ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ при использовании облачных технологий

Е.Кожемяка, ООО "Конфидент"

В статье раскрывается принцип действия облачных технологий и рассматриваются различные виды угроз, которым могут подвергаться данные в виртуальной среде. Особое внимание уделено средствам защиты информации, разработанным в ответ на существующие угрозы.

Облачные (рассеянные) технологии – технологии обработки данных, предоставляющие пользователю компьютерные ресурсы и мощности как интернет-сервис. Пользователь имеет доступ к своим данным, но не может управлять инфраструктурой, операционной системой и собственно программным обеспечением, с которым работает. Для поддержки облачных вычислительных сред используются технологии виртуализации. В бизнесе применяется несколько видов виртуализации:

- виртуализация серверов – перенос физических серверов в виртуальные машины (ВМ) одного физического сервера (хостовой системы), оснащенного средством виртуализации (гипервизором);
- виртуализация рабочих мест пользователей – централизованное хранение рабочих мест (виртуальных десктопов) в виде ВМ на сервере (хостовой системе) с предоставлением доступа по сети с физических рабочих мест (тонких клиентов);
- виртуализация терминалов – для пользователя терминала создается собственный сеанс работы в ОС.

Угрозы безопасности облачных технологий и виртуализации

Приведем наиболее актуальные угрозы для виртуально-облачной среды.

Среди угроз, направленных на АРМ конечных пользователей, можно выделить компрометацию клиентских устройств доступа в облако и атаки на клиентские браузеры. Эти угрозы актуальны вследствие слабой защиты АРМ конечных пользователей и отсутствия контроля политики информационной безопасности (ИБ) на АРМ пользователей при доступе в облака.

Через гипервизор реализуется такая угроза виртуальной инфраструктуре, как несанкционированный доступ (НСД) к среде виртуализации. Он возможен вследствие нарушения изоляции среды, предоставленной клиенту в рамках облачной услуги. Например, может использоваться уязвимость в реализации инструкции SYSRET всех процессоров Intel архитектуры x86-64. Также НСД возможен вследствие плохой очистки клиентской информации на стороне провайдера облачных услуг. Кроме того, вследствие некорректных настроек гипервизора возможен несанкционированный доступ к ресурсам ВМ из реальной или виртуальной среды. В рамках виртуальной среды НСД возможен вследствие программных закладок или ошибок в ПО гипервизора. Вследствие эксплуатации уязвимостей гипервизора возможны атаки на сервер с гипервизором из сетевой среды типа "переполнение буфера" и "отказ в обслуживании".

DDoS-атаки на сетевую инфраструктуру между облаком и клиентом возможны вследствие развертывания плохо защищенных ВМ и отсутствия в составе гипервизора средств защиты сетевой инфраструктуры. Случайное или умышленное стирание (искажение) образов ВМ возможно вследствие отсутствия средств разграничения доступа и контроля целостности виртуальной среды.

В числе угроз виртуальной инфраструктуре, реализуемых через систему управления виртуальной средой, можно назвать перехват аутентификационных данных для доступа к облаку через облачные API (Application Programming Interface – интерфейс прикладного программирования), а также получение несанкционированного доступа к консоли управления виртуальной средой путем подбора пароля или перехвата текущей сессии (атака "человек посередине") из-за отсутствия средств защищенного удаленного доступа и создания виртуальных частных сетей (VPN). Одной из угроз виртуальной инфраструктуре, реализуемой через сеть передачи данных, является перехват данных при передаче по незащищённым каналам связи между облаком и клиентом.

Некоторые традиционные угрозы виртуальной инфраструктуре реализуются вследствие уязвимости физических серверов, на которых она развернута. В их числе сетевые атаки между виртуальными машинами в рамках одного хоста, подмена и/или перехват данных и оперативной памяти ВМ в процессе их миграции средствами виртуальной среды, вирусное заражение ВМ и использование их уязвимостей. Причинами,порождающими эти угрозы, являются размещение плохо защищенных ВМ или ВМ с разным уровнем конфиденциальности в рамках единой аппаратной платформы и несоответствие политики ИБ процессу миграции ВМ. Такое несоответствие происходит из-за отсутствия в виртуальной инфраструктуре распределенных коммутаторов, позволяющих согласовывать политику безопасности при миграции ВМ.

Через систему хранения данных могут реализовываться такие угрозы виртуальной инфраструктуре, как несанкционированное копирование разделов системы хранения на съемные устройства хранения из-за отсутствия средств контроля доступа к съемным устройствам. Возможна кража или физическое уничтожение данных сети хранения из-за отсутствия средств защиты данных в процессе хранения (шифрование, резервное копирование). Также возможно получение несанкционированного доступа к АРМ администратора или интерфейсам сети хранения, несанкционированное копирование или уничтожение разделов сети хранения из-за отсутствия средств ограничения доступа и контроля целостности. Несанкционированное подключение разделов системы хранения (LUN) к аппаратной платформе с виртуальными машинами, не имеющими права обрабатывать эти данные, возможно из-за отсутствия средств контроля аппаратной конфигурации. Из-за отсутствия средств защиты удаленного доступа возможно проведение атак типа "спуфинг" или "человек посередине" на уровне сети хранения данных.

Таким образом, наиболее актуальными для облачных сервисов считаются такие угрозы, как компрометация клиентских устройств доступа в облако, перехват данных при передаче по незащищённым каналам связи и несанкционированный доступ к среде виртуализации.

Проблемы обеспечения безопасности облачных технологий

При организации защиты облачных сред существует целый ряд проблем. Кратко охарактеризуем некоторые из них.

В виртуальной среде следует применять новые средства защиты, способные обеспечить ее информационную безопасность. Далеко не все аппаратные средства защиты будут работать в виртуальной среде. Например, аппаратные межсетевые экраны не могут разграничить доступ к различным серверам, находящимся внутри одного хоста. Традиционный аппаратный коммутатор не сможет поместить ВМ одного хоста в разные VLAN.

Применение технологий виртуализации привносит в сетевую архитектуру новые элементы, например, гипервизор и средства управления виртуальной инфраструктурой, которые также нужно защищать, так как изменение инфраструктуры открывает возможности для новых методов атак. Комплексную и многоуровневую защиту могут обеспечить только специализированные средства.

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 серверы виртуализации и не проходит через физические

межсетевые экраны и другое физическое сетевое оборудование.

Уход от традиционного периметра к отсутствию контролируемой зоны, перемещение ВМ между физическими серверами приводит к необходимости реализации политик ИБ независимо от физических границ. Сложно найти баланс между централизованными мерами обеспечения ИБ, реализуемыми поставщиком инфраструктурных услуг, и локальными, обеспечиваемыми клиентом. Риск компрометации повышается при размещении ВМ с разным уровнем конфиденциальности на одном физическом сервере. Взлом гипервизора может привести к взлому всех ВМ.

Единоличная ответственность за сеть и за ИБ возникает из-за недооценки руководством информационных рисков компании и приводит к тому, что администратор сети – лицо, являющиеся потенциальным нарушителем, – имеет бесконтрольный доступ ко всем ресурсам. Он может, например, переписать на терабайтный съемный диск всю информацию, являющуюся интеллектуальной собственностью компании, или совершить любые другие злонамеренные действия, оставшись при этом незамеченным.

Правовые аспекты взаимодействия между клиентом и провайдером облачных сервисов не проработаны. Отсутствуют сертифицированные ФСТЭК и ФСБ решения для всех уровней безопасности виртуализации.

Средства защиты данных при использовании облачных технологий

Так какие же безопасные способы использования облачных технологий существуют? Предлагаем рассмотреть один из подходов к защите облачных технологий.

Для защиты от несанкционированного доступа рабочих мест пользователей, хостовой системы и системы хранения данных предлагается использовать традиционные сертифицированные средства защиты от НСД, такие как Dallas Lock компании "Конфидент" и Secret Net компании "Код безопасности".

Для антивирусной защиты ВМ предлагается использовать новаторский безагентный подход, обеспечивающий комплексную безопасность без установки агентского модуля в защищаемой системе. К примеру, безагентный режим использует решение Deep Security компании Trend Micro. В виртуальную среду внедряется виртуальное устройство – шлюз безопасности, который берет на себя функции антивируса для всех ВМ. Для шифрования трафика, усиленной аутентификации, аудита и межсетевого экранирования ВМ совместно с Deep Security предлагается использовать Secure Cloud компании Trend Micro.

Необходимо использовать системы обнаружения вторжений и межсетевого экранирования. С появлением виртуальных сред появилась новая проблема – неконтролируемое сетевое взаимодействие между ВМ. Общая рекомендация такова: контролировать внешние подключения к среде виртуализации следует с помощью аппаратных решений, а внутренние – с помощью программных решений, реализуя таким образом комбинированный подход. Для контроля трафика как между ВМ внутри хоста, так и со стороны каждой ВМ в отдельности предлагается использовать решение Deep Security компании Trend Micro.

Обеспечить эффективную защиту от сетевых угроз позволяет семейство продуктов StoneGate Virtual Security компании Stonesoft, включающее в себя виртуальный межсетевой экран StoneGate Virtual Firewall/VPN и систему предотвращения вторжений StoneGate Virtual IPS, а также StoneGate Virtual SSL VPN. Дополнительный плюс в том, что продукты Virtual Firewall/VPN и Virtual IPS сертифицированы ФСТЭК и ФСБ для платформ VMware ESX/vSphere и поддерживают технологию VMsafe.

Компания Cisco Systems предлагает виртуальную реализацию своих коммутаторов на базе Cisco Nexus 1000V, в том числе с возможностью создания распределенных коммутаторов на нескольких физических узлах, что позволяет создавать согласованные политики безопасности при миграции ВМ. Cisco Virtual Security Gateway и Cisco ASA 1000V Cloud добавляют возможности для расширенного контроля сетевого трафика. Эти виртуальные устройства интегрируются с коммутатором Cisco Nexus 1000V, который может поддерживать несколько гипервизоров и позволяет одному экземпляру ASA 1000V защищать несколько виртуальных серверов VMWARE с развернутыми на них виртуальными машинами.

Компания CheckPoint может предложить продукты VPN-1 VE (Virtual Edition) – виртуального устройства, которое обеспечивает защиту виртуальных сред от внешних и внутренних угроз безопасности. Продукт состоит из нескольких

модулей: межсетевого экрана, системы предотвращения вторжений, средства VPN, антиспама, антивирусного сканера сетевых потоков, URL-фильтра и защиты WEB-трафика.

Управление конфигурацией виртуальной среды и мониторинга состояния информационной безопасности зачастую не реализуется обычными средствами управления, такими как VMware vCenter. К лидирующим продуктам здесь можно отнести VMC компании Reflex и vSecurity компании Catbird. Оба решения имеют центр управления и виртуальные устройства, размещаемые на серверах VMware.

Еще одним средством защиты, заслуживающим внимания, является комплексное решение – Virtual Management Center (VMC) компании Reflex, позволяющее контролировать сетевой трафик. В Reflex VMC входят компоненты, которые позволяют повышать эффективность эксплуатации, защиту и расширенный мониторинг:

- vCapacity обеспечивает планирование основных параметров виртуальной среды и динамическое управления конфигурацией;
- vTrust выполняет функции обеспечения сетевой безопасности внутри виртуальной инфраструктуры. vTrust осуществляет мониторинг и контроль трафика между виртуальными машинами, реализует настройку политики безопасности на уровне виртуальных иашин, организует виртуальные зоны доверия, обеспечивает динамическое управление сетью вне зависимости от физического расположения виртуальных ресурсов;
- vWatch позволяет администратору получить всесторонний обзор состояния виртуальной среды на любой момент времени и оценить влияние изменения конфигурации на работу системы;
- vProfile осуществляет контроль за соблюдением требований внутренних и внешних стандартов, обеспечивает единую конфигурацию всей виртуальной инфраструктуры. Например, контроль соответствия политике безопасности позволяет в блокировать сетевое взаимодействие виртуальных машин, контроль основных настроек гипервизора позволяет быстро привести виртуальную среду в соответствие с рекомендациями производителя или отраслевыми стандартами (например, PCI DSS).

Решение vSecurity компании Catbird реализует расширенные функции аудита, инвентаризацию объектов и программного обеспечения виртуальной инфраструктуры (включая ПО, установленное на сами ВМ), сетевой контроль и защиту гипервизора от сетевых атак, а также управление конфигурациями. Решение гарантирует соблюдение заданных с точки зрения ИБ параметров и позволяет управлять изменениями и уязвимостями.

Сертифицированными средствами защиты информации от НСД, контроля выполнения политик информационной безопасности и управления доступом к виртуальной инфраструктуре для виртуальной среды на базе систем VMware vSphere 4 и VMware vSphere 5 служат продукты vGate R2 и vGate-S R2 компании "Код безопасности".

Защиту доступа к виртуальной инфраструктуре осуществляет решение HyTrust этой же компании. Как и многие средства защиты для виртуальных сред, оно представляет собой виртуальное устройство. Решение позволяет повысить безопасность виртуальной инфраструктуры за счет перехвата всех соединений пользователей с ней и разграничения доступа по ролям с применением меток безопасности.

Кроме традиционных средств защиты информации конечных пользователей, таких как средства защиты от НСД и антивирусных средств, особую важность приобретают контроль выполнения политики ИБ конечными устройствами и надежная аутентификация с применением аппаратных средств и безопасного удаленного доступа, для реализации которых используется, например, StoneGate Virtual SSL VPN. Эти средства помогут снизить риски одной из наиболее актуальных угроз – компрометации клиентских устройств.

В отдельный класс можно выделить средства резервного копирования, восстановления данных и миграции ВМ. Среди них Data Recovery от VMware, BackUp & Replication 5 от компании Veeam Soft-ware, System Recovery 2011 Virtual Edition от Symantec Corporation и Backup & Recovery 11.5 Advanced Platform от Acronis International.

Как мы видим, многие средства защиты обеспечивают сразу несколько функций, что позволяет удешевить систему защиты, построив ее на продукции одного вендора. Ряд средств защиты имеют сертификаты ФСТЭК и ФСБ России, что позволяет выполнить требования регуляторов при построении системы защиты в государственном секторе. ■