PCWEEK RUSSIAN EDITION REVIEW
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И РЕШЕНИЯ ДЛЯ БИЗНЕСА
ИТ-БЕЗОПАСНОСТЬ
МАЙ • 2013 • МОСКВА
http://www.pcweek.ru

О защите виртуализированных сред

ВАЛЕРИЙ ВАСИЛЬЕВ

Согласно результатам международного опроса, проведенного IDC в 2012 г., среди своих наиважнейших задач ИТ-руководители выдвигают на первое место консолидацию серверов и их виртуализацию. Результаты исследований этой же аналитической компании, завершенные в IV квартале 2012 г., показывают, что в России виртуализацией охвачено более 25% серверов. Это несколько больше, чем в США, и немногим меньше, чем в Германии и Великобритании.

ОБЗОРЫ

Начав с серверов и убедившись на практике в эффективности применения виртуализации в ИТ-инфраструктуре, заказчики стали распространять эту технологию на рабочие места, сетевой компонент ИТ-инфраструктуры и системы хранения данных (СХД).

Однако наряду с явными выгодами виртуализация привнесла новые, связанные с обеспечением информационной безопасности (ИБ), проблемы, специфичные для применения данной технологии в ИТ-среде. Эти проблемы можно разделить на две части: технологическую и организационную.

В нашем обзоре мы рассмотрим основные технологические особенности организации защиты составляющих ИТ-инфраструктуры — серверов, рабочих мест, корпоративной сети и систем хранения данных, которые связаны с виртуализацией этой инфраструктуры. Мы постараемся дать оценку состояния рынка средств защиты виртуализированных ИТ-ресурсов и опыта их применения, а также охарактеризуем действующую в нашей стране нормативно-правовую базу, относящуюся к аспектам регулирования использования виртуализации с позиций ИБ.

Уровень проникновения и перспективы виртуализации ИТ в России

Если объединить результаты исследований IDC с данными "Лаборатории Касперского", то можно сделать вывод, что не позднее чем через год серверную виртуализацию будут использовать более половины российских предприятий и организаций разных масштабов. При этом, как утверждает Михаил Чернышев, прогресс очевиден не только в традиционно благополучных для распространения современных технологий регионах вроде Москвы или Санкт-Петербурга — он наблюдает это практически повсюду, где в стране есть предприятия среднего и крупного масштаба (именно выйдя на такой уровень, компании, как правило, и начинают задумываться об экономии ИТ-ресурсов и повышении надежности).

Согласно наблюдениям Константина Воронкова, большая часть серверных приложений, которые компании используют сегодня в виртуальных средах (ВС), являются критически важными для бизнеса (это базы данных, электронная почта, системы ERP, CRM и т. п.), что резко отличается от ситуации, которая наблюдалась несколькими годами ранее, когда виртуализация только начинала обретать популярность и предприятия переносили в виртуальную среду свои наименее критичные приложения. Массовая виртуализация критически важных бизнес-приложений свидетельствует, как полагает г-н Воронков, о доверии заказчиков к этой технологии, а также о достижении определенного уровня зрелости самой технологии.

Виртуализация инфраструктуры рабочих станций (VDI), согласно данным "Лаборатории Касперского", пока не получила в нашей стране широкого распространения. Эксперты "Лаборатории" объясняют это тем, что VDI обычно используется в тех компаниях, чьи сотрудники выполняют типовые, строго регламентированные задачи (как, например, сотрудники call-центров, операционисты в банках, служащие многих государственных организаций).

Следует отметить, что потребность в таких рабочих местах испытывают далеко не все заказчики. Тем не менее по мере того, как технологии виртуализации рабочих станций совершенствуются, российские компании (в первую очередь крупные) всё чаще проводят пилотные внедрения VDI. В целом нынешнее положение виртуализации рабочих мест специалисты "Лаборатории Касперского" в нашей стране рассматривают как стартовое и предполагают активный рост количества внедрений решений виртуализации рабочих станций в близкой перспективе.

Основываясь на своем опыте проектной деятельности и обследования объектов ИТ и ИБ, Сергей Панин оценивает проникновение платформ виртуальных сред в России в сегментах среднего и крупного частного бизнеса примерно в 85%. Он также отмечет, что понимание преимуществ использования виртуализации есть и у российских государственных организаций. Так, проведенный им анализ сайта государственных закупок показывает большой рост количества заказов как на проектирование и внедрение виртуальных сред, так и на поставку неисключительных прав использования лицензионных виртуальных сред. При этом, как он отмечает, если не в первом же заказе, то в последующих заказчики поднимают вопрос о защите закупаемых решений.

Проникновение виртуализации в корпоративную ИТ-среду в целом в нашей стране Дмитрий Когай оценивает в 10—15% и полагает, что по этому показателю Россия существенно проигрывает экономически развитым странам. Вместе с тем темпы, которыми растет это ИТ-направление, превышают, по его мнению, таковые по ИТ-отрасли в целом. Ссылаясь на данные аналитиков из IDC, он прогнозирует, что в течение пяти ближайших лет Россия может выйти на 70% виртуализации всей ИТ-инфраструктуры.

Алексей Сабанов полагает, что виртуализация, несмотря на громкую рекламу, на практике пока еще используется слабо; в настоящее время идет тестирование технологии, устраняются нестыковки средств виртуализации разных производителей, в виртуальную среду переведено не более 8% бизнес-процессов, причем в основном в частные, полностью подконтрольные владельцам этих бизнес-процессов, виртуальные среды.

Солидарен с Алексеем Сабановым в оценке уровня проникновения средств виртуализации ИТ-ресурсов в России Вячеслав Медведев. По его мнению, этот показатель остается все еще достаточно низким. Г-н Медведев отмечает, что существует большое количество предложений по переводу всей или части ИТ-инфраструктуры в облачные структуры — частные, глобальные, гибридные. Но этих предложений, считает он, явно недостаточно для покрытия всей территории нашей страны. Но самое главное заключается в том, что потенциальные клиенты облачных ИТ-сервисов опасаются трудностей, появляющихся при переводе ИТ в облака, и прежде всего их пугает отсутствие финансовой ответственности поставщиков облачных услуг в случае возникновения различного рода ИБ-проблем, включая прерывание доступа к ИТ-сервисам и т. п. В дополнение к этому они предполагают рост затрат на безопасность, который обычно связывают с появлением новых рисков, присущих виртуализации и облачным технологиям.

К факторам, сдерживающим распространение виртуализации, Николай Романов помимо финансового аспекта относит необходимость существенного расширения систем хранения данных под виртуализацию и тщательную оценку возможных сценариев использования. Он обращает внимание на то, что до сих пор не все приложения и системы (например, графические системы, а также СХД сами по себе) могут быть перенесены в виртуальную среду. Что касается виртуализации корпоративных сетей, то это направление он оценивает как находящееся в начальной стадии.

Особенности обеспечения ИБ виртуализированных ИТ-сред

Опросы показывают, что более половины ИТ-специалистов все еще оценивают ИБ-риски для виртуализированных ИТ-ресурсов как более низкие, чем для физических. Тем, кто так считает, Алексей Воронцов напоминает, что только в идеале виртуализация позволяет строить потенциально более защищенные (по сравнению с невиртуализированными) ИТ-системы за счет грамотного применения изоляции сервисов в отдельных виртуальных машинах и возможностей фильтрации, предоставляемых виртуализированной сетевой инфраструктурой. В реальности же ситуация выглядит иначе. Виртуализированная ИТ-среда подвержена тем же угрозам, что и физическая. Кроме того, ей присущи и специфические, связанные с технологическими особенностями, уязвимости. Так, простота развертывания виртуальных машин (ВМ) приводит к тому, что обновления антивирусов и патчи на программное обеспечение не устанавливаются, а традиционные средства обнаружения сетевых атак и сетевые экраны не видят трафик внутри виртуальной сети.

Константин Воронков, в свою очередь, напоминает, что любая атака на физическую инфраструктуру может быть в итоге нацелена на виртуальные машины, и для ее проведения злоумышленникам про-

ПРОДОЛЖЕНИЕ НА С. 18 ▸

Наши эксперты

ИВАН БОЙЦОВ, *аналитик, "Код Безопасности"*

КОНСТАНТИН ВОРОНКОВ, *руководитель группы, "Лаборатория Касперского"*

АЛЕКСЕЙ ВОРОНЦОВ, *технический специалист по ПО безопасности, IBM*

ДМИТРИЙ КОГАЙ, *менеджер по продукту, "Аванпост"*

ВЯЧЕСЛАВ МЕДВЕДЕВ, *старший аналитик отдела развития, "Доктор Веб"*

СЕРГЕЙ ПАНИН, *инженер по системам информационной безопасности, LETA*

НИКОЛАЙ РОМАНОВ, *технический консультант, Trend Micro в России и странах СНГ*

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

ЕЛИЗАВЕТА СПАСЕННЫХ, *менеджер по развитию бизнеса, "Информзащита"*

МИХАИЛ ЧЕРНЫШЕВ, *технический консультант, McAfee в России и СНГ*

Проблемы защиты виртуализованных ИТ-сред

ИВАН ДУДОРОВ, МЕНЕДЖЕР ПО ПРОДУКТУ КОМПАНИИ "КОД БЕЗОПАСНОСТИ"

Основные меры по защите виртуальной инфраструктуры (ВИ) складываются как из специфики работы самой виртуальной среды, так и из особенностей обрабатываемой в ней информации. Стандартные подходы для защиты физических сред в данном случае малоприменимы: существует целый ряд специфических угроз, которые необходимо принимать во внимание при построении контура защиты виртуальной инфраструктуры.

Представьте себе ситуацию, когда администратор ВИ имеет доступ и к средствам управления виртуальной машиной (ВМ) и к обрабатываемым ею данным. При этом он может скопировать образ ВМ на какой-либо внешний носитель и вынести его за пределы защищаемого периметра, тем самым получив возможность извлечения любых данных из этого образа. Таким образом, любые конфиденциальные сведения будут скомпрометированы так называемым "суперпользователем".

Другой опасной ситуацией может стать атака на сервер виртуализации и соответственно компрометация всех развернутых на нем ВМ. Уязвимым участком виртуальной инфраструктуры является и обмен между ВМ и хостом. Нередки также ситуации, когда на одном сервере развернуты несколько ВМ с различными уровнями конфиденциальности, в результате чего атака на менее защищенную машину может быть использована в качестве одного из этапов для атаки на ВМ с более высоким уровнем доступа. А ведь отследить взаимодействие между ВМ с помощью стандартного межсетевого экрана попросту невозможно. В целом, если речь идет о защите ВИ, нельзя забывать о защите и более низкого уровня, физического, на котором происходит развертывание системы, так как виртуальная среда воспринимает этот уровень как доверенный. Другими словами, вопросы защиты серверов виртуализации от НСД, сегментация сетевой инфраструктуры и прочие атрибуты ИБ должны быть реализованы заранее, иначе теряется весь смысл защиты виртуализации. Не стоит также сбрасывать со счетов возможные атаки на вспомогательные компоненты ВИ, такие как средства репликации и СХД.

Существует и другая сторона рассматриваемого вопроса — нормативно-правовая, касающаяся регулирования информационной безопасности в сфере виртуализации. В декабре 2012 г. ФСТЭК России опубликовала два проекта приказов: "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" и "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных". Первый документ касается далеко не всех, а вот на второй следует обратить внимание большинству компаний: впервые в нормативно-правовых документах были определены 11 мер по защите среды виртуализации, включающие в себя аутентификацию компонентов, контроль и разграничение доступа, резервное копирование данных, контроль целостности, сегментирование ВИ и т. д. Можно быть уверенным, что в той или иной степени эти меры войдут и в окончательную версию приказа, а это означает последующую необходимость приведения в соответствие с законодательством виртуальных инфраструктур многих компаний с помощью сертифицированных средств защиты.

К сожалению, защита с помощью встроенных возможностей платформы виртуализации, даже будучи сертифицированной, зачастую является либо недостаточной для реализации требуемых мер, либо ее настройка и дальнейшее обслуживание оказываются нетривиальными и ресурсоемкими. Каким образом привести все в соответствие, если встроенных возможностей платформы виртуализации недостаточно? Один из наиболее эффективных вариантов — применить специализированные средства защиты от несанкционированного доступа (НСД) для ВИ. Такие средства защиты не только способны обезопасить среду виртуализации и контролировать ее состояние в будущем, но и, как правило, обладают соответствующими сертификатами ФСТЭК России. Кроме того, эти средства располагают достаточным функционалом, чтобы "закрывать" большую часть перечисленных в проекте приказа ФСТЭК России требований. Однако не стоит забывать про резервное копирование, распределенное хранение данных и восстановление информации, антивирусную защиту и обнаружение вторжений — эти функции также являются неотъемлемой частью общей концепции и требуют принятия мер ИБ.

Сегодня производители специализированных СЗИ для защиты ВИ частично предлагают требуемые продукты (например, средства доверенной загрузки сервера виртуализации), но речь о едином законченном решении от одного вендора здесь не идет. В результате очень часто приходится "городить огород", развертывая антивирус, IDS/IPS, средства защиты ВИ и т. д. от абсолютно разных поставщиков без возможности объединения их в единую консоль управления. К чему это приводит — говорить, полагаю, не нужно. Поэтому на данный момент среди самых перспективных направлений в разработке решений можно назвать создание некой "экосистемы безопасности", позволяющей гибко управлять политиками ИБ не только в сфере виртуализации, но и во всех смежных областях, таких как защита физической инфраструктуры, включая серверы, АРМ и информационные каналы данных. В конце концов, защита любого объекта должна быть комплексной, а развертывание, управление и мониторинг ИБ из единого графического интерфейса с помощью заранее созданных профилей безопасности — мечта любого администратора.

Применяя такой универсальный инструмент, можно было бы в несколько кликов получить защищенную виртуальную среду с четким контролем и мониторингом всех производимых администраторами и пользователями действий. И одновременно привести автоматизированную систему в соответствие с требованиями российского законодательства и зарубежных рекомендательных документов, таких как PCI DSS или VMware Security Hardening Guide. Однако в настоящий момент приходится ограничиваться отдельными сертифицированными средствами защиты от разных производителей и комбинировать их оптимальным способом под специфику работы компании. Будем надеяться, что в ближайшее время на российском рынке все же произойдут соответствующие изменения и мы сможем увидеть единое решение, закрывающее широкий спектр проблем в сфере ИБ.

СПЕЦПРОЕКТ КОМПАНИИ "КОД БЕЗОПАСНОСТИ"

О защите...

◂ ПРОДОЛЖЕНИЕ СО С. 17

ще использовать обычные уязвимости ИТ-инфраструктуры, нежели вести дорогостоящие разработки специализированных средств, ориентированных именно на виртуальные среды.

Как утверждает Дмитрий Когай, в виртуализированной среде периметр защиты должен создаваться вокруг каждой отдельной ВМ и независимо от ее перемещения следовать за нею.

Иван Бойцов предлагает разделять ИБ-угрозы, свойственные для виртуализированной ИТ-среды, на несколько групп. К первой группе он относит угрозы аппаратному обеспечению, на котором развертываются компоненты ВС. Это угрозы, знакомые большинству ИБ-специалистов: физические повреждения или несанкционированные изменения аппаратного обеспечения, его кража или уничтожение, нарушения в сетевой инфраструктуре, стихийные бедствия и аварии и т. д. Компоненты виртуальной инфраструктуры должны поддерживать кластеризацию, шифрование данных и другие стандартные способы защиты от подобных угроз.

Другую группу, по мнению г-на Бойцова, составляют угрозы гипервизору. Это их новый вид, включающий угрозы, связанные с особенностями эксплуатации ВС: ошибки в настройках гипервизора, виртуальных машин и других компонентов ВС, уязвимости в программных кодах гипервизора, подмена его компонентов, атаки типа "отказ в обслуживании", несанкционированный доступ к файлам образов ВМ. Эти угрозы он рекомендует закрывать программным обеспечением гипервизора и дополнительными средствами защиты ВС.

В отдельную группу г-н Бойцов выделяет угрозы системе управления виртуализированной ИТ-средой: несанкционированный доступ к системе управления, отсутствие разделения доступа между администраторами ВС или неправильная настройка такого разделения. Против них он рекомендует использовать усиленные механизмы аутентификации и разграничения доступа.

Еще одну группу, как считает г-н Бойцов, образуют угрозы виртуальным машинам. Они похожи на угрозы физическим серверам и рабочим станциям, к которым добавляются угрозы, связанные с виртуализацией аппаратного обеспечения в виртуальных машинах, в том числе и системы BIOS. В числе таких угроз — несанкционированная загрузка, остановка и выключение виртуальных машин, загрузка ВМ со стороннего носителя, изменение и подмена файлов образов ВМ, несанкционированное изменение конфигурации виртуальных машин. Для эффективной борьбы с угрозами такого рода он рекомендует механизмы контроля целостности и доверенной загрузки виртуальных машин.

Наконец, для сети передачи данных и систем хранения данных г-н Бойцов видит угрозы, типичные для аппаратной части, и угрозы, направленные на получение несанкционированного доступа к управлению этими компонентами.

Николай Романов обращает внимание на то, что в каждом из сегментов виртуальной среды есть свои болевые точки и что ранжировать риски, связанные с информационной безопасностью, имеет смысл по типу эксплуатации виртуализированных систем. С учетом специфики серверных платформ он прежде всего выделяет те, на которых базируются публичные сервисы (в первую очередь веб-серверы). Наряду с основными механизмами периметровой защиты на сетевом уровне (системами предотвращения вторжений, средствами защиты от DoS-атак) такие системы должны иметь аналогичные средства, работающие непосредственно в той среде, где они работают. Подобная методика позволяет закрыть тот спектр угроз, против которых типовые средства могут быть малоэффективны (контроль внутри гипервизора как на файловом, так и на сетевом уровне).

Отмечая, что переход к ВС породил ряд специфических ИБ-проблем, которые не связаны с типом сервисов, г-н Романов указывает на то, что безопасность в классическом понимании (блокирование уязвимостей без установки патчей средствами систем предотвращения вторжений, защита от вирусов, сбор данных о несанкционированных изменениях и др.) была расширена на уровне защиты от несанкционированного доступа в границах эксплуатации виртуализированных систем, обеспечивающем как возможности мандатного разграничения доступа к ВС, так и контроль целостности самого гипервизора.

На примере антивируса Константин Воронков поясняет возможные издержки применения традиционных средств защиты в ВС. Он утверждает, что традиционное антивирусное решение может защитить и виртуализированную ИТ-среду, однако при этом оно потребует установки антивирусных агентов, что означает развертывание антивирусного ядра и сигнатурных баз на каждой виртуальной машине. Это вызовет необходимость избыточного использования ресурсов памяти, дискового пространства и процессора хост-сервера, что практически сведет на нет одно из основных преимуществ виртуализации — эффективное использование вычислительных ресурсов.

Созданные специально для защиты ВС виртуальные устройства (Virtual Appliance) безопасности обеспечивают безагентную антивирусную защиту сразу нескольких виртуальных машин. В этом случае антивирус работает на уровне гипервизора. Перенос антивирусной защиты на специально выделенное устройство существенно снижает расходование системных ресурсов, повышает производительность аппаратного обеспечения и увеличивает плотность ВМ на хост-сервере.

Вместе с тем, как отмечает Константин Воронков, применение специализированных средств защиты ВС нередко приводит к появлению дополнительных консолей управления, что увеличивает нагрузку на администраторов и расходы.

По мнению Ивана Бойцова, большинство архитектурных и технологических сложностей в реализации защиты виртуализированных ИТ-сред уже преодолены, а те, что остались, связаны с закрытостью средств виртуализации, отсутствием необходимых для ИБ-вендоров инструментов API и SDK и другими проблемами, касающимися проприетарности платформ виртуализации.

Алексей Воронцов указывает не только на нехватку таких инструментов, как интерфейсы прикладного программирования (API) и пакеты программ для разработки приложений (SDK), но и на необходимость единого стандарта доступа для средств защиты к ВС. Он обращает внимание на то, что у каждого поставщика гипервизоров свои подходы к формированию ВС и ИБ-вендорам приходится ориентироваться на конкретные архитектуры.

Наиболее уязвимые компоненты ВС

Несмотря на отсутствие информации о реальных ИБ-инцидентах, связанных с нарушением защищенности гипервизора, наши эксперты рекомендуют при решении вопросов обеспечения информационной безопасности уделять ▸

Враг в кармане

ВЯЧЕСЛАВ МЕДВЕДЕВ, СТАРШИЙ АНАЛИТИК ОТДЕЛА РАЗВИТИЯ КОМПАНИИ "ДОКТОР ВЕБ"

В последние годы мобильные устройства неожиданно для многих обзавелись широким функционалом. Еще какие-то пять лет назад максимум, что можно было делать с их помощью, — это запускать простейшие игрушки на java и менять мелодии. Современные смартфоны — это процессоры, превосходящие по мощности процессоры настольных компьютеров, считавшихся топовыми еще совсем недавно, большой объем памяти, современная удобная операционная система, которую дополняют все необходимые для повседневной работы офисные приложения и большое количество игровых программ.

Все больше сотрудников компаний имеют такие "продвинутые" смартфоны, все чаще эти мобильные устройства используются для работы. Бизнесу это выгодно — сотрудники постоянно находятся на связи, больше времени отдают работе и т. д.

Есть ли в данном случае "но"? Да, и огромное! Эти устройства, как правило, принадлежат самим сотрудникам, а не компании — практика раздачи корпоративных устройств распространена, но далеко не общепринята. Личные устройства зачастую никак не защищены от злоумышленников. Немного статистики на основе нескольких исследований, представленных в публичных источниках:

- 40% планшетов не имеют никакой защиты (в том числе и iPad'ы);
- 48% работников пытаются обходить требования безопасности;
- только 21% работников координируют свои действия с ИТ-отделом.

Было бы странно, если бы злоумышленники не попытались выйти на этот рынок. Поначалу их попытки были достаточно робкими — вплоть до того, что вредоносные программы распространялись с инструкциями по их установке. Когда появились первые вирусы под Android — и соответственно первые антивирусы для противодействия им — многие не верили в саму возможность угроз.

Уверенные в безопасности своих устройств и доверяющие компании-производителю пользователи даже в те далекие времена активно участвовали в распространении вирусов. Только для одного такого вируса Android.Plankton.1 (его функцией был сбор и передача информации об устройстве злоумышленнику) было зарегистрировано 150 000 загрузок с Android Market.

Но постепенно возможности "мобильных" вредоносных программ росли, и сейчас уже всё "по-взрослому": для заражения зачастую достаточно зайти не на тот сайт или подключиться к зараженному компьютеру — и там, и там устройство уже ждут с распростертыми объятиями. Вот что могут современные вредоносные программы на вашем мобильном устройстве: блокировать телефон; звонить и производить несанкционированную рассылку СМС-сообщений по команде от сервера; отслеживать входящие и исходящие телефонные звонки; собирать и переправлять "куда надо" фотографии, хранящиеся на телефоне, отправляемые и получаемые почтовые сообщения, используемые пароли, СМС-сообщения, набираемый на клавиатуре текст, GPS-координаты; включать динамик без ведома пользователя.

Вы проводите совещание? Ваш Android к услугам злоумышленников — все переговоры будут записаны. Во время переговоров вы кладете свое мобильное устройство перед собой? Отлично, фотографии участников уйдут заказчикам слежки за вами. Нужно обыскать или ограбить офис или вашу квартиру? Android подскажет, где вы находитесь, и поможет спланировать преступление.

Думаете, это всё? Мобильные устройства на данный момент предоставляют злоумышленникам куда больше возможностей, чем обычные компьютеры.

Компания работает с системами дистанционного банковского обслуживания и получает подтверждения в СМС? У вас есть счет в банке и/или пластиковая карта и вы что-то оплачиваете с мобильного устройства? Ваши деньги — это именно то, что нужно криминальным структурам. Просим не любить и не жаловать: Android.SpyEye.2.origin, Android.Panda.2.origin, Android.SmsSpy.6.origin и Android.FakeSber.1.origin.

Для обеспечения безопасности финансовых операций в Интернете банковские системы отправляют СМС-сообщения с кодами подтверждения на привязанный к клиентскому счету номер мобильного телефона. Чтобы успешно завершить транзакцию, пользователь должен ввести в специальную веб-форму полученный код. Мобильные банковские троянцы предназначены для перехвата СМС-сообщений, передачи mTAN-кодов злоумышленникам, которые выполняют различные финансовые операции с электронными счетами ничего не подозревающих жертв.

Типичный способ распространения таких вредоносных программ — социальная инженерия. А Android.FakeSber.1.origin — первый Android-троянец, направленный против клиентов российского банка, — был даже помещен злоумышленниками непосредственно в официальный каталог приложений Google play. Троянец работал не сам по себе, а "в паре" со знаменитым Trojan.Carberp.

Необходимо отметить, что большая часть вредоносных программ создается для долговременного незаметного пребывания на зараженном компьютере — "доить" постепенно всегда выгоднее и безопаснее, чем сразу попытаться увести все деньги. Заметить их неподготовленному пользователю невозможно. К такому ПО, кроме уже упоминавшихся банковских троянцев, относятся шпионские программы и ПО, разработанное для проведения APT-атак. Так, Android.Luckycat.origin должен был обеспечивать не только сбор данных с зараженного устройства, загрузку различных файлов с мобильного устройства и на него, но и выполнение команд, поступающих с управляющего сервера. Android.MailSteal.1.origin, Android.Maxbet.1.origin, Android.Loozfon.origin и Android.EmailSpy.origin собирали всю информацию из телефонной книги (включая адреса электронной почты), а также идентификаторы устройства.

Прогресс криминальных структур хорошо иллюстрирует развитие СМС-троянцев, ведущих свою родословную от Android.SmsSend, появившегося еще в 2010 г. Эти вредоносные программы предназначены для отправки дорогостоящих СМС-сообщений и подписки абонентов на различные контент-услуги.

Количество зараженных мобильных устройств все время увеличивается — в прошлом году появились сообщения о создании первых бот-сетей на основе Android. Теперь DoS-атаку можно проводить уже и с мобильных устройств!

Не стоит думать, что список написанного злоумышленниками для мобильных устройств ограничивается только вышеописанными примерами. К сожалению, угрозы для "мобильников" растут опережающими темпами по сравнению с угрозами для обычных компьютеров.

Одной из причин поражения Египта в "войне Судного дня" стало то, что его армии вышли из-под "зонтика" ПВО. Лишившись надежной защиты, танковые соединения были уничтожены, что не позволило отразить встречную атаку… Если пользователи думают, что они сами смогут заметить и устранить любую угрозу, полезно вспомнить о данном случае!

первоочередное внимание именно ему, поскольку компрометация гипервизора легко может привести к компрометации всех обслуживаемых им виртуальных машин.

Хотя разработчики гипервизоров и заявляют о высокой степени безопасности своих продуктов, говорить об их полной защищенности не стоит, тем более что на международных ИБ-конференциях хакеры уже демонстрировали возможности их взлома.

Дмитрий Когай указывает на необходимость контроля сетевого трафика между виртуальными машинами, расположенными на одном физическом сервере, поскольку обычно считается, что трафик между такими ВМ не покидает пределы сервера и поэтому якобы является заведомо защищенным от взлома снаружи. Однако если злоумышленнику удается захватить контроль хотя бы за одной из виртуальных машин, то возникает возможность компрометации и остальных ВМ этого сервера с последующей эскалацией атаки на соседние серверы, особенно если не забывать о том, что традиционные системы сетевой фильтрации и предотвращения вторжений работают до границы платформы виртуализации и не могут отслеживать вредоносную активность внутри этих границ.

Первоочередное внимание, по мнению Сергея Панина, пользователи ВС должны уделять правильному конфигурированию ИТ- и ИБ-ресурсов в ВС и мониторингу действий привилегированных пользователей, что напрямую связано с установкой корпоративных приоритетов закрываемых уязвимостей.

С позиции приоритетов угроз он также предлагает подходить и к защите компонентов платформы виртуализации. Так, если высоким в компании считается приоритет внедрения вредоносного кода, то в связи с отсутствием реальных случаев появления такого кода на уровне "гипервизор — средство управления" наиболее уязвимым компонентом ВС, по его мнению, следует считать виртуальную машину, и первоочередное внимание нужно обращать на безопасность взаимодействия ВМ между собой и с компонентами внешней среды.

Николай Романов напоминает, что каждый компонент виртуализированной ИТ-среды имеет свои ИБ-проблемы и требует своих подходов к их решению. Так, перемещаемые в рамках ЦОДа (или между ЦОДами) виртуальные машины могут оказаться брешью в защите, если из доверенной среды они перемещаются в недоверенную (или из защищенной в незащищенную).

Алексей Сабанов полагает, что самым уязвимым компонентом ВС являются системы хранения данных. За ними по степени важности рисков следуют системы управления ВС, из которых объектом атак могут оказаться прежде всего системы управления доступом к ИТ-ресурсам.

По мнению Вячеслава Медведева, не стоит выделять как наиболее уязвимый какой-либо отдельный компонент виртуализированной ИТ-среды — безопасными должны быть они все, причем в соответствии с динамично изменяющимся ландшафтом угроз. Ведь хакеры, как говорит г-н Медведев, ищут и находят уязвимости там, где вчера их вроде бы и не было.

Готовность российского ИБ-рынка к обеспечению безопасности ВС

В оценках готовности участников российского рынка ИБ к обеспечению безопасности виртуализированных ИТ-сред у наших экспертов есть как совпадения во мнениях, так и заметные расхождения. Кто-то из них акцентирует внимание на таких аспектах, которые не попали в поле аналитического рассмотрения коллег.

Вендоры. Согласно наблюдениям Алексея Воронцова, ряд ведущих ИБ-вендоров мира уже предлагают специализированные средства защиты ВС, прежде всего функционирующие через уровень гипервизора, с использованием таких технологий доступа к гипервизору, как VMSafe. Появляются актуальные средства контроля сетевого трафика между виртуальными машинами, в том числе средства обнаружения атак, использующие поведенческий анализ.

Современные специализированные ИБ-решения, по мнению Константина Воронкова, в состоянии обеспечить надежную защиту (что важно — без потерь преимуществ, получаемых за счет виртуализации) и возможность централизованно управлять защитой всей корпоративной ИТ-инфраструктуры, включая как виртуализированные компоненты ИТ, так и невиртуализированные. Конечно, внедрение специализированных решений по сравнению с внедрением традиционных стоит дороже, однако, как считает г-н Воронков, преимущества их неоспоримы и в итоге они более выгодны.

Сегодняшний рынок информационной безопасности, отмечает Сергей Панин, насыщен большим количеством конкурирующих как узконаправленных, так и комплексных решений, обеспечивающих защиту виртуализированных сред и от внешних, и от внутренних угроз. Наряду со специализированными средствами для защиты ВС заказчики используют и классические: защиту от несанкционированного доступа, средства доверенной загрузки, инструменты контроля целостности, распределенные межсетевые экраны и т. д.

Елизавета Спасенных считает, что обеспечение защиты виртуализированной ИТ-среды все еще является задачей достаточно новой, требующей более основательной проработки деталей и учета особенностей реализуемых в ВС сервисов, спектр которых непрерывно расширяется, а вместе с ним расширяется и спектр возможных ИБ-рисков. Поиск и разработка дополнительных решений по обеспечению безопасного использования ВС остается актуальным процессом для ИБ-вендоров, в котором они, по ее мнению, достаточно результативно и оперативно участвуют.

Высоко оценивая возможности доступных на рынке средств защиты ВС для нейтрализации большинства ИБ-угроз, Иван Бойцов указывает на узкий круг поддерживаемых ими средств виртуализации. По его мнению, в полной мере поддерживаются (в том числе и сертифицированными средствами) только несколько наиболее распространенных на рынке продуктов.

В России, считает Николай Романов, заказчики пока еще не задаются всерьез вопросами, связанными со сменой провайдеров облачных сервисов (например, вопросами надлежащего уничтожения данных на площадке прежнего провайдера), или выполнением требований регуляторов при обработке персональных данных в ЦОДе провайдера, предоставляющего сервисы PaaS. Он обращает внимание на то, что по мере активизации перехода от обычных виртуализированных систем к облачным готовность провайдеров ИТ-сервисов к ответу на эти вопросы должна возрастать.

Что бы ни заявляли разработчики, ИБ-индустрия, как считает Алексей Сабанов, имея в виду прежде всего использование ВС в облачной архитектуре, пока не готова реализовать комплексный и взвешенный подход к обеспечению информационной безопасности в плохо еще

ПРОДОЛЖЕНИЕ НА С. 20 ▸

Специфика комплексной защиты виртуализированных ИТ-сред

Компания Trend Micro является в настоящее время одним из немногих в мире поставщиков комплексных решений для защиты облачных и виртуальных сред. Она первой в сотрудничестве с VMware разработала модель системы безопасности без использования агентов, базирующуюся на тесно интегрированных продуктах VMware vShield Endpoint и Trend Micro Deep Security. Об актуальных проблемах, связанных с обеспечением безопасности виртуализированных ИТ-ресурсов, и текущей ситуации в этой области рассказывает технический консультант Trend Micro в России и странах СНГ ***Николай Романов****.*


Николай Романов

Согласно прогнозу компании Gartner от 2010 г. даже к 2015 г. около 30% виртуальных машин по-прежнему будут защищены хуже физических (в 2010 г. таких виртуальных машин, согласно данным этой компании, было 60%). А как обстоят дела с защищенностью виртуализированных ИТ-компонентов сегодня?

Возможно, российские ИТ-пользователи оказались более зрелыми, чем предполагалось, или же сыграл свою роль активный информационный фон вокруг ИБ-проблем, связанных с виртуализацией, но ситуация у нас в стране не так плоха, как ее прогнозировала компания Gartner. Я бы сказал, что она даже лучше, чем в европейских странах, но несколько хуже, чем в США.

Виртуализация используется российскими компаниями прежде всего в ИТ-решениях, предназначенных для обслуживания бизнес-задач и задач из области самих ИТ. ИБ-проблемы виртуализации неплохо осознаются российскими заказчиками, представляющими различные отрасли, лучше — банками, слабее — производственными предприятиями.

Корпоративные ИТ-пользователи понимают, что виртуализированные среды наряду с трансформированными под специфику виртуализации аналогами классических средств защиты (антивирусами, межсетевыми экранами и др.) требуют решения сугубо специальных ИБ-задач, таких как защита от несанкционированного доступа к системе управления виртуализацией, защита гипервизора и др. Другое дело, что им не всегда ясно, с помощью каких средств можно решить такие задачи.

На защищенности каких виртуализированных компонентов ИТ-инфраструктуры сегодня сфокусирован интерес ИТ-пользователей и ИБ-вендоров?

В первую очередь сегодня компании защищают серверные платформы, потому что на них работают их ключевые бизнес-приложения. Активная виртуализация настольных систем требует также внимания и к их защите. При этом нельзя сказать, что проблемы, связанные с их уязвимостями, проще серверных, разве что связанные с ними риски потерь оцениваются ниже. Поэтому виртуализированные рабочие места по приоритету на втором месте.

Виртуализированные сети и системы хранения данных, несмотря на прямую вовлеченность в процесс построения описываемых систем, пока составляют ничтожно малую часть в проектах, связанных с обеспечением ИБ виртуальных сред. Причем если на сетевом уровне часть задач уже может быть решена даже встроенными средствами самих систем (VMware vShield App, например), то с СХД все обстоит несколько сложнее. То, что развитие виртуализированных сетей находится все еще в активной фазе, можно заметить на примере VMware, безоговорочном лидере в области платформ виртуализации, в прошлом году купившей стартап-копанию Nicira, занимающуюся виртуализированными сетевыми системами и управлением ими. Те отдельные компоненты защиты виртуализированных сетей, которые предлагают такие вендоры, как Cisco или Checkpoint, дополняют основные решения для виртуальных сред. Что касается полномасштабных аппаратно-программных систем хранения данных (на которые, кстати, виртуальная среда опирается в значительной степени), то их виртуализация пока применима далеко не везде (по причине некоторых ограничений и стоимости, главным образом). При этом реализация основных сценариев обеспечения защищенности будет явно пересекаться с защитой самой среды, на которой построены данные сервисы.

Готовы ли средства защиты виртуализированных сред к их интеграции в такие комплексы верхнего уровня, как центры управления инцидентами ИБ и системы управления корпоративной ИБ? Есть ли в этом потребность у российских заказчиков?

Распространенный вопрос заказчика, собирающегося построить защиту своей виртуализированной ИТ-среды, который он задает поставщикам средств защиты, — умеют ли их продукты работать с высокоуровневыми системами сбора и корреляции ИБ-событий и управления корпоративной ИБ. Тут, правда, нужно сделать поправку на отрасль, которую заказчик представляет. Как я уже говорил, компании разных отраслей находятся на разных уровнях зрелости ИБ. Соответственно и требования они предъявляют разные.

На рынке существуют ИБ-продукты, располагающие необходимыми интеграционными механизмами, а в продуктах Trend Micro такие возможности реализованы нативно.

Какой вызов безопасности виртуализированных сред вы относите к самым актуальным в настоящее время и в перспективе?

Прежде всего это функционирование средств защиты виртуальной среды без помех для работы тех ИТ-ресурсов, которые они защищают. Заказчики в первую очередь ориентируются на эти свойства при выборе ИБ-продуктов для виртуализированных ИТ-средств. Следующим по важности является вопрос обеспечения безопасности гипервизора.

В комплексных проектах заказчики начинают с задач несанкционированного доступа и сетевой безопасности — межсетевого экранирования и предотвращения вторжений.

Если же говорить о перспективе, то основные вызовы здесь связаны с развитием облачных ИТ-сервисов. Такие сервисы ориентированы прежде всего на бизнес-цели, а задачи ИБ отодвигаются на второй план. Даже компания Amazon в правилах пользования своими облачными сервисами ранее возлагала ответственность за ИБ на самих пользователей сервисов.

Хотя сегодня к вопросам безопасности облачных сервисов относятся более внимательно, нежели несколько лет назад, и нередко пытаются решать их одновременно с разработкой облачной архитектуры, довлеющими все же остаются вопросы стоимости и окупаемости таких проектов. Поэтому с ростом популярности облачных сервисов будет расширяться и спектр ИБ-угроз.

Пока это не слишком проявляется на практике ввиду все еще слабого распространения облачных сервисов. Но нужно отметить, что профессиональные ассоциации, такие как Cloud Security Alliance, уже активно работают над методами защиты подобных сервисов. Опираясь на их опыт, можно сделать вывод о том, что проблемы виртуализированных корпоративных сред пополнятся проблемами, связанными с облаками, среди которых в первую очередь следует упомянуть очистку данных на стороне провайдера облачных услуг при смене провайдера, шифрование данных, а также распределение прав доступа специалистов провайдера к клиентским ресурсам.

Как вы определяете комплексность защищенности виртуализированной ИТ-среды? Можно ли сегодня говорить о том, что она реализуема?

Думаю, что говорить об этом уже можно, поскольку некоторые из представленных на рынке систем защиты виртуальных сред, среди которых и наше решение Deep Security, могут интегрироваться как с платформами виртуализации, так и с внешними ИБ-системами (такими, например, как системы управления ИБ-инцидентами и защиты от несанкционированного доступа) и работать согласованно с ними как единый комплекс. При этом каждый из интегрированных компонентов решает свой круг задач.

Какие особенности характерны для специализированных ИБ-решений для защиты виртуализированных сред?

В виртуальной среде чрезвычайно важным является контроль целостности в реальном времени как всей среды, т. е. гипервизора, так и файлов и ключей реестра операционных систем и приложений, а также контроль нежелательного сетевого трафика.

Следующая особенность ИБ-решений заключается в том, что виртуальные машины могут пребывать долгое время в неактивном режиме, в результате средства антивирусной защиты устаревают, а необходимые критические обновления ОС и приложений отсутствуют. Одновременно возможно создание новых машин, не соответствующих корпоративной политике безопасности, например без средств антивирусной защиты. Указанные проблемы в Deep Security, например, решаются благодаря специальному компоненту Virtual Appliance, который устанавливается прямо в среду ESX-сервера и благодаря использованию средств API защищает сразу все виртуальные машины, работающие на защищаемом ESX.

Хотел бы отметить еще одно важное дополнение средств защиты корпоративных систем — виртуальный патчинг. Deep Security использует глубокий пакетный анализ для выявления и предотвращения атак, направленных на эксплуатацию уязвимостей в ОС и приложениях. Выделенный центр аналитиков информационной безопасности — Trend Micro Security Center — своевременно получает информацию об уязвимостях из десятков источников, таких как SANS, CERT, CVE, Bugtraq, VulnWatch, PacketStorm, Securiteam, а также непосредственно от производителей программного обеспечения, которые, например, участвуют в программе Microsoft Active Protections. На базе этой информации аналитики Security Center выпускают обновления правил для Deep Security, которые блокируют возможность использования уязвимостей, даже без установки патчей от производителей ПО.

О защите...

◂ ПРОДОЛЖЕНИЕ СО С. 19

изведанном виртуальном пространстве. Он, например, не видит адекватных методик оценки рисков и управления системой ИБ в публичных облаках и полагает, что в ближайшее время они не появятся; по его мнению, можно ожидать в скором времени только пилотные методики, но не индустриальные, стандартизованные методы.

Пользователи. Средств обеспечения безопасности ВС, как утверждает Михаил Чернышев, на рынке представлено много: от антивирусов до инструментов глубокого анализа трафика внутри виртуальной инфраструктуры. При их выборе и применении он рекомендует заказчикам руководствоваться принципом разумной достаточности. К примеру, если защита сети выстроена качественно и корпоративные ИБ-средства “знают”, что такое сигнатуры атак на гипервизор, то совершенно не обязательно бросаться на усиление безопасности сети — лучше обратить внимание на оптимизацию работы гостевых операционных систем, тем самым сосредоточившись на решении задачи защиты конечных точек.

По мнению Вячеслава Медведева, на российском ИБ-рынке сегодня есть не только все необходимые ИБ-продукты, но даже и методики, достаточные для обеспечения безопасности виртуализированных ИТ-сред. Дело, считает он, за заказчиками, которые, по его оценкам, пока не осознают уровня угроз, что, собственно, и затрудняет защиту таких сред.

Основным фактором, затрудняющим защиту виртуализированных ИТ-сред, г-н Чернышев называет простоту (в силу специфики средств виртуализации) проведения любого рода тестов в ВС. В итоге, говорит он, клиент оказывается в очень сложной ситуации, когда все протестированные решения его в общем-то устраивают, а окончательный выбор ему сделать непросто, поскольку формализовать свои требования в такой ситуации ему крайне тяжело.

К основной сложности обеспечения ИБ виртуализированной ИТ-среды Константин Воронков относит новизну технологии виртуализации. Корпоративные ИБ-службы, как он полагает, все еще плохо с нею знакомы, у них нет готовых для этой технологии ИБ-политик и правил обеспечения безопасной работы с нею. Традиционные ИБ-средства для технологии виртуализации подходят не всегда, а специализированные, как правило, поставляются по отдельности и являются сложно интегрируемыми с общей системой корпоративной ИБ. ИТ-специалисты только осваивают работу с этими новыми инструментами.

Константин Воронков отмечает, что в компаниях, особенно крупных, нередко возникает напряжение в отношениях между ИТ-департаментом и ИБ-службой, связанное с разделением ответственности за правильную настройку ИБ-решений, за их мониторинг и т. п. В случае с виртуализацией подобные функции (приводящие к конфликтам между ИТ- и ИБ-службами) оказываются еще более консолидированными, поскольку зачастую настройки самой ВС и решений для ▸

обеспечения ее защиты неотделимы друг от друга. Г-н Воронков полагает, что ИТ- и ИБ-подразделения обязаны искать общий язык, вырабатывать общие политики для того, чтобы грамотно и качественно защищать ВС.

Регулирование. По мнению Сергея Панина, из-за отсутствия регулятивных требований к защите виртуализированных ИТ-сред тормозится распространение виртуализации, и рынок ждет от регуляторов регламентирующих документов с описанием самих ВС и методик защиты хранимых в них данных. Он отмечает, что у ФСТЭК, одного из ведущих российских регуляторов в области ИБ, есть понимание того, что в отношении ВС следует вводить специальные критерии и признаки защищенности. Еще в 2012 г. из представителей экспертного сообщества была создана инициативная группа по разработке проекта стандарта безопасности ВС. Однако о результатах ее работы г-ну Панину пока ничего неизвестно.

Он напоминает, что для использования ВС в госструктурах необходимо, чтобы средства виртуализации были сертифицированы в соответствии с требованиями ФСТЭК и ФСБ. Однако поставщики средств виртуализации, как он считает, не могут позволить себе сертифицировать каждую новую версию своих продуктов (которые появляются довольно быстро на динамично развивающемся рынке виртуализации), что существенно сужает возможности построения защищенной ВС, удовлетворяющей требованиям, обязательным для госучреждений. Госструктурам, по мнению г-на Панина, сегодня гораздо проще (с позиции выполнения требований регуляторов) организовать обработку данных (особенно содержащих государственную тайну) без виртуализации.

Елизавета Спасенных отмечает, что ввиду недостаточности нормативной базы, регулирующей защиту виртуализированных ИТ-сред, и отсутствия рекомендаций по выбору и использованию мер и средств защиты ВС заказчикам приходится руководствоваться только здравой логикой и надеяться на то, что ряд сложностей будет снят оперативными действиями регуляторов, направленными на совершенствование нормативной базы.

В то же время, как отмечает Иван Бойцов, первые шаги регуляторами по актуализации российской нормативной базы в сторону защиты виртуализированных ИТ-сред уже сделаны. В частности, проекты приказов ФСТЭК по защите конфиденциальной информации в органах государственной власти и защите ИСПДн, которые находятся на регистрации в Минюсте, содержат ряд базовых требований по защите виртуализированных ИТ-ресурсов.

Несмотря на это, у регуляторов, считает г-н Бойцов, впереди еще много работы. По его наблюдениям, защита ВС никак не учитывается в требованиях к защите автоматизированных систем, в том числе обрабатывающих данные, представляющие собой государственную тайну, отсутствуют четкие требования к средствам защиты ВС (например, в формате профилей защиты, как это сделано для антивирусов и средств обнаружения вторжений).

Алексей Воронцов полагает, что большая часть представителей наших регуляторов всё еще мыслит с позиций физической инфраструктуры, и задачи вроде таких, как поставить сертифицированный во ФСТЭК межсетевой экран в виртуальную сеть или электронный замок на виртуальную машину, остаются вне нормативной базы. Вендоры, отмечает г-н Воронцов, пытаются восполнить нехватку сертифицированных средств защиты виртуализированных ИТ-сред, сертифицируя в качестве средств защиты свои продукты, предназначенные для обеспечения виртуализации ИТ-ресурсов. Однако, по его словам, это мало что дает помимо наклеенного на продукт знака соответствия нормативным требованиям.

По мнению Николая Романова, направление виртуализации в нашей стране не развивается достаточно свободно и регуляторы не препятствуют этому, а контролю с их стороны подвергаются либо сами средства защиты ВС, либо типы сервисов, построенные на базе этой технологии.

Алексей Сабанов полагает, что было бы неразумно требовать от наших регуляторов того, чего в мире (пока) не может никто. Российская регулятивная база, по его наблюдениям, всегда немного (а иногда сильно) запаздывает по отношению к регулятивным нормам развитых капиталистических стран. Но ведь на данный момент, говорит он, и там стандартов нет — есть только рекомендации, через некоторое время появятся требования по обеспечению ИБ виртуализированных сред, а потом и стандарты.

Тренды

Что касается подходов к обеспечению безопасности виртуализированных ИТ-ресурсов, то Вячеслав Медведев настоятельно рекомендует не забывать о пройденных технологических рубежах и накопленном эксплуатационном опыте. Он обращает внимание на то, что облачные ИТ-архитектуры и виртуализация ИТ-ресурсов являются частными случаями давно известных специалистам вычислительных систем с удаленным доступом, и напоминает, что первые компьютеры работали именно так: был сервер и к нему подключались рабочие места. Сегодня спираль развития совершает свой очередной виток.

Рассуждая о перспективах развития системы обеспечения безопасности ВС, Алексей Воронцов фактически оправдывает тех ИТ-специалистов, которые считают виртуализированные ИТ-ресурсы более безопасными, нежели невиртуализированные. Согласно его наблюдениям, пользователи и разработчики всё чаще рассматривают виртуализацию не только как способ экономии ИТ-ресурсов, но и как способ обеспечения информационной безопасности. Функционирование приложений и сервисов в изолированной ВС как возможность изоляции их друг от друга и от системных сервисов является, по его убеждению, плодотворным подходом к защите от атак, основанных на уязвимостях прикладного программного обеспечения. Он рассматривает его как одно из направлений развития виртуализации.

Константин Воронков отмечает, что поставщики средств виртуализации сами постоянно реализуют в своих продуктах новые, более эффективные способы защиты ВС (что является общим трендом в ИТ: ИТ-вендоры стремятся встраивать безопасность в жизненный цикл своих продуктов, начиная с этапа их разработки).

Перспективным г-ну Воронкову представляется развитие технологии Security as a Service. Она дает возможность реализовать, например, защиту по требованию виртуальных машин в ЦОДах силами провайдера ИБ-сервисов. Являясь результатом консолидации ИТ-ресурсов и постепенной передачи функций обеспечения информационной безопасности поставщикам услуг хостинга виртуальной инфраструктуры, SaaS особенно актуальна для малых и средних компаний, которые не имеют возможности создания собственных центров обработки данных и найма квалифицированных ИТ- и ИБ-специалистов.

Согласно наблюдениям Сергея Панина, индустрия ИТ и ИБ движется к консолидации управления их ресурсами. Одним из проявлений этого тренда является стремление ИБ-вендоров унифицировать свои решения в области защиты виртуализированных ИТ-сред. Г-н Панин предполагает, что на рынке появятся многофункциональные решения (например, объединяющие межсетевой экран, систему обнаружения и предотвращения вторжений, антивирусный шлюз, антиспам-функционал, средства веб-фильтрации, инструменты управления уязвимостями, средства контроля функционирования приложений и защиты баз данных), режим использования которых будет зависеть от затребованной заказчиком лицензии. Производители средств защиты ВС будут расширять линейки своих продуктов, добавляя к уже имеющимся новые компоненты по принципу “All-in-box”. При этом специализированные средства (скажем, средства резервного копирования, аутентификации и т. д.) также будут востребованы как нишевые. У ИБ-вендоров появится стимул интегрировать свои продукты с популярными облачными сервисами.

По оценкам Дмитрия Когая, изменения, связанные с эксплуатацией виртуализированных ИТ-сред, которые отразятся на обеспечении ее ИБ, проявятся уже в ближайшие два-три года, что, полагает он, будет продиктовано изменениями в условях функционирования отечественных бизнес-структур — изменениями не только технологическими, но и ментальными. До экономического кризиса вместе с ростом цен на нефть многие российские компании развивались стремительными темпами, выстраивали свои ИТ-инфраструктуры с заделом на будущее, и к настоящему времени в стране насчитывается немало таких ИТ-инфраструктур. У их владельцев (которые, согласно наблюдениям г-на Когая, в массе своей еще не вернулись на докризисный уровень) нет нужды в новых ИТ-решениях — те, которыми они располагают, вполне способны будут справляться со своими функциями еще два-три года.

Дмитрий Когай полагает, что к тому времени, когда российские компании восстановят после экономического кризиса свои бизнес-показатели, морально и физически устареют их ИТ-инфраструктуры, и бизнесу потребуется их обновление. И вот тогда отсутствие таких средств, какими они располагали в “тучные” докризисные времена, сделает, согласно его прогнозам, аутсорсинговую схему потребления ИТ-ресурсов, реализуемую посредством облачных архитектур, насущной потребностью российского бизнеса.

У российских компаний, предполагает г-н Когай, должно поменяться отношение к “зеленым” технологиям, в первую очередь к энергосберегающим, интерес к которым в нашей стране сегодня практически отсутствует в силу того, что расходы на электроэнергию не столь высоки, как в других странах. Однако уже в будущем году тарифы на электричество в России, вероятно, сравняются с тарифами США, а еще через год-два будут на уровне западноевропейских. Это означает, что в какой-то момент более “зеленые” предприятия станут опережать своих конкурентов в плане рентабельности. Г-н Когай рекомендует готовиться уже сегодня к внедрению “зеленых” технологий, с тем чтобы завтра с их помощью оптимизировать расходы, в том числе на электроэнергию.

Он обращает внимание ИТ- и ИБ-вендоров, интеграторов и регуляторов на то, что к тому времени, когда предприятия восстановятся после кризиса, большая часть технических вопросов, связанных с использованием ИТ, должна быть уже отработана, включая и те из них, которые относятся к обеспечению (на востребованном пользователями уровне) информационной безопасности в виртуальных и облачных средах.

ПОТРАТИВ ВСЕГО 5 МИНУТ НА ЗАПОЛНЕНИЕ АНКЕТЫ, ВЫ БУДЕТЕ БЕСПЛАТНО ПОЛУЧАТЬ PC Week/RE 50 НЕДЕЛЬ

PC WEEK RUSSIAN EDITION

КОРПОРАТИВНАЯ ПОДПИСКА

Уважаемые читатели!

Только полностью заполненная анкета, рассчитанная на руководителей, отвечающих за автоматизацию предприятий; специалистов по аппаратному и программному обеспечению, телекоммуникациям, сетевым и информационным технологиям из организаций, имеющих **более 10 компьютеров**, дает право на **бесплатную** подписку на газету PC Week/RE в течение года с момента получения анкеты. Вы также можете заполнить анкету на сайте: www.pcweek.ru/subscribe_print/.

Примечание. На домашний адрес еженедельник по бесплатной корпоративной подписке не высылается. Данная форма подписки распространяется только на территорию РФ.

Я хочу, чтобы моя организация получала PC Week/RE !

Название организации:

Почтовый адрес организации:

Индекс: Область:

Город:

Улица: Дом:

Фамилия, имя, отчество:

Подразделение / отдел:

Должность:

Телефон: Факс:

E-mail: WWW:

(Заполните анкету печатными буквами!)

1. К какой отрасли относится Ваше предприятие?

1. Энергетика ❑
2. Связь и телекоммуникации ❑
3. Производство, не связанное с вычислительной техникой (добывающие и перерабатывающие отрасли, машиностроение и т. п.) ❑
4. Финансовый сектор (кроме банков) ❑
5. Банковский сектор ❑
6. Архитектура и строительство ❑
7. Торговля товарами, не связанными с информационными технологиями ❑
8. Транспорт ❑
9. Информационные технологии (см. также вопрос 2) ❑
10. Реклама и маркетинг ❑
11. Научно-исследовательская деятельность (НИИ и вузы) ❑
12. Государственно-административные структуры ❑
13. Военные организации ❑
14. Образование ❑
15. Медицина ❑
16. Издательская деятельность и полиграфия ❑
17. Иное (что именно)

2. Если основной профиль Вашего предприятия – информационные технологии, то уточните, пожалуйста, сегмент, в котором предприятие работает:

1. Системная интеграция ❑
2. Дистрибуция ❑
3. Телекоммуникации ❑
4. Производство средств ВТ ❑
5. Продажа компьютеров ❑
6. Ремонт компьютерного оборудования ❑
7. Разработка и продажа ПО ❑
8. Консалтинг ❑
9. Иное (что именно)

3. Форма собственности Вашей организации (отметьте только один пункт)

1. Госпредприятие ❑
2. ОАО (открытое акционерное общество) ❑
3. ЗАО (закрытое акционерное общество) ❑
4. Зарубежная фирма ❑
5. СП (совместное предприятие) ❑
6. ТОО (товарищество с ограниченной ответственностью) или ООО (Общество с ограниченной ответственностью) ❑
7. ИЧП (индивидуальное частное предприятие) ❑
8. Иное (что именно)

4. К какой категории относится подразделение, в котором Вы работаете? (отметьте только один пункт)

1. Дирекция ❑
2. Информационно-аналитический отдел ❑
3. Техническая поддержка ❑
4. Служба АСУ/ИТ ❑
5. ВЦ ❑
6. Инженерно-конструкторский отдел (САПР) ❑
7. Отдел рекламы и маркетинга ❑
8. Бухгалтерия/Финансы ❑
9. Производственное подразделение ❑
10. Научно-исследовательское подразделение ❑
11. Учебное подразделение ❑
12. Отдел продаж ❑
13. Отдел закупок/логистики ❑
14. Иное (что именно)

5. Ваш должностной статус (отметьте только один пункт)

1. Директор / президент / владелец ❑
2. Зам. директора / вице-президент ❑
3. Руководитель подразделения ❑
4. Сотрудник / менеджер ❑
5. Консультант ❑
6. Иное (что именно)

6. Ваш возраст

1. До 20 лет ❑
2. 21–25 лет ❑
3. 26–30 лет ❑
4. 31–35 лет ❑
5. 36–40 лет ❑
6. 41–50 лет ❑
7. 51–60 лет ❑
8. Более 60 лет ❑

7. Численность сотрудников в Вашей организации

1. Менее 10 человек ❑
2. 10–100 человек ❑
3. 101–500 человек ❑
4. 501–1000 человек ❑
5. 1001–5000 человек ❑
6. Более 5000 человек ❑

8. Численность компьютерного парка Вашей организации

1. 10–20 компьютеров ❑
2. 21–50 компьютеров ❑
3. 51–100 компьютеров ❑
4. 101–500 компьютеров ❑
5. 501–1000 компьютеров ❑
6. 1001–3000 компьютеров ❑
7. 3001–5000 компьютеров ❑
8. Более 5000 компьютеров ❑

9. Какие ОС используются в Вашей организации ?

1. DOS ❑
2. Windows 3.xx ❑
3. Windows 9x/ME ❑
4. Windows NT/2K/XP/2003 ❑
5. OS/2 ❑
6. Mac OS ❑
7. Linux ❑
8. AIX ❑
9. Solaris/SunOS ❑
10. Free BSD ❑
11. HP/UX ❑
12. Novell NetWare ❑
13. OS/400 ❑
14. Другие варианты UNIX ❑
15. Иное (что именно)

10. Коммуникационные возможности компьютеров Вашей организации

1. Имеют выход в Интернет по выделенной линии ❑
2. Объединены в intranet ❑
3. Объединены в extranet ❑
4. Подключены к ЛВС ❑
5. Не объединены в сеть ❑
6. Dial Up доступ в Интернет ❑

11. Имеет ли сеть Вашей организации территориально распределенную структуру (охватывает более одного здания)?

Да ❑ Нет ❑

12. Собирается ли Ваше предприятие устанавливать интрасети (intranet) в ближайший год ?

Да ❑ Нет ❑

13. Сколько серверов в сети Вашей организации ?

14. Если в Вашей организации используются мэйнфреймы, то какие именно?

1. ЕС ЭВМ ❑
2. IBM ❑
3. Unisys ❑
4. VAX ❑
5. Иное (что именно)
6. Не используются ❑

15. Компьютеры каких фирм-изготовителей используются на Вашем предприятии?

	Настольные ПК	Портативные ПК	Серверы
"Аквариус"	❑	❑	❑
ВИСТ	❑	❑	❑
"Формоза"	❑	❑	❑
Acer	❑	❑	❑
Apple	❑	❑	❑
CLR	❑	❑	❑
Compaq	❑	❑	❑
Dell	❑	❑	❑
Fujitsu Siemens	❑	❑	❑
Gateway	❑	❑	❑
Hewlett-Packard	❑	❑	❑
IBM	❑	❑	❑
Kraftway	❑	❑	❑
R.&K.	❑	❑	❑
R-Style	❑	❑	❑
Rover Computers	❑	❑	❑
Sun	❑	❑	❑
Siemens Nixdorf	❑	❑	❑
Toshiba	❑	❑	❑

Иное (что именно)

16. Какое прикладное ПО используется в Вашей организации?

1. Средства разработки ПО ❑
2. Офисные приложения ❑
3. СУБД ❑
4. Бухгалтерские и складские программы ❑
5. Издательские системы ❑
6. Графические системы ❑
7. Статистические пакеты ❑
8. ПО для управления производственными процессами ❑
9. Программы электронной почты ❑
10. САПР ❑
11. Браузеры Internet ❑
12. Web-серверы ❑
13. Иное (что именно)

17. Если в Вашей организации установлено ПО масштаба предприятия, то каких фирм-разработчиков?

1. "1С" ❑
2. "АйТи" ❑
3. "Галактика" ❑
4. "Парус" ❑
5. BAAN ❑
6. Navision ❑
7. Oracle ❑
8. SAP ❑
9. Epicor Scala ❑
10. ПО собственной разработки ❑
11. Иное (что именно)
12. Не установлено никакое ❑

18. Существует ли на Вашем предприятии единая корпоративная информационная система?

Да ❑ Нет ❑

19. Если Ваша организация не имеет своего Web-узла, то собирается ли она в ближайший год завести его?

Да ❑ Нет ❑

20. Если Вы используете СУБД в своей деятельности, то какие именно?

1. Adabas ❑
2. Cache ❑
3. DB2 ❑
4. dBase ❑
5. FoxPro ❑
6. Informix ❑
7. Ingress ❑
8. MS Access ❑
9. MS SQL Server ❑
10. Oracle ❑
11. Progress ❑
12. Sybase ❑
13. Иное (что именно)
14. Не используем ❑

21. Как Вы оцениваете свое влияние на решение о покупке средств информационных технологий для своей организации? (отметьте только один пункт)

1. Принимаю решение о покупке (подписываю документ) ❑
2. Составляю спецификацию (выбираю средства) и рекомендую приобрести ❑
3. Не участвую в этом процессе ❑
4. Иное (что именно)

22. На приобретение каких из перечисленных групп продуктов или услуг Вы оказываете влияние (покупаете, рекомендуете, составляете спецификацию)?

Системы

1. Мэйнфреймы ❑
2. Миникомпьютеры ❑
3. Серверы ❑
4. Рабочие станции ❑
5. ПК ❑
6. Тонкие клиенты ❑
7. Ноутбуки ❑
8. Карманные ПК ❑

Сети

9. Концентраторы ❑
10. Коммутаторы ❑
11. Мосты ❑
12. Шлюзы ❑
13. Маршрутизаторы ❑
14. Сетевые адаптеры ❑
15. Беспроводные сети ❑
16. Глобальные сети ❑
17. Локальные сети ❑
18. Телекоммуникации ❑

Периферийное оборудование

19. Лазерные принтеры ❑
20. Струйные принтеры ❑
21. Мониторы ❑
22. Сканеры ❑
23. Модемы ❑
24. ИБП (UPS) ❑

Память

25. Жесткие диски ❑
26. CD-ROM ❑
27. Системы архивирования ❑
28. RAID ❑
29. Системы хранения данных ❑

Программное обеспечение

30. Электронная почта ❑
31. Групповое ПО ❑
32. СУБД ❑
33. Сетевое ПО ❑
34. Хранилища данных ❑
35. Электронная коммерция ❑
36. ПО для Web-дизайна ❑
37. ПО для Интернета ❑
38. Java ❑
39. Операционные системы ❑
40. Мультимедийные приложения ❑
41. Средства разработки программ ❑
42. CASE-системы ❑
43. САПР (CAD/CAM) ❑
44. Системы управления проектами ❑
45. ПО для архивирования ❑

Внешние сервисы

46. ❑

Ничего из вышеперечисленного

47. ❑

23. Каков наивысший уровень, для которого Вы оказываете влияние на покупку компьютерных изделий или услуг (служб)?

1. Более чем для одной компании ❑
2. Для всего предприятия ❑
3. Для подразделения, располагающегося в нескольких местах ❑
4. Для нескольких подразделений в одном здании ❑
5. Для одного подразделения ❑
6. Для рабочей группы ❑
7. Только для себя ❑
8. Не влияю ❑
9. Иное (что именно)

24. Через каких провайдеров в настоящее время Ваша фирма получает доступ в интернет и другие интернет-услуги?

1. "Демос" ❑
2. МТУ-Интел ❑
3. "Релком" ❑
4. Combellga ❑
5. Comstar ❑
6. Golden Telecom ❑
7. Equant ❑
8. ORC ❑
9. Telmos ❑
10. Zebra Telecom ❑
11. Через других (каких именно)

Дата заполнения

Отдайте заполненную анкету представителям PC Week/RE либо пришлите ее по адресу: **109147, Москва, ул. Марксистская, д. 34, корп. 10, PC Week/RE.**

Анкету можно отправить на e-mail: info@pcweek.ru

Аутсорсинг теряет свою привлекательность?

САМУЭЛЬ ГРИНГАРД

Последние пара десятилетий ознаменовались циклическим развитием аутсорсинговых инициатив. Сегодня практически невозможно найти компанию из списка 2000 наиболее крупных глобальных организаций, которая бы не отдавала на аутсорсинг какой-либо вид бизнес-деятельности или ИТ-задачи. Однако недавно обнародованный доклад Deloitte Consulting под названием "От Бенгалуру до Бостона: тенденция возвращения ИТ в организации" утверждает, что некоторые компании сворачивают аутсорсинговые инициативы и возвращают исполнение некоторых ИТ-задач в собственные подразделения.

Дейн Андерсон, директор Deloitte Consulting, описывает ситуацию как "незначительный, но развивающийся тренд". Тенденция основывается на возвращении к инсорсингу по причине низкого качества обслуживания, оплошностей и сбоев со стороны поставщиков аутсорсинговых услуг. Во многих случаях возможность сэкономить не оправдывает оттока клиентов, недовольных результатом.

Консалтинговое агентство, опросившее в ходе подготовки исследования представителей 22 ведущих отраслей в 23 странах мира, выяснило, что 48% респондентов расторгли контракт с аутсорсинговой компанией по причине невыполнения подрядчиком обязательств или неудобств в работе. Более того, 34% респондентов, разорвавших договор, решили продолжить работу силами своей компании.

В целом 62% респондентов сообщили, что для них было "очень важно" улучшить качество обслуживания и поддержки клиентов, а другие 38% охарактеризовали эту задачу как "важную". При этом 77% респондентов подчеркнули, что цена вопроса тоже была фактором, оправдавшим переход к инсорсингу.

Консалтинговое агентство выяснило, что 48% респондентов расторгли контракт с аутсорсером из-за невыполнения им обязательств или неудобств в работе.

"Нам показалось, что такой результат нелогичен, так как снижение издержек — это основная причина того, почему компании обращаются к аутсорсингу, — отметил Андерсон. — Однако полученные ответы могут означать, что качество работы аутсорсинговых поставщиков могло не соответствовать ожиданиям клиентов относительно снижения затрат или выполнения других задач".

Другими ключевыми факторами, послужившими причиной возвращения ИТ в организации, стали: желание лучше контролировать процессы (77%), переход к более гибким моделям использования человеческих ресурсов (77%), стремление консолидировать имеющиеся активы (69%), стремление повысить свою конкурентоспособность (62%), желание использовать новые технологии (54%) и возможность добиться налоговых послаблений (38%).

В целом 21% компаний, вернувшихся к практике инсорсинга, признаются, что они "очень довольны" результатами; 58% "довольны" и 21% относится к переходу "нейтрально".

Deloitte отмечает, что перед компаниями, возвращающимися к инсорсингу, стоит несколько проблем. Одной из основных можно считать неудовлетворительный уровень передачи знаний. Это часто происходит, если компания, расторгнувшая контракт по причине невыполнения ее требований, не может обеспечить наём осведомленных сотрудников из стана аутсорсера.

Другими преградами на пути успешного перехода к инсорсинговой модели считаются необходимость расширения внутренних возможностей, например по управлению поставками, и понимание, что реализация этого плана может повлечь за собой увеличение затрат, особенно на ранних стадиях перехода.

"Аутсорсинг до сих пор считается преобладающей моделью на рынке, — заключил Андерсон. — Но при этом наблюдается незначительный, но растущий обратный тренд в отдельных ситуациях и относительно исполнения конкретных функций. Компании, стремящиеся использовать инсорсинговую модель, должны отдавать себе отчет в том, что на этапе расторжения контракта могут возникнуть проблемы. Любые инициативы перехода на инсорсинг должны начинаться с составления подробного бизнес-плана и расчета затрат на переходный период".

НПП и НФАП...

◀ ПРОДОЛЖЕНИЕ СО С. 15

ектные и программные решения, а также конфигурации. Что касается зоны ответственности, то разработчикам типовых проектных решений для Минздрава позволено иметь "полуадминистративный" доступ к своему разделу, в котором хранится такое решение. Пользователям ФАП разрешено оставлять соответствующие комментарии, отзывы и т. п. с тем, чтобы потенциальные клиенты могли ознакомиться с проблемами внедрения и поддержки, узнать стоимость услуг и оценить конкурентное типовое проектное решение. Что касается СПО, то оно выложено в открытом доступе — это OpenOffice, MySpace, дистрибутивы Linux. Пользователю предоставляется виртуальная машина для сборки дистрибутива с автоматической проверкой на вирусы. Каждый файл сопровождается лицензией и электронной подписью человека, загрузившего его в ФАП, что обуславливает персональную ответственность за ПО.

Инфраструктура

При создании инфраструктуры НПП, считает Дмитрий Комиссаров, ни одно мероприятие более чем на 10% (по объемам работ) не выполнено, фактически сделаны только первые шаги в этом направлении. Задач, требующих решения, еще очень много. Сейчас НФАП включает прототипы ОС, системы сборки и т. д.

Для дальнейшего формирования и поддержки НФАП требуется выбрать оператора. "В качестве такового мы рекомендовали Минкомсвязи "Интеграл"", — рассказал г-н Комиссаров. Однако сейчас в качестве оператора в министерстве рассматриваются НИИ "Восход" и Ростелеком.

Следующий нерешенный вопрос — это регламенты. Их нужно разработать и внести на рассмотрение, под них нужно принять постановление Правительства. По его мнению, здесь работы еще года на полтора. Так, в НФАП должна быть закрытая часть: в ней хранится ПО под грифами ("секретно" и т. п.) или под соответствующей сертификацией, т. е. там много работы, за нее никто еще не брался. И здесь нужно получить мнения от ФСБ, ФСТЭК и других регуляторов.

Павел Фролов согласен с оценкой выполненного объема работ, которую дал г-н Комиссаров, но предлагает иметь в виду, что уже существуют продукты на базе СПО, внедренные в различных ведомствах страны. Эти продукты, по его мнению, уже можно включать в НПП в виде типовых проектных решений. Кроме того, у разработчиков СПО создана инфраструктура. В первую очередь имеются в виду разработчики ОС, у которых решены такие вопросы, как хранение пакетов ПО и их автоматизированная пересборка; в частности, компании РОСА и "Альт Линукс" имеют всю необходимую инфраструктуру. Таким образом, полагает он, в стране существуют как минимум три игрока, в числе которых РОСА и "Альт Линукс", которые могут закрыть потребности для НПП на уровне базового СПО, "а это уже немало, это уже шаг вперед, так как пять лет назад в этой области не было ни одного игрока, поскольку тогда были проблемы, требовавшие решения".

"Я не сомневаюсь, что когда государство вновь проявит интерес к НПП, эти имеющиеся наработки вместе помогут в части инфраструктуры совершить прыжок с 5 до 15—20% от уровня реализации программы", — сказал Павел Фролов.

В то же время некоторые эксперты дали более пессимистическую оценку, полагая, что хотя концепция инфраструктуры и проработана и имеются базовые ресурсы, но надо еще собрать работоспособную систему.

Президент РАСПО Юлия Овчинникова уверена: "В НПП заложены основы для создания ИТ-инфраструктуры в России и условия развития ПО, в том числе и СПО".