Владимир Безмалый

Внедряем DLP?

Под DLP (Data Leak Prevention) понимают технологии (и их программно-аппаратные реализации) предотвращения утечек, умышленных или нет, конфиденциальных данных из информационной системы организации. Сегодня много говорят о таких системах, но так ли с ними все просто?

Действительно, внедрение DLP-систем давно стало уже не только модой, но необходимостью, ведь утечка конфиденциальных данных может привести к огромному ущербу для любой компании, а главное – оказать не одномоментное, а длительное влияние на бизнес. При этом ущерб может носить не только прямой, но и косвенный характер. Ведь, кроме всего прочего, в результате подобного инцидента компания, что называется, теряет лицо, т. е. свою репутацию, оценить которую в денежном эквиваленте весьма и весьма непросто! Но еще сложнее организациям, использующим в своем бизнесе интеллектуальную собственность. Для них утечка может оказаться настоящей катастрофой и даже привести к полному краху. И тем не менее, так ли велики описанные риски?

Согласно исследованию Computer Crime and Security Survey 2008 (infowatch.ru/threats_and_risks/risks_analysis/), проведенному институтом CSI, почти половина (44%) компаний в течение года сталкиваются с негативными действиями инсайдеров и утечкой конфиденциальных данных. Помимо этого, 42% их общего числа заявили о краже у них мобильных носителей, а 2% ежегодно фиксируют у себя случаи саботажа. Иными словами, любая организация может столкнуться с действиями инсайдеров или потерей мобильных носителей с вероятностью 44 и 42% в год соответственно.

А исследователи из института Ponemon в своем отчете The 2008 Annual Study: Cost of a Data Breach оценивают средний размер ущерба, связанного с хищением конфиденциальной информации, в 6,6 млн долл. (в 2007 г. – 6,3 млн) для США, 1,4 млн фунтов стерлингов для Великобритании и 2,41 млн евро для Германии.

В наших реалиях цифры, конечно, будут несколько иными, но вывод останется тем же – в серьезности угроз утечки информации сомневаться не приходится. Однако это вовсе не означает, что нужно немедленно, сломя голову, бежать к поставщикам DLP-систем. Оказывается, добиться от них нужного эффекта не всегда просто. Почему?

С точки зрения бизнеса классическая DLP-система по сути представляется черным ящиком, на вход которого поступает анализируемая информация, а на выход – только разрешенная к пересылке. И чтобы все это работало, вроде бы нужно совсем не много – установить данную систему на сетевой шлюз и сконфигурировать правила. Так в чем же проблема?

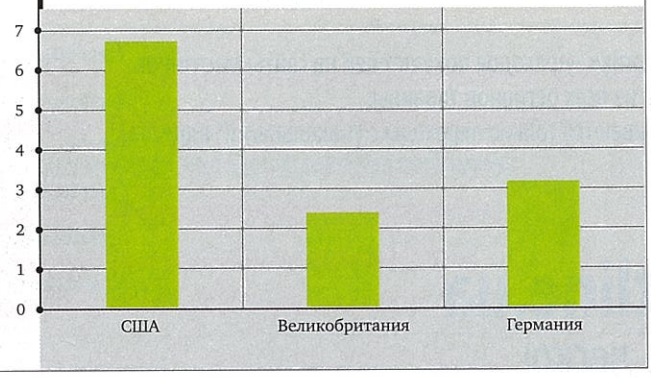
На самом деле создать исчерпывающий и эффективный комплект правил фильтрации не так-то просто. Ведь на практике бывает довольно сложно отличить информацию, легально покидающую вашу организацию, от нелегальной. Более того, весьма нередко, увы, компании даже не имеют формальных критериев для определения конфиденциальности данных.

Именно поэтому зачастую внедрение DLP-систем начинается с того, чем, по идее, должно заканчиваться. То есть DLP-система покупается, разворачивается, настраивается, и тут выясняется, что как таковой политики безопасности на предприятии не существует, классификация информации отсутствует, сотрудники не подозревают, что им можно пересылать, а что нет. Увы, это действительно не редкость.

А на самом деле начинать надо с гораздо более прозаичных вопросов. И прежде всего – с подготовки и принятия внутреннего документа с условным названием «Положение о конфиденциальной информации», в котором будет четко указано, какие данные на предприятии являются конфиденциальными (более подробно об этом написано в статье «Внутренние угрозы в период кризиса», ko-online.com.ua/41711).

Вместе с тем нельзя забывать о том, что обеспечение информационной безопасности – это непрерывный процесс, основное содержание которого составляет управление – людьми, рисками, ресурсами, средствами защиты и т. п. Ведь внедрение DLP-систем (как и мно-

Средний размер ущерба из-за утечек информации (млн долл.)



гих других) влияет на большинство внутренних бизнес-процессов, и именно в этом заключается главная проблема.

В частности, крайне важно осознать, что обслуживающий персонал и конечные пользователи являются неотъемлемой частью информационной системы. От того, каким образом они реализуют свои функции, существенно зависит не только ее работоспособность (эффективность решения задач), но и безопасность. Т. е. персонал надо обучать.

Принципиально также понимать, что DLP-система – не панацея. Ее внедрение – всего лишь часть комплекса мер по защите информации. Увы, быстрых, эффективных и дешевых решений в сфере безопасности не существует в природе!

Отдельного разговора заслуживает украинская специфика – куда же без нее. По моему мнению, перспективы применения DLP-технологий в Украине весьма туманны, и на то есть масса причин.

В первую очередь отечественный бизнес по-прежнему в значительной степени остается «стихийным». И согласитесь, странно ожидать регламентации работы с информацией там, где зачастую (а нередко это делается даже умышленно) не формализуются гораздо более очевидные моменты и отношения. А ведь, как говорилось выше, заниматься этим нужно постоянно!

Впрочем, это вопрос самоорганизации, т. е. фактически субъективный, а значит, при желании решаемый. Чего нельзя сказать о вопросах объективных, связанных в первую очередь с юридической стороной, о которой большинство поставщиков предпочитают умалчивать. Дело в том, что Конституция Украины гарантирует тайну переписки независимо от ее типа (частная, служебная, личная). Из этого мгновенно следует, что фирма, просматривающая, пусть даже и с помощью DLP-системы, письма своих сотрудников, фактически нарушает наш Основной Закон.

Но даже если закрыть глаза на этот нюанс или попробовать как-то подстраховаться с помощью грамотного юриста, надо понимать, что настройка DLP-систем далеко не тривиальное дело. Как минимум для этого необходим специалист с весьма широкими и глубокими познаниями в ИТ, в частности в области документооборота. А еще нужно будет организовать обучение пользователей корректному указанию грифов документов и проверять их навыки самым серьезным образом – иначе все усилия пропадут втуне.

Только не подумайте, что я отговариваю вас от использования DLP, вовсе нет! Я лишь хочу сказать, что внедрение этих технологий требует колоссальной работы, которая далеко не каждому окажется по плечу. Если же вы все-таки решитесь, то вот как примерно должны выглядеть ваши действия:

- аудит бизнес-процессов и существующего документооборота;
- классификация используемой информации;
- разработка системы грифов конфиденциальности;
- внедрение системы электронного документооборота;
- формализация прав сотрудников;
- обучение персонала правилам маркировки и обработки информации;
- закрепление требований информационной безопасности в должностных инструкциях;
- создание свода признаков конфиденциальной информации (т. е. будущих правил для DLP-системы);
- собственно покупка и внедрение DLP-системы.

Естественно, это достаточно грубая схема, и в каждом случае необходимо учитывать свои нюансы, однако невыполнение любого из этих шагов делает применение DLP-системы попросту бессмысленным.