

Безопасность виртуальной инфраструктуры

Александр Ширманов, сентябрь 2009 г

Обеспечение информационной безопасности ИТ-инфраструктуры предусматривает решение как минимум двух задач: обеспечение состояния конфиденциальности, целостности и доступности информации организационными и программно-техническими средствами и обеспечение соответствия требованиям законодательства в отношении защиты конфиденциальной информации и персональных данных. Вместе с тем обработка информации в виртуальной среде имеет свои специфические особенности, отсутствующие в физической среде:

- информация обрабатывается в гостевых машинах, которые находятся под полным контролем гипервизора, способного абсолютно незаметно для традиционных средств защиты информации перехватывать все данные, идущие через устройства;
- администратор виртуальной инфраструктуры, имеющий права доступа к гипервизору, становится очень важным субъектом безопасности информационной системы – фактически он может получить доступ к информационным ресурсам в обход существующей политики информационной безопасности компании;
- средства управления виртуальной инфраструктурой представляют собой самостоятельный объект атаки, проникновение к ним дает возможность нарушителю получить доступ к гипервизорам серверов виртуализации, а затем к конфиденциальным данным, обрабатываемым на гостевых машинах;
- традиционные средства защиты информации, разработанные для защиты физической инфраструктуры, могут не учитывать существование гипервизора, являющегося фактически нарушителем, реализующим атаку «человек в середине», при взаимодействии гостевой машины со всеми устройствами;
- диски гостевых машин обычно размещаются в сетевых хранилищах, которые должны физически защищаться как самостоятельные устройства;
- традиционные межсетевые экраны не контролируют трафик внутри сервера виртуализации, где могут находиться десятки гостевых машин, взаимодействующих между собой по сети, однако этот сетевой трафик не покидает сервера виртуализации и не проходит через физические межсетевые экраны и другое физическое сетевое оборудование;
- каналы передачи служебных данных серверов виртуализации обычно не защищены, хотя по этим каналам среди прочих данных передаются фрагменты оперативной памяти гостевых машин, которые, разумеется, могут содержать конфиденциальные данные.

К особенностям виртуальных инфраструктур относится также простота создания и ввода в эксплуатацию гостевых машин, что приводит к эффекту разрастания парка виртуальных машин, получившему отдельное название Virtual Sprawl. Слабоконтролируемый рост числа виртуальных машин приводит к проблемам безопасности, поскольку часть виртуальных машин не получает должного уровня администрирования, включая установку обновлений и настройку параметров безопасности.

Виртуальная инфраструктура повышает степень интеграции вычислительных средств, уменьшая количество физического оборудования при таком же или еще большем количестве сетевых приложений, сервисов, рабочих мест и т.п., что означает усложнение структуры взаимодействия субъектов. Поэтому повышать защищенность виртуальной инфраструктуры нужно комплексно, путем комбинации сетевых и локальных средств защиты с одновременной интеграцией широкого набора защитных механизмов: средств сетевой аутентификации и авторизации пользователей; межсетевого экранирования как внутри сервера виртуализации между гостевыми машинами, так и по периметру виртуальной инфраструктуры; систем регистрации, сбора и корреляционного анализа событий безопасности; средств разграничения доступа (и делегирования полномочий) к виртуальным машинам и к самому серверу виртуализации (и его гипервизору); систем контроля целостности конфигураций распределенных компонентов виртуальной инфраструктуры; средств антивирусной защиты и управления доступом к элементам виртуальной инфраструктуры.

Администратору виртуальной инфраструктуры предоставляется доступ к серверу виртуализации, что фактически означает предоставление доступа к десяткам виртуальных машин, поэтому здесь нужна политика управления доступом и организация ролевой модели управления, построенной на базе делегирования административных функций от главного администратора к подчиненным с целью уменьшения гранулярности предоставления доступа. Организациям, модель нарушителя которых включает администраторов серверов (например, подпункт 2 п. 6.7 СТО БР ИБСС-1.0-2008 стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»), следует так предоставлять полномочия, чтобы исключить возможность «самосанкционирования» (п. 7.4.3 СТО БР ИБСС-1.0-2008). Модель такого предоставления полномочий может реализовываться через:

- систему заявок на предоставление доступа, проходящих процедуру согласования у владельцев соответствующих информационных ресурсов и других лиц, отвечающих за информационную безопасность;
- специальный механизм управления правами в системе разграничения доступа администратором безопасности, не имеющим прав на систему виртуализации, а администратор системы виртуализации, в свою очередь, не имеет полномочий на назначение прав в системе разграничения доступа.

Разумно также использовать комбинацию этих двух подходов.

Важной задачей является обеспечение безопасности информации в сетевых хранилищах данных. Идеальное решение состоит в реконфигурации сети таким образом, чтобы файлы-изображения виртуальных машин размещались в изолированном сетевом хранилище, доступ к которому контролируется межсетевым экраном. Кроме того, если стоит задача обеспечить изоляцию данных в сетевом хранилище от администратора сервера виртуализации, то необходимо убедиться, что эта задача решается выбранными техническими средствами. Для получения доступа к данным виртуальных машин администратор может воспользоваться как штатными возможностями среды управления виртуализацией, так и своими административными полномочиями на самом сервере виртуализации, благодаря которым он может иметь прямой доступ к дискам виртуальных машин. Важно обеспечить такую модель безопасности, чтобы администратор мог в полном объеме выполнять свои функции по администрированию виртуальной инфраструктуры, но при этом не имел доступа к данным, обрабатываемым внутри виртуальных машин, которые создаются их пользователями.

Если отсутствует возможность выделить средство хранения данных для серверов виртуализации (а к этому хранилищу обращаются также приложения и сервисы с самих гостевых виртуальных машин и пользователи физических рабочих мест), то задача обеспечения безопасности усложняется. В этом случае необходимо обеспечить фильтрацию трафика по протоколам, которые поддерживаются сетевыми хранилищами данных, запретить создание несанкционированных устройств сетевого хранения данных на физических рабочих местах и внутри гостевых виртуальных машин.

Отдельно стоит отметить необходимость контроля целостности конфигураций виртуальных машин с целью предотвращения добавления неразрешенных устройств (в основном накопителей различных типов) в гостевой виртуальной машине, на которые нарушитель может выполнить копирование конфиденциальной информации. Необходимо также обеспечить доверенную загрузку и контроль целостности сервера виртуализации и гипервизора с помощью аппаратно-программных модулей доверенной загрузки или их аналогов.

В случае если в виртуальной среде обрабатываются персональные данные, защищенность виртуальной информационной системы должна соответствовать требованиям законодательства, однако требования Федерального закона № 152, Постановления Правительства РФ от 17.11.2007 г. № 781, методические рекомендации и материалы регуляторов по обеспечению безопасности персональных данных не делают различий между физической и виртуальной средой обработки. То же самое касается и руководящих документов регуляторов в части защиты конфиденциальной информации. Согласно всем этим нормативным актам, применяемые средства технической защиты информации должны быть сертифицированы, что означает необходимость использования и в виртуальной инфраструктуре сертифицированных средств защиты информации требуемого уровня защищенности и с отсутствующими в них недекларируемыми возможностями. В этой связи особую важность приобретает профессиональное проектирование системы, причем, в зависимости от категории обрабатываемых данных, требуется проводить аттестацию виртуальной информационной системы.

Нужно отметить, что при защите персональных данных, обрабатываемых на серверах виртуализации, требуется использование межсетевого экранирования высокого класса защищенности. В частности, необходимо проводить аутентификацию входящих и исходящих соединений, определять начало и окончание сеансов связи. Эти действия должны выполняться и в отношении соединений со стороны администратора виртуальной инфраструктуры.

Реальные примеры «виртуальных» угроз

Атака на сервер виртуализации и средства управления виртуальной инфраструктурой. Может быть реализована за счет несанкционированного доступа или эксплуатации уязвимостей ПО виртуализации. Защита обеспечивается комплексом организационных и технических мер, среди которых: отделение сети администрирования виртуальной инфраструктуры с последующей защитой периметра сети (обеспечивает Security Code vGate); контроль целостности и доверенная загрузка серверов виртуализации (обеспечивает электронный замок «Соболь»), ограничение физического доступа к ним; своевременная установка обновлений ПО виртуализации, и ряд других мер.

Атака на диск виртуальной машины. Реализуется за счет несанкционированного доступа к системе хранения данных или сети передачи данных через скомпрометированные элементы виртуальной или физической инфраструктуры. Защита также обеспечивается комплексом мер, среди которых защита сети передачи данных и разграничение доступа к системе хранения данных и отдельным разделам этой системы.

Атака на виртуальную машину с другой виртуальной машины. Поскольку трафик между виртуальными машинами может не покидать пределов сервера виртуализации, то традиционные межсетевые экраны не применимы для защиты от подобного вида атак. Требуется применения специализированных виртуальных межсетевых экранов.

Средства защиты виртуальных сред

Security Code vGate for VMware Infrastructure — специализированное средство защиты информации, предназначенное для обеспечения безопасности управления виртуальной инфраструктурой VMware Infrastructure 3 и VMware vSphere 4. Применение данного продукта совместно с организационными мерами позволяет деактуализировать основные виды характерных для виртуализации угроз.

Электронный замок «Соболь» — это аппаратно-программное средство защиты компьютера от несанкционированного доступа. Может применяться для доверенной загрузки и контроля целостности серверов виртуализации VMware ESX Server.