

CNews.ru: Обзоры и обзоры



Код безопасности
ГК «Информзащита»



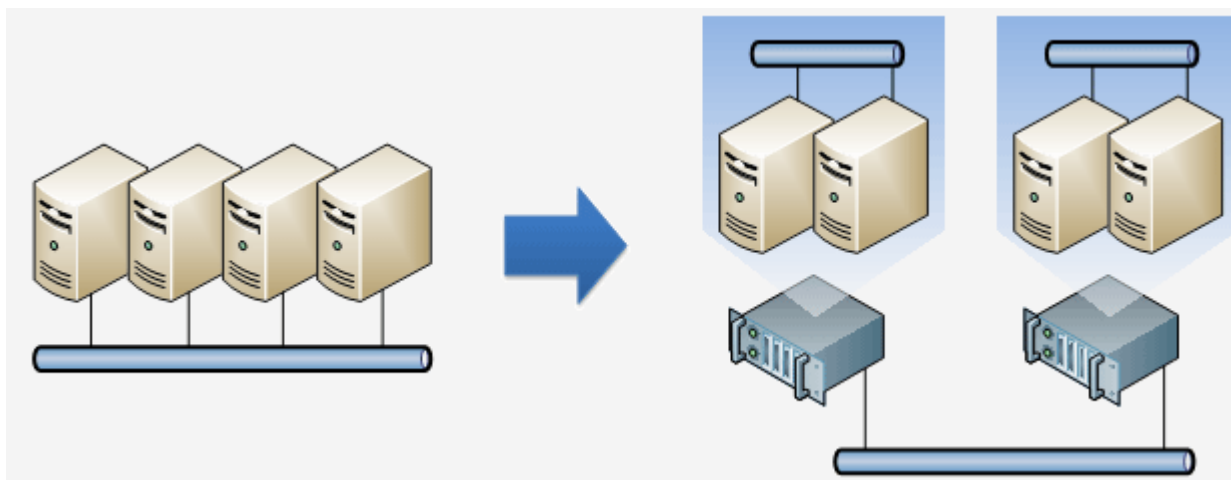
Почему безопасность виртуальных инфраструктур нельзя обеспечить только традиционными средствами защиты?

Возьмем за постулат то, что данные, которые мы обрабатываем в виртуальных машинах, должны быть защищены также надежно, как и в случае с физическими компьютерами. В чем же здесь различия?

Общеизвестно, какие преимущества приносит виртуализация. Это и радикальная экономия на инфраструктуре (за счет большей концентрации информационных систем на одном оборудовании), и повышение гибкости управления инфраструктурой, и повышение надежности работы приложений при сбоях «железа». Но, к сожалению, мало кто задумывается о том, что большинство этих, безусловно, положительных особенностей вносят дополнительные проблемы безопасности, которые нужно учитывать. А модели защиты традиционных средств защиты разрабатывались без учета особенностей виртуализации.

Предположим, у нас есть несколько компьютеров объединенных в локальную сеть и защищенных набором средств защиты. Стандартный набор средств защиты включает: средства аутентификации и управления доступом, межсетевые экраны, криптографические средства для шифрования или электронно-цифровой подписи, антивирусы, средства обнаружения вторжений и т.п. Кроме того, для полноты картины представим, что нами используются не только программные, но и аппаратные средства защиты. Такими могут быть, например, платы контроля целостности и доверенной загрузки компьютера (устройства PCI/PCI Express), аппаратные межсетевые экраны и отчуждаемые устройства для аутентификации или криптографии (смарт-карты, токены или «таблетки» Touch Memory).

Теперь представим ситуацию, что наша защищенная инфраструктура погружена в самую популярную виртуальную среду — VMware vSphere. Изменит ли это что-либо?



Сеть

Первое, что можно заметить — это то, что аппаратные межсетевые экраны становятся не везде применимы. Трафик между двумя виртуальными машинами, находящимися на одном хосте, уже не покинет его, а, следовательно, не будет проходить через межсетевой экран.

Таким образом, чтобы защититься от атаки одной скомпрометированной виртуальной машины на другую виртуальную машину, нам нужно применять иные решения. Кстати, ошибочно думать, что подобная угроза актуальна, только, в пределах одного хоста. Вполне можно представить себе ситуацию, когда на первом этапе скомпрометированная виртуальная машина получит контроль над виртуальными машинами на данном хосте, а на втором этапе, при vMotion одной из виртуальных машин на другой хост, компрометация распространится далее.

Второй важной сетевой особенностью виртуальных инфраструктур является то, что мы не можем больше закладываться исключительно на статические сетевые правила на коммутаторах. В физическом мире мы не привыкли (за исключением кластерных решений), что серверы могут постоянно перескакивать между физических портами, в то время как в виртуальной инфраструктуре в процессе vMotion это является порядком вещей.

Появились ли специализированные средства защиты на уровне сети в виртуальной среде? Да, и их достаточно много. Это входящий штатно в vSphere (начиная с редакции Advanced) виртуальный межсетевой экран vShield Zones. Также есть внушительное количество средств от сторонних производителей. Среди них: решение компании CheckPoint VPN-1 и продукт VMC от компании Reflex, продукты StoneGate Virtual IPS Appliance и StoneGate Virtual Firewall/VPN от компании StoneSoft. Существует также множество других решений.

Ложкой дегтя в данном случае является то, что на момент написания данной статьи на российском рынке еще не появились подобные сертифицированные решения по требованиям ФСБ или ФСТЭК. А значит, их применение официально не обеспечивает защиту персональных данных и конфиденциальной информации, обрабатываемой в виртуальной среде. Будем ждать развития в этой области.

Гипервизор и средства управления

Виртуальная инфраструктура помимо новых возможностей, несет еще и новые компоненты, по отношению к традиционной физической инфраструктуре. Этими компонентами являются собственно серверы виртуализации (включая ПО гипервизора и операционную систему), а также средства управления и обслуживания виртуальной инфраструктуры.

Поскольку появились новые программные компоненты, то появляются вопросы обеспечения их безопасности. Более того, с точки зрения информационной безопасности, ценность всех новых компонентов крайне высока. Причины тут две.

Во-первых, захват гипервизора или средств управления виртуальной инфраструктурой злоумышленником приведет к тому, что он сможет абсолютно незаметно для традиционных средств защиты информации (установленных в виртуальной машине) перехватывать данные, идущие через устройства ввода-вывода (включая сетевую активность, дисковую активность, и даже обращения к оперативной памяти). Кроме конфиденциальности данных, он, разумеется, также сможет нарушить целостность и доступность виртуальных машин.

Во-вторых, поскольку основная концепция виртуализации состоит в консолидации информационных систем на одном оборудовании (типичный коэффициент консолидации — 5-10 виртуальных серверов и до 60 виртуальных десктопов на одном хосте). Следовательно, вместе с плотностью растут и ставки потерь. Компрометация хоста будет приводить к компрометации всех виртуальных машин на нем, а захват централизованных средств управления виртуальной инфраструктурой, очевидно, приведет к компрометации всех виртуальных машин в рамках инфраструктуры. Очевидно, что защита данных компонентов стоит особняком.

В данной области хочется отметить продукты от компаний Catbird, HyTrust, а также продукт vGate for VMware Infrastructure российской компании «Код Безопасности». vGate в настоящий момент проходит сертификационные испытания ФСТЭК, что впоследствии даст возможность применять его для защиты конфиденциальной информации и персональных данных, обрабатываемых в виртуальной среде.

Аппаратные средства защиты

Виртуализация, по сути, разрывает прямую связь между нашими информационными системами и аппаратными средствами, на которых они работают. При разрыве нужно чем-то пожертвовать. Жертвой оказывается «куча железа», которую невозможно использовать в виртуальных машинах. В большинстве случаев с этим проблем не возникает, поскольку работает закон Парето — для 80% клиентов достаточно тех 20% поддерживаемого «железа».

Аппаратные средства защиты — устройства довольно специфические, и поэтому они зачастую и попадают в класс неподдерживаемого «железа». Это усугубляется тем, что разработчики таких устройств даже если желают, не всегда имеют достаточных возможностей для обеспечения их поддержки в виртуальной среде. Причина проста — при изначальном проектировании архитектуры устройства, никто не учитывал, что устройство может быть использовано одновременно несколькими операционными системами. Да если и учитывать при разработке такую возможность, то еще несколько лет назад не существовало для этого отработанных технологических решений, например, для PCI-устройств.

В общем, ситуация с традиционными аппаратными средствами в виртуальной среде на текущий момент не очень хорошая. Но есть надежда, что спустя некоторое время либо будут разработаны новые устройства, либо этот защитный функционал будет восполнен программными решениями, работающими в виде Virtual Appliances или агентов, функционирующих на ОС хоста.

Заключение

В качестве заключения, подведем некоторые выводы. Во-первых, в виртуальной среде следует применять новые средства защиты, учитывающие аспекты обеспечения информационной безопасности виртуализации. Во-вторых, далеко не все аппаратные средства защиты будут работать в виртуальной среде. В-третьих, новые компоненты (гипервизор, средства управления виртуальной инфраструктурой и т.п.) тоже нужно защищать. Причем комплексную и многоуровневую защиту могут обеспечить, только специализированные средства.

Константин Пичугов / менеджер по развитию продуктов компании «Код Безопасности»