Проблемы безопасности облачных вычислений
Кодолов П. А.

Кодолов Петр Андреевич / Kodolov Pyotr Andreevich - магистрант,
кафедра компьютерной и программной инженерии, факультет академия кино и телевидения,
Университет Туран, г. Алматы, Республика Казахстан

Аннотация: *в этой статье рассказывается о проблемах безопасности облачных вычислений, виды атак на облака и решение по их устранению, а так же наиболее эффективные способы защиты от CSA.*
Ключевые слова: *облачное хранилище данных, облачные сервисы, проблемы безопасности, атака на облака, Cloud Security Alliance.*

Проблемы безопасности облачных вычислении.

Контроль и управление облаками являются проблемой безопасности. Гарантий, что все ресурсы облака посчитаны, и в нем нет неконтролируемых виртуальных машин, не запущено лишних процессов, и не нарушена взаимная конфигурация элементов облака, нет. Это – высокоуровневый тип угроз, т.к. он связан с управляемостью облаком как единой информационной системой, и для него общую защиту нужно строить индивидуально. Для этого необходимо использовать модель управления рисками для облачных инфраструктур [1].

В основе обеспечения физической безопасности лежит строгий контроль физического доступа к серверам и сетевой инфраструктуре. В отличие от физической безопасности, сетевая безопасность в первую очередь представляет собой построение надежной модели угроз, включающей в себя защиту от вторжений и межсетевой экран. Использование межсетевого экрана подразумевает работу фильтра с целью разграничить внутренние сети ЦОД на подсети с разным уровнем доверия [2]. Это могут быть отдельно серверы, доступные из Интернета, или серверы из внутренних сетей.

Атака на облака и решение по их устранению.

1. Традиционные атаки на ПО.

Уязвимости операционных систем, модульных компонентов, сетевых протоколов – традиционные угрозы, для защиты от которых достаточно установить межсетевой экран, firewall, антивирус, систему предотвращения вторжений (Intrusion Prevention System – IPS) и другие компоненты. При этом важно, чтобы дан- ные средства защиты эффективно работали в условиях виртуализации.

2. Функциональные атаки на элементы облака.

Этот тип атак связан с многослойностью облака, общим принципом безопасности. В статье, об опасности облаков, было предложено следующее решение [3]: для защиты от функциональных атак для каждой части облака необходимо использовать следующие средства защиты: для прокси – эффективную защиту от DoS- атак, для веб-сервера – контроль целостности страниц, для сервера приложений – экран уровня приложений, для СУБД – защиту от SQL-инъекций, для системы хранения данных – правильные бэкапы (резервное копирование), разграничение доступа. В отдельности каждые из этих защитных механизмов уже созданы, но они не собраны вместе для комплексной защиты облака, поэтому задачу по интеграции их в единую систему нужно решать во время создания облака.

3. Атаки на клиента.

Большинство пользователей подключаются к облаку, используя браузер. Здесь рассматриваются такие атаки как Cross Site Scripting, «угон» паролей, перехваты веб-сессий, «человек посредине» и многие другие. На текущий момент, наиболее эффективной защитой от данного вида атак является правильная аутентификация и использование шифрованного соединения (SSL) с взаимной аутентификацией [4]. Однако данные средства защиты не очень удобны и очень расточительны для создателей облаков. В этой отрасли информационной безопасности есть еще множество нерешенных задач.

4. Атаки на системы управления.

Большое количество виртуальных машин, используемых в облаках, требует наличия систем управления, способных надежно контролировать создание, перенос и утилизацию виртуальных машин. Вмешательство в систему управления может привести к появлению виртуальных машин – невидимок, способных блокировать одни виртуальные машины и подставлять другие.

Решения по защите от угроз безопасности от компании Cloud Security Alliance (CSA).

Наиболее эффективные способы защиты в области безопасности облаков опубликовала организация Cloud Security Alliance (CSA). Проанализировав опубликованную компанией информацию, были предложены следующие решения [5]:

1. Сохранность данных. Шифрование.

Шифрование – один из самых эффективных способов защиты данных. Провайдер, предоставляющий доступ к данным, должен шифровать информацию клиента, хранящуюся в ЦОД, а также, в случае отсутствия необходимости, безвозвратно удалять.

2. Защита данных при передаче.

Зашифрованные данные при передаче должны быть доступны только после аутентификации. Данные не получится прочитать или сделать изменения, даже в случае доступа через ненадежные узлы. Такие технологии достаточно известны, алгоритмы и надежные протоколы AES, TLS, IPsec давно используются провайдерами.

3. Аутентификация.

Аутентификация – защита паролем. Для обеспечения более высокой надежности часто прибегают к таким средствам как токены и сертификаты. Для прозрачного взаимодействия провайдера с системой идентификации при авторизации также рекомендуется использовать LDAP (Lightweight Directory Access Protocol) и SAML (Security Assertion Markup Language).

Заключение.

Описанные решения по защите от угроз безопасности облачных вычислений неоднократно были применены системными интеграторами в проектах построения частных облаков. Практические применения и требования по безопасности подробно описаны в тезисах [1; 2]. После применения данных решений количество случившихся инцидентов существенно снизилось. Но многие проблемы, связанные с защитой виртуализации, до сих пор требуют тщательного анализа и проработанного решения.

Литература

1. *Бердник А. В.* Сравнительный анализ решений по безопасности SaaS сервиса от компании IBM и КРОК. Тюмень, 2012. С. 245-253.
2. *Бердник А. В., Бойко А.* Методы защиты виртуальной среды // Всероссийский журнал научных публикаций. 2013. № 3 (18). С. 24-27.
3. *Коржов В.* Опасны ли облака? [Электронный ресурс] // Сети / Network World. 2010. № 07. URL: http://www.osp.ru/nets/2010/07/13004633/ (дата обращения: 19.08.2013).
4. Облака: легенды и мифы [Электронный ресурс]. URL: http://www.anti-malware.ru/node/2333 (дата обращения: 19.08.2013).
5. [Электронный ресурс]. Облачные вычисления, «дырявые» облака и способы защиты данных URL: http://4by4.ru/ru/analytics/oblachnye-vychisleniya-dyryavye-oblaka-i-sposoby-zashchity-dannyh (дата обращения: 19.08.2013).