Безопасность частных и публичных облаков?

В интервью с Александром Лысенко – ведущим экспертом по вопросам защиты информации компании "Код Безопасности" – дается оценка некоторых архитектур современных платформ виртуализации на базе стандартных серверов для развертывания публичных и частных облаков с точки зрения обеспечения информационной безопасности в части возможности разграничения управления виртуальными инфраструктурами администраторами датацентров от их доступа к данным клиентов, а также рассматриваются возможные варианты повышения уровня ИБ для виртуализированных сред.

Александр Лысенко – ведущий эксперт по вопросам защиты информации компании "Код Безопасности".

Введение

Информационная безопасность, обеспечиваемая в виртуализированных инфраструктурах на базе стандартных серверов, в том числе, для частных и публичных облаков – одна из самых широко обсуждаемых тем в ИТ-сообществе. Основная проблема, которую необходимо решить, – это отделение управления виртуальными инфраструктурами администраторами датацентров от возможности их доступа к данным клиентов. Как показывают исследования, и с этим соглашается ряд вендоров – поставщиков платформ виртуализации – в настоящее время она в полной мере не решена, т.е. администраторы виртуальных инфраструктур имеют доступ к данным (если это частное облако, или виртуализированный датацентр – доступ к данным приложений компании, если публичное – к данным приложений клиентов). Необходимо отметить, что данная проблема не является проблемой проектирования (на чем иногда делается основной акцент) и, в основном, не решается базовыми средствами по виртуализации. Это отчасти объясняет и тот факт, что большинство мировых вендоров делают упор на продвижении частных, а не публичных облаков.

Для частных облаков, это, по сути, "старая" проблема защиты от инсайдеров. Она поддается контролю, например, за счет: 1) тщательного подбора персонала; 2) физического контроля доступа к аппаратным средствам; 3) использования дополнительных программно-аппаратных решений, например, для шифрования/дешифрования БД (и отдельных столбцов) при обработке, а также для разделения функций администрирования и доступа к данным и др. – и все это клиент может контролировать непосредственно. Однако в публичных облаках все эти вопросы могут контролироваться только опосредованно – уровнем доверия клиента к сервис-провайдеру – как поставщику ИТ-услуг – на основе, например, оценок третьих фирм без возможности какого-либо личного контроля. При этом сам сервис-провайдер, в свою очередь, может арендовать ресурсы/сервисы у другого сервис-провайдера. Это означает, что клиент должен всецело доверять сервис-провайдеру, от которого он непосредственно получает ИТ-услуги, если он озабочен безопасностью своих данных.

Однако, если бы в ближайшей перспективе для публичных облаков все же удалось бы полностью отделить управление виртуальной инфраструктурой от доступа к данным клиентов, что на деле могло бы, например, означать возможность полного управления ключами доступа к шифрованным данным с клиентской стороны и онлайновое шифрование/дешифрование данных при обработке, то и в этом случае проблема ИБ в публичных облаках не была бы решена. Это связано с тем, что в настоящий момент использование операций шифрования/дешифрования данных при обработке требует значительных процессорных мощностей, что может полностью нивелировать основные преимущества серверной виртуализации за счет более эффективной загрузки серверных процессоров (и соответственно повышение TCO ИТ-услуг). К этому нужно добавить и то, что гостовская криптография, в отличие от AES, не допускает разбиения блока данных на части и, соответственно, параллельную его обработку и, как следствие, – необходимость использования значительное более мощных универсальных/крипто-процессоров.

Как показывает ряд исследований проблема ИБ в публичных облаках в ближайшие годы останется актуальной. Так, 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 менее защищены, чем физические серверы, которые они заменяют. Но к 2015 г., как отмечает Gartner, эта величина снизится до 30%.

Проблема ИБ в публичных облаках в настоящее время решается несколькими способами. Во-первых, за счет максимального использования частных облаков и развития виртуализации в существующих традиционных датацентрах. Во-вторых, за счет перехода на аутсорсинг и колокацию ИТ-услуг, где вопросы контроля доступа к данным можно жестко контролировать, одновременно добиваясь снижения стоимости капитальных и эксплуатационных затрат ИТ-услуг (например, за счет все той же виртуализации). В-третьих, за счет передачи в публичные облака только тех ИТ-сервисов, для которых: 1) утечка данных не является критичной для компании; 2) утечка данных затруднена из-за того, что они всегда зашифрованы (например, дополнительные резервные копии), дешифрование которых происходит только на стороне клиента. В-четвертых, решением для некоторых была бы возможность онлайновой криптографии при обработке только наиболее критичных данных, но этот подход пока остается достаточно сложным для массового использования.

Надо полагать, что развитие микроэлектроники и использование новых поколений микропроцессоров/чипов со встроенным функционалом криптографии и управления ключами доступа уже через 3-5 лет позволят по-новому взглянуть на проблему ИБ в виртуальных средах и во многом решить

проблему ИБ для публичных облаков. В качестве примера можно привести одну ссылку на одну из публикаций на тему реализации AES в новых процессорах Intel – http://www.thg.ru/cpu/aes_clarkdale/index.html.

Информационная безопасность виртуализованных инфраструктур

SN. Снижает ли уровень ИБ перенос обработки данных в виртуальную среду?

А.Л. При переносе обработки конфиденциальных данных в виртуальную среду острота проблемы утечки конфиденциальной информации резко возрастает, и, прежде всего, из-за наличия так называемого "суперпользователя" в лице администратора виртуальной инфраструктуры (АВИ).

Основная проблема заключается в том, что АВИ могут получить доступ к обрабатываемым внутри виртуальных машин (ВМ) конфиденциальным данным, даже когда эти ВМ выключены. Мало того, при этом совершенно нет необходимости получать физический доступ к инфраструктуре виртуализации, а можно все сделать по сети. И, более того, суперпользователь может замести следы, очистив логи системы виртуализации, а любые системы защиты, находящиеся внутри операционной системы ВМ, в этот момент выключены, т.е. он не только может получить доступ, но и скрыть информацию об этом.

Виртуальную машину можно запросто перенести на другое физическое оборудование путем обычного копирования

Встроенные средства платформ виртуализации не позволяют разделить роли управления виртуальной инфраструктурой и доступа к данным

папки с файлами виртуальной машины. Все настройки виртуальной машины хранятся в файлах в доступном для чтения и редактирования формате, а файлы виртуальных дисков содержат в себе все обрабатываемые на виртуальной машине данные. Это справедливо для всех систем виртуализации.

Например, для платформы виртуализации на базе решений VMware известно, по крайней мере, четыре способа, используя которые АВИ может получить конфиденциальную информацию из ВМ. *Во-первых,* АВИ может скачать файлы дисков ВМ с помощью vSphere Client (команда *Download a file from this datastore to your local machine в Datastore Browser*) на свое рабочее место. После этого получение данных из файла – вопрос нескольких минут. Достаточно, например, просто подключить полученный файл как диск при создании ВМ или монтировать диск в хостовую операционную систему с помощью свободно распространяемой утилиты VMware DiskMount.

Во-вторых, АВИ может монтировать (команда *mount*) vmdk-файл непосредственно в сервисной консоли ESX-сервера.

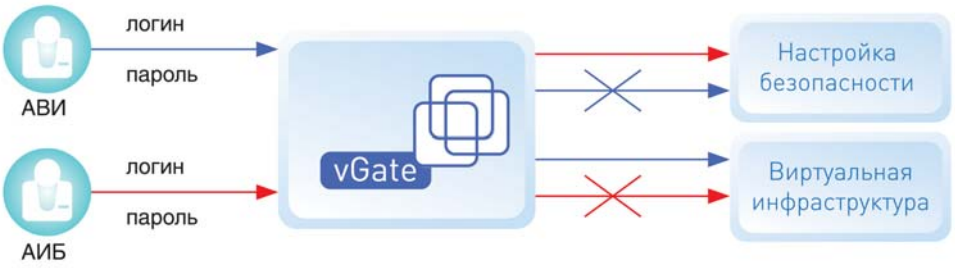

Рис. 1. Решение vGate позволяет все права по управлению виртуальной инфраструктуры закрепить за администратором виртуальной инфраструктуры (АВИ), а права по настройке полномочий АВИ – за администратором информационной безопасности.

В-третьих, АВИ может попасть внутрь ВМ через консоль в vSphere Client и скопировать интересующие его файлы.

И, *в-четвертых,* еще одним потенциальным способом получения конфиденциальных данных могут стать сторонние приложения, дающие доступ к содержимому ВМ через VIX API (средство разработки программ и скриптов для автоматизации операций внутри ВМ, запуска программ или управления файлами без участия гостевой операционной системы). По адресу *http://www.youtube.com/watch?v=lURuCCMHvp* доступен ролик, демонстрирующий возможность получения доступа к ВМ с помощью одного из таких приложений, VMware Guest Console.

Таким образом, угроза утечки конфиденциальных данных, обрабатываемых внутри ВМ, со стороны недобросовестного АВИ весьма реальна. И это не может не беспокоить владельцев организаций, особенно в случае обработки конфиденциальных данных в виртуальных ЦОД.

SN. Одним из наиболее успешных методов повышения ИБ и снижения вероятности утечек данных является разделение функций администрирования инфраструктурой (в том числе и виртуальной) и доступа к данным. Насколько успешно это реализовано в современных наиболее распространенных платформах виртуализации (VMware, MS, Citrix, Oracle, Linux, Parallels и др.) для стандартных серверов?

А.Л. В данном случае я могу дать комментарии пока только для решений VMware – наиболее исследованных нами. Мы сделали продукт для защиты виртуальной инфраструктуры VMWare, по остальным пока нет.

Для защиты данных виртуальных машин от потенциальной угрозы со стороны АВИ необходимо ограничение его полномочий с целью исключить любую возможность получить конфиденциальные данные из ВМ. Очевидно, что должна быть исключена, какая бы то ни было возможность самосанкционировать изменение собственных полномочий. Поэтому за назначение полномочий должно отвечать другое лицо, которое в свою очередь не должно иметь доступа к управлению виртуальной инфраструктурой.

Наиболее оптимальным способом решения проблемы "суперпользователя" является разделение ролей пользователей. Все права по управлению ВИ должны быть закреплены за АВИ, а права по настройке полномочий АВИ – за администратором информационной безопасности (АИБ). Очевидно, что и у того, и у другого должна отсутствовать возможность самосанкционировать изменение собственных полномочий (рис. 1).

При анализе возможности решения проблемы разделения ролей встроенными средствами VMware, в первую очередь, следует отметить то, что в среде VMware vSphere отдельная роль для АИБ не предусмотрена, поэтому ее придется настраивать самостоятельно.

Основная сложность состоит в том, что при формировании роли АИБ предстоит проанализировать более ста привилегий. В частности, в роль АИБ должны быть включены привилегии на управление правами доступа (*Allow disk access или Allow read-only disk access из группы Virtual machine->Provision*), ведению журналов событий (*Log events из группы Global*), управлению политиками безопасности (*Policy operation из группы Distributed Virtual Port Group или Distributed Virtual Switch*) и т.д. Очевидно, что привилегия назначения прав АВИ на управление каким-либо объектом ВИ (*modify permission*) должна быть также закреплена за ролью АИБ.

Следует отметить, что привязка роли к учетной записи пользователя осуществляется только при назначении прав (permission) на объект. Таким образом, АИБ может при назначении прав на объекты (*modify permission*) любой учетной записи может сопоставить любую роль, в том числе и самосанкционировать собственный доступ к объекту.

Другой особенностью является тот факт, что для авторизации в VMware vSphere Client используются учетные записи Windows. Все члены локальной группы администраторов на сервере, где развернут vCenter, получают по умолчанию роль Administrator (роль со всеми возможными привилегиями, включая возможность создания новых ролей и назначения прав доступа к объектам), т.е. являются "суперпользователями".

Таким образом, встроенные средства VMware не позволяют разделить роли: ограничить права АВИ и настроить полноценную роль АИБ.

SN. Какой функционал предлагается в составе vGate, разработанного Вашей компанией, для решения этой задачи?

А.Л. Функция разделения ролей является штатной функцией продукта vGate. Управление виртуальной инфраструктурой закреплено за АВИ, а управление безопасностью – за АИБ.

При этом выделяют две стандартные роли – АВИ и АИБ – с четким разделением ролей по административным функциям. АИБ отвечает за настройку и управление безопасностью виртуальной среды, АВИ – администрирование виртуальной инфрастуруктуры. Все управление осуществляется стандартным образом через VI-клиент.

Для авторизации в vGate настраиваются собственные учетные записи, при этом роль назначается на этапе создания учетной записи, а настройка учетных записей возможна только под учетной записью встроенного администратора безопасности.

При использовании vGate для защиты ВИ под управлением VMware vSphere все АВИ проходят усиленную аутентификацию. Сначала необходимо ввести параметры учетной записи vGate в специально устанавливаемом на рабочее место АВИ приложении, после чего в VI-клиенте уже можно указать учетную запись для работы в VMware-инфраструктуре.

Для каждой конкретной учетной записи vGate можно напрямую сопоставить учетную запись в VMware. После этого пользователь vGate сможет войти в среду VMware только под указанной учетной записью. Четкое сопоставление одной записи с другой ограничивает возможности самосанкционирования, т.е. администратор сможет работать с инфраструктурой VMware только под одной учетной записью, другие же – использовать не сможет. Кроме того, данный механизм позволяет ограничить полномочия АИБ при работе с виртуальной инфраструктурой. Для того, чтобы у АИБ появился доступ к инфраструктуре, его учетной записи надо явно назначать права на доступ к инфраструктуре. Кроме того, поскольку АИБ не администрирует ВИ, то у них в принципе может не быть учетных записей VMWare.

Отдельно следует отметить, что в состав vGate входят средства, позволяющие ограничить доступ АВИ к конфиденциальным данным, хранящимся внутри ВМ. В частности, сервер авторизации vGate блокирует все вызовы VIX API. Возможность монтирования vmdk-файла непосредственно в сервисной консоли ESX-сервера тоже можно исключить, поскольку vGate позволяет блокировать как локальный доступ к ESX-серверу, так и по SSH. Возможность скачивания файлов ВМ с помощью vSphere Client можно гибко задавать при настройке учетной записи для АВИ в vGate. Но даже АВИ с привилегией “разрешение скачивать vmdk-файлы виртуальных машин” сможет это сделать только у той ВМ, для которой это разрешено политикой безопасности vGate. Кроме того, информация об этом будет записана в журнал событий – кто, что, когда.

SN. Интегрирован ли vGate с vCloud Director? Сохраняются ли настройки безопасности при реконфигурации виртуальной инфраструктуры?

А.Л. vGate функционирует прозрачно для других продуктов. Он создает сферу безопасности, контролирует конфигурацию и загрузку виртуальных машин на ESX-серверах и доступ администраторов к виртуальной инфраструктуре.

SN. Может ли vGate интегрироваться с другими средствами ИБ, например, для БД (напр., eToken "Крипто БД" от Aladdin, SafeNet DataSecure) или, например, с системами документооборота (например, DocsVision, Documentum)? Или это будут две точки управления?

А.Л. Это разные точки управления, т.к. предназначены для разных задач, БД – задача прикладная, защищаем данные пользователей от других пользователей, vGate же защищает непосредственно инфраструктуру.

SN. Особенность современных (и перспективных) датацентров состоит в переходе от серверной виртуализации к глобальной виртуализации всей ИТ-инфраструктуры с глобально-распределенным получением ИТ-услуг. В таких инфраструктурах отсутствует жесткая привязка виртуальных серверов и хранимых данных к локальным устройствам/серверам/СХД (например, это можно делать с помощью таких решений как VPLEX и Atmos от EMC). Приложения могут выполняться, а данные храниться в любом географическом месте. Поддерживает ли такие инфраструктуры vGate?

А.Л. При конфигурировании vGate набором оборудования (на котором работает виртуальная инфраструктура) можно жестко управлять, т.е. сконфигурировать правило “машины с определенными метками должны жить на определенных серверах”. Можно управлять (точнее, ограничить) и тем, где будут лежать файлы виртуальных машин, и какие можно использовать сетевые карты и сети VLAN.

SN. Интегрирован ли vGate с VDI-решением (Virtual Desktop Infrastructure) VMware – VMware View?

А.Л. vGate может работать в инфраструктуре VMWare View и защищать ее, т.е. совместим с ней.

SN. Каким законодательным требованиям дает возможность удовлетворять использование vGate?

А.Л. Во-первых, vGate дает возможность использовать платформы Virtual Infrastructure 3.5/vSphere 4 в качестве сертифицированных для защиты персональных данных (по классам К1/К2/К3) и для применения в информационных системах государственного сектора (по классам 1Г/1В/1Б).

Также среди новых возможностей продукта vGate версии 2 можно назвать следующие: готовые шаблоны политик безопасности для приведения в соответствие виртуальной инфраструктуры требованиям PCI DSS (регламентация деятельности банковских и финансовых организаций), CIS VMware ESX Server 3.5 Benchmark и VMware Security Hardening Best Practice.

SN. Каким Вы видите комплексное решение для ИБ в облаках?

А.Л. В целом, комплексное решение для ИБ в облаках должно бы, на мой взгляд, включать:

1. Защиту виртуальной инфраструктуры (от специфических угроз).

2. Защиту виртуальных машин друг от друга, при помощи Firewall (создание независимого периметра для групп ресурсов разных клиентов).

3. Антивирусную защиту.

4. Защиту каналов передачи (СКЗИ – средство криптографической защиты информации, физическая защита).

5. Защиту информации внутри ВМ (СЗИ, СКЗИ).

SN. Представлен ли продукт vGate в других странах, кроме России?

А.Л. Да, с ноября 2010 г. vGate продвигается в западноевропейских странах: в странах Бенилюкс, Германии, Франции, Великобритании, Италии и др. Действует английский сайт продукта (*vgate.info*), на котором можно получить полную информацию о его возможностях, скачать демо-версию, ознакомиться с документацией. О коммерческих результатах говорить пока рано (так как у vGate длинный цикл сделок), но мы ожидаем подвести первые итоги по результатам 2011 г.