Барьерные рифы облачных вычислений

В конце 2013 года компания RadiusGroup планирует ввести в коммерческую эксплуатацию первый объект сети гиперЦОДов, которые будут находиться в управлении оператора RadiusHost. Уже сейчас компания создает специальное подразделение, призванное заниматься обеспечением информационной безопасности облаков. На вопросы журнала CIO ответил президент RadiusGroup Дмитрий Мариничев.

ТЕКСТ
Натальи Жилкиной

Насколько актуален вопрос безопасности для российских заказчиков облачных сервисов?

— Заказчики испытывают огромный интерес и вместе с тем большое недоверие к перспективам получения сервисов из публичного облака. Клиентов привлекает снижение капитальных расходов. Им не нужно тратиться на создание своего ЦОДа: для функционирования облака, из которого они получают услугу, уже есть подготовленная площадка с гарантированными электропитанием, климатическими системами, каналами связи и так далее. Их привлекает также возможность освободиться от бремени управления инфраструктурой и сконцентрироваться на более важных задачах. Один из важных факторов — возможность быстро получить нужную функциональность в рамках модели «по требованию», что обеспечивает соответствие информационных технологий бизнес—стратегиям. Другая сторона медали — озабоченность теми рисками, которые сопровождают облачные технологии. Прежде всего это тревога о недостаточном уровне безопасности и непрерывности бизнеса, а также опасения потери прямого контроля над системами, которые находятся в сфере ответственности заказчиков.

Есть ли специфика в подходах к обеспечению информационной безопасности, когда компания переходит к предоставлению услуг через облако?

— Принципиальное отличие заключается в том, что организация передает часть контроля над информационной безопасностью облачному провайдеру. Это можно сравнить с ситуацией, когда ИТ передаются на аутсорсинг в другую компанию. В обоих случаях организация должна быть уверена в надежности провайдера и в том, что информационная безопасность данных будет обеспечена на необходимом уровне. Для этого необходимо четко формулировать требования к информационной безопасности и прописывать их в договорах с облачным провайдером. Надо отметить, что последние обычно более надежно защищают данные, чем это делают клиенты для собственных ИТ-систем, поскольку для провайдеров предоставление и защита данных — профильная деятельность. До ввода в эксплуатацию первого ключевого объекта сети гиперЦОДов компании RadiusGroup остается почти год. Однако уже сейчас для реализации всего комплекса обеспечительных мер безопасности облачных сервисов создается подразделение информационной безопасности, которое будет решать весь круг перечисленных выше задач. Первоочередной целью подразделения информационной безопасности станет формирование требований к защите — как на физическом уровне, так и на уровне защиты информационных систем, инженерной инфраструктуры и т. д. Круг приоритетных задач службы информационной безопасности включает обеспечение выполнения различных требований — законодательства, клиентов и собственной безопасности.

Работа по созданию подразделения информационной безопасности в компании ведется на принципах, которые определялись, исходя из лучших практик и стандартов управления. Уже назначен ответственный за информационную безопасность в целом по организации: это человек, хорошо знающий бизнес компании

и разбирающийся во всех бизнес-процессах. По мнению руководства компании, он должен войти в состав совета директоров RadiusGroup. Те вопросы, которые он будет выносить на обсуждение, должны защищать интересы бизнеса.

Что является особенно проблематичным в сфере обеспечения облачной безопасности?

— Широкое использование технологий виртуализации для предоставления облачных услуг породило целый ряд задач, связанных с надежной изоляцией данных и сервисов. Огромные массивы ИТ-ресурсов являются общими для многих пользователей, поэтому необходимо свести к абсолютному минимуму возможность доступа к чужим данным и сервисам на всех уровнях защиты информации. Для моделей предоставления услуг Saas и Paas возникают дополнительные вопросы безопасности. Функционирующее в облаке приложение может взаимодействовать с другими приложениями, базами данных и так далее. Возникает целый ряд вопросов по их интеграции.

Ошибки на стадии сопряжения приложений требуют особого внимания. Нередки ситуации, когда не удается обеспечить прямое взаимодействие между двумя приложениями и необходимо разработать какие-то скрипты, в которых могут быть свои дополнительные уязвимости. Существует также целый ряд уязвимостей, связанных с выходом новых версий ПО. Система может быть создана, настроена и протестирована с соблюдением всех требований безопасности, но при выходе обновления, связанного, например, с расширением функционала, необходимо вновь произвести тестирование. Такая проверка обычно проводится лишь с точки зрения функционала, и если сроки поджимают, то безопасностью нередко пренебрегают. А между тем после внесения изменений совершенно необходимы тщательные проверки (то есть сканирование, тесты на проникновение и т. д.). Внесение изменений может быть сопряжено с отказом каких-то функций или их неправильной работой. Но если бизнес требует срочного восстановления работоспособности, то нередко запускают процедуру отмены изменений либо вообще могут отключить всю систему безопасности. И даже если изменения вернули назад, на случай, если во время внесения изменения или после этого что-то пойдет не так, должны готовиться планы отката на предыдущие конфигурации. После внесения любых изменений тестирование безопасности нужно проводить в обязательном порядке. Ведение журналов изменений и строгой дисциплины исполнения регламента должно быть постоянно на контроле, а изменения — выполняться незаметно для клиентов.

Какими рисками необходимо управлять в облаке?

— Перечень рисков, связанных с безопасностью и непрерывностью облачных услуг, охватывает широкий круг вопросов — от финансовой стабильности провайдера облачных услуг и его репутации до проработки плана Disaster Recovery, обеспечения безопасности бизнес-приложений и целостности данных. При оценке рисков, связанных с облаком, вопросы обеспечения надежности функционирования его элементов надо рассматривать в комплексе на всех уровнях. Причем не только в отношении физической безопасности, отказоустойчивости инженерной и сетевой инфраструктуры. Управление рисками включает в себя также решение всех вопросов, касающихся работоспособности приложений и всех программных систем, от функционирования которых зависит непрерывность бизнеса. Немаловажным фактором риска является соблюдение соответствия федеральным и отраслевым законодательным нормам. При этом надо разделять

> **Надежное облако развертывается на основе нескольких ЦОДов, территориально разнесенных на большие расстояния**

небезопасной может оказаться текущая конфигурация. А если все работы проводили в пятницу вечером и часть оставили на понедельник, то трудно гарантировать, что ничего не забыли. Те же вопросы возникают и при установке обновлений информационной безопасности. При всей важности установки патчей, закрывающих уязвимости, это зачастую не делается из-за необходимости провести большую подготовительную работу, чтобы убедиться, что установка патча не повлияет на функционирование системы.

Вывод: для провайдера особенно важно соблюдение жестких регламентов, которые должны неукоснительно выполняться. Изменения нужно тщательно планировать и тестировать, их необходимо проводить во время наименьшей загрузки критически важных систем.

риски безопасности, связанные с самим облаком и с доступностью каналов связи к этому облаку. В каких-то случаях это могут быть риски уже на стороне клиента. Необходимо учитывать также кадровую безопасность, то есть оценивать риски с учетом поведения сотрудников компании, предоставляющей облачные услуги на базе коммерческого ЦОДа.

Влияние человеческого фактора, — это, пожалуй, один из наибо-

лее сильных рисков безопасности для тех, кто решил связать свой бизнес с услугами из облака. Речь идет о случайных человеческих ошибках, о нарушении внутренних требований — либо даже о действиях в корыстных интересах.

Каковы возможные подходы к обеспечению соответствия регламентам в облаках? Кто за это должен отвечать?

— Ответственность за соблюдение требований законодательства и регуляторов в любом случае остается за организацией, которая подпадает под такие требования. В случае если организация пользуется услугами коммерческого дата-центра, она должна быть уверена в том, что безопасность будет обеспечена на должном уровне. При этом организация может переложить значительную часть вопросов обеспечения безопасности на такой центр, обязательно оставив за собой функции контроля над выполнением требований безопасности, предъявляемых к ЦОДу. По этой причине для владельца коммерческого дата-центра весьма актуальны вопросы, касающиеся соблюдения требований законодательства. Они могут касаться даже физического местоположения ЦОД или, например, устранения рисков несоответствия федеральному закону «О защите персональных данных».

Кроме этого, существуют еще требования регуляторов: например, стандарт Банка России СТО БР ИББС носит рекомендательный характер, тем не менее банки серьезно ориентируются на него. Провайдеру придется обеспечить соответствие и такому стандарту, как PCI DSS по защите данных платежных карт. Определенная категория клиентов может потребовать сертификации по стандарту ISO 27001. Возможно, в недалеком будущем будет разработан стандарт, аналогичный стандарту Банка России, в области здравоохранения, потому что эти данные являются весьма уязвимыми и требуют повышенного уровня защиты.

Чтобы подтвердить соответствие не только федеральным, но и отраслевым стандартам, провайдеру облачных сервисов придется пройти процедуру сертификации. Даже если стандарт не является обязательным, наличие сертификата соответствия станет серьезным конкурентным преимуществом для привлечения различных категорий клиентов. В том случае, когда организация, которая хочет воспользоваться услугами коммерческого ЦОДа, имеет глубокие компетенции и основанные на проведенном анализе рисков собственные высокие требования — более высокие, чем требования законодательства и стандартов, — заказчики могут прописать их в договоре с провайдером. В частности, таковым может стать требование проведения аудита.

Как клиенты, которые работают в облачной среде, могут минимизировать риски, связанные с размещением данных?

— Опытные клиенты обычно руководствуются простым правилом: надежное облако развертывается на основе нескольких ЦОДов, территориально разнесенных на большие расстояния. Приложение, с которым работает клиент, обращается к данным, часть которых может находиться в одном ЦОДе, а часть — в другом, расположенном за несколько десятков, сотен, а то и тысяч километров. Даже если в одном из центров происходит какой-то инцидент, пользователь этого просто не заметит, поскольку данные синхронизируются с другим дата-центром незаметно для приложения.

Одна из уникальных услуг безопасности, которая может быть предоставлена из облака гиперЦОДов RadiusGroup, — постоянная доступность данных. Если облако территориально распределено по стране, данные могут находиться сразу в нескольких ЦОДах с избыточностью. Даже в случае стихийного бедствия или какого-то иного инцидента данные останутся доступны для клиента. С точки зрения непрерывности сервиса открываются просто безграничные возможности. CIO

Безопасность облачных услуг

Александр Крупчик
директор центра информационной безопасности компании RadiusGroup

Для провайдера, который построил облачную платформу, существует определенная специфика защиты ИТ-ресурсов. Потому что в облачной среде присутствуют некие дополнительные уязвимости, присущие технологии Cloud. И первый вопрос, который возникает в таких случаях, — это изоляция данных. В облаке, предоставляющем услуги на коммерческой основе, хранятся данные многих компаний. Главная задача такого провайдера — обеспечить надежное разграничение между данными различных компаний, которые могут находиться на одном и том же физическом сервере или даже на одном диске. При этом эти данные могут обрабатываться разными виртуальными серверами, различными виртуальными системами, и требования по безопасности их хранения и обработки тоже могут разниться.

Например, кто-то из клиентов обрабатывает информацию, содержащую персональные данные или являющуюся банковской тайной. Часть машин может подпадать под требования стандарта PCI DSS, а часть — не подпадать. Чтобы исключить систему, которую не затрагивает действие стандарта PCI DSS, нужно обеспечить надежное изолирование данных и систем, которые их обрабатывают.

Легкость и удобство, с которыми клиенты могут получать услуги из облака, подразумевают также значительную сложность и большой объем программирования при создании платформы, на базе которой эти услуги предоставляются. Поэтому одна из специфических опасностей, подстерегающих в облачной среде, — ошибки программирования и интеграции. Некоторые уязвимости могут быть заложены на этапе составления ТЗ, некоторые — во время написания кода. В частности, на этапе составления ТЗ могут быть не учтены требования ИБ, а программист, которому поручено писать код, может не владеть в достаточной мере технологией безопасного программирования. Для выявления таких уязвимостей необходимо проводить тщательное тестирование. Конечно, выполнение тестирование не дает стопроцентной гарантии того, что ошибки исключены: это лишь позволяет при конкретных сценариях получить определенные результаты. Соответственно, сама эффективность тестирования в значительной степени зависит от того, какие сценарии были разработаны для него. Как правило, в первую очередь тестирование направлено на выявление ошибок, связанных с функционированием и интерфейсом, а вопросы безопасности могут тестироваться последними.

Вопросы безопасности при реализации проекта, в том числе при построении облака, нередко могут отходить на второй план — например, когда поджимают сроки или бюджет. Следовательно, при составлении документации могут быть описаны не все механизмы по настройке безопасности, и тогда не исключено, что какие-то настройки сделаны по умолчанию для удобства использования, но вместе с тем они заведомо небезопасны. Нередки случаи, когда разработчики отключают какие-то функции либо могут включить те, в которых нет особой надобности, но которые могут быть уязвимы. Такие вещи возможны не только на этапе разработки, но и на этапе внедрения программного продукта. ■