Защита виртуализации:
вчера, сегодня, завтра

Александр ВЕСЕЛОВ,
ведущий инженер, ЗАО «С-Терра СиЭсПи»

Уже не раз говорилось о преимуществах виртуализации: простота установки, перераспределение ресурсов между виртуальными машинами, удобное резервное копирование и восстановление, экономия электроэнергии и мест в стойке. К этому мы привыкли на прикладных сервисах, а теперь прогресс дошел до сетевого оборудования и средств защиты информации: межсетевые экраны, криптошлюзы, системы обнаружения вторжений и другие средства защиты теперь тоже работают в виртуальной среде. Но с распространением виртуализации возникли новые угрозы, связанные с особенностями этой перспективной технологии, – размытие понятия «периметр», несанкционированный доступ к виртуальным машинам, атаки на гипервизор и его недекларированные возможности. Для противодействия новым угрозам используются механизмы защиты, встроенные в гипервизоры, а также отдельные средства защиты виртуальной инфраструктуры.

Переход в виртуальное пространство повлек за собой появление нового сегмента рынка – аренда 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 и к отказу от предоставления отдельных компонентов.

При таких тенденциях влияние клиента на безопасность значительно снижается, а сфера ответственности компании, предоставляющей услугу, наоборот, расширяется. Может ли она обеспечить требуемый уровень конфиденциальности, доступности и целостности – большой вопрос. Отчасти это связано с тем, что обеспечение информационной безопасности во многих случаях является лицензируемым видом деятельности и подразумевает соответствие стандартам, нормативным документам, отраслевым требованиям и т. д. Причем законодательство существенно отстает от развития технологий, что приводит к значительным неудобствам, а в некоторых случаях к невозможности выполнения требований.

Ранее в органах регулирования не делали различий между традиционной и виртуальной инфраструктурами, но обновленная нормативная база уже начала формироваться. В финальной стадии согласования находятся проекты государственных стандартов «Требования по защите информации, обрабатываемой с использованием технологии виртуализации» и «Требования по защите информации, обрабатываемой с использованием технологий «облачных вычислений». Это основополагающие документы, которые позволят однозначно трактовать новые термины и станут основой для многих других нормативных актов. Требования по защите виртуализации в государственных информационных системах (ГИС) уже разработаны и утверждены ФСТЭК России.

Несмотря на то что требования появились относительно

недавно, рынок отреагировал на эти нововведения. Уже сейчас производители предлагают продукты как для обеспечения безопасной работы в виртуальной среде, так и для обеспечения безопасности самой виртуальной среды. Конечно, в гипервизорах есть встроенные механизмы защиты, но если они сертифицированы, то, как правило, представляют собой довольно старую версию, с невозможностью легитимной установки обновлений. Поэтому целесообразно использовать средства защиты в виде отдельных специализированных продуктов.

Специалистов по информационной безопасности сложно назвать энтузиастами рынка, они довольно прагматичны и стараются использовать проверенные средства защиты, которых немало в сегменте сетевой безопасности. Это продукты как западных компаний (например, межсетевые экраны Cisco Systems), так и отечественных (в частности, VPN-продукты «С-Терра»). Виртуальный шлюз С-Терра представляет собой не только сертифицированный межсетевой экран, но и средство криптографической защиты информации на основе технологии IPsec VPN с поддержкой алгоритмов ГОСТ. Основная его задача – построение защищенных соединений как между виртуальными машинами, находящимися на одном и нескольких физических серверах, так и с внешними объектами (site-to-site и/или remote access). Если раньше рядом с сервером виртуализации приходилось выделять для шлюза место в стойке, заботиться об электропитании, сетевых интерфейсах и т. д., то теперь можно встроить VPN-шлюз непосредственно в виртуальную инфраструктуру. Это позволяет значительно снизить энергопотребление и сократить расходы на развертывание. Виртуальный шлюз не зависит от аппаратной платформы, что дает возможность поставлять его в кратчайшие сроки и оперативно решать задачи заказчика. Перечисленные факторы особенно важны для компаний, предоставляющих «Безопасность как сервис» в комплекте с другими привычными услугами ЦОД. Кроме того, продукт сертифицирован ФСБ России по классу КС1 и позволяет выполнять требования современного законодательства (например, ФЗ № 152 «О персональных данных»).

> Требования по защите виртуализации в государственных информационных системах (ГИС) уже разработаны и утверждены ФСТЭК России.

Ближайшая потребность рынка – расширение перечня средств защиты виртуальной среды, а также традиционных продуктов, работающих в виртуальной среде. Ведь из-за их отсутствия заказчик вынужден в лучшем случае применять «компенсирующие» меры, а в худшем – использовать неполноценную систему защиты, подвергая свою информационную систему опасности. Кроме того, актуальной становится тема разработки доверенного отечественного гипервизора. Одной из угроз является не полностью документированная работа гипервизора: не всегда понятна работа с памятью, которую виртуальные машины делят между собой, под сомнением хранение ключевой информации. Вероятность, что западные производители пойдут на тесное сотрудничество, например раскрытие кода, с органами регулирования, крайне мала. А это влечет за собой отсутствие высоких классов сертификации. Выход здесь только один – разработка собственного гипервизора и дальнейшая его сертификация.

Подводя итоги и перечисляя многочисленные преимущества виртуализации, связанные с эксплуатацией инфраструктуры, не стоит забывать и о новых угрозах. Процесс миграции традиционных средств защиты в виртуальную среду необходим, но не достаточен. Требуется применять эти средства в комплексе со специализированными механизмами обеспечения безопасности виртуальной среды. Только в такой ситуации можно обеспечить легитимную и надежную защиту. ■

> Ближайшая потребность рынка – расширение перечня средств защиты виртуальной среды, а также традиционных продуктов, работающих в виртуальной среде.