Доверие в облаках

Основные задачи и технические средства их реализации в области повышения доверия пользователя к провайдеру облачной инфраструктуры

Сергей ВИХОРЕВ,
заместитель генерального директора по развитию ОАО «ЭЛВИС-ПЛЮС»

Все чаще в новостных лентах можно увидеть сообщения о том, что та или иная компания использует либо планирует использовать для обработки информации в своей корпоративной сети сервисы, предоставляемые провайдером облачной инфраструктуры. Однако при этом возникает множество проблем, и одна из важнейших – обеспечение безопасности. По некоторым данным, примерно половина рабочей нагрузки серверов сейчас уже виртуализирована, однако средства безопасности информации еще не отвечают новым требованиям. Приобретая облачный сервис, каждый пользователь рассчитывает на его надежность. Вместе с тем провайдеры не могут самостоятельно решить все вопросы защиты пользовательской информации, но и пользователь, получив виртуальную машину из облака и установив в нее собственное программное обеспечение, не в состоянии своими силами сделать такую систему эффективной. Провайдерам приходится каждого пользователя отдельно убеждать в надежности предоставляемых систем защиты.

Проблемы облаков

При организации защиты облачных технологий возникают две взаимосвязанные группы проблем: нормативно-правовые и технологические.

Нормативно-правовые проблемы объясняются отсутствием нормативов и требований по защите виртуальных сред и типовой модели угроз для облачной среды, непроработанностью концептуальных вопросов обеспечения безопасности информации, отсутствием правовой основы отношений провайдер-пользователь, неурегулированностью отношений при трансграничности облачной среды. Технологические же проблемы связаны с сужением возможности использования традиционных средств защиты (технологии виртуализации не всегда позволяют применять традиционные методы обеспечения безопасности информации, например, использование традиционных средств антивирусной защиты может привести к снижению производительности), наличием возможности доступа сисадмина к серверам и приложениям (сервисы, предоставляемые разным клиентам, базируются на единой инфраструктуре провайдера, а процедуры управления этой инфраструктурой в значительной степени непрозрачны для пользователя), обязательным присутствием в процессе обработки информации нового элемента – гипервизора (и, как следствие, проблемой обеспечения его целостности), динамичностью виртуальных машин и наличием ее бездействующих клонов, потере контроля над периметром сети (что усугубляется тем, что провайдер зачастую сам арендует мощности у других компаний). Вот и получается, что при использовании облачной среды необходимо защищаться как от давно известных и относительно универсальных угроз, так и от новых, присущих именно облачной среде. Если защиту от первых можно строить, используя существующие продукты и уже отработанные решения, то защита от специфических облачных рисков может потребовать разработки новых подходов и продуктов. И кроме того, в этих условиях остро стоит вопрос повышения доверия пользователя к провайдеру.

Триединая задача доверенного облака

Специфика применения облачных технологий обработки информации наглядно показывает, что добиться требуемого уровня доверия к провайдеру, решая по отдельности только нормативно-

Vihorev.indd 22 16.08.2012 18:39:20

правовые или технологические проблемы, невозможно. И как ни странно, решение технологических проблем стоит далеко не на последнем месте. Поэтому рассмотрим технологические аспекты проблем, одним из перспективных направлений решения которых является создание доверенного облака.

Защиту при использовании облачных технологий обработки информации логичнее всего представить в виде трех подсистем:

- подсистемы безопасности пользовательской (виртуальной) информационной системы;
- подсистемы безопасности провайдера: серверов, БД, ПО виртуализаторов и пр.;
- подсистемы обеспечения доверия пользователя к провайдеру.

Только решив эту триединую задачу можно быть уверенным в безопасности при использовании облачной инфраструктуры обработки информации. При этом доверенная среда облачной инфраструктуры должна позволять пользователю убедиться, что сама среда является безопасной. И именно пользователь должен иметь право принимать решение о возможности начала обработки информации. Спасение утопающих – дело рук самих утопающих!

Первые две подсистемы во многом похожи на подсистемы, применяемые для обеспечения безопасности информации в обычных, не облачных, информационных системах. Сейчас на рынке существует широкий спектр продуктов, реализующих такую защиту. Однако при их применении необходимо учитывать специфику облачной инфраструктуры, например отсутствие периметра виртуальной сети пользователя в обычном понимании (это, в частности, обусловливает необходимость использования топологии VPN «точка – точка» вместо VPN-шлюзов).

Третья подсистема является, пожалуй, основным элементом, специфичным именно для облачных вычислений. На сегодняшний день в качестве обеспечения доверия пользователя к провайдеру предлагается, по сути, только один способ: заключение соглашения об уровне услуг (Service Level Agreement, SLA). Ясно, что для многих пользователей этого будет недостаточно, особенно с учетом того факта, что провайдеры услуг неохотно берут на себя обязательства по защите информации. Например, один из крупнейших провайдеров услуг по облачным технологиям Amazon Web Services в своем «Соглашении с клиентом» особо отмечает: «…7.2. Безопасность. Мы стремимся обеспечить безопасность Ваших данных, однако не можем полностью гарантировать ее в связи с природой Интернета. Соответственно… Вы признаете, что несете полную ответственность за безопасность, защиту и резервное копирование своего содержимого и приложений». К тому же в российских условиях вопросы, связанные с несоблюдением SLA со стороны провайдера, очень далеки от решения.

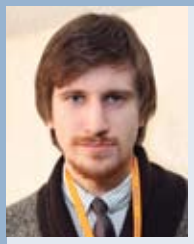
Ключевая проблема

Таким образом, одной из ключевых проблем при использовании облачных структур является вопрос доверия пользователя к провайдеру. Предоставить свои информационные ресурсы другой стороне в условиях, когда неизвестны ни серверы, на которых будут храниться и обрабатываться данные пользователя, ни даже место, где это будет происходить, достаточно рискованно, а для некоторых пользователей, например государственных структур, может оказаться просто неприемлемым. Следовательно, актуальна задача построения технологической составляющей системы безопасности, позволяющей поднять доверие пользователя к провайдеру на уровень выше, чем это обеспечивается соглашением об уровне услуг (SLA). Особое место в такой системе занимает механизм, позволяющий пользователю убедиться, что действия провайдера соответствуют принятому соглашению и регламенту обработки информации.

В исследованиях Gartner[1] среди специфических для облаков источников рисков безопасности, на которые необходимо обращать особое внимание при выборе провайдера, отмечена, в частности, необходимость оценки провайдера с точки зрения предоставления возможности сегрегации данных. Это имеет ключевое значение, если пользователь планирует разместить в облачной среде свою критичную информацию. Причем нужно отследить, что провайдер обеспечивает не только разделение информации (данных) между группами пользователей, но и

[1] *Jon Brodkin: Gartner: Seven Cloud-Computing Security Risks. CIO.com, July 03, 2008 – http://www.cio.com/article/423713/Gartner_Seven_Cloud_Computing_Security_Risks*

мнение специалиста



Юрий СЕРГЕЕВ,
системный архитектор Центра информационной безопасности компании «Инфосистемы Джет»

Основным сдерживающим фактором при переходе в публичное IaaS-облако, несмотря на все экономические преимущества, часто становится страх нарушения конфиденциальности данных компаний. Существуют два пути для реализации подобных нарушений. Первый становится возможным за счет копирования сотрудником провайдера виртуального жесткого диска с информацией. Второй – после того как часть дискового пространства, используемая вашим ресурсом, была передана вашему соседу по облаку без должной очистки остаточной информации.

Эффективно решить данные проблемы позволяет продукт Trend Micro SecureCloud, обеспечивающий криптографическую защиту на уровне жесткого диска. Основными его преимуществами являются простота использования и, что особенно важно, схема распределения ключей, обеспечивающая отсутствие ключей шифрования в защищаемой системе, которые могут быть использованы злоумышленником для компрометации данных. Вся ключевая информация хранится на сервере управления, который физически можно разместить на своей площадке либо воспользоваться услугами интегратора или производителя по модели Security-as-a-Service. При этом решение интегрируется с модулем контроля целостности продукта Deep Security, что позволяет при автоматизированном принятии решения о монтировании зашифрованного раздела проверять систему на предмет ее неизменности.

Vihorev.indd 23 16.08.2012 18:39:21

обособление информации (данных) всех пользователей от областей, доступных администраторам облачной инфраструктуры.

Обеспечение сегрегации информации (данных)

В настоящее время многие облачные структуры типа IaaS строятся на базисе существующих ЦОДов и уже выбранных технологий виртуализации. Поэтому актуальна задача создания в облачной инфраструктуре механизма, обеспечивающего надежную сегрегацию пользовательских данных разной категории и их изоляцию от администраторов самой облачной инфраструктуры. Желательно, чтобы такое решение не потребовало замены существующей облачной инфраструктуры – виртуализаторов, аппаратных платформ и т. п.

Обеспечение требуемой сегрегации критичной для пользователя информации при использовании облачной инфраструктуры типа IaaS возможно путем построения комплекса связанных друг с другом систем:

- доверенного контроля целостности виртуальной среды;
- контролируемого пользователем прозрачного шифрования виртуальных дисков критичных серверов;
- контролируемого пользователем шифрования виртуальных сетевых взаимодействий (VPN).

Первым шагом для построения подобного комплекса должна стать проверка в соответствующих испытательных лабораториях используемого для создания виртуальной инфраструктуры программного обеспечения на отсутствие недекларированных возможностей (НДВ), а также проверка возможности обеспечения таким ПО сегрегации (изолирования) данных между виртуальными машинами (ВМ) и способности исключить, в том числе и для администраторов облачной инфраструктуры, возможность получения внешнего доступа к оперативной памяти работающих виртуальных машин.

Система доверенного контроля целостности виртуальной среды должна обеспечивать доверенную загрузку виртуальной среды и контроль целостности виртуализатора (проверку соответствия контрольных сумм его текущего образа эталону). И только в случае положительных результатов такой проверки ключи аутентификации физического сервера могут быть доступными. Ядром такой системы является независимый аппаратно-программный компонент, хранящий критичную информацию (ключи, контрольные суммы) в защищенном виде и обеспечивающий доступ к результатам контроля только по защищенному каналу. Таким компонентом могут служить или уже имеющиеся модули доверенной загрузки в совокупности с электронными замками, или встроенный непосредственно в компьютер чип безопасности типа TPM. Последнее предпочтительней, так как встроенный чип обеспечивает строгую аутентификацию аппаратно-программной платформы облачной инфраструктуры.

Система доверенного контроля целостности виртуальной среды существенно облегчает решение и других специфических для облачных технологий рисков, связанных с неготовностью провайдера подвергнуть оценке соответствие облачной инфраструктуры установленным требованиям и необходимостью контроля местоположения данных, который позволит ограничить допустимые местоположения физических серверов из общего множества доступных для запуска виртуальной машины в зависимости от специфических требований пользователя к конфиденциальности обработки данных.

Следующая система – система контролируемого пользователем шифрования виртуальных дисков критичных серверов. Она позволяет прозрачным образом шифровать данные на диске пользовательской виртуальной машины как в выключенном, так и в работающем состоянии. Доступ к ключу шифрования контролирует пользователь виртуальной машины, который и принимает решение о предоставлении доступа к ключу шифрования на основании строгой аутентификации аппаратно-программной платформы физического сервера и результатов контроля целостности виртуализатора. Если контрольные суммы текущего образа виртуализатора соответствуют эталону, который исключает возможность внешнего доступа к оперативной памяти работающих виртуальных машин, пользователь может загрузить ключи шифрования в оперативную память своей виртуальной машины. При этом ключи шифрования критичных данных остаются под контролем обладателя информации. Данная процедура работы с ключами может происходить как в ручном, так и в автоматическом режиме. Техническая реализация системы может быть основана на решениях подобных MS BitLocker или на некоторых новых решениях компании ЭЛВИС-ПЛЮС. Система устанавливается в уже существующую и развернутую виртуальную машину как дополнительное приложение.

> Шифрование виртуальных дисков позволяет решить проблему конфиденциальности, связанную с еще одним источником риска при применении облачных технологий — необходимостью обеспечения восстановления данных (резервное копирование).

Шифрование виртуальных дисков позволяет решить проблему

Vihorev.indd 24 16.08.2012 18:39:21

конфиденциальности, связанную с еще одним источником риска при применении облачных технологий – необходимостью обеспечения восстановления данных (резервное копирование).

Система контролируемого пользователем шифрования виртуальных сетевых взаимодей-ствий (VPN) может быть развернута на базе любой системы защиты сетевых взаимодействий (IPsec, SSL). Для сегрегации передаваемых данных и защиты сетевых взаимодействий от администраторов облачной инфраструктуры создается выделенная защищенная подсеть, построенная по схеме «точка – точка» для всех серверов с критичными данными. Управление доступом к ключам пользователя осуществляется в этом случае аналогично системе шифрования виртуальных дисков.

В ряде случаев, когда требуются не только сегрегация критичных данных и изоляция их от администраторов облачной инфраструктуры, но и защита ключей и систем шифрования от самой пользовательской виртуальной машины, применима архитектура «матрешки»: система шифрования виртуальных дисков и VPN не устанавливается как дополнительные приложения непосредственно в ОС пользователя, а запускается внутри виртуальной машины, в которой работает уже сама рабочая пользовательская виртуальная машина или сервер.

Резюме

Проблема обеспечения без-опасности информации при использовании облачных технологий обработки информации в настоящее время еще не решена, но определенные шаги в этом направлении уже сделаны. Многие вендоры, производящие традиционные средства защиты, начали выпуск специализированных средств защиты, ориентированных на использование в виртуальных инфраструктурах. Создаются альянсы, направленные на создание интегрированных сервисов и специализированных решений для комплексной защиты облачных инфраструктур (средства защиты средств управления облачной инфраструктурой от несанкционированного доступа (НСД); средства контроля целостности конфигурации виртуальных машин и доверенной загрузки; средства аутентификации администраторов облачных инфраструктур и администраторов ИБ; межсетевые экраны, ориентированные на работу в виртуальных инфраструктурах; средства мониторинга и контроля трафика).

Итак, для того чтобы решить проблему повышения доверия пользователя к провайдеру облачных сервисов, пользователю, как минимум, необходимо:

1) заключить с провайдером соглашение об уровне услуг (SLA), где оговорить все нюансы процесса обработки критической информации;
2) получить от независимых экспертов подтверждение того, что используемое для создания облачной инфраструктуры ПО не имеет недекларированных возможностей (НДВ);
3) убедиться, что ПО, используемое провайдером, имеет специальные встроенные функции, позволяющие изолировать информацию (данные) одной виртуальной машины от другой и исключить возможность получения доступа к оперативной памяти работающей виртуальной машины администраторам облачной инфраструктуры;
4) установить на виртуальной машине специальное приложение, обеспечивающее прозрачное шифрование данных на диске пользовательской виртуальной машины;
5) контролировать доступ к ключу шифрования и предоставлять его только после строгой аутентификации аппаратно-программной платформы физического сервера и положительных результатов контроля целостности виртуализатора;
6) установить специальное приложение, обеспечивающее шифрованное VPN-соединение по схеме «точка – точка» со всеми элементами сетевой инфраструктуры, с которыми осуществляется взаимодействие в ходе обработки информации (данных). ■

Vihorev.indd 25 16.08.2012 18:39:22