Цена информации

Информация для любой компании является ценным ресурсом, обеспечивающим деятельность и репутацию на рынке. Этот ресурс так же значим, как и другие ценные активы — люди, земля, недвижимость, средства производства и др.

Джабраил Матиев, руководитель отдела информационной безопасности системного интегратора IBS Platformix

Впрочем, тут есть несколько важных особенностей. Во-первых, ценность информации зачастую определяется не только выгодами от владения ею, но и размерами потерь в случае утечки. В этой связи зачастую потеря информационного актива становится гораздо большей проблемой по сравнению с потерей неинформационного актива эквивалентной стоимости. Во-вторых, информация способна существенно изменять собственную ценность в разном контексте — например, в разных местах или в разное время. В-третьих, появление и применение концепции Big Data внесли огромную неопределенность в вопрос определения стоимости данных, позволяя извлекать ценнейшую информацию из больших объемов «мусора».

Масштаб потенциального ущерба от утечек информации заставил бизнес искать оптимальные способы защиты. В ответ на сформировавшуюся потребность рынок предложил решения класса «Средства защиты от утечки/потери данных» (DLP — Data Loss/Leak Prevention).

Эволюция защиты от утечек

DLP-решения прошли эволюционный путь от архиваторов почты с поисковиком до средств активного мониторинга всевозможных каналов передачи информации на всех уровнях (уровень сети, уровень систем хранения и уровень рабочих станций) и на всех стадиях (передачи (data-at-move), хранения (data-at-rest) и обработки (data-at-use)).

Морфологические механизмы, автоматический поиск конфиденциальной информации в системах хранения данных, продвинутые технологии детектирования

фактов утечки, распознавание данных «на лету» — это далеко не полный перечень функционала, который встраивался в DLP в процессе эволюции. В итоге DLP превратились в комплексные решения с множеством модулей на разных уровнях. Компании, внедряющие DLP, успешно находят нарушителей и полностью удовлетворены работой системы. И все было бы хорошо, но — утечки продолжаются.

DLP не работает?

Получается, что DLP-решения не работают? DLP работает, но выполняет она ровно те задачи и по тем алгоритмам, которые в нее заложены: ищет там, где умеет; так, как умеет; то, что вы ей скажете. Сами производители открыто заявляют, что DLP не панацея от утечек, ведь опытный специалист найдет способ обойти механизмы DLP и унести информацию, которая ему нужна. Механизмы, используемые в DLP, априори предполагают некую вероятность срабатывания, что в большинстве случаев просто недопустимо. Означает ли это, что DLP не нужна? Нет, это не так, но необходимо четко понимать роль и место DLP-системы в комплексной системе защиты информации компании.

Место DLP в иерархии средств защиты

Практика применения DLP-решений выявила две интересные особенности. Во-первых, DLP-решение хранит информацию о коммуникациях (даже если нарушений в них не было обнаружено). Во-вторых, DLP очень хорошо защищает от непреднамеренных, случайных утечек.

Получается, что, несмотря на то что DLP-решения не устраняют на 100% проблему утечек информации, они эффективно используются для выполнения других задач.

Их первая особенность приводит к тому, что DLP хорошо использовать для расследований фактов утечек (forensics — такой модуль имеется в решении компании InfoWatch), так как в них накапливается большое количество информации, полезной при разборе инцидентов. Вторая особенность обеспечивает другое применение DLP — повышение осведомленности персонала (awareness) и обучение персонала политике информационной безопасности (контроль выполнения). Решение обеих этих задач полностью оправдывает внедрение DLP.

А что делать с утечками?

DLP нашли свое применение, а вот задача защиты от утечек так и не была решена. Почему? Ответ прост: коробочного решения в данном случае быть не может. Борьба с утечками — это важная и комплексная задача, которую нужно решать на стыке технологий и организационных мер.

Что это означает на практике?

В первую очередь необходимо понимать, что утечки могут происходить как изнутри (с чем призваны бороться DLP-решения), так и извне — путем вторжения злоумышленника в корпоративную сеть.

Решение проблемы внутренних утечек целиком и полностью зависит от контроля внутренних процессов и потоков информации. Для контроля процессов необходимо классифицировать информацию ограниченного доступа, определить правила ее обработки и, самое главное, довести их до персонала путем обучения в рамках программ повышения осведомленности. Для разграничения потоков информации необходимо использовать специализированные решения (в том числе DLP). Совокупность мер контроля, повышение осведомленности и введение мер защиты помогут снизить риски внутренних утечек.

Когда речь идет о внешних утечках, необходимо защищать периметр сети. В этом случае нужно применять системы сетевой безопасности. Во-первых — межсетевые экраны следующего поколения (next generation firewall), консолидирующие в себе сразу несколько функций продвинутой защиты сети и блокирующие возможность успешных типовых атак, если речь не идет о целенаправленных атаках (advanced persistent threats APT). Во-вторых — специализированные решения по защите от продвинутых атак («песочницы», автоматизированные лаборатории и др.). В-третьих — решения по защите конечных устройств, реализованные в комплексных продуктах (Endpoint Protection). При правильном сочетании описанных мер риски внешних утечек заметно снижаются.

Если говорить о новом поколении DLP, то в качестве следующего этапа его развития мы прогнозируем появление более строгих вариантов DLP, которые жестко контролируют передвижение грифованной информации по принципу работы файервола с сетевыми пакетами. Для этого требуется решить другую непростую задачу по однозначной классификации информации с фиксацией метаданных. Одним из самых известных на сегодняшний день решений по классификации информации является продукт компании TITUS. С учетом того, что на российском рынке данное решение представлено очень слабо, да и в целом ниша систем классификации еще не занята, это может дать серьезную фору отечественным производителям для проработки и продвижения такого рода решений.