03.Maq. INFORME 3/5/06 17:00 Página 1

Estado y perspectivas del servicio de correo electrónico en RedIRIS

INFORME

Present situation and perspectives in RedIRIS Electronic Mail Service

Resumen

El impacto social que provocan los actuales problemas en el correo electrónico requiere mantener el servicio bajo continua vigilancia para su correcto funcionamiento en la comunidad RedIRIS. Las nuevas tendencias de seguridad en el correo implican no sólo ir ajustando los controles en los servidores locales, sino coordinar recomendaciones y proponer iniciativas y proyectos a nivel nacional e internacional. En este sentido desde RedIRIS, IRIS-MAIL intenta coordinar estas actividades respetando las políticas internas de cada institución. En este informe presentamos un análisis, una propuesta de recomendaciones y una iniciativa.

Palabras clave: Servicio de correo electrónico de RedIRIS,IRIS-MAIL, tráfico SMTP, cifrado

Summary

The social impact caused by problems related with electronic mail make it necessary to be alert with the service in order to have it working correctly in the academic community. New security tendencies moves you toward the control of local servers at the same time as towards coordination and presentation of national and international proposals. In the Spanish Academic Community RedIRIS, via IRIS-MAIL tries to coordinate these activities being respectful with the internal policy of each institution as shown in the now presented proposal and recomendations.

Keywords: Electronic Mail Service, RedIRIS, IRIS-MAIL, SMTP traffic, encriptation.

En RedIRIS, a través de IRIS-MAIL, se viene analizando el estado del correo a nivel nacional e internacional y colaborando con universidades e instituciones con el fin de conseguir un nivel óptimo en la calidad y seguridad del servicio

1.- Introducción

El correo electrónico se trata de un servicio crítico para el intercambio de información en la Comunidad RedIRIS. Como servicio de amplia difusión y estable que entra en contacto con el usuario final, viene sufriendo una creciente inseguridad que suele tener un alto impacto social y un menos conocido impacto en los recursos (tanto informáticos como humanos) necesarios para su operación. En RedIRIS, a través de IRIS-MAIL, se viene analizando el estado del correo a nivel nacional e internacional y colaborando con universidades e instituciones con el fin de conseguir un nivel óptimo en la calidad y seguridad del servicio. A lo largo del tiempo se han ido proponiendo, consensuando y desarrollando iniciativas y proyectos ajustados a la realidad tecnológica del momento.

En este informe presentamos un estudio general sobre el estado del spam en 2005 y las perspectivas para 2006. Como propuestas exponemos un resumen de "Política común de tráfico SMTP para la comunidad RedIRIS" basada en estándares que nos permitirá crear un frente común para enfrentarnos al problema del spam y al mismo tiempo servir de guía a otros proveedores. Esta propuesta de política podría ampliarse a redes académicas latinoamericanas a través de Proyecto HERMES (http://hermes.reuna.cl). Por último, como iniciativa a debatir presentamos un posible modelo de cifrado y autenticado de tráfico entre servidores de correo de la Comunidad RedIRIS.

2.- Estado del spam en 2005 y perspectivas

No sólo no ha sido eliminado el spam según las predicciones de Bill Gates, sino que se ha consolidado el crecimiento del phising –spam económicamente fraudulento–.

En enero de 2004, Bill Gates afirmó en el Foro Económico Mundial, que el spam sería eliminado en dos años, es decir en 2006, predicción que claramente no se ha cumplido. Por el contrario podríamos apuntar este año como el de la consolidación y crecimiento del spam económicamente fraudulento, el llamado *phishing* que ha afectado a varias entidades financieras españolas distribuyéndose millones

03.Maq. INFORME 3/5/06 17:00 Página 2

de mensajes. La posibilidad de llevar a cabo fraudes con suculentos beneficios económicos ha despertado el interés de spammers y hackers para participar en un negocio controlado por las cibermafias internacionales. La distribución de virus para controlar PCs, el alquiler de granjas de PC zombies para distribuir spam, troyanos o phishing está siendo un verdadero mercado "negro" y suculento negocio que está provocando un crecimiento desmesurado del spam y por supuesto un aumento de la inseguridad en la Red.

También debemos destacar en 2005 la irrupción en el mercado del sistema de GMAIL, el servicio de correo electrónico de Google que ha roto moldes en la forma de ofrecer un servicio de correo abierto y respetuoso con los estándares. Además el número de clientes que lo usan en este primer año ha sido lo suficientemente elevado como para tener un hueco en el mercado de los grandes (AOL, hotmail, yahoo, etc.) y ser tenido en cuenta en la toma de decisiones estratégicas acerca de nuevos estándares en el correo electrónico como veremos a continuación.

Pero lo más destacado de 2005 han sido los movimientos en el IETF para definir las líneas estratégicas de los estándares de autenticación del emisor en el correo electrónico. Por poner en antecedentes, durante los últimos dos años han surgido decenas de propuestas imaginativas que perseguían resolver el gran problema del correo electrónico "autenticar al emisor de correo electrónico y evitar la suplantación de identidad" sin estropear otras ventajas o servicios tales como las listas de distribución o los reenvíos. De estas decenas de interesantes propuestas presentadas al IETF, dos han sido las que han sido mejor valoradas y aceptadas como RFCs experimentales: SPF/Sender-Id (Sender Policy Framework) avalada por Microsoft, y DKIM (Domain Keys Identified Internet Mail) por Cisco y Yahoo.

El aumento exponencial de tráfico basura está motivado exclusivamente por malware instalados en PCs con conexión residencial

El posicionamiento y aceptación de cada una de las propuestas ha sido un juego de alianzas entre empresas tecnológicas del sector, donde cada una de ellas ha intentado que los grandes portales de correo (AOL, Yahoo, Hotmail y Gmail) apoyen sus iniciativas. Ambas son diferentes, aunque con los mismos objetivos: SPF/SenderID define un modelo simple para validar el origen, mientras que DKIM utiliza la criptografía que además sirve para garantizar la integridad de los mensajes. Básicamente DKIM propugna que el servidor de correo firme todos los mensajes salientes. Probablemente ambas acaben como estándares RFC y cada uno implemente una, otra o ambas, e incluso es posible que en un futuro aparezcan otros candidatos, pero todos esperamos el estándar para su implantación y que se solucione parte de los problemas del correo electrónico.

Hay colectivos, como por ejemplo las entidades financieras, donde la implantación de cualquiera de estos mecanismos de validación del dominio emisor reduciría muchos de los problemas del phishing, sin ir más lejos es una de las recomendaciones del Anti-phishing Working Group que en su última reunion en noviembre de 2005 (https://antiphishing.kavi.com/events/2005_11_fallconferencenotes/20051108_BestPracticesWorkingDoc.pdf) recomienda que las entidades financieras utilicen estos u otros sistemas de autenticación. La comunidad académica española, durante 2005 ha apostado por SPF ya que es el estándar más desarrollado hasta ahora.

2.1.- Estadísticas

Hay un aspecto estadísticamente indiscutible, y es que el aumento exponencial de tráfico basura está motivado exclusivamente por malware (troyanos, spyware,...) instalados en PCs con conexión residencial (ADSL, cable). Estos virus incluyen capacidades de motor SMTP que les permite actuar como un servidor de correo autónomo y controlar todo el proceso de envío y distribución de correo sin necesidad de pasar por el operador del usuario. Según las estadísticas de la red de sensores del Centro de Alerta Antivirus, en el último año el 85% de los correos analizados corresponden a virus con estas capacidades, especialmente variantes del Netsky, Sober, Zafir y Bagle. Estos virus comprometen miles de máquinas (zombies) que son gestionadas como una red (botnet) para diferentes actividades maliciosas: phishing, spam comercial, difusión de virus, etc., y las máquinas infectadas pertenecen en su gran mayoría a redes de acceso residencial. Spamhaus.org tiene una lista de 4 millones de máquinas infectadas –unas 60.000-100.000 por semana–. Para propagarse, los virus analizan el disco del ordenador comprometido buscando direcciones de correo en libreta, ficheros, etc., y una vez obtienen direcciones de correo de destino ya pueden llevar a cabo la distribución de miles de mensajes. En el proceso de envío, el virus falsifica la dirección del emisor, una de las tácticas más habituales, y su solución es uno de los frentes más activos en la lucha contra el spam. Una solución alternativa con cada vez más peso es la definición de un marco de autorregulación a nivel nacional acerca del intercambio de correo entre operadores, haciendo hincapié en que los

03.Maq. INFORME 3/5/06 17:00 Página 3

operadores de ADSL controlen el tráfico de estas conexiones residenciales. No debemos olvidar que estas redes de botnets sirven igual para hacer spam que para ataques de tipo DoS contra quien consideren oportuno.

El virus con más amplia difusión por correo ha sido el Sober.AG, que apareció en noviembre de 2005 y cuyo éxito ha radicado en el uso de direcciones del FBI o CIA (@fbi.gov y @cia.gov) como emisores del mensaje. Se acusaba a los receptores de haber visitado páginas ilegales y se solicitaba rellenar el cuestionario adjunto.

Actualmente la batalla contra el spam es la lucha contra la propagación de virus y aumento de zombies que son utilizados para distribuir spam, phishing y virus, todo un círculo vicioso que nunca hubiera existido si el protocolo de correo electrónico (SMTP) hubiera definido mecanismos para evitar la falsificación del emisor de los mensajes. Todos los esfuerzos anti-spam se concentran en identificar al emisor y, mientras no exista el estándar que garantice dicha identidad, se están utilizando filtros de contenidos y políticas de conexión unilaterales que perjudican con un preocupante aumento de falsos positivos. Las direcciones IP dinámicas de los ADSL residenciales son la gran preocupación de las operadoras que por oscuros motivos no pueden o no desean controlar ese tráfico de correo saliente que en un 100% de casos es malware, que está provocando una enorme inseguridad en la red y obligando a los destinatarios a bloquear este tráfico.

Los dos grandes objetivos del spammer son la búsqueda de direcciones de correo y la disponibilidad de servidores de distribución; lo que se está haciendo con las redes de zombies como ya hemos comentado. Pero la búsqueda de direcciones de correo válidas está creando enormes problemas a los servidores de correo. Hasta ahora la forma más simple es la localización de direcciones en las páginas web, aunque sigue siendo una técnica habitual los spammers, que buscan aumentar el volumen de nuevas direcciones.

Los dos grandes objetivos del spammer son la búsqueda de direcciones de correo y la disponibilidad de servidores de distribución

Uno de los incidentes más graves provocados por el spam durante el último año ha sido los ataques de DHA (Directory Harvest Attacks) sobre los servidores de correo. Son ataques con enormes flujos de spam para localizar nuevas direcciones de correo y para ello envían decenas de miles de mensajes sobre determinado dominio destinado a direcciones de usuario alfabéticamente ordenadas. Aprovechándose de la educación de los sistemas de correo y por un proceso de eliminación los mensajes devueltos con un informe como "Usuario desconocido" son interpretados por los hackers, spammers o programadores de virus como inexistentes y el resto se incorporan a la base de datos de direcciones correctas. Esto provoca una sobrecarga adicional en los servidores.

También hay que destacar el aumento de conceptos rudimentarios de seguridad que han adquirido. Se ha insistido tanto a los usuarios para que "no abran ciertos tipos de adjuntos maliciosos que reciben por correo de desconocidos" que los hackers han tenido que redoblar sus esfuerzos para contrarrestar estos consejos con los ficheros de doble extensión. Son adjuntos con extensiones del tipo "filename.txt.exe" para engañar al usuario que piensa que es un fichero txt. También hay ficheros .COM (ejecutables de dos) al final de una palabra y que parecen ser direcciones de Web acabadas en .com.

2.2.- Perspectivas para 2006

Se esperan tanto resultados, planes de trabajo y desarrollos de los nuevos estándares de correo electrónico SPF y DKIM que supongan una luz al final del túnel del spam, como el hecho de que algún organismo nacional o internacional fomente la autorregulación del sector para frenar la inseguridad que suponen los ADLS residenciales.

Por otro lado, se crearán nuevos tipos de spam de carácter más sociológico y enfocados a estafas y timos y los primeros tipos de spam para la Voz IP cuyas posibilidades son enormes con la realización de llamadas automáticas para preguntar por determinados datos y donde no hay control sobre el origen de la llamada; por este motivo se empezará a recomendar: "sólo recoja las llamadas de las personas de su confianza" con la diferencia de que si no se cogen se colapsan los terminales y no se pueden recibir nuevas llamadas.

El spam y los ataques continuarán, pero la experiencia y la gran cantidad de herramientas que existen hará más sencillo su control con los consabidos efectos de aumento de falsos positivos.

03.Maq. INFORME 3/5/06 17:00 Página 4

3.- Propuesta de "Política común de tráfico SMTP en RedIRIS"

Según los datos estadísticos de RedIRIS y la UJI (http://www.infospam.uji.es/?q=node/11), los servidores de correo procesan entre un 60-70% de tráfico no útil o tráfico oscuro y si a esto le añadimos el de virus se incrementaría hasta el 80%, siendo el resto tráfico de correo lícito o normal. Por tráfico oscuro entendemos el ocasionado por conexiones procedentes de IPs comprometidas con algún tipo de malware y con capacidad de motor SMTP propio que se emplean para difundir spam, virus, ataques de diccionario (Directory Harvest Attaks), denegación de Servicio (DoS) o mensajes a destinatarios no existentes. La mayor parte de las soluciones de seguridad en el correo electrónico no tienen en cuenta este tráfico indeseado a través del puerto 25 que se acepta, analiza y rechaza con el consiguiente empleo de recursos.

Hasta ahora, ha sido más sencillo definir spam detectado en función del contenido (cuerpo del mensaje) sin prestar atención al spam rechazado (sobre del mensaje) más allá de las clásicas listas negras vía DNS. Haciendo un análisis detallado, es posible entender que el tráfico SMTP oscuro es muy variado y complejo, y una de las mejores aproximaciones a él es el interpretado por las Greylistings, aunque no es suficiente. El objetivo de estas recomendaciones es intentar definir los límites entre el spam rechazado y el detectado, es decir, el bloqueo frente al filtrado.

El actual problema de seguridad en el correo electrónico es lo suficientemente grave como para tomar medidas contundentes, comunes y consensuadas por parte de una comunidad homogénea, como es la comunidad académica española. El problema ya no es una simple molestia a los usuarios, sino que supone una grave y continua usurpación de recursos.

El actual problema de seguridad en el correo es lo suficientemente grave como para tomar medidas contundentes, comunes y consensuadas por parte de una comunidad homogénea

A continuación proponemos un conjunto de recomendaciones con objeto de consensuar la gestión del tráfico SMTP entrante y que constituiría la política de este tráfico en la comunidad académica. Se trataría en definitiva de:

- Unir a la comunidad RedIRIS frente al spam.
- Servir de base para la construcción de un correo electrónico más seguro.
- Reducir los recursos necesarios para mitigar el spam.
- Estar preparados para los nuevos protocolos emergentes (SPF,DKIM,Sender-ID, etc.).
- Contribuir con el ejemplo a mejorar el correo global.

Las recomendaciones de esta política están basadas en el respeto a los actuales estándares y a las recomendaciones internacionales de buenas prácticas para operadores de red, y son independientes de productos y configuraciones de software y hardware. Esperamos que la aceptación y despliegue de esta política tenga un impacto directo en la reducción de los recursos de los servidores, en los buzones de los usuarios y en la propia satisfacción del servicio. Esta política está enfocada a pautas y recomendaciones que deberán seguir los servicios de correo electrónico de las instituciones de la comunidad RedIRIS y serán complementarias a cualquier configuración de seguridad de la institución. Cualquier duda para su implantación puede ser planteada a RedIRIS o canalizarse a través del Grupo de Coordinación IRIS-MAIL.

Para unificar esta política se especifican códigos de respuesta del protocolo SMTP recogidos en: RFC2821 y RFC1123 y para los códigos de los motivos el RFC1893 y RFC2034, pudiendo opcionalmente añadir una url a esta política general.

3.1.- Recomendaciones

Una transacción SMTP, según el estándar RFC821, se compone de varios elementos: Conexión (CONNECT), Presentación (HELO), Emisor (MAIL FROM), Receptor (RCP TO:) y Contenidos (DATA). Los datos de los Contenidos son los incorporados en el DATA y los utilizados en las técnicas del filtrado. El resto de las etapas se incluye en el Sobre y son las utilizadas en el bloqueo del spam. Los controles SMTP del Sobre de la transacción SMTP tienen como objeto verificar la validez de la dirección del servidor de correo remoto que solicita establecer dicha transacción para tomar las correspondientes acciones (bloqueo). A continuación se muestran las recomendaciones propuestas para esta política SMTP en RedIRIS, clasificadas en los diferentes niveles del protocolo anteriormente descritos que se corresponden exclusivamente con el tráfico entrante en los servidores de correo:

03.Maq. INFORME 3/5/06 17:00 Página 5

Conexión (CONNECT)

1.- Bloquear el establecimiento de conexión SMTP desde IPs y dominios incluidos en:

- Listas de bloqueo internacional como Spamhaus.
- Listas de IPs asociadas a conexiones residenciales de tipo ADSL/cable dinámica que no son servidores de correo autorizado por sus operadores.
- Listas de bloqueo locales.

Motivo: bloquear conexiones SMTP procedentes de IPs etiquetadas como no deseables a nivel internacional o local, asi como IPs dinámicas residenciales que utilizan inconscientemente el protocolo SMTP.

2.- Bloquear el establecimiento de conexión SMTP desde IPs que no dispongan de resolución inversa.

Motivo: la resolución inversa de una IP forma parte de los RFCs y es síntoma de una configuración incorrecta del servicio. Es una característica muy utilizada para la difusión de malware.

Presentación (HELO)

1.- Bloquear el establecimiento de conexión SMTP cuyo valor HELO/EHLO sea nulo o sin canonificar, tal como se especifica en el apartado 4.1.1.1 de RFC2821.

Motivo: los estándares SMTP (RFC-2821) indican claramente la obligación de colocar un valor correcto al campo HELO/EHLO.

Emisor (MAIL FROM)

1.- Bloquear las transacciones SMTP cuyo valor MAIL FROM: sea un dominio no existente.

Motivo: en un mensaje entrante si no existe un dominio emisor correcto no es posible responder.

2.- Bloquear las transacciones SMTP cuyo valor MAIL FROM: sea un dominio local.

Motivo: una transacción SMTP desde el exterior no puede proceder de una dirección local.

3.- Chequear la responsabilidad del servidor remoto con SPF, DKIM, SenderID para comprobar que el correo procede del servidor oficial responsable del dominio.

Motivo: RedIRIS debe apostar por el despliegue de estas tecnologías.

Receptor (RCPT TO)

1.- Bloquear la conexión si el dominio destinatario no es de nuestra responsabilidad.

Motivo: Una transacción SMTP externa no debe ser aceptada si va destinada a un dominio que no es de nuestra responsabilidad.

2.- Bloquear la conexión si la dirección destinataria no está permitida.

Motivo: Las bases de datos de los usuarios no suelen estar en el relay principal, pero es muy recomendable que sea capaz de chequear en tiempo SMTP la existencia de la parte usuario para interrumpir la conexión.

Otros (flujos)

1.- Sistema de control de flujos SMTP que permita controlar un número inusualmente elevado de conexiones SMTP comparando IP, From, To.

Motivo: La implementación del filtro SMTP de salida podría tener un efecto contraproducente en la propia red local si no se dispone de mecanismos de control de flujos para identificar esas posibles IPs comprometidas.

Contenidos (DATA)

1.- Analizar el contenido en busca del spam y malware. Este control se aplica después de haber sido analizada la transacción SMTP y depende de la política de contenidos de cada institución.

La resolución inversa de una IP forma parte de los RFCs y es síntoma de una configuración incorrecta del servicio

03.Maq. INFORME 8/5/06 15:55 Página 6

Motivo: Es recomendable que si un mensaje ha pasado los filtros anteriores sea analizado para identificar si se trata de correo no deseado. En cuyo caso deberá etiquetarlo o almacenarlo en cuarentena. Es muy útil la promoción de clientes de correo con filtros bayesianos.

4.- Cifrado de tráfico SMTP entre servidores de correo

En la reunión del grupo de trabajo IRIS-MAIL que tuvo lugar en Málaga (mayo 2005) se debatieron las ventajas y la posibilidad de autenticar y cifrar el tráfico SMTP entre servidores de correo de instituciones afiliadas a RedIRIS, concluyéndose una iniciativa a investigar. A lo largo de este tiempo en colaboración con la Universidad de Burgos se ha estado perfilando la idea para intentar evaluar y desplegar un servicio experimental que describimos a continuación.

SSL es un protocolo desarrollado por Netscape en 1994 y conocido por utilizarse en el protocolo HTTP para transferir información de forma segura en las transacciones web. Está utilizándose en aplicaciones en las que los datos son muy sensibles, como por ejemplo ocurre con la banca electrónica o el mundo de la telemedicina. Con la versión 3.1 de SSL nació TLS aplicable a otros protocolos que no sean HTTP, pudiendo así ampliar su uso a aplicaciones como el correo electrónico (SMTP). El uso de ambas tecnologías se conoce como SSL/TLS.

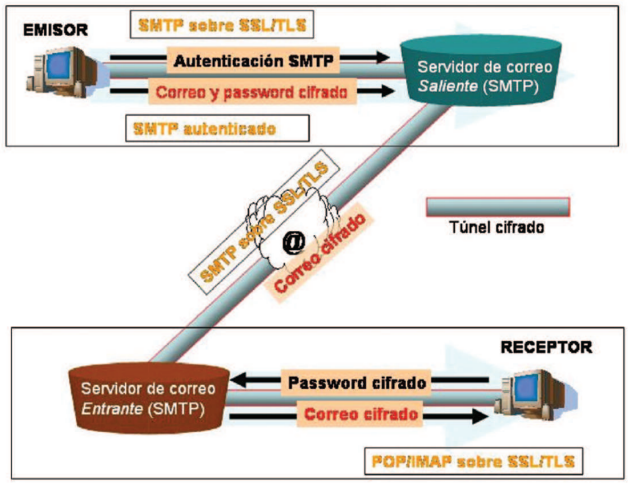
La tecnología TLS nos permite crear un "túnel seguro" para la transmisión de mensajes desde un servidor a otro protegiéndolos en el tránsito por la red. TLS nos ofrece un medio seguro para el intercambio de correo proporcionando: privacidad y confidencialidad (cifrado), verificación del servidor, origen e inalterabilidad del mensaje, ventajas suficientes para evaluar su viabilidad.

El modelo de seguridad basado en PGP lleva más de 10 años siendo utilizado en círculos reducidos y especializados

Este mecanismo de cifrado entre estafetas se complementa con las transferencias seguras entre emisor-estafeta (SMTP) y estafeta-destinatario (POP/IMAP) muy implantado en RedIRIS a través de la iniciativa RACE de RedIRIS. De esta forma todo el trayecto extremo a extremo (emisor-destinatario) quedaría cifrado, securizando el intercambio de correo entre usuarios de la comunidad de RedIRIS tal y como aparece en la figura.

Otra de las ventajas de este mecanismo es la transparencia de cara a los usuarios respecto a modelos individuales tales como PGP o S/MIME. En un modelo basado en un protocolo de transporte como TLS la capacidad de cifrado se deposita en la infraestructura sin intervención de los usuarios, mientras que en el individual se confía en las habilidades de los usuarios; ambos modelos son compatibles.

MODELO TLS DE TRANSACCIONES SEGURAS EXTREMO A EXTREMO



03.Maq. INFORME 8/5/06 15:55 Página 7

El modelo de seguridad basado en PGP lleva más de 10 años siendo utilizado en círculos reducidos y especializados. Estos métodos individuales, si bien son útiles, han venido planteando varios tipos de problemas que han ralentizado su utilización de forma habitual. Uno de ellos es el legal, ya que algunos países niegan a sus ciudadanos el acceso a métodos de cifrado en aras de la lucha contra el crimen. El segundo es de aprendizaje por parte del usuario, ya que estos métodos de cifrado no le son transparentes, requieren conocimientos informáticos e intervención. Un tercer problema que se plantea en una institución o empresa que implante una política de cifrado personal son los inconvenientes que surgen cuando una persona deja de trabajar en la institución (qué se hace con su clave, sus ficheros cifrados, etc). Dado que normalmente el cifrado sólo se utiliza para prevenir que datos sensibles circulen al descubierto por la red, un sistema de encriptación que funcione en el servidor y que sea transparente para los usuarios, como SMTP/TLS, podría ser una opción a evaluar. TLS nos permite crear túneles de cifrado entre servidores cuando la información viaja por las líneas de comunicaciones.

4.1.- Objetivo

El objetivo de esta iniciativa es desplegar una red segura de estafetas de correo electrónico en la comunidad RedIRIS que permita el intercambio de correo cifrado entre ellas. No sería necesaria ninguna inversión adicional de recursos, sino sólo modificaciones de configuración ampliamente conocidas. Si no se ha utilizado hasta ahora este mecanismo ha sido debido a la ausencia de confianza entre los relays (MTAs) de correo, pero RedIRIS es una comunidad donde hay lazos de confianza entre sus miembros y donde sería posible implementar estos modelos

Hay que resaltar que un servidor en esta red intercambiará tráfico de la forma habitual en que lo viene haciendo hasta ahora, pero con los miembros de la red lo hará en modo cifrado. Por ejemplo, el tráfico entre los dominios *ubu.es* y *uvigo.es* sería cifrado de forma automática y transparente si ambos forman parte de esta red y con otros dominios sería normal.

Los servidores que estén preparados con TLS hablarán y negociarán un intercambio seguro sin necesidad de intervención

Un modelo de estas características podría tener como objetivo de valor añadido mostrar al resto de los operadores las posibilidades de estas tecnologías, pudiendo estar interesados en unirse a esta red segura de intercambio de correo.

Los requisitos para el despliegue de una red segura serían:

1.- Protocolo. Configurar los servidores para que dialoguen el protocolo SMTP/TLS.
2.- Confianza. Las estafetas de esta red sólo dialogarán de forma segura con otros servidores que dispongan de un certificado raíz de confianza.
3.- Certificados. Crear una infraestructura (política, renovación, etc.) de certificados de clave pública para servidores de correo.

Los servidores que estén preparados con TLS hablarán y negociarán un intercambio seguro sin necesidad de intervención. El servidor que reciba la petición comprobará la raíz del certificado con las que él tiene y, si es correcto y confía en ella, se establecerá el canal cifrado para la transacción SMTP entre ambos servidores.

Las ventajas que nos ofrecería esta red de confianza serían:

- Confidencialidad para transmitir información sensible: resultados de investigaciones, calificaciones, datos personales, contraseñas, etc.
- Verificación del MTA origen. Al reconocerlo como seguro se pueden evitar: virus, spam, tráfico de servidores mal configurados, etc.
- Transparencia de cara al usuario, ya que no deben configurar nada en sus clientes de correo y se completaría la idea que tienen los usuarios del servicio cuando acceden a su buzón por medios seguros (RACE). El uso combinado de esta red y los criterios RACE redundarían en una seguridad extremo a extremo.
- Inalterabilidad de los mensajes en el tránsito.

03.Maq. INFORME 8/5/06 15:55 Página 8

- Ahorro de recursos, puesto que los mensajes provenientes de la red de confianza no deben pasar por costosos filtros antivirus/antispam que ralentizan su entrega.

Además, y no menos importante, es que la comunidad científica sería pionera y definiría un nuevo entorno en la seguridad y fiabilidad del correo electrónico en Internet que permitiría que otros proveedores o empresas se unieran a la iniciativa para crear un marco seguro de correo electrónico en Internet. Sería ampliable a otras instituciones académicas latinoamericanas (RedClara) a través del proyecto HERMES (Hacia un Entorno de Red de Mensajería Electrónica Segura).

Es necesario remarcar que con esta red de confianza y cifrado de tráfico SMTP no se rechazarán transacciones SMTP ni mensajes de correo que no estén en ella. El objetivo es confiar en las transacciones seguras entre instituciones de esta red, además de disfrutar de las ventajas ya mencionadas.

Jesús Sanz de las Heras
(Jesús.heras@rediris.es)
Servicio de correo electrónico