

Ризики інформаційної безпеки в хмарних сервісах

Денис Нікішин, Олександр Федюшин

Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, УКРАЇНА,
м. Харків, пр. Науки, 14,
E-mail: mus1kdamage@gmail.com,
oleksandr.fediushyn@nure.ua

Коротка аномалія – Models and methods of expert audit of information security in the cloud computing system are described. The purpose of the work is to increase the speed of response to incidents of information security breaches in the cloud services provision system by conducting an operational audit.

Ключові слова – Аудит інформаційної безпеки, хмарні послуги, хмарні технології, архітектура хмарних обчислень.

I. Вступ

На сьогоднішній день в індустрії інформаційних сервісів спостерігається стрімкий розвиток інформаційних систем, побудованих на основі хмарних технологій (ІСХТ).

У зв'язку з тим, що, найчастіше, компанії-споживачі хмарних послуг обробляють в хмарних середовищах критичні для них інформаційні активи, питання забезпечення інформаційної безпеки ІСХТ стає найбільш актуальним для споживача хмарних послуг.

Хоча постачальники, обслуговуючи підприємства з оборотом в мільярди доларів, роблять все можливе для забезпечення максимальної безпеки середини хмари, особливості побудови хмарної інфраструктури, використання технології віртуалізації і пов'язана з нею можливість порушення ізоляції віртуальних машин, а також паралельна обробка великих обсягів даних різних споживачів хмарних послуг, дозволяють говорити про нові потенційно можливі загрози інформаційної безпеки (ІБ), які будуть специфічними для хмари, обчислень.

II. Актуальність проблеми

Об'єктивна оцінка ступеня захищеності даних споживача хмарних послуг в хмарній інфраструктурі постачальника здійснюється в ході проведення аудиту інформаційної безпеки. В результаті аудиту інформаційної безпеки ІСХТ можна виявити, наскільки раціонально вирішені питання безпеки інформації та контролю доступу в хмарному середовищі, визначити, як мінімізувати ризики при обробці в ІСХТ конфіденційної інформації споживача хмарних послуг, локалізувати слабкі місця в системі забезпечення інформаційної безпеки і сформулювати рекомендації щодо шляхів вирішення існуючих проблем безпеки в системі. Крім того, споживач зацікавлений у визначенні постачальником конкретного об'єктивного механізму для оцінки якості пропонованої хмарної послуги.

Разом з тим, для забезпечення збереження конфіденційної інформації, що обробляється в хмарному середовищі, існуюча система забезпечення інформаційної безпеки ІСХТ повинна періодично піддаватися незалежному аудиту, який відповідно до вимог міжнародних стандартів, є одним з обов'язкових етапів життєвого циклу будь-якої інформаційної системи.

III. Аналіз проблеми

Багато експертів застерігають від надмірної довіри до заяв постачальників про безпеку хмарних обчислень [1], так як широко поширена думка, що споживач хмарних послуг має той рівень захищеності у хмарному середовищі, який забезпечується постачальником.

У США асоціація Cloud Security Alliance випустила Cloud Controls Matrix. Цей документ являє собою перелік існуючих технологій інформаційної безпеки, які можуть бути використані в хмарних сервісах. Хоча деякі фахівці вважають, що для управління ІБ при побудові хмари SaaS можуть бути використані стандарти ISO 27001 та ISO 27002, все ж необхідна розробка спеціальних стандартів для хмарних обчислень.

Для хмарних середовищ загрози віддаленого злому і зараження шкідливим кодом дуже значимі із-за паралельного існування безлічі віртуальних машин. Відмінною особливістю віртуальної машини, яку потрібно враховувати, є можливість її зараження у вимкненому стані [1], якщо є доступ до сховища образів віртуальних машин через мережу Інтернет. Тому особлива увага повинна бути приділена приватним політикам безпеки, особливо політикам розмежування доступу, інформаційних систем, побудованих на основі технологій хмарних обчислень.

Також варто відзначити, що спеціалізовані засоби забезпечення інформаційної безпеки, які застосовуються у сучасних інформаційних системах, знижують ефективність і швидкість обробки інформації клієнта у хмарі, а хмарні продукти безпеки, що допомагають подолати цю проблему, в даний час в нашій країні не сертифіковані.

Інформаційна безпека повинна забезпечуватися на всьому ланцюжку, включаючи постачальника хмарного рішення, споживача та пов'язуючі їх комунікації [2]. Споживач хмарних послуг зобов'язаний вводити до своєї системи відповідну політику безпеки, яка виключає передачу прав доступу до інформації, наданої постачальником, третім особам. Хмари не скасовують необхідність розробки і впровадження політики безпеки у сегменті споживача і використання сервісів безпеки, покликаних гарантувати захист призначених для користувача робочих місць на стороні споживача хмарних послуг.

IV. Розв'язання проблеми

При побудові системи забезпечення інформаційної безпеки системи хмарних обчислень (СХМО) необхідно брати до уваги загрози порушення інформаційної безпеки конкретного об'єкта захисту. В даній роботі складено перелік загроз в системі хмарних обчислень (СХМО) на основі моделі надання послуг SaaS.

1. Загрози безпеки інформації для споживача хмарних послуг:

- загрози безпеки інформації, пов'язані з невизначеністю відповідальності. Дані загрози з'являються у зв'язку з відсутністю чіткого поділу відповідальності в частині забезпечення інформаційної безпеки між споживачем і постачальником послуг SaaS, що є причиною невиконання деяких заходів щодо захисту інформації;
- загрози безпеки інформації, пов'язані з втратою управління. Використання хмарних послуг має на увазі передачу споживачем хмарних послуг частини функцій управління своєю інформаційною системою постачальнику хмарних послуг. Це призводить до того, що постачальник хмарних послуг може задати параметри інформаційної системи споживача хмарних послуг у відповідності зі сформованою у нього практикою;
- загрози безпеки інформації, пов'язані з втратою довіри. У загальному випадку користувачі хмарних послуг не можуть достовірно оцінити рівень довіри до постачальника хмарних послуг, в зв'язку із закритістю для користувачів застосовуваних постачальником хмарних технологій і програмних рішень. Невідомі еталонні значення будь-яких параметрів, які треба забезпечити постачальнику і користувачеві хмарних послуг для досягнення певного рівня безпеки. Крім того, користувачі хмарних послуг не мають можливість дати оцінку реалізованого рівня захищеності інформації, досягнутого постачальником;
- загрози безпеки інформації, пов'язані з здійсненням несанкціонованого доступу (НСД) з боку споживачів хмарних послуг. Так як хмарні ресурси надаються віддалено, то на хмарний сервер можуть бути проведені атаки, пов'язані з уразливими мережі споживача хмарних послуг;
- загрози безпеки інформації, пов'язані з недоліком управління хмарними ресурсами. Дана загроза зумовлена складністю визначення логічного і фізичного місця розташування хмарних ресурсів, недостатністю фізичного контролю доступу до сховищ даних, надійністю резервного копіювання та ін. Крім того, існують загрози споживачам хмарних послуг, пов'язані з передачею інформації, що захищається постачальникам хмарних послуг, які є резидентами інших країн зі своїми особливостями законодавства в області захисту інформації;
- загрози, пов'язані зі зловживаннями з боку споживачів хмарних послуг. У зв'язку з тим, що споживач хмарних послуг може встановлювати власне ПЗ на хмарний сервер, то для досягнення своїх неправомірних цілей споживач хмарних послуг може

встановити шкідливе ПЗ, за допомогою якого здійснювати розсилку спаму, несанкціонованого доступу до віртуальних машин інших клієнтів.

2. Загрози безпеки інформації для постачальників хмарних послуг:

- загрози, пов'язані з невизначеністю при розподілі відповідальності. У хмарі можуть бути визначені такі ролі, як провайдер хмарних послуг, користувач хмарних послуг, адміністратор клієнтської інформаційної системи, власник інформації і т.д. Організація безпеки інформації від таких загроз ускладнена тим, що її реалізація здатна привести до істотних розбіжностей між постачальником і споживачем хмарних послуг з питань, пов'язаних з визначенням їх прав та обов'язків;
- загрози, пов'язані з неузгодженістю політик безпеки. Внаслідок децентралізованого характеру архітектури системи хмарних обчислень, у постачальника і споживача хмарних послуг можуть бути реалізовані різні політики безпеки для одних і тих же засобів захисту;
- загрози, пов'язані з використанням технологій віртуалізації. У більшості випадків основою для створення хмарної інфраструктури є технології віртуалізації. При цьому один фізичний сервер, його обчислювальні ресурси і ресурси пам'яті діляться між безліччю віртуальних машин.

Висновки

В результаті аналізу виявлено такі проблеми забезпечення інформаційної безпеки у хмарних середовищах:

- відсутність в Україні нормативно-правової бази, що регулює питання забезпечення інформаційної безпеки для хмарних обчислень;
- застосування засобів забезпечення інформаційної безпеки, які широко використовуються у сучасних інформаційних системах, знижує ефективність і швидкість обробки інформації замовника хмарних послуг у хмарній інфраструктурі, що зводить на «ні» майже всі переваги хмарних середовищ у порівнянні з традиційними інформаційними системами;
- існуюча система забезпечення інформаційної безпеки хмарного середовища повинна періодично піддаватися незалежному експертному аудиту, який відповідно до вимог міжнародних стандартів, є одним з обов'язкових етапів життєвого циклу будь-якої інформаційної системи.

Література

- [1] The NIST Definition of Cloud Computing (англ.). [Електронний ресурс]: Режим доступа: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>
- [2] Документ України щодо обробки інформації в системах хмарних обчислень [Електронний ресурс] - Режим доступа : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=58527