ЦЕНТР НТИ МЭИ

ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ
ЭЛЕКТРОЭНЕРГИИ РАСПРЕДЕЛЕННЫХ
ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

Проблемные вопросы обеспечения информационной безопасности при использовании средств контейнеризации

Владимир Карантаев
к.т.н., доцент
MBA

WWW.NTI.MPEI.RU

Визитка: Владимир Карантаев

Практик

Стаж деятельности в области ИТ и ИБ - 20 лет (с 2002 года).

10 + лет экспертной и прикладной деятельности в направлении Кибербезопасность АСУ ТП

Ex ИнфоТеКС **Ex** Kaspersky

Проекты в ПАО Россети

Соавтор и организатор первых киберучений национального уровня

Преподаватель и исследователь

к.т.н. специальность 05.09.03 "Электротехнические комплексы и системы"

Автор курса лекций «Основы кибербезопасности РЗА энергосистем»

Центр НТИ МЭИ Кафедра РЗиАЭ.

Консультант

Вопросы для обсуждения

- Практики и вопросы разработки программных продуктов для АСУ
- Контейнеры и платформы оркестрации
- Публичные и частные облака при взаимодействии с АСУ ТП

Возможные вызовы для вендоров АСУ

- Готовность доказать "отечественность" своих программных продуктов, построенных на базе Open Source
- Внедрение практик DevOps
- Внедрение практик DevSecOps
- Внедрение **SCA** (Software Composition Analysis)- анализ зависимостей в проекте.
- Готовность предоставить и управлять Software Bill of Materials
- Готовность перенести инфраструктуру CI/CD в пределы РФ
- Готовность поддержать ОС Linux

Возможные вызовы для вендоров АСУ

29.3. Прикладное программное обеспечение, планируемое к внедрению в рамках создания (модернизации или реконструкции, ремонта) значимого объекта и обеспечивающее выполнение его функций по назначению (далее - программное обеспечение), должно соответствовать следующим требованиям по безопасности:

29.3.1. Требования по безопасной разработке программного обеспечения

29.3.2. Требования к испытаниям по выявлению уязвимостей в программном обеспечении:

- проведение статического анализа исходного кода программы;
- проведение фаззинг-тестирования программы, направленного на выявление в ней уязвимостей;
- проведение динамического анализа кода программы (для программного обеспечения, планируемого к применению в значимых объектах 1 категории значимости).

Возможные вызовы для вендоров АСУ

29.3.3. Требования к поддержке безопасности программного обеспечения:
наличие процедур отслеживания и исправления обнаруженных ошибок и уязвимостей программного обеспечения;
определение способов и сроков доведения разработчиком (производителем) программного обеспечения до его пользователей информации об уязвимостях программного обеспечения, о компенсирующих мерах по защите информации или ограничениях по применению программного обеспечения, способов получения пользователями программного обеспечения его обновлений, проверки их целостности и подлинности;
наличие процедур информирования субъекта критической информационной инфраструктуры об окончании производства и (или) поддержки программного обеспечения (для программного обеспечения, планируемого к применению в значимых объектах 1 категории значимости).

Контейнеры и платформы оркестрации

Вопросы:

Своевременного анализа угроз БИ

Вопросы применение отечественной криптографии

Вопросы эффективного применение встраиваемых механизмов безопасности на уровне ОС и кластера.

Перечень групп угроз БИ кластера K8S и контейнеризированных приложений

- Угрозы, реализуемые при эксплуатации уязвимостей в программном обеспечении контейнеризированных приложений
- Угрозы, реализуемые при эксплуатации уязвимостей в программном обеспечении образа контейнера,
- обеспечивающем выполнение приложения (зависимости).
- Угрозы, реализуемые при эксплуатации уязвимостей, появившихся в следствии ошибок , допущенных в ходе конфигурации сборки образа контейнера:

  Исполнение от имени суперпользователя

  Наличие и использование файлов в образе контейнера с установленным битом setuid
- Угрозы, реализуемые в процессе сборки образа контейнеров (Атаки на систему сборки образов контейнеров)
- Угрозы, реализуемые в промежутке между сборкой и развертыванием образа контейнеров (атаки на цепочку поставки)

National Security Agency. Kubernetes Hardening Guide 03.2022
Райс Лиз Безопасность контейнеров. Фундаментальный подход к защите контейнеризированных приложений 2021

Перечень групп угроз БИ кластера K8S и контейнеризированных приложений (Продолжение)

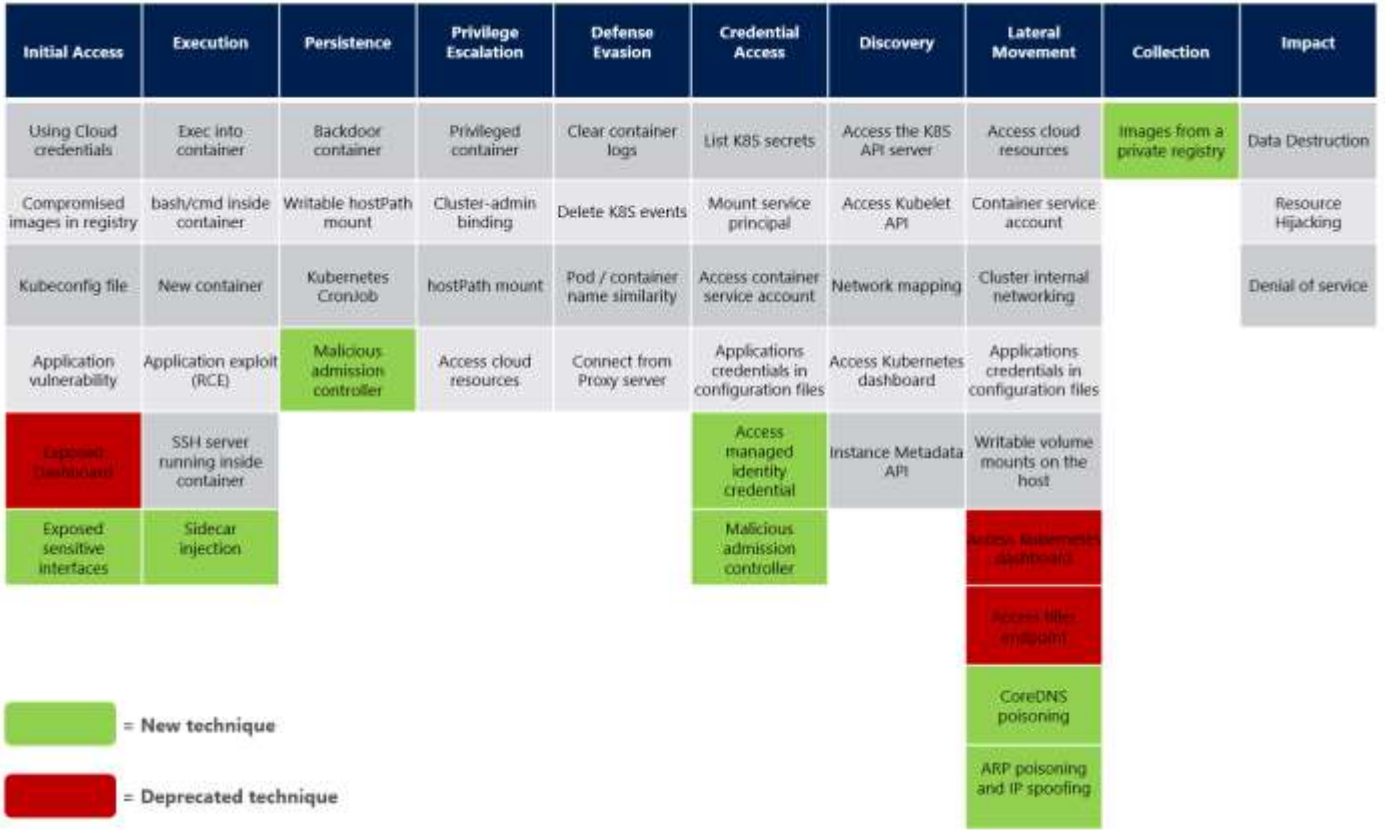
- Угрозы, реализуемые при эксплуатации уязвимостей, появившихся в следствии ошибок , допущенных в ходе настройки контейнеров
- Угрозы, реализуемые при использовании незащищенных механизмов межсетевого взаимодействия компонент кластера K8S между собой
- Угрозы, реализуемые при использовании незащищенных механизмов межсетевого взаимодействия контейнеров между собой
- Угрозы, реализуемые в рамках жизненного цикла Secrets кластера K8S.

  Всего восемь типов secrets.
- Угрозы, реализуемые при эксплуатации узявимостей в среде исполнения контейнеров (containerd и CRI-O)

  Выход за рамки контейнера
- Угрозы, реализуемые при эксплуатации узявимостей в компонентах программного обеспечения кластера K8S

National Security Agency. Kubernetes Hardening Guide 03.2022
Райс Лиз Безопасность контейнеров. Фундаментальный подход к защите контейнеризированных приложений 2021

Матрица атак на Kubernetes («Threat Matrix for Kubernetes») Microsoft



https://www.microsoft.com/en-us/security/blog/2021/03/23/secure-containerized-environments-with-updated-threat-matrix-for-kubernetes/

Матрица атак на Kubernetes MITRE

«Containers Matrix», MITRE: https://attack.mitre.org/matrices/enterprise/containers/

Нормативно-правовые требования

Приказом ФСТЭК России от 4 июля 2022 г. N 118 (зарегистрирован Минюстом России 29 сентября 2022 г., регистрационный N 70275) утверждены Требования по безопасности информации к средствам контейнеризации.

Возможные вызовы для вендоров

Применение отечественных СЗИ и СКЗИ:

- Предотвращения атак на цепочку поставки образов контейнеров
- Реализации элементов zero trust архитектуры на уровне сети кластера
- Разработка специализированной сборки ImmutableOS для платформы оркестрации
- Эффективная реализация и использование встроенных механизмов безопасности в ОС
- Эффективная реализация и использование встроенных механизмов безопасности в кластере

Возможные вызовы для вендоров

- Отсутствие продуктового предложения со стороны разработчиков отечественных ОС по использованию сред выполнения, например, Containerd, Kata Containers и CRI-O с адаптацией встроенных в ОС механизмов защиты.
- Отсутствие продуктового предложения с предложением специализированных ОС, для применения в платформах контейнеризации с встроенными механизмами защиты.
- Отсутствие решений, предотвращающих атаки на "цепочку поставки" образов контейнеров, реализованных на базе СКЗИ.
- Аналог ISTIO с ГОСТ TLS
- Управление секретами кластера с помощью отечественного продукта с использованием СКЗИ

Предложения

На основе отраслевой ассоциации рассмотреть целесообразность формирования требований к использованию сервисов Cloud по примеру ГосТех.

Спасибо за внимание

ул. Красноказарменная, д. 17
Москва, Россия

WWW.NTI.MPEI.RU

ЦЕНТР НТИ МЭИ