АЛЕКСЕЙ ПАРФЕНТЬЕВ,
руководитель отдела аналитики «СёрчИнформ»

Спокойствие, только спокойствие!

Как контролировать информацию «в покое» – защищаем базы данных и файловые системы.

Простого доступа к файлам и базам данных инсайдеру бывает достаточно, чтобы нанести родной компании миллионный ущерб. Ловить таких – тяжелый труд. Жизнь специалистам по безопасности сильно облегчают DCAP- и DAM- решения. Пока такие редко встречаются в ИТ-инфраструктуре компаний, но это временно. Давайте разберемся, кому имеет смысл присмотреться к программам и протестировать их?

Если информация не утекает, это еще не значит, что она в безопасности. Тот, кто забывает об этом, рискует получить неприятный сюрприз. О таком рассказывал один из наших клиентов.

КЕЙС 1

Компания (крупная торговая сеть) заказала маркетинговое исследование. Стоило оно десятки тысяч долларов, доступ к документу был у нескольких десятков человек: топ-менеджмента, представителей маркетингового департамента. В один день ИБ-специалисту становится известно, что файл оказался в даркнете, а еще через неделю – в открытом интернете. Это значит, что исследование могло попасть к конкурентам – не затратив копейки, они могли получить ценную информацию о рынке и планах ритейлера.

«Сюрприз» другого рода обнаружился в миграционной службе.

КЕЙС 2

К сотруднику УФМС по одной из российских областей обратился знакомый, который попросил скрыть информацию о двух правонарушениях в своем досье в базе данных «Мигрант». Работник знал, что это можно сделать удаленно, подключился к базе из дома и данные блокировал. За это получил вознаграждение 5000 рублей.

Объединяет два кейса то, что речь в них идет о так называемых «данных в покое». Контролировать их – задача сложная. А если компьютерная сеть в

вашей компании насчитывает больше 10 машин – читайте, почти невозможная. Чтобы видеть, кто обращается к данным, кто меняет или удаляет их, создает новые версии документов, нужны специализированные программы контроля. Речь идет о двух классах решений: DCAP-системе и DAM-системе. Сами термины еще не стали такими же привычными, как «антивирус» или «файрвол», поэтому давайте разберемся в понятиях.

Who is? DCAP-система (Data-Centric Audit and Protection)

DCAP – это решение для автоматизированного аудита файловых систем. В его задачи входит разобраться:

- Какие документы содержат критичную для бизнеса информацию?
- Сколько в компании таких данных и где они находятся?
- Кто имеет к ним доступ и может их редактировать?

Такие задачи могут стоять и перед ИТ-службой компании: DCAP спасает от бардака в файловой системе, потому что каждому документу присваивается категория («договоры», «прайсы», «персональные данные», «исследования» и т. д.). Не главная, но полезная функция программ этого класса – теневое копирование документов, что позволяет без проблем восстановить их, если что-то случится.

Но в первую очередь программа – инструмент ИБ-специалистов. Именно наше DCAP-решение (FileAuditor) помогло разобраться в причинах утечки исследования в кейсе 1. Стало понятно, что файл оказался доступен трем сотням сотрудников, хотя круг пользователей должен был быть в десять раз меньше. Если бы программа стояла раньше, об инциденте стало бы известно уже когда кто-то из сотрудников получил избыточные права доступа. А не по факту пересылки или появления документа в Интернете.

Вот как выглядит логика работы FileAuditor:

- Находит файл.
- Проверяет его по правилам и делает служебную метку (персданные, договор и т. д.).
- При необходимости копирует файл в хранилище.
- Логирует все действия с файлами и папками.
- Вычитывает права доступа для файлов и папок.

При последующих проверках система сканирует только измененные и вновь добавленные файлы.

DAM-системы (Database Activity Monitoring)

Это решение для автоматизированного мониторинга баз данных. Задача насущная, так как БД – это главный информационный актив бизнесов. Мошенникам интересен и весь массив, и точечный доступ к отдельным данным. DAM-система позволяет справиться с этой угрозой, например, наш DataBase Monitor фиксирует:

- Кто обращается к базам данных и с какой целью?
- Какую информацию выгружают из баз данных и в каком объеме?
- Какие изменения пользователи вносят в базы данных?

Работа по контролю автоматизируется, так как ИБ-специалист получает срочное уведомление, если кто-то обращается к базе с нарушением политик безопасности. Это может быть нарушение прав доступа. А может быть случаем, когда легальный пользователь совершает какой-то опасный набор действий. Кстати, вопрос контроля «людей с правами» (привилегированных пользователей) стоит очень остро. Многие инциденты оказываются нерасследованными, потому что внешне действия пользователя в базе данных выглядят совершенно безобидно.

Например, один из самых частых инцидентов в сотовом ритейле – когда сотрудник салона связи обращается к базе данных и оформляет перевыпуск sim-карт клиентов, чтобы снимать с них деньги. По заявлению абонента сотрудник, действительно, имеет право перевыпускать симку, и его действия в БД не покажутся никому подозрительными. Так он может успеть совершить множество эпизодов – до первого обращения пострадавшего. И службе безопасности придется разбираться с уже произошедшим эпизодом. Программа же подаст сигнал гораздо раньше – в тот момент, когда увидит подозрительную активность: что сотрудник не просто обращается к БД, но и делает выборку по абонентам, у которых на счету больше 5000 руб., например.

Такой контроль можно осуществлять и на уровне СУБД, но не все разработчики систем его предусматривают, получается, что часть баз данных в компании остаются без присмотра. А еще этот формат контроля просто неудобен: на разбор инцидента уходит слишком много времени. DAM-решения этих недостатков не имеют.

Банки, ритейл. Далее – везде

Пока российский рынок DAM- и DCAP-систем в начале своего пути. «СёрчИнформ FileAuditor» стал первым отечественным решением в своем классе. DataBase Monitor тоже в числе пионеров. Но развивается рынок очень бодро. Наши решения были разработаны под запрос клиентов из сфер, где давно поняли ценность автоматизированных средств контроля, – банковской отрасли и ритейла. Но после релиза запрос на обе программы появился в каждой сфере, с которой мы работаем. Лучшие практики мы собрали в «Белых книгах». Скачать их можно у нас на сайте.