Безопасность облачных вычислений

Обзор требований по информационной безопасности, которым должны удовлетворять виртуализованные ЦОД с доступом к ИТ-ресурсам через Интернет.

Михаил Кондрашин – эксперт по продуктам и сервисам Trend Micro.

Введение

Переход на облачные вычисления обещает заманчивые возможности, как для компаний, предоставляющих интернет-услуги, так и для предприятий, активно использующих ИТ-технологии в своей работе. Сделав ставку на облачные вычисления, предприятия могут обеспечить себе экономию средств, гибкость и свободный выбор вычислительных мощностей. Такой подход позволяет расширить свою ИТ-инфраструктуру, добавляя необходимую емкость по мере необходимости.

В данной статье мы рассмотрим облачные вычисления, которые получили название "инфраструктура по требованию" (Infrastructure as a Service – IaaS). Нас будут интересовать аспекты информационной безопасности, связанные с переходом к облачной инфраструктуре. Мы постараемся дать рекомендации по информационной безопасности провайдерам и предприятиям, которые позволят перейти к использованию инновационных технологий, не породив дополнительных рисков.

Новые возможности, которые дают облачные вычисления

Почему в последнее время столько шума вокруг облачных вычислений?

Общие тенденции индустрии. Независимые аналитики и компании, такие как Amazon, Cisco, Citrix, Dell, EMC, Google, HP, IBM, Microsoft, Sun, VMware и многие другие единодушно поддерживают облачные вычисления.

Гибкость. Гибкость, которую предлагает для современных предприятий облачный подход трудно переоценить. Например, можно полностью передать на внешний или внутренний (в случае частных облаков) аутсорсинг аппаратное обеспечение, но оставить за собой управление ИТ-инфраструктурой. С другой стороны, возможна передача всех аспектов своей ИТ-инфраструктуры провайдеру. Возможен и смешанный подход, который чаще всего реализуется под влиянием отдельных департаментов компании, – внедряется смешанная ИТ-инфраструктура, где присутствуют сегменты, частично переданные на аутсорсинг.

Экономия. Инфраструктура по требованию позволяет сделать затраты на ИТ более эффективными. Зачастую ограничения на число ИТ-специалистов, а также нежелание увеличивать капитальные расходы сдерживают внедрение инноваций. Сезонные всплески потребности в вычислительных ресурсах требуют построения избыточной ИТ-инфраструктуры. Облачные вычисления являются существенно более экономически оправданной альтернативой.

В самом простом понимании облачные вычисления существенно расширяют способности предприятий отвечать потребностям в вычислительной мощности в любой перспективе. Гибкость и свобода выбора, мобильность и масштабируемость, дополненные потенциальной возможностью экономии, являются серьезными аргументами в пользу перехода к облачным вычислениям. Тем не менее, есть один фактор, который сдерживает компании от перехода к использованию подобных технологий. Таким фактором является безопасность.

Компания IDC провела опрос 244 ИТ-руководителей и их коллег с целью выяснить уровень использования облачных услуг в их компаниях и их личное мнение относительно данных технологий. Угрозы безопасности оказались главным недостатком облачных вычислений (рис. 1).

Безопасность и законодательные требования в облачных вычислениях

Предоставление конфиденциальных данных за периметром корпоративной сети и размещение их в облачных средах порождает серьезные опасения у организаций, которые традиционно основываются на защите периметра сети как основного средства безопасности своих ЦОД (центров обработки данных). Кроме этого, такой шаг может нарушать некоторые государственные законы и стандарты в области ИБ. ИТ-руководители, осознавая преимущества, которые обеспечивают облачные вычисления и предполагают их использование, задаются следующими вопросами:

- Буду ли я иметь тот же уровень контроля над соблюдением политик безопасности при использовании моих приложенияй?
- Могу ли я доказать своей компании и клиентам, что все надежно защищено и все SLA (соглашения об уровне сервиса) будут соблюдены?
- Соответствует ли ИТ-инфраструктура законодательству и смогу ли я доказать это аудиторам?

Для того чтобы начать отвечать на поставленные вопросы, давайте кратко рассмотрим аспекты защиты традиционного ЦОД и влияние виртуализации, то есть той самой технологии, которая позволила начаться революции облачных вычислений.

Защита традиционного ЦОД

Термин "ЦОД" довольно долго ассоциировался с масштабными фермами серверов, размещенных в специальных закрытых помещениях, где бесперебойное электропитание и оптимальный микроклимат, не менее важны для доступности и защи-

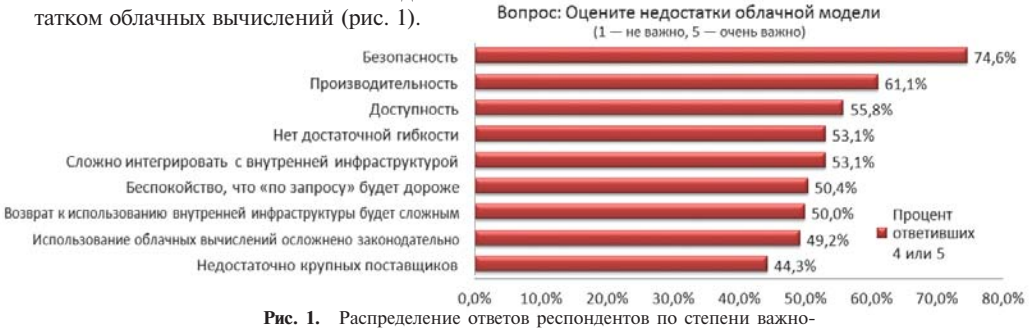

Рис. 1. Распределение ответов респондентов по степени важности недостатков облачной модели вычислений.

щенности данных, чем сетевая безопасность. Наиболее традиционным подходом к сетевой защите ЦОД является обеспечение безопасности периметра. Этот подход обычно предполагает использование пограничного брандмауэра, выделение демилитаризованных зон (DMZ), сегментацию сети, системы обнаружения и предотвращения вторжений (IDS/IPS), а также средства контроля состояния сети.

Виртуализация – катализатор перехода к облачным вычислениям

Виртуализация позволяет предприятиям получить больше вычислительной мощи от недоиспользованных вычислительных возможностей физических серверов. Соответственно, масштаб традиционного ЦОД уменьшается, позволяя снизить расходы на его обслуживание за счет консолидации серверов. Кроме этого, виртуализация позволяет предприятиям и сервис-провайдерам предоставлять индивидуальные услуги, используя приложения, которые изначально использовались единым способом всеми, размещая в разных виртуальных средах копии приложения с различными настройками.

Перемещение существующих физических/виртуальных машин (ВМ) из ЦОД во внешние облака или предоставление ИТ-сервисов вне безопасного периметра в частных облаках, приводит к тому, что периметр сети полностью теряет смысл, а общий уровень безопасности становится довольно низким. Невозможность физического разделения и применения аппаратных средств сетевой защиты в условиях, когда множество серверов размещено на одном физическом сервере приводит к необходимости размещения механизмов защиты приложений непосредственно на сервере или ВМ, а защиту информации связывать непосредственно с самими данными.

Только внедрение подобной линии обороны на самой ВМ позволит переместить критически важные приложения в облачные среды. Ниже описан продукт Trend Micro Deep Security, который обеспечивает необходимую защиту, но сначала нужно детально описать трудности, возникающие на пути к облачным вычислениям.

Трудности защиты облачных сред

На первый взгляд, требования к безопасности облачных вычислений кажутся сходными с требованиями к обычным ЦОД – применение средств сетевой безопасности и авторизации. Тем не менее, как было указано выше, физическое разделение и аппаратные средства сетевой защиты не могут защитить от атак на ВМ внутри одного сервера. Компании, предоставляющие услуги облачных вычислений, для повышения эффективности виртуализации вынуждены размещать ВМ разных организаций на одних и тех же физических ресурсах. Детальное рассмотрение перечисленных ниже аспектов является первоочередным при планировании перехода на любые виды облачных вычислений.

Доступ администраторов к серверам и приложениям

Одной из самых важных характеристик облачных вычислений является “самообслуживание”, то есть доступ через Интернет к управлению вычислительной мощностью. Такая возможность существенно отличается от работы в традиционных ЦОД, где доступ инженеров к серверам строго контролируется на физическом уровне. В облачных вычислениях доступ инженеров происходит через Интернет, что приводит к появлению соответствующих угроз. Соответственно, критически важным является строгий контроль доступа для администраторов, а также обеспечение контроля и прозрачность изменений на системной уровне.

Динамические ВМ: состояние ВМ и изменчивость

Виртуальные машины динамичны. Они могут быть оперативно возвращены в предыдущее состояние, а также легко приостановлены и перезапущены. Кроме этого, ВМ могут быть клонированы, а также перемещены между физическими серверами. Подобная изменчивость ВМ очень сильно усложняет создание и поддержание целостной системы безопасности. Уязвимости и ошибки в настройках могут бесконтрольно распространяться. Кроме этого, весьма непросто зафиксировать для последующего аудита состояние защиты в какой-либо определенный момент времени. В средах облачных вычислений требуется иметь возможность надежно зафиксировать состояние защиты системы, безотносительно от ее местоположения и состояния.

Уязвимости и атаки внутри виртуальной среды

Серверы облачных вычислений используют те же ОС и те же веб-приложения, что и локальные виртуальные и физические сервера. Соответственно, для облачных систем угроза удаленного взлома или заражения вредоносным кодом через уязвимости точно так же высока. На самом деле, риск для виртуальных систем даже выше, так как параллельное существование множества ВМ существенно увеличивает атакуемую поверхность. Кроме того, появляется угроза взлома или заражения внутри одной физической системы, когда одна ВМ заражает или атакует другую. Система обнаружения и предотвращения вторжений должна быть способной детектировать вредоносную активность на уровне ВМ, вне зависимости от расположения ВМ в облачной среде.

Защита бездействующих ВМ

В отличие от физической машины, когда ВМ выключена, все еще есть возможность ее компрометации или заражения. Для этого достаточно какого-либо доступа к хранилищу образов ВМ через сеть. С другой стороны, выключенная ВМ не имеет абсолютно никакой возможности запустить какое-либо ПО для защиты от вредоносного кода. В средах облачных вычислений ответственность за защиту и сканирование бездействующих ВМ лежит на провайдере. Предприятия, которые используют сервисы облачных вычислений, должны убедиться в том, что провайдер использует подобные средства безопасности в своей среде виртуализации.

Влияние традиционной безопасности на производительность

Существующие решения по безопасности создавались до появления технологии виртуализации систем x86 и, соответственно, они спроектированы без учета работы в виртуальной среде. В облачной среде, где ВМ различных пользователей разделяют единые аппаратные ресурсы, единовременное сканирование во всех виртуальных системах приведет к катастрофическому снижению производительности всей виртуальной среды. Провайдеры облачных услуг, предоставляющие базовые функции безопасности своим клиентам, в состоянии избежать этой проблемы, осуществляя ресурсоемкие сканирования на уровне гипервизора, избегая, таким образом, конкуренции за вычислительные ресурсы на уровне каждой ВМ.

Целостность данных: компрометация систем и кража данных

Согласно отчету “2008 Data Breach Investigations Report”, опубликованному Verizon Business Risk Team, 59% утечек данных являлись результатом взлома хакерами. Нужно полагать, что специализированные ресурсы являются более защищенными, чем ресурсы разделяемые. Соответственно, атакуемая поверхность полностью или частично разделяемой облачной среды должна быть больше и находится под большей угрозой. Предприятия должны обладать возможностью проверить лично и доказать внешним аудиторам, что ресурсам не нанесен вред и что системы не скомпрометированы, особенно в ситуации, когда они размещаются в разделяемой физической среде. Целостность операционной системы и файлов приложений, а также внутренняя активность должны контролироваться.

Шифрование и защита данных

Многие законы и стандарты, такие как PCI DSS и HIPAA, включают в себя требования использования криптографических средств для защиты важной информации, такой как информация о владельце кредитной карты и информация, идентифицирующая человека. Криптографическая защита подобных данных является “тихой гаванью”, то есть защищает компанию от санкций закона, в случае, если данные будут утеряны. Использование многопользовательских облачных сервисов усложняет следование требованиям стандартов и законов, что порождает непростую задачу обеспечения надежной защиты и безопасного доступа к важным данным.

Управление обновлениями

Услуги облачных вычислений предполагают самообслуживание, что может породить путаницу в управлении обновлениями. Как только компания подписалась на облачный сервис, например, создание веб-сервера из шаблонов, управление установкой обновлений на платформу и веб-сервер уже не находятся в ведении провайдера. С этого момента за обновление отвечает клиент. Отметим, что, в соответствии с упомянутым выше отчетом “2008 Data Breach Investigations Report” компании Verizon, для 90% известных уязвимостей, которые на практике использовались злоумышленниками, обновления были выпущены более чем за 6 месяцев до инцидента. Следовательно, организации, использующие облачные вы-

числения, должны быть бдительны и стараться обеспечить все приложения, работающие в облаке, новейшими обновлениями. Если оперативная установка обновлений невозможна или непрактична, то необходимо рассмотреть альтернативный подход – использование "виртуальных заплат". Технология "виртуальных заплат" предполагает блокировку нацеленных на уязвимости атак непосредственно на сетевом уровне, что не позволяет вредоносному коду или злоумышленникам каким-либо способом воспользоваться неустраненной уязвимостью.

Политики и соблюдение законов

Предприятия прикладывают существенные усилия для соответствия различным законам и следованию всевозможным стандартам, таким как PCI, HIPAA и GLBA, а кроме этого, проводят аудиты в соответствии с разнообразными рекомендациями (SAS70 и ISO). Необходимо обеспечить компании возможностью доказать соблюдение законов и стандартов безопасности, вне зависимости от расположения используемых систем, являющихся объектом регулирования (физические серверы, виртуальные серверы, серверы, размещенные в облачных средах).

Защита периметра и разграничение сети

При использовании облачных вычислений, периметр корпоративной сети исчезает, и защита наименее защищенной составляющей сети определяет общий уровень защищенности. Корпоративный брандмауэр, основной компонент для внедрения политик безопасности и разграничения сегментов сети, не в состоянии повлиять на серверы, размещенные в облачных средах. Его политики не в состоянии повлиять на доступ к тем или иным ресурсам – теперь это ответственность провайдера облачных вычислений. Для разграничения сегментов с разным уровнем доверия в облаке ВМ должны сами обеспечивать себя защитой, фактически перемещая сетевой периметр к самой ВМ.

Подготовка ВМ к использованию в облачной инфраструктуре

Виртуализация – это подготовка технологии к использованию в облачных вычислениях. Организации, которые не используют облачные вычисления сегодня, чаще всего рассматривают переход на них в будущем. ЦОДы, которые уже консолидировали свои физические серверы в виде ВМ, могут уже сейчас предпринять шаги для повышения уровня защиты своей виртуализованной среды, а также подготовить ВМ к миграции в облачные среды, когда такая необходимость возникнет.

Ниже приведен список 5 технологий безопасности, которые включают в себя продукт Trend Micro Deep Security: брандмауэр, обнаружение и предотвращение вторжений, контроль целостности, анализ журналов и защита от вредоносного ПО. Программные агенты этого продукта, будучи установленными на виртуальных и физических машинах (поддерживаются платформы Windows, Solaris, Linux, HP-UX и AIX), способны повысить уровень защищенности и соответствие законодательным требованиям на серверах при переносе в виртуальную и облачную среды.

Брандмауэр – уменьшение атакуемой поверхности виртуализированных серверов в средах облачных вычислений.

Брандмауэр содержит в себе предустановленные шаблоны для типовых корпоративных серверов, которые обеспечивают следующие возможности:

– изоляция ВМ;

– тонкая фильтрация трафика (адрес отправителя и получателя, порт);

– покрытие всех протоколов семейства IP (TCP, UDP, ICMP, ...);

– покрытие всех типов сетевых фреймов (IP, ARP, ...);

– предотвращение атак класса "отказ в обслуживании" (DoS);

– создание политик с точностью до каждого сетевого интерфейса;

– обнаружение и рекогносцировочное сканирование на серверах облачных вычислений;

– учет местоположения, что позволяет применять строгие политики одновременно с гибкостью, позволяющей перенос сервера из внутренней сети на облачные ресурсы;

Обнаружение и предотвращение вторжений (IDS/IPS) – экранирование уязвимостей операционной системы и корпоративных приложений до того момента, когда будут установлены "заплаты", для отражения известных и неизвестных (zero-day) атак.

Как было указано выше, ВМ и облачные серверы используют те же операционные системы и приложения, что и традиционные серверы. Внедрение системы обнаружения и предотвращения вторжений в виде программного агента на ВМ позволяет экранировать уязвимости, обнаруженные в ОС и приложениях:

– защита от любых атак на известные уязвимости без установки заплат;

– блокировка атак типа XSS и SQL Injection.

Контроль целостности – отслеживание изменений в файлах, системе и реестре.

Контроль целостности операционной системы и приложений позволяет выявить опасные изменения, которые являются следствием компрометации системы. Эта подсистема включает в себя:

– проверку по запросу или расписанию;

– всесторонний контроль свойств файлов, включая атрибуты (отвечает требованиям пункту 10.5.5 стандарта PCI);

– контроль на уровне директорий;

– гранулированную настройку объектов контроля;

– отчеты для аудита.

Анализ журналов – выявление существенных событий с точки зрения информационной безопасности в файлах журналов.

Анализ журналов собирает и анализирует журналы работы операционной системы и приложений на предмет событий безопасности. Правила анализа журналов позволяют выявить значимые события в огромном массиве записей. Это:

– обнаружение подозрительного поведения;

– сбор действий администратора, имеющих отношение к безопасности;

– сквозной сбор событий со всего ЦОД.

Защита от вредоносных программ, учитывающая виртуализацию – антивирус, адаптированный для использования в виртуальной среде.

Защита от вредоносных программ, учитывающая виртуализацию, использует специальные программные интерфейсы, которые предоставляет гипервизор, такие как VMsafe компании VMware, для защиты как активных, так и бездействующих ВМ. Защита включает в себя как уровень проверки самих виртуальных машин, так и агента внутри каждой ВМ, обеспечивающие проверку в реальном времени. Такой подход гарантирует, что ВМ очищена, даже если была неактивна, а также актуальность ее защиты при последующем запуске. Не менее важным свойством защиты, специализированной для защиты ВМ является бережное отношение к вычислительным ресурсам при проверке всей системы. Это:

– предотвращение угроз со стороны вредоносного кода для активных и бездействующих машин;

– защита от вредоносных программ, который деинсталлируют или блокируют работу антивируса;

– интеграция с панелью управления системой виртуализации (VMware vCenter);

– автоматическая настройка защиты новых ВМ.

Вместо заключения

Провайдеры облачных вычислений используют технологии виртуализации для предоставления своим клиентам доступ к недорогим вычислительным ресурсам. При этом ВМ клиентов разделяют одни и те же аппаратные ресурсы, что необходимо для достижения наибольшей экономической эффективности. Корпоративные заказчики, которые интересуются облачными вычислениями для расширения своей внутренней ИТ-инфраструктуры, должны учитывать угрозы, которые порождает подобный шаг. С переносом ВМ на публичные облачные сервисы периметр корпоративной сети теряет смысл и на общий уровень безопасности начинают значительно влиять наименее защищенные узлы. Невозможность физического разделения и применения аппаратных средств безопасности для отражения атак между ВМ приводит к потребности размещения механизма защиты на сервере виртуализации или на самих ВМ. Внедрение на самой ВМ рубежа защиты, включающего в себя программную реализацию брандмауэра, обнаружения и предотвращения вторжений, контроля целостности, анализа журналов и защиты от вредоносного кода, является наиболее эффективным способом защиты целостности, соответствия требованиям регуляторов, соблюдения политик безопасности при перемещении виртуальных ресурсов из внутренней сети в облачные среды. Дальновидные компании и сервис-провайдеры внедряют подобную защиту на свои ВМ уже сегодня, с тем, чтобы в будущем воспользоваться преимуществами облачных вычислений раньше своих конкурентов.

Михаил Кондрашин