УДК 004.056.53

БЕЗПЕКА ПРОГРАМНИХ СИСТЕМ НА БАЗІ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ

Шевчук Р.П.[1)], Тихий Р.Р.[2)]
Західноукраїнський національний університет
[1)]к.т.н., доцент, [2)]магістрант

I. Вступ

Архітектурою можна вважати набір певних структурних компонентів зв'язаних між собою, які задають поведінку всієї системи [1,2]. Програмні системи на базі мікросервісної архітектури спроектовані як набір незалежних розгорнутих невеликих сервісів, кожен з яких запускає унікальний процес і забезпечує комунікацію за допомогою чітко визначеного механізму [3]. Підхід проектування програмних систем як сукупності мікросервісів забезпечує масштабованість системи та дає можливість розподілити додаток на декількох фізичних та віртуальних машинах, що також забезпечує більшу надійність. Завдяки гнучкості і масштабованості ці архітектурні рішення найкраще підходять, коли необхідна підтримка великої кількості різнотипних платформ у конвергентній мережній інфраструктурі. Разом з цим збільшення кількості мікросервісів прямо пропорційно ускладнює завдання захищеності та складності керування програмною системою.

II. Мета роботи

Метою дослідження є аналіз основних проблем та підходів до захисту програмних систем на базі мікросервісної архітектури.

III. Загрози для програмних систем на базі мікросервісної архітектури

Програмні системи на базі мікросервісної архітектури, як правило характеризуються розмежувальною політикою доступу до ресурсів, великим об'ємом мережевого трафіку, наявністю різнотипних сторонніх засобів конфігурації та керування, що створює велику поверхнею атаки для зловмисників.

Через велику кількість API, портів та програмних компонентів, які використовуються мікросервісами, традиційні брандмауери не можуть забезпечити належної безпеки, що робить розгортання мікросервісів вразливими до різних загроз, таких як man-in the middle, injection attacks, cross-site scripting, DDoS та інших.

Безпека мережі це ще одна проблема, пов'язана з використанням мікросервісної архітектури [4]. Зокрема, незахищений програмний код, ідентифікація та контроль доступу набувають нового рівня складності.

Тому для ефективного захисту програмних систем на базі мікросервісних архітектур необхідно створювати хорошу стратегію захисту дотримуючись найкращих практик, звертаючи увагу на:

- захист мікросервісів та користувачів;
- забезпечення ідентифікації та управління доступом;
- захист даних;
- покращення безпеки зв'язку між послугами;
- моніторинг мікросервісів та систем безпеки.

Висновок

У даній роботі проведено аналіз основних проблем та підходів до захисту програмних систем на базі мікросервісної архітектури.

Список використаних джерел

1. Фаулер М. Архитектура корпоративных программных приложений / М. Фаулер. – М.: Издательский дом Вильямс, 2006 – 544 с.
2. Шевчук Р.П. Підвищення ефективності клієнт-серверних систем середньої складності / Р.П. Шевчук., А.І. Яцинич // Вісник Тернопільського державного технічного університету. —2010. —Том 15. —No 1. —С. 182—186
3. Ньюмен С. Создание микросервисов / Ньюмен С. – СПб.: Питер, 2016 – 304 с.
4. Комар М.П. Нейросетевой подход к обнаружению сетевых атак на компьютерные системы / М.П. Комар, И.О. Палий, Р.П. Шевчук, Т.Б. Федысив // Інформатика та математичні методи в моделюванні – 2011. – Том 1, №2. – С. 156-160.
5. Kasianchuk M., Yakymenko I., Ivasiev S., Shevchuk R., Tymoshenko L. The Method of Factorizing Multi-Digit Numbers Based on the Operation of Adding Odd Numbers. Proceedings of the conference «Advanced Computer Information Technology (ACIT 2018)» (Ceske Budejovice, Czech Republic). P. 232–235