Руководство медиаимперии News Corp. провело презентацию The Daily, первой газеты новостей, предназначенной специально для отображения на планшетном компьютере iPad. В Apple к выпуску The Daily приурочили ввод в действие системы оплаты по подписке. Стр. 4

Международный компьютерный еженедельник

computerworld россия

www.computerworld.ru №03 (724), 32 страницы 08/02/2011

Atom на перепутье

Нынешний год будет непростым для процессорного семейства Intel Atom, поскольку рынок нетбуков сейчас переживает не лучшие времена, а проникновение на новые рынки сопряжено с немалыми сложностями. Стр. 10

Под угрозой кибертерроризма

Угрожает ли России кибертерроризм? Ответить на этот вопрос попытались участники круглого стола, организованного Symantec совместно с Фондом содействия научным исследованиям проблем безопасности «Наука-XXI». Стр. 26

Попробуй Exadata

Компания «Инфосистемы Джет» и российское представительство корпорации Oracle объявили 21 января о вводе в действие демонстрационного центра на основе машины баз данных Oracle Exadata Database Machine. Стр. 12

Почему в HP меняют директоров?

В совете директоров Hewlett-Packard произошли перестановки. Руководящий орган компании пополнился технологическими экспертами и ветеранами бизнеса. Таким образом в HP пытаются дистанцироваться от прошлых скандалов. Стр. 11

От двух до пяти в Глобальной сети

Дети приобретают навыки владения компьютером раньше, чем обучаются более традиционным умениям, таким как катание на велосипеде и плавание, — об этом говорят результаты опроса, проведенного компанией AVG. Стр. 25

Где живут данные

С 2000 года девизом корпорации EMC стала образная фраза Where Information Lives. Действительно, потребительную стоимость имеет информация, а не данные, но физическим носителем информации являются данные, вот они-то и «живут» в системах хранения, которым была посвящена серия мероприятий корпорации EMC, прошедших под общим названием Record Breakers Event. Масштабное представление обновленных и абсолютно новых продуктов, осуществленное в январе последовательно, с интервалом в один день, в Нью-Йорке, Лондоне и Сингапуре, вполне заслуженно назвали «мегазапуском». Технологическим мероприятиям сопутствовали маркетинговые, в частности — помпезное установление четырех рекордов для Книги Гиннесса, в том числе прыжок на мотоцикле через стоящие в ряд накопители Symmetrix. Стр. 6

ISSN 15605213

9 771560 521007 11003>

Не упусти свои данные

Конфиденциальные данные нередко являются наиболее ценными активами предприятия, и их утечка может привести к ухудшению рыночного положения компании. В некоторых случаях утечки персональных данных могут повредить не самим компаниям, а их клиентам, что также отрицательно сказывается на репутации

ВАЛЕРИЙ КОРЖОВ
Computerworld Россия

Чтобы не допустить подобных инцидентов, компаниям приходится использовать специальные технические и организационные меры по защите от утечки данных (Data Leakage Protection, DLP).

«О каких бы утечках мы ни говорили, — отмечает Владимир Бычек, руководитель направления контент-безопасности компании «Аладдин Р.Д.», — выбору специального программного средства должна предшествовать очень серьезная работа по классифицированию информации, обрабатываемой и хранимой в компании, анализу информационных потоков и т. д.». Организация должна самостоятельно определить, какие именно данные являются конфиденциальными, где они хранятся и кто может получить к ним доступ. Только после этого можно приступать к их защите.

Модель угроз

Любая информация в любой информационной системе должна храниться, передаваться и обрабатываться. На каждом из этих этапов данные могут быть украдены, поэтому нужно предусмотреть соответствующие средства защиты. Собственно, с хранением и передачей все более или менее ясно — в этих двух случаях наиболее надежным способом защиты является шифрование. Поэтому стандартные средства шифрования дисков, баз данных и каналов связи ограждают компании от этого типа угроз.

Утечки данных при обработке в приложениях должны предотвращать системы контроля доступа, которые встроены в любое приложение, базу данных или операционную систему. Дыры систем контроля доступа можно закрыть с помощью программ для контроля периферийных устройств. Александр Ковалев, директор по маркетингу SecurIT, отмечает следующее: «Если говорить о традиционном видении DLP, то большая часть компаний пока ограничивается лишь защитой от утечек через подключаемые накопители и принтеры. Спрос на DLP, контролирующие электронную почту, вебсервисы, интернет-пейджеры, торренты и другие сетевые каналы утечки, пока существенно меньше, но он довольно уверенно растет».

Впрочем, не исключена также возможность, что в самой программе может быть встроена закладка, с помощью которой посторонние могут получить доступ к секретным данным. Именно поэтому закон «О персональных данных» (ФЗ-152) содержит требования по сертификации системы контроля от несанкционированного доступа и на отсутствие недекларированных возможностей. Требования по шифрованию данных и каналов связи также содержатся в документах, связанных с ФЗ-152. Там же есть требования по установке межсетевых экранов, антивирусного ПО, систем обнаружения вторжений и даже систем предотвращения утечек информации с помощью побочного электромагнитного излучения. Дмитрий Курашев, директор компании Entensys, отмечает: «В нашей стране люди зачастую не делают что-то правильное только потому, что это разумно. Очень важно наличие «кнута» в виде закона или чего-то подобного. Раньше надлежащим образом задумывались о безопасности персональных данных лишь особые организации, такие как силовые структуры, банки и т. д. Сейчас круг заинтересованных лиц резко расширяется». При этом требования закона покрывают практически все возможные пути утечки конфиденциальной информации из систем, которые их обрабатывают.

ПРОДУКТЫ ДЛЯ ПРЕДОТВРАЩЕНИЯ утечек становятся все более популярными в России

Следует отметить, что перечисленные в законе меры защищают только от внешних злоумышленников, которые пытаются получить доступ к данным, не имея на это полномочий. В то же время они практически не могут защитить от тех сотрудников, которые на законном основании имеют доступ к конфиденциальным данным. В этом случае и шифрование, и системы контроля доступа, и все другие защитные механизмы не становятся препятствием для доступа к информации. В то же время сам сотрудник в некоторых случаях может случайно или сознательно передать конфиденциальную информацию вовне. Для обнаружения и предотвращения подобных инцидентов разработаны специальные механизмы защиты, которые практически не рассматриваются в ФЗ-152. Поэтому вполне возможно, что системы защиты, которые полностью соответствуют требованиям закона «О персональных данных», могут допустить утечку секретной информации.

Для решения подобных проблем создан специальный класс продуктов, которые контролируют передачу данных за пределы компании. Если в этом потоке обнаружатся конфиденциальные данные, то их передача будет заблокирована. Андрей Митрофанов, менеджер компании SafeLine, так сформулировал основные цели работы подобных решений: «Современные программные и программно-аппаратные средства позволяют анализировать сетевую активность пользователей и оперативно реагировать на несанкционированные попытки передачи данных за периметр предприятия. Варианты реакций на такие действия гибко настраиваются в соответствии с принятыми политиками безопасности: от 'беспрепятственно пропустить' до 'заблокировать соединение и отправить оповещение службе безопасности'».

Правда, фильтрация происходит только в том случае, если данные передаются по открытым протоколам: с помощью почты, FTP, Web, IM и др. Именно такие продукты принято называть средствами предотвращения утечек (Data Leak Prevention). Современное состояние рынка DLP-решений в России описал Рустэм Хайретдинов, заместитель генерального директора InfoWatch: «Как и весь российский рынок информационной безопасности, рынок продуктов DLP начал догонять отложенный за 2009 год спрос, поэтому объемы продаж в 2010 году существенно увеличились. Несмотря на то что о наличии DLP-функционала стали заявлять практически все производители средств информационной безопасности, лидеры российского DLP-рынка не изменились. Тема модная, все пытаются к ней прислониться».

Следует отметить, что классические DLP в основном защищают от случайных утечек, поскольку профессиональные шпионы вряд ли бу-

дут пользоваться открытыми каналами передачи информации. Люди, проникшие в компанию с целью получить доступ к секретным сведениям и передать их «наружу», скорее всего будут пользоваться для этого скрытыми каналами, которые предлагает стеганография, шифрование или необычные протоколы связи. В любом случае для создания закрытых каналов передачи данных злоумышленники используют специальное программное обеспечение. Борьба с ним аналогична работе антивирусов, которые выявляют действия по созданию скрытых каналов передачи данных за пределы организации. Это направление принято называть защитой от утечек посредством вредоносных программ (Malware Data Leak Prevention, MDLP).

Классические DLP

Изначально средства DLP не предотвращали утечки, а только их фиксировали, но с совершенствованием технологий были разработаны и методы блокирования утечек. Тем не менее некоторые системы до сих пор занимаются только фиксацией факта передачи конфиденциальной информации — это нужно учитывать при построении систем защиты. Предотвращение утечек возможно с помощью контроля действий пользователей при работе с данными на локальном компьютере или оперативном выявлении конфиденциальных данных в потоке, который проходит через шлюз. Для реализации этих технологий были разработаны методы обнаружения конфиденциальной информации с помощью отпечатков, которые позволили ускорить процесс сравнения настолько, что оказалось возможным вырезать данные в реальном времени. Впрочем, системы противодействия утечкам могут предупреждать пользователя о нарушении политики обращения с конфиденциальной информацией уже при попытке отослать сообщение или скопировать данные в буфер обмена.

В результате современная система DLP может содержать не только модули, которые контролируют каналы передачи данных, но также компоненты, устанавливаемые на клиентские и серверные машины и следящие за работой систем контроля доступа в применении к конфиденциальной информации. Фактически такие системы уже выполняют функции не просто предотвращения утечек информации, а мониторинга за соблюдением правил корпоративной политики безопасности.

MDLP

Защита от утечек с помощью специализированных программ аналогична работе антивирусных средств с поиском программ-невидимок и другой вредоносной активности. Они могут узнавать программы для создания тайных каналов по сигнатурам или по попыткам получить доступ к конфиденциальным данным. Такие средства обнаружения хорошо встраиваются в концепцию современных антивирусных систем защиты класса Internet Security. В них уже есть встроенная система контроля за приложениями, которая получила название HIPS. Как только какая-нибудь программа пытается выполнить подозрительную последовательность действий, защита поднимает тревогу и начинает блокировать системные вызовы приложения.

Следует отметить, что современные антивирусы в большинстве своем уже находят троянцев и червей, которые создают тайные каналы для отправки информации, и удаляют их, то есть фактически выполняют роль MDLP, однако пока в них нет систем проактивной защиты, которые позволяли бы обнаружить и блокировать попытки доступа к конфиденциальным данным для неизвестных программ.

«Средний бизнес пока не готов вкладывать в полноценные DLP-решения, — отмечает Алексей Демин, управляющий продажами в корпоративном секторе G Data Software. — Для них более приемлемым является решение с функциями DLP. Отсюда и появление модулей DLP в программных продуктах, которых раньше на рынке не было. Например, как составная часть корпоративных антивирусных решений модули защиты от утечки информации уже никого не удивляют».

Об аналогичных разработках рассказал и Сергей Голованов, эксперт «Лаборатории Касперского». Его компания ведет разработки технологии, которая базируется на уже используемой в Kaspersky Internet Security системе HIPS и будет блокировать неправомочный доступ к конфиденциальным данным. Подобные технологии есть также у McAfee, Trend Micro и других производителей антивирусов.

Николай Романов, ведущий технический консультант Trend Micro в России и СНГ, отметил следующую тенденцию развития современных DLP-систем: большинство продуктов используют цифровые отпечатки для выявления конфиденциальной информации и построены по гибридному принципу, то есть включают шлюзовые фильтры, агенты на клиентских машинах, блокирование периферийных устройств и шифрование конфиденциальной информации. Все перечисленные механизмы защиты в комплексе могут обеспечить приемлемый уровень безопасности конфиденциальных данных. Дмитрий Михеев, эксперт центра информационной безопасности компании «Инфосистемы Джет», прогнозирует: «В ближайшее время ожидается выход новых версий продуктов, и, скорее всего, в них будет отражена реакция на существующие потребности и запросы российских пользователей. Кроме того, они будут осуществлять поддержку характерных для местных компаний данных».

Панацеи нет

Стопроцентной защиты от утечек не разработал еще ни один производитель. Проблемы с использованием DLP-продуктов Хайретдинов сформулировал так: «Для того чтобы эффективно использовать многолетний опыт борьбы с утечками, реализованный в программном обеспечении DLP-систем, компаниям придется принять, что существенная часть работы по обеспечению защиты от утечек должна быть сделана на стороне заказчика, поскольку никто лучше него не знает его собственных информационных потоков».

Демин также считает, что гарантированно защититься от утечек нельзя: «Надо понимать, что предотвратить утечку информации невозможно. Если информация имеет для кого-нибудь ценность, рано или поздно она будет получена. Программные средства могут сделать процесс получения этой информации более дорогостоящим и требующим больших временных затрат, что может значительно снизить выгоду обладания информацией, а также ее актуальность». Поэтому и эффективность работы DLP-систем стоит контролировать.

Если утечка все-таки произошла, то секретные данные с большой вероятностью появятся в Интернете в виде предложений об их продаже либо в виде общедоступной базы данных или сообщений в СМИ. Чтобы реагировать на подобные инциденты, надо постоянно сканировать Интернет для поиска собственных конфиденциальных сведений. В России есть несколько компаний, которые предлагают услуги по поиску и даже мониторингу конфиденциальных данных клиентов в открытых источниках. Покупка подобных услуг позволит компании вовремя заметить утечку и минимизировать ущерб от подобных действий злоумышленников с помощью оперативного юридического вмешательства или незамедлительно проведенной PR-кампании. Организациям нужно не только обеспечить техническую защиту собственно данных, но и попытаться минимизировать ущерб от произошедшей утечки.

Защита путем сравнения

Ключевым элементом технологии DLP является механизм поиска конфиденциальной информации. Традиционно при инсталляции DLP компания должна указать системе, какая информация собственно является конфиденциальной. Это можно сделать с помощью определения регулярных выражений, слов или словосочетаний, которые служат признаком секретной информации, например метки «Конфиденциально» или «Для служебного пользования», помещенной в документ. Развитием этого метода являются лингвистические методы анализа, настройку которых можно автоматизировать с помощью специального программного обеспечения.

Есть также метод определения уровня конфиденциальности информации с помощью специальных пометок в файле. При создании нового файла пользователь должен определить его уровень секретности, а при копировании данных из одного файла в другой уровень секретности также копируется. Как только система контроля утечек замечает, что из компании передается файл с меткой высокого уровня секретности, такая передача блокируется. Правда, подобный метод контроля утечек может быть реализован только с помощью специального агентского ПО, которое контролирует целостность меток секретности при работе с данными. Такие решения есть, но они постепенно уступают место технологии отпечатков.

Так называемый метод отпечатков становится сейчас наиболее популярной технологией защиты конфиденциальности данных. Он обрабатывает файлы с конфиденциальными данными и с помощью специальной хеш-функции генерирует их отпечатки. Поток контролируемой информации также хешируется с помощью той же функции и сравнивается с базой отпечатков. Если они похожи, то и передаваемые похитителем файлы могут содержать фрагменты конфиденциальной информации. Для работы этого метода хеш-функция должна, с одной стороны, работать быстро, а с другой — быть не очень чувствительной к добавлению шумовой информации и простых преобразований данных. Сейчас практически все DLP-решения используют отпечатки, хотя могут включать и другие технологии определения конфиденциальности данных.