Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1240

(04/2008)

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

Seguridad en el ciberespacio – Lucha contra el correo basura

Tecnologías utilizadas contra el correo basura

Recomendación UIT-T X.1240

Unión Internacional de Telecomunicaciones

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	
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	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

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

Recomendación UIT-T X.1240

Tecnologías utilizadas contra el correo basura

Resumen

En esta Recomendación se especifican los conceptos básicos, las características y los efectos del correo basura, así como las tecnologías utilizadas contra dicho tipo de correo. También se presentan las soluciones técnicas actuales y las actividades que están llevando a cabo diversas organizaciones de normalización y otras organizaciones pertinentes a fin de luchar contra el correo basura. Se facilitan directrices e información a los usuarios que desean desarrollar soluciones técnicas contra este tipo de correo. Esta Recomendación servirá de base para la elaboración futura de Recomendaciones técnicas contra el correo basura.

Orígenes

La Recomendación UIT-T X.1240 fue aprobada el 18 de abril de 2008 por la Comisión de Estudio 17 (2005-2008) del UIT-T por el procedimiento de la Resolución 1 de la AMNT.

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, 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 la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Introducción

Con arreglo a la Resolución 52 de la AMNT-2004, "Medios técnicos contra el correo basura", se inició una labor de normalización a fin de elaborar Recomendaciones que permitan luchar contra el correo basura por medios técnicos. La presente Recomendación forma parte de una serie sobre la lucha contra el correo basura que incluye directrices, requisitos, un marco técnico y estrategias técnicas. Se elaborarán como documentos separados otras Recomendaciones sobre la lucha contra el correo basura en las aplicaciones multimedios IP, por ejemplo en la telefonía IP, la mensajería instantánea y las conferencias.

Recomendación UIT-T X.1240

Tecnologías utilizadas contra el correo basura

1 Alcance

En esta Recomendación se especifican los conceptos básicos, las características y los efectos del correo basura, así como las tecnologías utilizadas contra dicho tipo de correo. También se presentan las soluciones técnicas actuales y las actividades que están llevando a cabo diversas organizaciones de normalización y otras organizaciones pertinentes a fin de luchar contra el correo basura. Se facilitan directrices e información a los usuarios que desean desarrollar soluciones técnicas contra este tipo de correo. Esta Recomendación servirá de base para la elaboración futura de Recomendaciones técnicas contra el correo basura.

NOTA – La utilización del término "identidad" en esta Recomendación no indica su significado absoluto. En particular, no constituye ninguna validación positiva.

2 Referencias

Ninguna.

3 Definiciones

En esta Recomendación se definen los siguientes términos:

3.1 generador de mensajes destinados al hurto de identidades y credenciales financieras (*phisher*): Entidad o individuo que lanza ataques utilizando mensajes de este tipo.

3.2 hurto de identidades y credenciales financieras (*phishing*): Ataques en los que se emplean técnicas de ingeniería social y subterfugios técnicos para hurtar los datos de identificación personal y las credenciales de las cuentas financieras del consumidor. Los métodos de ingeniería social se valen de correos electrónicos en los que se usurpa la identidad de alguna entidad ("spoofed e-mail") para hacer que los consumidores accedan a sitios web falsificados destinados a engañar a los destinatarios para que divulguen datos financieros tales como números de tarjetas de crédito, nombres de usuario de cuentas, contraseñas o números de la seguridad social. Al plagiar las marcas, emblemas y presentación de los sitios web de los bancos, las empresas de venta por Internet y las compañías de tarjetas de crédito, los remitentes de este tipo de correo consiguen a menudo que el destinatario responda. Algunos métodos técnicos subrepticios permiten "plantar" (de ahí la expresión inglesa "*pharming*") programas informáticos malintencionados en los PC de los usuarios que les permiten subutilizar directamente dicha información, a menudo a través de programas espía del tipo "caballo de Troya".

3.3 correo basura (*spam*): El significado de "correo basura" varía según la percepción que se tiene en cada país de la privacidad y de lo que constituye correo basura, visto desde una óptica tecnológica, económica, social y práctica. De hecho, su significado evoluciona y se amplía a medida que se desarrollan nuevas tecnologías y se presentan más posibilidades de utilización indebida de las comunicaciones electrónicas. Si bien no existe una definición universalmente aceptada del correo basura, este término se utiliza comúnmente para describir aquellas comunicaciones electrónicas masivas y no solicitadas, transmitidas a través del correo electrónico o la mensajería móvil, destinadas a promocionar la venta de productos o servicios comerciales.

3.4 generador de correo basura (*spammer*): Entidad o individuo que crea y envía correo basura.

4 Siglas y acrónimos

En esta Recomendación se utilizan las siguientes siglas y acrónimos:

API Interfaz de programa de aplicación (*application programming interface*)

CSV Validación de servidor certificado (*certified server validation*)

DKIM Correo identificado mediante la tecnología DomainKeys (*DomainKeys identified mail*)

DNS Sistema de nombres de dominio (*domain name system*)

DSN Notificación de estado de entrega (*delivery status notification*)

HTML Lenguaje de etiquetado hipertexto (*HyperText markup language*)

IM Mensajería instantánea (*instant messaging*)

META Ampliaciones de mensajes a los efectos de autorización de transmisión (*message enhancements for transmission authorization*)

MMS Servicio de mensajería multimedios (*multimedia message service*)

MTA Agente de transferencia de mensajes (*mail transfer agent*)

OCDE Organización de Cooperación y Desarrollo Económicos

OPES Servicios adaptadores de conexión integral (*open pluggable edge services*)

PGP Nivel de privacidad aceptable (*pretty good privacy*)

PSI Proveedor de servicios Internet (*Internet service provider*)

PTR Registro de puntero (*pointer record*)

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

SMTP Protocolo de transferencia de correo simple (*simple mail transfer protocol*)

SPF Convenio de remitentes (*sender policy framework*)

TEOS Norma abierta sobre correo electrónico de confianza (*trusted email open standard*)

5 Convenios

Ninguno.

6 Presentación de la lucha contra el correo basura

6.1 El concepto de correo basura y sus características

Si bien no existe una definición universalmente aceptada del correo basura, este término se utiliza comúnmente para describir aquellas comunicaciones electrónicas masivas y no solicitadas, transmitidas a través del correo electrónico, la mensajería móvil (SMS, MMS) y los servicios de mensajería instantánea, normalmente destinadas a promocionar la venta de productos o servicios comerciales.

Aunque el correo basura más conocido es el que se distribuye a través del correo electrónico, la expresión también se aplica a otros abusos similares que se cometen por otros medios, por ejemplo, a través de la mensajería con teléfonos móviles, de la telefonía IP, de la mensajería instantánea, de los grupos de noticias de Usenet, de los motores de búsqueda en la web y de las bitácoras (*blogs*). El contenido de los correos basura puede ir desde anuncios publicitarios hasta material pornográfico chocante. El correo basura que se distribuye a través del correo electrónico tiene varios efectos nocivos sobre los usuarios y sobre los proveedores de servicios Internet (PSI), a saber:

– Los destinatarios de dichos correos y los PSI emplean mucho tiempo, dinero y energía para identificar, suprimir y filtrar el correo basura.

– Es posible que el correo basura a través del correo electrónico contenga material engañoso atrayente para los destinatarios o material para adultos inadecuado para los niños.

– Los usuarios del correo electrónico y los PSI se ven afectados por el despilfarro de recursos de la red y de almacenamiento.

– La proliferación de virus y de programas espías puede convertirse en una amenaza para la seguridad de la red.

– El correo basura a través del correo electrónico reduce la visibilidad de los mensajes normales e importantes.

Un fenómeno reciente es el de la utilización creciente del correo basura con fines fraudulentos y delictivos, incluidos los intentos de obtención de información financiera (por ejemplo, números de cuentas y contraseñas) que se hacen simulando que los mensajes proceden de fuentes fiables ("*brand-spoofing*" (usurpación de marca) o "*phishing*" (hurto de identidades y credenciales financieras)), al igual que como medio de dispersión de virus y "gusanos" ("*worms*").

En los ataques de "*phishing*", se emplean técnicas de ingeniería social y subterfugios técnicos para apropiarse de la identidad de la persona y de sus credenciales financieras. Los métodos de ingeniería social se valen de correos electrónicos en los que se usurpa la identidad de alguna entidad para hacer que los consumidores accedan a sitios web falsificados destinados a engañar a los destinatarios para que divulguen datos financieros tales como números de tarjetas de crédito, nombres de usuario de cuentas, contraseñas o números de la seguridad social. Al plagiar las marcas, emblemas y presentación de los sitios web de los bancos, las empresas de venta por Internet y las compañías de tarjetas de crédito, los remitentes de este tipo de correo consiguen a menudo que el destinatario responda. Los mecanismos de subterfugio técnico permiten "plantar" programas informáticos malintencionados en los PC de los usuarios, que permiten subutilizar directamente sus credenciales, a menudo a través de programas espía para el registro de contraseñas del tipo "caballo de Troya". Los programas informáticos malintencionados del tipo "*pharming*" desvían a los usuarios hacia sitios fraudulentos o hacia servidores alternativos, habitualmente por medio de la apropiación indebida o de la contaminación del sistema de nombres de dominio (DNS).

Los spammers han demostrado con creces su habilidad para evitar ser detectados, recurriendo por ejemplo a la falsificación del origen del correo electrónico y a la utilización de contenido aleatorio para eludir los filtros. El problema ha adquirido tales dimensiones que en muchos países se han promulgado leyes para prevenirlo -aunque los métodos y remedios varían en función del país. Al mismo tiempo, la opinión es cada vez más unánime en el sentido de que, para que la lucha contra el correo basura sea eficaz, la coordinación y la cooperación internacionales resultan indispensables.

6.2 Enfoques de la lucha contra el correo basura

Al ser tan nocivo para los usuarios del correo electrónico, los PSI y los operadores de red, en muchos países se han desarrollado tecnologías y adoptado reglamentaciones para luchar contra la distribución de correo basura. No obstante, es difícil combatir dicho correo eficazmente utilizando una sola medida como, por ejemplo, los filtros o las sanciones penales, puesto que el correo basura

es un problema complejo. Por este motivo, para luchar eficazmente contra el correo basura, conviene aplicar varios métodos de manera simultánea:

– Reglamentación: Debe aprobarse una reglamentación contra el correo basura que permita una respuesta adecuada de los usuarios frente a dichos correos, así como incrementar la eficacia de las tecnologías para contrarrestarlos, tales como el filtrado de mensajes. Además, la reglamentación puede ayudar a los usuarios y a los PSI a protegerse del correo basura ilegal.

– Tecnología: El desarrollo de las tecnologías de lucha contra el correo basura resulta indispensable para impedir de manera eficaz la circulación de grandes cantidades de correos basura. Es preciso desarrollar diversas tecnologías tanto para impedir el envío de correo basura como para identificarlo y filtrarlo eficazmente.

– Medidas de carácter industrial: Conviene que los actores industriales, tales como los PSI o los operadores de red, desarrollen e instalen diversos tipos de tecnologías contra el correo basura, incluyendo la creación de listas negras o de listas de remitentes aceptados ("listas blancas"), y de funciones de filtrado. Los PSI también pueden adoptar políticas destinadas a luchar contra dicho correo.

– Cooperación internacional: Habida cuenta de que las redes de telecomunicaciones no conocen fronteras y de que la creación y las repercusiones del correo basura no se limitan al ámbito nacional, la cooperación internacional resulta necesaria. Dicha cooperación también es útil a la hora de compartir información acerca de la adopción de reglamentaciones eficaces, del desarrollo de tecnología contra el correo basura y de la formación destinada a los usuarios y los PSI.

– Formación: Es fundamental que los usuarios y los PSI reciban una formación que permita reducir al máximo los perjuicios ocasionados por el correo basura a través del correo electrónico. Se confía en que, gracias a dicha formación, los usuarios del correo electrónico tomen medidas apropiadas contra el correo basura, y los PSI adopten políticas y tecnologías contra este tipo de correo.

Entre las diversas medidas contra el correo basura presentadas más arriba, esta Recomendación se centra en los mecanismos técnicos para evitar dicho correo, tales como el desarrollo y aplicación de tecnologías específicas.

7 Tecnologías contra el correo basura

En el Informe presentado por el Grupo de Tareas de la OCDE para el correo basura [b-OECD TF], se tratan varios elementos destinados a luchar contra dicho correo, incluidos los enfoques reglamentarios, los problemas de aplicación de las leyes y las soluciones técnicas. En esta cláusula de la presente Recomendación se incluye una referencia al "Elemento IV" del citado Informe, que se refiere a las tecnologías de lucha contra el correo basura. Conviene tenerlo en cuenta, puesto que la herramienta contra el correo basura se publicó en mayo de 2006 y no ha sido actualizada desde entonces.

En esta cláusula se incluye una descripción de las diversas tecnologías contra el correo basura y las capacidades de que disponen en la actualidad, así como de los métodos que deben emplearse cuando se recibe dicho tipo de correo. Cualquier intento de luchar eficazmente contra el correo basura debe implicar la gestión inteligente y articulada de varias de estas tecnologías. Ninguno de los métodos descritos logrará un éxito total si se utiliza de manera aislada. La combinación efectiva de varias tecnologías contra el correo basura permite reducir drásticamente las repercusiones del correo basura para el sistema.

7.1 Visión general

El correo basura presenta desafíos técnicos muy complejos y, en consecuencia, las soluciones para eliminarlo han de basarse en medidas técnicas apropiadas. Si bien, la acción gubernamental y la legislación son útiles, no bastan para hacer frente a los desafíos planteados por este tipo de correo. De hecho, el correo basura es un problema fundamentalmente técnico, que resulta de un defecto del protocolo SMTP. El carácter técnico del problema hace especialmente difícil la identificación de los remitentes de dichos correos por parte de las autoridades y, por lo tanto, castigarlos.

A pesar de las diversas definiciones del correo basura, se dispone de tecnologías y técnicas eficaces para ayudar a controlar el problema de los correos electrónicos no deseados. Esta cláusula tiene como finalidad presentar una visión imparcial y de carácter general de los diversos tipos de herramientas y métodos técnicos, así como de los factores que se han de tener en cuenta antes de su aplicación. Se refiere de manera específica a las herramientas, y no a las soluciones. Si bien la tecnología permite abordar muchos de los problemas generados por el correo basura, y de hecho puede "resolver" algunos de los inconvenientes específicos relacionados con él, una solución global al problema sólo puede lograrse a través de una combinación de múltiples factores, tales como la tecnología, las políticas (incluida la regulación, cuando proceda), la práctica y la formación.

Las herramientas contra el correo basura funcionan en distinto planos – en el origen, en la troncal, en la pasarela y en el ordenador del usuario – y pueden utilizarse de manera aislada o en combinación. En el sitio web www.oecd-antispam.org se puede acceder a información y recursos actualizados al respecto.

Esta cláusula está especialmente destinada a los administradores de los servidores de correo electrónico, para que puedan comprender mejor las ventajas y los puntos débiles de cada técnica de filtrado, de manera que puedan escoger el programa más adaptado a sus políticas y necesidades en materia de correo electrónico, en función de la arquitectura correspondiente. La cláusula se centra en las prácticas que se aplican al correo electrónico entrante, pero también sería útil contar con prácticas destinadas a reducir el correo basura saliente. Al igual que los operadores de los servidores que reciben correo, los de los servidores que lo envían también tienen un papel que desempeñar. Los operadores de los servidores que envían correo pueden valerse de la limitación del enlace de salida y del bloqueo del puerto 25, y emplear otras medidas para reducir la cantidad de correo basura que se origina en sus servidores.

Las herramientas de lucha contra el correo basura tienen que centrarse tanto en el correo propiamente dicho como en los comportamientos conexos. Habida cuenta de esta diversidad de factores, muchos instrumentos y métodos se basan en conjuntos de reglas o hipótesis que funcionan de manera autónoma o en combinación para identificar los correos electrónicos sospechosos. Con el tiempo, el correo basura ha crecido hasta abarcar un número creciente de virus y programas informáticos malintencionados. Esto hace que la tecnología defensiva no pueda limitarse a las herramientas basadas en texto, sino que debe incluir herramientas de análisis de los factores de comportamiento y de contexto para determinar si debe aceptarse o rechazarse un correo concreto o incluso los intentos de conexión. Teniendo en cuenta la amenaza creciente que representa el correo basura, cabe esperar que las tecnologías contra dicho correo incluyan, o se combinen con, tecnologías avanzadas de seguridad y autorización.

7.2 La importancia del contexto de la herramienta/tecnología

Algunas de las herramientas/tecnologías consideradas en esta cláusula se han desarrollado específicamente para su aplicación a la entrada de la plataforma de correo electrónico, mientras que otras pueden aplicarse de manera más eficaz tras la recepción de los mensajes y antes de su entrega al destinatario final. Es importante señalar que algunas herramientas también se instalan en el computador del usuario. En cada etapa de la aplicación de filtros, la finalidad de una regla puede ser la de rehusar o rechazar el mensaje electrónico, o simplemente marcarlo o remitirlo al buzón de correo basura del usuario final.

Por consiguiente, la eficacia y utilidad de cada regla sólo pueden establecerse en términos del contexto concreto en el que se aplica, del momento del proceso de distribución de mensajes en que actúa y de lo que ocurra al final con la comunicación.

7.3 Combinación de pruebas

Todo enfoque destinado a acabar con el correo basura debería basarse en la tecnología. Se ha de ser consciente de que ninguna de las tecnologías que aquí se describen a continuación puede actuar como "panacea" o solución inmediata para resolver los problemas generados por el correo basura. En lugar de ello, ha de considerarse que todas las tecnologías son complementarias y serán más eficaces si se emplean de manera combinada. Para reducir el efecto nocivo de este tipo de correo sobre un sistema determinado, se requiere la integración de diversas tecnologías.

Las pruebas no deberían aplicarse buscando un resultado de éxito o fracaso total. Al contrario, es preferible combinarlas con el fin de lograr la intercepción del máximo número de mensajes de correo basura y, al mismo tiempo, reducir al mínimo el número de mensajes legítimos que se interceptan o rechazan inadvertidamente.

– Rechazo de tipo "todo o nada" – Es una de las posibles respuestas de los sistemas que utilizan listas negras. Se rechaza todo mensaje que no supere la prueba. No obstante, la posibilidad de que se produzca un error depende de la fase del proceso de distribución en que se efectúe la prueba.
– Privilegio de acceso – Es una de las posibles respuestas de los sistemas que utilizan listas blancas. Se acepta todo mensaje que supere la prueba. En este caso, es imposible que se rechace un mensaje legítimo, pero puede haber "falsos negativos". Por ejemplo, de poco sirve una lista blanca de nombres de dominio si el dominio del remitente no está autentificado utilizando el Convenio de remitentes (SPF, *sender policy framework*) o el correo identificado mediante la tecnología DomainKeys, (DKIM, *domainkeys identified mail*).
– Muchos correos basura o gusanos (*worms*) pretenden provenir de marcas comerciales conocidas, con la esperanza de obtener el privilegio de acceso.
– Sistema de puntuación (*scoring*) – Ésta es la manera en que los programas combinan las pruebas. Al evitar los inconvenientes del tipo "todo o nada", el método de puntuación es muy recomendable. Sin embargo, consume bastantes recursos físicos y es necesario actualizar constantemente los factores de puntuación para obtener el máximo número de aciertos y el menor número de falsos positivos.

El método que se suele utilizar consiste en aplicar primero varias pruebas de tipo "todo o nada", y luego puntuar los mensajes que han logrado superarlas.

7.4 Tipos de tecnologías contra el correo basura

7.4.1 Autentificación del correo electrónico

Los métodos de autentificación de correo electrónico forman parte de la categoría de reglas, las cuales, si bien ayudan a luchar contra el correo basura, no son tecnologías específicas para la lucha contra el mismo.

Tal vez un ejemplo sirva para aclarar esta afirmación. El hecho de tener un documento de identidad no es totalmente fiable, dado que los delincuentes también pueden disponer de él. A pesar de ello, los requisitos de transparencia siempre resultarán más beneficiosos para los remitentes legítimos que para quienes envían correo basura.

7.4.2 SPF y/o ID de remitente

Uno de los factores que más contribuyen a la proliferación del correo basura es la habilidad de quienes lo generan para ocultar la verdadera dirección de retorno de sus mensajes. La arquitectura del correo electrónico no implica un contacto previo entre el remitente y el destinatario de un mensaje. Esto hace que no sea posible limitarse a la autentificación sistemática. El problema es cada vez más grave, puesto que se han empleado direcciones falsas en estafas organizadas por medio del *phishing*, en las que se engaña al destinatario para que dé a conocer sus números de tarjetas de crédito y otras informaciones personales.

La aplicación de esta tecnología aún está en fase de introducción y, por lo tanto, adolece de una falta de normalización, pero la autentificación funciona marcando aquellos correos electrónicos cuyos remitentes verdaderos no pueden ser identificados. Un servidor que recibe mensajes puede optar por bloquear los mensajes que no estén autentificados, pero la tecnología no le impone hacerlo de manera sistemática. Esta tecnología se limita a poner marcas a los mensajes. La ventaja principal de la autentificación a escala del dominio radica en que permite reducir significativamente la cantidad de falsos positivos y filtrar de manera más fiable los mensajes sobre la base de la reputación. El mayor costo en que incurren los usuarios de esta tecnología se compensa por la entrega garantizada de los mensajes si los remitentes han sido autentificados y están utilizando el sistema legítimamente, o por un menor riesgo de procesos judiciales por utilización indebida de marcas registradas. Los detalles del proceso de verificación varían según el modelo escogido, y en la actualidad existen varios modelos de autentificación de servidor. Dos de los más utilizados son el convenio de remitentes (SPF) y el ID de remitente (*Sender-ID*).

Ambas técnicas pueden discutirse conjuntamente ya que comparten diversas características. No obstante, resulta más difícil determinar por cual de las dos optar.

SPF y Sender-ID se pueden emplear para verificar si un servidor de correo electrónico está autorizado para enviar un mensaje en nombre de un dominio determinado. Esto se logra a través de la publicación de un registro en el sistema de nombres de dominio (DNS, *domain name system*), sistema que establece la lista de servidores autorizados para cada dominio. Ambas técnicas difieren básicamente en la identidad que se debe verificar. SPF comprueba el MAIL FROM [b-IETF RFC 2821] del mensaje, mientras que Sender-ID verifica los encabezamientos [b-IETF RFC 2822].

Los administradores de servidores adoptan dos tipos de medidas – publican registros SPF en el DNS y los comprueban cuando llega un mensaje. Según un reciente informe [B-Lyris], actualmente la utilización de un registro SPF inadecuado reduce drásticamente la posibilidad de que se entregue un mensaje.

La autentificación del correo electrónico mediante la verificación de la dirección IP del servidor del remitente ayudará a reducir y a controlar el correo basura en el futuro. Es probable que esto requiera la creación de servicios de mayor nivel que el de autentificación, tales como las listas blancas privadas, los servicios de reputación y los servicios de autorización.

7.4.3 DKIM y/o META

El método del correo identificado mediante la tecnología DomainKeys, (DKIM, *DomainKeys identified mail*) y el método de ampliaciones de mensajes a los efectos de autorización de transmisión (META, *message enhancements for transmission authorization*) sirven para autentificar el dominio del remitente haciendo que el servidor de correo añada automáticamente una firma criptográfica. Esta autentificación del correo mediante una firma criptográfica podría servir en el futuro para reducir y controlar el correo basura.

El DKIM es el más conocido de estos modelos. Con este modelo, todos los mensajes salientes tienen que tener una firma digital o una clave privada. Los mensajes entrantes se autentifican en el nivel de los servidores de dominio y de correo electrónico, asegurándose de que la clave privada se

corresponde con la clave pública registrada. De esta manera, se garantiza que el mensaje sólo puede proceder del PSI de origen. Gracias al DKIM, el servidor de dominio del remitente tiene la garantía de que los mensajes se entregan sólo a los PSI que utilizan dicho método. El DKIM acaba de ser aprobado como RFC por el Grupo Especial sobre Ingeniería de Internet (IETF), convirtiéndose así en la norma IETF.

7.5 Existencia del dominio del remitente y provocación de una respuesta

A menudo, quienes envían correo basura lo hacen utilizando una dirección de origen que no existe. Es posible fijar una regla que filtre dichos mensajes, por ejemplo la directiva Postfix reject_unknown_sender_domain o la directiva BadMX j-chkmail. También se puede verificar la validez del registro del servidor entrante (MX) para el dominio dado en el campo "from" del mensaje. Algunos remitentes de correo basura crean un registro MX fantasma con el fin de evitar las respuestas de los destinatarios molestos que protestan por el correo (por ejemplo, el MX apunta a la dirección 127.0.0.1, es decir al remitente local).

Estas reglas utilizan una pequeña cantidad de tráfico DNS, la cual muy probablemente se habría empleado de todos modos en la respuesta, y también pueden rechazar cierta cantidad de correo basura.

7.6 Existencia de un registro de puntero (PTR, *pointer record*)

Se puede utilizar un PTR del DNS para traducir la dirección IP del servidor del remitente en un nombre, aunque sin comprobar necesariamente que dicho nombre se corresponda con el dominio del remitente.

La incorporación de estos registros no siempre está bajo el control del dominio del remitente (si, por ejemplo, no existe delegación addr.arpa por el IP), la cual, aunque esté justificada, tal vez incumpla la obligación. Estos registros pueden servir para determinar la fuente de un mensaje de correo electrónico y si es de confianza. Asimismo, es posible emplearlos para determinar si un mensaje proviene de una dirección IP residencial, o para redirigir un mensaje de error hacia el servidor adecuado.

7.7 Listas negras/listas blancas

Los métodos tradicionales de filtrado y el seguimiento de las quejas que se presentan en las comunidades de usuarios pueden conducir en último término al establecimiento de listas de remitentes aceptables (*listas blancas*) y listas de sospechosos de generar correo basura (*listas negras*). Este enfoque resulta a menudo ser una solución demasiado drástica como para ser aceptada por la mayoría de los usuarios. Las listas blancas requieren mucho tiempo para su establecimiento, y además tienen que ser actualizadas permanentemente. Las listas negras también requieren este tipo de verificación. Toda lista requiere mecanismos y procedimientos de actualización que se ocupen de los falsos positivos y de las quejas fraudulentas. La posibilidad de fraude y la existencia de repetidores sin control de acceso (abiertos) también pueden crear problemas ligados a la aparente procedencia del correo de una determinada fuente.

Las listas negras se basan en el principio del establecimiento de listas de fuentes de correo basura. Pueden incluir los nombres de máquinas, direcciones IP o direcciones electrónicas. Pueden ser aplicadas por una entidad determinada para su uso compartido, o introducidas y mantenidas por un servidor para que respondan a sus propios requisitos.

Gracias a los agentes de transferencia de mensajes (MTA, *mail transfer agent*) existentes, esta prueba se puede llevar a cabo en la sesión SMTP y, de esta manera, desembocar en un rechazo aun antes de que se envíe el mensaje. En algunas listas se incluyen repetidores abiertos que son no propiamente fuentes de correo basura. Es posible que las plataformas a las que se envía el correo consideren ilegítima esta configuración de repetidores abiertos.

La calidad de las listas negras varía bastante, en función de la profesionalidad de quien las elabora. En muchos casos están mal administradas, han sido abandonadas o son de dudosa integridad: es posible añadir nombres con rapidez, los criterios aplicados pueden ser poco transparentes, y la eliminación de la lista puede resultar prácticamente imposible o llevarse a cabo previo pago. Este problema se debe principalmente a la ausencia de un código de conducta o cualquier otra regulación que imponga una disciplina y limite el funcionamiento de las listas negras. Si se quiere utilizar esta solución en el futuro, será indispensable un esfuerzo de cooperación para establecer una lista de prácticas óptimas, especificando claramente cuáles son los casos en que pueden incluirse direcciones en una lista negra y las condiciones para sacarlas de la misma.

Es inevitable que las listas negras contengan deficiencias que impedirán que ciertos mensajes legítimos lleguen al consumidor. Este problema, conocido como el problema de los falsos positivos, ha dado lugar a procesos judiciales en casos en que remitentes legítimos consideraron haber sido incluidos por error en la lista negra de un PSI. Además, el problema de los falsos positivos tiene el gran inconveniente de que puede provocar que los usuarios sólo confíen en las tecnologías de filtrado tradicionales para cerrar el paso al correo basura. Sin embargo, la mayoría de las medidas contra el correo basura pueden producir falsos positivos. La autentificación de nivel de dominio debería contener este problema.

Aunque su utilización causa muchos problemas, las listas negras son una manera rápida de rechazar la conexión de aquellas máquinas cuyo comportamiento amenaza la seguridad o la calidad de los servicios de la plataforma a la que se envía el correo, o para rechazar mensajes provenientes de determinados remitentes.

7.8 La dirección del servidor remitente "dinámica" o "residencial"

Se trata de una modalidad específica de lista negra en la que el criterio para añadir una dirección a la lista es el hecho de que la dirección IP del remitente cuyos mensajes se están bloqueando corresponda a la máquina de un abonado individual a un PSI, y no al servidor de correo electrónico de una organización. La idea es que un abonado normal no envía correo directamente utilizando el SMTP, sino que pasa a través del PTA de su proveedor. Esto suele indicar que la máquina que se está bloqueando está enviando directamente correo basura desde la dirección de un usuario o, a menudo, que los mensajes están siendo enviados sin el consentimiento del usuario (es decir, la máquina ha sufrido un ataque y se ha convertido en un "zombie" que envía mensajes).

Las listas de este tipo no siempre son de fiar, dado que la mayoría de ellas han sido compiladas utilizando métodos heurísticos, tales como la presencia de la partícula "adsl" en el nombre de la máquina. La gestión de estas listas también consume bastantes recursos.

En cambio, algunas de estas listas, sobre todo las que establece el mismo servidor que las utiliza, pueden emplearse para distinguir entre los servidores autorizados para determinado dominio y las listas residenciales. Además, algunos dominios publican las selecciones de direcciones residenciales para su dominio.

Puede decirse que se trata de una prueba que discrimina entre "consumidores puros" y "proveedores". Estos últimos consideran legítima la política que permite al propietario de un dominio rechazar la conexión de sus máquinas a direcciones residenciales, dado que éstas son en la actualidad las principales fuentes de correo basura. Sin embargo, los consumidores aducen que el correo basura existe, y que debe protegerse la libertad de utilización del correo electrónico.

7.9 Filtrado

Es la tecnología más utilizada en la lucha contra el correo basura. Sus principales ventajas radican en que los filtros son fáciles de utilizar y en la flexibilidad de que disponen los usuarios para decidir cuáles son los mensajes que han de tratarse como correos basura. Los filtros heurísticos requieren que los usuarios especifiquen criterios, tales como palabras clave o una dirección de remitente, que harán que el filtro impida que ciertos mensajes lleguen al buzón de correo del consumidor. Los

remitentes de correo basura que comenten errores deliberados al escribir las palabras o las escriben en otro idioma eluden fácilmente la acción de filtros basados en palabras clave. Los filtros de tipo bayesiano se basan en la experiencia, y establecen estadísticas de los mensajes en un cuadro de reconocimiento, para que los usuarios puedan utilizarlas en el futuro como referencia para distinguir entre el correo basura y el correo legítimo. En este caso, el filtro sólo deja pasar aquellos mensajes que se parezcan a los anteriores correos legítimos del usuario. En un estudio realizado por la U.S. Federal Trade Commission en 2005 [b-FTC], se demostró que los filtros pueden bloquear un 90% del correo basura.

7.9.1 Filtros heurísticos

Son filtros que se basan en la comprobación de la presencia en el mensaje de ciertas características comunes del correo basura, tales como la utilización exclusiva del HTML o el tipo de consumidor al que se dirige el mensaje. La fiabilidad de la prueba se mejora a través de un proceso de aprendizaje basado en un conjunto de mensajes reconocidos como correo basura y en otro de mensajes legítimos (por tanto, las puntuaciones no son asignadas por una persona a fin de reducir la subjetividad).

Estos filtros conllevan el riesgo de clasificar como correo basura mensajes legítimos que empleen técnicas propias de quienes generan dicho tipo de correo (por ejemplo, los mensajes espectaculares en formato HTML). Además, debe señalarse que los filtros consumen grandes recursos de computación.

Estos filtros pueden detectar un alto porcentaje del correo basura, y no requieren entrenamiento ni configuración. No obstante, puesto que dichos filtros proceden a un gran número de pruebas, es conveniente saber que se puede decidir las pruebas que se van a realizar y qué método de puntuación se ha de aplicar para considerar que los mensajes son correo basura.

7.9.2 Filtros basados en palabras clave

Filtros binarios que buscan palabras clave ("Viagra," etc.). Hay un riesgo muy alto de falsos positivos, y resulta muy fácil eludir estos filtros introduciendo espacios, alternando caracteres y cometiendo deliberadamente errores de ortografía.

7.9.3 Filtros basados en resúmenes o valores *hash*

Filtros que establecen un valor *hash* del mensaje que se les somete e indican si ya ha sido identificado anteriormente como correo basura. Se produce un gran número de falsos negativos ya que varios tipos de correo basura no están identificados aun en el caso de que los servidores los analicen con filtros de valores *hash*. Por otra parte, en ocasiones el mensaje varía lo suficiente como para generar un valor *hash* diferente. Una solución al problema consiste en retardar el mensaje (tal como se hace en las "listas grises" *greylisting*). Generan pocos falsos positivos.

7.9.4 Filtros bayesianos

El filtro de tipo bayesiano se basa en el examen de una lista integrada por un conjunto de correos reconocidos como basura y un conjunto de correos reconocidos como legítimos, en el posterior aprendizaje del vocabulario utilizado por los generadores de correo basura de la lista conocida, y en la aplicación del cálculo de probabilidades bayesiano para determinar si un mensaje es un correo basura. En el caso de un filtro de grupo, el administrador del sistema suele ser el encargado de dirigir el aprendizaje.

Al basarse en el concepto de vocabulario de correos basura, estos filtros pueden plantear dificultades cuando son compartidos. Estas dificultades pueden resultar aceptables en entornos reducidos y muy uniformes (por ejemplo, en una empresa o en un departamento de una universidad, en el que todo el mundo trabaja en el mismo dominio y emplea un vocabulario similar). Sin embargo, estas dificultades resultarían inaceptables en el caso de los principales proveedores de servicio de correo electrónico y, especialmente, en el de los proveedores públicos, salvo si se ofrece

a cada cliente la posibilidad de configurar el filtro de su propia casilla de correo. El problema radica en que existe la posibilidad de que el vocabulario considerado aceptable por ciertos usuarios haya sido catalogado como vocabulario propio de correo basura por el grupo y, por consiguiente, active el filtro.

A pesar de los problemas que puede plantear su utilización por un grupo, estos filtros resultan muy eficaces cuando son utilizados por usuarios individuales, y constituyen una de las pocas soluciones que, utilizada como único recurso, puede filtrar la mayoría de los correos basura tras el correspondiente aprendizaje.

7.9.5 Filtros basados en el comportamiento

Este tipo de filtro examina el comportamiento del servidor distante, por ejemplo la cantidad de mensajes enviados por unidad de tiempo. La limitación de volumen (*rate limiting*) es un ejemplo de filtro de este tipo. La idea es que los mensajes electrónicos normales sólo se envían de uno en uno o en pequeñas cantidades, mientras que el correo basura suele enviarse en grandes cantidades.

Se trata de un tipo de filtro muy frágil, pues a menudo no hay manera de distinguir un generador de correo basura de una lista de distribución de correo legítimo, por ejemplo, un grupo de noticias (*newsgroup*).

Según ciertos expertos, resulta en cualquier caso legítimo que una plataforma rechace ciertas remesas de correo, ya sea por razón del volumen de la misma, o en cumplimiento de la misión que le incumbe de preservar la seguridad de sus redes. También parecería legítimo pedir a quienes envían grandes cantidades de correo electrónico que respeten los recursos de la plataforma distante y asuman los costes de distribución de sus mensajes sin tratar de enviarlos demasiado rápidamente, para evitar los costos inherentes a la utilización del correo electrónico como canal de comunicación.

7.10 HELO/CSV

Un computador que envía mensajes se identifica ante el que los recibe al inicio de cada transacción SMTP mediante la instrucción "EHLO" o "HELO".

La validación de servidor certificado (CSV, *certified server validation*) es un servicio que proporciona un mecanismo que permite a un servidor de correo electrónico evaluar a otro servidor que le envía correo. Se basa en la práctica corriente de los proveedores de servicio que autorizan las redes a partir de las cuales se conectan los sistemas remitentes.

Aunque la prueba HELO sirve para comprobar que el MTA distante está debidamente configurado, no indica si se trata o no de un generador de correo basura. Las pruebas CSV añaden al nombre una prueba de probabilidad: ¿corresponde realmente a un dominio? A diferencia de SPF o DKIM, la CSV no autentifica el dominio que envía el mensaje, sino el dominio del servidor de correo electrónico (que puede ser distinto, por ejemplo en el caso de un proveedor que presta servicio a un gran número de clientes).

Las directivas de configuración – por ejemplo, la directiva Postfix reject_invalid_hostname – verifican el nombre anunciado por el servidor. La utilización de pruebas HELO convencionales tiene como resultado el rechazo de gran cantidad de mensajes legítimos. Sin embargo, son pocos los sitios que saben en la actualidad cómo modificar HELO para que funcione adecuadamente. Es probable que esto cambie en el futuro, dado que serán cada vez más numerosos los sitios que aplicarán la prueba HELO, lo cual supondrá un incentivo para introducir mejoras.

7.11 Listas grises (*greylisting*)

Se trata del envío deliberado de un código de error SMTP 4xx (un error temporal, contrario al 5xx que es uno definitivo, véase el [b-IETF RFC 2821]) cada vez que se encuentra un nuevo remitente, el cual, si se trata de un MTA normal, enviará de nuevo el mensaje más tarde (normalmente unos 15 minutos después) y, sólo entonces, éste será aceptado. La mayoría de los programas que generan

correo basura no hacen varios intentos. Se trata de una técnica muy eficaz que bloquea todos los mensajes de correo basura que no son enviados a través de un repetidor abierto o por el MTA de un proveedor. Permite evitar la recepción de mensajes procedentes de servidores mal configurados, y se presta especialmente bien a su utilización combinada con una lista blanca.

7.12 Testigos/contraseñas

Estas técnicas tienen como finalidad incluir una contraseña en la dirección a la que se envía el correo electrónico o bien emplear un sistema de pregunta/respuesta, tal como la prueba de Turing. El programa informático que genera el correo basura no conocerá esta contraseña y no pasará la prueba.

Con estas técnicas no se producen falsos negativos, salvo que los generadores de correo basura decidan emplear a miles de personas con salarios muy bajos para que hagan el trabajo.

Algunos usuarios válidos no aceptarán o no podrán someterse a la prueba. En estos casos pues, se producirán muchos falsos positivos. Estas técnicas sólo son interesantes para destinatarios muy populares que ya reciben grandes cantidades de correo masivo, incluido el correo legítimo, o para cualquier destinatario que desee reducir la cantidad de mensajes que recibe, lo cual corresponde al ámbito de la libertad de comunicación. Cabe señalar que no todos los remitentes están dispuestos a aceptar la prueba que se les impone. Para disminuir los casos de no aceptación, es necesario formar a los usuarios para que entiendan la utilidad de esta tecnología y la importancia de pasar la prueba.

7.13 Técnicas diversas

Esta cláusula abarca diversas técnicas, en su mayoría experimentales o que no han sido probadas suficientemente.

7.13.1 Pruebas de envoltorio (validación de rótulo de dirección de rebote (BATV, *bounce address tag validation*) y remitente de envoltorio firmado (SES, *signed envelope sender*))

Las pruebas de envoltorio (*envelope tests*) son técnicas muy recientes cuyo uso aún no está muy extendido, por lo que no se tendrán en cuenta en esta Recomendación.

7.13.2 Certificación de envíos de correo masivos – Reputación del remitente

Aunque una autentificación eficaz de remitente facilita la tarea de control de correo basura por parte de los PSI, la autentificación es sólo un paso preliminar en el proceso de eliminación de dicho correo. Una vez que es posible identificar al remitente, se requiere disponer de factores tales como la reputación y la autorización para establecer si determinado mensaje se debe clasificar como basura antes de que llegue al usuario. El proceso de certificación y el establecimiento de criterios sería tarea de autoridades independientes. Un órgano de control, de carácter multisectorial, sería el encargado de supervisar a las autoridades de certificación.

Con este fin, el Grupo ePrivacy creó la norma abierta sobre correo electrónico de confianza (TEOS, *trusted email open standard*). La TEOS tiene su origen en el programa de ePrivacy para la autorregulación del sector, cuya finalidad es separar los correos legítimos de los correos basura. La TEOS no se limita a la autentificación, sino que crea una identidad fiable para los remitentes de correo electrónico, basada en firmas en los encabezamientos de los mensajes. A diferencia de las firmas de autentificación de DKIM, las firmas TEOS son sellos visibles en los mensajes, que certifican que el remitente cumple determinados requisitos.

Para reducir el problema del envío masivo de mensajes de correo electrónico filtrados por error como correo basura, el sector sigue discutiendo acerca de la eficacia de un mecanismo de certificación para los envíos masivos de correo. Por ejemplo, se podrían reconocer los correos voluminosos legítimos a nivel del PSI utilizando una etiqueta que fuera reconocida por el servidor, permitiendo así un recurso más fiable a los filtros de correo electrónico. El proceso de certificación

podría aplicar varios criterios, tales como un compromiso a seguir prácticas estrictas en favor de la privacidad. Francia, por ejemplo, está colaborando con su órgano nacional para la protección de los datos (CNIL) a fin de lograr un sistema de certificación de remitentes que notifique la utilización de registros de clientes.

Cada PSI mantendría una lista blanca de clientes certificados. Esta propuesta requiere que los PSI se pongan de acuerdo respecto del proceso de certificación y no implica ninguna intervención exterior. No obstante, para que el método fuera eficaz, tendría que contar con la participación de una masa crítica de PSI y debería basarse en la confianza entre éstos, al no haber un control externo del proceso de certificación. Además, fijar un número de envíos concreto para definir lo que se considera como un envío de correo masivo, podría resultar problemático. Los remitentes de correo basura más avispados podrían utilizar varias direcciones gratuitas de correo electrónico para enviar grandes cantidades de correo basura, cuidándose de enviar desde cada una de las cuentas un número de mensajes situado justo por debajo del umbral predefinido para el correo basura.

7.13.3 Validación del servidor del remitente

En estudio.

7.13.4 Firmas PGP

En estudio.

7.13.5 Configuración del sistema

Algunos ejemplos de utilización de la configuración del sistema contra el correo basura son las prácticas óptimas de seguridad, en el plano individual y del sector, para puertos, cortafuegos, redes, encaminadores, servidores intermediarios, accesos, contraseñas, protección de claves de permisos e instalación de programas informáticos. Al configurar el sistema para que bloquee el correo no deseado, sólo se capta un porcentaje del correo basura. Ahora bien, dado que aumenta el número de sistemas que cuentan con dichos mecanismos, los remitentes de correo basura tendrán que agudizar el ingenio pero, al mismo tiempo, serán cada vez menos sus alicientes para producir dichos correos, ya que tendrán que superar más obstáculos. En la actualidad, la razón por la cual la gente produce correo basura es porque hacerlo resulta simple, rápido y barato. Si dejara de serlo – y hay cientos de miles de administradores de sistema dedicados a lograrlo – se hará más difícil enviar con éxito correos de ese tipo.

7.13.6 Herramientas antivirus

Las herramientas antivirus son importantes tecnologías que permiten reducir el riesgo de infección de los sistemas informáticos que provoca el correo basura. A menudo, los correo basura malintencionados llevan ficheros que pueden introducir un virus. El programa antivirus permite verificar el contenido de los buzones de correo electrónico y así evitar infecciones por virus.

Algunos PSI se esfuerzan por verificar y actualizar continuamente su interfaz de programa de aplicación (API, *application programming interface*) antivirus, VSAPI, con el servidor de intercambio (*exchange server*). Esta tecnología permite hacer un barrido para buscar los virus en el buzón de correo del usuario, desde fuera de la red, con lo cual se disminuye los efectos de los virus y de los mensajes de correo electrónico contaminados sobre las infraestructuras de red. También es posible impedir que salga correo infectado de una organización efectuando el barrido, además de sobre el correo entrante, sobre el correo saliente.

7.14 Cómo utilizar el presente estudio sobre las tecnologías y factores que se han de tener en cuenta

La utilidad de cualquier herramienta depende de las necesidades, la capacidad técnica y la infraestructura del usuario de la misma. Las herramientas tienen que instalarse en diversas partes del sistema y con distintas finalidades. Al escoger e instalar herramientas contra el correo basura,

los usuarios tendrán que estudiar con sumo cuidado sus necesidades y estrategias de defensa. Las propias herramientas presentan variaciones en términos de madurez, eficacia, fiabilidad e instalación. Algunas son más proclives a los falsos positivos, otras son más eficaces en ciertas áreas y otras entrañan mayores gastos generales en términos de infraestructura o ancho de banda/capacidad y necesidad de conocimientos técnicos. Si bien se enumeran algunos de dichos factores a fin de que sean tenidos en cuenta, es al usuario a quien corresponde juzgar qué herramientas resultan más apropiadas en el contexto específico en que está prevista su aplicación.

Algunas de las pruebas mencionadas se han concebido para la lucha contra el correo basura, mientras que otras tienen como fin evitar ciertos comportamientos que o bien plantean riesgos para la seguridad y no respetan los recursos de la plataforma a la que se envía el correo, o bien simplemente incumplen las reglas aceptadas para el envío de mensajes electrónicos. Cuando se aplica una regla después del punto de recepción de la información que constituye el mensaje que se debe entregar, aún queda por decidir lo que se va a hacer con el citado mensaje. Esto dependerá, por supuesto, de los resultados de las pruebas que se hayan realizado. Algunas pruebas son más fiables que otras y, por consiguiente, justifican el recurso a medidas más drásticas. Asimismo, es posible que se decida efectuar otras pruebas más costosas sobre determinados mensajes.

A continuación se presentan las opciones para tratar un mensaje en función de la ubicación de la regla aplicada.

7.15 Rechazo en la sesión SMTP

El interés de dicho rechazo reside en que no hay que hacerse cargo del mensaje, cuya distribución sigue siendo responsabilidad del servidor distante, al que se informa de la situación. Además permite ahorrar ancho de banda, en primer lugar porque no se recibe el mensaje, y además porque el servidor distante no tiene que enviar las notificaciones de estado de entrega (DSN, *delivery status notification*), mensajes generados como respuesta a un rechazo (véase [b-IETF RFC 3461]) que podría generar el mensaje. Se traslada al servidor remitente la tarea de emitir la notificación de no entrega.

Sin embargo, este tipo de rechazo implica que no es posible conservar una copia del mensaje (y, en consecuencia, recuperar un mensaje legítimo que pudiera haberse rechazado, o simplemente investigar las razones de un rechazo).

Además, en la actualidad no todos los servidores SMTP están en condiciones de efectuar ciertas pruebas durante la sesión SMTP. Ahora bien, esto está cambiando con el uso cada vez más extendido de nuevos productos y, especialmente, de interfaces tales como "*milter*" de sendmail, "*policy server*" de Postfix o los futuros OPES, que serán capaces de conectar cualquier programa a la sesión SMTP.

7.16 Rechazo silencioso

Este método suele desconcertar a los usuarios regulares, que esperan que su correo sea entregado o que, por lo menos, se les informe cuando haya sido rechazado. Aunque la alternativa "entregar o avisar" es uno de los principios básicos del correo electrónico, es probable que deba ser abandonado debido a la cantidad de correos que pretenden haber sido enviados por un usuario, que no tiene que ver con ellos.

Lo ideal sería conservar un registro de los mensajes destruidos de esta manera, de modo que puedan emplearse técnicas como la de rastreo de mensajes (*message tracking*), por ejemplo mediante la utilización de la norma [b-IETF RFC 3885] y obtener así el protocolo de rastreo del mensaje, gracias al cual los usuarios pueden saber qué ha ocurrido con sus mensajes (algo similar al sistema de seguimiento con que cuentan las empresas de entrega de paquetes).

7.17 Rechazo mediante el envío de una DSN (notificación de estado de entrega o "rebote")

Es el método utilizado tradicionalmente en el correo electrónico. Sin embargo, debido a la presencia de los denominados "joejobs", existe el riesgo de penalizar remitentes inocentes, como puede ocurrir con los programas antivirus que envían los DSN por error.

7.18 Entrega a un buzón de correo basura

Cuando se bloquean pocos mensajes a la entrada de la plataforma, el buzón de correo basura puede contener gran cantidad de mensajes, lo cual puede incitar a los usuarios a renunciar a su lectura. El mensaje no se destruye, pero se ofrece al usuario la posibilidad de corregir falsos positivos.

7.19 Marcado de mensajes

El servidor no toma ninguna decisión, y se limita a poner una nota al correo electrónico. Aunque esta técnica proporciona al usuario un control total, el problema es que le obliga a descargar correo basura.

Cabe señalar que los proveedores de servicio de correo electrónico podrían dar al usuario la opción de escoger entre el simple marcado del mensaje o su entrega en el buzón del correo basura. La gestión es relativamente sencilla.

Apéndice I

Actividades de lucha contra el correo basura

(Este apéndice no forma parte integrante de la presente Recomendación)

I.1 Introducción

En este apéndice se describen las actividades recientes de diversas organizaciones, incluido el UIT-T, así como las especificaciones técnicas y las alianzas e iniciativas del sector para la lucha contra el correo basura. Las organizaciones que aquí se enumeran han sido reconocidas por la pertinencia de la labor que han llevado a cabo en la lucha contra el correo basura durante la elaboración de la presente Recomendación. Por lo tanto, el alcance y la validez de las especificaciones técnicas y la situación de las organizaciones mencionadas pueden variar en el futuro.

I.2 Actividades internacionales de lucha contra el correo basura

I.2.1 UIT

En la Declaración de Principios aprobada durante la primera fase de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), celebrada en Ginebra, en diciembre de 2003 [b-CMSI-2003], se consideró al correo basura como una posible amenaza para Internet y los servicios de correo electrónico. En consecuencia, los participantes en la CMSI reconocieron que dicho correo constituía "un problema considerable y creciente para los usuarios, las redes e Internet en general", y que, para generar confianza y garantizar la seguridad en la utilización de las TIC, era necesario adoptar medidas apropiadas en los planos nacional e internacional.

El interés de los Estados Miembros de la UIT por las cuestiones relativas al correo basura se puso de manifiesto durante la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que tuvo lugar en Florianópolis (Brasil), en octubre de 2004. Durante dicha Asamblea, los Miembros de la UIT aprobaron dos Resoluciones relativas a las actividades futuras de la UIT en materia de lucha contra el correo basura.

De una parte, la Resolución 51, "Lucha contra el correo basura", encarga a los Directores de los tres Sectores y al Secretario General que preparen con urgencia un Informe al Consejo sobre las iniciativas de la UIT y otras iniciativas internacionales para combatir el correo basura y que propongan – con la contribución de los Estados Miembros y Miembros de Sector – posibles medidas de seguimiento, para su examen por el Consejo. La Resolución invita además a los Estados Miembros a tomar las medidas adecuadas, dentro de sus marcos jurídicos nacionales, para garantizar que se adoptan disposiciones adecuadas y eficaces de lucha contra el correo basura.

Por otra parte, en la Resolución 52 acerca de los medios técnicos contra el correo basura, se reconoce "que el correo basura crea problemas de seguridad en las redes de telecomunicaciones, incluyendo el de transformar éstas en vehículo para la difusión de virus, gusanos, etc.". También se reconoce la existencia de las Recomendaciones UIT-T en esta materia, que podrían dar orientaciones para la futura evolución de la situación en este ámbito y, por consiguiente, se dan instrucciones a las Comisiones de Estudio competentes para que, en colaboración con el Grupo Especial sobre Ingeniería de Internet (IETF) y otros Grupos pertinentes, elaboren con carácter urgente Recomendaciones técnicas, incluyendo las definiciones necesarias, sobre la lucha contra el correo basura, según corresponda, e informen periódicamente sobre el avance de sus trabajos al Grupo Asesor de Normalización de las Telecomunicaciones. Asimismo, se encarga al Director de la Oficina de Normalización de las Telecomunicaciones que facilite toda la asistencia necesaria para acelerar esas actividades, e informe de ello al Consejo.

I.2.2 OCDE

El correo basura tiene una repercusión negativa sobre la economía digital, y ocasiona importantes costos económicos y sociales, tanto para los países de la OCDE como para los demás. Teniendo en cuenta los problemas potenciales que se puedan presentar en el futuro como resultado de la convergencia de las tecnologías de las comunicaciones y la aparición de las comunicaciones ubicuas y el Internet móvil, los Estados Miembros de la OCDE han de hallar métodos eficaces para luchar contra ese tipo de correo. Para responder a este desafío, el Comité de Política de Información, Informática y Comunicaciones (ICCP), durante su reunión del 3 al 4 de marzo de 2003, expresó su apoyo a la labor sobre esta cuestión, solicitando que se inscribiera en un procedimiento de aprobación rápida, y observó que se trataba de un problema de alcance mundial. El Comité sobre Políticas de Consumo (CCP) también expresó su interés por que se prosiguiera la labor de la OCDE en esta materia. En un documento sobre los antecedentes de la cuestión, así como en un taller sobre el correo basura organizado en Bruselas por la Comisión Europea en febrero de 2004, se llevó a cabo un estudio preliminar de los problemas ligados al correo basura.

El correo basura constituye un problema para varios sectores, pues afecta a la utilización de las redes, los aspectos relacionados con la congestión y otras cuestiones de las redes IP; a la privacidad y la seguridad de las redes; y a la protección del consumidor. A fin de coordinar mejor los trabajos relacionados con el correo basura y de acelerar la obtención un consenso sobre el marco de políticas necesario para hacer frente a todo lo relacionado con dicho correo, en julio de 2004 el Consejo de la OCDE decidió crear un "Grupo de Tareas sobre el correo basura". Se solicitó a dicho Grupo que presentara en julio de 2006 un Informe al CCP y al ICCP.

El objetivo básico del Grupo de Tareas era reunir a los coordinadores en materia de políticas contra el correo basura y propiciar la eficaz formulación de las herramientas políticas más urgentes para la lucha contra este tipo de correo, abordando el problema de una manera más global y aprovechando los conocimientos multidisciplinarios de la OCDE.

Se pidió al Grupo que estudiase, documentase y promoviese toda la gama de estrategias existentes e incipientes contra el correo basura en todos los sectores. Tras reconocer que no existía una panacea para acabar con el correo basura, en abril de 2006 el Grupo de Tareas desarrolló una colección de herramientas de lucha contra el correo basura, que se basaba en la premisa de que era necesario incorporar varios elementos diferentes y coordinados para afrontar este problema, con el fin de contribuir a la concepción y el desarrollo de estrategias y soluciones contra ese tipo de correo en los ámbitos técnico, regulatorio y de cumplimiento de las normas, y de para facilitar la cooperación internacional. Con esta colección de herramientas de la OCDE, lo que se pretende es reunir un conjunto de políticas coherentes y coordinadas y otro tipo de iniciativas (por ejemplo ligadas al cumplimiento de la aplicación de las normas). Su elaboración y aplicación dependían en gran medida de la contribución de las partes interesadas en las áreas correspondientes. El conjunto de herramientas se compone de ocho elementos relacionados entre sí, a saber:

– la normativa contra el correo basura;
– la cooperación internacional en materia de cumplimiento de su aplicación;
– las soluciones de carácter sectorial contra el correo basura;
– las tecnologías existentes e incipientes de lucha contra el correo basura;
– la educación y la toma de consciencia;
– los acuerdos de cooperación contra el correo basura;
– la medición de la incidencia del correo basura;
– la cooperación en el plano mundial (promoción).

El Grupo de Tareas preparó documentos de antecedentes sobre varios de los elementos de la colección de herramientas. En este apéndice se resumen la labor emprendida por el Grupo de Tareas y sus conclusiones. El apéndice se completa con la Recomendación del Consejo de la OCDE acerca

de cooperación internacional en materia de cumplimiento de las normas contra el correo basura, y con el sitio web de la OCDE contra dicho correo (www.oecd-antispam.org).

I.2.3 APEC

En la Cooperación Económica Asia-Pacifico (APEC), los asuntos relacionados con el correo basura se tratan en el Grupo de Trabajo sobre las Telecomunicaciones y la Información (TEL WG), que está dedicado a mejorar la infraestructura de telecomunicaciones e información de la región y a propiciar la cooperación eficaz, el libre comercio y la inversión, y el desarrollo duradero.

En el área de la seguridad de redes e infraestructuras, el TEL colabora con otras organizaciones y contribuye a la creación de un entorno en línea seguro en la sociedad de la información, ocupándose de aspectos tales como el correo basura, la lucha contra las amenazas a las redes, incluidas las medidas para el seguimiento de los Principios de Acción de la APEC contra el correo basura y de las Directrices de la APEC para la aplicación de medidas de lucha contra dicho correo, y la cooperación con organizaciones tales como la UIT, la OCDE y la ASEAN. En el sitio web del TEL WG de la APEC se proporciona más información al respecto (http://www.apectelwg.org/).

I.3 Desarrollo de especificaciones técnicas contra el correo basura

I.3.1 UIT-T

En su Resolución 52, la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT) (Florianópolis, 2004) dio instrucciones a las Comisiones de Estudio correspondientes para que, en colaboración con el Grupo de Tareas Especiales de Ingeniería en Internet (IETF) y otros Grupos pertinentes, elaboraran Recomendaciones técnicas apropiadas sobre la lucha contra el correo basura, con sus correspondientes definiciones, e informaran periódicamente al Grupo Asesor de Normalización de las Telecomunicaciones sobre el avance de sus trabajos.

En su calidad de Comisión encargada de las cuestiones de seguridad de las telecomunicaciones, y con arreglo a las disposiciones de las Resoluciones 50, 51 y 52 de la AMNT, la Comisión de Estudio 17 se encuentra en una posición ideal para examinar la gama de posibles medidas técnicas contra el correo basura, teniendo en cuenta su relación con la fortaleza y la estabilidad de las redes de telecomunicaciones. La Comisión de Estudio 17 del UIT-T creó un Grupo de Relator dedicado a esta Cuestión, el que trata de la Q.17/17, para que proporcionara soluciones técnicas para luchar con el correo basura. La labor inicial se centra en la elaboración de especificaciones técnicas de la lucha contra el correo basura. Más adelante, la labor se extenderá al desarrollo de soluciones técnicas contra ese problema para las aplicaciones multimedios IP, tales como la telefonía IP, la mensajería instantánea, etc. Las especificaciones técnicas abarcan, o tienen previsto abarcar, las directrices, los requisitos, el marco y los medios técnicos para luchar contra distintas variedades de correo basura.

I.3.2 IETF

El IETF ha publicado varias solicitudes de comentarios (*Requests for Comments* – RFC) sobre la lucha contra el correo basura, que van desde directrices hasta especificaciones técnicas, a saber:

– [b-IETF RFC 2505] "*Anti-Spam Recommendations for SMTP MTAs*" (Recomendaciones para los SMTP MTA en la lucha contra el correo basura):

  En este RFC se presenta una serie de recomendaciones de aplicación, destinadas a dotar a los MTA SMTP de mayor capacidad para reducir la incidencia del correo basura. La finalidad de estas recomendaciones es que, de aplicarse en un número suficiente de MTA SMTP en Internet, se contribuya a resolver la situación provocada por dicho correo, y que sirvan de directrices a los diversos proveedores de MTA. Aunque no se trata de una solución definitiva, si se aplicaran estas recomendaciones en todos los MTA SMPT de Internet las cosas mejorarían ostensiblemente, dejando tiempo para encontrar una solución a más largo plazo. En la sección dedicada a las futuras labores se sugieren algunas ideas que podrían formar parte de dicha solución a largo plazo. Es posible, no obstante, que la

solución definitiva sea de carácter social, político o jurídico, en lugar de técnico propiamente dicho. Conviene que quien utilice estas técnicas tenga presente el mayor riesgo de sufrir ataques de denegación de servicio a que podrían dar lugar varios de los métodos propuestos. Por ejemplo, una mayor cantidad de solicitudes a los servidores DNS y un mayor tamaño de los ficheros de tipo registro (*logfiles*) pueden conducir a una saturación y un colapso de los sistemas durante un ataque.

– [b-IETF RFC 2635] "*DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings*" (Directrices para los envíos masivos de correo y publicaciones):

  En este RFC se explica por qué los envíos masivos de correos electrónicos no solicitados resultan perjudiciales para la comunidad de redes. En él se proporciona un conjunto de directrices para tratar el correo no solicitado, destinadas a los usuarios, los administradores de sistemas, los administradores de sistemas de noticias, y los encargados de las listas de distribución. También se sugieren algunas prácticas que podrían aplicar los proveedores de servicios Internet.

– [b-IETF RFC 3685] "*SIEVE Spamtest and VirusTest Extensions*" (Extensiones spamtest y virustest de SIEVE):

  Las extensiones "spamtest" y "virustest" de SIEVE permiten a los usuarios emplear instrucciones simples y portátiles para las pruebas de detección de correo basura y virus en correos electrónicos. Cada extensión proporciona una nueva prueba que utiliza correspondencias con "puntuaciones" numéricas. Incumbe a la aplicación subyacente SIEVE proceder a las verificaciones reales que dan origen a los valores resultantes de las pruebas.

– [b-IETF RFC 4686] "*Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)*" (Análisis de las amenazas que dan lugar a la tecnología DKIM):

  En este RFC se analizan algunas de las amenazas contra el correo electrónico que en teoría pueden evitarse utilizando la autentificación de correos basada en firmas, en particular la técnica de correo identificado mediante los "DomainKeys". Se estudia la naturaleza y la ubicación de los actores malintencionados, cuáles son sus capacidades y qué pretenden con sus ataques.

Además de los anteriores, hay varios documentos que describen la autentificación en el plano de dominio, que pueden servir en la lucha contra el correo basura.

I.4 Lista de alianzas e iniciativas del sector contra el correo basura

A continuación, se presenta una lista de iniciativas de la industria en todo el mundo. No se trata de una enumeración exhaustiva, y habría de considerarse tan sólo como un intento de ilustrar la gran variedad de proyectos que están emprendiendo diversas organizaciones para combatir el correo basura de una manera más eficaz y coordinada.

I.4.1 Grupo de Trabajo contra el "*Phishing*" (APWG)

Este Grupo (APWG, *anti-phishing working group*) [b-APWG] es la asociación mundial del sector y la encargada de velar por el cumplimiento de la legislación, que se centra en la eliminación del fraude y del robo de identidades derivados de los crecientes problemas causados por el hurto de identidades y credenciales financieras (*phishing*), la usurpación de identidades, por el robo automático de información financiera mediante la "siembra" subrepticia de programas que obtienen dicha información ("*pharming*"), y por el fraude a través del correo electrónico. La organización cuenta con un foro en el que se debaten aspectos relacionados con el *phishing*, se define la magnitud del problema que ocasionan estas prácticas en términos de costos de equipos y programas, y se comparten información y prácticas óptimas para la eliminación del problema. De ser necesario, el APWG también considerará la posibilidad de compartir esta información con las autoridades encargadas de velar por el cumplimiento de la legislación.

I.4.2 Alianza para la autentificación y la confianza en línea (AOTA)

Fundada en octubre de 2004, "E-mail Authentication.org" ha evolucionado hasta convertirse en la Alianza para la autentificación y la confianza en línea (AOTA Inc., *Authentication and Online Trust Alliance*). La AOTA tiene por misión mejorar la confianza y la seguridad en todo tipo de mensajería electrónica, cibercomercio, ciberbanca e Internet, ayudando a que se perfeccionen la seguridad y la protección en línea de las empresas y de los consumidores. Entre sus objetivos figuran la promoción de prácticas óptimas, la circulación de información y la configuración de la autentificación del correo electrónico y de Internet, las normas y soluciones en materia de identidad y de reputación, y las estrategias de defensa de dominios, mediante el suministro de un ecosistema normativo y de asesoramiento práctico en un entorno independiente del fabricante. La AOTA está compuesta por importantes organizaciones empresariales, sectoriales y sin ánimo de lucro, que colaboran para mejorar la confianza y la seguridad en la mensajería electrónica, el cibercomercio e Internet. Ante la avalancha de mensajes de "*phishing*" y fraudulentos, esta colaboración es fundamental para contribuir a garantizar la fiabilidad y el reparto del correo electrónico, reforzar la confianza y la seguridad en línea, y proteger las marcas y los dominios de las empresas en todo el mundo.

A comienzos de 2004, un grupo de dirigentes empresariales, sectoriales y comerciales, entre los que destacaban Bigfoot Interactive, Email Sender and Provider Coalition (ESPC), Microsoft y Sendmail, comenzó a reunirse para buscar soluciones que permitieran autentificar el correo electrónico y mejorar la confianza del usuario. Tras la Cumbre sobre la autentificación, organizada por la Comisión Federal del Comercio de los Estados Unidos y que se celebró en noviembre de 2004, copatrocinada por el Instituto Nacional de Normalización y Tecnología del Departamento de Comercio de dicho país, se decidió emprender acciones eficaces para avanzar en el campo de la autentificación del correo electrónico, lo que condujo a la creación de la www.emailauthentication.org. Ante el torrente de correos electrónicos de *phishing* y engañosos que minan la confianza de los usuarios y las empresas, la mailauthentication.org se convirtió, en septiembre de 2006, en la AOTA.

Si bien su trabajo se concentra en el aspecto técnico de la autentificación del correo electrónico, la misión de la AOTA se amplió para que abarcase los problemas ligados a los huéspedes y las amenazas que afectan a la confianza y la seguridad en línea.

I.4.3 Red de contacto de las autoridades responsables en materia de correo basura (CNSA)

Por iniciativa de la Comisión Europea, se creó un Grupo informal compuesto por las autoridades nacionales responsables de hacer cumplir el Artículo 13 de la Directiva de la UE sobre la privacidad y las comunicaciones electrónicas, 2002/58/EC, denominada "red de contacto de las autoridades responsables en materia de correo basura (CNSA)".

En la CNSA, las autoridades nacionales comparten información acerca de las prácticas en vigor contra el correo basura, incluidas las prácticas idóneas para la recepción y el tratamiento de la información sobre quejas y los servicios de obtención de información, así como para investigar y contrarrestar el correo basura. La Comisión se encarga de los servicios de secretaría de la CNSA, que además cuenta con la colaboración de un coordinador, encargado de facilitar el flujo de información entre los Miembros de la CNSA y de apoyar a la secretaría. Actualmente, actúa como coordinador la oficina del Primer Ministro francés. La CNSA se reúne periódicamente (3-4 veces cada año) en Bruselas, y también celebra reuniones anuales conjuntas con el Plan de Acción de Londres (LAP).

La CNSA ha puesto en marcha un procedimiento de cooperación cuyo fin es propiciar la transmisión de información sobre quejas y otras informaciones entre las autoridades nacionales.

I.4.4 Digital PhishNet (DPN)

La Digital PhishNet (DPN) fue creada el 8 de diciembre de 2004 como una iniciativa de colaboración para velar por el cumplimiento de la legislación, con el fin de reunir a los principales actores del sector en los ámbitos de la tecnología, la banca, los servicios financieros y las subastas en línea, con las autoridades encargadas del cumplimiento de la legislación, con miras a combatir el "*phishing*", una modalidad destructiva y cada vez más frecuente de robo de identidad en línea.

El *phishing* es una amenaza en línea especialmente dañina y engañosa, que consiste en dirigir a los consumidores hacia sitios web falsos, a menudo mediante falsos correos electrónicos o la usurpación de identidades, con el fin de hacerlos introducir información financiera personal, por ejemplo números de tarjetas de crédito y contraseñas. Mientras que otros grupos del sector se han concentrado en la identificación de los sitios web dedicados a estas prácticas fraudulentas y a la difusión de prácticas idóneas e información sobre casos, la DPN es el primer grupo de este tipo dedicado a colaborar con las autoridades judiciales para arrestar y juzgar a los responsables de tales ataques. La DPN establece una línea única de comunicación entre la industria y las autoridades policiales, de modo que pueda recopilarse toda la información importante para la lucha contra el *phishing* y entregarse oportunamente a dichas autoridades.

I.4.5 Coalición entre remitentes y proveedores de correo electrónico (ESPC)

La Coalición entre remitentes y proveedores de correo electrónico (ESPC, *Email Sender and Provider Coalition*) es un grupo cooperativo de líderes del sector que se dedica a buscar soluciones a la proliferación continua del correo basura y a los problemas de reparto del correo que van surgiendo. Los Miembros de la ESPC han reconocido la necesidad de contar con soluciones drásticas para hacer frente al problema del correo basura y garantizar al mismo tiempo el reparto del correo legítimo, y se han mostrado muy activos en la lucha contra el correo basura. La ESPC se enfrenta al problema del correo basura y del reparto mediante una combinación de legislación, campañas de promoción, desarrollo tecnológico y normas industriales.

La ESPC se compone de cuatro subcomisiones, a saber:

– Legislativa – Es la que orienta los esfuerzos de influencia de la ESPC para obtener que se promulgue legislación federal y estatal contra el correo basura.

– Relaciones con el receptor – Se formó a fin de permitir una mejor comprensión y un diálogo permanente entre la comunidad de remitentes y la comunidad de destinatarios.

– Tecnología – Es la que evalúa y desarrolla soluciones tecnológicas destinadas a permitir una respuesta más apropiada al problema del correo basura (y a reducir el número de falsos positivos). Se ha creado un grupo técnico de trabajo dentro de esta subcomisión, cuyo objetivo es examinar y proponer soluciones de este tipo. Este grupo se reúne cada vez que es necesario, incluidas algunas reuniones personales ocasionales.

– Comunicaciones – Proporciona a la coalición una estrategia en asuntos relacionados con el público en general.

I.4.6 Instituto de políticas públicas en materia de correo basura e Internet (ISIPP)

El Instituto de políticas públicas en materia de correo basura e Internet (ISIPP, *Institute for Spam and Internet Public Policy*) se dedica a proporcionar análisis, información y consultoría sobre aspectos relacionados con el sector que tienen que ver con las políticas públicas y los procesos en relación con el correo basura, el correo electrónico, la entrega de correo electrónico e Internet. El ISIPP también ofrece un servicio muy conocido de autorización de remitentes de correo electrónico, SuretyMail, y organiza y patrocina foros del sector, tales como mesas redondas sobre la gestión del correo electrónico, cumbres sobre el tema de la entrega de correos electrónicos y conferencias sobre la legislación de Internet.

I.4.7 Plan de Acción de Londres (LAP)

El Plan de Acción de Londres (LAP, *London Action Plan*) es una red mundial integrada por organismos encargados de velar por el cumplimiento de la ley y por representantes del sector activos en la lucha contra el correo basura, el *phishing* y otras amenazas en línea. La Comisión Federal de Comercio de los Estados Unidos y la Oficina de Comercio Justo del Reino Unido protagonizaron la creación del LAP en 2004. El Plan cuenta actualmente con miembros de más de 20 países. Desde su inicio, ha fomentado las relaciones bilaterales y multilaterales entre los organismos encargados de velar por el cumplimiento de la ley, permitiendo así una mejor cooperación internacional en varios casos de investigaciones contra el correo basura. En 2005, el Plan colaboró con otras entidades gubernamentales en la iniciativa "Operation Spam Zombie", por la cual organismos de todo el mundo enviaron cartas a los PSI instándolos a aplicar medidas preventivas para evitar que los computadores de sus abonados se viesen "secuestrados" y utilizados para enviar correo basura.

Como se dijo anteriormente, el LAP celebra reuniones anuales con la CNSA, la tercera de las cuales tuvo lugar del 9 al 11 de octubre de 2007 en Washington, D.C. El seminario LAP-CNSA se celebró en paralelo con la undécima reunión general del MAAWG. El LAP y la CNSA celebraron varias reuniones conjuntas con el MAAWG, en las que se trataron temas de interés común.

Durante la reunión de 2007, el LAP también celebró sesiones de formación destinadas al personal de los organismos encargados de velar por el cumplimiento de la ley, analizó las ventajas de las iniciativas de cooperación entre los sectores público y privado, y estudió métodos para incentivar la cooperación transfronteriza en materia de cumplimiento de la ley. A la reunión conjunta asistieron representantes de organismos encargados de velar por el cumplimiento de la ley y del sector privado de más de 20 países.

I.4.8 Grupo de Trabajo contra los abusos en la mensajería (MAAWG)

El Grupo de Trabajo contra los abusos en la mensajería (MAAWG, *Messaging Anti-Abuse Working Group*) es una organización mundial dedicada a proteger la mensajería electrónica contra los abusos en línea, a fin de mejorar la confianza y seguridad del usuario, mientras se garantiza la entrega de los mensajes legítimos. Gracias a su amplia base, integrada por PSI y operadores de red cuyos abonados representan más de 600 millones de buzones de correo electrónico, por los principales productores de tecnología y por los remitentes, el MAAWG lucha contra dichos abusos concentrándose en la tecnología, la colaboración dentro del sector y las iniciativas de carácter público y privado.

Su objetivo es reunir al sector de la mensajería para que colabore y combata con éxito diversas formas de abusos en dicho campo, tales como el correo basura, los ataques con virus, los ataques de denegación de servicio y otros. Con este fin, el MAAWG está emprendiendo iniciativas en las tres áreas necesarias para resolver el problema del abuso, a saber la colaboración, la tecnología y la política pública.

I.4.9 Spamhaus

El Proyecto Spamhaus es una organización internacional sin ánimo de lucro cuya misión es seguir las huellas de las bandas que envían correo basura a través de Internet, con el fin de suministrar a las redes IP una protección en tiempo real contra dicho correo, colaborar con los organismos encargados de velar por el cumplimiento de la ley para la identificación y prosecución de quienes generan correo basura en todo el mundo, y ejercer su influencia ante los gobiernos para que se promulgue una legislación eficaz para acabar con este problema. El Spamhaus, fundado en 1998, tiene sus sedes en Ginebra (Suiza) y Londres (Reino Unido), y cuenta con una plantilla de 25 investigadores ubicados en nueve países.

El Spamhaus publica el Register Of Known Spam Operations (ROKSO), una base de datos que contiene información y pruebas sobre las "200" peores bandas de todo el mundo conocidas por enviar correo basura, gracias a la cual los PSI pueden evitar inscribir a "spammers" conocidos que podrían abusar de sus redes, y que permite a los organismos encargados de velar por el cumplimiento de la ley identificar y perseguir a los spammers profesionales.

El Spamhaus cuenta con varias bases de datos que sirven para el bloqueo de correo basura en tiempo real, entre las cuales figuran la Spamhaus Block List (SBL), la Exploits Block List (XBL) y la Policy Block List (PBL). Las listas de bloqueo de Spamhaus se difunden a través de una red de 40 servidores DNS en 17 países, y son utilizadas por las principales redes de PSI, empresariales, universitarias, gubernamentales y militares.

Su funcionamiento se financia a través de las donaciones y los patrocinadores. Para la infraestructura internacional, se obtienen fondos mediante la prestación del servicio de sincronización de la lista de bloqueo de correo basura ('Spamhaus Data Feed') que suministra una organización independiente desde el punto de vista logístico a las principales redes IP y a las empresas que producen filtros contra dicho correo.

I.4.10 Alianza para acabar con el correo basura (*Stop Spam Alliance*)

La Stop Spam Alliance es una iniciativa conjunta de la APEC, la CNSA de la UE, la UIT, el LAP, la OCDE y el Grupo Anti-Spam Seúl-Melbourne, cuyo fin es recopilar información y recursos en materia de lucha contra el correo basura.

Con arreglo al Programa de Acciones de Túnez para la Sociedad de la Información [b-CMSI-2005] – en el que se solicita a los miembros "hacer frente eficazmente al problema cada vez más importante que plantea el correo basura" y se exhorta "a todas las partes interesadas a que adopten un enfoque multidimensional para contrarrestar el correo basura" – las páginas de la Stop Spam Alliance proporcionan enlaces a todas las iniciativas en el campo de la lucha contra dicho correo y a las actividades en materia de cumplimiento de la ley, información al consumidor y a las empresas, prácticas óptimas y cooperación internacional.

Se dispone también de un "programa común de actos", en el que figuran los actos internacionales dedicados al correo basura y temas conexos, y que son organizados por las entidades correspondientes. Véase la dirección http://stopspamalliance.org/.

I.4.11 Foro para las comunicaciones electrónicas fiables (TECF)

El Foro para las comunicaciones electrónicas fiables (TECF, *Trusted Electronic Communications Forum*) es un consorcio intersectorial e internacional dedicado a la normalización de las tecnologías, técnicas y prácticas idóneas en materia de lucha contra el *phishing*, la usurpación (spoofing) y el robo de identidades. El TECF se dedica a concebir, instalar y aprobar soluciones eficaces a los problemas que le plantean los estudios de investigación, los analistas y sus miembros. Se patrocinan grupos de trabajo y comités a fin de que formulen o certifiquen técnicas y herramientas específicas para hacer frente a las amenazas de alto riesgo descritas por el TECF.

Bibliografía

[b-WSIS-2003] Primera fase de la CMSI (2003), *Declaración de Principios*. <http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160>

[b-WSIS-2005] Segunda fase de la CMSI (2005), *Agenda de Túnez para la Sociedad de la Información*. <http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2266|2267>

[b-APWG] Grupo de Trabajo contra el "*phishing*", <http://www.antiphishing.org/>.

[b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs*. <http://www.ietf.org/rfc/rfc2505.txt>

[b-IETF RFC 2635] IETF RFC 2635 (1999), *DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*).* <http://www.ietf.org/rfc/rfc2635.txt>

[b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol*. <http://www.ietf.org/rfc/rfc2821.txt>

[b-IETF RFC 2822] IETF RFC 2822 (2001), *Internet Message Format*. <http://www.ietf.org/rfc/rfc2822.txt>

[b-IETF RFC 3461] IETF RFC 3461 (2003), *Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)*. <http://www.ietf.org/rfc/rfc3461.txt>

[b-IETF RFC 3685] IETF RFC 3685 (2004), *SIEVE Email Filtering: Spamtest and VirusTest Extensions*. <http://www.ietf.org/rfc/rfc3685.txt>

[b-IETF RFC 3885] IETF RFC 3885 (2004), *SMTP Service Extension for Message Tracking*. <http://www.ietf.org/rfc/rfc3885.txt>

[b-IETF RFC 4686] IETF RFC 4686 (2006), Analysis of Threats Motivating DomainKeys Identified Mail (DKIM). <http://www.ietf.org/rfc/rfc4686.txt>

[b-FTC] Comisión Federal del Comercio de los Estados Unidos, *Email Address Harvesting and the Effectiveness of Anti-Spam Filters*, noviembre de 2005. <http://www.ftc.gov/opa/2005/11/spamharvest.pdf>

[b-Lyris] Lyris Technologies, Inc., *Email Advisor: ISP Email Deliverability Report Card*, 2nd quarter, 2007. <http://www.lyris.com/resources/reports/deliverability_report_Q22007.pdf>

[b-OECD TF] OECD Grupo de Tareas sobre el correo basura (2006), *Report of the OECD Task Force on Spam: Anti-Spam Toolkit of Recommended Policies and Measures*. <http://www.oecd.org/dataoecd/63/28/36494147.pdf>

-

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
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	Construcción, instalación y protección de los cables y otros 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	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
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 y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2009