PCWEEK RUSSIAN EDITION REVIEW
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И РЕШЕНИЯ ДЛЯ БИЗНЕСА
ИТ-БЕЗОПАСНОСТЬ
СЕНТЯБРЬ • 2012 • МОСКВА
http://www.pcweek.ru

Услуги в области ИТ-безопасности

ВАЛЕРИЙ ВАСИЛЬЕВ

Согласно исследованию аналитической компании IDC, объем российского рынка услуг в области информационной безопасности (ИБ) в 2011 г. составил 445 млн. долл., что на 43% превышает показатель предшествующего года. На 2012-й аналитики из IDC прогнозируют рост более чем на 30%. Таким образом, можно констатировать, что это один из наиболее быстро развивающихся сегментов ИТ-рынка России.

ОБЗОРЫ

Факторы, стимулирующие данный рост, опрошенные нами эксперты разделяют на общемировые и региональные. К общемировым они относят количественный и качественный рост кибератак. В их организации киберпреступники применяют уникальные технологии и методы, из-за чего, с одной стороны, как отметил менеджер компании ASBIS по развитию проектных решений Microsoft Андрей Пинк, значительно возросла цена утечки информации, а с другой, по словам генерального директора "McAfee в России и СНГ" Павла Эйгеса, объектами атак теперь становятся не только отдельные (в том числе и крупные) предприятия, но и целые государства.

Важным фактором роста российского ИБ-рынка служит также бóльшая осведомленность ИТ-потребителей в вопросах ИБ и их более зрелый подход к защите информации. На впечатляющие количественные показатели, зафиксированные IDC, как считает технический директор компании LETA Александр Бондаренко, оказывает влияние и то, что многие разработчики ИТ-продуктов стали встраивать в них функции безопасности, тем самым тоже демонстрируя зрелость в области ИБ. В результате в зачет объемов ИБ-рынка стали попадать и ИТ-продукты, которые раньше там не учитывались.

Из региональных факторов влияния на ИБ-рынок эксперты прежде всего называют усиление регулятивных норм в области применения информационных технологий — регламентацию работы с персональными данными, с электронными платежами, информационными и развлекательными ресурсами в Интернете.

Структура российского рынка ИБ-услуг

Как отмечает заместитель генерального директора компании "Аладдин Р.Д." Алексей Сабанов, на сегодняшний день в нашей стране не существует утвержденной классификации ИБ-услуг. Наиболее логичным, с его точки зрения, представляется разделение их на технико-аналитические, экспертно-аналитические и дополнительные.

Под технико-аналитическими ИБ-услугами он предлагает рассматривать комплексное обследование защищенности информационных систем, разработку документации, разработку, апробацию и внедрение решений по защите данных, техподдержку и сопровождение, а также установку и настройку средств защиты информации. Этот вид ИБ-услуг, по оценкам г-на Сабанова, сегодня наиболее востребован — на него, как он считает, приходится более 50% российского рынка ИБ-услуг.

К экспертно-аналитическим услугам г-н Сабанов относит анализ информационных рисков, аттестацию объектов информатизации, сертификационные испытания, расчет финансово-экономических показателей систем обеспечения безопасности информации (СОБИ), экспертизу проектов и решений. В числе дополнительных ИБ-услуг он называет консалтинг, обучение и аутсорсинг эксплуатации СОБИ.

Согласно оценкам директора по развитию бизнеса компании "Информзащита" Андрея Степаненко, около 40% российского рынка ИБ-услуг составляют услуги по внедрению и интеграции ИБ-средств, примерно треть его приходится на консалтинговые услуги, остальное — на услуги по поддержке, обучению, а также на ИБ-аутсорсинг, доля которого, как он полагает, будет расти по мере всеобщего перехода на сервисную модель обеспечения ИБ. Сегодня же, по его наблюдениям, ИБ-аутсорсинг используют наиболее зрелые в отношении ИБ заказчики.

Около 40% российского рынка ИБ-услуг составляют услуги по внедрению и интеграции ИБ-средств, примерно треть его приходится на консалтинговые услуги, остальное — на услуги по поддержке, обучению, а также на ИБ-аутсорсинг, доля которого, как он полагает, будет расти по мере всеобщего перехода на сервисную модель обеспечения ИБ.

Павел Эйгес обращает внимание на то, что в проектах по приведению ИТ- и ИБ-систем в соответствие с регулятивными требованиями необходимы этапы первоначального аудита и построения систем контроля над изменениями и отклонениями от сертифицированного состояния ИТ и ИБ. Это, по его оценкам, весьма дорогостоящие и длительные проекты. Тем не менее спрос на них значительно вырос за последние годы и будет расти и дальше.

Отмечая снижение спроса на доминировавший до недавнего времени на рынке ИБ-консалтинг, обусловленный законом "О персональных данных" (рынок сейчас находится в ожидании новых подзаконных актов), г-н Бондаренко считает, что вышедший летом прошлого года закон "О национальной платежной системе" в состоянии вернуть оживление на рынок ИБ-консалтинга. Активным спросом, по его оценкам, пользуются сегодня услуги и решения, обеспечивающие базовые потребности компаний в области ИБ, к которым следует отнести управление доступом, защиту сетей и каналов связи, защиту от утечек информации.

К этому перечню г-н Эйгес добавляет (пока еще слабо востребованные, но имеющие большие перспективы, если судить по общемировому ИБ-рынку) услуги по удалённой оценке наличия уязвимостей в корпоративной ИТ-инфраструктуре, по защите от DDoS-атак на ресурсы компаний на уровне провайдера услуг связи, защите мобильных данных (mobility data protection) на уровне операторов мобильной связи.

Андрей Пинк отмечает заметный спрос в нашей стране на антивирусную защиту как услугу, прежде всего со стороны индивидуальных российских ИТ-пользователей. Вместе с тем основными потребителями ИБ-услуг в нашей стране, по мнению г-на Сабанова, являются государственный и крупный корпоративный сектора, где системы защиты информации в основном уже построены, и нынешний рост рынка ИБ-услуг он связывает с необходимостью совершенствовать, поддерживать эти системы и управлять ими.

К важным факторам роста рынка ИБ г-н Сабанов относит также появление государственных и коммерческих услуг в электронном виде. Этот бурно развивающийся сегмент, по его мнению, требует ИБ-обеспечения, в том числе ИБ-сервисов, и одно из первых мест здесь занимает поддержка электронной подписи (ЭП). Оценивая объем рынка ИБ-услуг, он приводит такие данные. Сегодня одних только зарегистрированных удостоверяющих центров ЭП в стране насчитывается около 350, и их число продолжает расти; сервисный годовой контракт на обслуживание сертификата ключа ЭП стоит не менее 2 тыс. руб.; всего выдано свыше 3 млн. сертификатов ключей; в результате 6 млрд. руб. в сфере сервисов ИБ можно отнести только на поддержку сервиса ЭП.

Локомотивами этого рынка в ближайшие годы, по мнению г-на Сабанова, будут консалтинг, а также построение и поддержка единого пространства доверия. Последнему способствует активное развитие облачных ИТ-сервисов. Для получения доступа к ним пользователь должен будет обратиться к Единой системе идентификации и аутентификации (ЕСИА), где ему предоставляется личный кабинет. После авторизации пользователю транслируется определенный уровень доверия, в соответствии с которым он получает доступ к соответствующим этому уровню сервисам. "Ростелеком" к настоящему времени создал платформу для таких сервисов и начал набирать поставщиков услуг. По оценкам г-на Сабанова, такие сервисы появятся в стране через два-три года.

Росту рынка ИБ-услуг, как считает г-н Сабанов, способствует и тенденция к переводу обслуживания ИТ-систем на схему аутсорсинга: компании стремятся уменьшать штат ИТ-персонала, переводя его на сервисные контракты.

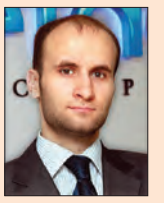
Давая свою оценку перспективам развития российского рынка ИБ-услуг, аналитик из компании "Доктор Веб" Вячеслав Медведев говорит, что появление их новых видов сомнительно, несмотря на активную рекламу. Более того, он отмечает сокращение разновидностей предоставляемых ИБ-услуг и сосредоточение провайдеров на наиболее популярных. Лидерами среди них, по его мнению, остаются интеграционные и консалтинговые, что он связывает с доминирующим у заказчиков традиционным восприятием понятия ИТ-услуги.

Преимущества и недостатки сервисной модели построения корпоративной ИБ

По мнению инженера-консультанта по информационной безопасности компании MONT Сергея Ласкина, принципиальных различий в обеспечении ИБ между традиционной и сервисной моделью нет. Если, например, требуется провести ИБ-аудит, то не имеет значения, кто его будет проводить — свой ИБ-персонал или внешний аудитор. Разве что у внешнего аудитора квалификация зачастую

ПРОДОЛЖЕНИЕ НА С. 30 ▸

Наши эксперты



АЛЕКСАНДР БОНДАРЕНКО, *технический директор, LETA*

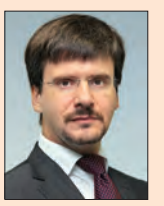
СЕРГЕЙ ЛАСКИН, *инженер-консультант по информационной безопасности, MONT*

ВЯЧЕСЛАВ МЕДВЕДЕВ, *аналитик, "Доктор Веб"*

АНДРЕЙ ПИНК, *менеджер по развитию проектных решений Microsoft, ASBIS*

АЛЕКСЕЙ САБАНОВ, *заместитель генерального директора, "Аладдин Р.Д."*

АНДРЕЙ СТЕПАНЕНКО, *директор по развитию бизнеса, "Информзащита"*



ПАВЕЛ ЭЙГЕС, *генеральный директор, "McAfee в России и СНГ"*

Подходы и механизмы снижения рисков ИБ и финансовых потерь от уязвимостей и ошибок в бизнес-приложениях

МАРИЯ КАНШИНА, МЕНЕДЖЕР ПО РАЗВИТИЮ БИЗНЕСА КОМПАНИИ "ИНФОРМЗАЩИТА"

Деятельность любой крупной организации во многом зависит от функционирования корпоративных приложений, автоматизирующих ключевые бизнес-процессы. Такие приложения содержат критичную для организации информацию (финансовую отчетность, данные о клиентах, персональные данные сотрудников и т. д.), поэтому они становятся одной из основных мишеней для атак злоумышленников. Последствиями таких атак могут стать сбои, простой информационных сервисов, потеря или утечка критичной информации — все это грозит прямыми финансовыми потерями, а также ущербом для репутации организации. Источником рисков в большинстве случаев являются ошибки и уязвимости, которые появились в ПО на разных этапах его разработки, внедрения и настройки.

Конечно, в настоящее время существуют и широко используются различные техники безопасного программирования, однако их применение не позволяет исключить влияние человеческого фактора. Также известны случаи, когда организации имели дело с преднамеренными злоумышленными программными закладками. Чтобы снизить риски возникновения уязвимостей в корпоративных бизнес-приложениях, организации следует внедрить процесс их поиска и устранения, отвечающий особенностям используемых приложений и необходимому уровню снижения риска.

Как правило, в организациях в том или ином виде уже выстроен процесс управления уязвимостями в корпоративной системе в целом. Обычно этот процесс курируется специалистами по информационной безопасности, а в качестве инструментов используются сканеры уязвимостей. Однако задача поиска и устранения уязвимостей в корпоративных бизнес-приложениях при этом решается только частично или не решается вообще, несмотря на то что многие компании самостоятельно разрабатывают приложения или заказывают их разработку, то есть имеют возможность влиять на устранение уязвимостей на самых ранних стадиях.

Чаще всего можно наблюдать один из следующих подходов.

1. **Проведение периодических внешних тестирований на проникновение (Penetration Tests)**

Данная услуга широко распространена на рынке ИБ и является возможным решением проблемы для организаций, не имеющих внутренних ресурсов для выявления уязвимостей собственными силами. Тестированию обычно подвергается уже внедренное приложение, результаты тестирования являются лишь "срезом" на конкретный момент времени и могут не выявить все имеющиеся уязвимости.

2. **Периодическое внутреннее тестирование на предмет уязвимостей**

Данное тестирование осуществляется силами внутренних экспертов либо "вручную", либо с помощью специальных решений для проведения аудита. Такие внутренние тестирования чаще всего проводятся непосредственно перед внедрением, а количество выявленных уязвимостей зависит от используемого инструмента и квалификации экспертов.

Общими недостатками обоих подходов является то, что выявление уязвимостей происходит на поздних стадиях разработки или на этапах внедрения и эксплуатации, когда процесс их устранения сопряжен с существенными затратами, а также отсутствие взаимодействия со специалистами, участвующими в разработке приложения.

Более эффективный подход заключается в построении полноценного процесса управления уязвимостями в корпоративных бизнес-приложениях, который обеспечивал бы взаимодействие всех групп специалистов на разных стадиях жизненного цикла ПО. Для этого необходимо специализированное решение или набор решений, реализующих различные методы и техники, применимые к типам бизнес-приложений, разрабатываемых и используемых в организации.

Особенно актуальным такой подход является для организаций, которые должны соблюдать требования стандартов в части обеспечения безопасности корпоративных приложений (например, PCI DSS), а также для тех, кто хочет снизить расходы на устранение уязвимостей на разных стадиях жизненного цикла ПО.

Существуют две основные технологии поиска уязвимостей в приложениях:

- статический анализ безопасности приложений (Static Application Security Testing, SAST), заключающийся в анализе исходного кода приложения на предмет уязвимостей, которые могут быть реализованы;
- динамический анализ безопасности приложений (Dynamic Application Security Testing, DAST), заключающийся в тестировании приложения на предмет уязвимостей в процессе его работы в среде функционирования с учетом всех сопутствующих факторов.

У этих технологий есть свои сильные и слабые стороны, связанные с ограничениями по типам поддерживаемых приложений, с этапами разработки, на которых они могут применяться, с возможностями точного определения причин возникновения уязвимостей и т. д. Несмотря на это, их применение является хорошей практикой для снижения потерь от ошибок в приложениях.

На текущий момент на рынке SAST/DAST присутствует широкий спектр как решений, так и сервисов различных вендоров. От простых статических анализаторов, предназначенных для поиска программных закладок, до модульных масштабируемых решений для анализа исходного кода. От простых инструментов для проведения тестирований на проникновение до сложных модульных централизованных решений для осуществления одновременного динамического анализа большого количества приложений.

Критериями выбора конкретного решения или сервиса могут стать ответы на следующие вопросы:

- каково происхождение приложений, которые будут анализироваться (собственная разработка, open source, сторонняя разработка, коммерческое ПО)?
- приложения какого типа будут анализироваться (клиент-серверные, Web-приложения, мобильные приложения и т. д.)?
- какие требования регуляторов в части обеспечения безопасности разработки приложений необходимо соблюдать?
- с какой периодичностью предполагается проводить анализ?
- кто будет конечным пользователем решения внутри организации (разработчики ПО, специалисты по ИБ, внутренние аудиторы и т. п.)?

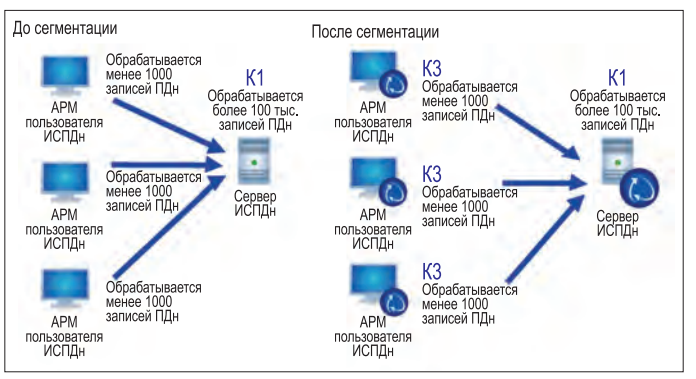
Решение или сервис, выбранные с учетом всех вышеперечисленных особенностей, позволят не просто выявить имеющиеся ошибки и уязвимости, но и снизить риски прямых финансовых потерь от последствий реализации уязвимостей в бизнес-приложениях, а также снизить затраты на их устранение за счет оптимизации процессов управления уязвимостями приложений внутри организации.

Межсетевой экран для защиты клиент-серверных ИСПДн

ОКСАНА УЛЬЯНИНКОВА, СПЕЦИАЛИСТ ПО ПРОДУКТУ TRUSTACCESS КОМПАНИИ "КОД БЕЗОПАСНОСТИ"

Довольно часто организации при выборе средств защиты информации опираются на выполнение законодательных требований, оставляя на втором плане интерфейс продукта, удобство эксплуатации, простоту управления и другие качественные характеристики решения, не связанные с защитным функционалом, определенным регулирующими органами. Представленные средства защиты информации, отвечающие требованиям законодательства, зачастую имеют громоздкий интерфейс, сложную систему управления, высокую трудоемкость настроек для получения отчетов, необходимых администратору ИБ, и требуют внесения изменений в топологию сети. Кроме того, компании, информационная система которых имеет клиент-серверную или многозвенную структуру, сталкиваются с определенными трудностями при выполнении требований законодательства в области защиты персональных данных. Трудности связаны с тем, что в этих системах персональные данные обрабатываются не только локально на компьютерах, но и на серверах баз данных, в клиентских приложениях, использующих сетевые сервисы, в веб-приложениях и т. д. Традиционные же средства защиты информации от несанкционированного доступа (НСД) ориентированы на защиту локальных ресурсов и при передаче данных по сети не обеспечивают их защиту. Кроме того, согласно требованиям приказа от 5 февраля 2010 г. № 58 ФСТЭК России, в рамках подсистемы управления доступом должна выполняться "идентификация и проверка подлинности пользователя при входе в систему информационной системы", трудности касаются также и выполнения предъявляемых требований к подсистеме регистрации и учета. Традиционные СЗИ от НСД не обеспечивают регистрацию событий, связанных с получением сетевого доступа к персональным данным в клиент-серверных и многозвенных ИСПДн.

Решением перечисленных проблем может стать использование сертифицированного межсетевого экрана TrustAccess с функцией аутентификации сетевых соединений. СЗИ TrustAccess представляет собой систему распределенных межсетевых экранов с централизованным управлением. Межсетевой экран TrustAccess имеет сертификат ФСТЭК России по уровню МЭ 2 и НДВ 4, что позволяет создавать защиту для ИСПДн до класса К1 включительно. Помимо этого TrustAccess обеспечивает эффективную защиту от большинства известных сетевых угроз, таких как Man in the Middle, подмена защищаемого объекта, replay-атака, IP-спуффинг, перехват сетевых пакетов, прослушивание сети, подмена сетевых пакетов, отказ в обслуживании. Решение также отличается широким набором защитных механизмов, среди них аутентификация сетевых соединений, фильтрация сетевых соединений, защита сетевого взаимодействия, ограничение работы по некоторым сетевым протоколам и ICMP-защита. Стоит отметить тот факт, что механизм аутентификации удостоверяет не только субъекты, но и объекты доступа, что позволяет деактуализировать угрозы, основанные на имитации (подмене) защищаемых объектов. В отличие от других средств защиты информации, также имеющих мощные защитные механизмы, TrustAccess, имея собственные механизмы аутентификации и разграничения доступа, не требует реконфигурации сетевой инфраструктуры, то есть можно использовать существующую топологию сети без внесения изменений. Для внедрения средства нет необходимости разбивать локальную сеть на сегменты, устанавливать дополнительные шлюзы и программное обеспечение. Аналогично TrustAccess не требует вносить изменения в логику работы информационных систем и менять протоколы сетевого взаимодействия компонентов информационной системы. Таким образом, защита TrustAccess является абсолютно прозрачной для приложений. Кроме того, TrustAccess обладает рядом отличительных черт, одной из которых является разграничение доступа как аутентифицированных пользователей, так и компьютеров, что выгодно отличает данный механизм от механизмов разграничения доступа, основанных на уровне только сетевых адресов и сетей TCP/IP. Правила разграничения доступа, оперирующие пользователями и компьютерами, представляют собой более совершенный механизм, учитывающий, например, перемещение пользователей с одного компьютера на другой. Особо стоит отметить пользовательский интерфейс АРМ администратора, позволяющий без труда управлять системой защиты с большим количеством защищаемых объектов. TrustAccess также позволяет настраивать необходимые отчеты событий ИБ в форматах PDF и HTML.



Снижение класса ИСПДн с помощью межсетевого экрана TrustAccess

Снижение класса ИСПДн с помощью межсетевого экрана TrustAccess

В свете необходимости привести информационные системы обработки персональных данных в соответствие с законодательными требованиями интересен сценарий использования межсетевого экрана TrustAccess для сегментирования сети. Известно, что одним из способов снижения финансовых затрат на защиту персональных данных является сегментирование сетевой ИСПДн с возможностью присвоить отдельным сегментам более низкий класс. Такой способ позволяет сократить объем обрабатываемой в ИСПДн информации, который является одним из критериев определения класса ИСПДн. В частности, снижение объемов обрабатываемых данных второй категории с более чем 100 тыс. записей до менее 1000 записей позволит понизить класс ИСПДн с К1 до К3. Очень важно, что сегментирование ИСПДн посредством сертифицированных межсетевых экранов является легитимным способом снижения класса ИСПДн. Согласно приказу 58 ФСТЭК России, "…при разделении информационной системы при помощи межсетевых экранов на отдельные части системы для указанных частей системы может устанавливаться более низкий класс, чем для информационной системы в целом".

На рисунке показан пример сегментирования ИСПДн с помощью сертифицированного межсетевого экрана TrustAccess. Оригинальная ИСПДн представляла собой многозвенную информационную систему класса К1 (в ИСПДн обрабатывается более 100 тыс. записей ПДн). Разбив систему с помощью межсетевого экрана на отдельные сегменты, рабочие станции можно классифицировать как ИСПДн класса К3, поскольку на каждой рабочей станции единовременно обрабатывается не более 1000 записей персональных данных.

"Система облачной безопасности должна быть интеллектуальной"

ПЕРЕХОД К ОБЛАЧНОЙ АРХИТЕКТУРЕ КАК ДОМИНИРУЮЩЕМУ СПОСОБУ ПОСТРОЕНИЯ И ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ТРЕБУЕТ АДЕКВАТНЫХ ИЗМЕНЕНИЙ В ОРГАНИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ИБ)

О том, как понимает эти изменения и как отвечает на современные требования к ИБ компания McAfee, один из ведущих мировых разработчиков средств защиты информации, рассказывает вице-президент McAfee по региону EMEA ***Герт-Ян Шенк****.*

Использование ИТ-ресурсов в виде облачных сервисов с каждым днем набирает обороты. А что происходит при этом с информационной безопасностью?

Действительно, облака стали для людей повседневной практикой. И главным движителем их распространения оказались конечные пользователи — идет активный процесс консьюмеризации ИТ. К примеру, облачный сервис iCloud позволяет бесплатно хранить до 5 Гб данных, и многие из нас, рядовых ИТ-пользователей, будучи представленными на одних и тех же устройствах, с одной стороны, как сотрудники компаний, а с другой, как частные лица, размещают в этом хранилище не только свою личную информацию, но и корпоративные данные: электронную почтовую переписку, деловые контакты, бизнес-документы и т. п., причем без должной защиты.

Но ведь специалисты давно уже говорят о том, что ИБ каждой технологии, каждого ИТ-продукта и решения должна закладываться на этапе их разработки. Реализуется ли этот принцип для облаков?

Компании и рядовые граждане игнорируют ИБ до тех пор, пока, как у вас говорят, не грянет гром. А сегодня в облаках "гром" уже "гремит". За последние пару лет мы оказались свидетелями утраты конфиденциальной информации многих компаний и частных граждан. Поэтому вопросам ИБ стали уделять заметно больше внимания. Если для McAfee до недавнего времени "точкой входа" к корпоративным заказчикам были ИБ-специалисты, то сегодня наряду с ними это и руководители ИТ-служб, и генеральные директора компаний, что явно свидетельствует о том, что задача ИБ стала для бизнеса одной из главных. Со своей стороны ИБ-вендоры выводят на рынок все больше средств обеспечения безопасности, разработанных специально для облаков, и они позволяют существенно снизить облачные ИБ-риски.

Однако и сложностей в облачной ИБ остается немало. Наиболее серьезной проблемой, на мой взгляд, здесь является комплексная идентификация ИТ-пользователей, учитывающая множество параметров и их изменения и характеризующая состояние, в котором пользователи находятся при обращении к ИТ-ресурсам: их ролевые полномочия, тип конечной точки доступа, место и время обращения...

В компаниях должны быть разработаны и задействованы ИБ-политики высокого уровня, блокирующие такие ситуации, когда, например, с интервалом в один час сначала регистрируется обращение сотрудника отдела кадров московской фирмы со своего настольного компьютера к системе HR, а затем его же обращение с мобильного устройства через расположенную в "Макдональдсе" Пекина точку Wi-Fi к корпоративной финансовой системе.

Существенным фактором при предоставлении облачных ИТ-услуг является также соответствие национальным нормативным требованиям. Так, по законам, действующим во многих странах (в том числе и в России), запрещены передача определенного вида данных за пределы государственной границы и ее хранение вне рубежей страны.

Герт-Ян Шенк

Таким образом, можно констатировать, что система облачной безопасности обязана быть интеллектуальной, что прежде всего подразумевает учет множества ИБ-факторов.

Два года минуло с того времени, как ваша компания была приобретена корпорацией Intel. Однако результаты этой сделки неочевидны до сих пор. Когда и каких явных её последствий можно ожидать?

Не могу с этим согласиться. После завершения сделки McAfee получила доступ к высококлассной системе управления качеством корпорации Intel, что положительно отразилось на наших бизнес-процессах, персонале, партнерах. Благодаря возможностям родительской компании существенно повысилась финансовая устойчивость McAfee, что позволило нам сосредоточить усилия на разработке новых продуктов. Расширились наши возможности по приобретению других ИБ-компаний. Совсем недавно мы совершили две такие сделки, благодаря которым удачно расширили свой продуктовый портфель. Свидетельством результативности нашей совместной работы могут служить также и новые совместные разработки DeepSAFE и Deep Command.

В DeepSAFE реализована защита вычислительных систем на уровне процессора, которая эффективнее защиты на уровне операционной системы против таких серьезных ИБ-угроз, как руткиты, целевые атаки повышенной сложности. К тому же такая защита значительно меньше нагружает вычислительные ресурсы защищаемых систем. По сравнению с другими ИБ-вендорами, которые предлагают аналогичную защиту, у McAfee есть преимущество в виде возможности наиболее глубоко проникать в архитектуру процессоров.

Продукт Deep Command использует технологию Intel Active Management Technology для удаленного управления средствами защиты конечных точек и реализации энергосберегающих режимов их эксплуатации, задействуя для этого платформу управления McAfee ePolicy Orchestrator.

Совсем недавно в московском офисе McAfee произошли изменения в руководстве. С чем это связано?

Мы начали расширять и перестраивать здешний офис с учетом его работы в ближайшее десятилетие, на протяжении которого Россия, согласно нашим планам, станет одним из ключевых регионов развития бизнеса McAfee. Это однозначно отразится на организации регионального партнерского канала. Так, в ближайшие год-два мы планируем расширить партнерский состав за счет крупных системных интеграторов. Будут увеличены вложения в подготовку специалистов компаний-партнеров, в первую очередь специалистов высшей квалификации. Предполагается ввести более четкую дифференциацию партнеров по уровням и привязку к ним соответствующих преференций.

Всем этим будет заниматься новый генеральный директор McAfee в России и СНГ Павел Эйгес — специалист, признанный высшим менеджментом McAfee и имеющий хорошие отношения с заказчиками и партнерами, понимающий, что значит занимать руководящую позицию в компании, которая предлагает рынку не отдельные ИБ-продукты, а портфель согласованных между собою компонентов, дополняющих друг друга до платформы, позволяющей развертывать ИБ-комплексы любой сложности.

В мае в нашей стране у McAfee появился новый дистрибьютор — компания ASBIS, специализирующаяся на дистрибуции розничных товаров. С чем связана ваша активизация в России в области антивирусных продуктов для домашних пользователей?

Мы давно работаем на консьюмерском направлении — в общий доход компании оно приносит более одной трети. По нашим оценкам, консьюмерский российский компьютерный рынок растет сегодня быстрее, чем во многих других странах. Разумеется, это стимулирует наш интерес к нему, и если до недавнего времени мы были сосредоточены в России на сегменте корпоративных заказчиков, то сегодня видим условия для работы на всем российском ИБ-рынке. Для розницы у нас есть интересные, как мне кажется, предложения, такие, например, как семейная лицензия, предоставляющая пакет средств защиты сразу на настольный компьютер, планшет и смартфон. Если у корпоративного клиента установлены наши средства защиты, то мы предлагаем его персоналу специальные цены на домашние продукты. При этом мы прекрасно понимаем, что работа на розничном рынке весьма способствует узнаваемости бренда компании.

В последние два года ваш московский офис активно занимался сертификацией продуктов McAfee на соответствие требованиям российских норм, действующих в области ИБ. Каковы результаты этих усилий?

Уже получены сертификаты на соответствие ТУ (Техническим условиям) для решений Host DLP и Total Protection for Endpoint (TEN), включающий в себя антивирус для конечных точек. В течение ближайших полутора месяцев ожидается получение сертификата на соответствие требованиям НДВ (проверка отсутствия недекларированных возможностей) 4-го уровня для Hist DLP, в конце 2012 года ожидается такой же сертификат для TEN. Также запущен процесс сертификации решения IPS на соответствие требованиям профиля защиты систем обнаружения вторжений уровня сети пятого класса защиты.

Услуги...

◂ ПРОДОЛЖЕНИЕ СО С. 27

(благодаря специализации) выше, зато возникает проблема доверия к его сотрудникам, которые будут проводить проверки, полагает он.

Другие наши эксперты не согласны с такой оценкой. Так, г-н Эйгес указывает на принципиальные различия между этими двумя моделями, связанные прежде всего с затратами (покупая ИБ в качестве сервиса, организация платит только за саму услугу, не делая существенных инвестиций в инфраструктуру), а также с гораздо более высокой надёжностью второй модели. По его словам, сервисная модель — не простая замена реализованных собственными силами ИБ-сервисов, а перевод их на качественно более высокий уровень с одновременным снижением расходов.

С поправкой на дефицит квалифицированных ИБ-специалистов, с учетом бюджета и размеров бизнеса заказчика г-н Пинк тоже считает сервисный вариант более выгодным для большей части компаний.

Согласно наблюдениям г-на Бондаренко, в традиционной модели построения ИБ корпоративной службе информационной безопасности выделяется определенный бюджет, который далеко не всегда соответствует потребностям бизнеса и существующим рискам (с погрешностями как в большую, так и в меньшую сторону), а ИБ-служба, в свою очередь, выполняет только те функции, которые она может выполнить исходя из имеющегося бюджета. Сервисная же модель предполагает четкое формулирование ожиданий бизнеса от функции безопасности и оплату только использованных сервисов.

В числе очевидных преимуществ сервисной модели г-н Степаненко называет возможность компании-заказчика сосредоточиться на своих непосредственных бизнес-задачах и отказаться от вспомогательных (к которым относится и ИБ), сокращение расходов на обучение и удержание ИБ-специалистов, задействованных в эксплуатации ИБ-средств, появление рычагов, позволяющих требовать от провайдера гарантированное качество ИБ-услуг, в виде договора на уровень качества обслуживания (SLA).

Обращаясь к проблемам перехода на сервисную модель обеспечения ИБ, г-н Степаненко указывает на то, что она, в отличие от сервисной модели потребления ИТ, крайне редко дает возможность оказывать прямое влияние на качество бизнес-сервисов и оперировать бизнес-терминологией, на которой как раз и строится обоснование внедрения сервисной модели. Поэтому иногда сложно обосновать финансовую выгоду от ИБ-сервиса.

По мнению г-на Медведева, использование сервисной модели требует гораздо более серьезной, чем традиционная модель, проработки документального оформления отношений между поставщиком и потребителем ИБ-услуги.

Подчеркивая этот же аспект, г-н Сабанов утверждает, что для правильного документального оформления таких отношений клиенты должны иметь в своем штате ИБ-специалистов очень высокой квалификации. Основная их задача заключается в том, чтобы составлять договоры SLA таким образом, чтобы интересы всех участников процесса поставки и потребления ИБ-сервиса были сбалансированными.

Организационно-технические аспекты предоставления ИБ-услуг

Переход на сервисную модель обеспечения ИБ в нашей стране, по мнению г-на Бондаренко, серьезно осложнен тем, что во многих организациях и компаниях даже ключевые бизнес-процессы пока не используют сервисные подходы. Поэтому говорить о сервисном подходе в ИБ еще рано. До недавнего времени вопросы обеспечения информационной безопасности вообще воспринимались бизнесом как часть задач ИТ-подразделения, причем далеко не самая важная.

К тому же сервисная модель, как подчеркивает г-н Бондаренко, предполагает участие сторонней компании в таком чувствительном для бизнеса вопросе, как ИБ. Здесь на первый план выходит вопрос доверия, а значит, нужны какие-то серьезные механизмы обеспечения этого доверия на рынке (такие, например, как сертификация), которые пока не созданы.

Серьёзную зависимость от провайдера ИБ-услуг г-н Степаненко определяет как оборотную сторону сервисной модели обеспечения ИБ. Положившись на поставщика ИБ-услуг, компания, отмечает он, в случае неудачного опыта будет испытывать сложности со сменой провайдера. Возврат же к прежней, традиционной модели обеспечения ИБ будет значительно затруднен в силу утраты собственных высококвалифицированных специалистов и соответственно внутренних компетенций в области информационной безопасности.

Среди наиболее очевидных причин, сдерживающих распространение потребления ИБ как сервиса в России, наши эксперты называют явный дефицит подготовленных специалистов, которым предстоит работать на стороне ИБ-провайдеров, а также недостаточный уровень проникновения широкополосного доступа в Интернет в регионах.

Временной, но существенной причиной, препятствующей распространению сервисной модели ИБ, является кризисная ситуация в мировой экономике, на что обращает внимание г-н Ласкин. В таких условиях компании стараются экономить ресурсы, используют проверенные способы ведения бизнеса и неохотно идут на какие-либо новации.

В то же время, как полагает г-н Бондаренко, многие российские интеграторы готовы предложить своим клиентам сервисную модель предоставления услуг по обеспечению корпоративной ИБ. Хотя, по мнению г-на Эйгеса, при этом они должны будут использовать зарубежные разработки и действовать им придется в жесткой конкуренции с зарубежными провайдерами, особенно если дело касается высокопроизводительных, надёжных, полнофункциональных облачных ИБ-решений для крупных заказчиков, поскольку ИБ-решений мирового уровня, как он считает, российские производители предложить рынку не могут.

Скептически оценивает готовность инфраструктуры нашей страны к переходу на сервисную модель ИБ г-н Сабанов, отмечая отсутствие регулирования и стандартизации в этой области. Он считает, что это мешает объективно сравнить многие имеющиеся на рынке технологии и решения. По его мнению, действующая в стране система сертификации до некоторой степени условна, поскольку вендоры часто сами пишут технические условия (ТУ), которым должен отвечать их продукт, и сертифицируют его именно по этим ТУ. Что же касается более универсальной сертификации ИБ-продуктов на соответствие общим руководящим документам, то делают это далеко не все ИБ-производители. В результате из-за отсутствия объективного сравнения (в принципе, его должен проводить какой-либо независимый институт, который еще нужно создать) заказчикам зачастую приходится поочередно внедрять несколько однородных решений от разных поставщиков.

Говоря об ИБ-услугах, г-н Сабанов обращается к вопросу их качества — надежности, доступности, времени отклика на запросы заказчика и т. д. Качество, по его мнению, должно измеряться по утвержденным стандартам, требованиям и т. п., которых, увы, сегодня нет, и SLA-договоры заключаются согласно сложившейся практике в том виде, в котором их составляют сами поставщики услуг, что, считает г-н Сабанов, не совсем правильно. Он предполагает, что в практике предоставления ИБ-услуг адекватная система качества появится только через несколько лет.

Наши эксперты обращают внимание на то, что переводу на сервисную модель поддаются не все функции ИБ — всегда останутся наиболее критичные бизнес-компоненты, процессы, данные, ИБ-обеспечение которых компании не захотят передавать на сторону. Поэтому они полагают, что наилучшего результата в организации ИБ можно добиться только в том случае, если сочетать работу собственных ИБ-специалистов (численность которых в сервисной модели резко сокращается, зато характер работы меняется на экспертно-управленческий и резко возрастают требования к их квалификации) с ИБ-услугами внешнего провайдера (которому перепоручаются рутинные ИБ-задачи).

Пока же приходится констатировать, что сегодня построение корпоративной ИБ по сервисной модели происходит в условиях, когда невозможно в достаточной степени документально подтвердить требуемые гарантии качества обслуживания, а значит, со стороны заказчика предполагается некоторая доля авантюризма.