Комплексные сертифицированные решения ИБ для виртуализированных сред

Полностью виртуализированные распределенные ЦОД с возможностью удаленного доступа становятся базовой компонентой при развертывании современных ИТ-услуг. В этих условиях комплексные решения ИБ приобретают особое значение, т.к. в настоящее время являются одним из основных сдерживающих факторов при миграции на более эффективные виртуальные ИТ-инфраструктуры.

Константин Пичугов – руководитель направления "Защита виртуальных инфраструктур" компании "Код Безопасности".

Введение

Рынок виртуализации развивается уже достаточно давно, но на аспект безопасности участники рынка, эксперты, регуляторы стали обращать внимание лишь недавно. Компания Gartner в 2010 г. провела первое исследование, связанное с безопасностью виртуализации ("Addressing the Most Common Security Risks in Data Center Virtualization Projects", январь 2010 г.). В соответствии с ним к 2012 г. 60% виртуализированных серверов будут меньше защищены, чем физические серверы, которые они заменяют. Но к 2015 г., как отмечает Gartner, эта величина снизится до 30%.

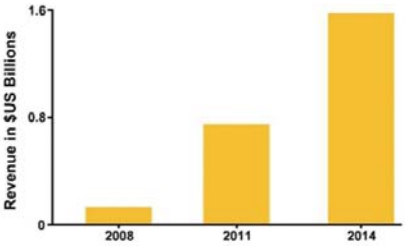
Gartner в своем отчете выделяет 6 основных рисков, из-за которых происходит снижение ИБ при виртуализации серверов:

- *информационная безопасность первоначально не была включена как компонента в проект по виртуализации;*
- *уязвимость гипервизора может стать причиной уязвимости всех рабочих нагрузок, хостируемых на этом сервере;*
- *недостаток видимости (прозрачности) и контроля внутренних виртуальных сетей, создаваемых для прямого взаимодействия VM-to-VM и блокирующих существующие политики и механизмы безопасности;*
- *консолидация рабочих нагрузок разных уровней на одном физическом сервере без их достаточной изоляции;*
- *недостаточный контроль за доступом администраторов к гипервизору/ВМ и административным инструментальным средствам;*
- *возможность потери контроля за разделением сетевым администрированием и управлением безопасностью.*

Разработчики стандарта PCI DSS (Payment Card Industry Data Security Standart) – обеспечение безопасности пластиковых карт Visa – создали рабочую группу, и недавно была принята вторая версия этого стандарта, где были учтены изменения, связанные с виртуализацией. Также подготовили свои рекомендации по обеспечению ИБ и ряд вендоров, занимающихся разработкой самих средств виртуализации, например, Microsoft, VMware, Citrix. Американский Институт по стандартам и технологиям (NIST – National Institute of Standards and Technologies) выпустил в июле 2010 г. предварительную версию документа по обеспечению безопасности для полностью виртуализованных технологий – "Guide to Security for Full Virtualization Technologies", NIST Special Publication 800-125. Независимые рабочие экспертные группы также готовят свои рекомендации. Например, известная группа CIS (Center for Internet Security), которая готовит рекомендации по безопасности для различных технологий, также подготовила свои рекомендации для виртуальных сред на базе решений VMware и Citrix.

Аналитическая группа Infonetics Research в своем отчете "Virtual Security Appliances Biannual Market and Forecasts (июнь, 2010) оценивает рынок средств обеспечения безопасности в виртуальных средах с ежегодными темпами роста до 119%, который к 2014 г. достигнет объема $1,6 млрд.

По прогнозам Infonetics Research мировой рынок virtual security appliance к 2014 г. вырастет до $1,6 млрд



Ист.: Infonetics Research, Virtual Security Appliances Biannual Market Size and Forecasts, June 2010

Рис. 1. Прогноз развития мирового рынка virtual security appliance.

Обеспечение должной степени безопасности данных клиентов, обрабатываемых в виртуализированных ЦОД, – важная и непростая задача. Ведь помимо обычных угроз безопасности данных, в ЦОД добавляются еще и специфичные угрозы, присущие виртуальной среде.

В большинстве случаев ЦОД находится вне IT-инфраструктуры предприятия. Поэтому клиентам гораздо труднее поддерживать целостность, доступность и конфиденциальность данных, а также следить за соответствием нормативным требованиям, чем при нахождении вычислительных ресурсов на территории собственной организации. Кроме того, многие проблемы в области безопасности и нормативного соответствия связаны с недостаточной прозрачностью процессов обеспечения безопасности в ЦОД.

Стоит отметить и то, что в некоторых случаях задача обеспечения безопасности ресурсов клиентов может быть возложена на владельца ЦОД. В таких случаях от клиентов требуется полностью доверить данные (в том числе и ограниченного доступа) сторонним лицам, что вызывает естественные опасения клиентов за безопасность данных, хранящихся в виртуализированном ЦОД.

Доверие клиентов – важная составляющая имиджа любого ЦОД. Для клиентов же основной потребностью является на-

дежное и безопасное хранение их данных, а также поддержание конфиденциальности и целостности этих данных. Вот почему повышенная безопасность нередко предлагается владельцами ЦОД как дополнительная услуга.

Поскольку для ряда клиентов также немаловажной является задача обеспечения соответствия требованиям отраслевых стандартов (например PCI DSS) или требованиям ФЗ-152 «О персональных данных», то возможность предоставления такой услуги может стать неплохим преимуществом для владельца ЦОД.

Классификация решений ИБ для виртуализированных ЦОД

Весь комплекс решений ИБ можно классифицировать по двум уровням:

– в зависимости от операции с данными/ВМ, проводимой в виртуальной среде и возникающих в связи с этим угрозах (рис. 1);

– от жесткости предъявляемых требований к обеспечению безопасности информации или степени ее важности – неконфиденциально/для служебного пользования/секретно/совершенно секретно.

vGate обеспечивает сертифицированную защиту самой платформы виртуализации, включающую серверы виртуализации и средства управления виртуальной средой.

Для защиты самих ВМ и персональных данных, обрабатываемых в них, можно использовать традиционные сертифицированные средства защиты. Для избежания проблем с совместимостью рекомендуется использовать продукты одной компании. Отдельно следует отметить, что все продукты компании "Код Безопасности" имеют сертификаты по линии ФСТЭК и могут применяться для систем различных классов защищенности (ИСПДн – до класса К1, АС – до классов 1Г, 1В, 1Б).

Для защиты каждой ВМ от НСД рекомендуется использовать продукт Secret Net, который обеспечивает разграничение доступа, доверенную информационную среду, а также защиту информации в процессе хранения. Если ВМ используется как сетевой ресурс, то для выполнения требований к межсетевому взаимодействию, рекомендуется использовать межсетевой экран TrustAccess.

Рис. 1. Классификация решений ИБ в зависимости от стадии обработки информации и возникающих в связи с этим угрозах.

Для обеспечения контроля целостности и доверенной программной среды серверов виртуализации рекомендуется установить в каждый такой сервер электронный замок "Соболь".

Жесткие требования к обеспечению безопасного межсетевого взаимодействия предъявляются только при наличии "взаимодействии информационных систем с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования)". Поэтому физическое отделение сети администрирования виртуальной инфраструктуры от остальных сетей позволит существенно сэкономить на технических средствах защиты.

На рис. 2 показан пример развертывания комплексной системы защиты персональных данных, обрабатываемых в виртуальной среде, на базе продуктов компании "Код Безопасности".

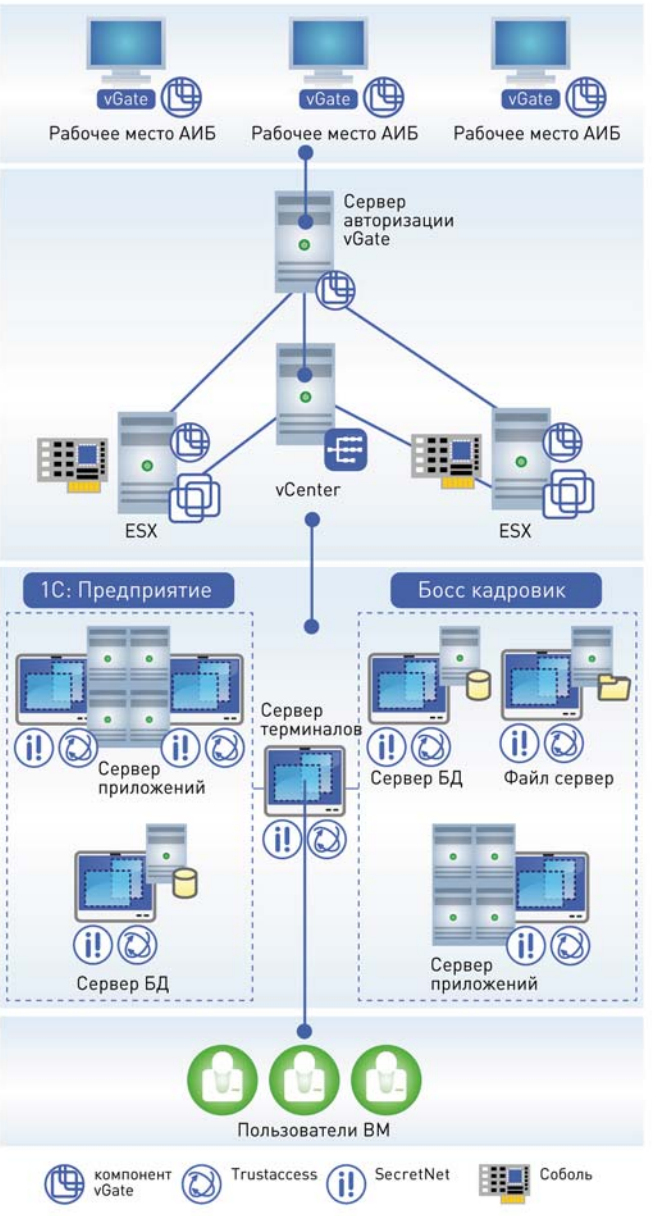


Рис. 2. Пример развертывания комплексной системы защиты персональных данных, обрабатываемых в виртуальной среде, на базе продуктов компании "Код Безопасности" (АВИ – администратор виртуальной инфраструктуры, АИБ – администратор информационной безопасности).

Специфика обеспечения безопасности в виртуализированных ЦОД

Основная проблема обеспечения безопасности виртуальной среды связана с тем, что традиционные средства защиты информации не способны обеспечить защиту от новых угроз безопасности информации, специфичных для виртуальной инфраструктуры. Кроме того, привычные решения не всегда совместимы со средой виртуализации, так как изначально разрабатывались для использования в физической среде. Если нарушитель получает доступ к средствам управления виртуальной инфраструктурой, операционная среда традиционных средств защиты информации оказывается полностью скомпрометированной. Например, через гипервизор (компонент виртуальной архитектуры) нарушитель может незаметно для традиционных средств защиты информации, работающих в виртуальных машинах, совершать следующие злоумышленные действия (см. рис. 1):

– копировать и блокировать поток данных, идущий на все устройства (HDD, принтер, USB, сеть, дискеты);

– читать и изменять данные на дисках виртуальных машин, даже когда они выключены или не работают, без участия программного обеспечения этих виртуальных машин.

Поэтому и выполнить требования по нормативному соответствию (например, требования отраслевого стандарта PCI DSS или ФЗ №152 «О персональных данных») в условиях виртуальной среды с помощью традиционных средств защиты информации довольно затруднительно.

Другим источником проблем может стать появление в виртуализированных ЦОД нового слоя привилегированных пользователей – администраторов виртуальной инфраструктуры, обладающих самыми широкими полномочиями по манипуляции с данными клиентов (дублирование ВМ, получение доступа к хранилищу ВМ, копирование файлов ВМ и т. д.), в том числе и получение доступа к данным виртуальных машин клиентов. Именно поэтому крайне важно контролировать действия таких пользователей ЦОД и по возможности ограничивать их полномо-

чия. Для устранения возможности ошибочных или злоумышленных действий со стороны администраторов оптимальным решением будет предоставление доступа к ресурсам клиента только тем администраторам, которые непосредственно занимаются настройкой и управлением ресурсами клиента, и только в минимальном для выполнения своих обязанностей объеме полномочий.

Важной особенностью виртуализации является возможность совместного хранения ресурсов разных клиентов (в качестве клиентов здесь, например, могут выступать различные компании, арендующие ИТ-услуги у одного сервис-провайдера, или различные подразделения одной организации, имеющие разный уровень доступа к информации): ВМ разных клиентов могут выполняться на одном сервере виртуализации, а их диски – находиться в одном хранилище. Совместное хранение ресурсов разных клиентов – источник ряда проблем, таких как потенциальный ущерб для соседей в случае компрометации ресурсов (ВМ) хотя бы одного клиента, а также возможность НСД к ресурсам соседа со стороны пользователей клиента. Очевидно, что эти проблемы решит разграничение (разделение) ресурсов разных клиентов, но в силу специфики виртуализации это не всегда просто.

При определенных обстоятельствах на территорию ЦОД могут получить физический доступ различные группы лиц. Это и персонал ЦОД, не имеющий непосредственного доступа к среде, и представители других организаций, арендующие стойки или серверы, представители третьих организаций и т. д. Как правило, в большинстве ЦОД эта проблема решается с помощью комплекса организационно-технических мер. При переносе данных клиентов в виртуальную среду появляются новые каналы утечки информации, специфичные для виртуальной среды. Поэтому стандартных организационных мер для решения этой проблемы может быть уже недостаточно.

Контроль доступа к ИТ-ресурсам с помощью vGate

vGate — оптимальное решение для обеспечения полноценной защиты ресурсов клиентов виртуализированного ЦОД, соответствия нормативным требованиям и отчетности о состоянии параметров безопасности виртуальной инфраструктуры.

Продукт может применяться для виртуальных инфраструктур, построенных на базе платформ VMware Infrastructure 3 и VMware vSphere 4 и соответствует требованиям: PCI DSS, ФЗ-152 (РД ФСТЭК), VMware Security Hardening Best Practice, CIS VMware ESX Server 3.5 Benchmark.

Для решения проблемы «суперпользователя» в vGate реализовано разделение ролей пользователей. Управление виртуальной инфраструктурой закреплено за администраторами, а управление безопасностью — за администратором безопасности. В случае использования vGate администратор получает доступ к виртуальной инфраструктуре только после обязательной процедуры аутентификации в vGate. После этого все действия администратора по управлению виртуальной инфраструктурой, а значит и доступ к ресурсам клиентов виртуального ЦОД, контролируются и фиксируются в журнале событий vGate. Кроме того, полномочия каждого администратора виртуальной инфраструктуры ограничены в соответствии с его задачами администратором безопасности (например, предоставлен доступ только к необходимым серверам, запрещена/разрешена возможность скачивания файлов виртуальных машин или создания назначенных заданий и т. д.). Казалось бы, тут появляется другой «суперпользователь» в лице администратора безопасности. Но этого не происходит, поскольку для этого пользователя ограничен доступ к виртуальной инфраструктуре и возможность самосанкционировать доступ к виртуальной инфраструктуре отсутствует (рис. 3).

Для управления доступом пользователей и разделения ресурсов разных клиентов в vGate реализовано мандатное управление доступом на основе меток конфиденциальности. Пометив ресурсы разных клиентов метками разных цветов, можно гарантировать логическое отделение ресурсов одних клиентов от ресурсов других. И хотя физически эти ресурсы могут находиться на одном сервере или в одном хранилище, такое логическое разделение гарантирует то, что ресурсы одной организации или ее сотрудники не получат доступа к ресурсам другой. С помощью меток конфиденциальности можно также разграничить доступ администраторов к ресурсам клиентов: администратор без нужной метки не сможет получить доступ к этим ресурсам.

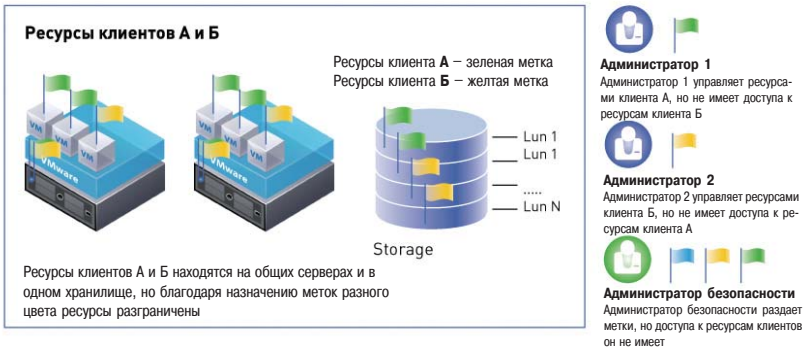


Рис. 3. Разделение доступа к ресурсам с помощью меток, расставляемых администратором безопасности.

Мандатное управление доступом на основе меток конфиденциальности, реализованное в vGate, определяет не только доступ администратора к объектам, но и условия выполнения основных операций с ними, например, таких как:

– создание, редактирование параметров и удаление ВМ;
– приостановка и возобновление работы ВМ;
– перезапуск и завершение гостевой ОС;
– перемещение ВМ на другой сервер и смена хранилища ВМ;
– доступ к хранилищу ВМ;
– редактирование различных сетевых параметров ВМ и т.д.

Примечательно, что для серверов виртуализации и ВМ метки конфиденциальности выполняют двойную роль: не только являются базой для мандатного управления доступом, но и дают возможность сопоставить этим объектам политики безопасности. Политики безопасности настраивают для конкретной метки индивидуально, после чего при назначении метки объекту (серверу виртуализации или ВМ) этот набор политик начинает действовать для него. Политики безопасности позволяют обеспечить соответствие требованиям PCI DSS, VMware Security Hardening Best Practice, CIS VMware ESX Server 3.5 Benchmark. Причем в vGate настроить такие соответствия крайне просто: достаточно включить нужный шаблон настроек при создании политики безопасности.

vGate содержит инструменты для обеспечения полноценной защиты гипервизора и средств управления виртуальной инфраструктурой от утечки информации по каналам, специфичным для виртуальной среды. Защиту от НСД к серверу виртуализации как внутри сети администрирования, так и от локального подключения можно организовать с помощью ряда настроек политик безопасности.

К таким настройкам относятся:

– список разрешенных для выполнения программ (доверенная программная среда сервера виртуализации);
– список запрещенных устройств (защита от несанкционированного копирования данных путем подключения внешних устройств);
– список пользователей, для которых разрешен локальный вход (защита от несанкционированного локального входа пользователей не из списка);
– запрет подключения USB-носителей (защита от несанкционированного копирования данных путем подключения USB-носителя);
– правила для брандмауэра (фильтрация трафика, поступающего на сервер виртуализации).

Политики безопасности позволяют исключить возможность несанкционированного выноса и неконтролируемый рост числа ВМ благодаря таким настройкам, как управление возможностью создания снимков и клонирования ВМ, проверка целостности ВМ.

Для защиты от несанкционированного запуска программ до запуска ОС рекомендуется обеспечить доверенную загрузку сервера виртуализации. Для этого в каждый сервер рекомендуется установить плату доверенной загрузки, например ПАК «Соболь».

Защиту хранилищ данных с файлами ВМ от хищения или несанкционированного выноса можно обеспечить с помощью комплекса организационных мер (контроль доступа в помещения с хранилищами, опечатывание стоек и т. д.).

Для устранения беспокойства клиента о сохранности ресурсов можно регулярно предоставлять ему отчеты о состоянии настроек безопасности, соответствии политик безопасности отраслевым стандартам, а также отчеты об изменениях конфигурации и произошедших событиях информационной безопасности. vGate позволяет подготовить широкий набор различных отчетов по запросу или автоматически по расписанию. Например, можно ежемесячно отправлять клиенту отчет о соответствии политик безопасности требованиям стандарта PCI DSS. После несложной настройки vGate будет создавать такой отчет автоматически на фирменном бланке с логотипом клиента.

Клиентам, использующим бухгалтерские и финансовые программы, системы управления предприятием и персоналом и другие программы, обрабатывающие персональные данные, необходимо обеспечить соответствие ФЗ-152 «О персональных данных». vGate имеет сертификат ФСТЭК*) и позволяет защитить ИСПДн до класса К1 включительно.

Заключение

Сертифицированные комплексные решения ИБ для виртуализованных сред позволяют, прежде всего, решить 3 задачи:

– *обеспечить решение новых проблем и требований, формулируемых регуляторами, а также возникающих при внедрении новых технологий;*
– *обеспечить преемственность "старых" требований при развертывании новых технологий;*
– *обеспечить поддержание качественно нового уровня ИТ-услуг при использовании современных информационных технологий.*

Константин Пичугов,
руководитель направления "Защита виртуальных инфраструктур" компании "Код Безопасности"

*) Уровень сертификации на версию vGate 2 с вышеописанным функционалом – сертификат ФСТЭК (СВТ 3, НДВ 2).

RSA: токенизация и шифрование одновременно

Ноябрь 2010 г. – Компания RSA, подразделение безопасности корпорации EMC, анонсировала программный продукт RSA Data Protection Manager, который обеспечивает широкие возможности защиты данных приложений. Продукт сочетает токенизацию с шифрованием – два популярных инструмента на основе приложений с усовершенствованным управлением метками и ключами для обеспечения комплексной защиты данных. Такое сочетание средств защиты данных и методов управления ключами гарантирует усиленную защиту информации. При этом за счет консолидации уровней управления уменьшаются текущие расходы на обеспечение безопасности. Защищая данные в источнике, внутри приложения, в котором они создаются или используются, продукт RSA помогает обеспечить прозрачную защиту информации на протяжении всего ее жизненного цикла.

"Большинство случаев утечки данных в онлайне происходит в пределах сервера или приложения, так что снижение этого риска имеет решающее значение для защиты информации в целом, – сказал Джон Олтсик (Jon Oltsik), главный аналитик Enterprise Strategy Group. – Защита данных на уровне приложений обеспечивает высокую степень безопасности, поскольку данные защищены в точке их появления и остаются защищенными на протяжении своего жизненного цикла. Шифрование и токенизация на уровне приложения может служить весьма эффективным средством для подобной защиты данных". "Требования по нормативно-правовому соответствию и управлению ключами продолжает довлеть над нашими клиентами, – отметил Дэн Шиппа (Dan Schiappa), старший вице-президент по продуктам RSA. Им нужно не только защитить все свои конфиденциальные данные, используя надежный метод защиты, например шифрование, но и обеспечить соответствие нормативам и правилам с помощью такого экономически эффективного решения, как токенизация. Объединение шифрования, токенизации и управления ключами в одном и том же продукте обеспечивает гибкость и снижает накладные расходы".

RSA Data Protection Manager (прежнее название RSA® Key Manager) защищает данные в момент их ввода и обеспечивает самый детальный уровень контроля над конфиденциальной информацией. Это решение использует следующие технологии:

– ***токенизация:*** замена конфиденциальной информации подменяющим значением, или значением метки, для защиты таких данных, как номера кредитных карт, номера банковских счетов, номера социального страхования и другая информация, идентифицирующая личность;
– ***шифрование приложения:*** применение шифрования и управление сильными ключами для защиты данных в момент их ввода;