Инструменты безопасности контейнерных сред

Игорь ДУША,
директор портфеля решений экосистемы в области информационной безопасности НОТА КУПОЛ

Согласно исследованиям, около половины всех приложений сегодня размещаются или разрабатываются в контейнерных средах, что позволяет ускорить их развертывание и повысить эффективность разработки. Однако наряду с этим формируется пространство для новых киберугроз. В 2023 г. 89% компаний столкнулись хотя бы с одним таким опасным инцидентом. Что можно противопоставить негативному развитию ситуации?

Зачем нужны контейнеры

Контейнеризация – это метод виртуализации, который позволяет запускать приложения и управлять ими в изолированном окружении. Контейнер содержит все необходимые компоненты для работы: код, библиотеки, инструменты, зависимости и конфигурации.

Технологию используют, чтобы обеспечить масштабируемость, гибкость разработки и развертывания приложений. Она помогает ИТ-специалистам создавать, тестировать продукты гораздо быстрее и эффективнее по сравнению с традиционными методами, в том числе с виртуальными машинами.

Во-первых, контейнеры позволяют добиться большей портативности. Поскольку они изолируют приложение от особенностей окружения (операционной системы, «железа»), их можно запускать на любом оборудовании, где установлена контейнерная платформа. Это значительно облегчает миграцию и развертывание ПО.

Во-вторых, с помощью контейнеризации компании оптимизируют ресурсы. Технология, эффективно расходующая технические мощности хост-системы, позволяет запускать несколько процессов параллельно. Таким образом, бизнес снижает издержки, повышая скорость разработки и сокращая бюджеты на закупку и обслуживание оборудования.

Угрозы безопасности

Такие контейнерные технологии, как Docker и Kubernetes, ставшие стандартом в индустрии, нашли широкое применение в различных секторах: от разработки ПО до облачных вычислений. Но несмотря на большое количество преимуществ как на этапе создания приложения, так и во время его эксплуатации, контейнеры могут быть уязвимы к атакам. Поэтому разработчикам необходимо уделять особое внимание вопросам безопасности при их использовании.

Защита современного ПО затруднена из-за его сложности, динамичности, использования микросервисной архитектуры, когда приложение разбивается на множество небольших сервисов, которые взаимодействуют между собой в контейнерах. Управление и обеспечение их безопасности – сложная задача, требующая специальных инструментов и навыков.

Основные векторы атаки

Вирусы и вредоносное ПО

Контейнерный образ (шаблон, на основе которого разработчики создают контейнеры) может стать мишенью для внедрения вредоносного ПО и вирусов – в атаках их используют 68% киберпреступников. Чтобы внедрить скомпрометированный код, злоумышленники эксплуатируют уязвимости в процессе сборки образов.

Это может случиться из-за того, что разработчик использует в сборке или загружает компоненты из непроверенных репозиториев. Однако даже репутация источника не всегда может полностью обезопасить разработчиков. Так, в 2022 г. публичный Docker Hub содержал более 1,5 тыс. образов контейнеров с вредоносным ПО. На тот момент он не обладал должными инструментами защиты. Сейчас

Источник: https://it-fabric.ru/

эта проблема есть у отечественных аналогов Docker Hub. Поэтому одним из российских вендоров разработан программный продукт, способный защитить потребителей и их сервисы.

Атаки на сеть и межконтейнерное взаимодействие

Контейнерные среды зачастую состоят из множества взаимосвязанных элементов, взаимодействующих через сеть. Именно это взаимодействие может стать мишенью для атак, направленных на перехват либо изменение данных.

Злоумышленники могут использовать атаки типа Man-in-the-Middle (MitM), DNS-спуфинг или другие механизмы подмены. В обоих случаях целью становится не само приложение, а каналы связи, отвечающие за его обращения к остальной инфраструктуре. Подобные угрозы особенно актуальны для облачных инфраструктур и в тех ситуациях, когда пользователи могут запустить собственный контейнер.

Уязвимости в образах контейнеров и библиотеках, внедрение вредоносного ПО

Контейнерные образы обычно содержат множество зависимостей и библиотек, для каждой из которых характерны собственные уязвимости. По аналогии с атаками на цепочки поставок интеграция собственного кода в устаревшие или уязвимые версии библиотек позволяет злоумышленникам выполнять вредоносные операции внутри контейнера.

Кроме того, попадать в конечные приложения могут и уязвимости, которые содержатся в базовых образах контейнеров. Недостаточное внимание к обновлению и патчингу этих компонентов приводит к серьезным проблемам безопасности: в одной из подобных атак зараженные компоненты больше года оставались без внимания, прежде чем сообщество приняло меры.

Неавторизованный доступ

Помимо вредоносного ПО и использования уязвимостей один из самых часто применяемых инструментов злоумышленников – социальная инженерия. В этом случае для получения доступа киберпреступники используют личную информацию, что иногда позволяет значительно упростить подбор пароля из-за его предсказуемости, а иногда – убедить человека перейти по ссылке или открыть зараженный файл. Таким образом, слабые механизмы аутентификации и контроля доступов могут позволить злоумышленникам получить неавторизованный доступ к данным и взаимодействиям.

Утечка данных через API

Многие контейнеризованные приложения используют для выполнения задач API и внешние сервисы. По сути это базовый механизм взаимодействия с приложением. Если такие компоненты не защищены должным образом, они могут стать объектом атаки.

API могут быть уязвимыми для различных веб-так (см. OWASP TOP 10), таких как XSS или SQL-инъекции.

Ошибки администрирования

Ошибки в конфигурации платформы управления контейнерами или самих контейнеров также могут создать уязвимости, которые злоумышленники используют для атак. Например, предоставить доступ к софту могут несанкционированное открытие портов и служб, а также отсутствие либо неправильная настройка политик безопасности.

Как обезопасить контейнерные среды

Рассмотрим подходы к обеспечению безопасности контейнерных сред.

- Изоляция и сегментация
  Фундаментальный принцип безопасности контейнеризованных приложений – изоляция, которая помогает минимизировать риски, связанные с компрометацией одного контейнера. Для этого используются механизмы типа Namespaces и Control Groups (cgroups):

– Namespaces позволяет создать отдельное пространство имен для процессов, обеспечивая их изоляцию в контексте сети, идентификаторов процессов и файловой системы;
– Cgroups ограничивает и контролирует использование ресурсов (CPU, память, дисковое пространство) контейнерами, предотвращая возможное воздействие одного контейнера на работу других.

- Автоматизация сканирования уязвимостей и вредоносного ПО
Автоматизация сканирования уязвимостей в контейнерных образах позволяет своевременно выявлять и устранять угрозы безопасности. Современные DevOps-контейнеры оснащены встроенными инструментами, которые выполняют функциональное и нагрузочное тестирование кода и содержащихся в нем зависимостей.
Таким образом, система не позволит собрать приложение с потенциально вредоносными компонентами.
- Мониторинг и обнаружение аномалий
Для обеспечения безопасности сред необходимы автоматический мониторинг процессов и пользовательской активности, а также своевременное обнаружение аномалий.
- Обеспечение соответствия требованиям и политик безопасности
Для соответствия нормативным требованиям и внутренним политикам безопасности компании используют различные инструменты и процессы, например, Open Policy Agent (OPA, универсальный механизм управления политиками), который может быть интегрирован с Kubernetes для обеспечения соблюдения политик безопасности.

Новые направления и тренды

Среди новых направлений развития инструментов защиты можно отметить следующие.

- Интеграция с DevSecOps-инструментами
DevSecOps – это эволюция традиционных DevOps-принципов, которая дополнительно включает аспекты безопасности на всех этапах жизненного цикла ПО. Интеграция Sec-практик в процессы разработки и эксплуатации контейнерных сред обеспечивает более эффективную защиту приложений и инфраструктуры:
– инструменты статического анализа кода (SAST) проверяют код на уязвимости на этапе написания, позволяя разработчикам исправлять ошибки до их интеграции;
– инструменты сканирования автоматически проверяют контейнерные образы на наличие известных уязвимостей перед их развертыванием;
– инструменты управления секретами (чувствительной информацией) позволяют обеспечить безопасный доступ к конфиденциальным данным и ключам API в контейнерных средах.
Современные платформы, выстроенные в соответствии с принципами DevSecOps, дают возможность не только повысить эффективность, но и автоматизировать процессы безопасности. За счет интеграции с пайплайнами CI/CD тесты выполняются автоматически, и приложение может быть развернуто только после успешного прохождения всех проверок. А системы мониторинга постоянно анализируют вызовы и события в реальном времени, обнаруживая аномалии и подозрительные действия, что позволяет быстро реагировать на инциденты.
- Искусственный интеллект
Технологии искусственного интеллекта (ИИ) и машинного обучения (МО), благодаря способности обрабатывать большие объемы данных и выявлять сложные угрозы, все чаще становятся одним из инструментов, обеспечивающих безопасность контейнеров.
ИИ-модели могут обучаться на данных о стандартном поведении контейнеров и приложений, что позволяет выявлять аномалии, которые указывают на атаки или сбои. Анализ сетевого трафика с помощью МО дает возможность обнаруживать подозрительные подключения или необычно высокий трафик, что может свидетельствовать о DDoS-атаке или утечке данных.
Более того, ИИ и МО интегрируются в системы безопасности контейнеров для создания самоуправляемых систем, которые могут автоматически адаптироваться к новым угрозам и изменяющимся условиям.

Влияние атак на бизнес

Атаки на контейнерные среды могут иметь серьезные последствия для бизнеса в зависимости от того, какие приложения и данные в них используются. Утрата данных и нарушение операционных процессов приводят к значительным финансовым потерям. Компрометация контейнеров может вылиться в утечку конфиденциальной информации, включая данные клиентов и корпоративные данные. А публичные инциденты безопасности наносят серьезный урон репутации компании, подрывая доверие заказчиков и партнеров.

Кроме того, атаки нарушают работу ИТ-инфраструктуры, что ведет к простоям и снижению производительности. В некоторых случаях оборудование выходит из строя, вынуждая предприятие резко увеличивать расходы на обновление «железа».

Внедрение современных средств безопасности помогает предотвратить растущие угрозы и атаки, обеспечивая надежность и стабильность ИТ-инфраструктуры. При выборе решений для защиты контейнерных сред особое внимание следует обратить на их функциональность, наличие инструментов автоматизации, поддержки и обновлений от разработчиков. Также рекомендуется учитывать возможности интеграции выбранных инструментов с существующими системами и процессами DevSecOps. ■