УДК 004.056.53

МОДЕЛИРОВАНИЕ И АНАЛИЗ ЦЕПОЧЕК АТАК В ГИБРИДНЫХ KUBERNETES-СИСТЕМАХ

Сумароков С. С.[1]
Научный руководитель – канд. физ.-мат. наук, доцент Комаров И. И.[1]
[1]Университет ИТМО
sumarokovsergei@yandex.ru

Введение

Современные информационные инфраструктуры, построенные на базе контейнерных приложений и управляемые оркестратором Kubernetes, все чаще разворачиваются в гибридных конфигурациях, обеспечивающих лучшую масштабируемость и гибкость эксплуатации [1]. Вместе с тем усложнение архитектуры взаимодействия компонентов, а также наличие нескольких контуров управления и политик доступа приводят к расширению поверхности атаки, особенно на границах взаимодействия систем. Отраслевые исследования фиксируют значительное количество уязвимостей, связанных с контейнеризацией и оркестрацией, и подчеркивают необходимость строгого применения политик и регулярного аудита [2].

Переход от локального анализа уязвимостей к системной оценке инфраструктуры ставит научную проблему разработки метода защищенности гибридной инфраструктуры с учетом связанности ее элементов.

Основная часть

Предлагается метод формализованного моделирования гибридной Kubernetes-инфраструктуры в виде графа компонентов, обогащенного данными безопасности, и производного графа атак с последующим анализом цепочек атак и ранжированием узлов по критичности. Подход обеспечивает не только выявление наиболее критичных и значимых элементов, но и позволяет получить количественную оценку влияния архитектурных изменений, конфигурационных параметров и сценариев продвижения атакующего на общий уровень безопасности [3].

Метод решает следующие задачи:

1. Формирование и нормализация модели информационной системы на базе артефактов, описаний инфраструктуры и динамических сведений о межкластерном взаимодействии.
2. Сопоставление и обогащение графа данными из баз знаний информационной безопасности, источниками уязвимостей, тактикам и техникам поведения атакующего.
3. Интерпретация графа атак и анализ прикладных метрик, обеспечивающих переход от перечня уязвимостей к оценке устойчивости всей топологии инфраструктуры.
4. Разработка формальной процедуры ранжирования узлов и цепочек атак на основе характеристик графа и коэффициентов модели.

Выводы

Предложенный метод обеспечивает целостную, формализуемую и воспроизводимую оценку защищенности гибридных Kubernetes-инфраструктур за счет явного учета связанности узлов в составе комплексной системы.

Литература

1. Dave S.A., Leveraging Kubernetes for Hybrid Cloud Architectures // International Journal of Current Science. – 2024. – ISNN:2250-1770. – С. 65-66.
2. Гадир Д., Джафар Х., Воробьева А.А., Повышение безопасности Kubernetes: решающая роль DevSecOps // Труды ИСА РАН. – 2024. – Том 74. – С. 80-82.
3. Kryukov R. O., Fedorchenko E. V., Kotenko I. V., Novikova E. S., Zima V. M. Security assessment based on attack graphs using NVD and MITRE ATT & CK database for heterogeneous infrastructures // Information and Control Systems. – 2024. – № 2 (129). – С. 39-40.