Экстренная блокировка доступа к данным на серверах

Secret Disk Server NG

Функция «Красная кнопка»

Версия	1.0
Статус	
Дата	02.07.2025

1. Проблема

Доступ злоумышленников или нежелательных лиц к особо ценным данным, хранящимся на серверах компании. Незаконное изъятие информации с корпоративных серверов без разрешения руководства компании. Физическое изъятие серверов и жестких дисков.

2. Решение - шифрование информации на серверах с возможностью применения функции «Красная кнопка» для экстренного блокирования доступа

Для чрезвычайных ситуаций в Secret Disk Server предусмотрен механизм подачи сигнала - "Тревога". Он приводит в действие команды, экстренно предотвращающие несанкционированный доступ к информации на сервере. Сигнал выполняется утилитой Secret Disk Alarm Service.

Данный механизм позволяет отключать защищённые диски, и при определённых настройках на стороне сервера удалять с сервера защищённое крипто-хранилище ключей шифрования. В результате, даже если злоумышленники завладеют нужным токеном или смарт-картой администратора безопасности, узнают пароль и будут обладать физическим доступом к серверу, они не смогут прочесть информацию, не располагая резервной копией защищённого хранилища.

Реакция на сигнал тревоги настраивается как для каждого из защищённых дисков в отдельности, так и для всего сервера.

Сигнал тревоги может быть подан:

- локально, с помощью клавиатуры компьютера или мыши;
- при нажатии физической "красной кнопки", подключённой к компьютеру в локальной сети;
- от радио-брелока;
- от различных датчиков обнаружения несанкционированного проникновения в серверную комнату или открывание серверной стойки (требует инженерной интеграции с модулем контроллера);
- с сотового телефона путём звонка на заданный номер и ввода требуемой комбинации цифр и пр. (также требует инженерной интеграции с модулем контроллера).

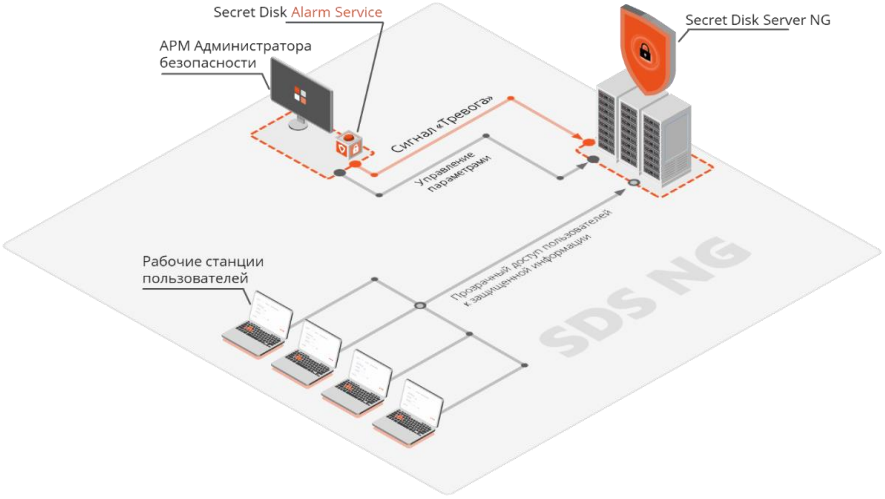
Для возобновления доступа к зашифрованным данным вначале потребуется восстановление защищённого крипто-хранилища из его резервной копии. Далее достаточно заново подключить зашифрованные диски с консоли администратора, применить электронный ключ администратора Secret Disk Server и ввести правильный пароль. В среднем, операция восстановления может занять 2-5 минут.

> **ВАЖНО! Возвращение доступа осуществляется только по решению руководства компании, ресурсы которой были зашифрованы. В целях соблюдения профессиональной этики разработчику такая возможность недоступна - продукт не имеет бэкдоров, инженерных ключей, технических учетных записей.**

3. Эффект от внедрения

- Снижение риска компрометации ценной информации.
- Полное управление доступом к защищаемой информации в сложных ситуациях.
- Противодействие незаконному изъятию физических дисков.
- Гарантированное противодействие взлому и криптоанализу защищаемых данных.

4. Как это работает



1. Диски сервера, содержащие бизнес-значимую информацию, зашифровываются с помощью Secret Disk Server NG. При этом применяются стойкие алгоритмы шифрования, на выбор клиента – отечественный ГОСТ Р 34.12-2015 (Кузнечик), зарубежный AES-256.
2. Для реализации схемы защиты администратор безопасности при настройке и управлении доступом к данным работает исключительно с применением строгой аутентификации.
3. Администратор информационной безопасности создает резервную копию крипто-хранилища, содержащую все ключи шифрования дисков сервера.
4. Резервная копия крипто-хранилища помещается на съемный носитель (например USB-накопитель) и переносится в безопасное место, контролируемое руководством компании. Хранить можно в сейфе и другом надежном месте.
5. На рабочей станции администратора безопасности устанавливается специальный программный модуль – Secret Disk Alarm Service, отправляющий сигнал тревоги. После установки в настройках модуля регистрируется сервер с зашифрованными дисками.
6. Пользователи и сервисы, осуществляющие доступ к информации на дисках сервера, продолжают свою работу в обычном режиме. Для доступа к защищенным данным не нужны программные агенты и другие дополнительные средства.
7. При наступлении чрезвычайной ситуации Администратор информационной безопасности подает сигнал тревоги, в следствии чего все зашифрованные диски сервера отключаются (прекращается доступ), а крипто-хранилище гарантированно уничтожается.
8. После срабатывания сигнала тревоги доступ к зашифрованным дискам сервера невозможен, даже при наличии у злоумышленников токена и ПИН-кода администратора информационной безопасности. Все ценные данные надежно защищены.
9. Получить доступ возможно только по решению руководства компании о восстановлении крипто-хранилища из резервной копии и подключении зашифрованных дисков.