Александр Ан,
IT-Team Service

Data Loss Prevention.

Предотвращение утечки конфиденциальных данных

Введение

На фоне стремительно развивающихся информационных технологий, их повсеместного вовлечения в жизнь общества, работу государственных органов, различных финансовых структур, здравоохранительных и образовательных учреждений и т. д., в геометрической прогрессии растут и объемы хранимой и обрабатываемой цифровой информации. Персональные данные, научно-исследовательские разработки, программный код, различная финансовая информация — вот лишь краткий перечень того, что может храниться в цифровом виде и являться при этом важнейшими информационными активами организации. Соответственно, актуальнейшей проблемой становится предотвращение случайной или намеренной утечки конфиденциальных данных. Помочь в этом могут специализированные решения класса Data Loss Prevention (DLP), предназначенные для проверки содержимого хранимых и перемещаемых данных и способные должным образом реагировать в случае обнаружения конфиденциальной информации, например, отправляя уведомления по электронной почте или блокируя передачу данных.

Несмотря на финансовый кризис, мировой рынок DLP активно развивается все последние годы. По оценкам международного независимого исследовательского агентства Гартнер, он составил свыше 425 миллионов долларов США в 2011 году и превысит 520 миллионов долларов в 2012 году. Рынок представлен решениями от различных широко известных вендоров, таких как Symantec, McAfee, RSA и т. д. Все предлагаемые решения различаются по своим функциональным возможностям и позиционированию на рынке.

В Узбекистане еще несколько лет назад никто всерьез не беспокоился о необходимости защиты своих конфиденциальных данных, однако за последний год ситуация кардинально изменилась. На сегодняшний день многие коммерческие банки, государственные учреждения и частные коммерческие организации прорабатывают вопрос о внедрении DLP в свою ИТ-инфраструктуру. Были проведены первые тестовые, так называемые «пилотные» проекты. В частности, компанией IT-Team Service, являющейся зарегистрированным партнером компании Symantec, были проведены несколько пилотных проектов с использованием решения Symantec Data Loss Prevention 11.

В то же время, несмотря на явно возросший интерес к данной проблеме, многие руководители, интересующиеся этим вопросом, не делают дальнейших шагов по приобретению и внедрению DLP, хотя необходимость в этом для них очевидна. Это связано со множеством факторов организационного, финансового и технического характера. В данной статье я постараюсь осветить подобные факторы, рассказать о проблемах, возникающих при внедрении DLP, раскрыть суть пилотного проекта DLP и, насколько это возможно, помочь выбрать правильное направление в защите конфиденциальной информации.

С чего начать?

Для начала стоит определиться, действительно ли вашей организации нужна система DLP и готовы ли вы к ее внедрению? Здесь неприменим подход «сначала купим, потом разберемся». Прежде чем прорабатывать вопрос о приобретении и внедрении какого-либо решения DLP, и даже до проведения пилотного проекта DLP, необходимо тщательно, всесторонне все обдумать. Как минимум, можно ответить на несколько простых, однако далеко не для всех руководителей очевидных вопросов:

- ***Имеется ли в организации конфиденциальная информация, подлежащая защите?*** *Понятно, что если такая информация отсутствует, то и системы DLP не нужны. Вариант «покупка на перспективу» не рассматриваем, как несерьезный.*

- ***Проведена ли в организации классификация информации?*** *В упрощенном варианте классификация информации подразумевает категорирование имеющихся информационных активов в зависимости от степени ущерба от их утечки (например, конфиденциальная, для служебного пользования, публичная и т. п.), а также определение владельцев информации. Применение в организации классификации информации может значительно облегчить внедрение системы DLP и повысить ее эффективность.*
- ***Разработана ли в организации концепция информационной безопасности?*** *Поскольку данный документ является основополагающим документом по информационной безопасности, отражающим отношение организации к обеспечению своей безопасности и определяющим, в частности, что именно необходимо защищать и каким образом, его наличие также является важным фактором для достижения успеха в защите конфиденциальной информации.*
- ***Какова вероятность утечки конфиденциальной информации?*** *При наличии технических каналов передачи данных, а таковые на сегодняшний день имеются практически в любой организации, и при отсутствии должного административно-технического контроля, вероятность утечки всегда будет высокой.*
- ***Каков возможный ущерб?*** *Утечка конфиденциальных данных может нанести организации как прямой (финансовый), так и косвенный (репутационный) ущерб, причем последний в конечном итоге так или иначе тоже приведет к финансовым потерям, хотя их и невозможно будет точно подсчитать. В мировой практике считается, что если сумма возможного ущерба сопоставима со стоимостью выбранного решения DLP, то внедрение имеет смысл.*
- ***Готово ли руководство организации к жестким мерам для предотвращения утечек данных и в случае обнаружения таковых?*** *Нельзя создавать прецеденты, когда пойманный за руку нарушитель (инсайдер), «сливающий» конфиденциальную информацию, останется безнаказанным (административно, в финансовом отношении, в судебном порядке и т. п.) — это лишит использование DLP всякого смысла. Кроме того, нужно учитывать и быть готовым к возможному недовольству пользователей, которых внедрение DLP и сопутствующее ужесточение политики информационной безопасности может лишить привычного рабочего окружения (веб-почты, интернет-пейджеров, альтернативных браузеров) или повлиять на привычный процесс работы.*

Необходимо учитывать морально-этический аспект внедрения DLP. При работе системы DLP в поле зрения сотрудников, ответственных за работу системы (администраторы, владельцы информации, координаторы), неизбежно попадает информация личного, интимного характера, причем зачастую нелицеприятная. Поэтому нужно подбирать ответственных лиц с такими моральными качествами, чтобы они, с одной стороны, считали для себя возможным читать чужую переписку полностью, поскольку это делается в служебных целях, а с другой стороны, не допускали дальнейшего распространения информации личного характера. Иными словами, сплетникам в команде DLP не место. Это очень важно хотя бы с точки зрения сохранения здоровой атмосферы в коллективе.

Кстати, я не зря упомянул термин «команда DLP». Нужно четко осознать, что эффективная работа системы DLP не может поддерживаться только одним человеком. К сожалению, многие руководители совершают грубую ошибку, возлагая задачи по администрированию системы DLP на системного администратора или сотрудника информационной безопасности. Проблема в том, что ни тот, ни другой не в состоянии самостоятельно определять, какую именно информацию нужно защищать в данный момент времени и, соответственно, не способен поддерживать политики, на основании которых работает система DLP, в актуальном состоянии. Здесь мы сталкиваемся с известной проблемой: сотрудники службы ИТ или ИБ не знают, что конкретно защищать, а владельцы данных не знают как. Именно поэтому важно создать специальную команду, в которую бы входили представители обеих сторон и некое координирующее лицо, обладающее соответствующими полномочиями.

Все перечисленное выше является просто набором рекомендаций, выработанных на основе практического опыта нашей компании, опыта специалистов компаний-производителей решений DLP и мнений независимых экспертов. Чисто технически ничто не мешает просто купить и внедрить выбранное решение DLP, без проведения подготовительных мероприятий и учета данных рекомендаций, однако эффективность системы, введенной в эксплуатацию таким образом, наверняка будет невысокой.

Пилотный проект

Пилотный проект в значительной мере облегчает выбор конкретного решения DLP. В рамках пилотного проекта организация может бесплатно проверить работу системы DLP в реальных условиях своей ИТ-инфраструктуры. По согласованию с компанией-производителем можно развернуть как весь комплекс решения, так и отдельные его модули. Поскольку компания IT-Team Service является партнером компании Symantec, дальнейшее описание хода пилотного проекта я буду давать, опираясь на опыт работы с решением Symantec Data Loss Prevention 11, однако значительная часть сказанного будет справедлива и для решений других компаний.

Symantec Data Loss Prevention 11 — это комплексное решение, предназначенное для контроля содержимого перемещаемых или хранимых данных на периметре сети (модули Network Monitor и Network Prevent) и конечных точках (модули Endpoint Discover и Endpoint Prevent) или в хранилищах данных (Network Discover, Network Protect Data Insight). Централизованное управление всеми модулями решения, развертывание универсальных политик общекорпоративного уровня, а также хранение обрабатываемых данных и формирование отчетов о работе системы обеспечивается платформой Enforce и базой данных Oracle.

Перед запуском пилотного проекта в первую очередь необходимо определить цели и задачи проекта. Это ключевой момент, поскольку без ясно обозначенных целей и четко поставленных задач по завершении проекта невозможно сделать обоснованные выводы о его результатах и максимум, что руководитель сможет увидеть в итоговом отчете — интуитивные оценки администратора системы из разряда «понравилось/не понравилось». Согласитесь, что оценки такого рода не удовлетворят руководителя, поскольку их недостаточно для принятия ответственного решения.

После определения целей и задач проекта необходимо уточнить его рам-

ки, а также выбрать технические каналы утечки данных, которые организация хочет контролировать. Определение количества пользователей, рабочих станций, файловых и почтовых серверов, каналов выхода в Интернет, участвующих в проекте, поможет выбрать нужные модули, входящие в состав тестируемого решения. Например, если в организации отсутствуют файловые сервера, базы данных, системы электронного документооборота, в которых может храниться конфиденциальная информация, то отпадает необходимость в модулях, обеспечивающих контроль хранилищ данных, что значительно сократит время, потраченное на реализацию проекта и его сложность.

Далее формируется команда пилотного проекта, в которую, как правило, входят представители IT-Team Service и сотрудники организации. Исходя из определенных ранее рамок проекта, подготавливается техническая среда, необходимая для развертывания выбранных модулей. Решение Symantec Data Loss Prevention 11 поддерживает работу своих модулей в виртуальной среде, что может значительно облегчить их развертывание и администрирование.

После запуска проекта сотрудники IT-Team Service фиксируют данные об организации в компании Symantec и запрашивают временную лицензию. После получения временной лицензии сотрудники IT-Team Service разворачивают в технической среде организации необходимое программное обеспечение, в частности, платформу Enforce и базу данных Oracle. Наш опыт в проведении пилотных проектов показывает, что с целью минимизации воздействия на существующую ИТ-инфраструктуру и бизнес-процессы организации, заказчики, как правило, предпочитают только контролировать конфиденциальную информацию, но не блокировать ее передачу. Поэтому чаще всего в ходе пилотного проекта используются следующие компоненты Symantec Data Loss Prevention 11:

- ***Network Monitor.*** *Копия сетевого трафика из нужных сегментов сети собирается для обработки специальными устройствами TAP либо с помощью портов SPAN (Mirror) на сетевом оборудовании.*
- ***Network Discover.*** *Для подключения к хранилищам данных у представителей организации запрашиваются соответствующие учетные данные.*
- ***Endpoint Discover и Endpoint Prevent.*** *Сбор данных ведется с помощью программных агентов на конечных точках. В случае отсутствия сетевого подключения к серверу Endpoint, агент продолжает собирать информацию и передает ее при восстановлении подключения.*

К моменту завершения развертывания программного обеспечения сотрудники организации должны подготовить стартовую базу информации, которая будет считаться конфиденциальной в рамках пилотного проекта. Это могут быть ключевые слова и фразы, регулярные выражения, образцы документов и т. д. На базе этих данных формируются и применяются политики поиска конфиденциальной информации и реагирования на инциденты. С сотрудниками IT-Team Service могут быть подписаны договора о неразглашении либо они могут быть отстранены от дальнейшей корректировки политик и обработки инцидентов.

По завершении проекта подготавливается отчет о ходе проекта и подводятся его итоги. В случае, если организация рассматривает решения от нескольких производителей, имеет смысл подготовить сравнительный анализ, с помощью которого можно будет сделать окончательный выбор.

Сравнительный анализ

При проведении сравнительного анализа нескольких систем DLP следует учитывать функционал, предлагаемый конкретной системой, ее системные требования, отзывы независимых исследовательских компаний и, разумеется, стоимость системы.

Простейший сравнительный анализ функциональных возможностей можно подготовить в виде таблицы, в которой каждой из рассматриваемых систем начисляется один балл за реализацию того или иного функционала. В итоге функционал систем сравнивается по количеству набранных баллов. Можно применить дифференцированный подход, когда в зависимости от степени важности для организации конкретного функционала или исходя из уровня его реализации начисляется разное количество баллов. Я приведу в качестве примера упрощенный сравнительный анализ трех систем, предлагаемых на рынке DLP Узбекистана (InfoWatch Traffic Monitor Enterprise, Дозор-Джет и Symantec Data Loss Prevention 11.1), который мне довелось проводить в рамках одного из пилотных проектов. Хочу подчеркнуть, что данный анализ ни в коем случае не претендует на полную достоверность и не является попыткой представить в выгодном свете решение от компании Symantec, предлагаемое IT-Team Service. В то же время информация о функциональных возможностях конкурирующих решений была получена из материалов, опубликованных на сайтах производителей, поэтому сравнение можно считать достаточно объективным. Список рассматриваемых функциональных возможностей, разумеется, не универсален и может быть расширен или сокращен в зависимости от требований конкретной организации (возможно, полностью запрещены интернет-пейджеры или отсутствуют файловые хранилища).

При оценке функциональных возможностей стоит обязательно проконсультироваться с техническими специалистами компаний, предлагающих решения DLP, поскольку менеджеры по продажам, как правило, либо не владеют всей технической информацией, либо умалчивают об особенностях реализации того или иного функционала, экономя время, отведенное на презентацию системы. Например, контроль и блокировка передачи данных по протоколам HTTP, HTTPS и FTP на периметре сети зачастую производится за счет интеграции с прокси-серверами организации, причем список поддерживаемых прокси-серверов очень ограничен, однако на презентациях об этом обычно не говорится.

Не стоит обращать особого внимания на список поддерживаемых конкретным решением интернет-пейджеров. Во-первых, организации, всерьез обеспокоенные проблемой DLP, в рамках ужесточения политики информационной безопасности и сокращения количества технических каналов утечки данных, зачастую вообще отказываются от интернет-пейджеров, если их использование не является жизненно необходимым для бизнес-процессов. Во-вторых, собственно утечка данных через интернет-пейджеры, как правило, представляет собой передачу файла или использование буфера обмена операционной системы для отправки текста в режиме чата (сомнительно, что инсайдер будет набирать вручную либо диктовать по Skype текст исходного кода программы или финансового отчета). Такие утечки многими решениями DLP контролируются за счет мониторинга обращений к файловой системе и буфера обмена, не-

Сравнительный анализ систем DLP

	InfoWatch Traffic Monitor Enterprise	Дозор-Джет	Symantec Data Loss Prevention 11.1
Технологии			
Ключевые слова и регулярные выражения	1	1	1
Лингвистический анализ	1	1	0
Анализ транслита	1	0	0
Цифровые отпечатки документов	1	1	1
Самообучающаяся система анализа данных (искусственный интеллект)	0	0	1
Оптическое распознавание текста (OCR)	1	0	0
Защита периметра			
Анализ HTTP	1	1	1
Анализ SMTP	1	1	1
Анализ HTTPS	1	1	1
Анализ FTP	0	1	1
Модификация SMTP-сообщений	0	1	1
Интернет-пейджеры и VoIP			
ICQ (OSCAR)	1	1	0
Mail.ru Agent	1	1	0
Skype	1	1	0
Windows Live Messenger	0	1	1
Yahoo! Messenger	0	0	1
Google Talk	0	1	0
Jabber	0	1	0
Хранилища данных			
Поиск и защита конфиденциальных данных в файловых хранилищах, базах данных, системах документооборота, на веб-сайтах	0	0	1
Аудит использования конфиденциальных данных	0	0	1
Определение владельца конфиденциальных данных	0	0	1
Защита рабочих станций			
Анализ HTTP	0	0	1
Анализ SMTP	0	0	1
Анализ HTTPS	0	0	1
Анализ FTP	0	0	1
Жесткие диски	1	1	1
Съемные носители (USB, CD, DVD и т.д.)	1	1	1
Печать на принтеры	1	1	1
Буфер обмена	0	0	1
Сетевые ресурсы (сетевые папки)	0	0	1
Сбор и последующая передача данных при отсутствии коммуникаций агента с сервером управления	0	0	1
Итого:	**14**	**17**	**23**

зависимо от используемого интернет-пейджера и его версии.

Технические требования достаточно высоки у всех решений DLP. В особенности это касается решения Symantec Data Loss Prevention 11, требующего значительных объемов оперативной памяти и дискового пространства. Здесь организации могут помочь технологии виртуализации, позволяющие эффективно использовать имеющееся серверное оборудование и системы хранения данных. Кроме того, некоторые вендоры выпускают свои продукты в виде аппаратных устройств, что упрощает их развертывание.

Многими вендорами применяется гибкая ценовая политика, учитывающая, например, количество пользователей в организации или форму собственности, поэтому при определении ориентировочной стоимости конкретного решения нужно обязательно проконсультироваться с менеджерами по продажам.

Если организация не может сделать окончательный выбор между несколькими решениями, примерно равными по стоимости и предлагаемому функционалу, есть смысл обратиться к мнениям международных независимых исследовательских компаний. В частности, можно изучить отчет «Magic Quadrant for Content-Aware Data Loss Prevention» от Gartner. Не менее интересным является отчет «The Forrester Wave: Data Leak Prevention Suites» от компании Forrester Research. В графическом виде представлены сводные результаты из этих отчетов.

Скрытое или публичное внедрение?

Важным фактором при внедрении системы DLP является определение метода внедрения. Внедрение системы DLP может быть как скрытым, так и публичным. У обоих методов есть свои преимущества и недостатки.

При скрытом внедрении возрастает вероятность поймать инсайдера за счет неосторожности последнего и его уверенности в своей безнаказанности. Большинство пилотных проектов также проводится скрытно с целью демонстрации максимального эффекта. Недостатком скрытного внедрения является невозможность использования полного функционала системы. Например, придется отказаться от функции блокирования передачи конфиденциальных данных, поскольку при первой же блокировке сотрудникам станет известно об использовании системы.

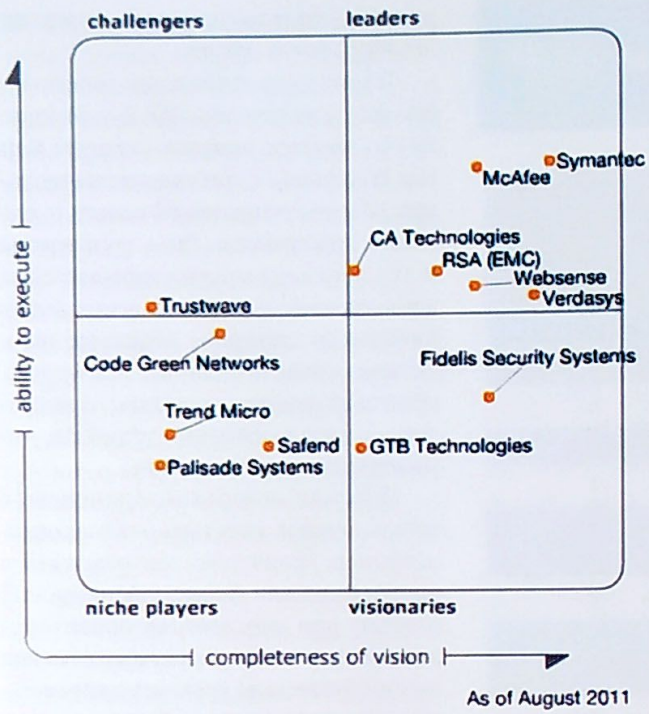

Рисунок 1. Magic Quadrant for Content-Aware Data Loss Prevention (Gartner)

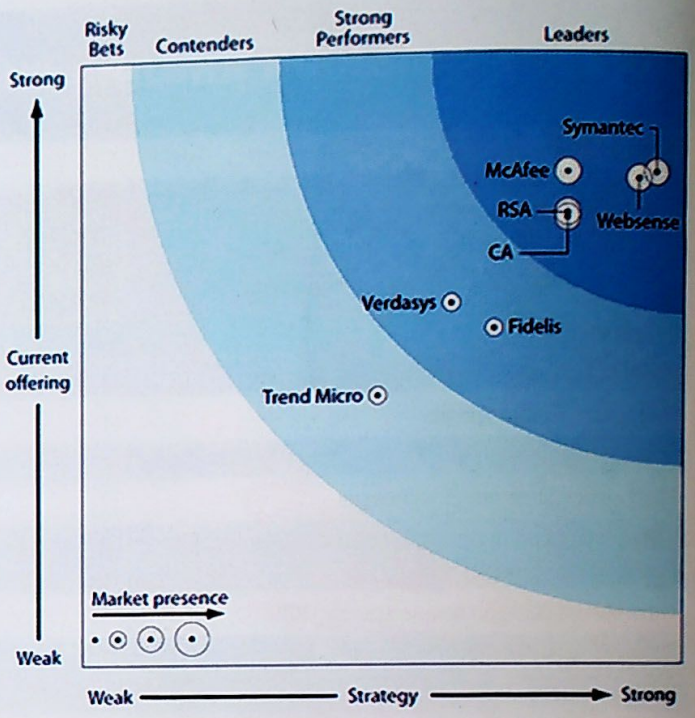

Рисунок 2. Forrester Data Leak Prevention Suites, Q4 2010 (Forrester)

Публичное внедрение может положительно сказаться на имидже организации. Кроме того, осознание того, что их действия контролируются, может повысить дисциплину сотрудников и снизить вероятность случайной утечки данных. Однако поймать инсайдера станет сложнее, поскольку он наверняка будет искать другие пути передачи данных за пределы организации.

Что нужно иметь ввиду?

Чтобы не сделать ошибку при выборе решения DLP и остаться довольным этим выбором, нужно учесть следующее:

- ***Необходимо правильно понимать назначение систем DLP.*** *Эти системы не решат проблему утечки данных, а позволят лишь, при правильном использовании, снизить риски утечки.*
- ***Системы DLP не относятся к классу «поставил и забыл».*** *Предотвращение утечек конфиденциальных данных — это непрерывный процесс, требующий постоянного вмешательства со стороны владельцев данных и администраторов системы.*
- ***Ни одна система DLP не способна перекрыть все существующие технические каналы передачи данных.*** *Нужно выбрать систему, способную контролировать наибольшее количество каналов по основным направлениям защиты (периметр сети, хранилища данных и конечные точки), и, по возможности, отказаться от использования каналов, оставшихся без контроля.*
- ***Решения DLP, как правило, стоят дорого.*** *Дешевые решения, скорее всего, предлагают ограниченный функционал.*
- ***Нехватка опыта или ресурсов неизбежно скажется на результате.*** *Решения DLP в большинстве своем достаточно сложны в развертывании и эксплуатации и требуют значительных временных затрат. Не стоит экономить на технической поддержке и сопровождении, поскольку, переоценив свои силы, организация рискует остаться один на один с возникшими проблемами.*

Заключение

Рынок DLP в Узбекистане только начинает развиваться. Исходя из активности в этом направлении наших коммерческих банков и других организаций, а также учитывая повышенный интерес со стороны производителей систем DLP, можно ожидать первых внедрений уже в текущем году. Этому могут помешать лишь ограничения бюджета, выделяемого службам ИТ и ИБ. Кроме того, может отрицательно сказаться отсутствие технических специалистов у некоторых локальных партнеров компаний, производящих системы DLP, — в таких случаях приходится вызывать специалистов из других стран (Россия, Украина, Казахстан), что усложняет согласование проекта, занимает много времени и может отразиться на конечной стоимости внедрения.

При создании статьи были использованы следующие источники информации:

- *Материалы 4-й Международной конференции DLP-Russia 2011 по вопросам защиты конфиденциальных данных от утечки и контроля информационных потоков (**www.dlprussia.ru**)*
- *Материалы Zecurion DLP Forum 2011 (**www.dlpforum.ru**)*
- *Magic Quadrant for Content-Aware Data Loss Prevention, August 2011 (**www.gartner.com**)*
- *The Forrester Wave: Data Leak Prevention Suites, Q4 2010 (**www.forrester.com**)*
- *Сайт компании InfoWatch (**www.infowatch.ru**)*
- *Сайт решения Дозор-Джет (**www.dozor-jet.ru**)*
- *Сайт компании Symantec (**www.symantec.com**)*