ITUPublications
Recomendaciones

Unión Internacional de Telecomunicaciones
Sector de Normalización

Recomendación

UIT-T X.1644 (03/2023)

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

---

Directrices de seguridad para la nube distribuida

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 (1)	
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)	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 (2)	
Comunicaciones de emergencia	X.1300-X.1309
Seguridad en las redes de sensores ubicuos	X.1310-X.1319
Seguridad de las redes eléctricas inteligentes	X.1330-X.1339
Correo certificado	X.1340-X.1349
Seguridad en la Internet de las cosas (IoT)	X.1350-X.1369
Seguridad en los sistemas de transporte inteligente (STI)	X.1370-X.1399
Seguridad de tecnología de libro mayor distribuido (DLT)	X.1400-X.1429
Seguridad de las aplicaciones (2)	X.1450-X.1459
Seguridad en 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
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700-X.1701
Generador de números aleatorio cuántico	X.1702-X.1709
Marco de seguridad QKDN	X.1710-X.1711
Diseño de seguridad para QKDN	X.1712-X.1719
Técnicas de seguridad para QKDN	X.1720-X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750-X.1759
Protección de los datos	X.1770-X.1789
SEGURIDAD EN LAS REDES IMT-2020	X.1800-X.1819

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

Recomendación UIT-T X.1644

Directrices de seguridad para la nube distribuida

Resumen

En la Recomendación UIT-T X.1644 se analizan las amenazas y los riesgos de seguridad en la nube distribuida y se proponen directrices de seguridad contra las amenazas de la nube distribuida, abarcando directrices de seguridad para la nube central, la nube regional y la nube periférica.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1644	03/03/2023	17	11.1002/1000/15112

Palabras clave

Directrices de seguridad, computación en la nube, nube distribuida

* 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-es.

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 propiedad intelectual, protegida por patente o derecho de autor, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios 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 http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1644

Directrices de seguridad para la nube distribuida

1 Alcance

En esta Recomendación se analizan las amenazas de seguridad de la nube distribuida y se proporcionan directrices de seguridad para la nube distribuida.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, por referencia a las mismas en este texto, constituyen disposiciones de esta Recomendación. En la fecha de publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios de esta Recomendación a que consideren la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en el marco de esta Recomendación no confiere al mismo, como documento autónomo, el rango de Recomendación.

[UIT-T X.1408] Recomendación UIT-T X.1408 (2021), *Amenazas y requisitos de seguridad para el acceso y la compartición de datos basados en la tecnología de libro mayor distribuido.*

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

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

[UIT-T Y.3508] Recomendación UIT-T Y.3508 (2019), *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:

3.1.1 tipo de capacidades de la nube [UIT-T Y.3500]: Clasificación de la funcionalidad facilitada por un servicio en la nube al cliente del servicio en la nube en función de los recursos utilizados.

NOTA – Los tipos de capacidades de la nube son el tipo capacidad de aplicación, el tipo capacidad de infraestructura y el tipo capacidad de plataforma.

3.1.2 computación en la nube [UIT-T Y.3500]: Paradigma para dar acceso a la red a un conjunto elástico y ampliable de recursos físicos o virtuales compartibles con administración y configuración en autoservicio previa solicitud.

3.1.3 servicio en la nube [UIT-T Y.3500]: Una o más capacidades que se ofrecen mediante computación en la nube a las que se accede mediante una interfaz definida.

3.1.4 cliente del servicio en la nube [UIT-T Y.3500]: Parte que mantiene una relación comercial a fin de utilizar los servicios en la nube.

NOTA – Una relación comercial no implica necesariamente un acuerdo financiero.

3.1.5 proveedor del servicio en la nube [UIT-T Y.3500]: Parte que ofrece servicios en la nube.

3.1.6 nube periférica [UIT-T Y.3508]: Computación en la nube implementada en el extremo de la red a la que acceden clientes de servicios en la nube (CSC) con recursos de capacidad reducida que permiten el servicio en la nube.

NOTA 1 – El servicio en la nube activado en la nube periférica es un servicio en la nube ligero prestado por un proveedor de servicios en la nube (CSP) en función de la categoría del servicio en la nube.

NOTA 2 – El servicio ligero en la nube se refiere a una parte del servicio en la nube para reconfigurar la funcionalidad del servicio en la nube de manera que se adapte a la nube periférica como la estación de base y la pasarela con recursos de capacidad reducida.

3.1.7 amenaza [UIT-T X.1408]: Posible causa de un incidente no deseado, que puede dañar un sistema o perjudicar a una organización.

3.2 Términos definidos en la presente Recomendación

En esta Recomendación se definen los siguientes términos:

3.2.1 nube central: Conjunto centralizado de servicios que abarca todos los servicios independientes de la geografía, los servicios que no son sensibles a la latencia, los servicios que requieren grandes recursos computacionales, los servicios de copia de seguridad y recuperación, y los servicios con alto nivel de seguridad de una red de computación en la nube.

3.2.2 nube distribuida: La nube distribuida es una extensión de los conceptos clásicos de computación en la nube, que amplía las capacidades de computación en la nube hasta la periferia de la red.

3.2.3 nube regional: Nube central que se implementa opcionalmente para lograr una configuración eficaz entre la nube central y una nube periférica a fin de reducir la carga de la nube central.

4 Abreviaturas y acrónimos

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

API Interfaz de servicio de aplicación (*application service interface*)

CC Nube central (*core cloud*)

CSC Cliente de servicios en la nube (*cloud service customer*)

CSP Proveedor de servicios en la nube (*cloud service provider*)

DDoS Denegación de servicio distribuida (*distributed denial of service*)

DoS Denegación de servicio (*denial of service*)

EC Nube periférica (*edge cloud*)

IoT Internet de las cosas (*Internet of things*)

OTA Por vía aérea (*over-the-air*)

REST Transferencia de estado representativo (*representational state transfer*)

TLS Seguridad de capa de transporte (*transport layer security*)

VPN Red privada virtual (*virtual private network*)

XML Lenguaje de marcado extensible (*extensible markup language*)

XSS Secuencias de comandos en sitios cruzados (*cross site scripting*)

5 Convenios

En la presente Recomendación:

La expresión **"es necesario"** indica que el requisito es absolutamente obligatorio y debe aplicarse sin excepción si se pretende declarar la conformidad con este documento.

La expresión **"se recomienda"** indica que se trata de un requisito recomendado y que, por ende, no es absolutamente obligatorio. Su cumplimiento no es indispensable para poder declarar la conformidad.

6 Generalidades

La nube distribuida está adquiriendo cada vez más importancia porque cada vez son más los servicios sensibles a la latencia (como los servicios de vídeo e Internet de las cosas (IoT)) que requieren velocidades de respuesta muy superiores; se trata de una extensión de la computación en la nube tradicional que amplía sus capacidades hasta el extremo de la red. Puede proporcionar servicios en la nube localizados de manera mucho más cercana al cliente y a la fuente de datos, y puede interactuar con otras nubes para prestar servicios distribuidos, de baja latencia y grandes resultados.

La nube distribuida abarca la distribución de los tipos de capacidades de la nube hasta el extremo de la red a fin de facilitar la prestación de servicios con poca latencia y procesamiento en tiempo real en un ancho de banda limitado, interactuando entre un conjunto de recursos físicos o virtuales [UIT-T Y.3508]. En la Figura 6-1 se describe una nube distribuida típica, que incluye la nube central, la nube regional y la nube periférica.

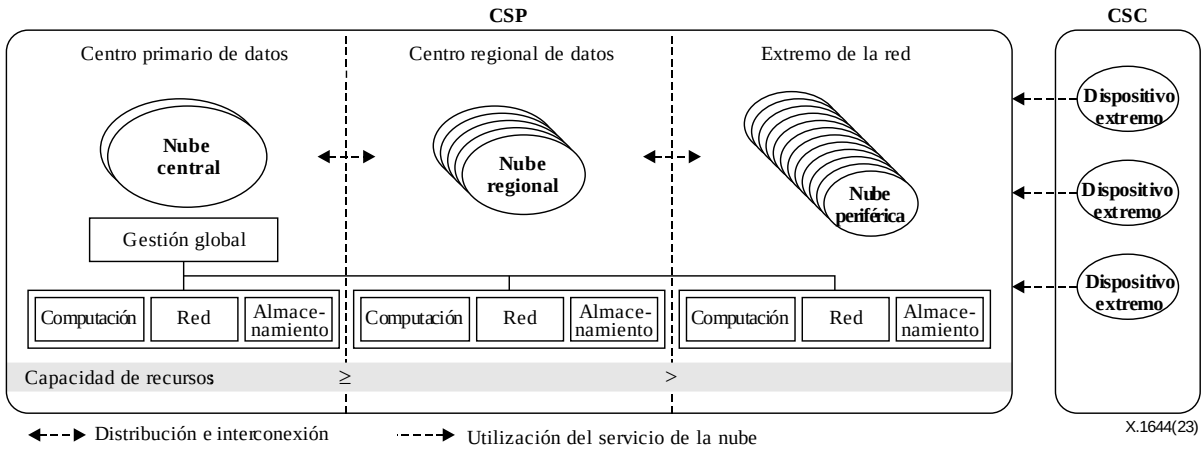

Figura 6-1 – Concepto de nube distribuida

La nube central tiene una amplia capacidad de recursos y un punto de gestión global para controlar los recursos de la nube en la nube distribuida. La nube central soporta los servicios en la nube que requieren grandes recursos computacionales y son independientes desde el plano geográfico.

La nube regional se implementa opcionalmente en determinadas regiones a partir de la nube central para compartir cargas y mejorar la calidad de servicio. La nube regional gestiona las solicitudes de servicios en la nube que proceden de la región controlada por la gestión global de la nube central.

NOTA 1 – La nube regional soporta menos latencia que la nube central al ejecutar servicios en la nube personalizados para los clientes de servicios en la nube (CSC) de una determinada región. Se supone que la latencia de red del CSC a la nube regional es inferior a la existente del CSC a la nube central y que la diferencia del tiempo de ejecución del servicio en la nube entre la nube central y la nube regional es insignificante.

NOTA 2 – La nube regional lleva a cabo el almacenamiento de la carga del servicio en la nube y la conservación de los datos de la nube central, y los proporciona a los CSC de la región.

La nube periférica se implementa en el extremo de la red a la que acceden los CSC y tiene una capacidad de recursos reducida. La nube periférica requiere recursos de *hardware* especializados para un fin; por ejemplo, los recursos de la nube periférica son limitados debido a las limitaciones de espacio o potencia. La nube periférica puede tener diferentes configuraciones de recursos y tipos de capacidades de la nube con recursos físicos y virtuales en función de las necesidades de servicios en la nube de los CSC y de las condiciones del entorno de implantación.

7 Riesgos y amenazas de seguridad de la nube distribuida

La utilización de una nube distribuida ofrece ventajas en lo que se refiere a la alta velocidad, eficiencia y rendimiento. En una nube distribuida, la nube central, la nube regional y la nube periférica plantean nuevos riesgos y amenazas de seguridad [UIT-T X.1601].

7.1 Riesgos y amenazas de seguridad de la nube central

La nube distribuida tiene infraestructuras de diferentes magnitudes con grandes capacidades de recursos en la nube central o la nube regional y capacidades de recursos reducidas en la nube periférica. La nube central utiliza una infraestructura heterogénea como único sistema para prestar diversos servicios a los CSC en la nube distribuida. Los riesgos y amenazas de seguridad de la nube central son los siguientes:

a) **Vulnerabilidades del sistema**: La infraestructura de la nube distribuida contiene vulnerabilidades del sistema, especialmente en redes que tienen infraestructuras complejas y múltiples plataformas de terceros, y la vulnerabilidad en la nube central también afecta a la nube regional y a la nube periférica.

b) **Daños físicos**: La infraestructura de la nube distribuida puede implementarse en entornos físicos no fiables y puede sufrir daños físicos provocados por usuarios malignos, condiciones meteorológicas adversas o terremotos. Los daños físicos de la nube central también podrían afectar a la seguridad de la nube regional y la nube periférica.

7.2 Riesgos y amenazas de seguridad de la nube regional

a) **Interceptación de la transmisión**: La nube central necesita transmitir datos a las nubes regionales y estos vínculos de transmisión pueden ser interceptados.

b) **Órdenes o solicitudes falsas**: Las órdenes o solicitudes malignas procedentes de una nube central, regional o periférica falsa pueden causar fugas de datos.

c) **Ataque a la interfaz**: Dado que la nube central tiene nexos con múltiples nubes regionales a través de interfaces abiertas, puede recibir ataques por conducto de estas interfaces.

d) **Ataque de sumidero**: Un intruso puede poner en peligro un dispositivo o introducir un dispositivo falsificado en la red y utilizarlo a continuación para lanzar un ataque de sumidero. Los ataques de sumidero son un tipo de ataque de la capa de red en que un dispositivo afectado envía información de encaminamiento falsa a sus vecinos para atraer el tráfico de red hacia él.

e) **Pasarelas malignas**: Es fácil que un atacante implemente una pasarela maligna. Una vez que se engaña al dispositivo legítimo para que se conecte a una pasarela maligna, puede recopilarse información confidencial de la conexión. Esto eludirá de manera eficaz muchas medidas de seguridad instauradas y podría causar interferencias radioeléctricas con la instalación oficial de la organización.

f) **Acceso no autorizado a pasarelas IoT**: Un atacante podría utilizar un acceso no autorizado a pasarelas IoT, lo que puede producir la divulgación de información confidencial, la modificación de datos y el uso ilícito de determinados recursos en la nube periférica.

7.3 Riesgos y amenazas de seguridad de la nube periférica

a) **Problemas de multiarrendamiento**: Muchas soluciones en la nube no proporcionan la protección de seguridad necesaria entre clientes, lo cual da lugar a la compartición de recursos, aplicaciones y sistemas. En esta situación, puede haber amenazas procedentes de otros clientes del servicio de computación en la nube, y las amenazas enfocadas hacia un cliente también podrían afectar a otros clientes.

b) **Solicitud falsa**: Si se origina una solicitud de una nube regional o periférica falsificada, y la nube central no la reconoce, esto tal vez dé lugar a una fuga de datos, entre otras cosas.

c) **Ataque de secuencias de comandos en sitios cruzados (XSS)**: Un ataque de secuencias de comandos en sitios cruzados puede utilizarse para aprovechar vulnerabilidades que existen en sitios web, introduciendo códigos malignos en las máquinas de los clientes y las credenciales de usuario se suplantan para llevar a cabo actividades malignas.

d) **Envoltura de lenguaje de marcado extensible (XML)**: XML es el lenguaje de marcado subyacente que permite la autenticación inicial de las aplicaciones en la nube periférica. Los piratas informáticos pueden lanzar ataques pirata utilizando técnicas de envoltura con reescritura o firma XML.

e) **Negligencia del personal**: La negligencia del personal sigue siendo uno de los mayores problemas de seguridad de todos los sistemas, pero la amenaza es especialmente importante en el caso de la gestión de la nube distribuida. El personal puede identificarse en plataformas de gestión de la nube distribuida a partir de sus teléfonos móviles, tabletas privadas y ordenadores privados, lo cual puede hacer que el sistema sea vulnerable a muchas amenazas externas.

f) **Suplantación de identidad y ataques de ingeniería social**: Debido a la naturaleza abierta de un sistema de nube distribuida, la suplantación de identidad y los ataques de ingeniería social se han convertido en un fenómeno especialmente frecuente. Una vez que se obtiene la información de conexión y otra información confidencial, un usuario maligno puede acceder potencialmente al sistema con facilidad.

g) **Pérdida de control**: Cuando los servicios de una organización se colocan en la nube distribuida, pierden el control y el conocimiento de donde pueden almacenarse en la nube. Entre tanto, desde el punto de vista del usuario, esto se convierte en un problema de seguridad grave, ya que el usuario no es consciente de ningún mecanismo de seguridad para proteger sus servicios.

h) **Usurpación de dispositivos**: Un atacante podría hacerse pasar por un dispositivo legítimo, y enviar datos falsos o malignos a la nube periférica o robar datos de usuarios.

i) **Captura de dispositivo periférico**: Hay muchos dispositivos extremos cerca de la nube periférica que pueden recabar datos, transferir datos a la nube periférica y recibir resultados o comandos de la nube periférica. Un dispositivo extremo puede ponerse fácilmente en peligro debido a su débil protección de seguridad.

j) **Ataque de denegación de servicio distribuida (DDoS)**: Los ataques de DDoS contra las nubes distribuidas han aumentado considerablemente su viabilidad. Si se inicia un tráfico maligno suficiente hacia un sistema de computación en la nube, el sistema de computación puede colapsarse por completo o experimentar dificultades. En particular, una nube periférica es una entidad de nube relativamente más pequeña con una protección de seguridad relativamente más baja, por lo que es más probable que reciba ataques de piratas informáticos y que se utilice para realizar ataques de DDoS u otras actividades ilegales.

k) **Seguridad de la virtualización**: En el entorno de nube periférica, la seguridad de la virtualización incluye la implementación de un aislamiento de seguridad y la mejora de las pasarelas, controladores y servidores periféricos sobre la base de la tecnología de virtualización. En comparación con la nube central y la nube regional, estos nodos periféricos con recursos de computación y almacenamiento limitados se enfrentan a vectores de ataque más complejos y amplios.

8 Directrices de seguridad para la nube distribuida

En esta cláusula se proporcionan directrices de seguridad relacionadas con la nube central, la nube regional y la nube periférica para los sistemas de nube distribuida descritos en la cláusula 6.

8.1 Directrices de seguridad para la nube central

Las directrices de seguridad para la nube central abarcan directrices para la seguridad de sistema de la nube central, la seguridad física, la seguridad relativa a la denegación de servicio y la seguridad de los dispositivos periféricos.

8.1.1 Seguridad de sistema de la nube central

Las directrices para la seguridad de sistema de la nube central son las siguientes:

a) Se recomienda utilizar herramientas de respuesta a los incidentes de vulnerabilidad.

b) Se recomienda prevenir la introducción de programas maliciosos en los servicios en la nube utilizando técnicas como el análisis de archivos, las listas blancas de aplicaciones, la detección de programas maliciosos basada en el aprendizaje automático y el análisis del tráfico de red.

c) Se recomienda revisar y actualizar las evaluaciones de riesgos para incluir los servicios en la nube. Así mismo, se recomienda identificar y abordar los factores de riesgo introducidos por entornos y proveedores de la nube central. Hay bases de datos de riesgos para proveedores en la nube que aceleran el proceso de evaluación.

8.1.2 Seguridad física

Las directrices para la seguridad física son las siguientes:

a) Se recomienda construir la infraestructura de la nube central en una ubicación adecuada en lugar de hacerlo en lugares como las vías de aterrizaje de los aeropuertos, las centrales eléctricas, las llanuras inundables, las líneas de fallas sísmicas u otras áreas que experimentan frecuentemente desastres naturales.

b) Se recomienda proporcionar procesos para modificar, mantener y supervisar las condiciones del entorno físico de las infraestructuras construidas bajo la tierra.

c) Se recomienda proporcionar sistemas de enfriamiento y normas de conformidad para las infraestructuras construidas bajo la tierra.

d) Se recomienda limitar los puntos de entrada de la infraestructura de nube central a fin de reducir los riesgos de introducción física.

e) Se recomienda proporcionar múltiples puntos de control en toda la infraestructura de nube central a fin de reducir al mínimo los riesgos relativos al acceso de intrusos malignos.

f) Se recomienda que el sistema de supervisión de la vigilancia ofrezca una seguridad física adicional.

g) Se recomienda que la redundancia ayude a la infraestructura de la nube central a hacer frente a cualquier incidente con el mínimo tiempo de interrupción.

8.1.3 Medidas contra la denegación de servicio

Las directrices relativas a la denegación de servicio son las siguientes:

a) Se recomienda que la capacidad del servidor de la nube central gestione los grandes picos de tráfico y tenga las herramientas de mitigación necesarias para hacer frente a los problemas de seguridad.

b) Se recomienda actualizar y parchear periódicamente los cortafuegos y programas de seguridad de la red.

8.2 Directrices de seguridad para la nube regional

Las directrices de seguridad para la nube regional abarcan directrices relativas a la seguridad de los datos transmitidos y los datos estáticos, la seguridad de la interfaz abierta y la seguridad de la pasarela de IoT.

8.2.1 Seguridad de los datos transmitidos y los datos estáticos

La nube regional presta servicios de nube central parciales o completos a una determinada región geográfica. Las directrices de seguridad de los datos transmitidos y los datos estáticos en la nube regional abarcan lo siguiente:

a) Se requiere que la nube regional utilice el cifrado con cierta intensidad a fin de cifrar las comunicaciones y los datos. También se recomienda dar soporte a los servicios de protocolo de transmisión segura a fin de evitar que los ataques basados en el protocolo vulneren la confidencialidad.

b) Se requiere que la nube regional autentique e identifique las identidades de los servicios y han de adoptarse estrategias estrictas relativas al aislamiento y al control del acceso. Se requiere dar soporte a la personalización y gestión de las estrategias de control del acceso.

c) Se recomienda que la nube regional preste apoyo a un sistema de intercambio de datos seguro, a fin de conseguir la supervisión y control en tiempo real del formato de datos, el contenido y el flujo, etc.

d) Se recomienda que el sistema de intercambio de datos seguro reúna diversos requisitos elásticos en el entorno de nube y que, entre otras cosas, proporcione métodos de despliegue flexibles, modos de planificación de recursos flexibles, y métodos seguros para intercambiar datos sobre la base de un fuerte aislamiento de seguridad centrado en el negocio, etc.

e) Se recomienda que la nube regional dé soporte a la detección de códigos malignos y a la supresión de los datos transmitidos.

f) Se requiere adoptar mecanismos de cifrado y verificación a fin de garantizar la integridad y la confidencialidad del almacenamiento local, en particular los datos de administración del sistema (como los ficheros índice, la información del servicio en la nube y las claves), la información de autenticación e importantes datos comerciales (como los datos de privacidad del usuario).

g) Se recomienda dar soporte a la autenticación de la identidad basada en funciones para el acceso a los datos y adoptar medidas estrictas de control del acceso contra el acceso ilícito.

8.2.2 Seguridad de las interfaces abiertas

El proveedor de servicios en la nube (CSP) necesita proporcionar interfaces de red e interfaces de programación de aplicaciones (API) para poder configurar, administrar, coordinar y supervisar diversos servicios en la nube, y también prestar servicios directamente. Suele haber terceros que prestan servicios adicionales sobre la base de estas interfaces. Las directrices para garantizar la seguridad de las API de la nube regional son las siguientes:

a) Se requiere utilizar técnicas de cifrado como la seguridad de capa de transporte (TLS) u otros métodos de cifrado para que la API utilizada para la transferencia de estado representativo (REST) cifre los datos durante la transmisión y evite su manipulación. También se requiere utilizar un mecanismo de firma para garantizar que solo los usuarios con derechos de acceso puedan descifrar y modificar los datos.

b) Se recomienda establecer identidades de confianza de las API a través de testigos, y a continuación garantizar que solo las identidades de confianza con testigo puedan acceder y controlar los servicios y los recursos de datos, etc.

c) Se recomienda llevar a cabo una supervisión en tiempo real y emitir alertas sobre las conductas alarmantes de la interfaz API abierta y la transmisión anormal de datos, por ejemplo, la limitación de la frecuencia de acceso a la interfaz API.

d) Se recomienda identificar activamente las vulnerabilidades de las API. Se podrían utilizar herramientas de detección para detectar la seguridad de las API y las fugas de datos y rastrear si las API han sufrido ataques y si se está aprovechando una vulnerabilidad en tiempo real.

e) Se recomienda utilizar pasarelas de seguridad de las API, ya que estas se han utilizado como tecnología clave para proteger la seguridad de las API. Dado que las pasarelas de seguridad de las API pueden utilizarse para controlar y administrar la utilización de las interfaces API, también pueden autenticar a los usuarios que utilizan las interfaces y los servicios de API.

8.2.3 Seguridad de las pasarelas de IoT

Los dispositivos de IoT se conectan a Internet mediante pasarelas de IoT, que se convierten en los principales blancos de los programas maliciosos y los ataques a las redes. Las directrices de seguridad relativas a las pasarelas de IoT son las siguientes:

a) Se recomienda que las pasarelas de IoT den soporte a la autenticación de dispositivos y el control del acceso; solo los usuarios y dispositivos autorizados pueden acceder e implementar sistemas de almacenamiento seguro o cámaras a fin de proteger la información confidencial como las claves y los certificados.

b) Se recomienda que las pasarelas de IoT den soporte a la gestión de políticas para configurar los derechos de acceso y controlar el acceso de los dispositivos a los servicios de aplicaciones (servicios técnicos, servicios comerciales, servicios de datos), los archivos (archivos de configuración, archivos de registro, archivos espejo) y otros objetos según las políticas de seguridad, y que las pasarelas puedan interrumpir las conexiones y sesiones ilícitas a tiempo.

c) Se recomienda que las pasarelas de IoT propicien la actualización por vía aérea (OTA) a fin de que puedan ejecutar los programas de *software* y *firmware* más recientes, y evitar las vulnerabilidades y riesgos comunes. El arranque seguro puede garantizar que la pasarela se inicie con una imagen de *firmware* cuya integridad y autenticidad se han cifrado y comprobado, previniendo así la utilización de *firmware* maligno para arrancar la pasarela.

d) Se recomienda que las pasarelas de IoT den soporte a diversas medidas de control de seguridad a fin de proteger los dispositivos de IoT. Por ejemplo, cuando se utiliza una pasarela de IoT como proxy de seguridad para redes y dispositivos, se recomienda que se implementen en la pasarela funciones de cortafuegos, filtrado del tráfico basado en normas y listas blancas.

e) Se recomienda que las pasarelas de IoT den soporte a registros de eventos detallados, a fin de adquirir una mayor comprensión de los procesos que se ejecutan en las pasarelas para las auditorías de seguridad.

8.3 Directrices de seguridad para la nube periférica

Las directrices de seguridad para la nube periférica abarcan directrices para la seguridad de la infraestructura de nube periférica, la seguridad de los datos transmitidos y los datos estáticos, la seguridad de la red en la nube, la seguridad web y la seguridad de los dispositivos extremo junto a la nube periférica.

8.3.1 Seguridad de la infraestructura de nube periférica

La infraestructura de nube periférica proporciona las bases tanto del *hardware* como del *software*, y la seguridad de la infraestructura periférica es un requisito fundamental de la nube periférica. Las directrices de seguridad relativas a la infraestructura de nube periférica son las siguientes:

a) Se recomienda proporcionar un marco de virtualización ligero e independiente del *hardware* e implementar mecanismos de aislamiento y mejora de la seguridad.

b) Se recomienda mejorar la protección de seguridad del propio hipervisor y reducir los vectores de ataques.

c) Se recomienda cooperar con los servidores de la nube periférica y proporcionar mecanismos de detección y prevención de códigos maliciosos del sistema operativo, un fuerte aislamiento de seguridad de las aplicaciones, un entorno de ejecución de confianza y otros mecanismos, a fin de garantizar la confidencialidad y la integridad de las diversas aplicaciones que se ejecutan en el sistema operativo, que se ve afectado por la reducida capacidad de recursos de computación o almacenamiento, ya que las políticas y mecanismos de seguridad tal vez no se sincronicen a tiempo con la nube central o regional.

d) Se recomienda que los proveedores de nube periférica implementen procesos de identificación y autenticación de manera automática, transparente y liviana. Esto se debe a que los nodos extremos y la estructura de red dinámica de la nube distribuida podrían dar lugar a la repetición de la identificación y la autenticación.

8.3.2 Seguridad de la red de nube periférica

Debido al importante número de nodos extremo y a la compleja tecnología de redes, que incrementa las vías de ataques, los atacantes pueden enviar fácilmente paquetes de redes maliciosos a los nodos de la nube periférica o lanzar ataques de denegación del servicio, que afectan a la fiabilidad de la red de nube periférica. Las directrices de seguridad relativas a la red de nube periférica son las siguientes:

a) Se recomienda garantizar la seguridad de protocolo tanto en la etapa de diseño como en la de implementación, que la nube periférica utiliza para satisfacer las diferentes necesidades de los CSC en materia de transmisión de datos.

b) Se recomienda añadir políticas de seguridad adicionales para posibles protocolos vulnerables, por ejemplo, implementando la transmisión de datos a través de redes privadas virtuales (VPN), TLS u otros canales seguros mediante la adición de módulos en las pasarelas.

c) Se recomienda llevar a cabo comprobaciones de la integridad y la seguridad respecto de la transmisión de la red entre máquinas virtuales que pertenecen a diferentes dominios, con miras a garantizar un aislamiento eficaz entre las diferentes unidades comerciales de comunicación. Además, los controladores pueden programar módulos de aislamiento en el entorno visualizado a fin de proporcionar capacidades de aislamiento.

d) Se recomienda realizar la supervisión de seguridad del tráfico de red a fin de alertar sobre los eventos de seguridad a tiempo e implementar respuestas a los incidentes de manera eficaz. Además, los sistemas de protección pueden bloquear directamente el tráfico malicioso.

8.3.3 Seguridad de la web de nube periférica

Las directrices para la seguridad de la web son las siguientes:

a) Se recomienda garantizar una vigilancia a distancia eficaz de las instalaciones de los sistemas de nube periférica.

b) Se recomienda que la seguridad de nube periférica esté acompañada de amplias medidas de educación. Se ha de informar al personal de lo que pueden o no pueden hacer con sus dispositivos y ayudarlos a identificar los riesgos de seguridad.

c) Se recomienda garantizar que los dispositivos más antiguos y desfasados no se sitúen junto a los más sofisticados para reducir los puntos de vulnerabilidad en la red.

8.3.4 Seguridad de los dispositivos extremo en la nube periférica

Las directrices de seguridad de los dispositivos extremo en la nube periférica son las siguientes:

a) Se recomienda bloquear el acceso cuando un dispositivo personal no autorizado intenta acceder a los datos de la nube periférica.

b) Se recomienda configurar la periferia con capacidades que incluyan características como la fuerte autenticación y los nodos de autenticación cifrados.

c) Se recomienda que los protocolos de seguridad de TI gestionen qué dispositivos pueden acceder a la red del sistema de nube periférica y en qué condiciones pueden hacerlo.

d) Se recomienda implementar y supervisar continuamente el entorno de nube periférica.

e) Se recomienda asumir que los dispositivos extremo ya se encuentran en peligro en lugar de confiar automáticamente en la información procedente de un dispositivo, ya que todos los datos pueden ser maliciosos a menos que se demuestre lo contrario.

f) Se recomienda que solo los dispositivos extremo autenticados puedan conectarse y transmitir datos a la nube central.

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

Publicado en Suiza
Ginebra, 2023