



ЦЕНТР НТИ МЭИ

ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ
ЭЛЕКТРОЭНЕРГИИ РАСПРЕДЕЛЕННЫХ
ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

Проблемные вопросы обеспечения информационной безопасности при использовании средств контейнеризации

Владимир Карантаев

К.Т.Н., доцент
МВА

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 поддерживать 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)



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 уязвимостей в среде исполнения контейнеров (containerd и CRI-O)
Выход за рамки контейнера
- Угрозы, реализуемые при эксплуатации уязвимостей в компонентах программного обеспечения кластера K8S



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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Impact
Using Cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List K8S secrets	Access the K8S API server	Access cloud resources	Images from a private registry	Data Destruction
Compromised images in registry	bash/cmd inside container	Writable hostPath mount	Cluster-admin binding	Delete K8S events	Mount service principal	Access Kubelet API	Container service account		Resource Hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod / container name similarity	Access container service account	Network mapping	Cluster internal networking		Denial of service
Application vulnerability	Application exploit (RCE)	Malicious admission controller	Access cloud resources	Connect from Proxy server	Applications credentials in configuration files	Access Kubernetes dashboard	Applications credentials in configuration files		
Exposed (dashboards)	SSH server running inside container				Access managed identity credential	Instance Metadata API	Writable volume mounts on the host		
Exposed sensitive interfaces	Sidecar injection				Malicious admission controller		Access Kubernetes dashboards		
							Access kube endpoint		
							CoreDNS poisoning		
							ARP poisoning and IP spoofing		

= New technique
 = Deprecated technique

<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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact
3 techniques	4 techniques	4 techniques	4 techniques	7 techniques	3 techniques	3 techniques	1 techniques	3 techniques
Exploit Public-Facing Application	Container Administration Command	External Remote Services	Escape to Host	Build Image on Host	Brute Force (3)	Container and Resource Discovery	Use Alternate Authentication Material (1)	Endpoint Denial of Service
External Remote Services	Deploy Container	Implant Internal Image	Exploitation for Privilege Escalation	Deploy Container	Steal Application Access Token	Network Service Discovery		Network Denial of Service
Valid Accounts (2)	Scheduled Task/Job (1)		Scheduled Task/Job (1)	Indicator Removal	Unsecured Credentials (2)	Permission Groups Discovery		Resource Hijacking
	User Execution (1)	Valid Accounts (2)	Valid Accounts (2)	Masquerading (1)				
				Use Alternate Authentication Material (1)				
				Valid Accounts (2)				

Last modified: 01 April 2022

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

