

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

На рынке DLP начался этап консолидации. В России этот сегмент также находится на пороге серьезного роста.

DLP на старте

Сергей Орлов

Как подсчитали аналитики Forrester Research, потеря одной записи с информацией о клиенте обходится компаниям в среднем в 173 доллара. На мировом рынке систем защиты от утечек конфиденциальной информации (Data Leakage Prevention, DLP) присутствуют как признанные вендоры, так и недавно созданные компании, причем доминирующую роль играют поставщики традиционных систем борьбы с вредоносными программами, у которых достаточно средств для приобретения начинающих разработчиков DLP. Однако даже у наиболее успешных производителей число заказчиков не превышает нескольких сотен.

По данным Forrester, лидерами мирового рынка DLP являются Websense, McAfee, Symantec, CA, RSA Security и Verdasys, а эксперты Gartner относят к группе ведущих разработчиков систем DLP, обеспечивающих анализ контента, компании RSA, Symantec и Websense (в «магическом квадранте» Gartner эти производители помещены в раздел «лидеры»). Помимо них отмечены также McAfee, CA, Vericert, Code Green Network («прогнозисты»), Fidelis Security Systems («претенденты») и Trend Micro, Verdasys, GTB Technologies, Palisade Systems, Workshare («нишевые игроки»). Число вендоров DLP продолжает расти. Функции DLP встраиваются в программное и аппаратное обеспечение коммутаторов, серверов и клиентских систем.

Характеризуя мировой рынок систем DLP как развивающийся, Forrester выражает уверенность, что в ближайшие три – пять лет его ожидает стремительный рост. Заказчики начинают воспринимать такие решения как необходимый элемент ИБ. Из 2000 опрошенных сотрудниками Forrester компаний 15% уже внедрили системы DLP, а 24% плани-

руют сделать это в текущем году. По прогнозу Gartner, данная технология получит повсеместное распространение. Как показывают результаты опроса GTB Technologies, основная причина внедрения DLP – стремление защитить репутацию компании (96%), желание избежать судебных исков (83%) и привести систему ИБ в соответствие с регулирующими требованиями (77%), обеспечение защиты интеллектуальной собственности (66%).

На российском рынке DLP лидером является компания InfoWatch. К настоящему времени спрос в достаточной степени сформировался, вследствие чего обострилась конкуренция между вендорами. В крупных инсталляциях предпочтение отдается продукции Symantec (Vontu) и Websense (Data Security Suite, DSS). В проектах сред-

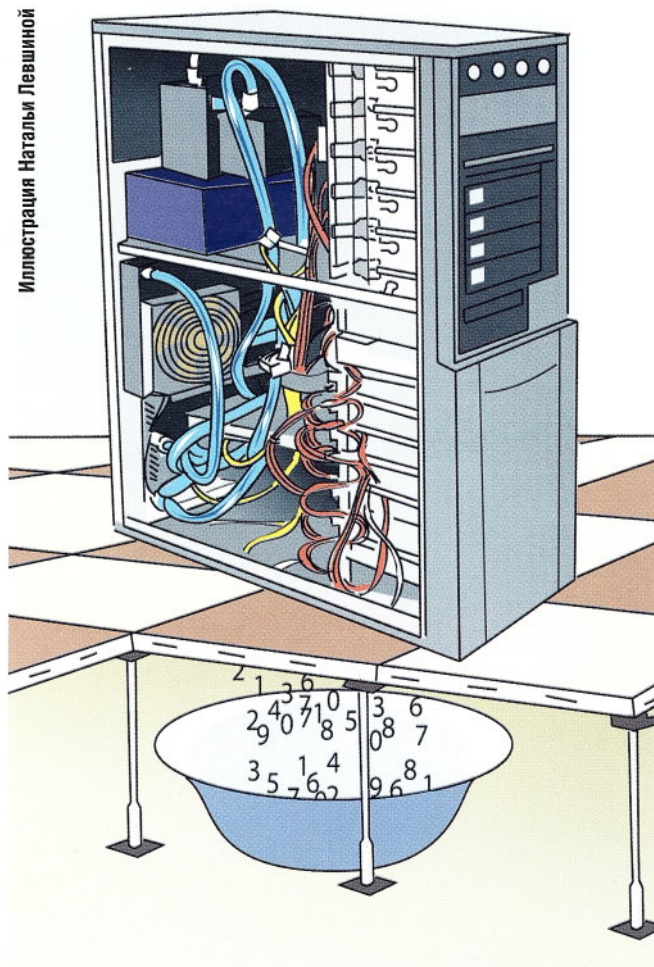
него масштаба Websense конкурирует с InfoWatch, а в сегменте SMB на ведущие позиции претендуют InfoWatch и McAfee. По оценкам Николая Зенина, руководителя направления защиты коммерческих тайн LETA IT-company, InfoWatch удерживает ведущие позиции (примерно 65%), но тенденция проникновения разработок западных вендоров (Symantec, Websense, McAfee) налицо, и у каждого из них примерно по 10% рынка DLP в России.

Основные потребители систем DLP в мире – компании с численностью сотрудников 1–5 тыс. пользователей. Крупные предприятия осознают проблемы утечек и всерьез ими занимаются. Небольшие компании (с годовым оборотом менее 500 млн долларов) идеей защиты от утечек данных пока не прониклись, но, по мнению аналитиков, в 2010–2011 гг. они начнут разворачивать такие системы.

Интерес к защите от утечек данных в сегменте SMB растет. Как поясняет Наталья Касперская, генеральный директор InfoWatch, малые и средние компании обычно не имеют выделенного специалиста по безопасности и службы ИБ, к тому же, как правило, у них нет регламентирующих процедур по защите информации, поэтому очень важным фактором для SMB является цена. Эти заказчики пока только присматриваются к системам DLP, но демонстрируют достаточно высокий уровень понимания проблемы утечек. Примерно 30% опрошенных InfoWatch компаний SMB используют какие-то элементы DLP, однако полнофункциональных систем не применяет никто. Главными препятствиями остаются финансовые ограничения (35%) и несоответствие систем предъявляемым к ним требованиям (10%).

(продолжение на странице 47)

Иллюстрация Натальи Левшиной



(начало на странице 48)

Как подчеркивает Наталья Касперская, рынок DLP находится в начальной стадии и потенциальные потребители пока лишь тестируют эти технологии. По мнению Кирилла Керценбаума, руководителя группы технических консультантов по безопасности Symantec, у российских заказчиков есть уникальная возможность внедрить уже опробованные за рубежом технологии и выбрать из спектра предлагаемых решений и подходов наиболее подходящие для конкретных условий.

По словам Николая Зенина, выбор систем DLP в России сейчас очень широк. Из 13 решений, рассмотренных в последнем отчете Gartner, как минимум шесть (Symantec, Websense, RSA, McAfee, Trend Micro, Verdasys) доступны для российского потребителя. Некоторые из них похожи (например, подходы, применяемые в RSA DLP Suite и Symantec DLP, во многом близки, а Verdasys очень напоминает McAfee Host DLP), поэтому не всегда есть необходимость рассматривать все варианты. Кроме того, InfoWatch предлагает собственную систему DLP, а вдобавок на рынке имеются специфиче-

ские (не подпадающие под определение DLP) решения.

Российским заказчикам известна также система SafeSpace производства Perimetrix. Определенным функционалом систем DLP наделили свои продукты компании «Инфосистемы Джет» («Дозор Джет» – СКВТ и СМАП), «Праймтех» (Insider), SecurIT (Zlock и Zgate), Smart Protection Labs Software (SpectorSoft Spector 360, SecrecyKeeper), «Информзащита» (Security Studio), «Инфооборона» («Инфопериметр»), «АтомПарк Софтваре» (StuffCop), Smart Protection Labs Software (SecrecyKeeper), SearchInform («Контур безопасности») и «Технологии Корпоративной Безопасности» («ТКБ мониторинг»).

LETA IT-company, сотрудничающая практически со всеми разработчиками решений DLP, присутствующими на российском рынке, старается выводить новые продукты совместно с вендорами. В первое время зарубежные вендоры испытывают определенные затруднения, поскольку они вынуждены учитывать российскую специфику (многообразие кодировок, словари). Symantec, McAfee и Websense прошли этот период адаптации в 2007–2009 гг.

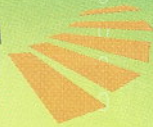
Как считает Валерий Боронин, руководитель лаборатории защиты информации от внутренних угроз компании «Лаборатория Касперского», в России основными причинами, заставляющими задуматься о внедрении DLP, могут быть экономическая оправданность этой процедуры, возрастание рисков и развитие предприятия. К внедрению DLP побуждает и вступление в силу закона «О персональных данных», а также прецеденты, связанные с утечкой информации.

Спрос наблюдается, в первую очередь, со стороны средних и крупных компаний, которые много лет занимаются своим бизнесом, — они ощущают на себе пристальное внимание регуляторов и уже обладают внутренними регламентами и политиками, необходимыми для успешного внедрения систем DLP. При этом даже среди компаний сектора SMB осведомленность о системах DLP, по некоторым оценкам, превысила 95%, что говорит о перспективах данного направления. LAN

Сергей Орлов — ведущий редактор «Журнала сетевых решений/LAN». С ним можно связаться по адресу: sorlov@lanmag.ru.

ИНТЕРНЕТ УНИВЕРСИТЕТ

ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ



Создайте свой университет!
<http://www.intuit.ru/scorm>

Учебные курсы для обучения сотрудников компаний и студентов в учебных заведениях

Интернет-Университет Информационных технологий предлагает более 250 курсов по информационным технологиям в формате SCORM2004

Готовые модули легко загружаются в системы дистанционного обучения (LMS – learning management systems)

Курсы поставляются на неограниченный срок и для неограниченного количества учащихся



SCORM2004

123056 Москва, Электрический пер., д. 8, стр. 3, ИНТУИТ.ру
 Тел. (+7 495) 253-9312, 253-9313, факс. 253-9310
<http://www.intuit.ru/scorm>
shop@intuit.ru

Реклама