Секція 1

ДОСЛІДЖЕННЯ ТА АНАЛІЗ IAC ПІДХОДУ ДЛЯ ПОБУДОВИ БЕЗПЕЧНОЇ ПРИВАТНОЇ ХМАРНОЇ ІНФРАСТРУКТУРИ

Лоцман Є. Р.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Цуранов М. В.

Актуальність. За результатами опитування USAID-Internews, популярність Інтернет технологій зросла на 30 відсотків за останні 5 років. Пікові показники зростання були зафіксовані під час всесвітньої пандемії вірусу Коронавірус [1]. Більшість населення планети зіткнулася з незвичними їй новими реаліями – зросла необхідність безконтактної оплати, з'явилися обмеження пересування та час перебування на вулиці, що призвело до зростання популярності онлайн сервісів.

Метою даної роботи є дослідження IAC подходу при побудові приватної хмарної інфраструктури.

В рамках проведеної роботи було проаналізовано підхід побудови інфраструктури на віртуальних серверах. До роботи було виділено визначення віртуалізації. Віртуалізація – це технологія, яка створює віртуальне представлення декількох комп'ютерів або серверів на апаратній базі одного фізичного комп'ютера, або кластера серверів. Ця апаратна база називається хостом; котрий має центральний процесор, оперативну пам'ять, накопичувальний простір та інше. Місткість фізичних ресурсів, диверсифікована гіпервізором, який забезпечує незалежність віртуальних машин одна від одної [2].

Основні положення. Документація сервісів та інформація про надійність та безпеку даних в рамках публічної хмари, яку публікують хмарні провайдери більше нагадують рекламні постери. Опублікована інформація може бути недостовірною та не дає змогу оцінити весь спектор вразливостей, загроз та надійність публічної хмари. Закрита політика хмарних провайдерів, стосовно питанньь інфраструктури та безпеки даних, демонструє обмеженність можливостей аналізу безпеки публічних хмар в порівнянні з приватними хмарами. За угодою з хмарним провайдером, клієнт має змогу запросити своїх експертів з інформаційної безпеки і провести часткове тестування системи для

оцінки її на предмет взразливостей та можливих загроз безпеки. Часткове тестування не дозволяє виявити всі можливі загрози і вразливості. Провайдер не може надати повний доступ до фізичних ресурсів, так як це приведе до компрометації даних інших користувачів хмари. Так як концепт публічної хмари передбачає використання фізичних ресурсів хмари одразу двома та більше клієнтами.

Безперервне зростання попиту на хмарні послуги потребує великих людських ресурсів для адміністрування та супроводу інфраструктури. Для спрощення адміністрування та масштабування було розроблено новий підхід до побудови інфраструктури – інфраструктура як код [3].

Висновки. В ході аналізу було виявлено, що IaC-обробка забезпечує більший контроль та прозорість, ніж адміністрування систем вручну. Файли конфігурації інфраструктури передаються до центрального репозиторію з контролем версій, де будь-який учасник команди може переглядати та редагувати дані інфраструктури. Це дозволяє проводити ефективний аудит. Наприклад, якщо команда проходить аудит відповідності стандартам безпеки PCI, та потрібно буде знати, чи використовується у відповідній частині інфраструктури шифрування SSL. За допомогою IaC-обробки можна швидко побачити налаштування SSL і виконати код, щоб переконатися, що інфраструктура, що діє, відповідає файлам конфігурації, що визначають використання SSL. Історія коммітів у системі контролю версій також є журналом з відомостями про час додавання або видалення налаштувань.

Список літератури

1. Лоцман Є. Р. Методи деанонимізації як засіб виявлення правопорушників. Протидія кіберзагрозам та торгівлі людьми: тези доп., м. Харків, 26 листоп. 2019 р. ХНУВС, 2019. С. 259 – 261;

2. Лоцман Є. Р., Цуранов М.В., Аналіз методів побудови приватної хмари. Проблеми інформатизації: тези доп., м. Харків, 26-27 листопада. 2020 р. ХПІ, 2020. С. 74;

3. Лоцман Є. Р., Цуранов М.В., Аналіз механізмів забезпечення кібербезпеки методології DevOps. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези доп., м. Харків, 9-10 квітня. 2020 р. ХПІ, 2020. С. 59.

Відомості про авторів

Лоцман Євгеній Романович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 097-546-49-43, e.lotsman@student.csn.khai.edu
Цуранов Михайло Віталійович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, m.tsuranov@csn.khai.edu