Как защитить данные от IaaS-провайдера?

Денис Безкоровайный – технический консультантTrend Micro в России и СНГ.

Снижение рисков утечки данных при развертывании корпоративных приложений в публичных облаках – одна из самых острых проблем, которая часто заставляет отказываться от преимуществ этого вида ИТ-услуг многие компании. И, хотя сейчас уже многие провайдеры предлагают собственные интегрированные средства обеспечения безопасности пользовательских данных, и на рынке также представлены соответствующие решения ИБ от третьих фирм, проблема остается.

Во-первых, это связано с тем, что, несмотря на подписание соответствующих соглашений с провайдером публичных ИТ-услуг, контроль за персоналом провайдера не доступен клиентам ИТ-услуг, что вызывает элемент беспокойства. *Во-вторых*, интеграция какого-либо дополнительного оборудования и/или ПО в инфраструктуру провайдера – это сложная процедура, требующая как времени, так и затрат, и часто добавить что-то по желанию клиента в типовую инфраструктуру провайдера просто невозможно.

Шифрование данных в облаке – один из основных защитных механизмов, снижающих риски компрометации данных, рекомендованных Cloud Security Alliance.

Компания Trend Micro – одна из первых стала предлагать решение Trend Micro™ SecureCloud (версия 1.1 анонсирована в марте 2011 г., текущая версия 2.0), которое при полной прозрачности для приложений и неизменности формата данных для приложений, а также какомлибо влиянии на инфраструктуру и ПО провайдера во многом позволяет снять остроту этой проблемы.

Решение Trend Micro™ SecureCloud реализует полное шифрование устройства/диска (FDE – Full Disk Encryption) на уровне операционной системы как для физических, так и для виртуальных машин (ВМ) в облачной среде. Криптографическое ядро продукта сертифицировано по FIPS 140-2.

Продукт позволяет напрямую интегрироваться с несколькими основными распространенными платформами для создания и управления платформой облачных сервисов (IaaS) и виртуальной инфраструктурой:

- VMware vCloud Director 1.0/1.5;
- VMware vSphere 4/5 (ESX 4/5);
- Eucalyptus 1.6/2.0;
- Amazon EC2.

Вендоры в своем стремлении быть интероперабельными предлагают решения, позволяющие управлять гетерогенными ресурсами и объединять вычислительные мощности под контролем различных гипервизоров в единую облачную инфраструктуру. Например, платформа для создания IaaS-облаков от Eucalyptus поддерживает как гипервизоры VMware, так и open-source гипервизоры Xen и KVM. Так как SecureCloud работает с IaaS-платформой, то защита будет одинаково эффективной для ВМ, работающих на любом из поддерживаемых облачной платформой гипервизоров.

В SecureCloud три основных компонента – агент, сервер управления ключами и консоль управления.

При загрузке операционной системы ВМ-агент SecureCloud формируется запрос на получение ключа расшифрования к серверу управления ключами. На сервере управления ключами выполняется обработка запроса – вручную администратором безопасности или автоматически на основе заранее настроенных политик. Политики определяют набор критериев, по которым одобряется или отвергается запрос на ключ. Например: кто запрашивает ключ; какая это виртуальная машина (имя, IP адрес и т.д); когда она была запущена и где (в каком датацентре); можно ли выдавать ключ этой машине; установлен ли на ней антивирус с последней версией сигнатур; присутствуют ли на ней другие системы защиты; не нарушена ли целостность критичных файлов? Все это можно проверить либо напрямую агентом SecureCloud, либо с помощью глубокой интеграции с другим продуктом для защиты датацентров от Trend Micro – Deep Security, используя который заказчик уже может иметь настроенные профили защиты и правила контроля целостности.

В случае одобрения запроса на выдачу ключа, агент получает ключ по защищенному каналу и осуществляет расшифровку и подключение защищенного диска к уже работающей ВМ. После этого зашифрованный диск становится прозрачно доступным для ОС и приложений, например, СУБД или веб-серверу.

Для расположения сервера управления ключами доступны несколько вариантов:

- в ЦОДе компании Trend Micro – высоконадежном и внешнеаудируемом, сертифицированном по ISO 27001;
- в ЦОДе компании-заказчика;
- в ЦОДе сервис-провайдера услуги управления ключами (это может быть провайдер, отличный от провайдера услуг IaaS).

В первом случае клиенты получают возможность управлять ключами шифрования с помощью внешней услуги SecureCloud от Trend Micro.

Поддержка в SecureCloud протокола KMIP позволяет использовать внешний аппаратный HSM (Hardware Security Module) для еще большей надежности хранения ключей.

При интеграции в приложение дополнительных операций по шифрованию/дешифрованию данных всегда встает вопрос о накладных затратах на процессор. Тестирование показывает, что накладные расходы при использовании продукта SecureCloud не превышают 3-7% от базового уровня.

Система шифрования и управления ключами Trend Micro™ SecureCloud позволяет:

- сделать все защищаемые данные клиента, украденные у сервис-провайдера, нечитаемыми и бесполезными для нарушителя;
- предотвращать несанкционированный доступ к данным клиента в облачном датацентре провайдера;
- контролировать ключи шифрования заказчиком и отделять функцию защиты данных от облачного провайдера;
- авторизовывать запросы на ключи вручную и автоматически на основе политик;
- гарантировать невозможность доступа других клиентов провайдера к защищаемым данным компании при повторном использовании жестких дисков в облачной среде;
- поддерживать масштабируемость для множества ВМ;
- поддерживать независимость от технологии облачного провайдера (снижение lock-in риска);
- обеспечивать контроль доступа к данным в облаке при ограниченных возможностях аудита облачного провайдера;
- обеспечивать контроль данных в облаке при смене провайдера или его закрытии;
- обеспечивать защиту данных при краже всей машины или ее виртуальных дисков.