

ЗАЩИТА ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ: общие международные подходы

Д.Костров, член Правления Межрегиональной общественной организации "Ассоциация руководителей служб информационной безопасности"

Применение облачных вычислений уже прочно вошло в главный инструментарий директоров по ИТ и ИБ. Но угрозы и проблемы "облаков", как и их защита, остаются на повестке дня.

К ИСТОРИИ ВОПРОСА

Облачные технологии – это среда для хранения и обработки информации, объединяющая аппаратные средства, лицензионное программное обеспечение, каналы связи, а также техническую поддержку пользователей. Для конечного пользователя облачные технологии интересны неприязнностью к аппаратной платформе и географической территории, а также масштабируемостью. В настоящее время Национальный институт стандартов и технологий США (NIST) описал облачные вычисления (cloud computing) как модель предоставления пользователю удобного доступа по требованию к массиву настраиваемых компьютерных ресурсов, которые могут быть быстро зарезервированы и высвобождены с минимальными действиями со стороны их провайдера. Хотя вначале чаще использовалось понятие облачных вычислений как информационно-технологической концепции, подразумевающей обеспечение повсеместного и удобного сетевого доступа по требованию к общему пулу конфигурируемых вычислительных ресурсов, которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами или обращениями к провайдеру.

Из истории мы помним, что замена собственных генераторов электричества на услугу

поставки электричества по проводам было первой "облачной" (повсеместной) услугой. Такие же изменения уже достаточно давно происходят в ИТ-мире, и обеспечение ИТ-услугами становится похожим на предоставление коммунальных услуг тепло- или водоснабжения.

Услуги облачных вычислений, как правило, предоставляются в определенных категориях: инфраструктура как услуга (Infrastructure as a service – IaaS), платформа как услуга (Platform as a service – PaaS), программное обеспечение как услуга (Software as a service – SaaS), сеть как услуга (Network as a service – NaaS) и т.д. Эти категории позволяют потребителям услуг облачных вычислений быстро и легко начать или изменить свою деятельность, не создавая новую инфраструктуру и новые системы информационно-коммуникационных технологий, и обеспечивают возможность гибкого предоставления ресурсов в необходимом количестве. Например, одни поставщики облачных услуг (Cloud Service Provider – CSP) могут предоставлять удаленные ресурсы аппаратного и программного обеспечения, которые предлагаются как услуга (IaaS или NaaS); другие – рассчитанные на облачную среду платформы (PaaS) или приложения (SaaS), позволяющие потребителям и партнерам быстро разрабатывать и внедрять новые приложения, которые настраиваются и используются дистанционно.

ЗАЩИТА "ОБЛАКОВ"

Защита "облаков" в принципе уже базируется на применении единых стандартов. В этой области работает Cloud Security Alliance (CSA) – некоммерческая организация, лидер в области разработки стандартов, рекомендаций и инициатив, направленных на повышение безопасности и защищенности использования облачных вычислений. Деятельностью CSA руководит обширная коалиция ведущих мировых экспертов в отрасли, передовых корпораций в ИТ-индустрии, известных профессиональных ассоциаций и крупнейших провайдеров облачных услуг (Google, eBay, Salesforce.com, RackSpace и др.).

Не стоит на месте и Международный союз электросвязи. Директора по ИБ могут применять международную рекомендацию X.1601 "Основы безопасности облачных вычислений", которая использует такое определение: "Облачные вычисления (cloud computing) – парадигма обеспечения сетевого доступа к масштабируемому и гибкому набору совместно используемых физических или виртуальных ресурсов с предоставлением и администрированием ресурсов на основе самообслуживания по запросу". Согласно рекомендации, облачные вычисления обеспечивают возможность удобного сетевого доступа по запросу к совместно используемому набору конфигурируемых ресурсов (например, сетям, серверам, запоминающим устройствам, приложениям и услугам), которые могут быть оперативно предоставлены и высвобождены при минимальном управленческом усилии или минимальном взаимодействии поставщиков услуг. Потребители могут использовать эти ресурсы для разработки, размещения и функционирования услуг и приложений по требованию и гибким образом на любом устройстве, в любое время и в любом месте в среде облачных вычислений.

В то же время внедрение облачных вычислений сопряжено с угрозами и проблемами безопасности, и требования к ее обеспечению существенно различаются для разных моделей развертывания и категорий услуг. Распределенный характер облачных вычислений, сопряженный с наличием нескольких групп внутренних пользователей, преобладание дистанционного доступа к услугам облачных вычислений и большое количество организаций, участвующих в каждом процессе, приводят к тому, что облачные вычисления изначально более уязвимы как к внутренним, так и к внешним угрозам безопасности, нежели другие парадигмы. Многие угрозы безопасности могут

быть уменьшены с применением традиционных процессов и механизмов обеспечения безопасности. Безопасность затрагивает многие составляющие услуг облачных вычислений и воздействует на них. В связи с этим одним из важнейших аспектов облачных вычислений является управление обеспечением безопасности услуг облачных вычислений, а также связанных с ними ресурсов.

УГРОЗЫ И ПРОБЛЕМЫ БЕЗОПАСНОСТИ

Прежде чем переводить систему ИКТ в среду облачных вычислений, потенциальному потребителю облачной услуги (Cloud Service Customer – CSC) следует выявить ее угрозы и проблемы безопасности. На основе оценки риска CSC может определить, стоит ли внедрять облачные вычисления, а также принять обоснованные решения относительно поставщиков услуг и архитектуры. Указанную выше оценку риска следует осуществлять с помощью принципов управления рисками информационной безопасности (например, принципов управления рисками, определенных в ISO/IEC 27005).

Угрозы безопасности облачных вычислений связаны с потенциальным ущербом ресурсам, например информации, процессам и системам, а значит – организациям. Они могут иметь стихийное или антропогенное происхождение и быть случайными или намеренными; могут возникнуть внутри или вне организации; разделяются на случайные или намеренные, а также активные или пассивные. Конкретные обнаруженные угрозы сильно зависят от выбранной конкретной облачной услуги. Угрозы безопасности для CSC – потеря и утечка данных, незащищенный доступ к услуге, внутренние угрозы. Угрозы безопасности для CSP – несанкционированный административный доступ, внутренние угрозы.

Проблемы безопасности включают отличные от непосредственной угрозы безопасности трудности, в том числе "косвенные", которые обусловлены характером и рабочей средой облачных услуг. Косвенная угроза имеет место в том случае, если какая-либо угроза одному пользователю облачной услуги может иметь отрицательные последствия для других пользователей. Проблемы безопасности для CSC связаны со сложностями среды или косвенными угрозами, которые могут быть причиной более непосредственных угроз интересам потребителя облачной услуги: неопределенность в отношении ответственности, потеря доверия, потеря управления, потеря

конфиденциальности, неготовность услуги, привязка к одному поставщику облачной услуги, неправомерное присвоение интеллектуальной собственности, потеря целостности программного обеспечения. Проблемы безопасности для CSP: неопределенность в отношении ответственности, совместно используемая среда, несогласованность и конфликт механизмов защиты, конфликт юрисдикций, связанные с изменениями риски, неудачный переход и интеграция (переход в облако нередко подразумевает перенос больших объемов данных и серьезные изменения конфигурации), перебои в деятельности, привязка к партнеру облачной услуги, уязвимость цепи поставок, взаимозависимость программного обеспечения. Проблемы безопасности для партнеров облачной услуги (CSN): неопределенность в отношении ответственности, неправомерное присвоение интеллектуальной собственности, потеря целостности программного обеспечения.

Для любой системы, в которой несколько поставщиков сотрудничают с целью оказания заслуживающей доверие услуги, необходима общая модель доверия. В связи с чрезвычайно распределенным характером облачных вычислений, сопряженным с наличием нескольких участников, необходимо чтобы среда облачных вычислений включала общую модель доверия. Эта модель доверия позволит создавать острова и/или федерации доверенных объектов таким образом, чтобы разрозненные элементы системы могли аутентифицировать идентичность и санкционированные права других объектов и компонентов. Каждый остров федерации доверия будет основан на одном или нескольких доверенных органах выдачи сертификатов инфраструктуры открытых ключей (PKI). Сегодня существует много моделей доверия, предназначенных для использования в облачной и необлачной среде.

ПРАКТИКАМ НА ЗАМЕТКУ

К услугам облачных вычислений имеют отношение много администраторов и пользователей, при этом доступ к этим услугам и их использование осуществляются внутренним (CSP) и внешним (CSC) образом. Поэтому необходимо управление определением идентичности и доступом (Identity and Access Management – IAM) для аутентификации идентичностей, а также компонентов системы, например загруженных программных модулей, приложений и наборов данных. Процесс IAM имеет важнейшее значение в облачных вычислениях, поскольку способствует

обеспечению конфиденциальности, целостности и готовности услуг и ресурсов. Кроме того, IAM обеспечивает возможность осуществления однократной регистрации и реализации федерации идентичности в облаках с помощью различных механизмов аутентификации или механизмов, распределенных по различным доменам безопасности.

Аудит транзакций обеспечивает защиту от непризнания участия, позволяет осуществлять экспертно-технические анализ после инцидентов безопасности и является средством предотвращения атак (как внешних, так и внутренних вторжений). Аудит транзакций подразумевает не просто ведение журнала, а включает и активный мониторинг с целью привлечения внимания к подозрительным действиям.

Также не забываем об обеспечении физической защиты. Доступ в помещения, содержащие оборудование CSP, разрешается только авторизованным лицам и только в те области, которые непосредственно необходимы для выполнения их функциональных обязанностей; эта задача является частью процесса IAM. Однако степень физической безопасности зависит от ценности данных и масштабов доступа, разрешенного множеству пользователей.

Доступные механизмы обеспечения безопасности интерфейсов, открытых для CSC и/или других привлекаемых на основании договора CSP, с помощью которых доставляются различные виды услуг облачных вычислений, включают одностороннюю / взаимную аутентификацию, контрольную сумму для проверки целостности, сквозное шифрование, цифровую подпись и т.д.

Безопасность виртуализации вычислений относится к безопасности всей среды виртуализации вычислений. Эта возможность обеспечивает защиту гипервизора от атак, защиту хост-платформы от угроз, возникающих в среде виртуализации вычислений, и защиту виртуальных машин на протяжении их срока действия.

В среде облачных вычислений безопасность сети позволяет изолировать физическую и виртуальную сети и обеспечить безопасную связь между всеми участниками. Эта возможность делает доступным разбиение домена безопасности, средства управления доступа на границе сети (например, брандмауэр), обнаружение и предотвращение вторжения, разделение сетевого трафика на основе политики безопасности. Кроме того, она обеспечивает защиту сети от атак в средах физической и виртуальной сетей.

Изолирование данных, защита данных и защита конфиденциальности – с помощью данной возможности решаются общие проблемы защиты данных, которые нередко имеют правовые последствия.

В связи с тем, что в разных услугах облачных вычислений подразумеваются разные способы реализации средств управления безопасностью, с помощью данной возможности обеспечения безопасности координируются действия различных механизмов обеспечения безопасности, чтобы не допустить конфликтов механизмов защиты.

Необходимые меры обеспечения эксплуатационной безопасности предполагают:

- определение набора принципов политики безопасности и деятельности по обеспечению безопасности, например управление конфигурацией, совершенствование корректировки, оценка безопасности, реагирование на инциденты и обеспечение правильного применения этих мер безопасности в целях выполнения требований применимого законодательства и договоров, включая любые SLA, связанные с безопасностью;
- контроль выполнения CSP мер безопасности и их эффективности и предоставление надлежащих отчетов затронутым CSC, а также соответствующим сторонним аудиторам (действующим как CSN), позволяющим CSC оценить, обеспечивает ли CSP выполнение обязательств в области безопасности, предусмотренных SLA.

В случае изменения мер безопасности CSP и их эффективности все нижестоящие CSP и CSC оповещаются о таких изменениях. Эти отчеты и оповещения позволяют авторизованным CSC просматривать информацию о соответствующих инцидентах, информацию аудита, а также

данные конфигурации, относящиеся к их услугам облачных вычислений.

Не следует забывать про управление инцидентами, которое предусматривает их мониторинг и прогнозирование, оповещение об инцидентах и реагирование на них. Для того чтобы знать, работает ли услуга облачных вычислений в штатном режиме в пределах всей инфраструктуры, необходим непрерывный мониторинг (например, мониторинг показателей работы виртуализированной платформы и виртуализированной машины в реальном времени). Это дает возможность системе собирать информацию о состоянии безопасности услуги, выявлять нештатные условия и обеспечивать раннее предупреждение о перегрузках системы безопасности, нарушениях работы, перебоих в обслуживании и т.д. После наступления событий инцидента безопасности обеспечивается выявление проблемы и быстрое реагирование на инцидент, осуществляемое либо автоматически, либо с вмешательством администратора-человека. Обработанные инциденты заносятся в журнал и проводится их анализ с целью создания на их основе шаблонов, с помощью которых в дальнейшем обеспечивается упреждающая обработка.

Оценка и аудит безопасности услуги позволяет авторизованной стороне проводить проверку соответствия облачной услуги применимым требованиям обеспечения безопасности и может осуществляться CSC, CSP или третьей стороной (CSN), а сертификация системы безопасности – выполняться авторизованной третьей стороной (CSN).

Также не надо забывать о необходимости при разработке принципов обеспечения облачных технологий для информационных систем воспользоваться международной рекомендацией X.1631, которая основана на методах контроля ISO/IEC 27002, а также дополнительных способах контроля, разработанных только для облачных технологий. ■