КЛАСИФІКАЦІЯ АТАК НА ХМАРНІ СИСТЕМИ

В. Ю. Шадхін[1α], В. О. Компанієць[2β], Д. Г. Дель[2γ]
[1] м. Черкаси, Черкаський державний технологічний університет
[2] м. Київ, Київський національний університет технологій та дизайну
[α] shadxin@mail.ru
[β] mail@slavka.net.ua
[γ] d.dell@gmail.com

За останні роки обчислювальні системи, що застосовуються в управлінні та виробництві, почали використовувати для вирішення більшої кількості задач. При цьому, швидкодії та продуктивності одного фізичного серверу у деяких випадках недостатньо. В таких ситуаціях створюються так звані «хмарні» сервери, що представляють собою один віртуальний сервер, який об'єднує в собі фізичні та логічні ресурси декількох фізичних серверів. Це дає змогу створити одну потужну віртуальну систему, для виконання більшої кількості задач.

Хмарні сервери перспективна та популярна технологія у наш час, яка також має ряд значних переваг, але це більш складна система, тому й в багатьох моментах більш вразлива у порівнянні з традиційними фізичними серверами.

Структура хмарної системи має свою певну ієрархію (рис. 1).

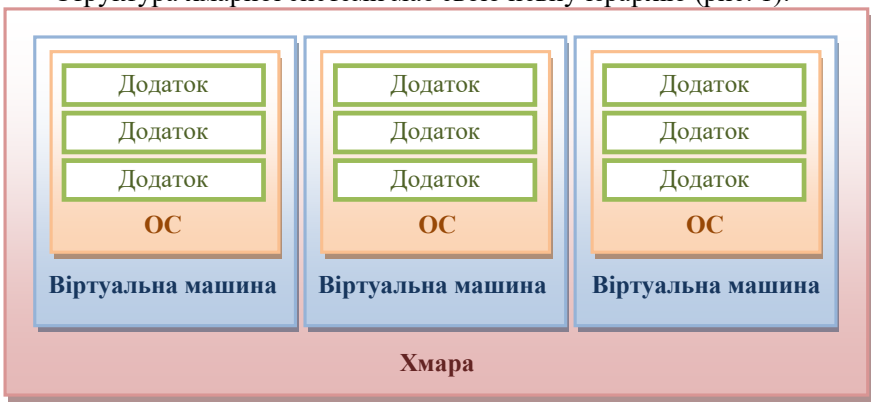

Рис. 1. Структура хмарної системи

Розглянемо вразливі місця та способи атаки на хмарний сервер:

1. Традиційна атака на програмне забезпечення

Даний тип атак спрямовано на вразливість встановленого у системі програмного забезпечення, як правило, пов'язані з мережевими протоколами, модулями ПЗ, компонентами і т.д.

2. Атака на окремий елемент хмари

Даний тип атак спрямовано на слабкі ланки хмари. Як приклад, звичайна DDoS-атака на один з віртуальних серверів хмари, може паралізувати роботу інших, в зв'язку з тим, що мережевий канал на фізичному рівні для усіх елементів – один.

3. Загрози віртуалізації

Такі атаки спрямовані на фізичний сервер та первинно встановлену на ньому операційну систему, отримавши доступ до якої, зловмисник може заволодіти усіма розміщеними на ньому віртуальними серверами, так як кожна система після віртуалізації не що інше, як звичайний файл з даними на жорсткому диску фізичної системи.

4. Комплексні атаки на системи управління хмарами

Такий тип атаки спрямований, як правило, на систему управління хмарами. Сам процес отримання контролю над ними може бути реалізовано будь-яким чином, від високорівневих атак до безпосередньо фізичного втручання.

5. Атаки на гіпервізор

Власне, ключовим елементом віртуальних систем є гіпервізор, котрий розподіляє ресурси фізичної системи між віртуальними. Втручання до цієї системи може викликати перехоплення змісту пам'яті або трафіку іншої віртуальної машини, чи навмисне викликати відмову однієї з віртуальних машин, лишивши її необхідних ресурсів. Але такі атаки дуже складні і дуже рідко зустрічаються.

Захистити хмару від більшості атак можливо тими засобами, що застосовуються й для звичайних фізичних систем – це фаєрволи, антивіруси, розмежування прав доступу, та комплексні програмні продукти для контролю поведінки ПЗ. Також багато питань вирішують спеціалізовані системи моніторингу периметру віртуальної мережі хмари, такі як VMware vShield, а також шифрування змісту дискової системи фізичного серверу.

Однак, не всім загрозам можливо запобігти. Наприклад, атаки на гіпервізор дуже важко попередити, цей напрям є перспективним для майбутніх досліджень.