Код безопасности
ГК «Информзащита»

Обеспечение информационной безопасности данных клиентов с помощью решения vGate при предоставлении услуг облачных ЦОДов

Информация, представленная в данной статье, будет полезна как для сервис-провайдеров, так и для клиентов облачных ЦОДов

ноябрь 2011

Обеспечение информационной безопасности данных клиентов с помощью решения vGate при предоставлении услуг облачных ЦОДов

Виртуализация на платформе VMware позволяет владельцам облачных ЦОДов предложить своим клиентам эффективные решения для бизнеса. Неограниченная масштабируемость ресурсов в сочетании с эффективной моделью оплаты, предлагаемой в модели облачных сервисов, делает услуги виртуализированных облачных ЦОДов, построенных с использованием технологий VMware, привлекательными для многих корпоративных пользователей.

Тем не менее, недоверие компаний к уровню обеспечения безопасности информации в облачных инфраструктурах все еще сказывается на том, что только ограниченное количество компаний принимает решение о переходе на использование этой модели. Облачная модель в понимании корпоративных заказчиков соотносится со многими рисками информационной безопасности.

Среди наиболее актуальных для компаний ИБ-рисков, препятствующих переходу на облачную модель, можно перечислить следующие:

- риски в области целостности данных, сохранности данных, восстановления данных;
- риски несанкционированного доступа к данным;
- риски невыполнения требований стандартов безопасности и регулирующего законодательства;
- риски ненадлежащего аудита и оценки соответствия стандартам и лучшим практикам (PCI DSS, CIS Networking и др.);
- риск возникновения несоответствия корпоративным политикам безопасности.

Выбирая провайдера, компании должны принимать решение о сотрудничестве с поставщиком облачных сервисов не только на основе общераспространенных критериев, касающихся доступности сервисов, масштабируемости системы, производительности системы, но и на основе оценки возможностей сервис-провайдера осуществлять предотвращение рисков информационной безопасности. При выборе сервис-провайдера компаниям необходимо учесть следующие аспекты информационной безопасности:

В области осуществления контроля доступа:

Круг людей, имеющих полномочия доступа к данным клиентов облачного ЦОДа, должен быть ограничен, и все входящие в него специалисты должны быть юридически ограничены действием Договоров о неразглашении (Non-Disclosure Agreements).

В области выполнения требований законодательства:

При использовании облачной модели сервис-провайдер должен брать на себя обязанности по выполнению требований законодательства, в юрисдикции которого находится компания-клиент. Доля ответственности провайдера должна быть определена и закреплена подписанием специального Договора.

В области осуществления контроля соответствия:

Клиенты провайдера облачных сервисов должны быть уверены, что все изменения виртуальных машин контролируются и не приводят к потере системой в целом соответствия требованиям стандартов и законодательства.

В случае, когда сервис-провайдер не может предложить своим клиентам решения для перечисленных проблем, его предложение услуг на рынке может значительно проигрывать по сравнению с другими предложениями от конкурирующих провайдеров. И напротив, внедрение специализированных средств защиты информации, может стать сильным конкурентным преимуществом, которое также поможет преодолевать недоверие клиентов, связанное с информационными рисками в облаке.

Для того, чтобы обеспечить сохранность данных клиентов и предложить учитывающую риски виртуализации на платформе VMware систему безопасности, виртуализированным ЦОДам, предоставляющим облачные сервисы, необходимо использовать специализированные ИБ -решения, такие как vGate разработки компании «Код Безопасности».

vGate – средство предотвращения рисков информационной безопасности в облаке

Разграничение доступа

vGate предоставляет возможности аутентификации ИТ-администраторов и разграничения доступа к данным, хранящимся и обрабатывающимся в облачной инфраструктуре, построенной на платформе VMware, что является одним из основных аспектов обеспечения информационной безопасности при использовании облачных вычислений.

При внедрении такого средства защиты, как vGate, все операции по настройке и обслуживанию инфраструктуры, производимые ИТ-персоналом датацентра, строго контролируются. Это возможно благодаря системе разграничения прав и контроля доступа, входящей в функциональные возможности vGate. При этом права на произведение настроек и конфигурацию инфраструктуры получают только те ИТ- специалисты, обслуживающие датацентр, которым предоставлены права на эти операции руководителями или специалистами службы информационной безопасности датацентра. При этом ИБ-специалисты получают в системе vGate только права на выдачу и подтверждение прав ИТ-специалистов, но не права на доступ к данным виртуальных машин и серверов. Таким образом, происходит разделение прав на конфигурацию и настройку (такие права получают ИТ-специалисты) и прав на предоставление и подтверждение данных полномочий ИТ-специалистам (такие права назначают и подтверждают ИБ-специалисты).

Защищенное хранение данных

vGate позволяет обеспечить разграничение данных и ресурсов разных клиентов датацентра с помощью встроенного механизма бизнес-меток. Таким образом, помеченные разными бизнес-метками хранилища, виртуальные машины и сервера защищены от доступа администраторов с отличными бизнес-метками. Это позволяет избежать рисков несанкционированного доступа к данным и использования ресурсов одной компании, являющейся клиентом облачного сервис-провайдера, администраторами другой компании-клиента этого сервис-провайдера.

Контроль выполнения политик безопасности

vGate обеспечивает формирование политик из готовых шаблонов, применение их и контроль выполнения политик безопасности на уровне виртуальных машин и предоставляет отчеты о произошедших изменениях настроек политик безопасности. Использование vGate позволяет производить автоматическое восстановление несанкционированно измененных настроек (путем восстановления заданной конфигурации или блокирования загрузки виртуальной машины с измененными настройками).

Обеспечение соответствия стандартам и лучшим практикам

В состав программного продукта vGate входят шаблоны настроек безопасности виртуальных инфраструктур в соответствии с положениями и требованиями отраслевых стандартов безопасности, таких как PCI DSS, CIS Networking, ESX Benchmark и других. На основе этих шаблонов настраиваются политики безопасности. Это позволяет автоматизировать приведение инфраструктуры в соответствие с названными стандартами и снизить нагрузку на IT администраторов, а также избежать ошибок при ручной настройке. Наличие шаблонов позволяет проводить проверку соответствия и необходимые настройки системы каждый раз, когда это необходимо.

Выполнение требований российского законодательства

Шаблоны настроек, включенные в vGate, также позволяют автоматически привести виртуализированные инфраструктуры в соотвествие с требованиями ФЗ-152 «О Персональных данных».

vGate сертифицирован ФСТЭК России и ФСБ России и может быть применен для защиты информации в АС до уровня 1Г включительно и в ИСПДН до уровня К1 включительно.

Специальная версия продукта vGate R2 может быть применена в АС, которым присвоен уровень 1Б, и в которых обрабатывается информация с грифом «государственная тайна».

Аудит и отчетность

vGate включает гранулированные системы предоставления отчетности как виртуальной инфраструктуры, так и собственных настроек vGate. Сервис-провайдер получает возможность предоставлять пользователям сервиса подробные индивидуализированные в зависимости от потребностей компании отчеты о событиях безопасности и настройках безопасности. Сервис-провайдер также может использовать возможности системы отчетности vGate для собственных задач контроля выполнения политик безопасности в облачном дата-центре.

Код Безопасности
ГК «Информзащита»

Почтовый адрес: 127018, Россия, Москва, а/я 55.
Адрес офиса в Москве: ул. Образцова, д. 38.
Адрес офиса в Санкт-Петербурге: Свердловская наб., д. 44.
Тел.: +7 (495) 980-2345 (многоканальный).
Факс: +7 (495) 980-2345.
E-mail: info@securitycode.ru
Запрос дополнительной информации о продуктах: info@securitycode.ru
По вопросам стоимости и покупки продуктов sales@securitycode.ru
По вопросам партнерства и сотрудничества info@securitycode.ru

Вы можете узнать подробную информацию о продуктах на сайте
www.securitycode.ru

О компании «Код Безопасности»

Компания «Код Безопасности» – российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, коммерческой и государственной тайны, а также среды виртуализации. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

«Код Безопасности» входит в группу компаний «Информзащита», которая уже около 15 лет является лидером российского рынка информационной безопасности.

ООО «Код Безопасности» ведет свою деятельность на основании лицензий ФСТЭК России и ФСБ России.