Replication: сервер бэкапа вне домена AD, MFA на консоль, Hardened Repository

по докам Veeam

30 дней

Срок иммутабельности бэкапов в Hardened Repository — перекрывает типичное «тихое» присутствие…

наш стандарт

4625

Event ID неудачного входа Windows: собираем в Zabbix 7.0 LTS ключом eventlog[Security], тригге…

по докам Zabbix

РЕАЛИЗАЦИЯ 1 ИЗ 3

Периметр: WireGuard на MikroTik и полный drop входящего

Что настраиваем

Пограничный роутер офиса (MikroTik, RouterOS 7.x long-term) и все публикации сервисов наружу

Как мы это делаем

1. Снимаем фактическую поверхность атаки: внешний скан портов WAN, сверка с NAT-правилами — каждая публикация либо обоснована, либо удаляется
2. Поднимаем WireGuard: interface + peer на сотрудника с AllowedIPs /32 и PersistentKeepalive 25; ключи генерируем на роутере, выдаём конфиг лично
3. Фаервол: в chain input политика drop, разрешены только established/related, порт WireGuard и ICMP; RDP, SQL и Winbox из WAN не видны вовсе
4. Отключаем лишние службы управления: в /ip service гасим telnet, ftp, www, api; winbox и ssh ограничиваем адресами LAN/VPN полем address
5. Резервный канал: второй VPN-профиль на отдельном порту + экспорт конфига роутера в наш репозиторий после каждого изменения

РЕЗУЛЬТАТ

Управляющие протоколы исчезают из поверхности атаки: боты видят закрытый периметр, подбор паролей к RDP прекращается физически. Удалёнка работает через VPN с подключением за секунды, а любое изменение периметра версионировано и обратимо.

КЛЮЧЕВОЙ НЮАНС

Порядок правил фаервола критичен: разрешение established/related ставим первым, drop — последним, и применяем изменения через safe mode, иначе легко отрезать себе доступ к роутеру.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Харднинг Windows-сервера 1С: учётки, RDP, службы, журналы

Что настраиваем

Windows Server 2022 в роли сервера 1С/RDS: политики входа, Defender, протоколы, аудит

Как мы это делаем

1. Политика блокировки: 5 неверных паролей — lockout 15 минут, минимальная длина пароля 12+ символов, включено требование сложности пароля
2. RDP: NLA обязателен (SecurityLayer=2/TLS, UserAuthentication=1), доступ только выделенной группе, второй фактор через RADIUS-провайдер поверх входа
3. Убираем лишнее: SMB1 удаляем (Remove-WindowsFeature FS-SMB1), IIS и FTP вне ролей сносим, локальный админ под Windows LAPS с авторотацией пароля
4. Defender: ASR-правила в блокирующем режиме и Controlled Folder Access на каталогах баз; исключения — только по документированному списку вендора
5. Аудит: Event ID 4625, 4740, 4720 уходят в Zabbix 7.0 LTS через eventlog[Security] активного агента; всплеск неудачных входов — алерт дежурному в Telegram

РЕЗУЛЬТАТ

Даже при утечке одного пароля атакующему негде развернуться: подбор блокируется lockout-политикой, пароли локальных админов уникальны на каждой машине, а всплеск событий 4625 виден дежурному раньше, чем начнётся шифрование.

КЛЮЧЕВОЙ НЮАНС

Windows LAPS теперь встроен в ОС и управляется политикой — отдельный агент legacy-LAPS не нужен; главное — не давать обеим версиям управлять одной учёткой: документация Microsoft прямо запрещает такое совмещен…

РЕАЛИЗАЦИЯ 3 ИЗ 3

Бэкапы, которые нельзя удалить: Veeam Hardened Repository

Что настраиваем

Veeam Backup & Replication v13: сервер вне домена AD, Linux-репозиторий с иммутабельностью, offsite-копия

Как мы это делаем

1. Сервер Veeam выводим из домена AD: отдельная учётка и MFA на консоль — шифровальщик с правами доменного админа до бэкапов не дотягивается
2. Разворачиваем Hardened Repository на Ubuntu LTS: подключение через single-use credentials (в v13 по умолчанию — сертификат), SSH после деплоя отключаем, иммутабельн…
3. Схема 3-2-1: ежедневные инкременты на репозиторий, GFS-полные на NAS, offsite-копия в S3-совместимое хранилище с Object Lock под отдельным ключом
4. Ежеквартально — учебное восстановление: поднимаем базу 1С из бэкапа на стенде, замеряем фактический RTO и фиксируем в паспорте клиента

РЕЗУЛЬТАТ

Последний рубеж перестаёт зависеть от воли атакующего: файлы бэкапа физически нельзя изменить или удалить до истечения срока иммутабельности даже с правами root на репозитории. Восстановление — проверенная процедура с известным временем, а не эксперимент в день аварии.

КЛЮЧЕВОЙ НЮАНС

По докам Veeam иммутабельность держится на атрибуте chattr +i и локальных часах репозитория: на хосте обязателен корректный NTP и закрытый доступ к BIOS/iLO, иначе срок защиты можно «промотать».

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Перенос RDP-порта вместо VPN**
  33890 сканируется так же, как 3389 — боты идут по всему диапазону. Мы закрываем RDP снаружи полностью и публикуем только порт WireGuard

- ✕ **Бэкап-сервер в том же домене AD**
  Доменный админ равен доступу к бэкапам — шифровальщик удаляет их первыми. Выносим Veeam из домена, репозиторий делаем иммутабельным

- ✕ **2FA только на VPN**
  Внутри сети RDP остаётся с одним паролем — заражённый ноутбук обходит контур. Ставим второй фактор и на вход в RDP и консоли администрирования

- ✕ **Плоская сеть /24 на весь офис**
  Один заражённый ПК видит сервер целиком. Режем VLAN: серверный сегмент принимает только нужные порты (1540–1541, 1560–1591, 445), остальное — drop

- ✕ **Учётки уволенных живут месяцами**
  Блокировка «когда вспомним». У нас чек-лист офбординга: disable учётки, отзыв VPN-профиля и смена общих секретов до конца последнего рабочего дня

- ✕ **Патчи установлены, ребута не было**
  Обновления ядра и ОС не активны до перезагрузки, а WSUS рапортует зелёным. Планируем окно ребута и контролируем uptime серверов мониторингом

- ✕ **Исключения антивируса на целый диск**
  Ради «скорости 1С» исключают весь том с базами — там и селится майнер. Исключаем только каталоги по докам вендора и аудируем список исключений

- ✕ **Админка роутера доступна из WAN**
  Winbox или веб-панель наружу — подбор пароля до полного захвата сети. В /ip service ограничиваем службы адресами LAN/VPN, извне — только VPN

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Закрыть RDP, SSH и SQL снаружи; удалённый доступ — только через WireGuard
- Lockout-политика 5/15 мин, пароли 12+ символов, блокировка уволенных день в день
- Ежедневный бэкап 1С на отдельное устройство плюс копия вне офиса

НОРМАЛЬНО

- 2FA на VPN и RDP, Windows LAPS на локальных админах, SMB1 удалён
- Сегментация VLAN: серверы, рабочие места, гостевой Wi-Fi и IoT — раздельно
- Veeam с репозиторием вне домена AD и ежемесячной проверкой восстановления
- Патч-менеджмент по расписанию (WSUS) с контролем перезагрузок

ХОРОШО

- Hardened Repository с иммутабельностью 30 дней + offsite-копия с Object Lock
- Централизованные логи и триггеры на 4625/4740 с алертом дежурному
- EDR на серверах и станциях, ASR-правила Defender в блокирующем режиме
- Ежеквартальные учебные восстановления с замером RTO и внешний скан периметра

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Внешний скан не видит ни одного управляющего порта: RDP, SSH, Winbox, SQL снаружи закрыты?
- [ ] Вход админов и удалённщиков защищён вторым фактором, а не одним паролем?
- [ ] Lockout-политика включена и перебор пароля реально блокирует учётку?
- [ ] Пароли локальных администраторов уникальны и ротируются автоматически (LAPS)?
- [ ] Сеть сегментирована: заражённый ПК бухгалтера не достаёт до сервера по всем портам?
- [ ] Бэкапы недоступны под учёткой продуктивной системы и есть неизменяемая копия?
- [ ] Последнее тестовое восстановление было не позже квартала назад и RTO известен?
- [ ] Учётки уволенных блокируются в последний рабочий день, общие секреты меняются?
- [ ] Серверы перезагружены после установки обновлений, а не копят патчи в ожидании?
- [ ] Всплеск неудачных входов ночью кто-то увидит: настроен алерт, а не просто журнал?

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 и харднинг за 2–3 дня: внешний скан, разбор NAT-правил, отчёт с приоритетами
- VPN-контур под ключ: WireGuard на MikroTik, профили сотрудников, резервный канал доступа
- Харднинг Windows-серверов 1С: политики входа, LAPS, 2FA на RDP, аудит с алертами
- Бэкап-контур Veeam с иммутабельным репозиторием и регламентом тестовых восстановлений
- Сопровождение: мониторинг Zabbix, патч-менеджмент, офбординг учёток по чек-листу

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 WireGuard — RouterOS Documentation (help.mikrotik.com — 7.x)

02 Hardened Repository — Veeam B&R User Guide (helpcenter.veeam.com — v13)

03 Windows LAPS: обзор и развёртывание (learn.microsoft.com — 2025)

04 Account Lockout Policy — security settings (learn.microsoft.com — 2025)

05 Attack surface reduction rules — Defender (learn.microsoft.com — 2025)

06 Zabbix Manual — Windows event log monitoring (zabbix.com — 7.0 LTS)

07 Паспорт безопасности офиса — шаблон ITfresh (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.