Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1643

(01/2022)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad de la computación en nube – Prácticas óptimas y directrices en materia de seguridad de la computación en nube

Requisitos y directrices de seguridad para los contenedores de virtualización en entornos de computación en la nube

Recomendación UIT-T X.1643

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	x.1150 –x.1159
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web (1)	X.1140–X.1149
Seguridad de las aplicaciones (1)	
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1350–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.13979
Seguridad de tecnología de libro mayor distribuido (2)	X.1400–X.1429
Seguridad de las aplicaciones (2)	X.1450–X.1459
Seguridad de la web (2)	X.1470–X.1489
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
Ciberdefensa	X.1590– X.1599
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600 –X.1601
Diseño de la seguridad de la computación en nube	X.1602 –X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	**X.1640 –X.1659**
Aplicación práctica de la seguridad de la computación en nube	X.1660 –X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680 –X.1699
COMUNICACIONES CUÁNTICAS	
Terminología	X.1700 –X.1701
Generador cuántico de números aleatorios cuánticos	X.1702 –X.1709
Marco de seguridad para QKDN	X.1710 –X.1711
Seguridad de diseño para OKBN	X.1712 –X.1719
Técnicas de seguridad para OKDN	X.1720 –X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de macrodatos	X.1750 –X.1759
Protección de datos	X.1770–X.1789
SEGURIDAD DE LAS IMT-2020	X.1800–X.1819

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1643

Requisitos y directrices de seguridad para los contenedores de virtualización en entornos de computación en la nube

Resumen

En esta Recomendación, se analizan las amenazas y los desafíos de seguridad relativos a los contenedores de virtualización en entornos de computación en la nube y se especifica un marco de referencia con directrices de seguridad para los contenedores de virtualización en la nube.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1643	2022-01-07	17	11.1002/1000/14804

Palabras clave

Computación en la nube, contenedor de virtualización, directrices de seguridad.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de la existencia de propiedad intelectual, protegida por patente o derecho de autor, que puede ser necesaria para implementar esta Recomendación. Sin embargo, debe señalarse a los implementadores que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT T disponibles en el sitio web del UIT T en http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1643

Requisitos y directrices de seguridad para los contenedores de virtualización en entornos de computación en la nube

1 Alcance

En esta Recomendación, se analizan las amenazas y los desafíos de seguridad relativos a los contenedores de virtualización en entornos de computación en la nube y se especifica un marco de referencia con directrices de seguridad para los contenedores de virtualización en la nube.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación

[UIT-T X.1162] Recomendación UIT-T X.1162 (2008), *Arquitectura de seguridad y operaciones para redes entre pares.*

[UIT-T X.1255] Recomendación UIT-T X.1255 (2013), *Marco para la indagación de información de gestión de identidades.*

[UIT-T X.1279] Recomendación UIT-T X.1279 (2020), *Marco de autenticación mejorada mediante telebiometría con mecanismos de detección antisuplantación.*

[UIT-T X.1601] Recomendación UIT-T X.1601 (2015), *Marco de seguridad para la computación en la nube*.

[UIT-T X.1605] Recomendación UIT-T X.1605 (2020), *Requisitos de seguridad de la infraestructura pública como servicio (IaaS) en la computación en la nube.*

[UIT-T Y.3508] Recomendación UIT-T Y.3508 (2019), *Computación en la nube – Visión general y requisitos de alto nivel de la nube distribuida.*

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.3.1 control de acceso [b-UIT-T X.800]: Prevención del uso no autorizado de un recurso, incluida la prevención del uso de un recurso de una manera no autorizada.

3.1.2 imagen de servicio en la nube [UIT-T Y.3508]: Un código ejecutable con información de estado de la máquina virtual (véase la cláusula 3.1.10) o del contenedor de virtualización (véase la cláusula 3.1.11).

3.1.3 entorno de ejecución [b-UIT-T Y.4500.1]: Entidad lógica que representa un entorno capaz de ejecutar módulos de *software*.

3.1.4 pasarela [b-UIT-T H.350.4]: Dispositivo que traduce de un protocolo a otro. A menudo, las pasarelas traducen entre la red IP y la red pública de voz conmutada para permitir la integración de ambas.

3.1.5 orquestación [b-UIT-T Y.3100]: En el contexto de las IMT-2020, son los procesos destinados a la organización, coordinación, instanciación y utilización automatizadas de las funciones y recursos de red tanto para infraestructuras físicas como virtuales mediante la aplicación de criterios de optimización.

3.1.6 red superpuesta [b-UIT-T X.1162]: Una red superpuesta es una red virtual que funciona sobre otra red. Como cualquier red, la red superpuesta está formada por un conjunto de nodos y de enlaces entre los mismos. Como los enlaces son lógicos, pueden corresponder a muchos enlaces físicos de la red subyacente.

3.1.7 registro [b-UIT-T X.1255]: Mecanismo para registrar metadatos sobre entidades digitales y almacenar estructuras de metadatos, y que permite buscar identificadores invariables en el registro a partir de la utilización de estructuras de metadatos.

3.1.8 suplantación [b-UIT-T X.1279]: Pretensión asumida por una entidad que afirma ser otra entidad diferente, mediante la presentación de una imagen grabada u otra muestra de datos biométricos, o una característica biométrica derivada artificialmente, a fin de hacerse pasar por un individuo.

3.1.9 seguridad de la capa de transporte [b-UIT-R BT.1699]: Protocolo utilizado para enviar y recibir datos codificados a través de Internet. Este protocolo admite una combinación de varias tecnologías de seguridad, como el criptosistema de clave compartida, los certificados digitales y las funciones *hash* para evitar las escuchas, la falsificación de mensajes y la suplantación.

3.1.10 máquina virtual (VM) [b-UIT-T Q.1743]: Programa informático que simula una unidad central de procesamiento ficticia. Los programas que ejecutados por una máquina virtual se representan como códigos de byte, que son operaciones primitivas del ordenador ficticio.

3.1.11 contenedor de virtualización [b-UIT-T L.1362]: Partición de un nodo de computación que proporciona un entorno de computación virtualizado aislado.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los términos siguientes:

3.2.1 fallo del nodo: Un error por el que no se ha podido acceder a uno o varios nodos de red en el sistema de orquestación.

3.2.2 ataque de rastreo de paquetes: Un método para intervenir de forma ilegal cada paquete mientras fluye por la red.

3.2.3 modo de red en puente de contenedores de virtualización: Un modo de red que asigna un espacio de nombres individual y una dirección de protocolo de Internet (IP) a cada contenedor de virtualización y permite que el contenedor de virtualización se comunique directamente con el anfitrión.

3.2.4 ataque de escape de contenedor de virtualización: El atacante obtiene ilegalmente la autoridad de "ejecución" del contenedor de virtualización y utiliza esta autoridad para obtener una autoridad superior de la máquina virtual (VM) anfitriona del contenedor de virtualización o del servidor anfitrión físico.

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes siglas y acrónimos:

ACL Lista de control de acceso (*access control list*)

API	Interfaz de programación de aplicaciones (*application programming interface*)
CPU	Unidad central de procesamiento (*central processing unit*)
DDoS	Denegación de servicio distribuida (*distributed denial of service*)
DOS	Denegación de servicio (*denial of service*)
DTLS	Seguridad de la capa de transporte de datagramas (*datagram transport layer security*)
IaaS	Infraestructura como servicio (*infrastructure as a service*)
IP	Protocolo Internet (*Internet protocol*)
IPsec	Seguridad del protocolo Internet (*Internet protocol security*)
MITM	Ataque de intermediario (*man-in-the-middle*)
OS	Sistema operativo (*operating system*)
TLS	Seguridad de capa de transporte (*transport layer security*)
VM	Máquina virtual (*virtual machine*)
VXLAN	Red virtual extensible de área local (*virtual extensible local area network*)

5 Convenios

En la presente Recomendación:

La expresión "**se tiene la opción de**" u "**opcionalmente**" indica que el requisito se permite, sin que ello signifique que se recomienda.

La expresión "**se requiere**" indica un requisito que debe cumplirse estrictamente, sin permitir desviación alguna si se va a invocar la conformidad con la presente Recomendación.

La expresión "**se recomienda**" indica que se trata de un requisito recomendado pero que no es absolutamente obligatorio. Por tanto, el cumplimiento de ese requisito no es necesario para invocar la conformidad.

La expresión "**se prohíbe**" indica un requisito que debe cumplirse estrictamente, sin permitirse desviación alguna si se va a invocar la conformidad con la presente Recomendación.

6 Generalidades

En esta Recomendación se especifica un marco de seguridad de los contenedores de virtualización que se muestra en la Figura 6-1 y que incluye la seguridad de la capa de usuario, la seguridad de la capa de acceso, la seguridad de la capa de recursos, la seguridad de la capa de servicios, la gestión de la seguridad y los servicios de seguridad.

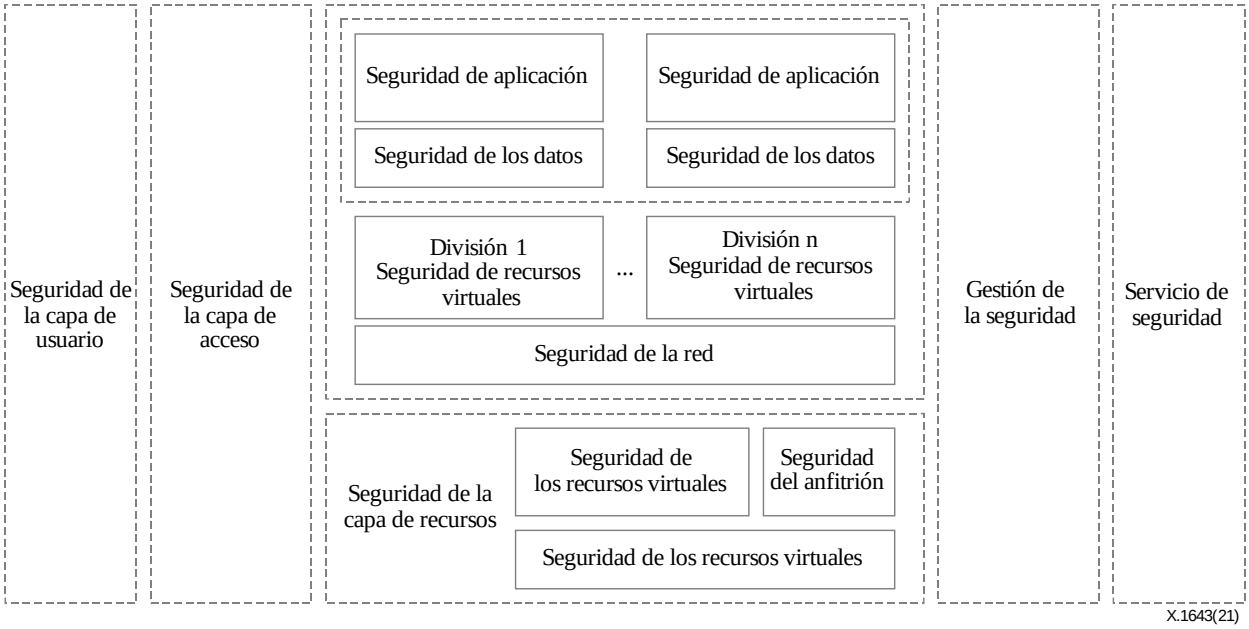

Figura 6-1 – Marco de seguridad de los contenedores de virtualización

El propósito al utilizar este marco es:

– garantizar la fiabilidad y estabilidad del contenedor de virtualización en el entorno de la computación en la nube;

– proteger la seguridad del contenedor de virtualización protegiendo la seguridad de todos los elementos que lo componen, por ejemplo, la capa de usuario, la capa de acceso, la capa de recursos, etc.; y

– proporcionar servicios de gestión de la seguridad y de seguridad a los clientes del servicio de contenedores de virtualización.

Con relación a la Figura 6.1:

a) **La seguridad de la capa de usuario** gestiona las funciones, la información de identificación y las operaciones de los usuarios para garantizar el control de acceso de los usuarios a los contenedores de virtualización, para autenticar a los usuarios y para auditar las operaciones de los usuarios.

b) **La seguridad de la capa de acceso** incluye mecanismos de control de acceso, como el acceso a la web o el acceso a la interfaz de programación de aplicaciones (API).

c) **Seguridad de la capa de recursos**: la seguridad de la capa de recursos se divide en seguridad de recursos físicos, seguridad del anfitrión y seguridad de los recursos virtuales.

   i) **La seguridad de los recursos físicos** se refiere a la seguridad de los recursos de equipos informáticos del contenedor de virtualización, como la seguridad de los recursos informáticos (unidad central de procesamiento (CPU), o memoria), los recursos de red (enrutador, conmutador), los recursos de almacenamiento, etc.

   ii) **La seguridad del anfitrión** se refiere al servidor anfitrión en el que se implementa el contenedor de virtualización, como la seguridad del sistema operativo (OS) del anfitrión, la VM, etc.

   iii) **La seguridad de los recursos virtuales** se refiere a la seguridad de los componentes virtuales de la virtualización, como la computación virtual, la red virtual, el almacenamiento virtual, etc.

d) **La gestión de la seguridad** se refiere a las funciones de gestión de la seguridad de un contenedor de virtualización en el entorno de la computación en la nube, incluyendo la gestión de la identidad, la gestión de la autenticación, la gestión de las políticas de seguridad, la gestión de las operaciones de seguridad, la gestión del mantenimiento, etc.

e) **Servicios de seguridad**: proporcionan capacidades de seguridad de los contenedores de virtualización a los usuarios en forma de servicios.

7 Retos y amenazas de seguridad para el contenedor de virtualización en la computación en la nube

7.1 Retos y amenazas de seguridad para el entorno de ejecución de contenedores de virtualización

El entorno de ejecución del contenedor de virtualización es la primera área que necesita protección ya que suele ser el lugar menos seguro y más fácil para insertar un código malicioso. Además, aquí pueden tener lugar más amenazas, por ejemplo, cambios maliciosos o ilógicos en el código fuente, alteraciones maliciosas o erróneas en los controladores de compilación automatizados, *scripts* de configuración cargados de errores y la adición de bibliotecas inseguras o de versiones inseguras del código existente.

7.2 Retos y amenazas de seguridad para el contenedor de virtualización durante el tiempo de ejecución

7.2.1 Retos y amenazas de seguridad para el seguimiento del tiempo de ejecución de los contenedores de virtualización

Los contenedores de virtualización son efímeros. Pero este valor fundamental hace que el seguimiento sea difícil. Además, las herramientas de seguimiento no tienen visibilidad o conocimiento dentro del contenedor de virtualización a nivel de la API, lo que hace más difícil el seguimiento de los comportamientos del contenedor de virtualización durante su tiempo de ejecución.

7.2.2 Retos y amenazas de seguridad para el aislamiento del tiempo de ejecución de los contenedores de virtualización

El aislamiento es un mecanismo de seguridad fundamental de los contenedores de virtualización. Según [UIT-T X.1605], el escape de máquina virtual (VM), es decir, las vulnerabilidades de las interfaces entre las VM que los atacantes podrían explotar para controlar la VM o el anfitrión de la VM, es uno de los principales desafíos de seguridad para la infraestructura como servicio (IaaS) en la computación en nube. Del mismo modo, con un aislamiento inseguro, el motor del contenedor de virtualización podría sufrir un ataque de escape del contenedor de virtualización, es decir, los atacantes podrían explotar un contenedor de virtualización comprometido para atacar a otros contenedores de virtualización que comparten el mismo sistema operativo del anfitrión y además atacar el sistema operativo del anfitrión subyacente o al anfitrión directamente.

Las manipulaciones inadecuadas después de la ejecución del contenedor de virtualización también pueden introducir otras amenazas críticas para la seguridad: 1) podría filtrarse información sensible residual a los atacantes; 2) si no pudieran liberarse los recursos informáticos o de red adecuadamente, es posible que otros contenedores de virtualización no adquieran los recursos necesarios.

7.3 Retos y amenazas de seguridad para el registro de contenedores de virtualización

Tal y como se define en [UIT-T X.1255], el registro es un mecanismo para registrar metadatos sobre entidades digitales y almacenar estructuras de metadatos, que permite buscar identificadores invariables en el registro a partir de la utilización de estructuras de metadatos. Adicionalmente, el registro de un contenedor de virtualización contiene importante información de identificación para la autorización. Ya se trate de controles de seguridad mal configurados o de la explotación de una

vulnerabilidad, los atacantes podrían obtener acceso a un registro del contenedor de virtualización de forma ilegal y alterar o eliminar el contenido por completo. El *software* obsoleto puede tener vulnerabilidades y el registro puede sufrirlas, ya que los atacantes podrían explotar dichas vulnerabilidades para obtener acceso a través de ataques por la puerta trasera. Además, los atacantes también podrían aprovechar configuraciones mal gestionadas para secuestrar el registro del contenedor de virtualización.

7.4 Retos y amenazas de seguridad para la imagen de los servicios en la nube

Tal y como se define en [UIT-T Y.3508], la imagen de servicio en la nube es un código ejecutable con información de estado de las máquinas virtuales o de los contenedores de virtualización, e incluye los sistemas operativos, las bibliotecas, los archivos de datos, las aplicaciones, etc. Dado que los contenedores de virtualización se despliegan sobre la base de imágenes de servicio en la nube, la seguridad de las imágenes de servicio en la nube es la condición previa de la seguridad de los contenedores de virtualización. Las imágenes de servicio en la nube se enfrentan a las siguientes amenazas principales:

a) El *software* de las imágenes de los servicios en la nube puede contener vulnerabilidades que pueden ser explotadas por los atacantes.

b) Con una configuración inadecuada, podría fallar la verificación de la integridad de la imagen del servicio en la nube. Además, la responsabilidad de validar la integridad de la imagen del servicio en la nube depende de los escenarios de aplicación, en los cuales los proveedores de servicios en la nube son responsables si los usuarios despliegan contenedores de virtualización basados en imágenes de servicio en la nube proporcionadas por los proveedores de servicios en la nube; mientras que los usuarios son responsables si los contenedores de virtualización desplegados se basan en imágenes de servicio en la nube de otra procedencia, como la descarga a partir de un registro.

c) Los archivos de imagen de los servicios en la nube pueden manipularse furtivamente. Por ejemplo, durante la carga o la descarga, los atacantes podrían implantar puertas traseras o *software* malicioso en los archivos de imagen de los servicios en la nube.

7.5 Retos y amenazas para la seguridad de los sistemas operativos (OS)

En el entorno de contenedores de virtualización, todos los contenedores de virtualización "comparten" con el sistema anfitrión el núcleo (*kernel*) y otros recursos del anfitrión. Por lo tanto, el sistema operativo anfitrión subyacente representa el objetivo más decisivo para los ataques. Si el sistema operativo se ve comprometido, todos los contenedores de virtualización también lo estarán. Además, los controles basados en el anfitrión y las políticas de seguridad pueden aplicarse en cada contenedor de virtualización. Por otra parte, los ataques de escape de contenedores de virtualización que se producen a través de errores en el código de la aplicación y que pueden eludir el motor y acceder al sistema operativo anfitrión y al núcleo que controla todas las demás aplicaciones.

7.6 Retos y amenazas de seguridad para el sistema de gestión de orquestación de contenedores de virtualización

Tal como se define en [b-UIT-T Y.3100], la orquestación se compone de los procesos destinados a la organización, coordinación, instanciación y utilización automatizadas de las funciones y recursos de red para las infraestructuras tanto físicas como virtuales mediante criterios de optimización, y es una tecnología típica utilizada en las redes virtuales (como en entornos de computación en la nube). En un entorno de contenedores de virtualización en la nube, un sistema de gestión de la orquestación permite la gestión de los contenedores de virtualización a gran escala que se despliegan en la nube, y se enfrenta a varios retos y amenazas de seguridad como los siguientes:

a) Abuso de privilegios: Si la política de seguridad del sistema de gestión de la orquestación no sigue el principio del mínimo privilegio, los usuarios podrían hacer uso de ella y operar los contenedores de virtualización más allá de sus propios privilegios, lo que daría lugar a importantes consecuencias en términos de seguridad.

b) Acceso no autorizado a API abiertas: Las API abiertas y otros recursos de red de acceso público, como los puertos de red en Internet, exponen nuevas superficies de ataque. Los atacantes podrían explotar las vulnerabilidades de las API abiertas, como la autenticación, la autorización o la comprobación de integridad inadecuadas, etc., y obtener acceso a la orquestación del contenedor de virtualización, y seguir operando o modificando sus contenedores de virtualización.

c) Gestión de los fallos de los nodos: El fallo de un nodo significa que no se puede acceder a uno o varios nodos de la red en un sistema de gestión de la orquestación. Una gestión inadecuada de los fallos de los nodos podría interferir con otros nodos ordinarios y con la gestión de la orquestación. Los atacantes podrían aprovecharse de ello de forma maliciosa y reducir la calidad de funcionamiento de las orquestaciones.

d) Gestión de la configuración: un sistema de gestión de la orquestación de un contenedor de virtualización introduce diferentes configuraciones en una enorme cantidad de activos y varios tipos de servicios, lo que exige una política de alto nivel y segura para la gestión de la configuración. Una configuración errónea podría ampliar las superficies de ataque y dar lugar a importantes riesgos de seguridad. Por ejemplo, los atacantes podrían penetrar en el *software* de orquestación interno a través de aplicaciones de contenedores de virtualización de acceso público.

7.7 Retos y amenazas de seguridad para la red de contenedores de virtualización

Una red de contenedores de virtualización puede funcionar bajo dos modos de red típicos, el modo de red en puente de contenedores de virtualización y el modo de red de superposición de contenedores de virtualización, para comunicarse con otros contenedores de virtualización en el mismo anfitrión, a través de diferentes anfitriones, o dentro de los contenedores de virtualización.

El modo de red en puente de contenedores de virtualización asigna un espacio de nombres individual y una dirección de protocolo de Internet (IP) a cada contenedor de virtualización y permite que el contenedor de virtualización se comunique directamente con el anfitrión.

Tal como se define en [UIT-T X.1162], una red superpuesta es una red virtual que se ejecuta sobre otra red. Como cualquier otra red, la red superpuesta comprende un conjunto de nodos y de enlaces entre ellos. Como se trata de enlaces lógicos, pueden corresponder a muchos enlaces físicos de la red subyacente. En el entorno de contenedores de virtualización en la nube, una red superpuesta de contenedores de virtualización conecta los contenedores de virtualización distribuidos. En concreto, construye una red virtual superpuesta sobre la red subyacente de cada anfitrión mediante la técnica de la red de área local virtual extensible (VXLAN), para permitir la interconexión de los contenedores de virtualización y permitir que los contenedores de virtualización se comuniquen entre anfitriones.

Los retos y amenazas de seguridad comunes para los dos modos de red del contenedor de virtualización incluyen:

– **Ataque de denegación de servicio (DoS) o de denegación de servicio distribuida (DDoS)**

  Una red de contenedores de virtualización se enfrenta a amenazas de ataques DoS/DDoS tanto de redes tanto internas como externas:

  a) Amenazas DoS/DDoS desde redes internas: un atacante podría explotar contenedores de virtualización comprometidos para lanzar ataques DoS/DDoS dirigidos a otros contenedores de virtualización en la misma red, y sobrecargar los recursos informáticos de objetivos como el ancho de banda, las CPU, etc.

b) Amenazas DoS/DDoS desde redes externas: los contenedores de virtualización en el mismo anfitrión comparten los mismos adaptadores de red físicos. Adicionalmente, si un atacante lanza ataques DoS/DDoS sobre un contenedor de virtualización objetivo mediante el envío de un gran volumen de paquetes de datos desde los anfitriones de redes robots, podría no sólo dañar el contenedor de virtualización objetivo, sino también sobrecargar el ancho de banda de la red de la máquina anfitriona, lo que provocaría ataques DoS/DDoS dirigidos al anfitrión así como a otros contenedores de virtualización.

– **Ataque de intermediario**

Los contenedores de virtualización bajo varios modos de red no proporcionan inicialmente mecanismos de encriptación, lo que resulta en contenedores de virtualización que son realmente vulnerables a los ataques de intermediario (MITM). Por ejemplo, como se define en [UIT-T X.1279], la suplantación es la pretensión asumida por una entidad que afirma ser otra entidad diferente, mediante la presentación de una imagen grabada u otra muestra de datos biométricos, o una característica biométrica derivada artificialmente, a fin de hacerse pasar por un individuo, y es una amenaza de seguridad típica. Un atacante podría explotar un contenedor de virtualización comprendido y realizar ataques de suplantación a un contenedor de virtualización objetivo en la misma red virtual. Además, si tiene éxito, el atacante puede secuestrar el tráfico de red normal de un contenedor de virtualización, y luego realizar una serie de ataques de intermediario.

Las aplicaciones dentro de los contenedores de virtualización pueden optar por realizar su propia encriptación, utilizando protocolos como *Transport Layer Security* (TLS) o *Datagram Transport Layer Security* (DTLS). En estos casos, un implementador que entiende el tráfico dentro del contenedor de virtualización – o, el tráfico que se mueve entre contenedores de virtualización, puede elegir no duplicar la provisión de encriptación. El objetivo de este enfoque es aumentar al máximo la protección del tráfico entre contenedores de virtualización al tiempo que se minimiza la sobrecarga computacional asociada a la encriptación del mismo tráfico más de una vez.

En las cláusulas 7.7.1 y 7.7.2 se describen las amenazas de seguridad particulares a las que se enfrentan el modo de red en puente de contenedores de virtualización y el modo de red de superposición de contenedores de virtualización.

7.7.1 Modo de red en puente de contenedores de virtualización

En el modo de red en puente de contenedores de virtualización, un contenedor de virtualización se conecta a una red virtual a través de su interfaz de red virtual, lo que permite que el contenedor de virtualización se comunique con el anfitrión directamente y actúe como puerta de enlace inicial. Los paquetes de red de un contenedor de virtualización se enviarán primero a la pasarela inicial y luego se enrutarán a otros contenedores de virtualización. Los contenedores de virtualización de una misma red virtual están interconectados.

Sin una política de seguridad de red para el modo de red en puente de contenedores de virtualización, no hay control de acceso a la red entre los contenedores de virtualización. Si no hay un cortafuegos y otros mecanismos de defensa de la red, un atacante se sitúa en un contenedor de virtualización y puede lanzar fácilmente varios ataques a otros contenedores de virtualización, por ejemplo, mediante suplantación de identidad, el ataque de rastreo de paquetes, etc., lo que tiene graves consecuencias, como la fuga de información sensible, etc.

Por lo tanto, sin una política de control de acceso a la red eficaz, en el modo de red en puente de contenedores de virtualización, existen riesgos para la seguridad de la red entre los contenedores de virtualización de un mismo anfitrión.

7.7.2 Modo de red de superposición de contenedores de virtualización

El modo de red superpuesta de contenedores de virtualización no tiene una política inicial de control de acceso a la red para los contenedores de virtualización. Además, como el tráfico de red VXLAN

no está cifrado por defecto, es necesario utilizar otros protocolos de tunelización, como el protocolo de seguridad IP (IPsec), etc., para encriptar el tráfico de red VXLAN y garantizar la seguridad de la transferencia de datos.

8 Requisitos y directrices de seguridad para contenedores de virtualización en entornos de computación en la nube

En esta cláusula se proporcionan los requisitos y las directrices de seguridad de acuerdo con los retos y amenazas de seguridad para el contenedor de virtualización que se describen en la cláusula 7.

8.1 Requisitos y directrices de seguridad para contenedores de virtualización durante el tiempo de ejecución

a) Al realizar una actualización de las aplicaciones o de los servicios, los contenedores de virtualización en ejecución deberán detenerse y sustituirse por nuevos contenedores de virtualización.

b) Se deben utilizar herramientas para buscar vulnerabilidades comunes en los tiempos de ejecución desplegados. Se renovarán todas las instancias que estén en riesgo.

c) Ningún usuario no autorizado debe tener acceso al *daemon* del contenedor de virtualización.

8.2 Requisitos y directrices de seguridad para contenedores de virtualización

a) El servidor que aloja el registro debería estar bloqueado para mitigar el riesgo de ataque en el mismo.

b) Las herramientas de desarrollo, el sistema de gestión de orquestación y los contenedores de virtualización deben configurarse para que sólo se conecten a los registros a través de canales encriptados.

c) Los registros deberían ser depurados de imágenes de servicio en la nube inseguras y vulnerables que ya no se utilizarán.

d) Todos los accesos al registro deberían requerir autenticación para garantizar que sólo se puedan añadir imágenes de servicio en la nube procedentes de entidades de confianza.

8.3 Requisitos y directrices de seguridad de las imágenes de servicio en la nube de contenedores de virtualización

a) El objeto de las imágenes de servicio en la nube es crear un contenedor de virtualización de aplicaciones o servicios. No deben utilizarse imágenes de servicio en la nube para otras tareas.

b) Las firmas de las imágenes de servicio en la nube deben ser validadas antes de ejecutarse las imágenes de servicio en la nube para asegurar que las mismas proceden de fuentes de confianza y no han sido alteradas.

c) Deberá implementarse un control y mantenimiento continuos de los registros para garantizar que las imágenes de servicio en la nube que contienen se mantienen y actualizan a medida que cambian las vulnerabilidades y los requisitos de configuración.

d) El acceso a las imágenes de servicio en la nube debe utilizar nombres inmutables que especifiquen versiones diferenciadas de las imágenes de servicio en la nube.

8.4 Requisitos y directrices del sistema operativo del anfitrión de los contenedores de virtualización

a) Deben reducirse al mínimo los vectores de ataque, eliminando del entorno del anfitrión todo lo que no sea esencial.

b) No deben mezclarse cargas de trabajo de contenedores virtualizados y no virtualizados en la misma instancia del anfitrión.

c) La versión del sistema operativo del anfitrión debe ser validada mediante la implementación de prácticas y herramientas de gestión.

d) Toda autenticación del sistema operativo debe ser auditada.

e) Los contenedores de virtualización deben ejecutarse con el conjunto mínimo de permisos del sistema de archivos requerido. Cualquier cambio de archivo en el sistema operativo del anfitrión del contenedor de virtualización debe realizarse únicamente mediante políticas de autorización.

8.5 Requisitos y directrices de seguridad del sistema de gestión de la orquestación de los contenedores de virtualización

a) El sistema de gestión de la orquestación debe instalarse desde una fuente oficial, de confianza y actualizada.

b) El sistema de gestión de la orquestación debe estar configurado para proporcionar una alta disponibilidad y una conmutación por error automática en la medida de lo posible.

c) El sistema de gestión de la orquestación debe utilizar un modelo de acceso de mínimo privilegio en el que el usuario sólo tenga la capacidad de realizar las acciones específicas en el anfitrión específico, el contenedor de virtualización y la imagen del servicio en la nube.

d) Para las cuentas administrativas del sistema de gestión de la orquestación se deben utilizar métodos de autenticación fuertes, como la exigencia de una autenticación de múltiples factores en lugar de una simple contraseña.

e) El sistema de gestión de la orquestación debe estar configurado para separar el tráfico de red en redes virtuales diferenciadas por nivel de sensibilidad.

f) El sistema de gestión de la orquestación debe configurarse para aislar los despliegues en conjuntos específicos de anfitriones en función de los niveles de sensibilidad.

8.6 Requisitos y directrices de seguridad de los contenedores de virtualización en diferentes modos de red

8.6.1 Restricción del tráfico entre contenedores de virtualización para el modo de red en puente de contenedores de virtualización

En el modo de red en puente, la configuración de seguridad inicial por defecto del contenedor de virtualización no controla ni restringe el acceso a la red. Para prevenir posibles amenazas DoS/DDoS, deben existir políticas de control de acceso a la red en función de los requerimientos reales, y para ello:

a) Se prohibirá por completo la comunicación entre contenedores de virtualización si ello es posible. En escenarios de aplicación específicos, si los contenedores de virtualización del anfitrión no necesitan comunicarse en red entre sí, podría prohibirse la comunicación entre contenedores de virtualización cambiando la configuración de seguridad por defecto.

b) Deben implementarse políticas de control de acceso entre contenedores de virtualización: en un entorno de nube de contenedores de virtualización en el que existe multiarrendamiento, puede darse la situación de que un solo contenedor de virtualización ocupe muchos anfitriones y sobrecargue el ancho de banda de otros contenedores de virtualización. Para garantizar la comunicación regular entre los contenedores de virtualización y evitar el tráfico anormal causado por los ataques DoS/DDoS, se deben implementar mecanismos de restricción del tráfico de comunicación entre los contenedores de virtualización.

c) Deben implementarse mecanismos y políticas de encriptación, por ejemplo, utilizar el protocolo IPsec para encriptar el tráfico y garantizar la confidencialidad de la comunicación

entre contenedores de virtualización, evitando así que se produzcan ataques de rastreo en la red o ataques de intermediario.

8.6.2 Control de acceso entre contenedores de virtualización

a) Control de acceso para el modo de red en puente de contenedores de virtualización

En el modo de red en puente, la configuración de seguridad inicial por defecto de los contenedores de virtualización permite que los contenedores de virtualización se conecten a la misma red virtual y se comuniquen entre sí directamente. Por lo tanto, para evitar accesos anómalos, deben configurarse mecanismos y políticas de control de acceso bajo demanda. Para ello:

1) Deben configurarse diferentes redes virtuales para los contenedores de virtualización a fin de lograr el aislamiento de la red entre los diferentes contenedores de virtualización. Ello bloqueará el tráfico de comunicación con otras redes y se logrará el propósito del aislamiento entre las redes de los contenedores de virtualización.

2) Debe implementarse el control de acceso basado en la política de lista blanca con el fin de garantizar la seguridad de la red entre los contenedores de virtualización, debe prohibirse por defecto la comunicación entre los contenedores de virtualización, y luego deben configurarse las reglas de control de acceso bajo demanda. El control de acceso basado en la política de lista blanca reduce la superficie de ataque mediante una estrategia de reducción al mínimo.

b) Control de acceso para el modo de red superpuesta de contenedores de virtualización.

En el modo de red superpuesta de contenedores de virtualización, diferentes contenedores de virtualización pueden acceder entre sí directamente en la misma subred y en el mismo anfitrión. Deben añadirse manualmente reglas de entrada a la lista de control de acceso (ACL) en las políticas de control de acceso del anfitrión, o debe desplegarse un cortafuegos en el anfitrión, con el fin de controlar el acceso de los anfitriones externos a las aplicaciones internas del contenedor de virtualización.

En un entorno de nube de contenedores de virtualización de gran tamaño, podría no ser práctico actualizar manualmente las reglas del cortafuegos debido a las frecuentes actualizaciones dinámicas de los microservicios [b-UIT-T J.1301]. Se recomienda utilizar algunas herramientas para gestionar el proceso automáticamente, como la microsegmentación de contenedores de virtualización, que es una técnica de cortafuegos de contenedores de virtualización que proporciona mecanismos de aislamiento de segmentación de red muy precisos y puede realizar el aislamiento de segmentación para un solo contenedor de virtualización, para contenedores de virtualización en un mismo subconjunto de red, o para aplicaciones de contenedores de virtualización, y poder implementar en consecuencia las políticas de control de acceso a la red.

Bibliografía

[b-ITU-T H.350.4] Recomendación UIT-T H.350.4 (2011), *Arquitectura de servicios de directorio para el protocolo de iniciación de sesión.*

[b-ITU-T J.1301] Recomendación UIT-T J.1301 (2021), *Especificación de un servicio de medios convergentes basado en la nube capaz de soportar el protocolo Internet y la televisión por cable – Requisitos.*

[b-ITU-T L.1362] Recomendación UIT-T L.1362 (2019), *Interfaz para la gestión de potencia en los entornos de virtualización de la función de red – Capa de abstracción verde versión 2.*

[b-ITU-T Q.1743] Recomendación UIT-T Q.1743 (2016), *Referencias de las IMT-Avanzadas a la versión 11 de la red básica de paquetes evolucionada de LTE-Avanzada.*

[b-ITU-T X.800] Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT.*

[b-UIT-T X.810] Recomendación UIT-T X.810 (1995), *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Visión general.*

[b-ITU-T X.1162] Recomendación UIT-T X.1162 (2008), *Arquitectura de seguridad y operaciones para redes entre pares.*

[b-UIT-T X.1251] Recomendación UIT-T X.1251 (2019), *Expresión estructurada de información sobre amenazas: casos de uso.*

[b-ITU-T X.1255] Recomendación UIT-T X.1255 (2013), *Marco para la indagación de información de gestión de identidades.*

[b-ITU-T X.1279] Recomendación UIT-T X.1279 (2020), *Marco de autenticación mejorada mediante telebiometría con mecanismos de detección antisuplantación.*

[b-UIT-T X.1604] Recomendación UIT-T X.1604 (2020), *Requisitos de seguridad de la red como servicio (NaaS) en la computación en la nube.*

[b-UIT-T Y.3500] Recomendación UIT-T Y.3500 (2014), *Tecnología de la información – Computación en nube – Visión general y vocabulario.*

[b-UIT-T Y.3502] Recomendación UIT-T Y.3502 (2014), *Tecnología de la información – Computación en la nube – Arquitectura de referencia.*

[b-ITU-T Y.4500.1] Recomendación UIT-T Y.4500.1 (2018), *Sistema oneM2M – Arquitectura funcional.*

[b-ITU-R BT.1699] Recomendación UIT-R BT.1699 (2013), *Armonización de los formatos de aplicaciones declarativas para la televisión interactiva.*

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

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

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

[b-ISO/CEI 29100] ISO/CEI 29100 (2011), *Information technology –Security techniques –Privacy framework.*

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2022