

Прогнозы экспертов говорят о том, что в 2010 году кибератаки на российские компании будут оставаться на уровне 2009 года. Однако в области информационной безопасности выделены три основных направления. Выявление и устранение проблем, связанных с утечкой данных из компаний. Это обусловлено тем, что ожидается увеличение доли утечек, осуществляемых преднамеренными злоумышленниками, а также усиление ответственности за нарушения в этой области.



Под грифом «секретно»

Наталья Жилкина /
nzhilkina@computerra.ru/

Преступление и наказание

Данные о происходящих в мире наиболее громких утечках периодически публикует аналитический центр компании InfoWatch. Согласно официальным отчетам, опубликованным в СМИ США, около 60% всех утечек были допущены преднамеренно, а оставшиеся 40% произошли по недосмотру персонала компаний.

Николай Федотов, ведущий аналитик InfoWatch, приводит следующие данные: «Подсчеты InfoWatch подтверждают, что преднамеренных утечек в целом происходит больше, чем случайных. Наше соотношение на 2009 год — 51:43,5, на 2008-й — 46:42. А еще раньше, в 2007 году, доля намеренных утечек была существенно меньше, чем случайных».

Как отмечает Николай Федотов, в Великобритании ужесточается наказание за получение, раскрытие и передачу анкетных данных третьему лицу, а также за особо тяжкие случаи нарушения DPA. В США только утечка/утрата/разглашение персональных данных влечет за собой наказание, а за неправильное хранение уголовной или административной ответственности не предусмотрено. «В России ответственность за утечку персональных данных отсутствует вовсе. Зато предусмотрено наказание за несоблюдение установленных правил их защиты», — говорит Николай Федотов. Более подробно о ситуации вокруг российского «Закона о персональных данных» (ФЗ-152) см. в комментарии «Затянувшийся прыжок» Алексея Сабанова, заместителя генерального директора ЗАО «Аладдин Р. Д.».

По словам Николая Федотова, во многих случаях первая же предотвращенная утечка с помощью специального класса решений DLP (Data Leakage Protection) окупает затраты.

«Повсеместное внедрение DLP-решений влечет снижение доли случайных инцидентов, — говорит Федоров. — Но вот абсолютное число зарегистрированных инцидентов продолжает расти. Как и ущерб, причиняемый среднему предприятию средней утечкой».

Оружие против утечек

В 2008–2008 годах многие компании, специализирующиеся на разработке продуктов для защиты от утечек данных, стали предметом повышенного внимания со стороны ведущих игроков рынка информационной безопасности: практически все ведущие зарубежные игроки уже приобрели фирмы, ведущие разработки в нише DLP-решений. Trend Micro приобрела компанию Provilla, Websense — Porth Authority, Symantec — Vontu.

Не стала исключением и McAfee, которая охватила сразу два направления DLP, поглотив сначала компанию Onigma (активность на хостах) и не так давно — Reconnex (сетевая активность). Еще одно приобретение, SafeBoot, дополнило набор продуктов по утечкам функционалом шифрования файлов, папок, дисков.

Объединение линеек Onigma и Reconnex в едином продукте — это вопрос самого ближайшего времени. Однако уже сейчас оба DLP-продукта McAfee работают с ePolicy Orchestrator (ePO). У McAfee это одно из основных внутренних требований. Разрабатывая или приобретая какую-либо технологию, компания производит интеграцию этой технологии в ePO — единое средство для управления любыми продуктами McAfee.

«На текущий момент линейки DLP-продуктов, специализирующихся на сетевой активности и активности на хостах, напрямую друг с другом не интегрированы, но у них и задачи несколько раз-

важно все способы утечек конфиденциальных данных. Против фотографирования экрана дисплея, например, DLP-продукты бесспорны; в этом случае могут помочь средства физической безопасности, такие как строгий контроль доступа, системы видеонаблюдения и организационные мероприятия».

Что предлагает McAfee? Первое — защищать все операции с данными (копирование, вставка, печать, изменение, передача). Второе — предоставлять администратору полный список действий при попытках нарушения политик, с нарушителями и данными (слежение за пользователями и данными, блокирование в реальном времени конфиденциальной информации, уведомление пользователя и администратора, сохранение всех доказательств в карантине).

С грифом «Секретно»

Степень секретности сведений в организации должна соответствовать степени тяжести ущерба, нанесенного ее интересам в той области деятельности, на которой она специализируется. «Фактически все современные механизмы идентификации (как, в принципе, и любая правильно созданная продуманная система DLP) имеют внутреннюю систему назначения грифа секретности, — рассказывает Алексей Чередниченко. — Эта система очень напоминает принципы работы отделов безопасности на режимном предприятии. По сути, DLP — это „Первый отдел“, перенесенный, скажем так, в электронную среду».

Стратегия внедрения DLP-продуктов McAfee на начальном этапе предлагает воспользоваться средствами создания классификатора. Предусмотрены уровни секретности информации, по аналогии с тем, как сведения, отнесенные к государственной тайне, подразделяются на сведения «особой важности», «совершенно секретные» и просто «секретные».

Система понимает классификацию данных — по расположению, по содержанию, по типу файла и по отпечатку. Правила реагирования — это слежение за движением, предотвращение утечки, оповещение администратора, и пользователя. Дополнительно при выходе из сети можно выполнить шифрование данных — то есть разрешить данным уходить из сети, но при этом их шифровать.

Помимо стандартного, можно придумать собственный внутрикорпоративный классификатор уровней секретности информации, в соответствии со спецификой конкретной компании. Заказчик с помощью настроек DLP-продуктов McAfee может сам создавать любые градации информации, он может самостоятельно определить их количество и степень критичности. Характерно, что классификация документов происходит в процессе их движения.

— Никакого специального отдела, принимающего решение о выдаче того или иного грифа секретности, здесь нет, а есть здравый смысл и формальная логика, — поясняет Алексей Чередниченко. — Чаще всего совет правления или кто-то из владельцев компании принимает решение на основе своего мнения или мнения экспертов, которые могут быть привлечены для этой цели. То есть решение принимается не о том, какие конкретно документы отнести к тому или иному уровню секретности; оно имеет более общий характер: какие

■ Алексей Чередниченко: «Применяя одновременно сетевой и хостовый DLP, можно добиться максимальной эффективности».



предметные области для компании являются важными или особо критичными?

Изначально принимается формальное решение о том, какие типы документов для предприятия являются важными, но не критичными, какие документы являются жизненно важными (настолько, что если именно этот документ станет достоянием конкурентов или гласности, то это нанесет непоправимый коммерческий ущерб компании).

Системе DLP остается лишь определить, к какому типу относится тот или иной передаваемый документ, и на основании этого принять решение о том, какие группы документов являются важными, какие — критичными, какие — закрытыми или открытыми.

Как это работает?

В соответствии с формальной логикой определяется количество градаций в классификаторе, а дальше в форме описания в настройках эти сведения просто заносятся внутрь продукта. После этого необходимо определить, что является критерием для причисления документа к данной категории классификатора.

После того как сформирована группа критериев и продукт настроен на выявление документов, соответствующих тому или иному критерию, документу можно с уверенностью присвоить определенный гриф секретности. В качестве критерия можно использовать словари, цифровые отпечатки документа и проч.

После того как критерии занесены внутрь продукта, система может четко распознавать, является ли документ критичным и в какой степени. А далее сначала просто включается режим обзора, и система работает как наблюдатель, никуда не вмешиваясь. Это делается для того, чтобы можно было произвести настройку системы: зачастую на начальном этапе, когда велико влияние человеческого фактора, ошибки не исключены. В результате система просто наблюдает, какие документы попадают под тот или иной классификатор. Но в процессе работы в результате постоянной подстройки достигается приемлемая точность работы технологии.

Далее систему переключают в боевой режим, и начинается собственно работа. Если документ не был классифицирован на этапе создания и на этапе его движения, то при попадании в среду, контролируемую DLP McAfee, на одном из последующих этапов это обязательно произойдет. Делается это один раз, но переклассификация также возможна. Простой пример: в конфиденциальном документе действительно конфиденциальной может оказаться только часть информации. Если из него изъять критичный контент и вставить в новый документ, то формально старый потеряет свою конфиденциальность. Но новый документ, который при этом был создан, становится конфиденциальным, а значит, прежний, если он сохраняется в новом виде, не должен иметь тот же классификатор критичности, который имел ранее. Поэтому интеллектуальная система присваивает ему новый классификатор в соответствии с осуществленными действиями.

DLP-продукты McAfee отслеживают изменения в документе при работе с ними из самых разных приложений. Если документ реально понизил степень критичности, ему будет присвоен новый классификатор в соответствии с изменением. Это происходит автоматически при любых изменениях документа — при конвертации из одного формата в другой (был текст — стала картинка).

Помимо полного функционала, решение McAfee отличается от существующих на рынке продуктов DLP еще и гораздо более низкой ценой. «По соотношению „цена — функциональность“ это, пожалуй, одно из лучших на рынке решений», — добавляет ведущий специалист McAfee.

Одно из наиболее выгодных предложений для защиты хоста — комплексное решение Total Protection for Data — включает в себя

антивирус, персональный firewall, модуль antispyware, модуль Encryption и хост DLP. «Применяя этот бандл, мы получаем вполне крепкую комплексную защиту на уровне хоста, в том числе и от утечек», — говорит Алексей Чередниченко.

Для DLP-продуктов применяются статистические методы оценки, которые являются наиболее используемым критерием в любой области. Если с течением времени статистически оценивать динамику попыток утечки, то по характеру этих попыток можно судить о побудительных причинах нарушения.

Сроки реализации

Реализация DLP-решения в организации — это сложная задача, которая может быть решена с привлечением аудиторов и различных консультантов. Помимо того, что само по себе решение DLP может стоить недешево, его реализация грозит обойтись еще дороже.

При внедрении продуктов DLP классическим подходом считается следующая процедура. На первом этапе команда консультантов обследует уровень критичности информации в организации, создает классификаторы, выявляет все данные. Далее формируется решение и настраивается продукт.

Таким образом, основная (и самая дорогостоящая) часть заключается в предварительной, очень кропотливой и трудоемкой работе. На этом этапе необходимо выявить все источники, где порождаются конфиденциальные данные, пути их перемещения, места хранения, инструменты (приложения), которыми они обрабатываются, пользователей, которые это делают, и т. д. И эта работа может занимать от нескольких месяцев до года. О том, что стоимость ее весьма высока, производители стараются не говорить. Стоимость такого проекта может оказаться (и обычно оказывается!) больше стоимости внедряемого продукта. И это уже задача самого заказчика — кого привлечь к выполнению данного этапа работы.

Достоинством McAfee является тот факт, что компания предлагает DLP-продукты, которые позволяют создавать простые и дешевые решения. Задача по утечке данных DLP от McAfee может быть решена легко и просто, без превращения ее в долгий, сложный и дорогостоящий проект.

«На данный момент компания McAfee сама не ведет в России проектный бизнес ввиду отсутствия локальных ресурсов, — поясняет Алексей Чередниченко. — В России у нас достаточно большое число партнеров, которые позиционируют себя как специалистов в области DLP. Привлечение западных ресурсов, конечно, возможно, но не слишком рентабельно, особенно в момент кризиса».

«Главное достоинство продукта McAfee заключается в том, что у McAfee технология DLP позволяет автоматизировать рутинную часть, — говорит Алексей Чередниченко. — Потому что, когда мы ставим свой продукт в режим наблюдения, мониторинга — в течение нескольких дней картина становится полной. Единственное, что нам нужно сделать, — это выявить сами документы и сформировать классификатор. А дальше продукт выявит все места, где хранятся эти документы, пути их передачи, какие пользователи с ними работают, какие физические лица являются пользователями этих документов, какие приложения их обрабатывают».

Таким образом, продукт McAfee DLP позволяет внутри организации получить полную картину, касающуюся этих документов. В результате сроки внедрения такого продукта резко сокращаются. Это одно из основных конкурентных преимуществ технологии McAfee, которая позволяет намного сократить цикл внедрения без привлечения высококвалифицированных кадров. Данная технология весьма позитивно влияет и на сроки, и на стоимость внедрения». <