электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

 # 10, октябрь 2015

УДК 004.632.4

Вопросы безопасного размещения данных в «облаке»

Кудряшов Н.И., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Компьютерные системы и сети»

Научный руководитель: Гуренко В.В., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
кафедра «Компьютерные системы и сети»
wgurenko@bmstu.ru

1. Облачные вычисления

Для того, чтобы понять, как защищать облачную инфраструктуру, нужно понять, какую систему необходимо обезопасить и, что она из себя представляет. Существует ряд определений «облачных вычислений». На рис. 1 представлены логотипы компаний, давших наиболее знаменитые определения облачных технологий.

а *б* *в*

Рис. 1. Логотипы:
а — Gartner, б — Forrester, *в* — NIST

Вот, например, определение от Gartner — исследовательской и консалтинговой компании, специализирующейся на рынках информационных технологий [1]: «*...стиль вычислений, в котором масштабируемость и эластичность готовых IT решений предоставляется внешним заказчикам при помощи интернет технологий в виде службы...*»

Forrester Research (еще одна известная независимая консалтинговая компания) дала свое определение: «*...стандартизованное IT-решение (сервис, программное обеспечение*

или инфраструктура), доставляемая при помощи Интернет в pay-per-use (оплата за потребление) и self-service (самообслуживание) виде...»

Национальный Институт Стандартов и Технологий (NIST) сумел дать такое определение, которое было принято большинством специалистов в IT-индустрии: «*Облачные вычисления — это модель для предоставления повсеместного удобного сетевого доступа к общему пулу настраиваемых вычислительных ресурсов (таких как сети, сервера, дисковые системы хранения, приложения и сервисы), которые могут быть быстро предоставлены минимальными усилиями со стороны провайдера сервиса*».

2. Угрозы облачным хранилищам и соответствующие методы защиты

Каждая из ранее указанных проблем имеет свои, свойственные только ей особенности. Рассмотрим далее каждую угрозу и возможные предостережения.

2.1 Потеря и кража размещаемого контента

Размещаемые в облаке данные и программные разработки занимают место в каком-то удаленном от клиента месте. Таким образом сам пользователь не имеет возможности следить за безопасностью своего контента. За сохранностью данных должен следить облачный провайдер.

Если база данных облака с множественной арендой не продумана должным образом, то изъян в приложении одного клиента может открыть взломщикам доступ к данным не только этого клиента, но и всех остальных пользователей облака. Данные, хранящиеся в облаке, могут быть украдены злоумышленниками или потеряны по другой причине [2,3]. Если поставщик облачных услуг не внедрит должные меры резервного копирования, данные случайно может удалить сам провайдер или они пострадают при пожаре или стихийном бедствии. С другой стороны, заказчик, который шифрует данные до того, как выгрузить их в облако, вдруг потерявший шифровальный ключ, также утратит свои данные. Чаще всего данные проблемы решаются с помощью запоминающих устройств (рис. 2) с большим запасом памяти, но такой способ требует слишком много затрат.

а

б

в

Рис. 2. Устройства хранения данных:

а — Дисковые массивы; б — Ленточные библиотеки; *в* — Оптические библиотеки;

В качестве дополнительных решений данных проблем следует заранее обдумать всю инфраструктуру облака, чтобы при взломе одного приложения клиента, остальные приложения оставались нетронуты. Вдобавок к этому организации должны провести обширную, тщательную проверку своих внутренних систем и потенциального поставщика облака, чтобы полностью уяснить все риски, которым они себя подвергают, переходя на новую модель. При потере данных можно использовать систему резервирования, если такая имеется. К тому же следует рассмотреть возможность о ведении дополнительной отчетности. Таким образом облачный менеджер сможет хранить все данные в текстовом формате, а это в свою очередь сэкономит ресурсы. Он сможет в любой момент использовать нужные файлы, привязанные к определённой дате, если возникнет необходимость.

2.2 Отказ в обслуживании

На облако могут быть предприняты атаки типа «отказ в обслуживании», которые вызывают перегрузку инфраструктуры, заставляя задействовать огромный объем системных ресурсов и не давая заказчикам пользоваться этой услугой. Внимание прессы чаще всего привлекают распределенные, или DDoS-атаки (рис. 3), но есть и другие типы DoS-атак, которые могут блокировать облачные вычисления.

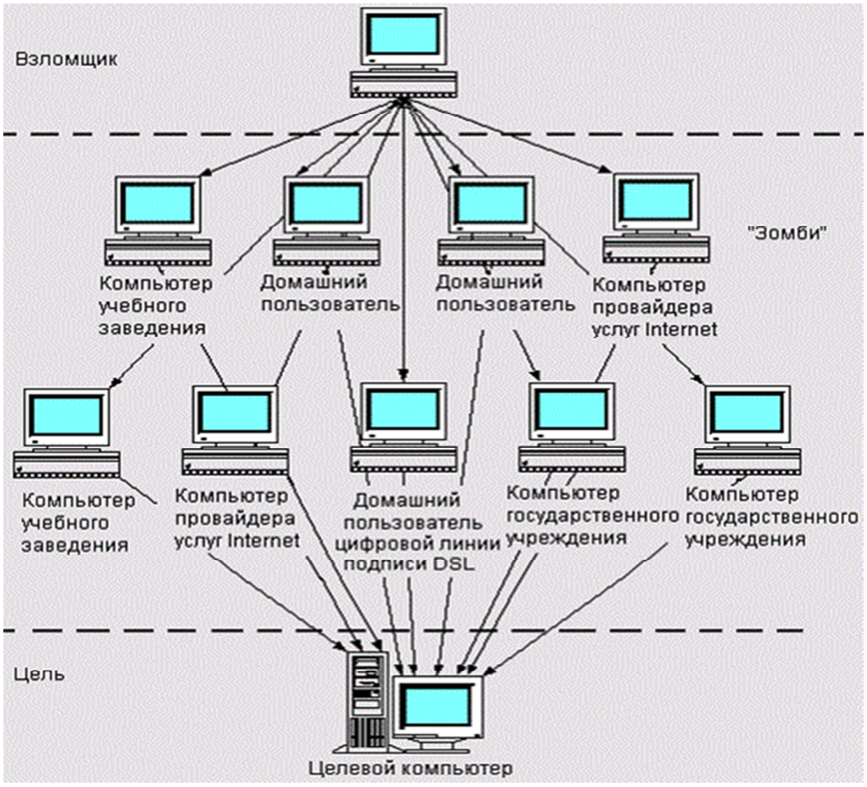

Рис. 3. Пример DoS атаки

К примеру, злоумышленники могут запустить асимметричные DoS-атаки прикладного уровня, используя уязвимости в Web-серверах, базах данных или других облачных ресурсах, чтобы завалить приложение с очень малой полезной нагрузкой. Общепринятым решением являются использование фильтров для анализа трафика [4].

Предлагаемый усовершенствованием является повышение допустимой нагрузки на серверы. Таким образом даже если зараженный запрос дойдет до главного устройства, отвечающего за работу всей системы, то оно не будет перегружено. Данный способ не требует большого количества энергоресурсов, в связи с чем является очень выгодным.

2.3 Использование облачных ресурсов хакерами

Облачные вычисления дают возможность организациям любого размера задействовать огромную вычислительную мощь, но кто-то может захотеть сделать это с неблаговидными намерениями. К примеру, хакер может использовать совокупную мощь серверов облака, чтобы взломать шифровальный ключ в считанные минуты. Обычно против таких видов атак используют шифрование и аутентификацию (рис. 4).

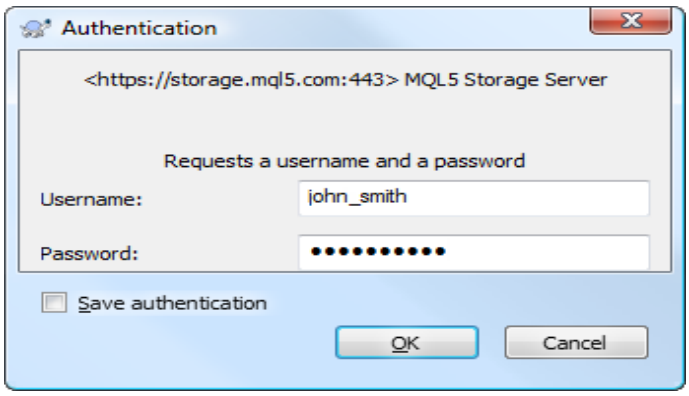

Рис. 4. Пример простейшей аутентификации

Поставщики облачных услуг должны продумать, как они будут отслеживать людей, использующих мощь облачной инфраструктуры во вред, каким образом будут выявляться и предотвращаться такие злоупотребления [4,5].

В качестве новых методов предлагается использовать новые технологии, а именно: OTP (One Time Password) и Helo Netsec, сервис компании CloudPassage. Первый позволяет использовать пароль всего один раз. Это очень эффективно, так как даже если злоумышленник украл логин и пароль пользователя, то пароль уже устареет. Пароль пользователю может передаваться через специальное приложение или же через почту. Второй метод имеет возможность использования межсетевого экрана и двойной аутентификации.

2.4 Похищение аккаунтов и взлом услуг

В облачной среде взломщик может использовать украденную регистрационную информацию, чтобы перехватывать, подделывать или выдавать искаженные данные перенаправлять пользователей на вредоносные сайты. Организациям следует запретить раздачу своих регистрационных данных другим служащим и использование одних и тех же паролей для всех сервисов. Нужно также внедрить надежную, двухфакторную аутентификацию для снижения риска. В среде IaaS, PaaS или SaaS, где не обеспечен должный уровень безопасности, инсайдер, имеющий неблаговидные намерения (например, системный администратор), может получить доступ к конфиденциальной информации, которая ему не предназначена [5,6].

Системы, которые в обеспечении безопасности полагаются только на поставщика облачных услуг, подвергают себя большому риску [1,2]. Даже если внедрено шифрование, если ключи не хранятся только у заказчика, будучи доступны лишь на время пользования данными, то система всё еще подвержена злонамеренным действиям инсайдера.

Заключение

Проведенный анализ позволяет констатировать, что каждый вариант представляет интерес с точки зрения разработчика. Можно утверждать, что для экономии ресурсов выгоднее использовать предложенные способы решения проблем. Наиболее эффективным является комбинирование выше упомянутых методов защиты данных. В перспективе представляется целесообразным разработать свою систему безопасности контента, размещенного в облаке.

Список литературы

1. Защита безопасности облачных технологий. Режим доступа: http://www.la.by/forum/oblachnaya-bezopasnost/zashchita-bezopasnosti-oblachnyh-tehnologiy (дата обращения 12.05.2015).
2. Игорь Емельянов. Облачная защита – технология против идеологии. Режим доступа: http://www.computerra.ru/95632/oblachnaya-zashhita-tehnologiya-protiv-ideologii/ (дата обращения 12.0.2015).
3. Защита в облачных технологиях. Режим доступа: http://www.shpionazha.net/zashhita-v-oblachnyx-texnologiyax.php (дата обращения 12.05.2015).
4. Юрий Машевский. Антивирусный прогноз погоды: облачно. Режим доступа: http://www.antivirus-navigator.com/articles/kaspersky-cloud.htm (дата обращения 12.05.2015).
5. Угрозы безопасности в облаке. Режим доступа: http://www.tadviser.ru/index.php/Статья:Главные_угрозы_безопасности_в_облаке (дата обращения 12.05.2015).
6. Eric Griffith. What is cloud computing. Режим доступа: http://www.pcmag.com/article2/0,2817,2372163,00.asp (дата обращения 12.05.2015).