Виртуализация и безопасность

Публикация – обзор возможных угроз с точки зрения информационной безопасности в ИТ-среде на базе серверной виртуализации и методов борьбы с ними.

Алексей Чеканов – генеральный директор, компания Almitech

Введение

Виртуализация в последние годы является, пожалуй, самым перспективным направлением развития информационных технологий, и большинство организаций уже используют ее для решения своих задач. При этом, задавая вопрос "а насколько безопасна виртуальная инфраструктура", можно получить самый широкий спектр ответов. Производители заявляют, что решения виртуализации обеспечивают более высокий уровень безопасности, чем их "железные" аналоги, а наиболее скептически настроенные пользователи, напротив, пока не готовы доверить решениям по виртуализации свои критические данные. Истина, как водится, находится где-то посередине. Т.е. безопасность обеспечить можно, но как – до конца еще непонятно.

В этой статье мы попробуем на нескольких наиболее ярких примерах, связанных с серверной виртуализацией, разобраться, что же появилось принципиально нового с точки зрения безопасности и как с этими угрозами можно бороться.

Новые угрозы

Атаки на гипервизор

Ключевой элемент архитектуры сред виртуализации, который отсутствует в традиционных серверных инфраструктурах, – гипервизор. Учитывая практически неограниченные возможности, которые может получить злоумышленник, получив контроль над гипервизором, логично предположить, что именно к нему будет приковано внимание хакеров. Если посмотреть на доклады на конференциях типа Black Hat, какое-то время назад возможность скомпрометировать гипервизор обсуждалось крайне активно, однако потом эта тема практически сошла на нет.

И, действительно, несмотря на серьезные последствия в случае осуществления такой угрозы, на другой чаше весов оказалось слишком много аргументов, среди которых – пристальное внимание производителей ПО виртуализации к данной проблеме, оперативное устранение обнаруженных уязвимостей, и, наконец, ограниченное пространство для поиска уязвимостей в силу относительно небольшого размера кода гипервизора.

В результате, применением классических мер безопасности, таких как оперативная установка обновлений, жесткий контроль доступа к гипервизору и к среде управления, контроль целостности, вероятность этой угрозы удалось понизить до вполне приемлемых величин. По-крайней мере, на сегодняшний день еще не приходилось слышать о сколь-нибудь масштабных проблемах в реальных информационных системах, связанных с компрометацией гипервизора.

Аналогичная ситуация наблюдается и со средой управления виртуальной инфраструктурой – наличие механизмов контроля доступа и действий администраторов позволяет минимизировать данный риск.

Плохо управляемый парк виртуальных машин

Часто приходиться слышать, что серьезной угрозой безопасности, возникающей при использовании технологии виртуализации, является неконтролируемое разрастание парка виртуальных машин (ВМ). Если для физических машин есть серьезное препятствие в виде стоимости приобретения нового сервера, то для виртуальной среды создание или копирование виртуальной машины может быть выполнено за несколько кликов мыши. Действительно, это так, но при одном условии – если у администраторов есть возможность бесконтрольно выполнять подобного рода действия.

Решается данная проблема достаточно эффективно сочетанием двух мер: четкими регламентами, описывающими жизненный цикл машин – от момента создания до момента вывода из эксплуатации, и использованием специализированных решений, позволяющих контролировать действия администраторов.

Было бы, по меньшей мере, неразумно отказываться от возможностей, предлагаемых новыми технологиями, но важно с самого начала выстроить четкие процессы управления.

Сетевая безопасность

Задача обеспечения сетевой безопасности в среде виртуализации несколько отличается от той же задачи в инфраструктуре физической, в основном по причинам:

- невозможности применять уже привычные средства обеспечения сетевой безопасности (межсетевые экраны, системы предотвращения вторжений) в том виде, в котором они существуют;
- высокой динамики среды, связанной с перемещением виртуальных машин.

Тем не менее, и эта угроза уже не так страшна. Начиная с этого года, базовые средства обеспечения сетевой безопасности внутри виртуальной инфраструктуры появились в решении VMware, а продукты третьих фирм, об одном из которых пойдет речь далее в статье, достигли уровня зрелости, сопоставимого с их аналогами из мира "физического".

Безопасность СХД, используемых ВМ

Поскольку ВМ представляет собой совокупность файлов, возникает риск того, что эти файлы могут быть скопированы либо подменены. Угроза действительно реальная, причем риск модификации ВМ представляет, пожалуй, большую угрозу, чем просто копирование самой ВМ. По той простой причине, что чаще всего в серьезных промышленных решениях данные отделены от серверов их обрабатывающих, а вот модифицированный сервер может выполнять любую вредоносную нагрузку.

Впрочем, меры противодействия данному риску не отличаются особенной сложностью. За редкими исключениями, в продуктивных системах файлы виртуальных машин хранятся на внешних, по отношению к серверам, системам хранения данных. Соответственно, задача обеспечения безопасности во многом решается ограничением на уровне СХД

доступа к файлам виртуальных машин только со стороны серверов виртуальной инфраструктуры. Протоколирование таких действий, как клонирование виртуальных машин, резервное копирование и т.п., позволяет контролировать администраторов, а правильное определение ролей позволяет минимизировать число администраторов, которым доступны подобные действия.

Параллельно с контролем доступа к СХД необходимо также обеспечить комплекс мер по защите резервных копий виртуальных машин, что, впрочем, так же важно и для резервных копий обыкновенных серверов.

Атаки на виртуальные машины

Сравнивая уязвимость самих виртуальных машин, видим, что они подвержены абсолютно тем же атакам, что и машины физические, что, впрочем, абсолютно естественно, ведь концепция виртуализации и заключается в том, чтобы быть прозрачной для самих виртуальных машин. Единственная особенность, пожалуй, заключается в том, что виртуальная машина может долгое время пребывать в оффлайне, что приводит к тому, что последние обновления и базы данных антивирусов могут оказаться неустановленными на эту машину. Но тут нам на помощь приходят новые технологии, предоставляемые средствами виртуализации.

Новые возможности

Security API

В этой области VMware выступила ярким лидером, представив сообществу своих партнеров технологию VMsafe. Технология VMsafe позволяет без установки агентов внутрь виртуальных машин осуществлять контроль всех составляющих виртуальной инфраструктуры: памяти, дисков, сетевого взаимодействия и т.п. VMsafe позволяет работать даже с машинами, находящимися в выключенном состоянии, например, осуществлять их антивирусное сканирование. Интеграция с технологией перемещения виртуальных машин vMotion позволяет применять при перемещении машины в новое окружение (например, из ЦОД организации в ЦОД сервис-провайдера, или, используя "облачную" терминологию, из внутреннего облака во внешнее) новые политики информационной безопасности.

Этот шаг позволил VMware, не проходя самостоятельно путь по созданию полноценного набора средств обеспечения информационной безопасности, дать лидерам рынка решений ИБ доступ к своему гипервизору, обеспечивая контроль за действиями виртуальных машин на самом низком уровне, и в результате поддержать должный уровень защиты инфраструктуры.

Новые решения

Чтобы воплотить сказанное выше в конкретные решения, которые могут быть использованы на практике, в этом разделе вкратце рассмотрим два продукта, победившие в категории "Безопасность и виртуализация" на VMworld в 2008 и 2009 г.

Reflex VMC

С тех пор, как решение Reflex VMC получило две награды на VMworld 2008, произошло немало изменений – вышла новая версия, решение было первым сертифицировано VMware на использование технологии VMsafe, получило еще два приза от Red Herring и Network Products Guide.

Итак, какие возможности предоставляет продукт сегодня? Reflex VMC позиционируется, как комплексное решение по управлению и обеспечению безопасности в средах виртуализации. Не претендуя на замену встроенных инструментов управления, Reflex VMC существенно расширяет их возможности.

Основные функции Reflex VMC:

- *обеспечение сетевой безопасности внутри сетевой инфраструктуры.*

  Помимо функциональности межсетевого экрана и системы предотвращения вторжений, Reflex VMC предоставляет гибкий механизм динамического формирования так называемых "зон доверия", для которых позволяет определять политики безопасности;

- *контроль соответствия (compliance).*

  Определяя политики соответствия для индивидуальных виртуальных машин, или зон доверия, Reflex VMC контролирует их выполнение, и, в случае нарушения, позволяет предпринимать корректирующее воздействие (например, блокировать сетевое взаимодействие виртуальной машины), или просто информировать заданный круг лиц;

- *мониторинг основных параметров.*

  Протоколируя все изменения среды, Reflex VMC позволяет администратору получить целостную картину конфигурации по состоянию на любой момент времени, а возможности корреляции событий позволяют оценить влияние изменений конфигурации на работу систем.

Версия Reflex VMC для сервис-провайдеров позволяет обеспечивать необходимый уровень безопасности и для "облачных" технологий, когда при миграции виртуальных машин из ЦОДа заказчика в ЦОД сервис-провайдера, вместе с ними мигрируют (или даже применяются более жесткие) политики обеспечения безопасности.

Пожалуй, на сегодняшний день Reflex VMC является наиболее комплексным решением по обеспечению безопасности внутри виртуальной инфраструктуры.

HyTrust

Призером VMworld 2009 г. стала компания HyTrust, предложившая решение, ориентированное на контроль действий администраторов виртуальной инфраструктуры. Как уже говорилось выше, значительное количество угроз безопасности виртуальной инфраструктуры может быть нейтрализовано на уровне регламентов и ограничения прав доступа к управляющей инфраструктуре. Именно для решения этой задачи и предназначено решение HyTrust.

HyTrust Appliance перехватывает взаимодействие по всем каналам управления виртуальной инфраструктурой: доступ к Virtual Center, прямой доступ к серверам ESX, и т.п. и ограничивает действия администратора в строгом соответствии с определенными политиками безопасности. При этом, все действия администраторов протоколируются с детализацией, достаточной, как для проведения расследования инцидентов.

Еще одной особенностью HyTrust Appliance является возможность проверки конфигурации гипервизора в соответствии с рекомендациями производителя, требованиями отраслевых (например, PCI DSS) и корпоративных стандартов и устранения несоответствий одним щелчком мыши.

Если решение Reflex VMC сфокусировано на контроле и управлении действиями самих виртуальных машин, то HyTrust отлично дополняет его в части контроля соблюдения корпоративных политик безопасности в области контроля конфигураций и действий администраторов.

Заключение

Подводя итоги, можно сказать, что задача обеспечения требуемого уровня информационной безопасности в средах виртуализации уже вполне реализуема. Да, это не простой процесс, который потребует разработки внутренних стандартов и политик, внедрения новых регламентов, выбора и внедрения подходящих решений. Зато в конце пути вы сможете получать все преимущества от технологии виртуализации, не подвергая риску свою информацию.

Алексей Чеканов,
компания Almitech

Расширение функциональности Cisco MDS9000

Август 2009 г. – Компания Cisco анонсировала дополнительную функциональность для своего семейства MDS9000: Multilayer Directors – 9506, 9513, 9509 и Multilayer Fabric Switch – 9216. Новые возможности повышают уровень безопасности и ускоряют передачу данных на большие расстояния для сред хранения с мэйнфреймами IBM System z и на основе открытых систем.

Технологические расширения для семейства многоуровневых директоров Cisco MDS 9000:

- *более быстрая передача данных на расстояние – Cisco XRC Acceleration.*

  Разработанное совместно с IBM и предназначенное для использования с системой IBM z/OS Global Mirror, решение Cisco XRC Acceleration ускоряет передачу данных на большие расстояния через глобальную сеть (WAN), снижает нагрузку на канал передачи данных и сокращает время, необходимое для обновлений;

- *защита данных, передаваемых за пределы центра обработки данных – Cisco TrustSec Fibre Channel Link Encryption.*