Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1233

(09/2021)

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

Seguridad en el ciberespacio – Lucha contra el correo basura

Directrices para contrarrestar los mensajes basura por mensajería instantánea

Recomendación UIT-T X.1233

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	X.1140–X.1149
Protocolos de seguridad (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.1360–X.1369
Seguridad en los sistemas de transporte inteligente (STI)	X.1370–X.1389
Seguridad de tecnología de libro mayor distribuido (DLT)	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido (DLT)	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
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
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
SEGURIDAD DE IMT-2020	X.1800–X.1819

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

Recomendación UIT-T X.1233

Directrices para contrarrestar los mensajes basura por mensajería instantánea

Resumen

En la Recomendación UIT-T X.1233 se establecen directrices cuyo objetivo es ayudar a los proveedores (PS) y los usuarios de los servicios de mensajería instantánea (MI) a contrarrestar los mensajes basura por mensajería instantánea (SPIM), reducir su propagación en el ciberespacio y mejorar la experiencia de los usuarios de MI.

También se analizan supuestos de generación de mensajes basura en el ámbito de la mensajería instantánea, se especifican medidas técnicas y mecanismos que permiten a los proveedores de servicios de MI contrarrestar el SPIM y se establecen directrices para que los usuarios de MI puedan hacerle frente.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1233	03/09/2021	17	11.1002/1000/14773

Palabras clave

Contrarrestar el SPIM, directrices, proveedores de servicios de MI, usuarios de MI.

* 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, https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11830&lang=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 (TIC). 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

Página

1 Alcance 1

2 Referencias 1

3 Definiciones 1

3.1 Términos definidos en otros documentos 1

3.2 Términos definidos en la presente Recomendación 1

4 Abreviaturas y acrónimos 1

5 Convenios 1

6 Casos de mensajes basura por mensajería instantánea 2

7 Directrices para ayudar a los proveedores de servicios de MI a contrarrestar el SPIM 2

7.1 Configuración de funciones anti-SPIM 2

7.2 Supervisión y control del comportamiento 3

7.3 Auditoría y registro 3

7.4 Respuesta de emergencia 4

7.5 Gestión de la evaluación de riesgos 4

7.6 Medidas de protección de la seguridad 5

8 Función de los usuarios de MI en la lucha contra el SPIM 5

9 Directrices para ayudar a los proveedores de servicios u operadores de red a contrarrestar el SPIM 6

Bibliografía 8

Introducción

Gracias a la popularidad de la que gozan, las aplicaciones de mensajería instantánea (MI) se han convertido en un importante vehículo de transmisión de mensajes basura, junto con los servicios vocales, de mensajes cortos (SMS) y de correo electrónico. La MI permite transmitir mensajes de forma eficiente y en tiempo real, lo que facilita en gran medida el contacto social. Sin embargo, también brinda a los remitentes de mensajes basura la oportunidad de enviar mensajes basura por mensajería instantánea (SPIM). El volumen de mensajes basura, ya sean anuncios, material pornográfico u otro contenido de carácter ilegal, como información para la suplantación de identidad, virus, gusanos troyanos o programas espía, enviado por mensajería instantánea está creciendo exponencialmente. En consecuencia, no solo están proliferando los casos de acoso e incluso de pérdidas económicas entre los usuarios, sino que la seguridad del ciberespacio también se está viendo gravemente afectada. La lucha contra el SPIM se ha convertido en un elemento importante para contrarrestar los mensajes basura en general.

Sin embargo, los proveedores de servicios (PS) y los usuarios siguen careciendo de orientaciones sobre cómo contrarrestar el SPIM mientras explotan o utilizan aplicaciones de MI. Esto significa que los esfuerzos por contrarrestar el SPIM no se han gestionado eficazmente. Por consiguiente, urge elaborar normas en la materia, que orienten a los operadores y los usuarios de estas aplicaciones en cuanto a las técnicas y medidas de gestión que pueden aplicar para prevenir el SPIM.

Recomendación UIT-T X.1233

Directrices para contrarrestar los mensajes basura por mensajería instantánea

1 Alcance

En la presente Recomendación se establecen directrices cuyo objetivo es ayudar a los proveedores (PS) y los usuarios de los servicios de MI a contrarrestar los mensajes basura por mensajería instantánea (SPIM). El texto abarca supuestos de generación de mensajes basura en el ámbito de la mensajería instantánea, medidas técnicas y mecanismos que permiten a los proveedores de servicios de MI contrarrestar el SPIM y medidas de respuesta en caso de emergencia para que los usuarios de MI puedan hacerle frente.

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 mensajes basura por mensajería instantánea (SPIM) [b-UIT-T X.1244]: Mensajes basura dirigidos a los usuarios de un servicio de mensajería instantánea.

NOTA – A los efectos de esta Recomendación, no se define el término "correo basura".

3.1.2 spimmer [b-UIT-T X.1244]: Emisor de SPIM.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación, se define el siguiente término:

3.2.1 mensajería instantánea (MI): Intercambio de contenido entre un grupo de usuarios en tiempo casi real. Por norma general, el contenido son mensajes de texto breves, aunque no necesariamente.

NOTA – Sobre la base de [b-IETF RFC 3428].

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

IP protocolo Internet (*Internet protocol*)

MI Mensajería instantánea

OR Operador de red

PS Proveedor de servicios

SMS Servicio de mensajes cortos (*short message service*)

SPIM Mensajes basura por mensajería instantánea (*spam over instant messaging*)

5 Convenios

La expresión "deberá" indica un requisito que ha de cumplirse rigurosamente para observar lo dispuesto en la presente Recomendación.

Las expresiones "debería" y "no debería" indican que una de entre varias posibilidades se considera especialmente adecuada, sin mencionar ni excluir a las demás; o que se prefiere un curso de acción determinado, sin exigirlo necesariamente; o que (en la forma negativa) una determinada posibilidad o un determinado curso de acción se desaprueba, pero no se prohíbe.

La expresión "puede" indica un requisito opcional, cuya aplicación está permitida. Este término no implica que el sistema en cuestión deba prever la opción mencionada.

6 Casos de mensajes basura por mensajería instantánea

El SPIM se está convirtiendo en un importante desafío para los servicios de MI. El SPIM afecta a la calidad de funcionamiento de los sistemas de MI de varias maneras, como el desperdicio de recursos en términos de memoria, unidad central de procesamiento, espacio de almacenamiento y ancho de banda, y puede causar problemas graves, incluida la propagación de gusanos y los ataques de denegación de servicio. Entre los casos de SPIM están, entre otros, los siguientes:

– Utilización de medios automatizados para el registro de un gran número de cuentas con fines nefastos, como la propagación de SPIM.
– Utilización de una cuenta sin autorización de su titular para iniciar sesión y difundir SPIM.
– La falta de mecanismos de seguridad integrados, por ejemplo, un mecanismo de confirmación para la adición de amigos, crea un entorno en el que el SPIM puede propagarse rápidamente.
– Revelación de mensajes a través de un canal de transmisión no seguro. Los piratas informáticos pueden manipular los mensajes instantáneos durante su transmisión. También es posible insertar anuncios o códigos maliciosos en el mensaje original, convirtiéndolo en SPIM.
– Los fabricantes que actúan de manera ilegal alientan a los usuarios a abonarse a SPIM, para obtener beneficios comerciales.

7 Directrices para ayudar a los proveedores de servicios de MI a contrarrestar el SPIM

7.1 Configuración de funciones anti-SPIM

El proveedor de servicios de MI deberá proporcionar funciones anti-SPIM, en el momento en que preste servicios de MI. Entre las funciones anti-SPIM deberían figurar, entre otras, las siguientes:

– detección y control del registro automático de usuarios;
– control por autorización para la adición de amigos;
– detección y limitación de la tasa de envío de mensajes;
– filtrado de mensajes basado en listas negras; y
– establecimiento de una plataforma de reclamaciones para los usuarios, con funcionalidades tales como un sencillo mecanismo de retroalimentación que avise a un proveedor de servicios de MI del SPIM recibido.

Al mismo tiempo, el proveedor de servicios de MI deberá mantener una serie de funciones anti-SPIM en la fase de explotación. Entre las medidas conexas deberían figurar, entre otras, las siguientes:

– mantener bases de datos anti-SPIM, en especial listas de amigos y listas negras, velando por su disponibilidad y estabilidad;
– mantener la información relativa a las quejas de los usuarios, para mejorar la exactitud de la misma; y
– ajustar los umbrales utilizados en las funciones anti-SPIM, como el umbral de limitación de la tasa de envío de mensajes y el umbral del número de quejas que puede recibir una cuenta antes de su adición a una lista negra.

7.2 Supervisión y control del comportamiento

El proveedor de servicios de MI deberá tomar medidas para supervisar los siguientes comportamientos y generar alarmas en los casos en que se detecten anomalías. Entre los comportamientos objeto de supervisión deberían figurar, entre otros, los siguientes:

– Comportamiento relativo al fallo de autenticación. Por ejemplo, cuando se envía un número de solicitudes de autenticación desde la misma dirección de protocolo Internet (IP). Si este comportamiento se produce muchas veces, podría ocurrir que un spimmer estuviera robando cuentas para enviar SPIM. Este comportamiento debería activar una alarma y las solicitudes de autenticación que se enviasen posteriormente desde esa dirección IP deberían ser descartadas.

– Comportamiento relativo al envío de quejas maliciosas. Por ejemplo, un usuario envía un gran número de quejas desde una misma cuenta en una unidad de tiempo determinada; independientemente de que las quejas se refieran a diferentes cuentas o a una sola, si superan en número el umbral establecido, deberían activar una alarma y pasar a ser ignoradas, mejorando así la precisión del sistema.

– Comportamiento relativo a la adición maliciosa de cuentas a listas negras. Por ejemplo, si una serie de cuentas añade una cuenta específica a una lista negra, debería comprobarse si esas cuentas aparecen en alguna lista de cuentas sospechosas. Si la mayoría de ellas figura en una de esas listas, debería activarse una alarma. Estos intentos de añadir una cuenta específica a listas negras no deberían tenerse en cuenta en el cómputo de adiciones de la cuenta en cuestión a una lista negra, mejorando así la precisión de esta lista.

7.3 Auditoría y registro

Los proveedores de servicios de MI deberán adoptar medidas técnicas para auditar y registrar los comportamientos de los usuarios y los incidentes de ciberseguridad, a fin de contrarrestar el SPIM. Entre los registros que el servicio de MI debería auditar figuran, entre otros, los siguientes:

– Registros de comportamiento de usuarios, que incluyan información sobre el comportamiento y la autenticación de los usuarios, entre otros datos. Por ejemplo, el proveedor de servicios de MI debería crear un historial de actividad del usuario (incluidos comportamientos tales como el envío de un número de mensajes que supere el umbral de limitación de la tasa de envío de mensajes, el envío de quejas maliciosas, etc.). Los registros de comportamientos relacionados con el envío de mensajes deberían incluir datos tales como: información sobre la cuenta del remitente (por ejemplo, dirección IP, nombre de usuario, si el remitente aparece en una lista sospechosa o negra), información sobre la cuenta del destinatario, tipo de relación entre el remitente y el destinatario (por ejemplo, si son amigos o no, si pertenecen a un grupo como amigos o no, si son amigos en otros sistemas de MI y si comparten contactos telefónicos). Los proveedores de servidores de MI deberían analizar esta información para detectar actividades sospechosas o maliciosas. Los registros de comportamientos relacionados con quejas maliciosas deberían incluir datos tales como: información sobre la cuenta del denunciante (por ejemplo, dirección IP, nombre de usuario, si aparece en una lista sospechosa o negra), información sobre la cuenta objeto de la queja y número de quejas formuladas en un periodo de tiempo determinado. Si el número de quejas supera el umbral aplicable, las quejas procedentes de la cuenta del denunciante se ignorarán, mejorando así la precisión de la plataforma de reclamaciones.

– Registros de filtrado de SPIM, que incluyan información sobre los comportamientos de filtrado de SPIM y los mensajes filtrados. Los registros de comportamientos relacionados con el filtrado de SPIM deberían incluir datos tales como: información sobre la cuenta remitente del mensaje filtrado (por ejemplo, dirección IP, nombre de usuario, si aparece en una lista sospechosa o negra) y las medidas de filtrado utilizadas (por ejemplo, filtros basados en listas negras, control de la tasa de envío o control por autorización). El mensaje filtrado debería quedar registrado para que pudiera volver a enviarse si se hubiera filtrado por error.

7.4 Respuesta de emergencia

Cada proveedor de servicios de MI debería elaborar un plan de respuesta en caso de emergencia para hacer frente a las principales maniobras relacionadas con el SPIM.

El plan de respuesta en caso de emergencia debería abarcar las principales maniobras en la materia, incluidas las siguientes:

– modificación, invasión o toma de control de la base de datos anti-SPIM del servidor de MI;

– modificación, invasión o toma de control de la plataforma de reclamaciones en materia de SPIM;

– modificación ilegal del umbral de una función de registro automático;

– presentación de quejas contra SPIM a gran escala en una unidad de tiempo determinada.

Cada proveedor de servicios de MI debería determinar el tipo y el grado de cada una de estas actividades en función de la situación real, y definir un proceso de respuesta en caso de emergencia y unas directrices de funcionamiento en caso de emergencia para los distintos tipos y grados de maniobras relacionadas con el SPIM.

Cada proveedor de servicios de MI debería establecer un mecanismo de supervisión y alerta para este tipo de maniobras, detectarlas y notificárselas al personal competente de manera oportuna.

Cada proveedor de servicios de MI también debería resumir las causas de las principales maniobras relacionadas con el SPIM tras implementar la respuesta en caso de emergencia, evaluar la eficacia de las correspondientes medidas de respuesta y rectificar los problemas de manera oportuna.

7.5 Gestión de la evaluación de riesgos

Los proveedores de servicios de MI deberían llevar a cabo una evaluación de riesgos para valorar la probabilidad y la gravedad de las maniobras relacionadas con el SPIM. La gestión de los riesgos debería integrarse en todas las actividades básicas, desde la evaluación de la gestión hasta la evaluación funcional y de la seguridad. La gestión de la evaluación de riesgos debería incluir, entre otras cosas, lo siguiente:

– Cada proveedor de servicios de MI debería llevar a cabo una evaluación de la gestión, que abarcase aspectos tales como la elaboración de una política anti-SPIM y la supervisión de los procesos y estrategias de cumplimiento de las normas de seguridad para mitigar los riesgos inherentes al SPIM; además, debería facilitar la aplicación de la política correspondiente. Cada proveedor de servicios de MI también debería revisar y actualizar la política y el procedimiento de evaluación de riesgos en vigor, con la frecuencia definida por la organización competente o cada vez que se introdujesen cambios significativos en el sistema de MI o en el entorno operativo.

– El proveedor de servicios de MI debería llevar a cabo una evaluación de la seguridad, que incluyera aspectos tales como la automatización del proceso de gestión de las vulnerabilidades mediante la aplicación de normas (por ejemplo, la enumeración de defectos de aplicaciones y configuraciones inadecuadas, y la preparación de listas de comprobación y procedimientos de prueba), con miras a determinar la causa más probable del SPIM (por ejemplo, contraseñas vulnerables, configuraciones poco seguras de los cortafuegos y gusanos

troyanos), y cuantificar las condiciones que predisponen a los principales contratiempos relacionados con el SPIM.

– Cada proveedor de servicios de MI debería llevar a cabo una evaluación funcional, que incluyera aspectos tales como el descubrimiento de los errores ilógicos de procesamiento y en cascada que pueden hallarse en el código de un sistema de MI (por ejemplo, el registro automático de usuarios, la tasa ilimitada de envíos por usuario en un periodo de tiempo determinado, la falta de mecanismos de seguridad integrados y la revelación de mensajes a través de un canal de entrega no seguro) durante la actualización del sistema de MI.

– Cada proveedor de servicios de MI debería evaluar los riesgos con regularidad o revisar y actualizar su política de evaluación de riesgos según proceda. Las evaluaciones de riesgos deberían articularse en torno a tres componentes interrelacionados: las evaluaciones de la gestión, la seguridad y funcionales. Por ejemplo, las evaluaciones de la gestión y de la seguridad deberían llevarse a cabo junto con la evaluación general de riesgos, y la evaluación funcional debería llevarse a cabo antes de la actualización del sistema de MI, durante la misma, o en ambas ocasiones. Al mismo tiempo, el proveedor de servicios de MI debería corregir los fallos legítimos en los tiempos de respuesta definidos por la organización competente, o aplicar controles para evitar que el remitente de mensajes basura explote la vulnerabilidad.

7.6 Medidas de protección de la seguridad

Cada proveedor de servicios de MI debería adoptar medidas de protección de la seguridad para contrarrestar el SPIM. Entre estas medidas deberían figurar, entre otras, las siguientes:

– Cada proveedor de servicios de MI debería instaurar medidas contra los ataques por denegación de servicio distribuido, con el objetivo tanto de proteger la biblioteca de listas negras, la plataforma de reclamaciones, la supervisión de la seguridad y los métodos de auditoría, como de mejorar la disponibilidad de las funciones anti-SPIM.

– El proveedor de servicios de MI debería instaurar medidas antivirus, antitroyanos y antigusanos, con mira a evitar que los remitentes de mensajes basura infecten el servidor, lo controlen y modifiquen las configuraciones anti-SPIM o desactiven las funciones anti-SPIM para poder enviar dichos mensajes.

– El proveedor de servicios de MI debería establecer múltiples métodos de control del acceso en los límites de la red, los sistemas y las aplicaciones del sistema de MI, a fin de evitar el acceso no autorizado de remitentes de mensajes basura que puedan modificar las configuraciones anti-SPIM o desactivar las funciones anti-SPIM para poder enviar dichos mensajes.

– El proveedor de servicios de MI debería establecer métodos de detección de intrusos y protección, con objeto de detectar ataques a la red y evitar que los remitentes de mensajes basura invadan el sistema de MI y modifiquen la configuración o desactiven las funciones anti-SPIM para poder enviar dichos mensajes.

8 Función de los usuarios de MI en la lucha contra el SPIM

Los usuarios de MI deberían tener la posibilidad de configurar los programas de MI para protegerse contra el SPIM cuando los utilicen. Entre las opciones de configuración deberían figurar, entre otras, las siguientes: El usuario de MI debería tener la posibilidad de:

– utilizar un mecanismo de verificación basado en la confirmación, que le permita confirmar las solicitudes de autenticación y las adiciones de grupos, para garantizar que todas las acciones gocen de su aprobación;

– configurar los ajustes para impedir la recepción de mensajes o archivos de usuarios no autorizados;

– configurar una lista negra a su debido tiempo, para impedir la recepción de mensajes o archivos de cuentas sospechosas;
– utilizar una contraseña segura, así como modificarla periódicamente, para evitar que le roben la cuenta y la utilicen para enviar SPIM;
– supervisar la ejecución de las funciones privilegiadas, así como de deshabilitar y modificar las configuraciones establecidas, ya que pueden generar SPIM (por ejemplo, aceptar la solicitud de autenticación de un extraño, etc.).

9 Directrices para ayudar a los proveedores de servicios u operadores de red a contrarrestar el SPIM

Los proveedores de servicios u operadores de red (PS/OR) pueden ayudar a contrarrestar el SPIM adoptando medidas tales como la creación de una plataforma unificada de reclamaciones en materia de SPIM, la creación de una base de datos unificada de listas negras para evitar el SPIM, la puesta a prueba y la verificación de las funciones anti-SPIM de un sistema de MI y la prestación de servicios de detección de SPIM para proveedores de servicios de MI. Esto incluye, entre otras cosas, lo siguiente:

– Los PS/OR deberían crear una plataforma unificada de reclamaciones para múltiples servicios de MI. Dicha plataforma podría admitir quejas de usuarios sobre una cuenta remitente de SPIM y clasificarlas en función de los diferentes servicios de MI. Cuando el número de quejas de usuarios sobre una misma cuenta de MI alcanzase un número determinado, los detalles de la cuenta de MI se enviarían a la base de datos de la lista negra del servicio de MI correspondiente.
– Los PS/OR deberían crear una base de datos unificada de listas negras para múltiples servicios de MI. La base de datos de listas negras se sincronizaría con la base de datos de la lista negra de cada servicio de MI en la red. Existen dos formas de alimentar una lista negra, a saber, mediante la inclusión en la base de datos de dicha lista de cuentas que bien:
  • son objeto de denuncias, a través de la plataforma de reclamaciones anterior; o
  • se han detectado como remitentes de SPIM, a través del servicio de detección de SPIM.
– Los PS/OR deberían proporcionar un servicio de verificación basado en pruebas de marcación periódicas para proveedores de servicios de MI, a fin de evitar que las funciones anti-SPIM de un sistema de MI puedan desactivarse, por ejemplo, a causa de un ataque de un pirata informático. Si de la verificación resulta que la función correspondiente no está activada, el PS/OR puede enviar una alarma al proveedor de servicios de MI. Entre las opciones de verificación basadas en pruebas de marcación figuran, entre otras, las simulaciones de:
  • un procedimiento de registro automático, y la comprobación de si el sistema de MI es capaz de detectarlo e impedirlo;
  • el envío de múltiples mensajes por una cuenta en una unidad de tiempo determinada (el número de mensajes superaría el umbral establecido por el sistema de MI), y la comprobación de si el sistema de MI puede detectar y descartar los mensajes enviados por la cuenta posteriormente;
  • el envío de un mensaje por una cuenta incluida en una lista negra, y la comprobación de si el sistema de MI es capaz de descartarlo; y
  • las quejas maliciosas, y la comprobación de si el sistema de MI es capaz de detectarlas y descartarlas.

– Los PS/OR pueden prestar servicios de detección de SPIM al proveedor de servicios de MI. A tal efecto, deberían firmar un acuerdo de prestación de servicios con cada proveedor de servicios de MI, en el que se estipulasen los términos de confidencialidad, para proteger la privacidad de los usuarios. Los PS/OR siguen el siguiente proceso para detectar el SPIM:

  • implantan sistemas de detección en los nodos clave de la red y detectan el encabezamiento de paquetes de los mensajes de MI autorizados por un proveedor de servicios de MI;

  • analizan el comportamiento relativo al envío de varios mensajes por MI mediante una cuenta de MI – Si el número de mensajes enviados por la cuenta de MI dentro de una unidad de tiempo determinada supera el umbral establecido, puede determinarse que la cuenta está enviando SPIM;

  • descartan directamente los mensajes de MI enviados por la cuenta antes mencionada;

  • incluyen dicha cuenta en la base de datos de la lista negra.

El servicio de detección de SPIM proporcionado por los PS/OR permite localizar y descartar el SPIM en el límite cercano, lo que no solo facilita el ahorro de ancho de banda de red, sino que también evita el consumo de recursos del servidor de MI.

Bibliografía

[b-UIT-T X.1244] Recomendación UIT-T X.1244 (2008), *Características generales de la lucha contra el correo basura (spam) en aplicaciones multimedios basadas en IP*.

[b-IETF RFC 3428] IETF RFC 3428 (2002), *Session initiation protocol (SIP) extension for instant messaging*. Disponible en: https://tools.ietf.org/html/rfc3428 [consultado el 09/10/2021].

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, 2021