УДК 004.77
ББК 32.973.202
Д 58

Довгаль В.А.
Кандидат технических наук, доцент кафедры автоматизированных систем обработки информации и управления инженерно-физического факультета Адыгейского государственного университета, Майкоп, тел. (8772) 59-39-11, e-mail: urmia@mail.ru

Методы повышения безопасности в сфере «облачных» технологий

(Рецензирована)

Аннотация. *Рассматриваются методы предотвращения угроз при передаче данных между провайдером, предоставляемым услуги «облачных» сервисов, и заказчиком. Проведен анализ угроз информации, обрабатываемой с помощью «облачных» технологий, а также решений для устранения указанных проблем. Предлагается комплекс мероприятий, применяемый для предотвращения угроз безопасности в частных «облаках» и обеспечения необходимого уровня безопасности информации.*

Ключевые слова: *«облачные» технологии, угрозы информации в «облаках», методы предотвращения угроз при передаче данных в «облаках».*

Dovgal V.A.
Candidate of Technical Sciences, Associate Professor of Department of Automated Systems of Processing Information and Control of Engineering-Physics Faculty, Adyghe State University, Maikop, ph. (8772) 59-39-11, e-mail: urmia@mail.ru

Methods of safety increase in the sphere of «cloud» technologies

Abstract. *The paper discusses the methods of threats prevention at data transmission between the provider of «cloud» services and the customer. An analysis is made of threats to information processed by means of «cloud» technologies, as well as of solutions to eliminate the specified problems. The complex of actions is proposed to prevent threats to security in private «clouds» and to ensure the necessary level of information safety.*

Keywords: *«cloud» technologies, threats to information in «clouds», methods of threats prevention at data transmission in «clouds».*

«Облачные» («Cloud») технологии – это совокупность методов и средств обработки данных, предоставляющих пользователю сети Интернет компьютерные ресурсы как онлайн-сервис. «Cloud» является некоторой виртуальной сложной структурой со скрытыми техническими деталями. Основная функция «облачных» технологий – предоставление услуг удаленной обработки данных, использующихся в настоящее время не только в публичной сфере, но и в частном секторе. Совершенствование технологий виртуализации и увеличение пропускной способности каналов открывает перед частными «облаками» широкие перспективы [1].

В тоже время они актуализируют проблему обеспечения достаточного уровня безопасности «облачных» сервисов. По сути, основным фактором, который тормозит развитие последних, является отсутствие мероприятий и средств информационной безопасности для таких сред.

Поскольку в «облаке» отсутствует понятие периметр защиты, то ключевое внимание необходимо уделять вопросам обеспечения безопасности, доступности и защиты данных при передаче информации в обоих направлениях. В реализации проекта и снижении его стоимости одним из важнейших шагов будет построение модели процесса для формализации этой задачи. Недостаточно продуманная на этом этапе работа приведет к созданию неэффективных решений, цена которых очень высока. С точки зрения технической составляющей, перед поставщиками услуг стоит задача обеспечения конфиденциальности, доступности и целостности данных на всем пути от дата-центра к пользователю. Очевидно, что «облачные» решения должны базироваться на современных стандартах безопасности – применении эффективных методов шифрования, акту-

альных средств антивирусной защиты, блокировании атак, обеспечении безопасности рабочих мест пользователей. Одним из наиболее качественных решений этой проблемы является использование виртуальных машин, обеспечивающих защиту рабочего места непосредственно в центре обработки данных. Кроме того, поставщики «облачных» услуг обращают внимание на доступность сервисов. Разработчикам проекта частного «облака» необходимо предусмотреть альтернативные варианты доступа в случае аппаратных и других сбоев.

Для достижения высокого уровня обеспечения информационной безопасности заказчик услуг и потребитель должны объединить свои усилия. Безопасность «облака» будет состоять из стандартных элементов защиты систем, и, невзирая на достаточно хорошо отработанные методики, интеграция этих решений может нуждаться в новых подходах в сфере информационной безопасности [2].

Рассмотрим виды угроз информации, обрабатываемой с помощью «облачных» технологий:

– традиционные атаки на программное обеспечение, связанные с уязвимостью применяемых сетевых протоколов, операционных систем, модульных компонентов и т.п. Для защиты от таких угроз достаточно установить антивирус, межсетевой экран и другие средства. Важным здесь представляется адаптация средств защиты к «облачной» инфраструктуре и их эффективная работа в условиях виртуализации;

– функциональные атаки на элементы «облака», связанные с многослойностью «облака». Общий принцип безопасности здесь состоит в защите самого слабого звена системы. Например, успешная DoS-атака на обратный прокси-сервер, установленный перед «облаком», заблокирует доступ ко всему «облаку», несмотря на то, что внутри системы все соединения будут работать без препятствий. Для защиты от функциональных атак для каждого слоя «облака» необходимо использовать специфические для него средства защиты: для прокси-серверов это может быть защита от DoS-атак, для веб-серверов – контроль целостности страниц, для сервера программ – экран уровня программ, для слоя СУБД – защита от SQL-инъекций, для системы хранения – резервное копирование и разграничение доступа. Каждые из этих защитных механизмов по отдельности уже созданы, но они все еще не собраны вместе для комплексной защиты «облака», поэтому работы по их интеграции в единую систему необходимо решать во время создания «облака»;

– атаки на клиента – тип атак, отработанный в веб-среде, но актуальный и для «облака», т.к. клиенты подключаются к «облачному» сервису, как правило, с помощью браузера, который, в свою очередь, подвержен таким атакам, как перехваты веб-сессий, кража паролей, «противник в середине» и другие. Традиционно защита от этих атак основывается на строгой аутентификации и использовании шифрованного соединения с взаимной аутентификацией;

– угрозы виртуализации связаны с традиционным использованием виртуальных сред как платформ для компонентов «облака». Очевидно, что атаки на систему виртуализации угрожают и всему «облаку» в целом;

– комплексные угрозы «облачным» сервисам возникают из-за некорректного контроля инфраструктуры и управления ими. Нет гарантии, что в «облаке отсутствуют лишние виртуальные машины или не запущены лишние бизнес-процессы. Этот тип угроз связан с управлением «облаком» как единой информационной системой и поиском злоупотреблений или других нарушений в работе «облака», которые могут привести к лишним расходам в поддержку работоспособности информационной системы.

«Облачные» сервисы для решения проблем информационной безопасности имеются уже в настоящий момент. К ним относятся средства по обеспечению безопасности электронной почты и по контролю веб-трафика, возможности антивирусной защиты и

блокирования программного обеспечения злоумышленников, предоставляемого как сервис. Самый простой и экономичный в настоящее время способ создания частного «облака» – виртуализация IT-инфраструктуры (виртуализация серверов, виртуализация сетевого оборудования и т.п.). Но при переходе от традиционной IT-инфраструктуры в виртуальную кроме оставшихся традиционных вопросов обеспечения информационной безопасности добавляются новые. Прежде всего, можно выделить неограниченные права администраторов виртуальной инфраструктуры, в том числе неограниченный доступ к данным пользователей.

Из новых вопросов информационной безопасности можно отметить безопасное функционирование гипервизора на серверах, что обеспечивает безопасное функционирование системы управления виртуальной инфраструктурой и независимое функционирование виртуальных машин. С одной стороны, «облачные» вычисления обеспечивают экономичность и легкость в управлении и мониторинге ресурсов, с другой – это новое направление, в котором возникают нетипичные задания.

В настоящее время ведущие операторы связи предлагают комплекс решений по переходу к построению IT-систем на основе «облака»: создание частного «облака», услуги по резервированию, а также предложения в сфере обеспечения их безопасности.

Кроме того, сейчас развивается технология предоставления услуг безопасности таких, как SaaS (Software as a Service – программное обеспечение как сервис). Сервисы SaaS основаны на принципе подписки: программное обеспечение работает на стороне провайдера и предоставляется абонентам в аренду (оплата зависит от числа пользователей, объема транзакций и т.п.). Например, услуга Anti-DDoS.

Оформляя свои решения шаблонными методами виртуализации в «облаке», поставщики технологий обеспечения безопасности получают в первую очередь максимум оперативности и простоты. В тоже время, и их клиенты получают оперативность их развертывания и внедрения своих практических задач. Более того, «облачные» технологии позволили с максимальной простотой комбинировать и наращивать технологии безопасности, т.к. до недавнего времени переход от их проектирования к реализации в реальные решения был трудоемким. Используя «облачные» технологии, эта задача теперь становится простой и требует минимум усилий, финансовых и временных расходов.

Другой важнейшей задачей является обеспечение безопасности мобильных технологий, которые позволяют расширять сеть за счет планшетов и смартфонов, выполняющих функции конечных устройств. В связи с этим в прошлое отходит традиционный подход к обеспечению информационной безопасности в виде периметра. Поскольку понятие периметра размывается, а границы сети исчезают, то возникает сложность в отношениях между провайдером и заказчиком. Между ними необходимо четко распределить ответственность, контроль, проанализировать риски, определить компенсации, страховку и т.д. Применение «облачных» вычислений дает большое преимущество: профессионализм самого заказчика в области информационной безопасности некритичен – заказчик лишь получает услугу. Важен профессионализм провайдера, который должен обеспечить глобальную политику безопасности на основе новейших технологий и последних требований. «Облачные» вычисления строятся на основе технологий виртуализации. Поэтому при обеспечении безопасности данных в «облаках» не обойтись без применения специализированных инструментов защиты, способных нейтрализовать специфические угрозы среды виртуализации. Среди других необходимо вспомнить несанкционированный доступ к данным виртуальных машин через гипервизор, а также посредством средства управления инфраструктурой виртуализации. Правильная настройка платформы виртуализации, позволяющая снизить стоимость проекта по защите информации, может быть выполнена IT-администраторами двумя способами:

– вручную (с временными затратами, постоянным контролем и соответствующи-

ми расходами на поддержку соответствия IT-инфраструктуры, принятым политикам информационной безопасности);

– с помощью специальных средств защиты информации, обеспечивающими функциями автоматизации настроек и контролем исполнения политик.

Существует несколько типов подобных услуг, которые условно можно назвать Security-as-a-service – фактически это модель аутсорсинга для управления безопасностью, в которую включены защита от спама, антивирусная защита, фильтрация URL-адресов и защита от DDoS-атак.

Основная проблема при использовании «облачных» сервисов – угроза нарушения конфиденциальности, доступности и целостности данных при их передаче от заказчика провайдеру сервиса. Также нет гарантии, что поставщик услуг не воспользуется или не ознакомится с конфиденциальной информацией [3]. Для предотвращения этих угроз предлагается применить комплекс мероприятий, которые обеспечат необходимый уровень безопасности.

1. Использовать безопасное шифрованное соединение при передаче данных между заказчиком и провайдером «облачных» сервисов. Например, необходимо использовать криптографический протокол SSL (Secure Sockets Layer), обеспечивающий установление безопасного соединения и конфиденциальность обмена данными между клиентом и сервером на основе TCP/IP и использующий для шифрования асимметричный алгоритм с открытым ключом. Шифрование с открытым ключом использует два ключа – открытый ключ передается по открытому (незащищенному, доступному для наблюдения) каналу и используется для проверки электронной подписи и для шифрования сообщения. Для генерации электронной подписи и для расшифровки сообщения используется закрытый ключ. Используя такую схему, можно получать защищенные сообщения, публикуя открытый ключ и храня в секрете секретный ключ.

Работу безопасного протокола SSL можно разделить на два уровня:

а) слой протокола подтверждения подключения (Handshake Protocol Layer), в свою очередь состоящего из трех подпротоколов: протокола подтверждения подключения (Handshake Protocol), протокола изменения параметров шифра (Change Cipher Spec Protocol) и предупредительного протокола (Alert protocol);

б) слой протокола записи – это уровневый протокол, определяющий формат передачи данных.

Применение протокола SSL позволяет предоставить канал, который имеет три основных свойства:

– с точки зрения аутентификации: сервер всегда аутентифицируется, в то время как клиент аутентифицируется в зависимости от алгоритма;

– с точки зрения целостности: обмен сообщениями включает в себя проверку целостности;

– с точки зрения конфиденциальности канала: шифрование используется после установления соединения и используется для всех последующих сообщений.

2. Провайдер «облачных» сервисов должен предоставить заказчику услугу VPS (Virtual Private Server) – современная технология хостинга, позволяющая создавать собственный виртуальный выделенный сервер, расположенный на отдельной физической машине. Услуга предоставит возможность заказчику загрузить код, который поможет создать собственный виртуальный тоннель внутри защищенного соединения, внутри которого будут передаваться данные между заказчиком и провайдером «облачных» сервисов. Данные в таком тоннеле могут передаваться как в зашифрованном, так и незашифрованном виде. Их шифрование позволит обеспечить безопасность конфиденциальных данных. В случаях, когда не требуется высокий уровень безопасности и необходима высокая производительность системы, данные могут отправляться в незашиф-

рованном виде. Шифрование данных можно проводить с помощью различных популярных и не очень распространенных алгоритмов. Например, можно применить широко используемый алгоритм RSA – криптографический алгоритм с открытым ключом. В криптографической системе с открытым ключом каждый участник располагает открытым и закрытым ключами, которые он создает самостоятельно. Кроме того, каждый ключ состоит из пары целых чисел. Закрытый ключ является секретным, а открытый ключ можно сообщать кому угодно. Эти ключи у каждого участника обмена сообщениями в криптосистеме RSA образуют «согласованную пару» в том смысле, что они являются взаимно обратными. С помощью алгоритма RSA можно шифровать данные, которые требуют высокого уровня безопасности.

Если к данным не предъявляются высокие требования по их защите, то можно воспользоваться, например, простым, но достаточно эффективным алгоритмом XOR с использованием длинного ключа. Данный способ повысит уровень защищенности при передаче данных и не допустит ознакомления с конфиденциальной информацией провайдера «облачных» сервисов.

Таким образом, применение предложенных мероприятий повышает надежность защиты данных при передаче между заказчиком и провайдером «облачных» сервисов, т.е. снижается вероятность нарушения конфиденциальности, целостности и доступности данных. Кроме того, усложняется возможность несанкционированного доступа к конфиденциальным данным провайдера «облачных» услуг. Такая система универсальна и подходит для любого вида информации. Данные можно зашифровывать как стойкими и надежными алгоритмами шифрования, так и применять менее ресурсоемкие алгоритмы, если к информации не предъявляются высокие требования защиты.

Использование «облачных» технологий выгодно для конечного потребителя и небольших компаний. Они подходят для решения простых и понятных задач, когда нецелесообразно инвестирование средств в полномасштабное IT-решение. Примерами таких задач является Web-hosting, хранение личных данных в «облаке», электронная почта, антивирусная защита и т.п. Экономические и организационные выгоды здесь очевидны: нет нужды платить за использование серверов, маршрутизаторов, дисковых массивов и держать штат сотрудников для их обслуживания.

Примечания:

1. Валентинова Т. Что в действительности представляют собой облачные сервисы. URL: http://www.hwp.ru/articles/CHto_-v_deystvitelnosti_predstavlyayut_soboy_oblachnie_servisi/
2. Винклер В. Облачные вычисления: оценка «облачных» рисков // TechNet Magazine. URL: http://technet.microsoft.com/ru-ru/magazine/hh-750397.aspx
3. Дремач К. Облачные сервисы: проблемы в доверии // Information Security = Информационная безопасность. URL: http://www.itsec.ru/articles2/cloud-security/oblachnie-servisi-problemi-v-doverii

References:

1. Valentinova T. What the cloud services actually represent: URL: http://www.hwp.ru/articles/CHto_-v_deystvitelnosti_predstavlyayut_soboy_oblachnie_servisi/
2. Winkler V. Cloud computing: An assessment of «cloudy» risks // TechNet Magazine. URL: http://technet.microsoft.com/ru-ru/magazine/hh-750397.aspx
3. Dremach K. Cloudy services: problems in trust // Information Security. URL: http://www.itsec.ru/articles2/cloud-security/oblachnie-servisi-problemi-v-doverii