УДК 004.056.5
М. Приймаченко; Т. Лечаченко, доктор філософії
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ МЕТОДІВ ВИЯВЛЕННЯ АНОМАЛІЙ У ВЕБТРАФІКУ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНОЇ СИСТЕМИ АНАЛІЗУ ЛОГ-ДАНИХ

UDC 004.056.5
M. Priymachenko; T. Lechachenko, PhD.

RESEARCH OF METHODS FOR DETECTING ANOMALIES IN WEB TRAFFIC USING A LOG DATA ANALYSIS INFORMATION SYSTEM

Вебтрафік є ключовим джерелом даних для оцінювання стану безпеки інформаційних систем, оскільки саме через вебінтерфейси найчастіше здійснюються атаки, такі як SQL Injection, XSS, brute-force, directory traversal, сканування портів та спроби обходу автентифікації. Тому побудова ефективної системи аналізу логів, що дозволяє оперативно виявляти аномалії, є одним із пріоритетних напрямів кібербезпеки.

У дослідженні розглянуто можливість застосування стеку ELK (Elasticsearch, Logstash, Kibana) для збору, обробки, зберігання й аналітики лог-даних вебсерверів. Logstash або Filebeat забезпечують отримання, нормалізацію та парсинг логів у реальному часі, формуючи уніфіковану структуру записів. Elasticsearch використовується як високопродуктивне сховище та платформа для індексації й пошуку багатовимірних характеристик вебтрафіку. Kibana слугує інструментом візуалізації, моніторингу та дослідження аномальних патернів.

Розроблена інформаційна система дозволяє аналізувати динаміку HTTP-запитів, визначати перевищення порогових значень за кількістю помилок 4xx/5xx, відстежувати підозрілу частоту звернень з одного IP, визначати нетипові User-Agent, а також здійснювати геоаналіз активності. Особливу увагу приділено можливості застосування Machine Learning jobs у Kibana (Anomaly Detection), які використовують алгоритм Elastic ML для автоматичного виявлення нетипових відхилень у часових рядах.

Експериментальні результати показали, що спільне використання алгоритмів машинного навчання та інструментів Kibana дозволяє виявляти приховані аномалії, зокрема «повільні» сканування вебресурсів, спроби підбору логінів, а також сплески бот-активності. Візуальні панелі (dashboards) значно спрощують моніторинг, забезпечуючи швидке реагування на потенційні загрози.

Розроблена система може бути інтегрована у процес адміністрування, а також використана як компонент SIEM-платформи, підвищуючи рівень безпеки вебресурсів шляхом своєчасного виявлення аномальної поведінки користувачів та ботів.

Література

1. O’Malley M. Elasticsearch: The Definitive Guide. O’Reilly, 2022.
2. Sokolov A. Log analysis and anomaly detection using ELK Stack // Cybersecurity Review, 2023.
3. Aggarwal C. Outlier Analysis. Springer, 2017.