ванию, изменению защищаемых данных сохраняются в журнале, с которым можно работать централизованно. Однако передача информации по сети не контролируется.

Американская компания Verdasys реализовала с помощью агентов для ПК комплексное решение по защите: устанавливаемые на ПК и ноутбуки агенты контроля Digital Guardian предотвращают все каналы утечек непосредственно на компьютерах пользователей. При этом сервер управления используется для централизованного развертывания, настройки политик контроля и сбора журнала событий.

Еще один класс решений — системы, контролирующие информацию при передаче по сети. Обычно эти приложения используются для мониторинга почтового или сетевого трафика.

Продукты «Дозор-Джет», разработанные российской компанией «Инфосистемы Джет», предназначены прежде всего для контроля веб-трафика, фильтрации и архивирования электронной почты. Предотвращение потенциальных утечек обеспечивается за счет блокирования подозрительных соединений и писем (помещение в карантин). Кроме того, реализована важная функция накопления архива почтовых сообщений.

Некоторые системы, такие, как Onigma Platform (приобретенная в прошлом году McAfee), совмещают в себе функции пользовательских агентов и контроля трафика. При этом системы обеспечивают, как минимум, функции централизованного управления и развертывания, а также ведения журналов.

У систем, использующих фрагментарный подход, есть несколько существенных минусов. Например, ПО, контролирующее десктопы пользователей, обычно не обеспечивает архивирование электронной почты, тогда как наличие архива переписки обычно очень важно для расследования инцидентов безопасности и сбора доказательств. Кроме того, большинство из них не имеют возможности предотвратить (блокировать) утечку данных, инцидент безопасности может быть выявлен только постфактум, при анализе журналов.

Эволюцией решений, защищающих локальные участки, стали комплексные системы, контролирующие все возможные направления утечки данных.

Комплексные решения стремятся контролировать операции с данными на всех стадиях их хранения (серверы, базы данных), использования (рабочие станции пользователей, операции копирования изменения, печати и т. п.) и передачи по внутренним и внешним каналам (в сети, по электронной почте, на веб-узлы и т. п.). Непременным условием является хранение архива переданной информации (например, электронной почты) и действий по использованию защищаемых данных. Например, в решении российского производителя InfoWatch архивируются все сообщения электронной почты за семь лет и ведутся журналы отчетов от модулей контроля в универсальном архиве. Все это сопровождается функциями выявления инцидентов и создания отчетов по использованию данных.

Важной особенностью корпоративного решения InfoWatch является разделение прав операторов («офицеров информационной безопасности») для разделения ответственности. Это позволяет контролировать важную угрозу — похищение данных ИТ-персоналом или сотрудниками службы безопасности, имеющими доступ к данным (по мнению экспертов, ряд последних утечек из госорганов и банковских структур произошел при посредничестве обиженных работодателями ИТ-специалистов).

Для определения конфиденциальной информации, требующей защиты, в системах ILD&P в основном применяются вероятностные методы распознавания защищаемых данных — морфологический и сигнатурный анализ, а также технология «водяных знаков» (digital fingerprints). При применении сигнатур (наборов ключевых слов) (используется, например, в MIMEsweeper и Symantec Gateway Security) в базе фильтрации необходимо хранить все синтаксические формы ключевого слова (падежи, роды, спряжения, число и их сочетания). Для русского языка задача осложняется тем, что все словоформы должны храниться во всех кодировках.

КАКИЕ ПРОГРАММЫ ДОЛЖНЫ БЫТЬ НА НЕМ УСТАНОВЛЕНЫ, РЕШАЕТ РУКОВОДСТВО КОМПАНИИ. СОТРУДНИК, ВЫПОЛНЯЯ СВОИ СЛУЖЕБНЫЕ ОБЯЗАННОСТИ, ДОЛЖЕН ПОЛУЧАТЬ ДОСТУП ТОЛЬКО К ТОЙ ИНФОРМАЦИИ, НА КОТОРУЮ ИМЕЕТ ПРАВО

В решении InfoWatch используется комбинированный подход: пересылаемые данные сканируются на предмет наличия предопределенных ключевых слов и фраз. Лингвистический анализ позволяет учесть контекст, в котором используются ключевые слова и фразы. Кроме того, передаваемые данные сравниваются с постоянно обновляемыми «шаблонами» конфиденциальных сообщений, специфичных для каждого конкретного заказчика. При любом из этих методов требуется существенная настройка на информационную среду заказчика.

ОХРАНЯЕМЫЙ ПЕРИМЕТР Но пока продукты ILD&P нацелены на крупных корпоративных заказчиков. В мелких и средних фирмах такой уровень защиты данных от утечек зачастую не нужен, а ИТ-бюджет не предусматривает серьезных трат на этот аспект информационной безопасности.

Например, 55% всех внедрений программных продуктов «Дозор-Джет» осуществлены в крупных организациях (от 1 тыс. до 15 тыс. сотрудников), 28% — в средних (от 300 до 1 тыс. сотрудников) и лишь 17% — в организациях малого бизнеса (до 300 сотрудников). По данным компании InfoWatch, стоимость системы, включая затраты на внедрение, может составить $300–400 на одно рабочее место.

То есть пока ILD&P-системы не являются «коробочным» продуктом и требуют комплексного внедрения, подразумевающего стадии консалтинга (оценка существующей ИТ-инфраструктуры, коррекция или разработка политики защиты данных, установка и настройка ПО, обучение специалистов, отвечающих в компании за ИТ-безопасность).

Вендоры ПО защиты от внутренних утечек разрабатывают методологии внедрения, помогающие системным интеграторам и заказчикам интегрировать систему защиты от утечек в существующую ИТ-инфраструктуру и перекрыть все возможные каналы утечки данных. Кроме того, обычно решение требует значительной кастомизации в соответствии с требованиями заказчика и настройки под конкретные типы защищаемых данных.

Интенсивное развитие продуктов этого класса в ближайшие несколько лет приведет к стандартизации подходов, используемых для защиты данных внутри «охраняемого периметра». По мнению Дениса Зенкина из InfoWatch, продукты станут более «коробочными» и вендоры, окончательно поделившие рынок крупных клиентов, ринутся в сегмент небольших компаний.

Впрочем, уже сейчас очевидно, что обнаружение утечки после того, как она произошла, не может устраивать пользователей подобных систем. Функции интеллектуального предотвращения инцидентов являются основным полем для конкуренции и развития продуктов. Разработка ведется в направлении проактивных методов защиты, когда утечка распознается и блокируется на ранней стадии благодаря сопоставлениям действий пользователя с шаблонами подозрительной активности, а также выявлениям нетипичных операций.

Часть функций систем защиты от утечек может быть возложена на выделенные аппаратные компоненты. Модули системы, которым необходимо обслуживать большой объем операций (например, средства фильтрации данных, передаваемых по интернет-протоколам, или обращения к серверу баз данных), могут предлагаться заказчику в виде специализированного устройства (заменяющего выделенный сервер, на который устанавливается аналогичный программный компонент). В некоторых ситуациях это позволяет сократить затраты на оборудование и упростить развертывание решения в филиалах компании.

Тем не менее даже при использовании самых совершенных систем защиты от утечек требуется комплекс организационных мер — таких, как лишение пользователей прав администратора на ПК и стандартизация ПО. Такие меры способны затруднить использование средств, например шифрования и стеганографии, затрудняющих работу механизмов контентной фильтрации.

Будущее ПО обеспечения информационной безопасности — интеграция функций защиты от различных типов угроз, внутренних и внешних, в единые системы комплексной защиты. ■

«ДЕФИЦИТ КВАЛИФИЦИРОВАННЫХ УПРАВЛЕНЦЕВ»

Информационная безопасность — это необходимая часть корпоративной культуры, за которую несут ответственность все сотрудники компании, уверен РОБЕРТ ЭЙДЖИ, вице-президент, глава представительства компании Cisco Systems в странах СНГ. Об особенностях информационной безопасности с представителем крупнейшей мировой компании, определяющей принципы и подходы развития рынка ИТ-безопасности, беседовал ЕВГЕНИЙ ЧЕРЕШНЕВ.

BUSINESS GUIDE: Как вы оцениваете уровень развития рынка информационной безопасности в России?

РОБЕРТ ЭЙДЖИ: Скажем так, до совершенства еще далеко. Россия перестала изобретать велосипед, начала интегрировать, лицензировать и адаптировать международный опыт в области информационной безопасности в свою практику.

BG: Российский бизнес, на ваш взгляд, готов перенимать западный опыт в области информационной безопасности?

Р. Э.: Информационная безопасность и в США тема открытая, ею занимаются многие, но даже там впервые задумались о том, как просчитать окупаемость вложений в IT только два-три года назад. А до того, чтобы оценить возврат инвестиций в информационную безопасность, дело еще даже там не дошло.

BG: В ближайшие годы ситуация изменится?

Р. Э.: Как сегодня решаются проблемы безопасности? Наверняка где-то на периметре установлен FireWall и антивирус, как максимум — VPN. Редко дело доходит до более сложных систем. Поэтому в данных условиях, я думаю, в России все будет протекать весьма медленно и спокойно. Думаю, ничего революционного не произойдет. Все, что так или иначе востребовано рынком, уже изобретено, запатентовано, и в настоящее время компании пытаются все это изобилие превратить в нечто удобное, простое в управлении и для интеграции. В свое время по рынку долго ходил анекдот: «Чем отличается Windows 95 от Windows 98? Тем, что в первой не используется 95% ее возможностей, а во второй — 98%». Это утрированная ситуация, но не лишенная смысла.

BG: А в чем тогда проблема — в недостаточной квалификации ИТ-специалистов?

Р. Э.: В России действительно наблюдается острый дефицит квалифицированных управленцев. Отделы безопасности, как правило, возглавляют выросшие системные администраторы, программисты и математики, прекрасно владеющие технической стороной вопроса, но далекие от бизнеса — они попросту не умеют объясниться с руководителем на языке бизнеса, а не специфической терминологии. Второй вариант — директора по информационной безопасности старой закалки, которым, как правило, существенно за 50, а следовательно, и безопасность для них ассоциируется с противодействием на электромагнитных импульсах и наводках, шифровании и режимном документообороте. Что старомодно.

Но главная причина в другом. Российский топ-менеджмент еще не осознал, что информационная безопасность не технологическая проблема, а такой же бизнес-процесс, как, например, биллинг. Это часть корпоративной ответственности, за что отвечает и IT-директор, и CEO компании, и HR-отдел. Каждый сотрудник компании, все должны быть вовлечены в обеспечение безопасности.

BG: Зачем при этом вовлекать всех сотрудников?

Р. Э.: Человеческий фактор в информационной безопасности играет огромную роль. Утечки информации часто имеют место не потому, что FireWall пропустил атаку, а антивирус упустил свежего интернет-червя. Сотрудники теряют информацию, потому что не знают, как ее уберечь, или, что страшнее, делают это сознательно.

BG: Бывает и обратная ситуация. Системный администратор урезает права сотрудника так, что не открывается даже календарь! И к этому в итоге сводится обеспечение безопасности компании…

Р. Э.: Компьютер, за которым работает сотрудник, ему не принадлежит, поэтому то, какие программы должны быть на нем установлены, решает сама компания. Сотрудник, выполняя свои служебные обязанности, должен получать доступ только к той информации, на которую имеет право. Однако все это совершенно не означает, что надо впадать в крайность. Проблема России в известном максимализме: зачастую сотрудники привязаны к офису, а их рабочие места настроены так, что для качественного выполнения своих обязанностей им попросту не хватает инструментов. Такое положение вещей к информационной безопасности не имеет никакого отношения.

КРУПНЕЙШИЕ УТЕЧКИ ИНФОРМАЦИИ В РОССИИ

В 1992 году в Москве впервые появились компакт-диски с информацией о физических лицах—абонентах МГТС. Источник утечки не найден.

В 1996 году в продаже появилась информация об абонентах сотового оператора «Вымпелком». Компания позднее заявила, что нашла и наказала виновных.

В ноябре 2002 года в Москве появились диски с данными об абонентах сети МТС, в январе 2003 года вышел второй — с информацией о 5,5 млн абонентов. Источник утечки не найден.

20 мая 2003 года в Санкт-Петербурге появились диски с данными о 4,5 млн клиентов сотовых компаний «МегаФон», «Телеком XXI», «Северо-Западный телеком» и «Петерстар». По одной из версий, утечка была через правоохранителей.

В июле 2004 года «Вымпелком» сообщил о сайте sherlok.ru, предлагавшем информацию об абонентах «Билайна», «МегаФона» и МТС в Москве и Санкт-Петербурге. 26 ноября задержаны семеро подозреваемых, в числе которых трое сотрудников «Вымпелкома». В марте 2005 года суд приговорил их к штрафам.

В феврале 2005 года в Москве появилась база данных о банковских операциях Центробанка в 2003–2004 годах, 20 мая вышло дополненное издание. 25 октября заместитель главы управления безопасности и защиты информации МУ ЦБ Владимир Бабкин заявил, что канал утечки перекрыт.

В ноябре 2005 года появились в продаже данные о доходах за 2004 год 9,9 млн жителей Москвы и области. 16 ноября 2005 года ФСБ объявила о задержании лиц, причастных к хищению баз данных Центробанка РФ и ФНС. Их имена и судьба неизвестны.

15 августа 2006 года ряд бюро кредитных историй и банков получили предложение купить базу данных заемщиков, бравших потребительские кредиты. База содержала 700 тыс. записей. 7 сентября гендиректор Национального бюро кредитных историй Александр Викулин заявил, что утечка была из нескольких банков.

В октябре 2006 года Генпрокуратура РФ возбудила уголовное дело в отношении чиновников из аппарата правительства РФ, передавших представителю компании ТНК-ВР «копии документов с конфиденциальной информацией». В сообщении Генпрокуратуры подчеркивалось, что материалы могли быть использованы в целях, противоречащих «интересам государства в области энергетики».

За месяц до выхода нового романа Виктора Пелевина «Empire V», назначенного на начало ноября 2006 года, его текст появился в сети. Роман был украден из компьютерной системы издательства. По словам главы издательства «Эксмо», где готовили к печати рукопись, Леонида Шкуровича, удалось вычислить личность похитителя, но не удалось собрать против него конкретных улик. Подозреваемый не был штатным сотрудником «Эксмо».

АНДРЕЙ ВИНОКУРОВ