УДК 004.75:65.012.8

ПРОБЛЕМЫ БЕЗОПАСНОСТИ “ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ”

Стасивский Л.С., Масальская Е.О.
Государственный ВУЗ “Национальный горный университет”, nmu.org.ua, stasivskyj@yandex.ru

Переход в “облака” сулит новые возможности, но требует тщательной проработки вопросов безопасности. В докладе идет речь об актуальных угрозах облачным вычислениям и о механизмах обеспечения безопасности.

Ключевые слова – облачные вычисления; безопасность.

ВСТУП

Наиболее актуальным вопросом "облачных вычисленияй", является вопрос информационной безопасности, так как данные хранятся и обрабатываются на удаленных, не контролируемых пользователями информационных ресурсах. Решение по обеспечению информационной безопасности полностью ложится на провайдер, который обязан позаботиться об охране доступа, в том числе и о физической, а также об устойчивости к сбоям.

ПРОБЛЕМЫ БЕЗОПАСНОСТИ “ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ”

1. Проблема выбора провайдера, предоставляющего облако;
2. Проблема организации доступа к ресурсу;
3. Проблема хранения и конфиденциальности данных;
4. Проблема изоляции ресурсов;
5. Проблема авторизации пользователей через социальные сети.

РЕШЕНИЕ ПРОБЛЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В “ОБЛАКАХ”

Проблема выбора провайдера предоставляющего облако. Первоначально стандарты безопасности представляет владелец «облака». Дополнительно провайдер проходит аудит и сертификацию по стандартам ISO/IEC 27001:2005 и SAS 70 Type II и Type I. (По многочисленным требованиям клиентов, провайдер может пойти на дополнительную сертификацию по выполнению стандартов ИТ-безопасности, например на федеральном уровне США в соответствии с актом FISMA (Federal Information Security Management Act).

Проблема организации доступа к ресурсу. Приложение и вся база данных пользователей находится на серверах, и существует возможность “падение” этих серверов. Для поддержания постоянной доступности к данным целесообразно использование нескольких “fault domain” (технология обеспечения распределения сервиса между двумя серверами с помощью коммутатора) на сервис (автоматически ваш заказанный сервис будет реплицирован, например, на два “fault domain” и при падении одного “fault domain” ваша работа продолжится на другом)

Проблема хранения и конфиденциальности данных. Для обеспечения сохранности хранимых конфиденциальных данных провайдер должен шифровать как данные при передаче (например, с помощью TSL) так и хранящуюся на своих серверах информацию клиента для предотвращения случаев неправомерного доступа. Провайдер обязан безвозвратно удалять данные тогда, когда они больше не нужны и не потребуются пользователю в будущем.

Проблема изоляции ресурсов. Лучшим способом разделения данных и приложения одного клиента от данных и приложений другого клиента является ситуація, когда каждый из ресурсов использует индивидуальную виртуальную машину (Virtual Machine – VM) и виртуальную сеть. Виртуальные сети, в свою очередь, развертываются с применением стандартных технологий, таких как VLAN (Virtual Local Area Network), VPLS (Virtual Private LAN Service) и VPN (Virtual Private Network).

Проблема авторизации пользователей через социальные сети. Каждый пользователь должен иметь уникальный логин. Не должно быть никакого объединения с существующими учетными записями (OAuth). Так как сами провайдеры OAuth (например, facebook) шифруют только сам процесс авторизации, а все артефакты (куки), которые используются для аутентификации, после авторизации идут в незашифрованном виде, поэтому возможен перехват данных и доступ к “облаку” пользователя.

Таким образом, следует выделить основные меры защиты которые могут быть внедрены в облачные вычисления:

- сертификация согласно международным стандартам информационной безопасности;
- разрешение доступа к “облакам” только из доверенных узлов;
- использование надежных паролей;
- использование “fault domain”;
- использование VM для отдельных ресурсов.

ПЕРЕЧЕНЬ ИССПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Статья: “Безопасность облачных вычислений: есть вопросы?”/ Способ доступа: URL: http://cloudzone.ru/articles/analytics/11.html– Загол. з екрана.