Безопасность облаков.
Общие вопросы

Алексей АФАНАСЬЕВ,
эксперт провайдера #CloudMTS по информационной безопасности

Облачные сервисы дешевле, удобнее и быстрее традиционных решений. Сегодня все больше компаний и госучреждений в том или ином виде используют облака, размещая свои приложения и данные в облачных средах. Отдельный интерес вызывают вопросы защиты данных и безопасной работы в облаке. Что чаще всего атакуют злоумышленники, как организовать надежную защиту в облачной инфраструктуре и учесть все регуляторные требования при работе с чувствительными данными, рассказал эксперт по информационной безопасности облачного провайдера #CloudMTS Алексей Афанасьев.

Зачем атаковать облака?

Облако дает возможность быстро применить новейшие технологии, связанные, например, с организацией виртуальных рабочих мест, сервисами контейнеризации или современными платформами веб-сайтов. Облака можно быстро протестировать и максимально гибко использовать, но часто возникают сомнения в защищенности полученного решения. В традиционных ИТ-моделях компании, как правило, лучше ориентируются: хорошо представляют ИТ-ландшафт, могут оценить риски той или иной угрозы и построить систему защиты. Но это не означает, что облака хуже защищены и менее безопасны, чем собственная инфраструктура.

В последнее время по публикациям в СМИ мы видим множество примеров утечек персональных данных, причем в разных проектах – и частных, и государственных. Далеко не всегда эти истории связаны с облаками и новыми технологиями. Как правило, во главу угла встает человеческий фактор.

В стремлении сократить time-to-market новые ИТ-проекты часто запускаются без должной оценки их защищенности и безопасности. Например, в B2C-компаниях остро стоит вопрос сокращения времени на разработку и выпуск новых клиентских приложений. При этом часто вопросы безопасности конфликтуют с вопросами функциональности, удобства использования и временем, необходимым на разработку. И тут без разницы – традиционная это инфраструктура или облачная.

Фактически приложение – это ворота, интерфейс к тем данным, которые находятся в хранилище, базе данных компании. Злоумышленники, получившие доступ к данным, могут по своему усмотрению оперировать ими – перепродавать, шантажировать компанию или владельцев данных, нередко использовать в более сложных схемах. Например, украв платежные данные, преступники могут совершать платежи от имени клиентов.

Что защищать в облаке?

Облако представляет собой набор сервисов. У облака есть серверная инфраструктура с процессорами, оперативной памятью, жесткими дисками. Есть сетевая инфраструктура, которая представлена виртуальными сетевыми устройствами и программно-определяемой сетью, устройствами безопасности и т. д. Кроме того, в инфраструктуре облака можно выделить систему идентификации пользователей, службы каталога, механизмы управления виртуальными машинами или контейнерами. Все эти элементы – фундамент облачной инфраструктуры, важный для провайдера уровень. За него отвечает компания – владелец облака и несут ответственность службы безопасности провайдера.

Именно на этот фундамент компания-клиент переносит свою информационную систему, свои приложения. Зачастую компания собирает необходимое из набора имеющихся у провайдера инфраструктурных «кубиков» и внутри них запускает свои приложения. Например, провайдер может предоставить набор виртуальных машин, внутри которых будут запущены ядро базы данных, веб-сервер и другие компоненты информационной системы клиента.

Настройки клиентских приложений – это крайне важная задача, но ее решение не на стороне провайдера, это зона ответственности компании – клиента облака. Ею должна заниматься сама компания. Ведь именно внутри построенной компанией информационной системы накапливаются бизнес-данные, за которыми охотятся злоумышленники. Киберпреступники могут проникнуть туда разными путями: через слой инфраструктуры провайдера или через слой приложений, которые настраиваются самой компанией.

Таким образом, ИБ-защита необходима на всех уровнях. Ответственность разделяется между провайдером и его клиентом, который создает свое приложение и управляет им. Важно, чтобы все звенья цепи были одинаково надежны, тогда у злоумышленников не будет шансов. Например, если компания установила ненадежный веб-движок, то это ее риски и ее зона ответственности. И если через такой веб-движок утекли данные, то провайдер, как бы ни старался, не сможет защитить этого клиента.

Провайдер охраняет и контролирует свою инфраструктуру, не имея доступа к данным и настройкам приложений клиентов. Например, часто атака с помощью ворованных учетных записей невидима для провайдера инфраструктуры. Внешне с уровня управления инфраструктурой провайдера все выглядит вполне легитимно.

Конечно, компания может усомниться в безопасности инфраструктуры провайдера и подвергнуть самостоятельному анализу ее защищенность – это вполне нормальный подход. Для этого компания может даже заказать внешний аудит. Надежные провайдеры не будут этому препятствовать, им скрывать нечего. При этом компания-клиент может выбрать любую внешнюю организацию-консультанта. Такие специализированные организации предлагают услуги по полноценному аудиту защищенности, например тестированию на проникновения. Такой анализ защищенности затронет различные уровни: тестироваться будет как инфраструктура облака, так и защищенность приложений клиента.

Как защитить облака?

Обычно у крупных облачных провайдеров подготовлен целый набор ИБ-решений. Допустим, у компании есть персональные данные и веб-сайт, который работает с этими данными. Также у него есть мобильное приложение, которое получает доступ к его ИСПДн. При этом компании надо связать базу данных в облаке с информационной системой в офисе, кроме того, организовать резервное копирование данных и обеспечить их постоянную доступность.

В таком случае провайдер может предложить клиенту аттестованную инфраструктуру, которая специально предназначена для работы с персональными данными. Кроме того, если речь про веб-сервисы, то хорошо бы использовать защиту в виде межсетевого экрана (WAF) на уровне приложений, а также защиту от DDoS-атак. Все эти решения провайдеры могут предоставить в виде сервиса по подписке. Таким образом клиент получит комплексную защиту как сервис для своего приложения внутри облака.

> Настройки клиентских приложений – это крайне важная задача, но ее решение не на стороне провайдера, это зона ответственности компании – клиента облака.

Крупные провайдеры часто предлагают систему распределенного облака, в котором ЦОД расположены в нескольких локациях. Такие решения обладают катастрофоустойчивостью и повышенной надежностью, что особенно важно для крупных бизнес-клиентов. В качестве основного клиент может выбрать один дата-центр, где будут развернуты его веб-сайт, база данных и другие компоненты приложения. В другом дата-центре

будут находиться резервные копии, при этом будут соблюдаться все нормативные требования. В случае ЧП в основной локации все сервисы можно будет быстро запустить на другой площадке из резервной копии и продолжить работу. При этом провайдер будет обеспечивать непрерывную защиту от DDoS-атак, будет защищать веб-приложения с помощью WAF независимо от расположения веб-сайта клиента.

В дополнение к этому сегодня облачные провайдеры могут предоставить сервис круглосуточного мониторинга рисков безопасности – услуги коммерческого SOC. Это комплексный механизм защиты и предупреждения угроз. К примеру, операторы SOC оперативно связываются с заказчиком, когда атака на информационные ресурсы еще не началась, но обнаружены первые признаки нападения злоумышленников: вход с нетипового устройства, подозрительное подключение к инфраструктуре, подбор пароля, попытки сканирования или поиска уязвимостей в веб-приложениях.

Таким образом, приложение или ИТ-система компании комплексно защищены внутри облака провайдера. Компании-клиенту нет необходимости держать свой штат специалистов ИБ и организовывать круглосуточный мониторинг. Услуги SOC клиент покупает как один из сервисов ИБ. У провайдера #CloudMTS есть подобный SOC, который ежедневно защищает и информирует российские компании об угрозах. Это позволяет на ранних этапах предотвратить атаку, многоуровневая эшелонированная защита минимизирует риски для наших клиентов.

Как работать с персональными данными и ГИС?

У большинства российских провайдеров есть выделенные и соответствующие требованиям регуляторов сегменты для работы с персональными, финансовыми и банковскими данными, также ГИС. Например, облако, в котором обрабатываются платежные данные банковских карт, обычно сертифицируется по требованиям международного стандарта PCI DSS (Payment Card Industry Data Security Standard, стандарт безопасности данных индустрии платежных карт).

Если компания планирует размещать ГИС или обрабатывать персональные данные, то провайдер может и должен продемонстрировать уровень и класс защищенности своего облака, показав аттестат. Например, у нас есть аттестованные сегменты, которые подпадают под требования регуляции ИСПДн и ГИС.

В нашем облаке можно хранить и обрабатывать любые виды персональных данных, также размещать государственные информационные системы всех уровней и масштабов. За исключением тех, которые содержат гостайну. Это могут быть паспортные и медицинские данные человека, а также специальные категории персональных данных, которые установлены постановлением Правительства и требуют первого (УЗ-1), наивысшего уровня защиты. Конечно, сегодня есть различные подходы работе с ПДн, и компания-заказчик может на свой страх и риск использовать неаттестованные решения и иностранные облака.

Часто информационная система клиента неоднородна и содержит смешанные данные. Если в системах клиента обрабатываются и персональные данные, и обезличенные, то оптимальным вариантом будет использовать разные сегменты облака. Обезличенные данные можно обрабатывать в неаттестованных облачных сегментах, которые, как правило, дешевле и, возможно, имеют большую

Сегодня облачные провайдеры могут предоставить сервис круглосуточного мониторинга рисков безопасности – услуги коммерческого SOC. Это комплексный механизм защиты и предупреждения угроз.

функциональность. Делать это можно у одного и того же провайдера. В таком случае клиент получает большую гибкость.

Конечно, работа с чувствительными данными накладывает некоторые ограничения. Например, удаленному пользователю при работе с ГИС придется использовать сертифицированные средства защиты для организации VPN-соединения. В других случаях для удаленного доступа нужно будет лишь организовать доступ с помощью протокола HTTPS без использования сертифицированных средств защиты. Это законодательные ограничения, которые обычному пользователю могут показаться некомфортными для работы. К сожалению, вопрос безопасности иногда конфликтует с удобством и функциональностью решений.

Как не ошибиться?

Не всегда компании могут адекватно построить защиту собственных ресурсов. Например, часто встречается ситуация, когда компания размещает базу данных, используя Linux-сервер.

При этом компания может считать серверы на Linux достаточно защищенными и не требующими дополнительных средств защиты. В таком случае часто не обеспечивается необходимый уровень защиты. Конечно, злоумышленники «не догадываются» о такой защищенности базы данных, могут успешно выполнить атаку и, например, зашифровать данные, а далее потребовать выкуп. Компания, как правило, в таком случае обращается к провайдеру с претензией о потерянных данных.

Максимум, что сможет сделать провайдер, – это предоставить записи по доступу к данному серверу, но минимизировать последствия допущенных просчетов в настройках безопасности самого сервера и базы данных не сможет. В таком случае провайдер может только косвенно предположить, как была выполнена атака. Выходом из ситуации могут быть сохранившиеся резервные копии.

Этот пример показывает, что провайдер и клиент должны заранее разграничить зоны ответственности и внимательно подходить к выбору решений защиты для размещаемых данных. Другой частый сценарий – компания помещает в код приложения ключи доступа. Злоумышленник, анализируя приложение, находит эти ключи и может ими воспользоваться. Это позволит ему иметь административный доступ к ресурсам, расположенным в облаке. Такие ситуации могут привести к злоупотреблению ресурсами или потере всех данных компании. Ответственность при такой компрометации ключей доступа лежит полностью на клиенте.

> Интенсивность использования облачных сред, на наш взгляд, будет расти, в том числе с использованием нескольких географических локаций и мультиоблачных конфигураций.

Что нам готовит грядущее?

Интенсивность использования облачных сред, на наш взгляд, будет расти, в том числе с использованием нескольких географических локаций и мультиоблачных конфигураций.

Использование мультиоблаков позволит бизнесу получать еще больший выбор сервисов и функциональных решений, большую гибкость для бизнеса, разные уровни защиты данных, максимально выгодные цены на ресурсы и лучшие сервисы информационной безопасности. В дальнейшем эта тенденция будет усиливаться.

В свою очередь, облачные игроки продолжат строить распределенные системы, что позволит им удовлетворять самые разные требования клиентов с точки зрения географии и набора сервисов, в том числе по кибербезопасности. ■