УДК 531

Кошелев С.О., ст. преподаватель кафедры «Информационная безопасность»
Дальневосточный Федеральный Университет
Россия, г. Владивосток
Коваленко И.В., Споданейко А.С., Груц Е.А.
студенты
4 курс, специальность «Компьютерная безопасность»
Дальневосточный Федеральный Университет
Россия, г. Владивосток

БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

Аннотация: *Продвижение облачных сервисов на рынке связано с их реальными преимуществами, и с успехами рекламы, зачастую представляющей услуги удаленных серверов как принципиально новую технологию. В данной статье рассматривается проблема информационной безопасности в облачных технологиях и сервисах. Приведены механизмы обеспечения защиты данных при пользовании «облачными» хранилищами. Анализируются уязвимости и предлагаются варианты улучшения обеспечения ИБ в облачных технологиях.*

Abstract:*the Promotion of cloud services in the market is associated with their real advantages, and with the success of advertising, often representing the services of remote servers as a fundamentally new technology. This article deals with the problem of information security in cloud technologies and services. The mechanisms of data protection in the use of "cloud" storage. The vulnerabilities are analyzed and options for improving the security of is in cloud technologies are offered.*

Ключевые слова: *облачные вычисления, безопасность облачных технологий, защита данных.*

Keywords: *cloud computing, security of cloud technologies, data protection.*

Распространение облачных технологий носит массовый, «взрывной» характер. Продвижение облачных сервисов на рынке связано и с их реальными преимуществами, и с успехами рекламы, зачастую представляющей услуги удаленных серверов как принципиально новую технологию.

На самом деле «облачные» технологии появились вместе с интернетом и даже немного раньше, во времена больших ЭВМ, к интеллекту которых обращались десятки пользователей со своих рабочих мест. Программы, базы данных находились в памяти большой машины, а пользователи имели дисплей, клавиатуру и средства подключения к общей сети.

Облачные сервисы делятся на три части, в зависимости от включенности пользователей в управление «облаком»: публичные, частные и гибридные.

Публичное «облако» используют множество компаний и сервисов. Пользователи не могут управлять данным облаком, вся ответственность лежит на организации, которая является владельцем. Публичное облако могут использовать как частные пользователи, как и целые компании. Примерами данного типа облака являются Amazon EC2, GoogleApps/Docs, Salesforce.com, MicrosoftOfficeWeb, сервис BPMOnline компании Terrasoft [3]. Этот тип в основном подходит малым и средним предприятиям, особенно тем, для которых конфиденциальность данных не является первостепенной причиной выбора «облака».

Частное «облако» контролируется и используется одной компанией. Инфраструктура может размещаться либо в здании самой компании, либо у оператора, либо частично в обоих местах.

Гибридное «облако» использует лучшие стороны предыдущих двух типов. Основное отличие от других в том, что доступ к ресурсам происходит через публичное «облако», а часть операций на частном облаке перебрасывается на публичное, если частное не справляется с потоком [5].

Частные облака лучше использовать крупным предприятия или большим производственным объединениям. В этом случае информация не будет передаваться в «третьи руки», т.е. практически уничтожается главный недостаток «облачных» хранилищ.

Тема безопасности данных в интернете на данный момент является одной из самых актуальных. Обеспечение безопасности данных можно разделить на три направления: правовую защиту, физическую, аппаратно-программную [1].

При использовании «облачных» технологий возникает риск, связанный с выполнением требований законодательства в сфере информационной безопасности, например, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», согласно которому предприятия обязаны принимать достаточные и необходимые меры по защите персональных данных. 17 декабря 2014 года Госдумой были приняты поправки к этому закону. В соответствии с поправками, компании обязаны хранить обработанные в интернете персональные данные россиян на серверах, расположенных на территории России, уже с 1 сентября 2015 года [7].

Но, к сожалению, в настоящее время в РФ нет нормативной базы, которая регулирует вопросы обеспечения защиты информации, обрабатываемой с применением облачных технологий.

Если предприятие или компания использует «облака», располагаемые на территории других стран, то в ход идут законы той страны, связанные с обработкой и хранением конфиденциальной информации.

Правительство США разработало программу FederalRiskandAuthorizationManagementProgram (FedRAMP), которая стремится к тому, чтобы облачные решения соответствовали требованиям отдельных агентств [9].

Пользователи «облаков» в Канаде, США и Европейском Союзе должны следовать многим нормативным требованиям, к примеру «Задачи

информационных технологий» (COBIT), положение о «безопасной гавани» (SafeHarbor). Они регулируют хранение, передачу и конфиденциальность данных [8].

Любое «облако» включает в себя несколько уровней защиты, которые защищают информацию от злоумышленников.

Физический аспект безопасности связан с расположением сервера, его сокрытии. Вынести сервер из здания тяжело в любом смысле этого слова, пробраться к ним порой очень сложно, т.к. практически все компании хранят информацию в местах с охраной, видеонаблюдением и открывают доступ к информации только ограниченному кругу лиц. Так что вероятность того, что информацию получат посторонние, проникнув в здание, близится к нулю.

Кроме того, уважающие себя компании не хранят информацию на одном сервере, подобно тому, как люди хранят деньги в разных банках и на разных счетах. То есть если злоумышленники проберутся к одному серверу, то взлом становится менее болезненным. Часто при взломе сервера просто копируют базу адресов, что ограничивается только спамом на электронную почту [2].

С физической точки зрения «облачные» хранилища вполне надежны, т.к. пробраться к самим серверам очень трудно. Основные риски содержатся на программно-аппаратном уровне обеспечения защиты информации.

Существует 3 архитектуры «облачных» технологий: IaaS, PaaS и SaaS.

К категории IaaS («инфраструктура как услуга») относятся такие решения, как виртуальные серверы, хранилища данных и базы данных, на одной платформе дляразработки и выполнения приложений, системы для совместной работы с файлами в Интернете, системы резервного копирования или архивирования и поисковые средства [6].

В отличие от IaaS, при использовании PaaS («платформа как услуга») разработчик может применять какие-то специфические технологии, предоставляемые той или иной платформой виртуализации для создания более эффективных программных продуктов.

Определяющим фактором уникальности PaaS является то, что она позволяет разработчикам создавать и развертывать Web-приложения на предлагаемой инфраструктуре. Инфраструктура для PaaS является эластичной, поэтому PaaS позволяет воспользоваться практически безграничными вычислительными ресурсами за счет расширения облака [4, 6].

В PaaS уровень, который продвигает сервис, ориентирован на IT-производительность, или производительность неких логических ресурсов, таких как базы данных, файловые системы и приложения операционной среды. В настоящее время развиваются следующие PaaS-технологии: RationalDeveloperCloud от IBM, Azure от Microsoft и AppEngine от Google.

На уровне SaaS («программное обеспечение как услуга») поставщики «облачных» услуг предоставляют доступ по сети к коммерческому программному обеспечению. В этом случае нет необходимости покупать лицензию на каждый компьютер, поскольку программное обеспечение используется по требованию [4, 6]. На этом уровне вовлечены следующие технологии: Web 2.0, гибриды веб-приложений (Mashup) и SOA (сервис-ориентированная архитектура).

Программное обеспечение как услуга (SaaS) включает, в частности, технологии для работы с потоковым мультимедиа (Netflix), социальные сети (ВКонтакте, Facebook и Twitter), службы обмена фотографиями (Instagram) и среды для совместного использования файлов (Dropbox, GoogleDrive, Яндекс. Диск), электронные почтовые ящики, онлайн-средства прослушивания музыки и службы резервного копирования. Другой, менее очевидной реализацией SaaS является значительная часть растущего рынка мобильных приложений [6].

Одной из самых серьезных проблем «облачных» технологий является то, что не все сервисы могут гарантировать безопасность передачи данных. Самой уязвимой частью являются каналы передачи данных, потому что соединение бывает недостаточно защищенным. В связи с этим злоумышленники могут

получить доступ к передаваемой и хранящейся информации. Известные инциденты: 19 июня 2011 года, в течение 4 часов, любой желающий мог получить доступ к данным пользователей Dropbox; в 2014 году в Интернет попали интимные фотографии многих знаменитостей, которые были загружены в облачное хранилище iCloud.

Большинство пользователей используют для подключения к «облаку» веббраузер. При этом возможны такие атаки, как CrossSiteScripting (XSS), перехват паролей и веб-сессий, «человек посредине» и другие. Единственной защитой от таких атак является правильная аутентификация и использование шифрованного соединения с помощью протокола SSL/TLS с взаимной аутентификацией. Однако, данные средства защиты не очень удобны и затратны для владельцев облаков.

Часто проблема безопасности данных заключается также в использовании устаревших версий протокола и слабых при текущем уровне вычислительных мощностей криптоалгоритмов или же в наличии уязвимостей используемого ПО. Известные уязвимости SSL/TLS (Beast, Poodle, Heartbleed, Freak, Logjam) позволяют расшифровывать сессии, перехватывать и подменять данные, передаваемые между пользователем и облаком. Все это ставит под угрозу безопасность передаваемой информации.

Для защиты от функциональных атак на каждую часть «облака» необходимо использовать следующие средства защиты: для прокси - эффективную защиту от DoS-атак, для веб-сервера — контроль целостности страниц и защиту от XSS, для сервера приложений — экран уровня приложений, для СУБД — защиту от SQL-инъекций, для системы хранения данных - правильную настройку резервного копирования, а также разграничение доступа.

В отдельности эти защитные механизмы уже созданы, но не интегрированы в единую систему. Поэтому для комплексной защиты облака эту задачу нужно решать во время его создания. Для решения такой задачи

требуются большие средства, из-за чего компании-поставщики услуг могут сэкономить на этой области, пренебрегая рисками, связанными с нарушением конфиденциальности информации.

Частные «облака» требуют наличие квалифицированных работников, осознающих необходимость соблюдения облачной безопасности и способных обеспечить эффективную работу виртуализационного программного обеспечения, поддерживать нужный уровень сервиса и отвечать за работу приложений в облачной среде. Не во всех организациях есть достаточное количество таких работников, в связи с этим возрастает роль публичных «облаков».

Кроме того, для взаимодействия с «облаками», управления и мониторинга, поставщики услуг предоставляют интерфейсы прикладного программирования (API). От того, насколько защищены эти интерфейсы, зависит безопасность передаваемой информации. Серьезные угрозы для безопасности представляют открытые способы аутентификации, неправильно настроенные средства контроля доступа и ненадлежащая авторизация, к тому же возможности мониторинга для клиента ограничены. Может показаться, что клиенты находятся во власти поставщика услуг, когда дело касается доступа к ресурсам, за которые клиенты платят.

Самым безопасным видом архитектуры «облачных» хранилищ является PaaS, но при условии, если ее использовать как среду разработки своих приложений, что поможет обеспечить большую защиту данных. И тогда пользователи могут быть уверены, что их информацию не увидит владелец «облака», в отличие от SaaS, где пользователям предоставляется уже готовое приложение, в котором они не видят степень защиты и не могут быть уверены в безопасности данных на 100%.

«Облака» появились сравнительно недавно, поэтому эффективные меры по защите информации находятся еще в стадии разработки, особенно в нашей стране, в силу следующих причин:

— Отсутствие нормативной правовой базы, которая контролировала бы поставщиков «облачных» услуг, которые часто экономят на аспекте безопасности;

— зависимость безопасности данных от самих пользователей, от защищенности их компьютеров и других «гаджетов», что тоже является очень затратным. Если добавить к этому то, что используя «облака», созданные на архитектуре IaaS, пользователи не могут контролировать действия владельцев и разработчиков облака, то безопасность данных находится под угрозой.

— большинство потребителей «облачных» услуг не являются специалистами в этой сфере, и могут быть обмануты.

Сергей Комаров, руководитель отдела антивирусных разработок и исследований компании «Доктор Веб»: «Надо понимать, что если вы пользуетесь облачными хранилищами, то полагаетесь на некую вторую сторону, которой априори доверяете.

Чтобы как-то обезопасить себя при этом, всё, что вы можете сделать, это прочесть лицензионное соглашение и полагаться на то, что оно будет соблюдено. И, если оно было нарушено, пытаться возместить ущерб».

В наше революционное время облачные технологии могут предоставить организациям средства и методы, необходимые для обеспечения финансовой стабильности и высокого уровня обслуживания. Естественно, при их внедрении не стоит забывать о рисках, связанных с обеспечением информационной безопасности.

Список литературы

1. Широкова Е. А. Облачные технологии/ Е. А. Широкова // Современные тенденции технических наук: материалы междунар. науч. конф. (г. Уфа, октябрь 2011 г.).— Уфа: Лето, 2011. — С. 30-33.

2. Клементьев И.П., Устинов В.А. Введение в облачные вычисления. Учебное пособие. Издательство ИНТУИТ.

3. Эйдлина Г.М. «Облачная» информационная система управления бизнеспроцессами компании Terrasoft // Международный журнал прикладных и фундаментальных исследований. 2013. - № 10. - С. 87-88.

4. Экономическая информатика: Учебник и практикум. 1-е изд. - Сер. 61 Бакалавр и магистр. Академический курс / под ред. Ю. Д. Романовой. — М.: Юрайт, 2015.

5. Стратегия фирмы «Ай Би Эм» в области технологии [Электронный ресурс]: https://studopedia.ru/8_3649_strategiya-firmi-ay-bi-em-v-oblasti-tehnologii.html

6. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ [Электронный ресурс]: http://www.consultant.ru/document/cons_doc_LAW_61801/

7. Актуальные организационно-правовые вопросы использования облачных технологий: российский и международный опыт (Полякова Т.А., Химченко А.И.) [Электронный ресурс]: http://xn----7sbbaj7auwnffhk.xn--p1ai/article/6994

8. О стратегических направлениях развития ИТ в России [Электронный ресурс]: http://www.crn.ru/numbers/spec-numbers/detail.php?ID=46995

9. FEDERAL CLOUD COMPUTING STRATEGY Vivek Kundra U.S. Chief Information Officer [Электронный ресурс]: http://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloudcomputing-strategy.pdf