Мурсалов В. Р., магістрант
Головня О. С., к.пед.н., доц.
Державний університет «Житомирська політехніка»

ПІДВИЩЕННЯ БЕЗПЕКИ КОНТЕЙНЕРИЗОВАНИХ ДОДАТКІВ НА БАЗІ DOCKER

Docker — це один з найпопулярніших інструментів для контейнеризації, який дозволяє запускати додатки в ізольованих середовищах. Контейнери широко використовуються для розгортання мікросервісів та інших архітектурних рішень. Однак, ізоляція процесів у Docker має свої обмеження, що створює потенційні ризики для безпеки контейнеризованих додатків.

Актуальність дослідження зумовлена необхідністю виявлення вразливостей контейнерів та розробки ефективних методів для їхнього усунення.

Метою дослідження є проаналізувати ключові аспекти безпеки контейнеризованих додатків на базі Docker і надати рекомендації щодо зменшення ризиків кіберзагроз для контейнеризованих середовищ.

Методом дослідження застосовано аналітичний метод.

Основні результати

Один із ключових принципів безпеки Docker – запуск контейнерів із найменшими необхідними привілеями. Рекомендується уникати запуску контейнерів від імені root-користувача та замість цього налаштовувати менш привілейованих користувачів. Це значно знижує ризики компрометації системи.

Використання Docker Daemon потребує забезпечення відповідного контролю доступу. Оскільки Daemon працює з високими привілеями, важливо обмежити доступ до нього за допомогою аутентифікації та шифрування з'єднань, що можна реалізувати через TLS. Це запобігає можливим атакам шляхом несанкціонованого підключення до Daemon [2].

Базові образи контейнерів повинні завантажуватися з перевірених джерел, таких як офіційний Docker Hub, і регулярно оновлюватися для зниження ризику, пов'язаного з використанням застарілих компонентів. Це допомагає уникати багатьох поширених вразливостей.

Docker підтримує можливість обмежувати використання ресурсів контейнерами за допомогою контрольних груп (cgroups) [1]. Встановлення обмежень на CPU, пам'ять та I/O для кожного контейнера дозволяє захистити систему від перевантажень та запобігає можливості атак шляхом виснаження ресурсів.

Контейнери мають бути ізольовані один від одного і від зовнішньої мережі, щоб запобігти міжмережевим атакам. Використання окремих віртуальних мереж Docker і конфігурація мережевого фаєрволу для кожного контейнера підвищує рівень безпеки, захищаючи контейнери від несанкціонованих з'єднань.

Регулярне сканування контейнерів на наявність уразливостей є обов'язковою практикою для підтримки безпеки. Інструменти, такі як Trivy або Clair, дозволяють виявляти відомі вразливості в образах Docker, що знижує ризик експлуатації зловмисниками [2].

Для виявлення та швидкого реагування на підозрілі активності у контейнерах критично важливим є налаштування логування та моніторингу дій у контейнеризованому середовищі. Логи забезпечують доказову базу для аналізу інцидентів безпеки та можуть допомогти виявити спроби несанкціонованого доступу або інші загрози.

Використання шифрування для зберігання конфіденційних даних та змінних середовища в контейнерах захищає дані від витоку [2]. OWASP рекомендує уникати розміщення секретних даних у контейнерах, а замість цього зберігати їх у захищених сховищах, наприклад, Docker Secrets.

Результати дослідження свідчать про необхідність впровадження низки заходів для підвищення рівня безпеки контейнеризованих додатків на базі Docker. Дотримання зазначених рекомендацій сприяє зменшенню ризиків, пов’язаних із потенційними вразливостями контейнерів. Подальші дослідження можуть бути спрямовані на вдосконалення автоматизованих засобів перевірки та захисту контейнеризованих додатків.

Список використанх джерел

1. Security. (б. д.). Docker Documentation. URL: https://docs.docker.com/engine/ security/
2. Docker Security - OWASP Cheat Sheet Series. (б. д.). Introduction - OWASP Cheat Sheet Series. URL: https://cheatsheetseries.owasp.org/cheatsheets /Docker_Security_Cheat_Sheet.html