Защита файловых хранилищ: с какими проблемами можно столкнуться и как их решить?

Сергей Добрушский, *директор по развитию продуктов ООО "СайберПик"*
Виктор Сердюк, *генеральный директор АО "ДиалогНаука"*

Неструктурированные данные являются одним из основных информационных активов любой компании. К ним относятся электронные документы и файлы, расположенные в корпоративных хранилищах, а именно офисные документы, файлы PDF, скан-копии, аудио- и видеоконтент. То есть практически любая информация, не расположенная внутри СУБД, причисляется к неструктурированным данным.

Безопасность файловых хранилищ

Проблема защиты хранилищ неструктурированных данных стоит остро во многих компаниях. Прежде чем переходить к способам защиты и к описанию этих проблем, необходимо определить, почему задача защиты подобных систем является актуальной.

По различным оценкам, средний объем неструктурированных данных может достигать 80% общего объема электронных данных, находящихся на жестких дисках компании. При этом большая часть неструктурированных данных часто не приносит пользы для бизнеса. Во многих корпоративных хранилищах можно найти дубликаты документов, которые создаются сотрудниками из-за отсутствия контроля копирования, устаревшие файлы, к которым не обращались пару лет, и контент, не связанный с деятельностью компании (фото, видео, файлы). Отметим также, что средний рост объема хранилищ неструктурированных данных может достигать 30% в год, что требует постоянного расширения этого объема.

Отсутствие контроля за такими данными приводит не только к лишним тратам на хранилища, но и несет в себе риски нарушения требований регуляторов и утечки важной коммерческой информации.

Решения класса DCAP/DAG

Для контроля неструктурированных данных на рынке решений информационной безопасности присутствует отдельный класс продуктов – DAG (Data Access Governance)/DCAP (Data-Centric Audit and Protection). Существует ряд российских и зарубежных систем подобного класса со своими плюсами и минусами, которые решают следующие, обязательные для класса DCAP/DAG, задачи:

- аудит действий пользователей по отношению к хранилищам неструктурированных данных;
- классификация документов, расположенных на защищаемых хранилищах;
- анализ и управление правами доступа пользователей к данным.

Какие хранилища неструктурированных данных используются в компаниях?

Инфраструктура даже средней компании может включать разные типы файловых хранилищ от целого списка вендоров. Выделим наиболее часто встречающиеся:

- файловые хранилища под управлением ОС Windows Server, включая DFS;
- хранилища на базе ОС Linux, включая сертифицированные типы ОС;
- порталы MS SharePoint, включая облачные версии;
- почтовые серверы MS Exchange;
- облачные хранилища NextCloud;
- NAS-системы NetApp и Dell EMC;
- базы знаний Atlassian Confluence.

Отдельно отметим контроллеры домена MS Active Directory. Формально их нельзя назвать хранилищами неструктурированных данных, но их защитой обычно занимаются решения класса DAG.

Для компаний, имеющих разнородные файловые хранилища либо же инфраструктуру, включающую в себя несколько связанных между собой доменов, использование решений класса DCAP/DAG становится еще более актуальным. Решения DCAP/DAG позволяют управлять из единого интерфейса всеми функциями безопасности, необходимыми для данных хранилищ.

"Спектр" – DAG от компании "СайберПик"

Рынок российских систем класса DCAP/DAG начал формироваться несколько лет назад. До этого в решении схожих задач могли помочь продукты класса DLP, но их функционал в части защиты хранилищ неструктурированных данных часто ограничивался функционалом классификации. При этом из-за специфики DLP-систем (контроль за действиями пользователей на рабочих станциях) на больших объемах хранилищ неструктурированных данных пользоваться данным функционалом в полной мере было сложно.

Одной из систем, которая отвечает всем функциональным требованиям для решений класса защиты хранилищ неструктурированных данных, является решение "Спектр" от российской компании "Сайберпик", резидента "Сколково". Продукт "Спектр" включен в реестр отечественного ПО и, что важно, не требует для своей работы никаких сторонних коммерческих модулей, как СУБД, так и ОС, на которых он может работать.

Основные задачи, для решения которых нужны системы класса DCAP/DAG

Системы подобного класса обычно используются для вполне четких задач, таких как контроль за данными и правами доступа к ним, а также непосредственное обеспечение доступа к данным, которые расположены на корпоративных хранилищах.

Рассмотрим пример базовой важной задачи, в решении которой помогают продукты класса DCAP/DAG – поиск местонахождения (или классификация) критичной информации на корпоративных хранилищах.

Для решения этой задачи система "Спектр" имеет большое количество предустановленных категорий информации, подпадающих под требования российского и международного законодательства и отраслевых требований, а также система поддерживает существенный список форматов файлов.

"Спектр" позволяет настраивать категории, что добавляет гибкости при поиске нетиповой информации, но при этом актуальной для той или иной компании в отдельности. Сами категории представляют собой комбинации фраз, слов, регулярных выражений и частоты их вхождений. Система дает возможность создать свои или использовать предустановленные категории таким образом, чтобы количество ложных срабатываний было минимальным.

При этом есть функция анализа содержимого графических форматов данных как с помощью модуля OCR, так и при помощи модуля поиска шаблонов сканкопий документов, построенном на основе нейронных сетей.

Данный модуль является востребованным, учитывая, что большинство сотрудников ИТ- и ИБ-подразделений в полной мере не обладают информацией о том, где именно содержится наиболее ценная информация компании. Непрерывная классификация файловых хранилищ, которую обеспечивает система "Спектр", позволяет снизить риск утечек критичной информации и упростить прохождение различных аудитов, в список которых часто попадают файловые хранилища компаний.

Анализ и минимизация прав доступа к данным

Понимание местонахождения критичной информации влечет за собой вторую важную задачу – определение текущих прав доступа к ресурсам компании. Для решения этой задачи также принято использовать продукты класса DAG. Речь идет как об анализе прав доступа к конкретному каталогу/документу, так и о возможности просмотра всех доступных для определенного сотрудника ресурсов. Надо сказать, что даже в простой инфраструктуре с файловым сервером под управлением ОС Windows Server и контроллером домена без продукта класса DAG эту задачу решить крайне сложно, учитывая, что права могут выдаваться как напрямую, так и через группы безопасности, которые, в свою очередь, могут наследоваться. Не стоит забывать и про такие риски, как наличие критичных документов в общем доступе, прямых прав у сотрудников либо же неуправляемых каталогов.

Используя решения DAG и систему "Спектр" в частности, можно автоматически выявлять вышеописанные риски и сокращать избыточные права доступа. Так, для безопасного сокращения прав в продукте присутствует возможность моделирования изменений прав – это позволяет еще до фактического изменения понять, к каким ресурсам сотрудник может потерять доступ на основании его предыдущих активностей с данными.

Выявление фактов неправомерного доступа к данным и, как следствие, их утечек

Аудит действий сотрудников в части доступа к данным является одной из важнейших опций продуктов класса DCAP/DAG. При этом аудит действий – это не только возможность ретроспективного расследования инцидентов информационной безопасности, но и решение таких каждодневных проблем, как потеря документов сотрудниками. Обычно такие задачи решаются путем направления заявки в ИТ-службу компании, которая, в свою очередь, либо восстанавливает документ из резервных копий, либо производит поиск "потерянного документа" с использованием организационно-технических мер в течение длительного времени.

Система "Спектр" фиксирует все факты обращения к документу, включая факты перемещения, переименования, удаления и изменения прав доступа. Благодаря "Спектру" обработка заявки по поиску или восстановление доступа к документу займет несколько минут.

DAG для представителей ИТ-департаментов

"Спектр" полезен не только для решения задач ИБ-департамента, но и для представителей ИТ. Система поможет ИТ-специалистам решить задачи, связанные с оптимизацией нагрузки на файловые хранилища. Так, "Спектр" может выявить наличие дубликатов больших файлов, определить ресурсы, к которым длительное время не было обращений, либо в целом провести анализ документов, занимающих большую часть дискового пространства. Функционал защиты контроллеров домена часто используется представителями ИТ-отделов. Это задачи, связанные с контролем изменений на уровне Active Directory, а также анализ конфигураций

и настроек учетных записей в домене. Так, со "Спектром" можно быстро определить перечень учетных записей с постоянными паролями, наличие пустых групп безопасности или неактивных учетных записей.

Соответствие требованиям регуляторов

Перечисление полного списка стандартов, требований, федеральных законов и НПА, для закрытия которых полезна система "Спектр", требует отдельного обзора. Отметим лишь, что опции аудита доступа и анализа содержимого файловых хранилищ, например на наличие персональных данных, может серьезно снизить затраты на подготовку и прохождение аудитов, при этом повысив внутренний уровень информационной безопасности компаний.

Результаты применения решений защиты хранилищ неструктурированных данных

Проблемы, описанные в этой статье, являются актуальными для компаний с численностью от 100 сотрудников. Решать их можно разными продуктами, от полуавтоматических систем с применением скриптов до полнофункциональных систем класса DCAP/DAG.

Практическая польза от систем класса DCAP/DAG часто становится видна не только использующим их подразделениям, но и представителям бизнеса. Системы обладают высоким уровнем автоматизации и позволяют снизить затраты ресурсов, которые требуются для решения их задач.

Отдельно отметим серьезный функционал DCAP/DAG в части оптимизации файловых хранилищ, который при ограниченном количестве вычислительных ресурсов может обеспечить бесперебойную работу бизнеса. ●

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