Как обеспечить обмен конфиденциальной информацией между организациями для совместной работы без риска компрометации?

Рыбин Андрей, *директор по развитию компании Perimetrix*

Количество обрабатываемых электронных данных конфиденциального характера стремительно увеличивается. По этой причине возрастает потребность рынка в решениях, позволяющих безопасно передавать по открытым каналам конфиденциальную информацию между контрагентами, компаниями одной группы и не допускать ее утечки у получателя, одновременно с этим минимизируя затраты участников обмена на покупку специализированного ПО, выделение отдельных рабочих станций и наращивание серверных мощностей.

Специалистам по информационной безопасности хорошо известно, что для передачи конфиденциальной (защищаемой) информации вовне (вне периметра) по незащищенным каналам связи существует два основных варианта:

1. Передача данных в криптоконтейнере, позволяющая безопасно передать информацию и обеспечить доступ к ней определенному лицу (ID рабочей станции, пароль и т.д.). При получении доступа к данным (их расшифровке) пользователь волен поступать с ними по своему усмотрению. Вердикт: небезопасно!

2. Передача данных в закрытом формате, позволяющем только просмотр данных (электронные книги и др.). Отсутствует возможность работы (редактирования и т.д.) с такими данными. Вердикт: нет доступа (полноценного). Существует также много средств, позволяющих записать экран в момент просмотра данных и распорядиться этой записью по своему усмотрению. Вердикт: также небезопасно.

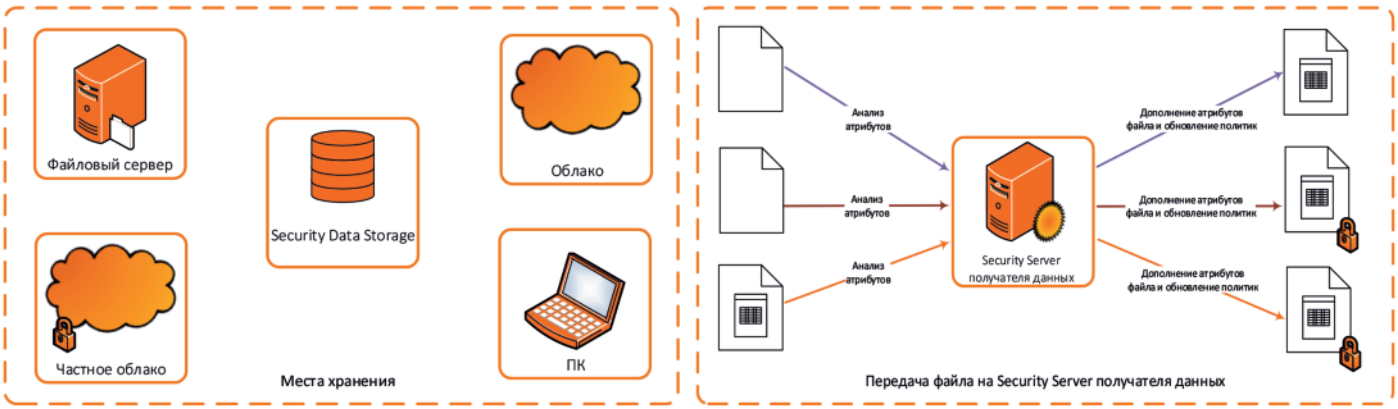
Очевидно, ни тот, ни другой вариант не обеспечивают адекватный уровень безопасности и доступ для обработки конфиденциальных данных одновременно.

Необходимый технический функционал

Нужен новый подход, который позволит вести обмен конфиденциальной шифрованной информацией между организациями с учетом ее ценности и даст возможность ее обработки без риска компрометации, исключив недостатки, описанные выше, в том числе без доступа к внутренней корпоративной сети отправителя, при условии наличия подключения к сети Интернет.

Для этого нужно реализовать следующие технические решения:

- "компактный" агент, легко загружаемый из сети Интернет;



Механизм классификации данных и применения ограничительных политик

- механизм прозрачного шифрования (шифрация и дешифрация "на лету" – в процессе работы с документами);
- передача политик безопасности вместе с конфиденциальным документом;
- предоставление доступа к конфиденциальным данным, ограниченного по времени;
- универсальная классификационная метка (конфиденциальные данные должны помечаться вне зависимости от формата, приложений для работы с ними или файловой системы на рабочей станции);
- автоматическая классификация данных в зависимости от информационной системы – источника данных.

По имеющейся у нас информации, перечисленный функционал отсутствует у представленных на рынке решений.

Главные выгоды для пользователя

Основными технико-экономическими преимуществами такого решения для потребителя должны стать:

- **обеспечение безопасного обмена конфиденциальными данными с подрядчиками, партнерами либо в рамках группы компаний;**
- **сокращение временных затрат и трудозатрат на классификацию данных;**
- **повышение эффективности работы с данными в электронном виде (упорядочивание, четкая фиксация мест хранения и используемых приложений, контроль доступа);**
- **улучшение работы комплексной системы защиты информации;**
- **определение минимального набора политик, которые обеспечат необходимый уровень защищенности данных;**
- **обеспечение безопасного обмена конфиденциальными данными с подрядчиками, партнерами либо в рамках группы компаний.**

6 принципов целевого продукта

Защищенный периметр для хранения конфиденциальной информации при использовании целевого продукта может включать в себя публичное или частное облако, файловый сервер, персональный компьютер или рабочую станцию работника и базу данных.

При прохождении конфиденциального документа через серверный компонент получателя данных должен происходить анализ атрибутов документов, их доопределение и анализ на предмет соответствия политикам безопасности, доступным получателю, и присвоение меток.

Основные принципы, заложенные в целевой продукт, можно определить следующим образом:

Требуется новый подход, который должен обеспечить возможность обмена конфиденциальной шифрованной информацией между организациями с учетом ее ценности и возможностью её обработки без риска компрометации, исключив недостатки, в том числе без доступа к внутренней корпоративной сети отправителя, при условии наличия подключения к сети Интернет.

1. Все создаваемые конфиденциальные документы на рабочих местах обогащаются дополнительными атрибутами.
2. Обеспечивается возможность использования как частных, так и глобальных политик всех серверов в рамках единой системы.
3. На основании дополнительных атрибутов, в том числе искусственно присваиваемых в процессе ручной классификации, осуществляется применение политик безопасности – совокупности правил работы с классифицированными объектами.
4. Информация о правах конкретного пользователя хранится на одном или более связанных серверах.
5. Любое обращение к конфиденциальному документу сопровождается проверкой соответствия прав доступа к документу, основываясь на ограничениях обращающегося, установленных на объекте в соответствии с политиками, за счет обращения к серверной компоненте.
6. При проверке соответствия прав доступа к документу и политик производится поиск наличия разрешения по всем связанным серверам в рамках единой системы.

Адаптация к цифровым условиям

Окружающая нас документальная и, можно сказать, общая информационная составляющая имеет в подавляющем большинстве цифровой вид, а значит средства владения, хранения, трансформации и передачи данных нужно адаптировать к новым цифровым условиям. Можно с большой уверенностью предположить, что для оперирования цифровой информацией необходима возможность классифицировать ее по самым широким и многочисленным признакам и поддержать эту классификацию программным продуктом, который обеспечит соблюдение классификационных правил взаимодействия с информацией и гарантирует ее конфиденциальность. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru