Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

MSP-чеклист безопасности: 9 пунктов до подписания договора

Как мы в ITfresh проверяем аутсорсера: аудит AD, immutable-бэкапы, LAPS, MFA, SIEM

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Компания передаёт инфраструктуру на аутсорсинг и не может проверить, что именно делает подрядчик: бэкапы «есть», патчи «ставятся», мониторинг «ведётся» — но всё это на словах. Проверить нечем: нет приёмочного аудита AD, нет теста восстановления, нет SLA в договоре. Первый же шифровальщик или уход админа превращает поддержку в лотерею, а восстановление — в недели простоя.

Почему это важно бизнесу

- Простой файлового сервера и 1С — это остановка отгрузок, зарплаты и отчётности; час простоя дороже месячного бюджета на поддержку.
- Бэкап без квартального теста восстановления — необеспеченный риск: платите за копии, которые могут не развернуться.
- Отсутствие SLA в часах означает, что за ночную атаку никто не отвечает: формально подрядчик ничего не нарушил.
- Плоская сеть и общий пароль локального админа отдают шифровальщику весь парк за часы вместо одной машины.
- Смена подрядчика без регламента передачи документации и доступов — окно уязвимости на месяцы.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

13.1.1.18

Билд Veeam B&R, на котором мы держим hardened-репозиторий и immutability-период

по докам Veeam B&R 13.1

4.14.7

Стабильная ветка Wazuh под SIEM; ветку 5.0 держим в лаборатории, в прод не выносим

по докам Wazuh 4.x

30 дн.

PasswordAgeDays в Windows LAPS — ротация пароля локального администратора

по докам Windows LAPS

24

PasswordLength LAPS: по докам дефолт 14 при диапазоне 8–64, наш стандарт — 24

наш стандарт + доки Windows LAPS

7 / 30 дн.

SLA на патчи: критичные (CVSS 9.0+) — 7 дней, прочие — 30, письменно в договоре

наш стандарт

15 мин

Целевая реакция дежурного инженера на критичный алерт SIEM в режиме 24/7

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 3

Приёмочный аудит AD и периметра до подписания договора

Что настраиваем

Домен заказчика целиком: DC, GPO, учётные записи и публикуемые наружу сервисы; сбор ведём с выделенного коллектора

Как мы это делаем

1. PingCastle --healthcheck по домену: получаем оценку риска 0–100 по четырём категориям и уровень зрелости 1–5, плюс список сработавших правил — фиксируем как baselin…
2. SharpHound -c All → BloodHound CE: строим граф и смотрим Shortest Path to Domain Admins; каждое ребро закрываем или обосновываем письменно.
3. Get-ADUser/Get-ADComputer с LastLogonDate, Enabled, PasswordNeverExpires в CSV: отключаем всё, что молчит дольше 90 дней.
4. Get-GPOReport -ReportType Html по всем политикам плюс repadmin /replsummary: ищем неприменяемые GPO и разрывы репликации между DC.
5. Инвентарь слушающих портов (Get-NetTCPConnection -State Listen) и внешний скан периметра: RDP и SMB наружу закрываем до старта обслуживания.

РЕЗУЛЬТАТ

Через 3–5 рабочих дней у заказчика есть измеримая картина: оценка риска и уровень зрелости по PingCastle, список привилегированных путей из BloodHound, перечень мёртвых учёток и открытых портов. Первый месяц обслуживания идёт по приоритетам из отчёта, а не по звонкам пользователей.

КЛЮЧЕВОЙ НЮАНС

PingCastle и BloodHound дают не «оценку», а список правил с идентификаторами: в отчёте мы всегда указываем конкретное правило и что именно закрыли, иначе повторный аудит не с чем сравнивать.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Immutable-бэкапы 3-2-1 и квартальная проверка восстановления

Что настраиваем

Veeam B&R 13.1 на выделенном сервере, hardened Linux-репозиторий на XFS и off-site-копия; охват — DC, файловый сервер, 1С и SQL

Как мы это делаем

1. Первичный репозиторий на локальном сервере, доступ только у сервисной учётной записи Veeam; доменных админов в правах репозитория нет.
2. Hardened Linux Repository на XFS с reflink: single-use credentials, доступ только на добавление, immutability period 30 дней (минимум по доке — 7).
3. Третья копия off-site — Backup Copy Job в S3-совместимое хранилище с Object Lock либо на физически отчуждаемый носитель.
4. Fast Clone на XFS: synthetic full без переписывания блоков — экономим место и держим цепочку в рамках immutability-окна.
5. SureBackup-задание еженедельно плюс ручное восстановление одной боевой ВМ раз в квартал с замером фактического RTO.

РЕЗУЛЬТАТ

Компрометация доменного администратора не даёт удалить резервные копии: в течение immutability-периода файлы нельзя изменить или удалить, только скопировать. RPO и RTO перестают быть декларацией — по каждой критичной системе есть замеренное время восстановления из последнего теста.

КЛЮЧЕВОЙ НЮАНС

Hardened-репозиторий требует forward incremental с active или synthetic full: reverse и forever forward запрещены, иначе задание не встанет на репозиторий. Это первое, что мы сверяем с разделом требований и ог…

РЕАЛИЗАЦИЯ 3 ИЗ 3

Tier-модель, Windows LAPS и SIEM-алерты на привилегии

Что настраиваем

Административная модель домена и слой обнаружения: Windows LAPS на всех PC и серверах, Wazuh 4.14 плюс Sysmon 15.2 на источниках

Как мы это делаем

1. Update-LapsADSchema на DC, затем Set-LapsADComputerSelfPermission на OU рабочих станций — компьютер сам пишет свой пароль в AD.
2. GPO LAPS: BackupDirectory = Active Directory, PasswordAgeDays 30, PasswordLength 24, полная сложность; чтение — Get-LapsADPassword узкой группой.
3. Tier-0 только с выделенной адмін-станции и FIDO2-ключа, Tier-1 — через бастион, Tier-2 helpdesk без прав на серверах, через делегирование в OU.
4. Агенты Wazuh и Sysmon: правила на 4728/4732/4756 (добавление в привилегированные группы), всплески 4625, 5136 по объектам AD, 1102 — очистка журнала.
5. Алерты высокого уровня уходят в дежурный канал с эскалацией; повторные сбои заданий бэкапа обрабатываем как событие безопасности.

РЕЗУЛЬТАТ

Пароль локального администратора уникален на каждой машине и ротируется раз в 30 дней, поэтому боковое перемещение по парку с одного добытого секрета перестаёт работать. Любое расширение привилегий в домене видно в SIEM за минуты, а не обнаруживается по факту шифрования.

КЛЮЧЕВОЙ НЮАНС

Windows LAPS и legacy-LAPS — разные продукты с разными атрибутами и политиками; при миграции проверяем режим совместимости, иначе часть машин тихо остаётся без ротации.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Бэкап живёт в той же AD, что и продакшен**
  Учётка репозитория доменная, компрометация Domain Admin стирает копии. Выносим репозиторий из домена и используем single-use credentials Veeam.

- ✕ **Immutability при неподходящем режиме бэкапа**
  Hardened-репозиторий по требованиям Veeam не принимает reverse incremental и forever forward incremental. Переводим задания на forward incremental с…

- ✕ **Ставка на WSUS как на вечное решение**
  Роль объявлена устаревшей и не развивается. Держим её как транспорт, но параллельно закладываем сторонний деплой патчей и обкатку на test-ring.

- ✕ **SMS в качестве второго фактора**
  Перехват кода и подмена SIM обходят SMS. Пользователям — TOTP-приложение, привилегированным учёткам — только аппаратный FIDO2-ключ.

- ✕ **SIEM без Sysmon и без тюнинга правил**
  Одни Windows Security-логи не показывают дерево процессов, а без подавления шума дежурный перестаёт читать алерты за неделю.

- ✕ **Плоская сеть на одном VLAN**
  Принтеры, гостевой Wi-Fi и серверы в одном сегменте. Разносим по VLAN на RouterOS 7.24.2 (bridge vlan-filtering) с фильтром между сегментами и запрет…

- ✕ **Тест восстановления «по документам»**
  Отчёт зелёный, а последний реальный разворот был год назад. Раз в квартал поднимаем боевую ВМ в изолированной сети и замеряем RTO.

- ✕ **Передача дел не прописана в договоре**
  При расторжении подрядчик формально не обязан отдавать пароли и схемы. Фиксируем срок и состав передачи документации и доступов отдельным пунктом.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Приёмочный аудит AD (PingCastle healthcheck) и внешний скан периметра до договора
- Две копии бэкапа, одна вне домена; ежемесячная проверка восстановления файла
- MFA на VPN и почте, RDP не опубликован в интернет
- Письменный SLA на реакцию и на критичные патчи в календарных днях

НОРМАЛЬНО

- Hardened-репозиторий на XFS, immutability 30 дней, SureBackup еженедельно
- Windows LAPS на всех машинах: BackupDirectory = AD, ротация 30 дней
- VLAN-сегментация: серверы, офис, гости, принтеры и IoT — раздельно
- Wazuh с агентами на серверах и PC, алерты по привилегированным группам

ХОРОШО

- Tier-0/1/2 с выделенной админ-станцией и FIDO2 для доменных админов
- Sysmon на всех узлах, правила под 4625/4728/5136/1102, дежурство 24/7
- Off-site третья копия с Object Lock и квартальный замер фактического RTO
- Incident Response Plan с ролями и учения по сценарию раз в квартал

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Есть ли отчёт приёмочного аудита AD с оценкой риска, уровнем зрелости и списком закрытых правил?
- [ ] Вынесен ли репозиторий бэкапов из домена и включён ли immutability-период?
- [ ] Когда последний раз разворачивали боевую систему из копии и сколько это заняло?
- [ ] Прописаны ли в договоре сроки установки критичных патчей в календарных днях?
- [ ] Уникален ли пароль локального админа на каждой машине и как часто он ротируется?
- [ ] Отделены ли доменные админы от повседневных учёток и есть ли у них аппаратный фактор?
- [ ] Разнесены ли серверы, офис, гости и принтеры по разным VLAN с фильтром между ними?
- [ ] Собираются ли логи в SIEM с агентами на PC и есть ли алерт на изменение Domain Admins?
- [ ] Кто и за сколько минут реагирует на критичный алерт ночью и в выходные?
- [ ] Есть ли план реагирования с ролями, телефонами и шаблонами уведомлений и учения по нему?

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).

- Проводим приёмочный аудит AD и периметра за 3–5 дней: PingCastle, BloodHound CE, инвентарь GPO и портов
- Разворачиваем Veeam 13.1 с hardened-репозиторием на XFS, off-site-копией и квартальным тестом восстановления
- Внедряем Windows LAPS, Tier-модель и MFA: FIDO2 для админов, приложение-аутентификатор для остальных
- Строим SIEM на Wazuh с Sysmon и правилами под привилегии, бэкапы и аномалии входов
- Готовим договорную часть: SLA в часах, план реагирования, регламент передачи доступов при расторжении

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 Configure policy settings for Windows LAPS (learn.microsoft.com — 2026)

02 Hardened Repository: requirements and limitations (helpcenter.veeam.com — 13.1)

03 Fast Clone (block cloning) на XFS и ReFS (helpcenter.veeam.com — 13.1)

04 Wazuh: агенты, правила и уровни алертов (documentation.wazuh.com — 4.14.7)

05 Sysmon: конфигурация и идентификаторы событий (learn.microsoft.com — 15.2)

06 RouterOS: VLAN filtering и firewall между сегментами (help.mikrotik.com — 7.24.2)

07 PingCastle Healthcheck: методология, правила и уровни зрелости (pingcastle.com — 2026)

08 Наш шаблон договора MSP: SLA, отчётность, передача дел (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.