Cryptallit NSM

Защита файловых серверов вашей организации

Какая информация является ценной и почему её важно защищать?

На каждом предприятии и в каждой организации есть свой список конфиденциальной информации, при работе с которой сотрудники должны соблюдать предусмотрительную аккуратность. В этот список могут попасть финансовые данные, данные о клиентах, в том числе защищаемые Законом о персональных данных, стратегические планы, управленческие отчёты и т.д.

Не ошибемся, если скажем, что не всегда есть время, желание и силы заниматься сложной классификацией информации и разделением её на ту, какую надо защищать, а какую не надо. Классификация крайне сложна на практике, поэтому принцип «Защищать всё» в отношении неструктурированной информации в этом случае наиболее приемлем. Такой подход более гибкий и экономит много усилий.

Защита данных в быстрорастущих организациях?

Несмотря на внедрение различных систем хранения данных с правами доступа, чаще всего большая часть информации хранится в папке на сервере Windows (файловый сервер), а так же на личных компьютерах пользователей, которые имеют доступ к серверу. В особенности это касается динамично растущих компаний, где всё делается стремительно, направлено на быстрое расширение бизнеса и времени на внедрение сложных политик безопасности попросту нет.

Какие вопросы должен задать себе собственник или менеджер, отвечающий за работу организации?

- IT-Администратор Windows владеет доступом ко всей информации? Он может «унести» всю информацию?
- В небольших организациях IT-Администратор часто еще и на аутсорсе – кто он? На кого еще работает?
- Готов ли я потратиться на проверку уровня конфиденциальности тысяч документов, лежащих общих папках на файловом сервере?
- Возможно ли перехватить конфиденциальные файлы, когда сотрудники скачивают их с сервера к себе на ноутбук?
- Если мои файловые серверы находятся во внешнем центре обработки данных (ЦОД), могут ли сотрудники ЦОДа, имеющие физический доступ к серверам, получить и доступ к моим данным?

Cryptallit NSM
Модуль локальной безопасности

Какая система позволяет защитить все данные?

Cryptallit NSM — это система защиты файловых серверов, которая реализует максимально надежный метод противодействия утечкам ценной информации при помощи стойких криптографических алгоритмов. Система обеспечивает защиту информации в сетевых папках организации, а в сочетанием с модулем локальной безопасности **Cryptallit LSM,** защищающим рабочие станции под управлением Windows, создается замкнутое пространство обработки и хранения всей конфиденциальной информации.

Как работает система и почему это эффективно?

1. Все папки на серверах зашифрованы и без специального разрешения ITшник больше не имеет доступа к конфиденциальной информации, администраторы ЦОД тоже.
2. Никакой нагрузки на файловый сервер – все «тяжелые» операции осуществляются на компьютерах пользователей.
3. Устанавливаем агентов безопасности на компьютеры сотрудников, которые должны иметь доступ к конфиденциальной информации.
4. Управляем системой централизованно, с консоли администратора информационной безопасности.

Преимущества продукта

Эффект от использования **Cryptallit NSM** дает ряд значимых преимуществ, которые заметно выделяют эту систему безопасности на фоне остальных программ защиты данных.

Отечественное решение
Продукт обладает полной санкционной независимостью. Создан в России и зарегистрирован в реестре отечественного ПО (№20257 от 27.11.2023)

Надежность защиты
Защитит всю информацию на файловых серверах вашей организации и предотвратит используя наиболее надежные методы защиты.

Простота и экономичность
Внедрение системы защиты не потребует дорогого проекта, а эксплуатация возможна силами существующих ИТ-специалистов, не имеющих специальных знаний.

Полная прозрачность
Защитные механизмы системы работают на системном уровне ОС Windows, что делает защиты данных прозрачной для легитимных пользователей.

https://cryptallit.ru
sales@cryptallit.ru
+7(495)215-27-23