Нетребяк М.Р., здобувач
Возняк С.І., викладач
Західноукраїнський національний університет

БЕЗПЕКА КОНТЕЙНЕРИЗАЦІЇ DOCKER

Контейнеризація на сьогодні є важливим етапом у створенні та користуванні сучасними інформаційними технологіями, яка дає змогу створювати невеликі і численні ізольовані середовища для додатків з залежностями різних версій, без впливу на основну систему. Цей підхід значно підвищив ефективність розроблення, розгортання та тестування програмного продукту, адже контейнери забезпечують зручніше адміністрування систем та налаштуванням мережі між ними, ізоляцію процесів та значно ефективніше використовують ресурси, ніж традиційна віртуалізація. Однак до появи Docker контейнеризація залишалася відносно складним і повільним процесом. Docker-образи зробили революцію в розробці та розгортанні програмного забезпечення і стали стандартом для контейнеризації, а забезпечення їх безпеки має вирішальне значення для захисту програм та даних [1].

Зараз віртуалізація стала фундаментальною технологією для оптимізації роботи серверів, спрощення процесів розробки та розгортання додатків. Проте, водночас з перевагами контейнеризації почали зростати і виклики та способи проникнення, пов'язані із безпекою контейнерів. Незважаючи на ізольоване середовище, контейнери продовжують бути вразливими до кібератак та комп'ютерних інцидентів, якщо не дотримуватися належних заходів безпеки та їх експлуатації. Тому питання безпеки контейнерів є важливим у роботі з контейнеризацією і її необхідно враховувати при їх розгортанні у робочому середовищі. Існує досить багато рішень для забезпечення надійності і безпеки образів та контейнерів. Використання таких інструментів, як Clair, Trivy або Docker Scout, має вирішальне значення для виявлення та усунення потенційних вразливостей у образах Docker [2].

1) Clair - це інструмент з відкритим вихідним кодом призначений для аналізу вразливостей образів контейнерів, що сканує образи на наявність відомих вразливостей у програмних пакетах та бібліотеках.

2) Trivy - ще один потужний сканер вразливостей з відкритим вихідним кодом, створений спеціально для контейнерів. Він високоефективний і надає швидкі результати сканування, який перевіряє уразливості в образі, й шукає проблеми в бібліотеках.

3) Docker Scout аналізує вміст образу і створює детальний звіт про виявлені помилки у конфігураціях та вразливості. Він може надати рекомендації щодо усунення проблем, виявлених під час аналізу образу.

Методи сканування Docker-образів на предмет вразливостей застосовують різноманітні технології та алгоритми, але мають однакову мету – нівелювати потенційні проблеми та вразливості, що виникають при контейнеризації. Виділяють статичний та динамічний аналіз Docker-образів. Статичний здійснює аналіз даних перевіряючи відомі бази та порівнюючи компоненти образу з даними в них. Натомість динамічний симулює виконання образу та виявляє потенційні вразливості шляхом перехоплення взаємодії із системою.

Іншим, критично важливим заходом безпеки є використання образів лише від офіційних розробників, що значно підвищує ймовірність, що вони не були підроблені перед розгортанням. В свою чергу використання Docker-образів від неофіційних розробників потребує додаткової перевірки на вразливості. Це зумовлено тим, що неофіційні розробники зазвичай недооцінюють важливість безпеки та не мають достатньо досвіду для захисту конфіденційних даних. Тому, деякі компанію забороняють використання Docker-образів від неофіційних розробників, оскільки вони не надають достатнього рівня безпеки та надійності для їх IT-інфраструктури.

Ще одним поширеним методом захисту при використанні Docker-образів від неофіційних розробників є одночасне застосування декількох інструментів для виявлення та усунення потенційних вразливостей. Їх поєднання дає змогу різносторонньо проаналізувати запропоновані образи та підвищити точність і повноту перевірки, що сприяє виявленню більшої кількості потенційних проблем.

Список використаних джерел:

1. Acharya J.N., Suthar A.C. Docker Container Orchestration Management: A Review. In: Sharma H., Vyas V.K., Pandey R.K., Prasad M. (eds) Proceedings of the International Conference on Intelligent Vision and Computing (ICIVC 2021). ICIVC 2021. Proceedings in Adaptation, Learning and Optimization, vol 15. Springer, Cham, 2022.
2. Дарієнко Д.Г., Когут Н.М. Методи сканування образу Docker контейнерів на предмет вразливостей безпеки. Computer systems and networks, Vol. 6, No. 2, pp. 35-44, 2024.