Облака – это не омут

Не бросайтесь в них с головой! Важно выработать стратегию перехода, которая будет учитывать все особенности бизнеса компании. На вопросы «БИТа» отвечают эксперты ведущих ИТ-компаний

1. *В прошлом году заметно повысился интерес компаний к технологиям контейнерной виртуализации. Чем, по-вашему, этот интерес вызван?*
2. *Как понять, каков будет экономический эффект от виртуализации в период кризиса? Она требует серьезных инвестиций, экономия же достигается в долгосрочной перспективе.*
3. *Прогнозы по поводу развития инфраструктуры виртуальных десктопов (VDI) не оправдались. Почему?*
4. *Каковы актуальные угрозы и уязвимости виртуальных сред?*
5. *Теория – это всегда интересно, но работают ли облака на практике?*
6. *По наблюдениям экспертов облачные технологии уже находятся на высокой стадии технической зрелости. А как обстоят дела со зрелостью юридической и управленческой?*
7. *Какие решения и услуги в области виртуализации, облачных технологий предлагает ваша компания?*

Александр Веселов, начальник отдела технического консалтинга ООО «С-Терра СиЭсПи»

2. Во многих ситуациях виртуализация позволяет существенно экономить в долгосрочной перспективе. Но далеко не всегда это означает инвестирование в собственную виртуальную инфраструктуру. Повсеместный переход в виртуальное пространство повлек за собой появление нового сегмента рынка – аренду услуг ЦОД. Клиент может арендовать не только место в стойке, но и инфраструктуру, доступ к определенным приложениям и даже обеспечение бизнес-процессов. Постепенно рынок движется в сторону полноценных, законченных услуг.

Давайте подумаем, насколько сегодня актуальна дилемма – инвестировать в собственную виртуальную инфраструктуру или принять сервисную модель?

Мы наблюдаем регулярное, порой скачкообразное, повышение цен, которое приводит к невозможности бюджетирования будущих инвестиций. Сервисная модель позволяет сократить краткосрочные расходы и обеспечивает прогнозируемое планирование, поэтому в последнее время позиции сервисной модели значительно окрепли.

Если ранее заказчик планировал развернуть инфраструктуру на собственных мощностях, то при нынешней экономической ситуации его выбор чаще останавливается на различных услугах ЦОД – PaaS, IaaS и даже BPaaS. Таким образом, заказчик может за умеренную стоимость обеспечить свои текущие потребности.

Похвастаться долгосрочным планом сейчас может далеко не каждая компания, поэтому направление инвестиций в собственную инфраструктуру постепенно ослабевает.

4. При нынешних тенденциях (использование сервисной модели виртуализации) влияние клиента на безопасность значительно снижается, а сфера ответственности компании, предоставляющей услугу, наоборот, значительно расширяется. Может ли она обеспечить требуемый уровень конфиденциальности, доступности и целостности – большой вопрос.

При пользовании услугами ЦОД на первый план выходит угроза несанкционированного доступа – как со стороны сотрудников ЦОД, так и от других арендаторов. Чтобы не переживать об утечке конфиденциальных данных из ЦОД, нужно выбирать проверенных поставщиков услуг с прозрачным SLA или пойти более сложным путем – построить свой собственный ЦОД (пусть и не такой масштабный, как у поставщиков услуг).

Следующий момент – работа гипервизора. В виртуальной среде несколько виртуальных машин работает на одном физическом сервере и теоретически может каким-то образом влиять друг на друга. Что делать в этом случае: доверять лидерам рынка гипервизоров, использовать специализированные средства защиты или переходить на отечественные гипервизоры? Однозначного ответа здесь нет и быть не может, обсуждение этих вопросов достойно отдельной статьи.

7. При централизации ресурсов (как правило, в ЦОД) возникает задача защищенного удаленного доступа к данным (мы говорим об информации, составляющей, например, коммерческую тайну, или о персональных данных). Задача, которая при расположении ресурсов в офисе решалась сама собой, теперь требует отдельной проработки и выбора средств криптографической защиты. Кроме того, виртуальная среда обычно разделена на сегменты с различными уровнями доступа (к ним и между ними), например: общедоступные извне серверы, сервисы для контрагентов и внутренние сегменты. Разграничение доступа между этими областями – важная и далеко не простая задача.

Компания «С-Терра СиЭсПи» предлагает заказчику проверенное решение на базе VPN-продуктов С-Терра, которое гармонично впишется в виртуальную инфраструктуру.

Виртуальный шлюз С-Терра, встраиваемый непосредственно в виртуальную среду, является концентратором VPN-туннелей для центральной точки. Криптошлюз работает согласно международным стандартам IKE/IPsec (RFC 2401-2412), с применением алгоритмов шифрования ГОСТ. Ключевым преимуществом виртуального шлюза является наличие сертификата ФСБ РФ как СКЗИ класса КС1, а также сертификатов ФСТЭК. Применение виртуального шлюза позволит не только экономить место в стойке и энергопитание, но и соблюдать требования современного законодательства нашей страны.

С-Терра Виртуальный Шлюз для гипервизоров VMware, Xen, KVM и Hyper-V сертифицирован ФСБ РФ по классу КС1

С помощью виртуального шлюза можно обеспечить как безопасную связь с территориально распределенными офисами, так и защищенный удаленный доступ сотрудников. Более того, виртуальный шлюз позволяет защитить также трафик внутри виртуальной среды, обеспечив безопасное взаимодействие различных компонентов. Благодаря наличию в нем сертифицированного межсетевого экрана есть возможность выделения нескольких зон безопасности с разными категориями доступа внутри виртуальной среды.

Для объектов, которым необходим защищенный удаленный доступ к виртуальным ресурсам, мы можем предложить широкий спектр VPN-продуктов: шлюз в виде виртуальной машины или программно-аппаратного комплекса, клиенты под ОС Windows и Android, а также специальный защищенный терминал.