Международный союз электросвязи

МСЭ-Т X.1643

(01/2022)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность облачных вычислений – Передовой опыт и руководящие указания в области облачных вычислений

Требования безопасности и руководящие указания по безопасности контейнеров виртуализации в среде облачных вычислений

Рекомендация МСЭ-Т X.1643

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды (1)	X.1140–X.1149
Безопасность приложений (1)	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность умных электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1350–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1399
Безопасность технологии распределенного реестра (DLT)	X.1400–X.1429
Безопасность приложений (2)	X.1450–X.1459
Безопасность веб-среды (2)	X.1470–X.1489
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
Киберзащита	X.1590–X.1599
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	**X.1640–X.1659**
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
Защита данных	X.1770–X.1789
БЕЗОПАСНОСТЬ СЕТЕЙ IMT-2020	X.1800–X.1819

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1643

Требования безопасности и руководящие указания по безопасности контейнеров виртуализации в среде облачных вычислений

Резюме

В Рекомендации МСЭ-Т X.1643 анализируются угрозы и проблемы безопасности для контейнеров виртуализации в среде облачных вычислений, а также определена эталонная структура, включающая руководящие указания по безопасности контейнеров виртуализации в облаке.

Хронологическая справка

Издание	Рекомендация	Утверждено	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1643	07.01.2022 г.	17-я	11.1002/1000/14804

Ключевые слова

Облачные вычисления, руководящие указания по безопасности, контейнер виртуализации.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации.
Например: http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним в целях стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" (shall) или некоторые другие обязывающие выражения, такие как "обязан" (must), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1643

Требования безопасности и руководящие указания по безопасности контейнеров виртуализации в среде облачных вычислений

1 Сфера применения

В настоящей Рекомендации анализируются угрозы и проблемы безопасности для контейнеров виртуализации в среде облачных вычислений, а также определена эталонная структура, включающая руководящие указания по безопасности контейнеров виртуализации в облаке.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру; поэтому пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ в данной Рекомендации не придает ему как отдельному документу статус Рекомендации.

[ITU-T X.1162] Recommendation ITU-T X.1162 (2008), *Security architecture and operations for peer-to-peer networks.*

[ITU-T X.1255] Рекомендация МСЭ-Т X.1255 (2013 г.), *Структура обнаружения информации по управлению определением идентичности.*

[ITU-T X.1279] Рекомендация МСЭ-Т X.1279 (2020 г.), *Система расширенной аутентификации с использованием телебиометрии с антиспуфинговыми механизмами обнаружения.*

[ITU-T X.1601] Рекомендация МСЭ-Т X.1601 (2015 г.), *Основы безопасности облачных вычислений.*

[ITU-T X.1605] Рекомендация МСЭ-Т X.1605 (2020 г.), *Требования безопасности к открытой инфраструктуре как услуге (IaaS) в среде облачных вычислений.*

[ITU-T Y.3508] Recommendation ITU-T Y.3508 (2019), *Cloud computing – Overview and high-level requirements of distributed cloud.*

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

3.1.1 управление доступом (access control) [b-ITU-T X.800]: Предотвращение несанкционированного использования ресурса, в том числе предотвращение использования ресурса несанкционированным способом.

3.1.2 образ облачной услуги (cloud service image) [ITU-T Y.3508]: Исполняемый код с информацией о состоянии виртуальной машины (см. пункт 3.1.10) или контейнера (см. пункт 3.1.11).

3.1.3 среда выполнения (execution environment) [b-ITU-T Y.4500.1]: Логический объект, представляющий собой среду, в которой могут выполняться программные модули.

3.1.4 шлюз (gateway) [b-ITU-T H.350.4]: Устройство, выполняющее трансляцию одного протокола в другой. Нередко шлюзы обеспечивают трансляцию между IP-сетью и коммутируемой сетью голосовой связи общего пользования для интеграции этих двух сетей.

3.1.5 оркестрация (orchestration) [b-ITU-T Y.3100]: В контексте IMT-2020 процессы, направленные на автоматическую организацию, координацию, реализацию и использование сетевых функций и ресурсов физической и виртуальной инфраструктуры по заданным критериям оптимизации.

3.1.6 оверлейная сеть (overlay network) [b-ITU-T X.1162]: Виртуальная сеть, работающая поверх другой сети. Подобно любой другой сети, она состоит из набора узлов и связей между ними. Поскольку связи имеют логический характер, они могут соответствовать множеству физических каналов базовой сети.

3.1.7 регистр (registry) [b-ITU-T X.1255]: Механизм, предназначенный для регистрации метаданных о цифровых объектах и хранения схем метаданных, который обеспечивает возможность поиска в регистре постоянных идентификаторов на основе использования схем метаданных.

3.1.8 спуфинг (spoofing) [b-ITU-T X.1279]: Попытка объекта выдать себя за другой объект путем демонстрации записанного изображения, другого образца биометрических данных или искусственно полученной биометрической характеристики в целях имитации того или иного индивида.

3.1.9 безопасность транспортного уровня (transport layer security) [b-ITU-R BT.1699]: Протокол, используемый для передачи и приема через интернет закодированных данных. Поддерживает комбинацию различных технологий обеспечения безопасности, включая криптосистему с общими ключами, цифровые сертификаты, а также хеш-функции для защиты от прослушивания, подделки сообщений и спуфинга.

3.1.10 виртуальная машина (virtual machine (VM)) [b-ITU-T Q.1743]: Программа, имитирующая работу центрального процессора гипотетического компьютера. Программы, выполняемые виртуальной машиной, представлены в байтовых кодах, которые являются элементарными операциями для такого гипотетического компьютера.

3.1.11 контейнер виртуализации (virtualization container) [b-ITU-T L.1362]: Часть вычислительного узла, предоставляющая изолированную виртуализированную среду вычислений.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

3.2.1 отказ узла (node failure): Ошибка, выражающаяся в отсутствии доступа к одному или нескольким узлам сети в системе оркестрации.

3.2.2 атака с анализом пакетов (packet sniffing attack): Метод атаки с неправомерным перехватом каждого пакета во время его прохождения по сети.

3.2.3 режим мостовой сети контейнеров виртуализации (virtualization container bridge network mode): Сетевой режим, в котором каждому контейнеру виртуализации выделяется отдельное пространство имен и IP-адрес, что позволяет контейнеру связываться с хостом напрямую.

3.2.4 атака с выходом за пределы контейнера виртуализации (virtualization container escape attack): Атака, при которой злоумышленник неправомерно получает полномочия на выполнение кода в контейнере виртуализации и использует эти полномочия, чтобы получить более широкие полномочия на виртуальной машине или физическом сервере, на которых работает этот контейнер.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

ACL	Access Control List		Список управления доступом
API	Application Programming Interface		Интерфейс прикладного программирования
CPU	Central Processing Unit	ЦП	Центральный процессор
DDoS	Distributed Denial of Service		Распределенный отказ в обслуживании
DoS	Denial of Service		Отказ в обслуживании

DTLS	Datagram Transport Layer Security		Протокол дейтаграмм безопасности транспортного уровня
IaaS	Infrastructure as a Service		Инфраструктура как услуга
IP	Internet Protocol		Протокол Интернет
IPsec	IP Security protocol		Протокол безопасности IP
MITM	Man-in-the-Middle		Посредник
OS	Operating System	ОС	Операционная система
TLS	Transport Layer Security		Протокол безопасности транспортного уровня
VM	Virtual Machine		Виртуальная машина
VXLAN	Virtual eXtensible Local Area Network		Виртуальная расширяемая локальная сеть

5 Соглашения

В настоящей Рекомендации:

ключевое слово "**может**" означает необязательное требование, которое допустимо, но не имеет рекомендательного значения;

ключевые слова "**должен**" или "**требуется**" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации;

ключевое слово "**следует**" означает требование, которое рекомендуется, но не является абсолютно необходимым; таким образом, для заявления о соответствии настоящей Рекомендации это требование не является обязательным;

ключевые слова "**не должен**" или "**запрещается**" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации.

6 Обзор

Настоящая Рекомендация устанавливает структуру безопасности контейнера виртуализации, показанную на рисунке 6-1. Она включает в себя безопасность на уровнях пользователя, доступа, ресурсов и услуг, а также управление безопасностью и услуги по обеспечению безопасности.

Рисунок 6-1 – Структура безопасности контейнера виртуализации

Цель использования этой структуры состоит в том, чтобы:

– обеспечивать надежность и стабильность работы контейнера виртуализации в среде облачных вычислений;

– обеспечивать безопасность контейнера виртуализации путем защиты всех его составляющих, в частности уровней пользователя, доступа, ресурсов и т. д.; и

– осуществлять управление безопасностью и предоставлять услуги по обеспечению безопасности клиентам службы контейнеров виртуализации.

В соответствии с рисунком 6-1

a) **Безопасность на уровне пользователя** состоит в управлении ролями, идентификационными данными и действиями пользователя для управления доступом пользователей к контейнерам виртуализации, аутентификации пользователей и аудита их действий.

b) **Безопасность на уровне доступа** включает в себя механизмы управления доступом, такие как веб-доступ и доступ через интерфейс прикладного программирования (API).

c) **Безопасность на уровне ресурсов** подразделяется на безопасность физических ресурсов, безопасность хост-компьютера и безопасность виртуальных ресурсов.

   i. Под **физическими ресурсами** понимаются аппаратные ресурсы контейнера виртуализации, то есть вычислительные ресурсы (центральный процессор (ЦП) или память), сетевые ресурсы (маршрутизатор, коммутатор), ресурсы хранилища и т. д.

   ii. Под **хосто**м понимается сервер, на котором реализован контейнер виртуализации, например операционная система (ОС), VM и т. д.

   iii. Под **виртуальными ресурсами** понимаются собственно виртуальные компоненты виртуализации, например виртуальные вычисления, виртуальная сеть, виртуальное хранилище и т. д.

d) **Управление безопасностью** – это функции управления безопасностью контейнера виртуализации в среде облачных вычислений, в том числе управление определением идентичности, аутентификацией, политиками безопасности, мероприятиями по обеспечению безопасности, техническим обслуживанием и т. д.

e) **Услуги по обеспечению безопасности** – это предоставление пользователям возможностей обеспечения безопасности контейнеров виртуализации в форме услуг.

7 Проблемы и угрозы безопасности контейнеров виртуализации в среде облачных вычислений

7.1 Проблемы и угрозы безопасности среды выполнения контейнера виртуализации

Среда выполнения контейнера виртуализации – первая область, которая требует защиты, поскольку именно она, как правило, наименее защищена и в нее легче всего внедрить вредоносный код. Кроме того, здесь возможны и другие угрозы, например вредоносные или непродуманные изменения в исходном коде, вредоносные или ошибочные модификации в контроллерах автоматизированной сборки, ошибки в сценариях настройки, а также добавление небезопасных библиотек или небезопасных версий существующего кода.

7.2 Проблемы и угрозы безопасности контейнера виртуализации во время его работы

7.2.1 Проблемы и угрозы безопасности мониторинга работы контейнера виртуализации

Контейнеры виртуализации по своему характеру эфемерны, но именно это основополагающее преимущество усложняет мониторинг. Кроме того, у средств мониторинга нет возможности наблюдать или получить информацию о происходящем внутри контейнера виртуализации на уровне API, что существенно затрудняет мониторинг поведения контейнера виртуализации во время его работы.

7.2.2 Проблемы и угрозы безопасности изоляции работающего контейнера виртуализации

Изоляция – базовый механизм обеспечения безопасности контейнера виртуализации. Согласно [ITU-T X.1605] выход за пределы VM, то есть использование уязвимостей интерфейсов между виртуальными машинами для управления самой VM или ее хостом – одна из главных проблем безопасности инфраструктуры как услуги (IaaS) в сфере облачных вычислений. Аналогичным образом, если изоляция не обеспечивает достаточную защиту, подсистема контейнеров виртуализации может подвергнуться атаке с выходом за пределы контейнера виртуализации, то есть злоумышленники могут воспользоваться скомпрометированным контейнером виртуализации для атак на другие такие контейнеры, работающие в той же ОС хоста, и далее атаковать саму эту ОС или же непосредственно хост.

Ненадлежащие действия по завершении работы контейнера виртуализации могут привести к возникновению других критически важных угроз безопасности: 1) возможна утечка оставшейся конфиденциальной информации к злоумышленникам; 2) если вычислительные или сетевые ресурсы не были освобождены надлежащим образом, другие контейнеры виртуализации могут не получить необходимых им ресурсов.

7.3 Проблемы и угрозы безопасности регистра контейнера виртуализации

В соответствии с определением, данным в [ITU-T X.1255], регистр – это механизм регистрации метаданных о цифровых объектах и хранения схем метаданных, обеспечивающий возможность поиска в регистре постоянных идентификаторов на основе использования схем метаданных. Кроме того, регистр контейнера виртуализации содержит идентификационные данные, важные для авторизации. Воспользовавшись ошибками в конфигурации средств безопасности или уязвимостями, злоумышленники могут неправомерно получить доступ к контейнеру виртуализации и полностью изменить или удалить его содержимое. В устаревшем программном обеспечении могут быть уязвимости, позволяющие получить несанкционированный доступ к регистру посредством атак с использованием программных закладок. Кроме того, злоумышленники могут получить доступ к регистру контейнера виртуализации, используя недочеты в управлении конфигурациями.

7.4 Проблемы и угрозы безопасности образа облачной услуги

В соответствии с определением, данным в [ITU-T Y.3508], образ облачной услуги – это исполняемый код с информацией о состоянии виртуальных машин или контейнеров виртуализации. Он включает в себя операционные системы, библиотеки, файлы данных, приложения и т. п. Кроме того, развертывание контейнеров виртуализации производится на основе образов облачной услуги, безопасность этих образов является необходимым условием безопасности контейнеров виртуализации. Образы облачных услуг подвержены следующим угрозам.

a) Программное обеспечение в составе образов облачных услуг может иметь уязвимости, которыми могут воспользоваться злоумышленники.

b) При ненадлежащих настройках может не сработать проверка целостности образа облачной услуги. Кроме того, ответственность за проверку целостности образа облачной услуги может возлагаться на разные стороны в зависимости от сценариев применения, в которых если пользователи развертывают контейнеры виртуализации на основе образов облачных услуг, предоставляемых поставщиками облачных услуг, то отвечают поставщики; если же пользователи берут образы облачных услуг для развертывания контейнеров виртуализации из других источников, например загружают из регистра, то отвечают сами пользователи.

c) Злоумышленники могут скрыто вносить изменения в файлы образов облачных услуг. Например, они могут внедрить в образ закладку или другое вредоносное программное обеспечение во время его размещения или загрузки.

7.5 Проблемы и угрозы безопасности операционной системы (ОС)

В виртуализированной контейнеризованной среде все контейнеры виртуализации совместно используют ядро ОС и другие ресурсы хост-системы, поэтому базовая ОС хоста представляет собой наиболее критичную мишень для атак. Если скомпрометирована ОС, то скомпрометированы и все контейнеры виртуализации. Кроме того, к каждому контейнеру виртуализации могут применяться средства контроля и политики безопасности хост-компьютера. Наконец, атаки с выходом за пределы

контейнеров, эксплуатирующие ошибки в коде приложений, могут обходить подсистему контейнеров виртуализации и получать доступ к ОС хоста и ее ядру, под контролем которого работают все прочие приложения.

7.6 Проблемы и угрозы безопасности системы управления оркестрацией контейнера виртуализации

В соответствии с определением, данным в [b-ITU-T Y.3100], оркестрация – это процессы, направленные на автоматическую организацию, координацию, реализацию и использование сетевых функций и ресурсов физической и виртуальной инфраструктуры по заданным критериям оптимизации. Это типичный пример технологии, используемой в виртуальных сетях, например в среде облачных вычислений. В облачной среде контейнеров виртуализации система управления оркестрацией позволяет управлять развернутыми в облаке контейнерами виртуализации большого размера. При этом она сталкивается со следующими проблемами и угрозами безопасности.

a) Злоупотребление привилегиями. Если политика безопасности системы управления оркестрацией не осуществляется на основе принципа наименьших привилегий, пользователи смогут использовать контейнеры виртуализации более свободно, нежели предполагают назначенные им привилегии, что влечет серьезные последствия для безопасности.

b) Несанкционированный доступ к открытым API. Открытые API и другие общедоступные сетевые ресурсы, например сетевые порты, открывают доступ к новым поверхностям атаки. Злоумышленники могут пользоваться уязвимостями открытых API, например недочетами в аутентификации, авторизации, проверке целостности и т. д., для получения доступа к функциям оркестрации контейнеров виртуализации и несанкционированно их запускать или изменять.

c) Компенсация отказа узла. Под отказом узла понимается ошибка, выражающаяся в отсутствии доступа к одному или нескольким узлам сети в системе управления оркестрацией. Ненадлежащая компенсация отказа узла может создать помехи работе других узлов и управлению оркестрацией. Злоумышленники могут этим воспользоваться во вредоносных целях и снизить качество оркестрации.

d) Управление конфигурацией. Система управления оркестрацией контейнера виртуализации задает различные конфигурации для огромного числа активов и разнообразных услуг, в связи с чем необходима высокоуровневая политика безопасности управления конфигурацией. Ненадлежащая конфигурация может привести к увеличению поверхности атаки и, соответственно, существенно повысить риски безопасности. Например, злоумышленники могут получить несанкционированный доступ к внутреннему программному обеспечению оркестрации через общедоступные приложения контейнеров виртуализации.

7.7 Проблемы и угрозы безопасности сети контейнеров виртуализации

Сеть контейнеров виртуализации, предназначенная для связи с другими контейнерами виртуализации на том же хосте или разных хостах, а также внутри контейнеров виртуализации, может работать в одном из двух типовых режимов – в режиме мостовой сети и режиме оверлейной сети.

В режиме мостовой сети каждому контейнеру виртуализации выделяется отдельное пространство имен и IP-адрес, что позволяет контейнеру связываться с хостом напрямую.

Согласно определению, данному в [ITU-T X.1162], оверлейная сеть – это виртуальная сеть, работающая поверх другой сети. Подобно любой другой сети, она состоит из набора узлов и связей между ними. Поскольку связи имеют логический характер, они могут соответствовать множеству физических каналов базовой сети. В облачной среде контейнеров виртуализации оверлейная сеть связывает между собой распределенные контейнеры виртуализации. А именно, она работает поверх базовой сети каждого хоста по технологии виртуальных расширяемых локальных сетей (VXLAN), позволяя соединять контейнеры виртуализации между собой и обеспечивая взаимодействие контейнеров, находящихся в разных хостах.

Распространенные проблемы и угрозы безопасности обоих сетевых режимов контейнеров виртуализации включают в себя следующее.

– **Атака типа отказ в обслуживании (DoS) или распределенный отказ в обслуживании (DDoS)**

Сеть контейнеров виртуализации подвержена угрозам DoS/DDoS-атак из внутренних и внешних сетей.

a) DoS/DDoS-атаки из внутренних сетей. Злоумышленник может воспользоваться скомпрометированными контейнерами виртуализации для проведения DoS/DDoS-атак на другие контейнеры виртуализации в той же сети, чтобы перегрузить их вычислительные ресурсы, например забить полосу пропускания сети, перегрузить ЦП и т. д.

b) DoS/DDoS-атаки из внешних сетей. Контейнеры виртуализации, располагающиеся на одном и том же хосте, совместно используют один набор физических сетевых адаптеров. Кроме того, если злоумышленник проведет DoS/DDoS-атаку на контейнер виртуализации путем передачи в его адрес большого числа пакетов с хост-компьютеров, являющихся частью бот-сети, это может привести не только к порче данного контейнера, но и к забиванию полосы пропускания сети хост-компьютера, результатом чего могут явиться DoS/DDoS-атаки на сам хост, а также другие контейнеры виртуализации.

– **Атака через посредника**

В виртуальных контейнерах в составе сети, работающей в том или ином режиме, изначально не предусмотрены механизмы шифрования, в результате чего эти контейнеры уязвимы в отношении атаки через посредника (MITM). Один из примеров такой атаки – это спуфинг, то есть, согласно определению, данному в [ITU-T X.1279], попытка объекта выдать себя за другой объект путем демонстрации записанного изображения, другого образца биометрических данных или искусственно полученной биометрической характеристики в целях имитации того или иного индивида. Злоумышленник может воспользоваться скомпрометированным контейнером виртуализации для атаки на другой контейнер виртуализации в той же виртуальной сети. Кроме того, если атака увенчается успехом, злоумышленник сможет перехватывать обычный сетевой трафик контейнера виртуализации, а затем провести ряд атак через посредника.

Разработчики приложений, работающих внутри контейнеров виртуализации, могут в инициативном порядке применять в них собственные средства шифрования, такие как протокол безопасности транспортного уровня (TLS) или протокол безопасности дейтаграмм транспортного уровня (DTLS). В этих случаях разработчик, которому известно, что трафик в контейнере виртуализации или между контейнерами виртуализации будет зашифрован, может отказаться от дополнительного шифрования. Цель этого подхода состоит в том, чтобы обеспечить максимальную защиту трафика внутри контейнера виртуализации, сведя при этом к минимуму накладные расходы вычислительных ресурсов на неоднократное шифрование одного и того же трафика.

Конкретные угрозы безопасности сетей контейнеров виртуализации, работающих в режиме мостовой сети и оверлейной сети, описаны в пунктах 7.7.1 и 7.7.2.

7.7.1 Режим мостовой сети контейнеров виртуализации

В режиме мостовой сети контейнер виртуализации подключается к виртуальной сети через свой виртуальный сетевой интерфейс, который позволяет ему связываться с хостом напрямую, а также действует в качестве первичного шлюза. Сетевые пакеты контейнера виртуализации вначале передаются на первичный шлюз, а затем маршрутизируются к другим контейнерам виртуализации. Контейнеры виртуализации, располагающиеся в одной виртуальной сети, соединены друг с другом.

Если для режима мостовой сети контейнеров виртуализации не установлена политика сетевой безопасности, управление доступом между контейнерами виртуализации отсутствует. В отсутствие межсетевого экрана и других механизмов защиты сети злоумышленник, имеющий доступ к одному контейнеру виртуализации, может с легкостью проводить различные атаки на другие контейнеры виртуализации, например, при помощи спуфинга, атаки с анализом пакетов и т. д., что чревато серьезными последствиями, такими как утечка конфиденциальной информации и т. п.

Из этого следует, что в отсутствие действенной политики управления доступом между контейнерами виртуализации, расположенными на одном и том же хосте, сеть контейнеров виртуализации, работающая в режиме мостовой сети, подвержена рискам, связанным с сетевой безопасностью.

7.7.2 Режим оверлейной сети контейнеров виртуализации

В режиме оверлейной сети контейнеров виртуализации нет изначально установленной политики управления доступом для контейнеров виртуализации. Кроме того, поскольку сетевой трафик VXLAN по умолчанию не шифруется, необходимо использовать другие протоколы туннелирования, например протокол безопасности IP (IPsec) и прочее для шифрования этого трафика и обеспечения безопасной передачи данных.

8 Требования безопасности и руководящие указания для безопасности контейнеров виртуализации в среде облачных вычислений

В этом разделе излагаются требования безопасности и руководящие указания по безопасности в соответствии с проблемами и угрозами безопасности контейнеров виртуализации, описанными в разделе 7.

8.1 Требования безопасности и руководящие указания по безопасности контейнеров виртуализации во время работы

a) При обновлении приложений или услуг требуется останавливать контейнеры виртуализации и заменять их новыми.

b) Следует использовать средства для поиска распространенных уязвимостей во внутренних средах выполнения контейнеров виртуализации. Все экземпляры, подверженные риску, должны быть обновлены.

c) Требуется исключить несанкционированный доступ пользователей к демону контейнера виртуализации.

8.2 Требования безопасности и руководящие указания по безопасности регистра контейнеров виртуализации

a) Следует усилить защиту сервера, на котором размещен регистр, чтобы снизить риск атак по этому направлению.

b) Следует настроить средства разработки, систему управления оркестрацией и контейнеры виртуализации таким образом, чтобы они подключались к регистрам только через шифрованные каналы связи.

c) Следует очищать регистры от небезопасных, уязвимых образов облачных услуг, которые не должны использоваться в дальнейшем.

d) При любом доступе к регистру следует проводить аутентификацию, чтобы в него можно было добавлять только образы облачных услуг из доверенных источников.

8.3 Требования безопасности и руководящие указания по безопасности образов облачных услуг для создания контейнеров виртуализации

a) Образы облачных услуг предназначены для создания (запуска) контейнеров виртуализации приложений или услуг. Запрещается использовать образы облачных услуг, имеющие другое назначение.

b) Следует проверять подписи на образе облачных услуг перед их запуском, чтобы удостовериться, что образы происходят из доверенных источников и не претерпели несанкционированных изменений.

c) Следует реализовать непрерывный мониторинг и техническое обслуживание регистров для перенастройки и обновления хранящихся в них образов облачных услуг по мере изменения актуального набора уязвимостей и требований к конфигурации.

d) Следует организовать доступ к образам облачных услуг только по неизменяемым именам, содержащим указание на конкретную версию образа.

8.4 Требования безопасности и руководящие указания по безопасности ОС хоста контейнеров виртуализации

a) Следует сократить число векторов атаки, удалив из среды хост-компьютера все компоненты, кроме действительно необходимых.

b) Запрещается запускать в одном и том же экземпляре ОС хоста рабочие нагрузки, контейнеризованные на основе виртуализации и на основе других методов.

c) Следует валидировать версию ОС хоста, внедрив соответствующие практики и средства управления.

d) Следует вести аудит всех попыток аутентификации доступа к ОС.

e) Следует обеспечить, чтобы контейнеры виртуализации работали с минимально необходимым набором разрешений на доступ к файловой системе. Любые изменения файлов ОС хоста контейнера виртуализации следует выполнять в рамках политик авторизации.

8.5 Требования безопасности и руководящие указания по безопасности системы управления оркестрацией контейнеров виртуализации

a) Следует устанавливать систему управления оркестрацией из официального, доверенного, актуального источника.

b) Следует по мере возможности настраивать систему управления оркестрацией так, чтобы обеспечить ее высокую доступность и автоматическое переключение в случае отказа.

c) Следует использовать для системы управления оркестрацией модель доступа с наименьшими привилегиями, в которой пользователю предоставляются права на выполнение конкретных действий с конкретными хост-компьютером, контейнером виртуализации и образом облачной услуги.

d) Следует применять для административных учетных записей системы управления оркестрацией надежные методы аутентификации, например требовать многофакторной аутентификации, а не просто предъявления пароля.

e) Следует настраивать систему управления оркестрацией так, чтобы сетевой трафик разделялся на отдельные виртуальные сети по уровням конфиденциальности.

f) Следует настраивать систему управления оркестрацией так, чтобы изолировать развертывание на конкретных наборах хост-компьютеров по уровням конфиденциальности.

8.6 Требования безопасности и руководящие указания по безопасности контейнеров виртуализации в различных сетевых режимах

8.6.1 Ограничение трафика внутри контейнера виртуализации в режиме мостовой сети контейнеров виртуализации

При заданной по умолчанию конфигурации безопасности контейнера виртуализации в режиме мостовой сети отсутствует управление доступом и ограничение доступа к сети. Чтобы предотвратить угрозы DoS/DDoS-атак, следует установить политики управления доступом к сети в соответствии с фактическими требованиями, включая следующее.

a) Требуется полностью запретить связь между контейнерами виртуализации, если это возможно. В конкретных прикладных сценариях, если нет необходимости в том, чтобы у всех контейнеров виртуализации была сетевая связь друг с другом, можно запретить связь между ними путем изменения заданной по умолчанию конфигурации безопасности.

b) Следует установить политики управления доступом между контейнерами виртуализации. В облачной среде контейнеров виртуализации, когда ресурсы распределяются между множеством арендаторов, возможна ситуация, когда один контейнер занимает множество хостов и забивает полосу пропускания других контейнеров. Чтобы обеспечить регулярную связь между контейнерами виртуализации и избежать аномального трафика, вызванного DoS/DDoS-атаками, следует ограничить механизмы передачи трафика между контейнерами.

c) Следует реализовать механизмы и политики шифрования, например использовать протокол IPsec для шифрования трафика и обеспечения конфиденциальности связи между контейнерами виртуализации, чтобы предотвратить анализ пакетов и атаки через посредника.

8.6.2 Управление доступом между контейнерами виртуализации

a) Управление доступом в режиме мостовой сети контейнеров виртуализации

В режиме мостовой сети заданная по умолчанию конфигурация безопасности контейнеров виртуализации позволяет разным контейнерам подключаться к одной и той же виртуальной сети и связываться друг с другом напрямую. Поэтому для предотвращения несанкционированного доступа следует реализовать механизмы и установить политики управления доступом в соответствии с потребностями, включая следующее.

1) Следует настроить для контейнеров виртуализации разные виртуальные сети, чтобы обеспечить сетевую изоляцию между контейнерами. При этом будет блокироваться межсетевой трафик, то есть цель изоляции сетей контейнеров виртуализации будет достигнута.

2) Следует реализовать управление доступом на основе политики белого списка, чтобы обеспечить безопасность сети между контейнерами виртуализации. Следует по умолчанию запретить связь между контейнерами виртуализации, а для тех случаев, когда она необходима, настроить соответствующие правила управления доступом. Управление доступом на основе политики белого списка уменьшает поверхность атаки за счет минимизации доступа.

b) Управление доступом в режиме оверлейной сети контейнеров виртуализации

В режиме оверлейной сети контейнеров виртуализации разные контейнеры, находящиеся в одной подсети и на одном хосте, могут непосредственно связываться друг с другом. Для управления доступом с внешних хост-компьютеров к внутренним приложениям контейнеров виртуализации следует вручную задать правила доступа по списку управления доступом (ACL) в политиках управления доступом на хосте или развернуть межсетевой экран на хост-компьютере.

В большой по размерам облачной среде контейнеров виртуализации ручное обновление правил межсетевого экрана может оказаться неосуществимым на практике из-за частого динамического обновления микросервисов [b-ITU-T J.1301]. Рекомендуется применять те или иные методы или средства автоматического управления этим процессом, например микросегментацию контейнера виртуализации – метод защиты межсетевым экраном контейнера виртуализации с использованием высокодетализированных механизмов сетевой изоляции на базе сегментирования, который позволяет изолировать путем сегментирования одиночный контейнер виртуализации, контейнеры виртуализации в пределах одной и той же подсети или приложения контейнеров виртуализации и реализовать соответствующие политики управления доступом.

Библиография

[b-ITU-T H.350.4] Recommendation ITU-T H.350.4 (2011), *Directory services architecture for SIP.*

[b-ITU-T J.1301] Recommendation ITU-T J.1301 (2021), *Specification of cloud-based converged media service to support Internet protocol and broadcast cable television – Requirements.*

[b-ITU-T L.1362] Recommendation ITU-T L.1362 (2019), *Interface for power management in network function virtualization environments – Green abstraction Layer version 2.*

[b-ITU-T Q.1743] Recommendation ITU-T Q.1743 (2016), *IMT-Advanced references to Release 11 of LTE-Advanced evolved packet core network.*

[b-ITU-T X.800] Рекомендация МСЭ-T X.800 (1991 г.), *Архитектура безопасности для взаимосвязи открытых систем для приложений МККТТ.*

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview.*

[b-ITU-T X.1162] Recommendation ITU-T X.1162 (2008), *Security architecture and operations for peer-to-peer networks.*

[b-ITU-T X.1251] Рекомендация МСЭ-T X.1251 (2019 г.), *Структура осуществляемого пользователем управления в отношении цифровой идентичности.*

[b-ITU-T X.1255] Рекомендация МСЭ-T X.1255 (2013 г.), *Структура обнаружения информации по управлению определением идентичности.*

[b-ITU-T X.1279] Рекомендация МСЭ-T X.1279 (2020 г.), *Система расширенной аутентификации с использованием телебиометрии с антиспуфинговыми механизмами обнаружения.*

[b-ITU-T X.1604] Рекомендация МСЭ-T X.1604 (2020 г.), *Требования безопасности к сети как услуге (NaaS) в среде облачных вычислений.*

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network.*

[b-ITU-T Y.3500] Рекомендация МСЭ-T Y.3500 (2014 г.), *Информационные технологии – Облачные вычисления – Обзор и терминология.*

[b-ITU-T Y.3502] Рекомендация МСЭ-T Y.3502 (2014 г.), *Информационные технологии – Облачные вычисления – Эталонная архитектура.*

[b-ITU-T Y.4500.1] Recommendation ITU-T Y.4500.1 (2018), *oneM2M – Functional architecture.*

[b-ITU-R BT.1699] Рекомендация МСЭ-R BT.1699 (2013 г.), *Согласование форматов декларативных приложений для интерактивного ТВ.*

[b-ISO/IEC 19944] ISO/IEC 19944:2016, *Information technology – Cloud services and devices: Data flow, data categories and data use.*

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology –Security techniques – Information security management systems – Overview and vocabulary.*

[b-ISO/IEC 27729] ISO/IEC 27729:2012, *Information and documentation – International standard name identifier (ISNI).*

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework.*

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет, сети последующих поколений, интернет вещей и умные города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2022 г.