DLP: двойная защита

Вадим Здор, *ведущий консультант по вопросам защиты информации компании InfoWatch*

Подход к защите информации от утечек формировался исходя из условий замкнутого пространства и контролируемого доступа к чувствительным данным. Однако в сегодняшних реалиях, когда информационные технологии превратились в важнейший инструмент развития бизнеса, концепция защищенного периметра дала трещину. И куда пойдет направление DLP, сказать очень непросто.

Тренды

Впрочем, при ближайшем рассмотрении можно выделить несколько стержневых трендов, которые неизбежно повлияют на идеологию DLP завтрашнего дня. Во-первых, это принципиальное отличие типов информации и требований к ее защите в зависимости от специфики организаций. Даже в компаниях, относящихся к одному и тому же сегменту (банки, госорганизации, телекоммуникации), структура информационных активов неодинакова. Как результат, нет и не может быть единого инструмента, единой технологии защиты информации. DLP-проекты плохо масштабируются даже в пределах одной вертикали. Потому, собственно, и нет до сих пор типового "коробочного" DLP-софта.

Еще один концепт, обуславливающий неизбежное изменение подходов к защите информации, – инициатива BYOD (Bring Your Own Device). Более 90% сотрудников используют для работы собственные гаджеты. Бизнес не может игнорировать этот тренд – BYOD делает работников более продуктивными.

Вообще, налаживание контактов и достижение результатов посредством обмена информацией в онлайн-пространстве неизбежно станет доминирующим видом коллаборативного взаимодействия. Облачные технологии, о которых так много говорится последние пару лет, в реальности уже обеспечивают большую часть функциональности, необходимой для организации коллективной работы. Не за горами повсеместная адаптация технологий социальных сетей для бизнеса.

Интеграция систем DLP и Rights Management

Универсальный подход к защите информации довольно прост и существует давно: шифрование контента, подлежащего защите; аутентификация пользователей, имеющих доступ к этому контенту; контроль действий пользователей с контентом. Очевидно, что именно с контролем, в случае выхода контента за пределы периметра, и возникают проблемы.

Собственно, вопрос можно переформулировать: как и что сделать для того, чтобы системы предотвращения утечек информации работали и внутри, и вне организаций? Можно ли избавить защиту информации от географической (или сетевой) привязки с тем, чтобы контролировать свои данные вовне, в том числе в средах партнеров и клиентов?

Такой функционал уже реализован в системах управления правами доступа (Rights Management), но они довольно сложны в плане архитектуры. Слабое место таких систем – пользователь. Он сам решает, какая информация подлежит защите. Конфиденциальные данные могут быть просто "не запакованы" из-за невнимательности.

Решение напрашивается само собой – необходимо "развернуть" DLP-систему, сориентировав ее не только вовнутрь (контроль исходящей информации), но и вовне. Достаточно добавить к существующему пулу каналов, которые контролирует и анализирует система, еще один – данные от поисковой машины, собирающей информацию на просторах глобальной сети.

Технически это несложно. Поисковики умеют индексировать открытый Интернет. Отфильтровав информацию, по различным признакам относящуюся к нашей компании, мы получаем готовый поток документов, сообщений, изображений и прочее. Это могут быть упоминания компании, высказывания сотрудников, мнения клиентов. Зачастую среди прочего встречается конфиденциальная информация, случайно или намеренно оказавшаяся в сети.

Причины различны: ошибки пользователя, неверные политики безопасности… Важно, что в случае работы DLP в обе стороны мы можем выстроить двойную защиту. Даже если DLP-система, контролирующая исходящий поток, что-то пропустит, поисковый сервис зарегистрирует факт утечки при публикации документа в сети. Достаточно лишь проанализировать "внешний" поток уже имеющимися лингвистическими средствами DLP-системы, и мы получим реальное представление о том, что за информация ушла из компании, когда это случилось и, что важно, кто ее разместил в Интернете.

InfoWatch Крибрум

Подход "DLP вовне" может быть реализован на основе облачного сервиса InfoWatch Крибрум, который пока используется для мониторинга и анализа социальных медиа. Отметим лишь, что стремление заказчика к минимизации количества разнородных IT-решений в среде компании неизменно приведет к интеграции таких систем в рамках концепции "двойной защиты". То есть не будет отдельного DLP "вовнутрь" и DLP "наружу" – только единое решение.

Легко видеть, что вендор, предложивший лучшее и наиболее функциональное сочетание DLP с системами мониторинга и анализа информации в Интернете, имеет очень хорошие шансы перекроить рыночный пирог в свою пользу.

Именно такие решения будут представлять собой переходную фазу к абсолютно новым технологиям, работающим в облачных инфраструктурах, вне пределов корпоративных систем обеспечения информационной безопасности. ●

Как известно, технологии защиты информации от нежелательных утечек (обычно обозначаются как DLP – Data Leakage Protection) появились давно – еще во времена "холодной войны". Тогда сети представляли собой замкнутые, автономно функционирующие системы с ярко выраженным периметром и сильно ограниченными или полностью отсутствующими механизмами передачи информации вовне. Да и потребности в распространении чего-либо за пределы контура не было.

NM ●
АДРЕСА И ТЕЛЕФОНЫ ГРУППЫ КОМПАНИЙ "INFOWATCH"
см. стр. 80