УДК 004.056

Дослідження загроз для віртуальної інфраструктури хмари та методи її захисту

Ладигіна О.А., асистент
Кіровоградський національний технічний університет, м. Кіровоград

На даний час дата-центри наступного покоління розмивають кордони між фізичними та віртуальними середовищами, між публічними і приватними хмарами, що призводить до розширення ряду питань щодо захисту інформації в хмарних обчисленнях і для вирішення яких потрібні постійно удосконалючі рішення [1].

Забезпечення фізичної безпеки лежить на основі суворого контролю фізичного доступу до серверів та мережевої інфраструктури. Мережева безпека заснована на побудові надійної моделі загроз, що враховує захист від вторгнень і міжмережевий екран, з метою розмежування внутрішніх мереж дата-центрів на підмережі з різним рівнем довіри.

У хмарних обчисленнях технологія віртуалізації відіграє особливу роль і полягає в:

- віртуалізації серверів - перенесення фізичних серверів у віртуальні машини однієї хостової системи, оснащеної гіпервізором - засобом віртуалізації;

- віртуалізації робочих користувальницьких місць - централізоване зберігання робочих місць у вигляді віртуальних машин на хостовій системі з наданням роздільного доступу по мережі з фізичних робочих місць;

- віртуалізації терміналів - для окремого користувача терміналу в операційній системі створюється власний сеанс роботи.

Концепція хмарних технологій полягає в наданні користувачам віддаленого динамічного доступу до послуг, обчислювальних ресурсів і додатків, включаючи операційні системи та інфраструктуру через різні канали доступу, в тому числі і через Інтернет. Така великомасштабна інфраструктура являє підвищені ризики і досить обмежену можливість контролю над її ресурсами. У цьому і полягає актуальність проблем хмарних обчислень - захист інформації та довірливе ставлення користувачів до хмарних провайдерів.

Застосування спеціалізованого програмного забезпечення для віртуального середовища вимагає значної зміни у підходах до забезпечення інформаційної безпеки хмарних систем [2].

Рішення задач забезпечення безпеки об'єднує в собі традиційні та специфічні рішення з особливостями, які в процесі виконання задач повинні оптимізовуватись для економії продуктивності віртуального середовища із забезпеченням захисту інформації і хмарних ресурсів.

Для забезпечення безпеки і збереження цілісності даних досліджуються актуальні загрози для віртуальної інфраструктури хмари [3, 4]:

- відсутність контролю внутрішньомережевого трафіку, а також можливість прослуховування всього трафіку між віртуальними машинами;

- єдине сховище віртуальних машин, над якими можна отримати несанкціонований контроль;

- захоплення всіх ресурсів хоста віртуалізації однією віртуальною машиною, в результаті якого інші віртуальні машини можуть викликати відмову в обслуговуванні;

- незахищеність вразливих місць дискової підсистеми віртуальних машин;

- компрометація клієнтських терміналів і атака на браузери клієнтів;

- несанкціонований доступ до ресурсів віртуалізації через гіпервізор з віртуального чи

реального середовища;

- перехоплення аутентифікаційних даних для доступу до хмари через хмарні API;
- несанкціонований доступ до консолі управління віртуальним середовищем;
- відсутність у віртуальній інфраструктурі розподілених комутаторів, які при міграції віртуальних машин дозволяють погоджувати політику безпеки;
- перехоплення даних при передачі по незахищених зовнішніх каналах зв'язку.

Одним з головних джерел загрози безпеки є сервер централізованого управління віртуальної інфраструктури, отримавши контроль над яким, зловмисник отримує повний доступ до всіх віртуальних машин, хостів віртуалізації, віртуальних мереж і сховищ даних.

Тому необхідно, в першу чергу, ретельно захищати сам сервер управління, звертати посилену увагу на засоби аутентифікації і розмежування прав доступу, для чого має сенс використовувати додаткове програмне забезпечення, що розроблене спеціально для віртуальних інфраструктур. Доступ до сервера віртуалізації повинен здійснюватися за безпечними протоколами, а доступ адміністраторів повинен бути обмежений за IP-адресами.

Важливо також, щоб мережі управління віртуальною інфраструктурою та виробничого середовища віртуальних машин були розділені логічно і фізично для запобігання несанкціонованого втручання.

При дослідженні загроз ще слід враховувати також специфіку обробки персональних даних у віртуальному середовищі [5, 6]:

- обробляються в рамках віртуальних машин;
- передаються між віртуальними машинами всередині віртуального середовища;
- передаються між віртуальним середовищем і зовнішніми середовищами, як реального, так і віртуального.

Для забезпечення захисту даних у хмарі, які розміщені за межами сфери фізичного доступу клієнта, здійснюють шифрування віртуальних жорстких дисків. При зчитуванні з диска дані розшифровуються і при записі на диск зашифровуються. При цьому ключі зберігаються на окремому сервері управління ключами, який спочатку перевіряє ідентифікаційні дані і цілісність хмарного сервера, який направив запит. У разі позитивного відгуку надається ключ і хмарний сервер отримує доступ до інформації, що зберігається і ресурсів хмари.

Більш потужний варіант безпеки даних являє собою комбінування технологій шифрування даних і захищеної передачі.

Для підвищення безпечного використання хмарних технологій доцільно використовувати системи виявлення вторгнень і міжмережевого екранування з контролем зовнішніх підключень до середовища віртуалізації за допомогою апаратних рішень, а внутрішніх - за допомогою програмних рішень, реалізуючи, таким чином, комбінований підхід.

Швидко виявити атаки зловмисника дозволяють журнальні записи, зроблені серверами хмари, які служать важливим джерелом інформації при проведенні інженерно-технічних експертиз. Тому збереження журнальних записів за весь термін служби хмарного сервера є важливою, необхідною мірою і дозволить здійснити подальший аналіз збору даних, їх об'єднання та виведення на зовнішні інструменти, платформу безпеки або на систему управління подіями інформаційної безпеки.

Наступними ефективними засобами захисту хмар є:

- довірене завантаження серверів віртуалізації, віртуальної машини, серверів управління віртуалізацією;
- сегментування віртуальної інфраструктури для обробки персональних даних користувачем або групою користувачів;
- ідентифікація та аутентифікація доступу та об'єктів доступу у віртуальній інфраструктурі, в тому числі адміністраторів управління засобами віртуалізації;
- управління доступом суб'єктів доступу до об'єктів доступу у віртуальній інфраструктурі, в тому числі всередині віртуальних машин;

- управління потоками інформації між компонентами віртуальної інфраструктури, а також по периметру віртуальної інфраструктури.

Для антивірусного захисту віртуальних машин краще використовувати безагентний підхід, що забезпечує комплексну безпеку без установки агентського модуля в захищаємій системі, тобто у віртуальне середовище впроваджується віртуальний пристрій - шлюз безпеки, який бере на себе функції антивіруса для всіх віртуальних машин.

Вірно підібрані рішення безпеки дозволяють отримати уявлення про рівень використовуваних ресурсів і своєчасно виявити атаки, які націлені на різні хмарні об'єкти.

Для зниження операційних витрат, пов'язаних із засобами захисту систем віртуалізації, рекомендується використовувати спеціально розроблене програмне забезпечення, що адаптоване для хмарних обчислень.

Але все ж ще залишаються проблеми адаптації захисту віртуалізації в хмарі, які вимагають подальшого аналізу і вдосконаленого рішення.

Список літератури:

1. Котяшичев И. А. Защита информации в «Облачных технологиях» как предмет национальной безопасности / И. А. Котяшичев, Е. А. Бырылова // Молодой ученый. — 2015. — №6.4. — С. 30-34.

2. Ладигіна О.А. Перспективи захисту інформації в хмарних обчисленнях від атак на засоби віртуалізації // Збірник тез доповідей науково-практичної конференції «Інформаційні технології та комп'ютерна інженерія».- Кіровоград: КНТУ, 2014. -164 с

3. Ширманов А. Безопасность виртуализации при обработке данных ограниченного доступа // Москва, ЭКСПОЦЕНТР, InfoSecurity Russia. 30 сентября 2009

4. Е. Кожемяка Обеспечение безопасности данных при использовании облачных технологий/ [Електронний ресурс]. – Режим доступу: http://www.lastmile.su/files/article_pdf/3/article_3823_334.pdf

5. Котяшичев И. А. К вопросу о безопасности облачных технологий в информационной среде/ И. А. Котяшичев, С. В. Смоленцев // Молодой ученый. — 2014. — №5.1. — С. 25-28.

6. Бойко А., Бердник А. Методы защиты виртуальной среды. Программный комплекс для проведения автоматизированного аудита виртуальной среды на предмет наличия ошибок в конфигурации безопасности/ [Електронний ресурс]. – Режим доступу: http://cyberleninka.ru/article/n/metody-zaschity-virtualnoy-sredy-programmnyy-kompleks-dlya-provedeniya-avtomatizirovannogo-audita-virtualnoy-sredy-na-predmet

УДК 004.75:378.147

Аналіз безпеки даних в хмарних сервісах

Ліщина Н.М., канд. техн. наук, доцент
Луцький національний технічний університет, м. Луцьк

Хмарні технології визначають як динамічно масштабований вільний спосіб доступу до зовнішніх обчислювальних інформаційних ресурсів у вигляді сервісів, що надаються за допомогою мережі Інтернет.

Хмарні технології дозволяють споживачам використовувати програми без установки і доступу до особистих файлів з будь-якого комп'ютера, що має доступ в Інтернет. Ця технологія дозволяє вести значно ефективніше управління підприємством за рахунок централізації управлінської та облікової інформації, обробки, пропускної здатності та надійності зберігання даних.

Головним стримуючим фактором при роботі з «хмарними» ресурсами є питання безпеки – відсутність контролю над серверами, обчислювальними процесами, можливість витоку критично важливої інформації. Серед інших стримуючих факторів можна відзначити сумніви в якості «хмарних» послуг, незначна кількість пропозицій, відсутність методик оцінки ефективності, неготовність змінювати підходи до IT-стратегій, неприйняття IT-