УДК 004.056

РАЗРАБОТКА МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ МЕТОДОЛОГИИ DEVSECOPS

Пестряков П.А. (Университет ИТМО)
Научный руководитель — преподаватель факультета инфокоммуникационных технологий Филянин И.В. (Университет ИТМО)

Аннотация. Исследование фокусируется на укреплении защиты контейнеризированных приложений через интеграцию методологии DevSecOps и применение передовых инструментов безопасности. Анализ охватывал инструменты для диагностики уязвимостей, а также для проведения аудита и мониторинга. Значительное внимание уделялось разработке автоматизированной системы, способствующей ускорению обнаружения и решения проблем безопасности, что в конечном счете способствует повышению уровня защиты данных и инфраструктуры.

Введение. С увеличением применения технологий контейнеризации происходят значительные изменения в подходах к разработке и развертыванию приложений. Контейнеризация обеспечивает высокую степень масштабируемости, портативности и эффективности, однако вместе с этими преимуществами появляются новые вызовы в обеспечении информационной безопасности. Когда приложения и сервисы становятся более динамичными и распределенными, традиционные методы обеспечения безопасности часто оказываются недостаточными. Это подчеркивает необходимость внедрения таких методологий, как DevSecOps (Development, Security и Operations). DevSecOps представляет собой методологию, которая интегрирует практики обеспечения безопасности непосредственно в жизненный цикл разработки программного обеспечения, делая безопасность неотъемлемой частью разработки и эксплуатации, что обеспечивает более высокий уровень защиты приложений и данных. С применением технологий контейнеризации, особое внимание следует уделять аспектам управления конфигурацией и секретами, а также проведению всестороннего мониторинга и аудита. Эффективная интеграция практик и инструментов DevSecOps становится ключевой для обеспечения безопасности и уменьшения потенциальных угроз.

Основная часть. Цель исследования: анализ и разработка эффективных методов и стратегий обеспечения информационной безопасности в контексте контейнеризированных приложений, с использованием методологии DevSecOps и современных инструментов для обеспечения безопасности.

В рамках работы был проведен тщательный анализ научной литературы, технической документации и практического опыта внедрения методологии DevSecOps в контексте контейнеризированных приложений. Исследование позволило выявить ключевые критерии и стратегии, которые эффективно способствуют повышению безопасности на всех этапах жизненного цикла таких приложений. Особое внимание было уделено определению методов и инструментов, наиболее подходящих для обнаружения и устранения уязвимостей, а также для интеграции практик безопасности непосредственно в процесс разработки и эксплуатации. В зависимости от функциональности и применения инструменты были классифицированы на следующие категории: для сканирования и анализа уязвимостей (Trivy, Checkov, Snyk), для аудита и мониторинга (Falco, Prowler, ScoutSuite) и для управления секретами и конфиденциальной информацией (Vault, Yandex Lockbox). Исследование подчеркнуло значимость всех категорий инструментов в создании комплексной системы безопасности, при этом особое внимание было уделено инструментам аудита и мониторинга.

В ходе работы была разработана методика тестирования безопасности, включающая использование различных инструментов для аудита и мониторинга. Это позволило не только углубить понимание текущего состояния безопасности контейнеризированных приложений, но и выявить потенциал для значительного улучшения существующих решений в этой области. Было определено, что усовершенствование эффективности инструментов аудита и мониторинга возможно за счет интеграции дополнительного сервиса оптимизации взаимодействия с инструментами. Разработанный сервис обеспечивает автоматизацию процессов получения отчетов и проведения регулярного сканирования, а также включает в себя систему управления угрозами, которая позволяет классифицировать и приоритизировать уязвимости на основе степени риска.

Эта методика тестирования и предложенные улучшения инструментов аудита и мониторинга значительно повышают безопасность контейнеризированных приложений, автоматизируя критически важные процессы безопасности, оптимизируя работу с инструментами и ускоряя устранение уязвимостей. Таким образом, разработка и внедрение усовершенствованной системы безопасности в контексте DevSecOps позволяют достичь более высокого уровня защиты приложений, эффективно предотвращая кибератаки и другие нарушения безопасности данных, что является критически важным для обеспечения надежности и устойчивости современных информационных систем.

Вывод. Результаты исследования подтвердили значимость интегрированного подхода к безопасности в контексте контейнеризированных приложений, подчеркивая необходимость комплексного использования инструментов безопасности. Разработанная система демонстрирует улучшение в области обнаружения и управления угрозами, предлагая автоматизированные процессы для регулярного мониторинга и оперативного реагирования на потенциальные уязвимости. Внедрение данной системы в практику разработки и эксплуатации контейнеризированных приложений позволяет достичь более высокого уровня безопасности, эффективно снижая риски кибератак и других нарушений безопасности данных.

Список использованных источников:

1. Тулеубаева А. А., Камолов А. Б., Рычков В. А. Современные методологии разработки безопасного программного обеспечения //Цифровая экономика в контексте национальной безопасности. – 2022. – С. 97-105.
2. Alawneh M., Abbadi I. M. Expanding DevSecOps Practices and Clarifying the Concepts within Kubernetes Ecosystem //2022 Ninth International Conference on Software Defined Systems (SDS). – IEEE, 2022. – С. 1-7.
3. Hsu T. H. C. Hands-On Security in DevOps: Ensure continuous security, deployment, and delivery with DevSecOps. – Packt Publishing Ltd, 2018.
4. OWASP Kubernetes Top Ten [Электронный ресурс]. Режим доступа: https://owasp.org/www-project-kubernetes-top-ten/ (дата обращения: 31.01.24)
5. Kubernetes Scanning Tutorial [Электронный ресурс]. Режим доступа: https://aquasecurity.github.io/trivy/v0.33/tutorials/kubernetes/cluster-scanning/ (дата обращения: 31.01.24)

Пестряков П.А. (автор) Подпись

Филянин И.В. (научный руководитель) Подпись