Международный союз электросвязи
Сектор стандартизации

Рекомендация

МСЭ-Т X.1644 (03/2023)

СЕРИЯ X: Сети передачи данных, взаимосвязь открытых систем и безопасность

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

Руководящие указания по обеспечению безопасности распределенного облака

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.1644

Руководящие указания по обеспечению безопасности распределенного облака

Резюме

В Рекомендации МСЭ-Т X.1644 приведен анализ угроз и проблем безопасности в распределенном облаке и представлены руководящие указания по обеспечению безопасности в отношении таких угроз, включая руководящие указания по обеспечению безопасности базового облака, регионального облака и периферийного облака.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1644	03.03.2023 г.	17-я	11.1002/1000/15112

Ключевые слова

Облачные вычисления, распределенное облако, руководящие указания по обеспечению безопасности

* 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/авторскими правами на программное обеспечение, 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 соответствующим базам данных МСЭ-Т, доступным на веб-сайте МСЭ-Т по адресу http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1644

Руководящие указания по обеспечению безопасности распределенного облака

1 Сфера применения

В настоящей Рекомендации приведен анализ угроз в распределенном облаке и предлагаются руководящие указания по обеспечению безопасности в отношении таких угроз.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылки 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 источников, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[ITU-T X.1408] Recommendation ITU-T X.1408 (2021), *Security threats and requirements for data access and sharing based on the distributed ledger technology*.

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

[ITU-T Y.3500] Рекомендация МСЭ-Т Y.3500 (2014 г.) | ISO/IEC 17788:2014, *Информационные технологии – Облачные вычисления – Обзор и терминология.*

[ITU-T Y.3508] Recommendation ITU-T Y.3508 (2019), *Distributed cloud overview and high-level requirements.*

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 тип облачных возможностей (cloud capabilities type) [ITU-T Y.3500]: Классификация функций, предоставляемых облачной услугой клиенту облачной услуги на основании используемых ресурсов.

ПРИМЕЧАНИЕ. – Типы облачных возможностей – это тип возможностей приложения, тип возможностей инфраструктуры и тип возможностей платформы.

3.1.2 облачные вычисления (cloud computing) [ITU-T Y.3500]: Парадигма обеспечения сетевого доступа к масштабируемому и гибкому набору совместно используемых физических или виртуальных ресурсов с предоставлением и администрированием ресурсов на основе самообслуживания по запросу.

3.1.3 облачная услуга (cloud service) [ITU-T Y.3500]: Одна или несколько возможностей, предоставляемых с использованием облачных вычислений, которые активируются с помощью заявленного интерфейса.

3.1.4 потребитель облачной услуги (cloud service customer) [ITU-T Y.3500]: Сторона, которая состоит в деловых отношениях в целях использования облачной услуги.

ПРИМЕЧАНИЕ. – Деловые отношения не обязательно предполагают наличие финансовых соглашений.

3.1.5 поставщик облачной услуги (cloud service provider) [ITU-T Y.3500]: Сторона, которая предоставляет облачные услуги.

3.1.6 периферийное облако (edge cloud) [ITU-T Y.3508]: Облачные вычисления, развернутые на периферии сети и обеспечивающие облачные услуги с малой ресурсоемкостью для потребителей облачных услуг (CSC).

ПРИМЕЧАНИЕ 1. – В периферийном облаке доступны облегченные облачные услуги, предоставляемые поставщиками облачных услуг (CSP) той или иной категории.

ПРИМЕЧАНИЕ 2. – Облегченной облачной услугой называется часть облачной услуги, предназначенная для перенастройки функциональных возможностей в целях применения этой облачной услуги в периферийном облаке, например в базовой станции или шлюзе с ограниченным ресурсом емкости.

3.1.7 угроза (threat) [ITU-T X.1408]: Потенциальная причина нежелательного инцидента, который может нанести ущерб системе или организации.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации используются следующие термины:

3.2.1 базовое облако (core cloud): Централизованный набор услуг, который включает любые услуги, не зависящие от географического местоположения, услуги, не чувствительные к задержкам, услуги с высокой вычислительной нагрузкой, услуги резервного копирования и восстановления данных, а также услуги с высоким уровнем защиты.

3.2.2 распределенное облако (distributed cloud): Расширение классических концепций облачных вычислений, распространяющее возможности облачных вычислений на периферию сети.

3.2.3 региональное облако (regional cloud): Базовое облако, которое может быть развернуто для достижения эффективной общей конфигурации базового облака и периферийного облака в целях снижения нагрузки на базовое облако.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

API	Application Service Interface	Интерфейс службы приложений
CC	Core Cloud	Базовое облако
CSC	Cloud Service Customer	Потребитель облачных услуг
CSP	Cloud Service Provider	Поставщик облачных услуг
DDoS	Distributed Denial of Service	Распределенный отказ в обслуживании
DoS	Denial of Service	Отказ в обслуживании
EC	Edge Cloud	Периферийное облако
IoT	Internet of Thing	Интернет вещей
OTA	Over-The-Air	Беспроводная связь
REST	Representational State Transfer	Передача репрезентативного состояния
TLS	Transport Layer Security	Безопасность транспортного уровня
VPN	Virtual Private Network	Виртуальная частная сеть
XML	Extensible Markup Language	Расширяемый язык разметки
XSS	Cross Site Scripting	Межсайтовый скриптинг

5 Соглашения по терминологии

В настоящей Рекомендации:

ключевое слово "**требуется**" означает требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящему документу;

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

6 Обзор

Распределенное облако образуется, когда для все более и более чувствительных к задержке услуг (таких, как услуги передачи видеоизображения и интернета вещей (IoT)) требуются гораздо более высокие скорости реакции; это расширение традиционных облачных вычислений, распространяющее их возможности на периферию сети. Оно позволяет предоставлять локализованные облачные услуги, значительно приблизив их к пользователю и источнику данных, а также взаимодействовать с другими облаками для предоставления распределенных высокоскоростных услуг с короткой задержкой.

Распределенное облако предусматривает распространение облачных функций на периферию сети для предоставления облачных услуг с короткой задержкой и возможностью обработки данных в режиме реального времени в ограниченной полосе пропускания за счет взаимодействия между элементами пула физических или виртуальных ресурсов [ITU-T Y.3508]. Типичное распределенное облако показано на рисунке 6-1 и включает в себя базовое облако, региональное облако и периферийное облако.

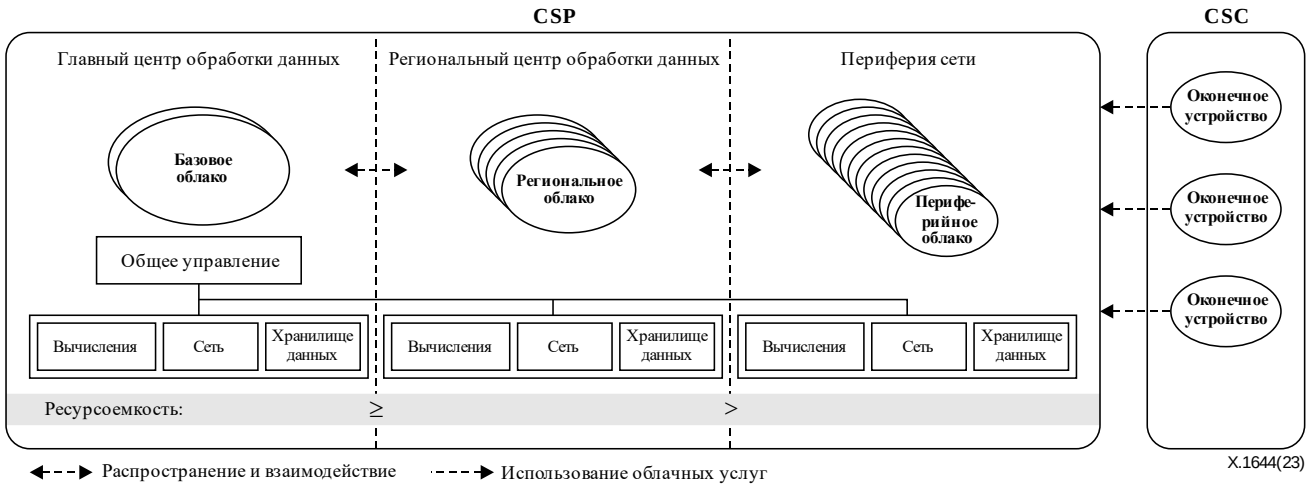

Рисунок 6-1 – Концепция распределенного облака

Базовое облако обладает большой ресурсоемкостью и имеет общий центр управления для управления облачными ресурсами в распределенном облаке. Базовое облако поддерживает облачные услуги с высокоинтенсивными вычислениями, не зависящие от географического местоположения.

Региональное облако может быть развернуто в отдельных регионах из основного облака для распределения нагрузки и повышения качества обслуживания. Региональное облако обрабатывает запросы облачных услуг внутри региона под общим управлением, осуществляемым из базового облака.

ПРИМЕЧАНИЕ 1. – Региональное облако обеспечивает более короткую задержку, чем базовое облако, предоставляя оптимизированные облачные услуги потребителям облачных услуг (CSC) в данном регионе. Предполагается, что время задержки при передаче данных по сети от CSC до регионального облака меньше, чем от CSC до базового облака, и что разница во времени обработки данных при выполнении облачных услуг в базовом и в региональном облаках пренебрежимо мала.

ПРИМЕЧАНИЕ 2. – Региональное облако обеспечивает буферизацию нагрузки облачных услуг и кеширование данных из базового облака и предоставляет их CSC, расположенным в регионе.

Периферийное облако развертывается на периферии сети – там, где к ней обращаются CSC, – и имеет небольшую ресурсоемкость. Для периферийного облака требуются узкоспециализированные целевые аппаратные ресурсы, т. е. ресурсы периферийного облака ограниченны ввиду ограниченности доступных площадей или электроэнергии. Периферийное облако может иметь разные конфигурации ресурсов и обеспечивать разные облачные функции с использованием физических и виртуальных ресурсов в зависимости от требований, предъявляемых CSC к облачным услугам, и условий в среде развертывания.

7 Вызовы и угрозы безопасности для распределенного облака

Использование распределенного облака дает преимущества высокого быстродействия, высокой эффективности и лучших характеристик. Наличие базового, региональных и периферийных облаков в составе распределенного облака создают новые проблемы и угрозы безопасности [ITU-T X.1601].

7.1 Проблемы и угрозы безопасности, характерные для базового облака

Распределенное облако отличается неравномерной инфраструктурой: у базового или регионального облака большая ресурсоемкость, а у периферийного – ограниченная. Базовое облако функционирует на основе неоднородной инфраструктуры, служащей единой системой предоставления CSC различных услуг в распределенном облаке. Для базового облака характерны следующие проблемы безопасности и угрозы.

a) **Системные уязвимости**. В распределенной облачной инфраструктуре имеются системные уязвимости, особенно в сетях со сложной инфраструктурой и несколькими сторонними платформами, а уязвимость базового облака также затрагивает региональное и периферийное облако.

b) **Физическое повреждение**. Распределенная облачная инфраструктура может быть развернута в ненадежной физической среде и подвергнуться физическому повреждению в результате действий злоумышленников, плохих погодных условий или землетрясения. Физическое повреждение базового облака также может повлиять на безопасность регионального и периферийного облака.

7.2 Проблемы и угрозы безопасности, характерные для регионального облака

a) **Перехват данных при передаче**. Базовому облаку необходимо обмениваться данными с региональными облаками, и эти каналы передачи данных могут подвергнуться взлому. b) **Подложный заказ или запрос**. В результате вредоносного заказа или запроса из подложного базового, регионального или периферийного облака может произойти утечка данных.

c) **Атака через интерфейс**. Поскольку базовое облако связано с несколькими региональными облаками через открытые интерфейсы, оно может подвергнуться атаке через эти интерфейсы.

d) **Атака типа "черная дыра"**. Злоумышленник может взломать устройство или внедрить в сеть подложное устройство, а затем использовать его для атаки типа "черная дыра". Это атака на уровне сети, когда взломанное устройство передает соседним устройствам ложную информацию о маршрутизации, чтобы замкнуть сетевой трафик на себя.

e) **Несанкционированные шлюзы**. Злоумышленник может легко установить несанкционированный шлюз. Если удастся обманным путем подключить легитимное устройство к такому шлюзу, можно собрать конфиденциальную информацию о соединении. Это позволит эффективно обойти многие применяемые меры безопасности и вызвать радиопомехи в служебном оборудовании организации.

f) **Несанкционированный доступ к шлюзам IoT**. Злоумышленник может получить несанкционированный доступ к шлюзам IoT, что чревато раскрытием конфиденциальной информации, внесением изменений в данные и незаконным использованием некоторых ресурсов в периферийном облаке.

7.3 Проблемы и угрозы безопасности, характерные для периферийного облака

a) **Проблемы, связанные с наличием нескольких арендаторов**. Многие облачные решения не обеспечивают необходимой защитной изоляции между клиентами, что приводит к совместному использованию ресурсов, приложений и систем. В этой ситуации угрозы могут исходить от других пользователей облачных услуг и угрозы, затрагивающие одного клиента, могут повлиять и на других.

b) **Подложный запрос**. Запрос, поступивший из поддельного регионального или периферийного облака, может привести к утечке данных, если базовое облако не обнаружит подлог.

c) **Атака с использованием межсайтового скриптинга (XSS)**. При атаке с применением сценариев межсайтового скриптинга в компьютеры клиентов внедряется вредоносный код, использующий уязвимости веб-сайтов, и выполняются вредоносные действия от имени пользователей.

d) **Упаковка кода на расширяемом языке разметки (XML)**. XML – это преимущественный язык разметки, который допускает аутентификацию источника для приложений в периферийном облаке. Хакеры могут организовывать атаки по захвату учетных записей, используя методы упаковки перезаписанного кода XML или цифровой подписи.

e) **Халатность сотрудников**. Халатность сотрудников остается одной из самых серьезных проблем безопасности всех систем, но для системы управления распределенным облаком эта проблема является наиболее острой. Сотрудники могут входить в систему управления распределенного облака со своих мобильных телефонов, домашних планшетов или ПК, что делает систему уязвимой для многих внешних угроз.

f) **Атаки на основе фишинга и социальной инженерии**. Ввиду открытости распределенной облачной системы особенно широко распространены атаки на основе фишинга и социальной инженерии. Получив данные, необходимые для входа в систему, или другую конфиденциальную информацию, злоумышленник может легко проникнуть в эту систему.

g) **Потеря контроля**. Когда службы организации размещаются в распределенном облаке, они теряют контроль и лишаются информации о том, где именно в облаке хранятся их данные. Это становится серьезной проблемой безопасности, поскольку пользователи не осведомлены о каких-либо механизмах, способных защитить их услуги.

h) **Подмена устройств**. Злоумышленник может замаскироваться под легитимное устройство и отправлять в периферийное облако подложные или вредоносные данные или похищать данные у пользователей.

i) **Захват периферийного устройства**. Вокруг периферийного облака расположено множество оконечных устройств, которые могут собирать данные, передавать данные в периферийное облако и получать результаты или команды из периферийного облака. Оконечное устройство легко поддается взлому в силу его слабой защиты.

j) **Атака типа "распределенный отказ в обслуживании" (DDoS)**. Эффективность DDoS-атак на распределенные облака значительно возросла. Если на систему облачных вычислений обрушивается достаточное количество вредоносного трафика, она может полностью выйти из строя или получить повреждения. В частности, периферийное облако представляет собой относительно меньший облачный объект с относительно более слабой защитой безопасности, поэтому оно с большей вероятностью может быть атаковано хакерами с использованием DDoS-атак или других неправомерных действий.

k) **Защитная виртуализация.** Защитная виртуализация в периферийной облачной среде подразумевает изоляцию и усиление защиты периферийных шлюзов, контроллеров и серверов, выполненных на основе технологии виртуализации. По сравнению с базовым и региональным облаками, таким периферийным узлам с ограниченными ресурсами хранения и вычислительными ресурсами угрожают более сложные и масштабные векторы атак.

8 Руководящие указания по обеспечению безопасности распределенного облака

В этом разделе содержатся руководящие указания по обеспечению безопасности базового, регионального и периферийного облаков в составе распределенных облачных систем, описанных в разделе 6.

8.1 Руководящие указания по обеспечению безопасности базового облака

Руководящие указания по обеспечению безопасности базового облака относятся к обеспечению безопасности системы базового облака, физической безопасности, защите от атак типа "отказ в обслуживании" и безопасности периферийных устройств.

8.1.1 Безопасность системы базового облака

Руководящие указания по обеспечению безопасности системы базового облака состоят в следующем:

a) рекомендуется использовать инструменты реагирования на инциденты, связанные с уязвимостями;

b) рекомендуется предотвращать проникновение вредоносных программ в облачные услуги с помощью таких методов, как сканирование файлов, добавление приложений в белый список, обнаружение вредоносных программ на основе машинного обучения и анализ сетевого трафика;

c) рекомендуется пересматривать и обновлять оценки рисков, включая в них облачные услуги, а также выявлять и устранять факторы риска, создаваемые системами и поставщиками базового облака. Для ускорения процесса оценки имеются базы данных рисков, связанных с поставщиками облачных услуг.

8.1.2 Физическая защита

Руководящие указания по физической защите состоят в следующем:

a) рекомендуется создавать инфраструктуру базового облака в подходящих местах, исключая такие зоны, как траектории посадки воздушных судов в районах аэропортов, электростанции, поймы рек, линии разломов при землетрясениях или другие места, где могут происходить стихийные бедствия;

b) для подземной инфраструктуры рекомендуется предусмотреть процессы регулирования, поддержания и контроля физических условий окружающей среды;

c) для подземной инфраструктуры рекомендуется предусмотреть системы охлаждения и обеспечить соблюдение стандартов соответствия;

d) для того чтобы снизить риск физического взлома, рекомендуется ограничить количество точек входа из инфраструктуры базового облака;

e) рекомендуется предусмотреть несколько контрольных точек в инфраструктуре базового облака, чтобы свести к минимуму риск получения доступа злоумышленниками;

f) рекомендуется обеспечить дополнительную физическую защиту с использованием системы видеонаблюдения;

g) рекомендуется использовать резервирование, чтобы инфраструктура базового облака могла выдержать любой инцидент при минимальном времени простоя.

8.1.3 Защита от атак типа "отказ в обслуживании"

Руководящие указания по защите от атак типа "отказ в обслуживании" состоят в следующем:

a) рекомендуется, чтобы производительность сервера базового облака позволяла справляться с резкими скачками трафика и располагала средствами смягчения последствий, необходимыми для решения проблем безопасности;

b) рекомендуется регулярно обновлять и вносить исправления в брандмауэры и программы защиты сети.

8.2 Руководящие указания по обеспечению безопасности регионального облака

Рекомендации по обеспечению безопасности регионального облака включают рекомендации по обеспечению безопасности передаваемых и статических данных, открытого интерфейса и шлюза IoT.

8.2.1 Безопасность передаваемых и статических данных

Региональное облако предоставляет все или часть услуг базового облака в определенном географическом регионе. Руководящие указания по обеспечению безопасности передаваемых и статических данных в региональном облаке состоят в следующем:

a) требуется, чтобы в региональном облаке для шифрования сообщений и данных применялось шифрование с определенной степенью надежности. Также рекомендуется, чтобы поддерживались службы защищенного протокола передачи данных для предотвращения нарушения конфиденциальности в результате атак на основе протокола;

b) требуется, чтобы в региональном облаке выполнялись аутентификация и идентификация идентификаторов услуг, а также применялись строгая защитная изоляция и стратегии контроля доступа. Требуется, чтобы поддерживалась настройка стратегий контроля доступа и управления ими;

c) рекомендуется, чтобы в региональном облаке поддерживалась безопасная система обмена данными для обеспечения мониторинга и контроля в режиме реального времени форматов данных, контента, потоков и т. д.;

d) рекомендуется, чтобы система безопасного обмена данными соответствовала различным требованиям гибкости в облачной среде, включая гибкие методы развертывания, гибкие режимы планирования ресурсов, безопасные методы обмена данными, основанные на строгой защитной изоляции между отдельными предприятиями, и т. д.;

e) рекомендуется, чтобы региональное облако поддерживало обнаружение вредоносного кода и удаление передаваемых данных;

f) требуется наличие механизмов шифрования и проверки для обеспечения целостности и конфиденциальности локального хранилища данных, включая данные управления системой (такие, как файлы указателей, информация об облачных услугах и ключи), информацию аутентификации и важные деловые данные (например, данные, относящиеся к конфиденциальности пользователей);

g) рекомендуется, чтобы поддерживалась аутентификация на основе ролей для доступа к данным и принимались строгие меры контроля доступа во избежание несанкционированного доступа.

8.2.2 Безопасность открытого интерфейса

Поставщик облачных услуг (CSP) должен предоставить сетевые интерфейсы и интерфейсы прикладного программирования (API) в целях обеспечения возможности настройки, управления, координации и контроля различных облачных услуг, а также предоставления услуг напрямую. На основе этих интерфейсов третьи стороны обычно разрабатывают средства для предоставления дополнительных услуг. Руководящие указания по обеспечению безопасности API регионального облака состоят в следующем:

a) требуется использовать шифрование, например на основе протокола безопасности транспортного уровня (TLS), или другие методы шифрования для API на основе передачи репрезентативного состояния (REST) для шифрования данных во время передачи и предотвращения подлога. Также требуется использовать механизм цифровой подписи, чтобы расшифровывать и изменять данные могли только пользователи, обладающие правами доступа;

b) рекомендуется установить надежные удостоверения API с использованием токенов, чтобы возможность доступа к услугам, ресурсам данных и т. д. и управления ими обеспечивали только надежные удостоверения с токеном;

c) рекомендуется осуществлять мониторинг в режиме реального времени и выдавать предупреждения о поведении вызовов открытого API-интерфейса и аномалиях передачи данных, таких как ограничение частоты доступа к API-интерфейсу;

d) рекомендуется активно выявлять уязвимости API. Для обнаружения угроз безопасности API и утечки данных, а также для отслеживания в режиме реального времени атак на API и использования каких-либо уязвимостей могут применяться специальные инструменты;

e) рекомендуется использовать шлюзы безопасности API, поскольку они стали ключевой технологией, применяемой для обеспечения безопасности API. Так как шлюзы безопасности API можно использовать для контроля и управления использованием API-интерфейсов, они также могут аутентифицировать пользователей, работающих с API-интерфейсами и услугами.

8.2.3 Безопасность шлюза интернета вещей

Устройства IoT подключаются к интернету через шлюзы IoT, которые становятся основной мишенью для вредоносных программ и сетевых атак. Руководящие указания по обеспечению безопасности шлюзов IoT состоят в следующем:

a) рекомендуется, чтобы шлюзы IoT поддерживали аутентификацию устройств и управление доступом; доступ и создание безопасных хранилищ для защиты конфиденциальной информации, такой как ключи и сертификаты, должны быть разрешены только авторизованным пользователям и устройствам;

b) рекомендуется, чтобы шлюзы IoT поддерживали управление правилами настройки прав доступа и контроля доступа устройств к услугам приложений (техническим, деловым, информационным услугам), файлам (файлам конфигурации, журналам событий, файлам зеркала) и другим объектам в соответствии с политикой безопасности, и чтобы шлюз мог вовремя прервать несанкционированное соединение или сеанс;

c) рекомендуется, чтобы шлюзы IoT поддерживали обновление по каналам беспроводной связи (OTA), чтобы гарантировать использование новейшего программного и микропрограммного обеспечения шлюза для устранения известных уязвимостей и рисков. Безопасная загрузка может гарантировать, что шлюз будет загружен из образа микропрограммы, целостность и подлинность которого гарантированы шифрованием и проверкой, во избежание использования для загрузки шлюза вредоносной микропрограммы;

d) рекомендуется, чтобы шлюзы IoT поддерживали различные меры безопасности для защиты устройств IoT. Например, когда в качестве прокси-сервера безопасности для сетей и устройств используется шлюз IoT, рекомендуется, чтобы в этом шлюзе были установлены функции брандмауэра, фильтрации трафика на основе правил и белого списка;

e) рекомендуется, чтобы шлюзы IoT поддерживали подробные журналы событий, дающие более глубокое представление о процессах, запущенных в шлюзе, в целях проверки безопасности.

8.3 Руководящие указания по обеспечению безопасности периферийного облака

Руководящие указания по обеспечению безопасности периферийного облака включают руководящие указания по обеспечению безопасности инфраструктуры периферийного облака, передаваемых и статических данных в сети периферийного облака, веб-безопасности и безопасности оконечных устройств, располагаемых вблизи периферийного облака.

8.3.1 Безопасность инфраструктуры периферийного облака

Инфраструктура периферийного облака обеспечивает как аппаратную, так и программную основу, и обеспечение безопасности периферийной инфраструктуры – фундаментальное требование периферийного облака. Руководящие указания по обеспечению безопасности инфраструктуры периферийного облака состоят в следующем:

a) рекомендуется обеспечить облегченную аппаратно независимую платформу виртуализации и реализовать механизмы изоляции и усиления защиты;

b) рекомендуется усилить защиту гипервизора и уменьшить векторы атак;

c) рекомендуется во взаимодействии с серверами периферийного облака обеспечить обнаружение и предотвращение возможности проникновения вредоносного кода в ОС, строгую изоляцию приложений, поддержку доверенной среды выполнения и другие важные механизмы, чтобы гарантировать конфиденциальность и целостность приложений, работающих поверх ОС в условиях ограниченных вычислительных ресурсов или ресурсов хранения данных, так что правила и механизмы обеспечения безопасности могут не синхронизироваться с базовым или региональными облаками;

d) рекомендуется, чтобы поставщики услуг периферийного облака реализовывали автоматические, прозрачные и упрощенные процессы идентификации и аутентификации, поскольку периферийные узлы и динамическая сетевая структура распределенного облака могут вызывать повторную идентификацию и аутентификацию.

8.3.2 Безопасность сети периферийного облака

Ввиду большого количества периферийных узлов и сложной топологии сети, что увеличивает количество путей атак, злоумышленники могут легко отправлять вредоносные сетевые пакеты в узлы периферийного облака или инициировать атаки типа "отказ в обслуживании", подрывающие надежность сети периферийного облака. Руководящие указания по обеспечению безопасности сети периферийного облака состоят в следующем:

a) рекомендуется обеспечить безопасность протокола – как на этапах проектирования, так и на этапах реализации, – который используется периферийным облаком для удовлетворения различных требований по передаче данных для CSC;

b) рекомендуется ввести дополнительные правила безопасности для потенциально уязвимых протоколов, например, реализовав передачу данных через виртуальную частную сеть (VPN), TLS или другие защищенные каналы путем добавления модулей в шлюзы;

c) рекомендуется выполнять проверку целостности и безопасности передачи по сети между виртуальными машинами, принадлежащими к разным доменам, чтобы обеспечить эффективную изоляцию между различными элементами системы бизнес-коммуникаций. Кроме того, для обеспечения возможностей изоляции создание модулей изоляции может планироваться контроллерами в визуализированной среде;

d) рекомендуется выполнять мониторинг безопасности сетевого трафика, чтобы вовремя предупреждать о событиях безопасности и эффективно реагировать на инциденты. Кроме того, системы защиты могут напрямую блокировать вредоносный трафик.

8.3.3 Безопасность периферийного облака в киберпространстве

Руководящие указания по обеспечению безопасности периферийного облака в киберпространстве состоят в следующем:

a) рекомендуется обеспечить эффективный удаленный мониторинг объектов системы периферийного облака;

b) рекомендуется, чтобы обеспечение безопасности периферийного облака сопровождалось активными усилиями по обучению персонала. Сотрудников информируют о том, что они могут и чего не могут делать со своими устройствами, а также помогают им выявить риски безопасности;

c) рекомендуется следить за тем, чтобы устаревшие устройства не располагались рядом с более сложными, с тем чтобы уменьшить количество точек уязвимости в сети.

8.3.4 Безопасность оконечных устройств в периферийном облаке

Руководящие указания по обеспечению безопасности оконечных устройств в периферийном облаке состоят в следующем:

a) когда неавторизованное персональное устройство пытается получить доступ к данным периферийного облака, рекомендуется блокировать его;

b) рекомендуется наделить периферийное устройство такими функциями, как строгая аутентификация и узлы аутентификации с шифрованием;

c) рекомендуется, чтобы протоколы ИТ-безопасности контролировали, какие устройства могут получить доступ к сети системы периферийного облака и при каких условиях;

d) рекомендуется реализовать и постоянно контролировать среду периферийного облака;

e) рекомендуется исходить из предположения, что периферийные устройства уже взломаны, и не доверять автоматически информации, поступающей от них, поскольку, пока не доказано обратное, все данные могут быть ложными;

f) рекомендуется, чтобы подключаться и передавать данные в базовое облако могли только аутентифицированные периферийные устройства.

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, 2023 г.