УДК 004.056

Аспірант Комісар Д.О., студент Хмеловський М.Є.

**Національний технічний університет України
«Київський політехнічний інститут»**

МЕТОДИКА ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ДАНИХ КОРИСТУВАЧА В «ХМАРНИХ» ТЕХНОЛОГІЯХ

Abstract

Dmitriy A. Komisar, graduate student, Maksim Khmelovsky, student
Method of evaluation user data protection in-the-cloud technology

This article presents a methodology of estimating security of user data that are in the cloud. The possible threat and methods of protection were presented. The formula of the integral evaluation were composed.

Вступ

«Хмарні» обчислення стають все популярнішими. Постійно в соціальних мережах з'являються нові акаунти з особистою інформацією про користувача, його фотографії та іншими даними. Деякі прогресивні користувачі відкривають власні сховища і переносять всі дані з комп'ютера до серверів компаній постачальника послуги. Дехто вже не зберігає на комп'ютері жодних даних і використовує його тільки як засіб спілкування з «хмарами» де встановлена операційна система і зберігаються всі файли користувача. Це дуже зручно, але постає питання про безпеку такого використання.

Аналітики Kaspersky Lab вже проводили огляд даної проблеми[1].

Постановка задачі

Для визначення рівня захищеності даних в «хмарних» технологіях необхідно розробити методику оцінювання. Потрібно провести огляд можливих загроз та методів боротьби з ними.

Термінологія

«Хмарні» обчислення (cloud computing) - технологія розподіленої обробки даних, в якій комп'ютерні ресурси і потужності надаються користувачеві як Інтернет-сервіс.

Існує три класи «хмарних» обчислень: програмне забезпечення як сервіс, платформа як сервіс, інфраструктура як сервіс.

Програмне забезпечення як сервіс (software as a service, скор. SaaS) - бізнес-модель продажу і використання програмного забезпечення, при якій постачальник розробляє веб-додаток і самостійно керує ним, надаючи замовникам доступ до програмного забезпечення через Інтернет.

Платформа як сервіс (platform as a service, скор. PaaS) - це надання інтегрованої платформи як Інтернет-сервісу для розробки, тестування, розгортання та підтримки програмного забезпечення як послуги.

Інфраструктура як сервіс (infrastructure as a service, скор. IaaS) - це надання комп'ютерної інфраструктури (як правило у формі віртуалізації) як послуги для розгортки платформи необхідної при вирішенні поставленої задачі.

Гіпервізор – програмний або апаратний комплекс, що забезпечує паралельне функціонування кількох або навіть багатьох операційних систем на одному сервері.

Можливі атаки

Розглянемо можливі атаки які загрожують «хмарним» сервісам і користувачам даних сервісів. Їх можна розділити на такі рівні:

1)*Атаки клієнтської складової.* Оскільки в більшості випадків користувач послуги в якості клієнта використовує браузер, то всі загрози, які існують в мережі Інтернет, справедливі й для «хмарних» клієнтів. До цього типу атак можна віднести перехоплення веб-сесії, підключення до каналу зв’язку, крадіжку паролів чи Cross Site Scripting (XSS).[2]

2)*Атаки на програмне забезпечення.* Такі атаки пов’язані з вразливими місцями в операційних системах, додатках та в мережевих протоколах.

3)*Функціональні атаки на елементи «хмари».* Прикладом такої атаки може бути DoS атака на зворотний проксі. Якщо атака буде успішною, то доступу до «хмари» не буде, але роботоспроможність системи не буде порушено. Також як атаку можна враховувати SQL-ін’єкцію, при виконані якої можна відкрити повний доступ до бази данних.

4)*Загрози віртуалізації.* Вся система «хмарних» технологій будується на засобах віртуалізації. Можна виділити такі види атак:

- *Атаки на гіпервізор*. Втручання в роботу гіпервізора може призвести до неправильного розподілу ресурсів, будь-яка з віртуальних машин зможе перехоплювати трафік іншої машини, змінювати кількість ресурсів які виділяються для

роботи віртуальної машини, або повністю вимкнути віртуальні машини.

- *Атаки на системи управління*. У публічних «хмарах» існує значна кількість віртуальних машин, постійно створюються нові,змінюються та утилізуються невикористовувані за цим процесом слідкує система управління.
- *Перенесення віртуальної машини*. Оскільки віртуальна машина являє собою файл, який можна запускати в різних вузлах «хмари»,то є загроза її викрадення. Тобто, є можливість запуску віртуальної машини за межами хмари і отримання даних користувача.[3]

Методи боротьби

Для вирішення проблем з атаками можна запропонувати такі методи захисту по кожному із попередніх пунктів:

Клієнтську частину, програмне забезпечення(SaaS, Paas) та кожен із елементів «хмари» можна захистити використовуючи стандартні засоби, які використовуються при локальній реалізації. Також можна використовувати шифрований протокол https або встановити плагін до браузера і організовувати спілкування з сервером по спеціальному виділеному каналу зв'язку.[4]

Загрози, що стосуються віртуалізації мають певні складнощі, оскільки це новий тип загроз. Але це найнебезпечніша загроза «хмарам». Отже, засоби захисту «хмари» необхідно враховувати ще на етапі проектуванні системи. Для цього пропонується зберігати віртуальні машини не єдиним файлом, а розбивати на декілька файлів. Кожну частину потрібну шифрувати окремим методом і використовувати хеш файлів як ключ для запуску.

Методика оцінювання

Для оцінки захищеності даних у «хмарах» пропонується використовувати такі критерії:

$Attack_i$ - коефіцієнт, який може набувати значення 1 або 0 залежно від того, чи була успішною атака *i*-го рівня.

$\Pr otection_i$ - коефіцієнт, який відповідає якості захисту від атак *i*-го рівня. Коефіцієнт обирається аналітиком залежно від якості захисту.

$Cloud(x)$ - коефіцієнт, що обирається при успішній атаці на шари «хмари». Коефіцієнт обирається аналітиком залежно від того, наскільки важливим був сервіс, який відмовив при успішній атаці.

$$Cloud(IaaS) > Cloud(PaaS) > Cloud(SaaS)$$

Загальна формула підрахунку оцінки захищеності даних у «хмарних» технологіях має такий вигляд:

$$F = \sum_i (\Pr otection_i - Attack_i * Cloud(x))$$

Висновки

Представлена методика оцінки захищеності даних користувача в «хмарних» технологіях дає змогу аналітикам, які тестують «хмари» виставити оцінку для будь-якого сервісу. Постачальник послуги «хмарних» сервісів може надавати об'єктивні результати оцінювання і користувач зможе обирати найбільш захищені ресурси для зберігання даних, розробки додатків чи виконання інших задач.

Література

1. Ясное небо до самого горизонта: «облачные» вычисления и безопасность «из облака» Магнус Калькуль [електронний ресурс http://www.securelist.com/ru/analysis/204007652/Yasnoe_nebo_do_samogo_gorizonta_oblachnye_vychisleniya_i_bezopasnost_iz_oblaka], дату візиту 10.03.2011
2. *Daniel Bilar*. Callgraph properties of executables. – 2007. – P. 156-185.
3. *Daniel Bilar*. FINGERPRINTING MALICIOUS CODE THROUGH STATISTICAL OPCODE ANALYSIS. – 2007. – P. 317-385.
4. *Felix Leder*. Classification and Detection of Metamorphic Malware using Value Set Analysis. – 2009. – P. 245-253.