Resumen de la 24 reunión de Grupo de Coordinación IRIS-MAIL (IRIS-MAIL/24)

Dia: 1 de Julio 2006
Duración: 2h
Lugar: Universidad Autonoma de Madrid

Esta convocatoria IRIS-MAIL/24 contó 45 asistentes, se expusieron diferentes iniciativas y debido al escaso tiempo se lanzó una pequeña encuesta orientativa sobre dichos temas, cuyos resultados se incluyen al final de este Documento donde se incluyen comentarios, ideas y opiniones de los miembros de IRIS-MAIL, lo cual es de agradecer.
Los temas concretos de esta reunión fueron:

1. Un tutorial: "Tunning de Spamassassin"
2. Presentación de la "Política RedIRIS para el intercambio de tráfico SMTP"
3. Whitelisting para Comunidad RedIRIS

Un esquema del tutorial de Spamassassin podréis recogerlo en:
http://cvu.rediris.es/bscw/bscw.cgi/d713546/TunningSA.pdf

El documento es provisional ya hay un pequeño compromiso de hacer uno mas amplio y mejor estructurado. Se agradece el trabajo de Marcos Cobelo Juncal (Univ. de la Coruña) en este tutorial magistral y se demostró que sería digno de una sesión mucho más amplia y monográfica sobre el tema. Algunos asistentes mostraron cierto malestar ya que no disponían de Spamassassin y no estaban interesados en el tema. En la Agenda del grupo estaba puesto el tema.

Con respecto al documento para definir una política común de tráfico SMTP, se expusieron los objetivos del documento y se explicaron los diferentes criterios definidos. De la encuesta se concluye que es de **interés** que RedIRIS disponga de una Política de este estilo. En lo que respecta al contenido del documento tuvo buena acogida en la reunión tal como demuestran los resultados de la encuesta: **muy interesante.** El documento se define como ***recomendación*** por lo que habrá algunos aspectos que aunque técnicamente sean correctos y todos estemos de acuerdo, por aspecto internos sean difíciles de implementar en lo Servicios institucionales. El objetivo de esta política son los posibles beneficios derivados de una política común en RedIRIS que permita presionar con buenas prácticas para conseguir un servicio de correo electrónico más seguro.

El objetivo es que el documento se revise y sea aprobado por IRIS-MAIL en la próxima reunión del Grupo de Trabajo. Por lo que cualquier que desee enviar comentarios al respecto serán bien recibidos.

Otra de las iniciativas expuestas en la reunión IRIS-MAIL/24 fue crear una Whitelisting para la comunidad RedIRIS que esperamos ponerla en marcha cuado antes se pueda ya que la utilidad parece demostrada y la encuesta concluye que es de interés.

Analizando el resto de la Encuesta vemos que las dos de las iniciativas mejor valoradas son:

- Puesta en marcha de un Servicio RedIRIS para el intercambio de ficheros pesados
- Interés en unas Jornadas monográficas sobre aspectos de diseño, seguridad, optimización, calidad en el Correo Electrónico

Las cuales serán tenidos en cuenta para evaluar su viabilidad en RedIRIS. El resto de iniciativas son bien valorados y quizás algo menos la necesidad de crear “Red Académica de intercambio cifrado/autenticado de tráfico SMTP”

Jesús Sanz de las Heras
RedIRIS
Coordinador IRIS-MAIL

Anexo 1. Consulta iniciativas RedIRIS

[[En este ANEXO se incluye las encuestas realizadas, los resultados y una trascripción de los comentarios, ideas y opiniones que han incluido algunos compañeros.]

Objetivo: Disponer de información de las instituciones RedIRIS acerca de las diferentes iniciativas de correo electrónico que se plantean desde el Grupo de Coordinación IRIS-MAIL. Los resultados serán orientativos para RedIRIS con el objetivo de priorizar y poner en marcha las diferentes iniciativas propuestas.

Datos
Institución a la que representa:

Consulta

Valore entre 1-5 las siguientes consultas

(1) Ningún interés
(2) Algo interesante
(3) Interesante
(4) Muy interesante
(5) Altamente interesante

1. Necesidad de una "Política común de intercambio de Tráfico SMTP"
2. ¿Estaría de acuerdo con el actual documento de "Política de Tráfico SMTP"? Tal como se describe en:
   http://www.rediris.es/mail/gt/jn06/docus/AUPsmtpRedIRIS.pdf
3. Puesta en marcha de una base de datos de Servidores de confianza a nivel nacional: Whitelisting.
   http://www.rediris.es/mail/gt/jn06/docus/Lexcepcion.pdf
4. Puesta en marcha de una de Red Académica de intercambio cifrado/autenticado de tráfico SMTP
   http://www.rediris.es/mail/gt/jn06/docus/SSMTP.pdf
5. Puesta en marcha de un Servicio RedIRIS para el intercambio de ficheros pesados
   http://www.rediris.es/mail/gt/jn06/docus/SAUIFP.pdf
6. Interés en unas Jornadas monográficas sobre aspectos de diseño, seguridad, optimización, calidad en el Correo Electrónico
7. Evolución y dinámica del GT IRIS-MAIL
8. Otros temas que considere de interés sobre el Servicio de correo electrónico en el entorno de RedIRIS

Resultados

	1	**2**	**3**	**4**	**5**	**6**	**7**
UC3M	5	3	4	4	5	5	4
UCAM	5	4	4	3	5	5	4
UPC	4	4	4	3	5	5	4
UCLM	3	4	3	3	4	3	4
UNED	4	4	3	4	3	5	4
URL	4	3	5	2	5	4	4
UMA	3	4	5	3	4	5	3
UPF	3	4	5	3	3	4	3
UAX	4	4	4	3	5	4	4
UNIOVI	4	4	5	1	5	5	2
UAB	2	3	1	4	4	4	4
INTA	3	4	3	4	5	3	4
CNB	4	4	5	4	4	5	4
UJI	4	5	3	3	3	3	4
UPCO	3	3	4	3	4	5	4
US	5	4	3	3	5	5	3
UPM	4	4	2	3	4	5	4
UCLM	4	4	5	2	5	5	4
BOE	2	3	2	1	5	4	4
ICFO	4	4	5	4	5	3	4
CEDEX	4	4	4	3	3	5	4
INIA	4	3	4	3	5	4	4
UJAEN	5	4	5	3	5	5	5
UCA	4	4	5	4	5	5	4
CARTIF	4	5	3	3	5	5	4
MEDIA	4	4	4	3	4+	4+	4

Comentarios:

- **UJAEN**. (Antonio Rabadán)

Respecto al documento de “Política de Tráfico SMTP”:

En principio no eliminaría nada, siempre que quede como una recomendación. Particularizando a nuestra universidad, veo en estos momentos, algo complicada la aplicación de los puntos 1, 2 y 3. En nuestra normativa de correo se eliminó el uso de listas negras, y se decidió que todo el correo se entregaría al usuario. Ahora sólo utilizamos etiquetado de correo electrónico.

- **UAB**. (Maribel Jiménez)

Respecto al documento de “Política de Tráfico SMTP”:

Me parece bien el documento como recomendación pero supongo que no todos los mta's soportan todas las opciones ni les puede interesar aplicarlas todas.

- **INTA**.(Mariano Herrera García)

Respecto al documento de “Política de Tráfico SMTP”:

i. PUNTO 1: DE TODOS ES SABIDO QUE EL SPAM CADA VEZ ES MÁS ESPECÍFICO Y ELIGE MEJOR A SUS VICTIMAS, CREO QUE SERÍA INTERESANTE GENERAR UNA LISTA DE BLOQUEO PROPIA Y ESPECIFICA ADEMAS, CLARO ESTÁ, DE SEGUIR USANDO LAS GENERALES.

ii. PUNTO 2: CREO QUE A DÍA DE HOY MUY POCOS PUEDEN PERMITIRSE RECHAZAR CONEXIONES SMTP CUYAS IPs NO TENGAN RESOLUCION DNS. YO DE MOMENTO EL PUNTO DOS DEL DOCUMENTO NO LO TENGO IMPLEMENTADO. A PARTE ESTÁ EL QUE ALGUNAS IPs TIENEN RESOLUCION INVERSA Y SON: "11.red-81-32-199.dynamicip.rima-tde.net"

iii. PUNTO 6 (SPF): ES OTRA MEDIDA MAS, QUE PARA NADA ES DEFINITIVA (SUPONIENDO QUE TODOS LO USARAMOS, UN SPAMER SERIO SIEMPRE PUEDE DAR DE ALTA UN DOMINO, UN DNS CON SU ENTRADA SPF CORRESPONDIENTE)

iv. PUNTO 8: ME ENCANTARIA PODER IMPLEMENTARLO PERO NO VEO LA FORMA DE IMPLEMENTARLO EN NUESTRO SISTEMA, LO QUE HACEMOS ES "COMERNOS" LOS MENSAJES Y LUEGO BORRARLOS, EVITANDO ASÍ LOS ATAQUES DE DICCIONARIO.

v. RESPECTO A LO DEL TAMAÑO DEL MENSAJE HE DE DECIR, QUE LO HE AUMENTADO A 50MB COMO HAS PROPUESTO (ME PARECE RAZONABLE) Y MUCHAS VECES SE GENERA MAS TRÁFICO (Y MAS MÁQUINA) RECHAZANDO MUCHOS MENSAJES DE 30MB Ó 40MB QUE DEJÁNDOLOS PASAR.

- **UPM**. (Juan Carlos Sanchez)

Respecto al documento de “Política de Tráfico SMTP”:

i. Listas Negras: El problema es la "calidad" de las listas negras. Una recomendacion generica puede llevar a que alguien utilice una lista negra "mala" y se ampare en esta AUP para justificarlo.

ii. ADSL-dinamicas:Sin problema siempre que este claro-claro que esas IP dinamicas residenciales lo son y que efectivamente no tienen posibilidad de albergar servidores de correo. ¿Los contratos tipo de estas ADSL obligan al usuario a enviar su correo electronico por los servidores del ISP? En todo caso, entiendo que se bloquea el correo hacia el puerto 25, pero el usuario de adsl con IP dinamica, podra seguir usando submit ¿no?; quizas habria que cambiar la redaccion para aclarar esto.

iii. Resolucion inversa: Que aparezca esta norma aqui puede servir para que algun ISP cuide mas que sus servidores tengar resolucion inversa. En todo caso, por lo que dice algun compañero, la implementacion práctica lleva a rechazar demasiado correo "bueno" y a que lluevan quejas y haya que dejar de hacerlo.

iv. Apartado 11. Lo quitaría o cambiaria 50 por 20-25 como máximo. Añade pesadez al correo (especialmente a la descarga pop o imap) . Creo que hay que buscar/ofrecer alternativas a nuestros usuarios para que no "tengan" que usar el correo electrónico para mandar adjuntos tan grandes.

- **US** (Carmen López)

Respecto al documento de “Política de Tráfico SMTP”:

Eliminaría la parte de tamaño de mensaje superior a 50 Mb. Nuestros alumnos tienen una cuota de 50 Mb y los pdis y pas 200Mb. Me parece que no están acordes las cifras. En este sentido creo que cada institución, dependiendo de la cuota del buzón debe poner un tamaño máximo de mensaje.

Sobre la iniciativa de Whitelisting “ Porque la valoro como 3 y no 5? Porque pienso que has puesto en marcha algo mucho mejor que esto: RACE, y da la sensación que estás bajando listones. Creo que no tendrías que hacerlo. Hay que seguir motivando a la gente a avanzar hasta los niveles más altos. No sé, eso pienso yo..”

Otros temas de interés. “Movilidad en el correo electrónico. Integración correo con LDAP”

- **UCLM** (Evangelino Valverde)

Respecto al documento de “Política de Tráfico SMTP”:

El tamaño de fichero me parece un poco alto considerando que se va a suministrar un servicio alternativo. Yo creo que 20M es bastante razonable.
- Aunque opinas que no es labor de RedIRIS, yo creo que no estaría mal complementarlo (en otros documentos, claro) con unas directrices sobre como

implementarlo en Postfix y Sendmail.

- **UNIOVI** (Jose A. Corrales)

Otros de temas de interés:

- Retardos al denegar una transacción, para ralentizar a los spammers.
- Algo tan simple (que estoy pensando hacer) como capturar todas las direcciones email con remitente acabado en uniovi.es que SALEN de mi estafeta y usar eso como lista de entrada para chequear la existencia de buzón. Con esto resuelvo el problema de los subdominios secundarios que no estan en un LDAP.

Eso sí, cada usuario nuevo debe enviar un correo a cualquier sitio para que pueda empezar a recibir. Igual que como hacemos ahora con los teléfonos móviles.

- Un sniffer. Algo que se pueda colocar en la misma red donde están las estafetas de correo (sobre todo la saliente) y con un forward de puertos del switch me monitorice el correo saliente y/o entrante para prevenir spammers internos a mi organización. Debe ser repito una herramienta no intrusiva que no suponga tocar nada del soft ni del hard de cualquier estefeta, es decir un appliance tipo sniffer del TCP 25.

- Estudiar mecanismos de priorización en el correo. Que un mensaje corto se despache rápido y los pesados por la noche...

- Algo que permita a mis usuarios saber si un mensaje llegó a su destinatario (no que lo haya leído). Ya sé que existen cosas de esas pero no se están empleando. Curiosamente algunos de mis usuarios quieren a veces saber de una forma sencilla si su correo a no se quien en USA está ya en su máquina aunque todavía no lo haya leído. Es decir una especie de entrega certificada como en Correos.

- **UC3M**.

Otros temas de interés:

1. Sería interesante un Servicio de Mailbackup a dos niveles:
   - Backup nocturno, infraestructura convencional de backup.
   - Backup horario, cada x horas para perdidas accidentales entre backups nocturnos.
2. ¿Qué sucede con RACE?
3. Herramientas de generación de estadísticas
4. Análisis de ficheros de log