http://www.lanmag.ru ФЕВРАЛЬ 2010

ЖУРНАЛ СЕТЕВЫХ РЕШЕНИЙ LAN

ЗАЩИТА

ОТ УТЕЧКИ ДАННЫХ

> СГБП для небольшого ЦОД

> Виртуализация на всех уровнях

> Как защитить базу данных

ISSN 1027086-8
10002
9 771027 086001

Перспективные технологии защиты от внутренних угроз

Ценность информации повышается, а вместе с ней – и средний ущерб предприятия при утечке конфиденциальных данных. Поэтому системы защиты от таких утечек пользуются стабильным спросом, что, в свою очередь, стимулирует новые исследования в этой области.

Николай Федотов

Современный уровень развития технологий предотвращения внутренних угроз, в частности, систем защиты от утечек конфиденциальной информации (Data Leackage Prevention, DLP) не может полностью удовлетворить потребности компаний в обеспечении безопасности данных. Новые каналы передачи, через которые могут происходить утечки, появляются быстрее, чем для них разрабатываются модули контроля. Неизвестные ранее способы злоупотреблений не находят своевременного отражения в политиках безопасности и стандартах.

К тому же не все системы DLP справляются с обработкой больших объемов данных. Так, с технической точки зрения нет никаких препятствий для хранения всего переданного трафика, но услуга по индексации огромного массива данных и запуску в нем инструментов поиска и аналитики все еще оказывается достаточно дорогой для заказчиков. Однако главным камнем преткновения всех технических средств защиты информации является то обстоятельство, что человек как элемент информационной системы остается плохо предсказуемым и трудно контролируемым, причем полностью исключить его из процесса обработки информации вряд ли возможно даже теоретически.

Все вышеперечисленные трудности, с которыми сталкиваются разработчики систем защиты от внутренних угроз, в том числе и систем DLP, способствуют развитию новых технологий в данной области. Так, по прогнозам исследовательской компании IDC, в ближайшие годы рынок защиты данных от утечки ждет стабильный рост на 30–40% ежегодно. Какие же технические новинки можно ожидать в недалеком будущем?

РАСПОЗНАВАНИЕ СМЫСЛА

Даже у современных систем DLP имеются развитые средства лингвистического анализа, то есть детектирование происходит не просто по маске, а с учетом форм слова, синонимов, опечаток и т. д. Впрочем, далеко не все существующие системы DLP оснащены эффективным лингвистическим анализом.

DLP весьма скоро станут выполнять поиск фрагментов, близких к образцу не только по форме, но и по смыслу. Кроме того, ожидается, что они смогут находить сходные с образцом изображения и мультимедийные объекты. В общем, поставщикам соответствующих систем еще есть над чем работать.

К примеру, при заданном поисковом образце «падение цены акции» хорошая система DLP найдет не только фразу «цена падает» (те же слова в иных формах), но также и фрагмент «игра на понижение курса» (иные слова) или даже «тактика медведя» (идиома).

ПРИНУДИТЕЛЬНОЕ ШИФРОВАНИЕ

Шифрование предохраняет от утечки данных в случае утери или кражи носителя информации. Однако зачастую сотрудники игнорируют это действенное средство защиты данных: в офисах повсеместно практикуется использование личных USB-устройств для копирования на них, скажем, содержимого рабочего каталога. При этом не организуется криптоконтейнер и не создается шифрованный архив, поскольку персонал предпочитает избегать малейшей дополнительной работы.

Решение вчерашнего дня состоит в удалении или опечатывании соответствующего разъема либо в его программной блокировке. Решение сегодняшнее заключается в отслеживании при помощи системы DLP всей информации, записываемой на внешний накопитель, причем процесс будет прерван, если система выявит факт записи конфиденциальной информации. Этот метод значительно эффективнее прямолинейного запрета.

Перспективным направлением представляется не только отслеживание, но и автоматическое шифрование всего содержимого внешнего носителя (или только конфиденциальных файлов), что избавляет как от хлопот по созданию криптоконтейнера, так и от соблазна вообще отказаться от шифрования. В принципе, можно пойти дальше и шифровать содержимое при помощи открытых ключей всех субъектов, у которых есть право доступа (чтения) к зашифрованной информации (эти субъекты легко задаются автоматически). Такая технология позволяет избежать инцидентов, связанных с утерей или кражей носителя, но противоправных действий работника она не предотвратит. Впрочем, случайные утечки, согласно статистике, составляют от 67 до 75% всех инцидентов, происходящих с конфиденциальными данными.

Первые шаги на пути организации принудительного шифрования, правда, только для электронной почты, предприняла компания RSA Security совместно со своим партнером Voltage.

ПРЕОДОЛЕНИЕ ШИФРОВАНИЯ

Как известно, зашифрованное сообщение проверить невозможно. Поэтому многие системы DLP попросту запрещают передачу шифрованных сообщений или шифрованного трафика. Хорошего в этом мало — шифрованный обмен данными столь же необходим бизнесу, как и проверка сообщений.

Из этой ситуации нет универсального выхода, но во многих случаях можно кое-что предпринять. Например, трафик HTTPS можно перехватить при

помощи известной атаки Man-in-the-Middle (MitM), некоторые ключи шифрования разместить в системе DLP, а слабую криптографию дешифровать, подобрав ключ, или же внутрь защищенной области (например, в туннель VPN) ввести сенсор DLP, чтобы иметь доступ к незашифрованным данным. В некоторых случаях образцы и сигнатуры удается отыскать прямо в зашифрованных данных, не имея возможности их расшифровать (по аналогии со «слепой» цифровой подписью).

Словом, отказываться от криптозащиты в угоду защите от утечек никто не собирается, но эти две задачи во многих случаях можно примирить, и производители соответствующих систем постоянно работают над поиском наилучшего решения.

ОБНАРУЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Как было отмечено в начале статьи, ценность, а вместе с ней и стоимость конфиденциальной информации, растет, и быстрее всего — стоимость персональных данных. Это происходит отчасти из-за действительной ценности таких данных для мошенников, а в определенной степени вследствие усиления государственного контроля за обработкой персональных данных и введения санкций за их утечку.

Следовательно, системы DLP должны обладать отдельной функциональностью по детектированию персональных данных. Естественно, детектироваться должны любые, а не предварительно введенные данные. Автор не исключает, что могут появиться редуцированные версии систем DLP, которые заботятся только о персональных данных — для тех предприятий, где их утечка представляет основной риск для бизнеса.

СУЖЕНИЕ ПЕРИМЕТРА

Один из подходов к защите от внутренних угроз представляет собой сужение периметра. Придуман он давно и реализован тоже. Автору известны случаи, когда описанным способом защищалась информация, содержащая гостайну, но лишь в последнее время появились относительно недорогие и массовые способы внедрения такого решения на обыкновенном предприятии.

Чтобы не выискивать конфиденциальную информацию по всему офису, на рабочих станциях, их USB-разъемах и CD-приводах, в кабелях и принтерах, вся защищаемая информация концентрируется на одном сервере и здесь же обрабатывается. Пользователи получают доступ по протоколу X-Windows. Таким образом, по сети передаются лишь графические копии экрана, но не сама информация. За конфиденциальной информацией, сконцентрированной на одном сервере, следить значительно проще.

В результате остается один канал утечки — пользователь. Человек может что-то запомнить или записать на бумажке. Но этот канал перекрывать техническими средствами пока не научились.

Кроме существенного сокращения охраняемого периметра информационной системы (в данном случае лишь подсистемы) решение обещает экономию средств. Персональные компьютеры можно заменить дешевыми бездисковыми рабочими станциями (терминалами) и таким образом заметно уменьшить не только стоимость техники, но и трудоемкость настройки и администрирования.

НОВАЯ ФУНКЦИОНАЛЬНОСТЬ

И, конечно, кроме внедрения революционных новинок, будет наращиваться функциональность «обычных» DLP, в частности:

- вместо запрета доступа к «непрофильным» или развлекательным ресурсам следует разрешить такой доступ, но с ограничением по времени;
- некоторые запреты, как показали исследования, вообще являются излишними, поскольку не увеличивают, а снижают производительность, поэтому от них надо отказываться (даже если заказчик высказывает пожелания такого рода, например о блокировании доступа к социальным сетям);
- для оператора DLP появятся новые формы представления информации, такие как новые типы диаграмм, автоматическое преобразование текстов, звуковое представление событий, визуализация корреляции разных событий;
- точно так же, как системы антивирусов и антиспамов, DLP научатся скачивать обновления сигнатур и правил с сервера производителя или из центрального офиса предприятия.

ПРОТИВОДЕЙСТВИЕ

Согласно закону физики, «действие равно противодействию». Как только распространенность систем DLP превысит некоторый порог (по субъективному ощущению автора ждать осталось недолго), начнутся промышленные разработки и серийный выпуск средств противодействия. Сейчас есть только кустарный инструментарий такого рода, не самый эффективный и, главное, малоизвестный и слабо доступный среднему офисному работнику.

А когда появятся массовые и простые в обращении средства обхода, системы DLP и иные системы защиты от внутренних угроз будут оснащены, как и антивирусы, контрсредствами для активного и пассивного противодействия. Не исключено, что это приведет к сращиванию хостовой части DLP с антивирусным монитором.

ОТКАЗ ОТ КОРОБОЧНЫХ ВЕРСИЙ

В настоящее время системы DLP и аналогичные средства защиты информации поставляются в так называемом коробочном варианте, то есть предназначенном для самостоятельной установки и настройки пользователем, и в комплекте с консалтинговыми услугами, когда установку и настройку производит интегратор после подробного изучения информационной системы клиента и категоризации циркулирующей там информации.

Второй способ внедрения, без сомнений, намного эффективнее, но — и более дорогой. Между тем любому производителю хочется охватить разные сегменты рынка — не только крупные, но также средние и малые предприятия, которым не по карману такие услуги интегратора. Поэтому для борьбы с утечками появляются «коробочные» продукты с урезанной функциональностью, упрощенными типизированными настройками и даже — страшно сказать — под управлением Windows! Очевидно, что эффективными они быть не могут и дают не столько защиту, сколько иллюзию таковой.

Представляется, что «коробочные» DLP должны в будущем либо совсем уйти с рынка, либо стать маргинальными продуктами для контроля единственного канала передачи данных, например, электронной почты или для «чайников» — продуктами, в действенность которых не верит даже их продавец. А в целях удовлетворения потребности среднего и малого бизнеса придется развивать направление «DLP как услуга». При этом одна полноценная система DLP будет обслуживать несколько предприятий, а управление ею поделят между собой провайдер услуги и его клиент.

ФОРМАЛИЗАЦИЯ

Следующая тенденция, точнее опасность, — постепенное превращение систем защиты от утечек в бюрократическую формальность. На этот путь указывают такие аспекты защиты информации, как сертификация технических средств защиты и работа по стандартам ISO-17799 и ISO-27001.

Автор вовсе не утверждает, что сертификация и стандартизация стали бесполезными. Польза от них есть, но она давно уже не является аргументом для принятия решений — в качестве веских доводов выступают «так приказано», «так положено» и «так принято». При этом для руководителя не имеет никакого значения, проведена ли сертификация на самом деле или соответствующий документ получен каким-то иным способом.

Поскольку полезность системы DLP уже очевидна для всех специалистов по ИБ, вскоре ее наличие начнет становиться желательным, а затем и обязательным. Далее, возможно, понадобится не само наличие защиты, а лишь справка об этом.

МЕТКИ НА ВСЕМ

Чтобы тщательнее контролировать пути движения информации, можно попытаться отслеживать перемещение носителей. А для этого их нужно идентифицировать.

Метками или уникальными индивидуальными (серийными) характеристиками могут быть снабжены чистые носители: бумага, книги, флэш-накопители, новые CD- и DVD-диски. Индивидуальные метки наносятся при помощи устройств записи: принтеров, процессоров, пишущих приводов, экземпляров ОС. Например, CD и DVD уже давно снабжаются индивидуальными номерами (просто их еще нельзя считывать дистанционно), а значительная часть принтеров ставит на печатаемые документы скрытые метки.

Технически реализовать идентификацию всех прочих носителей не очень сложно. Но в этом мало смысла, пока не налажена система глобального учета меток. Над решением данной организационной задачи сейчас и работают.

Для подобного глобального учета вряд ли нашлись бы средства, если бы речь шла только об утечках, деанонимизации, борьбе с нарушением авторских прав и прочих исключительно информационных проблемах, но в нем заинтересованы и товаропроизводители, готовые выделять средства на исследования. Индивидуальный и притом автоматизированный учет товаров обещает удешевить дистрибуцию и продажу, улучшить логистику и оценку пожеланий потребителя. Иначе говоря, RFID-метка на ваших трусах и индивидуальный номер во флэш-накопителе — это следствия одних и тех же причин.

ДАТЧИКИ НА ЧЕЛОВЕКЕ

Эта перспективная технология — самая революционная и неоднозначная из всех. Как уже упоминалось, из всех носителей информации труднее всего контролировать человека. Впрочем, «трудно» не значит невозможно. Характер нажатий клавиш и движений мыши исследуются уже давно. Уже ведутся первые опыты по перманентному снятию и расшифровке доступных данных, характеризующих пользователя компьютера: пульс, кожно-гальваническая реакция, дыхание, движение глаз и т. п. Очевидно, что все эти параметры зависят от настроения человека, его лояльности, наличия у него деструктивных намерений. Значит, всю эту информацию можно попытаться извлечь. В случае удачи инсайдерам придется туго.

Персональные датчики станут не только еще одним методом защиты информационной системы — они принесут пользу и работнику. Например, на основе полученных данных можно будет подобрать характер деятельности и режим работы, наиболее подходящие для каждого сотрудника, вовремя выявить конфликты в коллективе, указать на неэффективное управление, численно оценить способности и трудозатраты каждого (для справедливой оплаты), заблаговременно выявить усталость, стрессы и заболевания, обнаружить наличие алкогольного опьянения и тому подобное. К сожалению, нарушить тайну частной жизни тоже станет легче.

DLP-СИСТЕМА МАКРОМАСШТАБА

Как известно, в каждой стране есть орган технической разведки (бывает, и не один), такой, например, как АНБ США. Он собирает информацию с доступных каналов связи для последующего поиска заказанных сведений или превентивного анализа, иногда — не только пассивно.

Технологии перехвата и анализа огромных потоков данных, которые применяют технические разведки, становятся все более доступны. Государство может себе позволить использовать их не только в целях безопасности, но и для более прозаических потребностей — борьбы с уголовной преступностью, защиты от идеологических диверсий, борьбы с распространением спама и порнографии, противодействия нарушению авторских прав, а также для промышленного шпионажа и контршпионажа. Такие действия уже предпринимаются.

Эксперты по DLP планируют организацию своеобразного «второго кольца защиты». Перехватчики на магистральных каналах связи и соответствующие системы обработки позволят предотвратить утечку конфиденциальной информации (равно как и «приток» вредоносной), которая была незамечена средствами защиты на периметре корпоративных сетей.

Например, лишь немногие (единицы) магистральные каналы пересекают границы России. Снабдить их все соответствующими перехватчиками — задача вполне осуществимая. Кроме того, специалисты задумываются о перекрытии другого трансграничного канала — так называемого офлайнового перемещения носителей. Например, пограничные и таможенные органы некоторых стран начали проводить досмотр и копирование информации с носителей, перевозимых через госграницу. Полезны будут анализаторы на поисковых системах — этих перекрестках виртуального мира.

В итоге начинает вырисовываться своеобразная DLP-система государственного масштаба, которую было бы неразумно использовать только в военных целях или для спецслужб. Задач для нее предвидится много, в том числе неплохо оплачиваемых.

КОНФЛИКТЫ

Некоторые из планируемых нововведений, безусловно, не будут соответствовать требованиям современного законодательства — придется либо вносить поправки, либо строить хитрые юридические конструкции для обхода регламентных препон. Определенная часть новшеств вообще выходит за пределы правового поля, например, вживление сенсоров DLP в работника. С техническим прогрессом часто так бывает: он приводит к принципиально новым общественным отношениям, которые позже приходится регулировать с помощью законов.

В жизни социума есть «белые пятна», где законодательство вообще никак не регламентирует общественные отношения, поскольку их «не знает». А вот мораль, в отличие от закона, всегда имеет суждение и может выдать оценку явления, которого прежде не существовало. С моралью технический прогресс тоже постоянно конфликтует. Правда, в большинстве случаев эти конфликты заканчивались победой прогресса, а мораль под него подстраивалась.

В любом случае функциональность новых систем DLP неизбежно будет вступать в противоречие с законом и моралью. Бояться этого не стоит. Наличие конфликтов свидетельствует, что техника развивается, выходит в новые, неисследованные области. Отсутствие же конфликтов означало бы, что мы топчемся на месте. LAN

Николай Федотов — главный аналитик компании InfoWatch. С ним можно связаться по адресу: Nikolay.Fedotov@infowatch.com.