По следам Ходжи Насреддина, или

Как купить DLP-систему и не остаться в дураках

Игорь СОБЕТСКИЙ,
преподаватель учебного центра «Информзащита»

Наша компания рада предложить вам удобную, надежную и дешевую систему. Выберите любые два пункта!
Из рекламы

Освещаемая в данной статье проблема выбора и установки DLP-системы актуальна для малых и средних компаний численностью до 1000 человек. Казалось бы, в настоящее время приобретение DLP-системы не представляет никаких сложностей для большинства российских компаний. Рынок DLP-систем конкурентен, и каждый поставщик рад предоставить более или менее полную информацию по своему продукту. При необходимости дополнительные сведения можно почерпнуть из обзоров, распространяемых в сети.

Однако при внимательном рассмотрении рынок DLP-систем носит все признаки восточного базара времен Хивинского ханства. Разумный выбор DLP-системы на данный момент возможен только для крупных компаний с большим бюджетом. Такие компании выбирают грандов – InfoWatch, Websense или Symantec. При такой покупке главное – убедительно выступить на бюджетном комитете, вопросы реальной эффективности отходят на второй план. Надо признать к тому же, что названные системы со своей задачей справляются и не создают каких-то серьезных проблем в эксплуатации.

Увы, для средних и тем более мелких фирм такой подход неприемлем. Прежде чем вкладывать серьезные средства в развертывание DLP-системы, заказчик хотел бы иметь гарантии экономической отдачи от этих средств. С такими гарантиями далеко не все в порядке. Начнем с того, что российский рынок DLP-систем совершенно непрозрачен. Большинство компаний-поставщиков до последнего скрывают стоимость своих продуктов. Информация о ценах

отсутствует на сайтах производителей, крайне неохотно сообщается по телефону , а получение в письменном виде коммерческого предложения с указанием цены становится чем-то из разряда фантастики. Вместо всего этого поставщики предлагают организовать у заказчика некий пилотный проект, продемонстрировать свою систему и лишь затем вести переговоры о цене.

Такая секретность, вообще говоря, нетипична для рынка высокотехнологичных товаров. В подавляющем большинстве случаев поставщик отнюдь не скрывает ни цену, ни условия поставки. Даже в случае продажи разного рода модульных систем — от дорогих автомобилей до систем SAP — поставщик либо указывает диапазон цен, либо размещает в открытом доступе калькулятор, позволяющий подсчитать цену конкретной комплектации. И это вполне понятно — мало кому понравится на этапе планирования закупки руководствоваться коммерческим предложением типа «Заходи, дорогой, чаю попьем, плова поедим, систему как-нибудь продадим!». По секретным ценам продаются лишь оружие и аналогичные товары «с политическим подтекстом».

Но у поставщиков DLP-систем своя логика. Ценообразование в этой сфере навевает упорные ассоциации с восточным базаром. Более или менее открыты лишь данные об обороте компаний, но при отсутствии сведений об объемах поставок выяснить цену одной сделки не представляется возможным. Автору известен случай, когда одна уважаемая организация с государственным участием объявила об аукционе на поставку DLP-системы. В качестве начальной максимальной цены были указаны данные из вырванного буквально с мясом коммерческого предложения одного из поставщиков. В пользу данной цены приводилась вполне себе базарная аргументация со ссылками на издержки фирмы-поставщика («Не могу уступить ни таньга, о, достопочтенный! Дома меня ждут семеро голодных детей!»). Каково же было удивление покупателей, когда в ходе аукциона начальная цена была снижена в девять раз. Сделка состоялась, поставленная DLP-система функционирует, а поставщик вовсе не чувствует себя обделенным. Поневоле возникают некоторые сомнения в обоснованности первоначальной цены.

Оказалось, что такой подход к ценообразованию нельзя считать единичным случаем. Во многих российских компаниях, ставших обладателями DLP-системы, автору рассказывали об обстоятельствах покупки практически одно и то же. Представитель компании, поняв, что вместо рынка оказался на базаре, ограничивал аппетиты поставщика столь же базарными способами, ссылаясь на ограниченность бюджета. В большинстве случае сделка проходила вполне нормально.

На самом деле, несмотря на видимую анекдотичность, такая ситуация вовсе не смешна. Базарная методика согласования цен затрудняет сравнение различных продуктов, ведь цена на один и тот же товар может сильно различаться от сделки к сделке. При проведении внешнего аудита — например, при выходе на IPO — руководство компании может попасть под подозрения в получении откатов. Почему за систему заплачено N рублей, если другая фирма заплатила за ту же систему N/3? Ну и, конечно, в такой ситуации создается благоприятная почва для разного рода этически сомнительных управленческих решений.

К сожалению, сложности при закупке DLP-системы отнюдь не исчерпываются финансовыми вопросами. Встающие перед покупателем технические проблемы оказываются не менее сложными. Оказывается, что поставщики DLP-систем обычно не сообщают весьма существенных параметров своего товара. Конечно, некоторые сведения о продаваемой системе все-таки предоставляются потенциальным покупателям. Так, обычно являются общедоступными сведения о:

- перехватываемых каналах обмена данными;
- функционале рабочего места администратора безопасности;
- аппаратных требованиях к серверу безопасности;
- необходимых серверной части DLP-системы операционной системе и СУБД;
- способах установки агента на контролируемые рабочие станции;
- возможностях блокировки неправомерной активности пользователя.

Конечно, эта информация очень важна, но принимать решение о закупке системы, основываясь только на ней, было бы весьма опрометчивым. Очень хотелось бы также получить у поставщика системы такие данные, как:

- аппаратные требования к контролируемым компьютерам, в том числе процент снижения быстродействия при установке агента;
- совместимость агента с бизнес-приложениями, в том числе с антивирусными программами;
- поведение агента системы в ситуации высокой нагрузки на контролируемый компьютер (самостоятельное отключение агента, зависание компьютера, появление предупреждающих системных сообщений и т. д.);
- работа агента в автономном режиме, если контролируемый компьютер (ноутбук) выносится из офиса;
- защита агента от обнаружения пользователем контролируемого компьютера;
- возможность контроля работников IT-отдела и привилегированных пользователей;
- скорость реакции системы на действия пользователя (у некоторых систем интервал времени от осуществления пользователем контролируемого компьютера тех или иных действий до появления информации об этих действиях на сервере системы может составлять несколько часов);
- скорость обработки данных — время формирования запрошенных специалистом отчетов и поиска информации в базе;
- наличие известных способов обхода системы (например, некоторые DLP-системы не перехватывают данные, вводимые с помощью экранной клавиатуры);
- возможные сбои в работе агента (кратковременное резкое снижение быстродействия, самопроизвольные изменения настроек системы, странные системные сообщения и т. д.).

Подобную информацию — если она вообще существует — потенциальные покупатели DLP-системы вынуждены собирать самостоятельно при помощи различных форумов в сети интернет, личных связей и других столь же достоверных и надежных методов. Поставщик системы при этом, как правило, не комментирует собранную информацию.

В результате реальная эффективность приобретенной DLP-системы оказывается под вопросом и существенно зависит от продемонстрированных заказчиком до покупки навыков промышленного шпионажа. При этом можно предположить, что поставщики DLP-систем не делятся важной информацией вовсе не из жадности, а лишь потому, что и сами ею не владеют. Для сбора подобных сведений требуется расширенное тестирование, испытание на большом количестве конфигураций, возможно, даже совместные проекты с крупными компаниями производственного и финансового сектора. Между тем все это стоит денег и отодвигает дату выхода продукта на рынок. Поэтому тестирование продукта разработчиком осуществляется, как правило, на некой усредненной конфигурации. Если при таком тестировании система работает, она направляется в продажу. А дальше уже задача отдела продаж убедить заказчиков установить в своей системе нового высокотехнологичного кота в мешке. А при наличии свободного времени у разработчиков можно выслушать замечания старых клиентов и даже некоторые из них учесть при производстве новой версии. Таким образом, на покупателей DLP-систем неофициально возлагаются функции бета-тестеров. К тому же по окончании пилотного проекта бывает очень непросто расстаться с компанией-поставщиком и начать выбор системы с нуля — предстоит отчитываться перед руководством как минимум за потерянное время.

Но и это еще не все проблемы. При создании DLP-систем в погоне за производительностью ряд модулей пишется на ассемблере. Конечно, такие модули работают быстрее. Но в результате готовый продукт становится аппаратно-зависимым. Многим, вероятно, приходилось сталкиваться с удивительной ситуацией, когда в спецификации на DLP-систему указываются одни требования к аппаратной части, а в процессе подготовки сделки выясняется, что на самом деле требования совсем другие. Официально поставщик объявляет, что его продукт требует, например, операционную систему Microsoft® Windows Server 2012, 64 гигабайта оперативной памяти и 20 гигабайт на жестком диске. По факту же оказывается, что сервер должен быть строго производства компании A, иметь оперативную память строго производства компании B, причем объемом не менее 256 гигабайт, сетевые адаптеры строго фирмы C, а в качестве операционной системы требуется строго Microsoft® Windows Server 2012 R1 — и ни в коем случае не ставьте второй сервис-пак, иначе в работе системы начинаются непонятные сбои.

Поскольку эта информация обычно широко не обсуждается поставщиками, приходится самостоятельно принимать меры предосторожности. При покупке DLP-системы должно вызывать здоровую паранойю желание поставщика продать непременно аппаратно-программный комплекс целиком. Скорее всего, такое решение является аппаратно-зависимым. В результате поставленное серверное оборудование ремонту и апгрейду не подлежит, малейшее изменение аппаратной конфигурации может привести к неработоспособности всей системы.

От большинства перечисленных недостатков свободны DLP-системы экономкласса. Во всяком случае они работают практически на любом «железе» , а цены на них не являются секретом. Однако совместимость агента этих систем с бизнес-приложениями на контролируемых рабочих станциях по-прежнему никем не гарантирована и может быть проверена только в ходе самостоятельного тестирования заказчиком.

Описанные в статье трудности закупки DLP-систем приводят к весьма печальному выводу. Для приобретения не только хорошей, но и работающей именно в вашей компании системы еще до формирования бюджета предстоит провести самостоятельное тестирование нескольких систем на предмет совместимости как с программными и аппаратными компонентами на контролируемых рабочих станциях, так и с требованиями специалистов службы безопасности компании по функционалу системы. При этом все прямые и косвенные расходы на такое тестирование ложатся на бюджет компании независимо от принятия итогового решения. Желающие же сэкономить, отказавшись от собственного исследования, не должны забывать старую пословицу — скупой платит дважды. В нашем случае даже трижды: вначале за первую, непригодную для вашей компании систему, потом за тестирование и наконец за нужную систему.

Сейчас на рынке DLP-систем остро не хватает описания поставщиками предлагаемых систем по стандартному набору формальных критериев, типа приведенных выше. Поскольку сами поставщики систем не торопятся собрать данные о своем товаре, остается надеяться на независимых тестеров и других энтузиастов. Составленный ими рейтинг систем мог бы существенно оживить рынок.