АНАЛИЗ РЫНКА ОБЛАЧНЫХ УСЛУГ. МЕТОДЫ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СЕРВИСОВ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Госса А.И.

Лагутин А.Е. – к.т.н.,доцент

Исследования рынка облачных вычислений представлены агенством TAdviser[1].

По форме предоставления услуг на рынке выделяется два сегмента:

- проектные услуги (выбор, внедрение, интеграция, обучение);
- услуги операционного управления (плата за пользование сервисом, включая управление биллингом, учитывающим неравномерность потребления).

Анализ рынка публичных облачных услуг также включает функциональные сегменты:

- приложение как услуга (Software as a Service, SaaS);
- платформа как услуга (Platform as a Service, PaaS);
- инфраструктура как услуга: системное ПО, серверы и СХД (Infrastructure as a Service, IaaS).

По данным исследования, крупный бизнес максимально готов к использованию облачных услуг: в этом сегменте свыше 90% опрошенных знают про облачные услуги, в малом бизнесе – свыше 70%. При этом в крупном бизнесе 54,5% опрошенных пользуется одновременно облачными услугами из 2-х и более категорий, в среднем бизнесе – 50%, в малом – 43%.

Большинство респондентов ассоциируют облачные услуги с виртуальной инфраструктурой (IaaS), хотя сейчас наибольшую долю на рынке занимает модель SaaS — 58,9%. На IaaS и PaaS пока приходится соответственно 37,2% и 3,9% в объеме рынка. По данным исследования доля SaaS к 2020 году увеличится до 62,4%, а IaaS - снизится до 32,3%[1].

Риски использования облачных сервисов

Наиболее полный список угроз облачным сервисам в составе референсной архитектуры информационной безопасности частного облака от Microsoft насчитывает 50 разнообразных угроз на девяти уровнях, полный анализ которых в рамках одной статьи невозможен. Можно выделить ключевые угрозы, представляющие наибольший риск для потребителей облачных сервисов[2]:

- блокировка данных (lock-in) внутри инфраструктуры провайдера из-за отсутствия возможности экспорта данных, хранения в нестандартизированных форматах или потери криптографических ключей для расшифрования данных;
- компрометация административного доступа клиента вследствие успешного перебора паролей или компрометации рабочего места сотрудника клиента;
- потеря контроля над данными вследствие делегирования его провайдеру облачных сервисов, архитектура и организация информационной безопасности которого могут иметь существенные недостатки на уровнях инженерной и ИТ-инфраструктуры, гипервизора и др.;
- неэффективная работа механизмов разграничения доступа между клиентскими данными, обусловленная ошибками в реализации гипервизоров (уязвимостей ПО);
- нарушение нормативных требований по защите данных или обеспечения достоверности финансовой отчетности, что обусловлено передачей данных между юрисдикциями или невыполнением требований по защите чувствительных с точки зрения конфиденциальности/целостности данных;
- утечка клиентских данных, что обусловлено плохой организацией процедуры безопасного удаления данных с мест хранения;
- недоступность облачного сервиса вследствие изменения рыночной стратегии провайдера, покупки провайдера, плохой организации производственного процесса провайдера либо DDoS-атаки;
- непредвиденные затраты недопустимого уровня на оплату облачного ресурса в результате DDoS-атаки против клиента (economical DDoS).

На данную тему произведены исследования, в соответствии с которыми многообразие угроз облачным сервисам не позволяет обеспечить эффективную защиту в разумные сроки и бюджеты. Тем не менее каждая компания может реализовать подходящую ей стратегию информационной безопасности(ИБ) облаков.

Выбор стратегии информационной безопасности облачных сервисов

Специфика обеспечения ИБ облачных сервисов заключается в том, что итоговый уровень информационной безопасности является суммой уровней ИБ провайдера и клиента, из чего следуют два практических тезиса[2]:

- клиент никак не сможет закрыть проблемы в стратегии ИБ провайдера, поэтому выбор провайдера облачных услуг и работа над договором о предоставлении облачных услуг являются наиболее важным элементом;

- не имеющий специалистов и не обладающий ресурсами для обеспечения ИБ клиент может переложить операционные задачи по обеспечению ИБ на провайдера (при этом SaaS дает максимум контроля провайдеру, IaaS, наоборот, клиенту).

Исходя из этого, можно использовать одну из четырех стратегий обеспечения облачной безопасности для бизнеса разных размеров с разными требованиями к конфиденциальности.

Стратегия "Минимум ошибок"

Стратегия предполагает максимальное использование лидирующих SaaS-сервисов не обладающими необходимой экспертизой предприятиями малого бизнеса, поскольку они вряд ли достигнут сравнимого уровня ИБ самостоятельно.

Стратегия "Минимальные усилия"

Стратегия предусматривает максимальное использование лидирующих SaaS-сервисов и дополнительно тщательное изучение и использование доступных встроенных сервисов безопасности, например: двухфакторной аутентификации, защиты паролем загружаемых в Google Drive документов, аккаунта Google на других сайтах ("кустарная" реализация принципа SSO), хранение резервных учетных записей Google и удаление учетных записей сотрудников при их увольнении.

Стратегия "Точечное внимание"

Стратегия заключается в снижении общепризнанных рисков и активном противодействии базовым угрозам. Ключевой посыл - противодействие управляемому количеству угроз, концентрация ресурсов и экспертиз на самых важных направлениях. Как минимум девять указанных угроз ИБ облаков должны быть смягчены, по возможности интегрированы с платформой сервис-провайдера для снижения капитальных и операционных затрат. В случае отсутствия интегрированных мер необходимо внедрение выделенных решений/мер по ИБ облаков. При выборе мер можно использовать как лучшие практики от ENISA, так и описанные ниже продукты ИБ (в том числе интегрированные с платформами сервис-провайдеров).

Стратегия "Многослойная оборона"

Стратегия предполагает разработку целостной комплексной концепции обеспечения облачной безопасности на основе глубокого анализа рисков, тщательного выбора сервис-провайдера, с учетом вопросов обеспечения ИБ и соответствия требованиям законодательства, а также последующего проектирования и внедрения организационных и технических мероприятий по защите информации. Исходя из значимости и количества чувствительной информации, система защиты по возможности должна быть независима от провайдера облачных сервисов. Все средства защиты информации должны быть переданы в промышленную эксплуатацию и эксплуатироваться командой экспертов. В случае отсутствия внутренних ресурсов - сертифицированных специалистов по облачной безопасности, аудиту и контролю ИТ желательно привлекать внешних экспертов на постоянной основе - как через открытие новых позиций, так и путем аутсорсинга или аутстаффинга.

Список используемых источников:

1.Облачные сервисы [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/index.php/ http://www.tadviser.ru/index.php/Статья:Облачные_сервисы_%28рынок_России%29

2.Защита облачных сервисов: стратегия информационной безопасности и продукты. [Электронный ресурс]. – Режим доступа: http://астерос.рф/press/press/2477/