электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель Общероссийская общественная организация "Академия инженерных наук им. А.М. Прохорова"
ISSN 2307-0609

 # 02, июнь 2018

УДК 004.056.2

Обеспечение целостности информации, хранящейся в облачных структурах

Назарова Е.К., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»
alenan95@mail.ru

Научный руководитель: Медведев Н.В., к.т.н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»
iu8@bmstu.ru

Аннотация: В статье анализируются основные актуальные угрозы, от которых зависит требуемый уровень защищенности данных, хранящихся в облачных структурах. Перечислены основные способы, связанные с защитой информации, хранящейся в облачных структурах.

Ключевые слова: облачные технологии, защита информации, целостность информации, DDos-атаки, защищаемый сетевой ресурс.

Введение

Активное развитие информационных технологий в настоящее время, приводит к необходимости тщательнее обеспечивать безопасность персональных данных, хранящихся в облачных структурах коммерческого применения. Облачные технологии позволяют бизнесу разгружать собственные компьютеры. Но хранение информации на неизвестных серверах повышает требования к информационной безопасности. Особенности защиты связаны с тем, что облачные структуры постоянно доступны через интернет, в том числе для злоумышленников.

* * *

Обеспечение безопасности строится по трём уровням. Очень важно, чтобы все 3 аспекта присутствовали и имели высокое качество. Это необходимо из-за того, что каждый уровень влияет на другие. Провал в одном аспекте сразу делает бессмысленными все остальные усилия.

1. **Техническая составляющая.** К ним относятся технические мощности и характеристики серверов, а также наличие других приборов. Например, бессмысленно вести учёт действий всех пользователей и событий (программная составляющая безопасности), если злоумышленник может обрушить сервер с этими данными с помощью DDoS-атак.
2. **Программная составляющая.** К ней относится хеширование данных, передача только зашифрованной информации и другие аспекты. Нет смысла делать множество паролей и контролировать каждого сотрудника, чтобы он их не передавал посторонним, когда пароли может украсть каждый хакер прямо с сервера.
3. **Управленческая составляющая.** Сюда относят внутренние правила в компании, контроль сотрудников, регулярное обновление паролей, соблюдение корпоративных тайн. Не имеют значения программные и технические новшества, если пьяные сотрудники на вечеринке сообщают пароли и оставляют карточки доступа.

Рассмотрим многофакторную аутентификацию, представляющую собой способ защиты данных, когда для авторизации пользователя в системы ему нужно предоставить несколько доказательств механизма аутентификации. Приведём несколько примеров:

Знание. В первую очередь сюда относится пароль, но к так же могут быть причислены персональные данные, кодовые слова. Это наиболее распространённый способ. Однако пароль легко похищается через интернет, так что он не является абсолютно надёжным. К тому же если он довольно простой, то злоумышленник может подобрать его самостоятельно.

Владение. Подразумевает, что доступ к данным может получить лишь человек, который обладает определённым предметом: карточкой, магнитным ключом, сотовым телефоном. Например, для доступа человеку необходимо подтвердить свой мобильный номер. Для чего пользователю отправляется СМС с одноразовым паролем.

Свойство человека. Сюда относятся различные биометрические данные: отпечаток пальца, черты лица, голос, сетчатка глаза. Значительно более дорогой метод защиты, который редко применяется для защиты облачных данных. Но он при совмещении с предыдущим методом имеет гораздо более высокую степень защиты.

Также, необходимо ограничивать число попыток аутентификации, то есть у пользователя есть ограниченное число попыток ввода логина или пароля. Если пользователь ввёл неправильные данные несколько раз подряд в течение короткого

времени, то он блокируется по IP-адресу. После этого вход можно осуществить только с определённого компьютера или для авторизации потребуется гораздо больше информации.

Пример многофакторной аутентификации изображен на рисунке 1.

Рис. 1. Многофакторная аутентификация

Многофакторная аутентификация может оказаться недостаточно эффективна, если будут осуществляться DDos-атаки на защищаемый сетевой ресурс.

Смысл DDoS-атаки в том, чтобы загрузить сервер огромным количеством запросов. Самым распространённым и надёжным методом защиты является ограничение числа запросов для каждого IP-адреса. Но абсолютной гарантии такой способ не даёт. Поэтому дополнительно рекомендуется иметь в резерве дополнительные вычислительные ресурсы. Что облачные серверы могут довольно легко предоставить.

Рассмотрим такое понятие, как обеспечение безопасности в глубине. Под этим следует понимать, что в большинстве случаев, облачная база данных имеет монолитную структуру, из-за чего при взломе защиты на одном уровне мгновенно возникает угроза и для остальной информации. Чтобы этого не произошло, необходимо создавать несколько требований аутентификации. То есть пользователь для входа в общее поле информации должен сначала ввести один пароль. Затем для авторизации на каком-то уровне от него требуется уже другой пароль.

Для предоставления аутентификации в глубину, необходимо анализировать вводимые данные на каждом этапе аутентификации для предотвращения подбора ключей.

Нередко базы данных переносятся с одного сервера на другой, по-разному систематизируются. Из-за этого в долговременной перспективе становится сложно постоянно отслеживать вход/выход пользователя, передаваемые программы и обновления. В итоге если злоумышленник будет делать атаки редко, то есть каждый раз на новый сервер или с нового IP-адреса, то его будет трудно отследить.

Для предотвращения такой ситуации необходимо, чтобы действия всех пользователей, установленные программы, целостность данных регистрировалась в отдельном журнале. Это позволит найти и обезвредить таких злоумышленников. Но сам журнал всех действий – ценная информация для хакера, так что эту базу данных нужно обезопасить максимально.

Одним из наиболее эффективных способов обеспечения целостности информации, хранящейся в облачных структурах, является хеширование.

Все пароли, логины и другие ценные данные должны храниться не в форме открытых файлов, а в виде хешей. Хеширование – способ шифрования информации, который в настоящий момент является наиболее надёжным алгоритмом. Его почти невозможно взломать. Теоретически это можно сделать, но на практике понадобятся слишком большие ресурсы.

Хешировать нужно не только хранящиеся данные, но и передаваемую информацию. То есть при авторизации с компьютера пользователя для сверки должен передаваться не пароль, а его хеш. То же самое касается любой передачи особо ценных данных. Разумеется, необходимо использовать современные алгоритмы, которые не искажают информацию при хешировании.

При передаче и получении данных информация в интернете обязательно шифруется. В целях их защиты в публичном облаке используется туннель виртуальной частной сети, который представляет собой совокупность двух сетей для формирования автономной логической сети. Это технология, которая создает безопасное и зашифрованное соединение в менее защищенной сети, например, в Интернете.

Заключение

В данной статье были проанализированы основные методы обеспечения целостности информации, хранящейся в облачных структурах. Для эффективного обеспечения безопасности информации, необходимо применение нескольких способов защиты и использование только криптографически стойких алгоритмов.

Список литературы

[1]. Клементьев И.П., Устинов В.А. Введение в облачные вычисления // Интернет университет информационных технологий. Режим доступа: http://www.intuit.ru/department/se/incloudc/ (дата обращения: 22.10.2016).

[2]. Коммуникации для бизнеса. Надежна ли защита у вашего Internet-провайдера. Режим доступа: http://www.osp.ru (дата обращения: 12.05.2018).

[3]. Машкина И.В., Рахимов Е.А., Васильев В.И. Методика построения модели комплексной оценки угроз информации, циркулирующей на объекте информатизации. // Известия ТРТУ. Материалы VIII научно-практической конференции «Информационная безопасность». Таганрог: ТРТУ. 2006. С. 70-76

[4]. Мельников В.В. Безопасность информации в автоматизированных системах. М.: Финансы и статистика. 2003. 368 с.

[5]. Gentry C. A fully homomorphic encryption scheme / C. Gentry. Stanford University, Ph.D. thesis. 2009.

[6]. Li J., Wang Q., Wang C., Cao N., Ren K., Lou W. Fuzzy keyword search over encrypted data in cloud computing. Mini-Conf. IEEE INFOCOM. 2010. 5 p. DOI: 10.1109/INFOCOM.2010.5462196

[7]. Miller R. Who Has the Most Web Servers? 2012. Режим доступа: http://www.datacenterknowledge.com/archives/2009/05/14/whos-got-the-most-web-servers/ (дата обращения: 14.05.2018).

[8]. R. L. Rivest, L. Adleman, M. L. Dertouzos. On data banks and privacy homomorphisms // Foundations of secure computation. 1978. Vol. 32. No. 4. Pp. 169–178.