1С на своём сервере: 5 настроек, которые проверяют первыми

Короткий технический чек-лист к разбору на aisga.kz. Отдайте его своему ИТ-специалисту или подрядчику и попросите отметить, что из этого настроено.

Пустой квадрат — повод разобраться, а не повод искать виноватого: почти в каждой компании часть пунктов закрыта не полностью.

1 Доступ к 1С снаружи — только через VPN и второй фактор

Чем грозит: Сервер терминалов или сервер СУБД, опубликованный в интернет напрямую, подбирают автоматическими сканерами за часы.

- ☐ Проверить, какие порты домена и внешних адресов открыты наружу (RDP 3389, SQL 1433, сервер 1С 1540–1541, 1560–1591, веб-публикации).
- ☐ Убедиться, что удалённая работа идёт через VPN с многофакторной аутентификацией, а не прямым подключением.
- ☐ Если публикация в интернет всё же нужна — вынести её за шлюз (RD Gateway, обратный прокси) с MFA и ограничением по географии.
- ☐ Включить блокировку после серии неудачных входов и следить за журналом подборов.

2 Права администратора — поимённый список, а не «исторически сложилось»

Чем грозит: Учётные записи подрядчиков, франчайзи 1С и уволенных сотрудников с административными правами — типовая точка входа.

- ☐ Выгрузить состав Domain Admins, Enterprise Admins, Schema Admins, локальных администраторов серверов и администраторов 1С.
- ☐ Найти учётные записи без входа более 90 дней и отключить их (не удалять сразу).
- ☐ Проверить сервисные учётные записи: права по минимуму, пароль не вечный, по возможности gMSA.
- ☐ Развести учётные записи администраторов: повседневная и административная отдельно.
- ☐ Для локальных администраторов включить LAPS, чтобы пароли не совпадали на всех машинах.

3 Резервные копии — минимум одна вне досягаемости рабочей сети

Чем грозит: Копия в соседней папке того же сервера шифруется вместе с базой. Восстанавливаться будет не из чего.

- ☐ Схема 3-2-1: три копии, два разных носителя, одна вне площадки.
- ☐ Одна копия недоступна из рабочей сети: неизменяемое хранилище, объектное хранилище с блокировкой удаления или отключаемый носитель.
- ☐ У системы резервного копирования отдельные учётные данные, не совпадающие с доменной учётной записью администратора.
- ☐ Тестовое восстановление базы 1С проводилось за последние полгода, время восстановления зафиксировано.
- ☐ Настроено оповещение об ошибке задания и об удалении точек восстановления.

4 Сервер 1С отделён от пользовательских компьютеров

Чем грозит: Заражение одного ноутбука в отделе продаж не должно давать сетевой доступ к серверу баз данных.

- ☐ Серверный сегмент отделён от пользовательского (VLAN, правила на межсетевом экране).
- ☐ К серверу 1С и СУБД открыты только нужные порты и только с нужных адресов.
- ☐ SMBv1 отключён, административные шары ограничены, удалённый рабочий стол на сервере — только для администраторов.
- ☐ Учтены подрядчики: их доступ ограничен по времени и адресам, подключения журналируются.

5 Есть тот, кто узнает об инциденте ночью

Чем грозит: Атака, замеченная в понедельник утром, обходится в разы дороже атаки, замеченной в момент начала.

- ☐ Журналы контроллеров домена и серверов собираются в одно место и хранятся не меньше 90 дней.
- ☐ Настроены оповещения: создание учётной записи и добавление в административные группы (4720, 4728, 4732, 4756), массовые неудачные входы (4625), очистка журнала (1102).
- ☐ Оповещение при отключении антивируса или защиты в реальном времени и при удалении резервных копий.
- ☐ Определено, кому уходит оповещение в нерабочее время и что этот человек делает дальше.

Если отмечено не всё

Это нормально: чек-лист показывает, где искать, но не показывает масштаб. Чтобы понять, что именно под угрозой в вашей инфраструктуре, во что обойдётся простой и что исправлять первым, нужна независимая оценка ИТ-рисков.

- Знакомство — 20–30 минут, ни к чему не обязывает.
- Проверка — 5–10 рабочих дней, без остановки работы компании.
- Отчёт — 5–10 рабочих дней: итог для руководства и технический отчёт для ИТ.
- Стоимость — от 350 000 ₸, точную сумму называем после знакомства.

Связаться: +7 (701) 717-66-24 · info@aisga.kz · aisga.kz

Документ носит справочный характер и не заменяет проектное решение по вашей инфраструктуре.