Современные вызовы
Вопрос для дискуссии?

к.т.н., Карантаев Владимир

РГ «Кибербезопасность» НТИ «Энерджинет»

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 узявимостей в программном обеспечении контейнеризированных приложений
- Угрозы, реализуемые при эксплуатации узявимостей 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

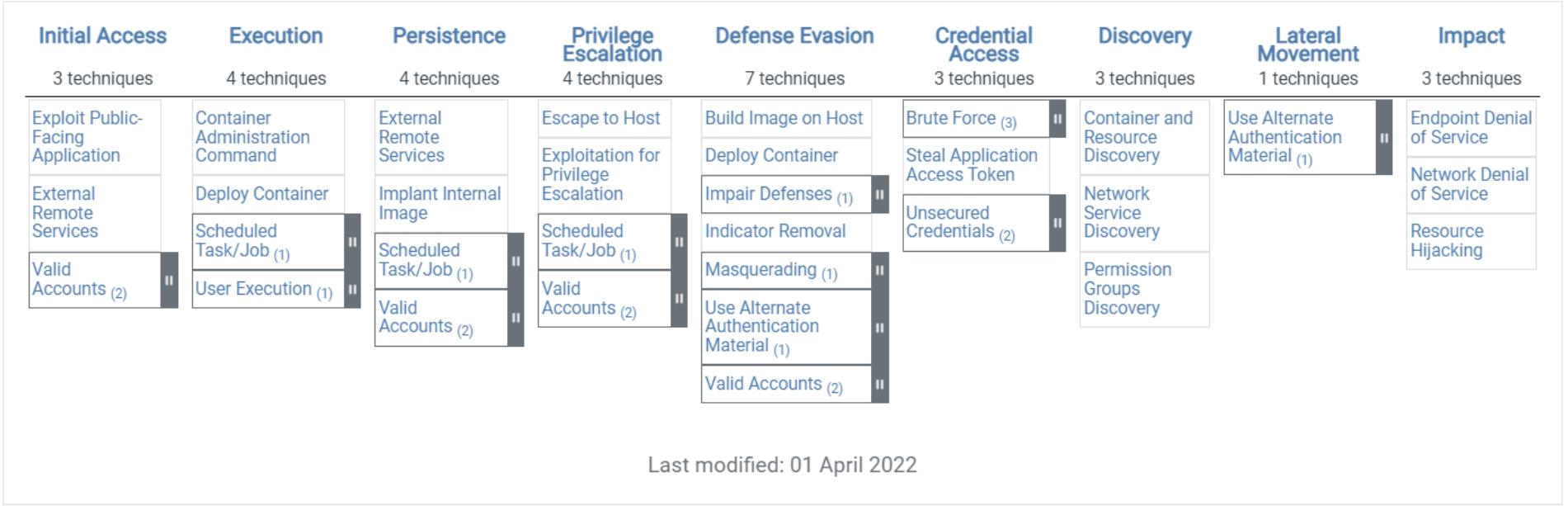
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Impact
Using Cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List K8S secrets	Access the K8S API server	Access cloud resources	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 Dashboard	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 dashboard		
							Access tiller 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



«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

Нормативно-правовые требования

Приказом ФСТЭК России от 27 октября 2022 г. N 187 (зарегистрирован Минюстом России 22 декабря 2022 г., регистрационный N 71774) утверждены Требования по безопасности информации к средствам виртуализации

Предложения

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

РГ «КИБЕРБЕЗОПАСНОСТЬ»

EnergyNet

Объединяем компетенции и формируем системный подход к обеспечению кибербезопасности

EnergyNetCS@ya.ru

Вопросы в определении отдельных сфер, в которых функционируют различные объекты

Существует вопросы в определении отдельных сфер, в которых функционируют различные объекты, что может привести к ошибкам в отнесении к объектам КИИ управляющих ими АСУТП

Объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;

Субъекты критической информационной инфраструктуры - государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, **функционирующие в сфере … топливно-энергетического комплекса**, ….

Объекты КИИ – ИС, АСУ и ИТКС на объектах ТЭК

Объекты ТЭК

ВОПРОС

Относятся ли котельные к объектам ТЭК, предусмотренным п. 9 ст. 2 Федерального закона от 21.07.2011 N 256-ФЗ "О безопасности объектов топливно-энергетического комплекса", регулирующего организационные и правовые основы в сфере их антитеррористической защищенности и защищенности от актов незаконного вмешательства?)

Объекты ТЭК

ГИПОТЕЗА

Правовой анализ 256-ФЗ позволяет сделать вывод, что да, относятся все, так как не выявлено каких либо критериев, которые могли бы их разделить на «объекты ТЭК» и «не объекты ТЭК» (например, исключить котельные малой тепловой мощности или котельные, не относящиеся к ОПО в рамках 116-ФЗ и т.д.).

Котельные, являясь объектами теплоснабжения, в соответствии с п. 9 ст. 2 Федерального закона № 256 относятся к объектам ТЭК.

Федеральным законом № 256 и подзаконными актами к нему не установлены критерии разграничения всех объектов теплоснабжения и газоснабжения на объекты, относящиеся к объектам топливно-энергетического комплекса (далее - ТЭК), предусмотренным п. 9 ст. 2 Федерального закона N 256, и объектам, которые не являются таковыми.

Объекты ТЭК

Анализ судебной практики также не выявил правовых позиций судов, в соответствии с которыми какие-либо объекты теплоснабжения возможно исключить из категории объектов ТЭК, предусмотренной Федеральным законом N 256.

Кроме того, выявлена судебная практика в соответствии с которой по искам органов прокуратуры суды принимали решения о понуждении собственников котельных обратиться в уполномоченные государственные органы субъекта Российской Федерации с предложением о включении котельных в перечень объектов ТЭК, подлежащих категорированию, для последующей процедуры категорирования, разработки паспорта безопасности и выполнения иных процедур Федерального закона N 256 (Решение Ванинского районного суда Хабаровского края от 24.10.2016 по делу N 2-1006/2016).

Однако, возможно, в практике применения 256-ФЗ есть иная позиция, например критерии Приказа Минэнерго № 48 для включения объектов ТЭК в перечень для категорирования в рамках 256-ФЗ, ст. 2 Федерального закона от 31.03.1999 № 69 «О газоснабжении в Российской Федерации» и пр.

Котельная как объект ТЭК

Объекты ТЭК

Изложенные выше выводы имеют определённую степень «субъективности» в связи со спецификой Федерального закона № 256 и особенностями практики его применения в разных субъектах Российской Федерации, в связи с чем, целесообразным является направление запроса в Министерство энергетики Российской Федерации для получения письменных разъяснений.

Открытые системы получения знаний

Открытая база знаний по Кибербезопасности

EnergyNet

https://github.com/SecureEnergynet/Research

Открытая группа по кибербезопасности

RUSCADASEC

www.discord.gg.nJjrmgM9sm.ru

t.me|RuScadaSec

Ассоциация по вопросам защиты информации

BISA BUSINESS INFORMATION SECURITY ASSOCIATION

https://bisa.ru/

ЦК КБ «КИБЕРБЕЗОПАСНОСТЬ»

EnergyNet

Объединяем компетенции и формируем системный подход к обеспечению кибербезопасности

https://energynet.ru/people#cyb

EnergyNetCS@ya.ru

Инфосистемы Джет

РГУ нефти и газа имени И.М. Губкина

INFOWATCH

СИБИНТЕК

iGrids

СИСТЕМА

УЦСБ

Уральский федеральный университет имени первого Президента России Б.Н.Ельцина

ЧГУ