УДК 004.

Б.В Черновол
О. П. Войтович

МОНІТОРИНГ САЙТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ДОСТУПНІСТЬ

Вінницький національний технічний університет

Анотація

Метою роботи є покращення кібербезпеки критичної інфраструктури держави за рахунок моніторингу списка сайтів з допомогою запропонованого мікросервіса на основі стеку протоколів TCP/IP. Вихідним результатом роботи такого мікросервісу є дані про стабільну роботу та доступність досліджуваного ресурсу.

Ключові слова: мікросервіси, протоколи TCP/IP, пінгування, моніторинг, критична інфраструктура.

Abstract

The aim of the work is to improve the cybersecurity of the critical infrastructure of the state by monitoring the list of sites using the proposed microservice based on the stack of TCP / IP protocols. The initial result of such a microservice is data on the stable operation and availability of the studied resource.

Keywords: microservices, TCP / IP protocols, pinging, monitoring, critical infrastructure.

Вступ

Моніторинг веб-сайтів - це процес тестування та реєстрації стану та продуктивності роботи одного або декількох веб-сайтів. Цей інструмент моніторингу забезпечує доступність веб-сайтів для всіх користувачів, а підприємства та організації використовуються для того, щоб час роботи, функціональність та ефективність веб-сайтів завжди відповідали стандартам[1].

Метою роботи в першу чергу є виявлення відхилень від нормального функціонування сайту критичної інфраструктури, а також інформування та сповіщення про збій роботи об’єкта.

Результати дослідження

Першим етапом, потрібно визначитись з переліком сайтів критичної інфраструктури, над якими необхідно здійснювати моніторинг [2]. Для цього, до об’єктів моніторингу періодично надсилаються спеціально сформовані пакети та ведеться аналіз отриманих відповідей, а також перевірка отриманих результатів з попереднім станом веб-сайту.

У випадку відхилення від нормального функціювання веб-сайту [3], наприклад при виявленні змін, оператору надається відповідне сповіщення про те, де та в який час виникла конфліктна ситуація.

Одними із аналогічних мікросервісів є SiteUptime, BasicState та Uptime Doctor [4].

Безкоштовний тариф SiteUptime передбачає перевірку 1 сайту на його доступність для відвідувачів. Моніторинг проводиться кожні 30 хвилин з восьми локацій. Оповіщення по електронній пошті відправляються, як тільки виявиться даунтайм.

Сервіс BasicState дозволяє контролювати необмежену кількість веб-сайтів з 15-хвилинними інтервалами. BasicState відправляє SMS або електронні листи, якщо відбувається збій в роботі сервера, мережі чи конфігурації DNS, або коли сервер перевантажений [5]. Ще однією можливістю є отримання звіти щодо аптайму з двотижневою історією по електронній пошті.

За допомогою Uptime Doctor можна контролювати лише 5 сайтів без плати за це, однак кожної хвилини. Сповіщення через SMS і по електронній пошті містять назву сайту чи сер-

вера, його поточний стан, дату і час даунтайму, і відповідне повідомлення про тип помилки. Додатковою можливістю є отримання миттєвих push-повідомлень на мобільний додаток Android або IOS.

На основі проведеного аналізу запропоновано структуру мікросервісу (рис.1).

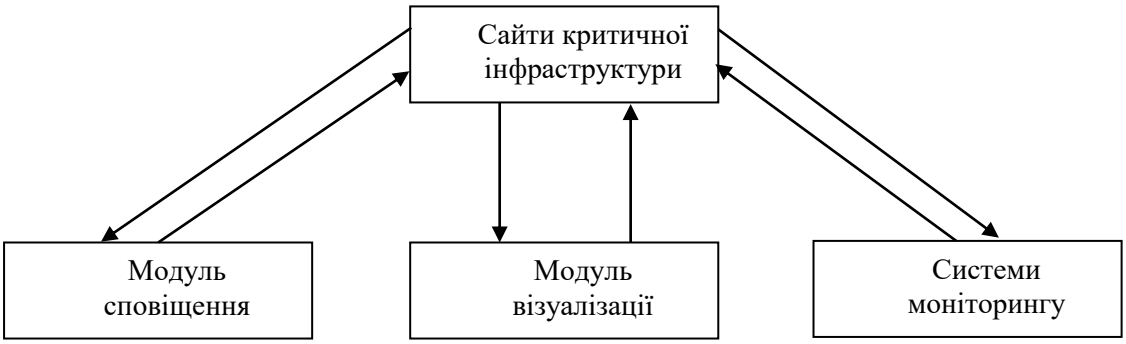

Рисунок 1. Структурна схема роботи мікросервіса.

Його основними перевагами є поєднання переваг існуючих систем, зокрема відслідковування роботи сайтів критичної інфраструктури в реальному часі і швидке реагування на збої, що виникають.

Висновки

Отже, запропонований додаток є відносно простим, проте важливим та дієвим у сфері моніторингу сайтів критичної інфраструктури. Також має значні переваги перед аналоговими сервісами.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Панов, І. *П’ять основних функцій систем моніторингу продуктивності мережі*. 2011. [Електронний ресурс] / Ігор Панов – Режим доступу до ресурсу: *https://networkguru.ru/piat-cliuchevykh-funktcii-sistem-monitoringaproizvoditelnosti-seti/.*
2. *Cecil, A.* A Summary of Network Traffic Monitoring and Analysis Techniques [Електронний ресурс] / Alisha Cecil – Режим доступу до ресурсу: *http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring/index.html.*
3. Wong E. Network Monitoring Fundamentals and Standards [Електронний ресурс] / Edmund Wong – Режим доступу до ресурсу: https://www.cse.wustl.edu/~jain/cis788-97/ftp/net_monitoring.pdf
4. Сервіси моніторингу аптайму серверра [Електроний ресурс] – Режим достпуту до ресурсу: https://internetdevels.ua/blog/free-uptime-monitoring-services
5. Засоби моніторингу та аналізу мережі [Електронний ресурс] – Режим доступу до ресурсу: https://wiki.cuspu.edu.ua/index.php/Засоби_моніторингу_та_аналізу_мережі.

Черновол Борис Віталійович — студент групи 2бс-18б, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: boryacernovol@gmail.com

Войтович Олеся Петрівна — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет

Науковий керівник: ***Войтович Олеся Петрівна*** — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Chernovol Borys V. — Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : boryacernovol@gmail.com

Voitovych Olesia P. — Cand. Sc. (Eng), Assistant Professor of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia