RACEv2: Red Avanzada de Correo Electrónico

Criterios de calidad para la creación de un red avanzada de confianza

Criterios de encaminamiento SMTP

Comité RACEv2 V2.2

11/03/2008

3. Niveles de Calidad

En las siguientes secciones se detalla cada criterio, su nivel, su valoración en puntos, sus recomendaciones asociadas y posibles enlaces a documentación de apoyo.

Cada criterio muestra la valoración establecida por el Grupo de Trabajo RACEv2, con un máximo de 100 puntos para cada uno. La suma total del valor de los criterios que cumple una institución permite asignarle un nivel cuantitativo que mide la calidad de su Servicio de Correo Electrónico. En paralelo, se establece un nivel cualitativo que requiere por parte de la organización auditada el cumplimiento de todos los criterios obligatorios (DEBE, OBLIGATORIO,...) y, adicionalmente, el cumplimiento de algun criterio recomendado (DEBERÍA, RECOMENDABLE,...).

3.1 Criterios de encaminamiento SMTP

Los criterios de encaminamiento SMTP engloban el conjunto de normas básicas que los administradores del Servicio de Correo Electrónico deben tener presentes a la hora de implementar y configurar el primer nivel de su infraestructura. Afectan, por tanto, en su totalidad a las estafetas de primer nivel, nodos de entrada/salida o *relays* de la organización, según las diferentes referencias disponibles para su identificación dentro de su institución.

El origen de cada criterio es variado: En ocasiones fruto del consenso de la comunidad académica al considerarlo la 'mejor práctica actual', proveniente de exigencias propias de los RFCs asociados al servicio o fruto de la necesidad del cumplimiento de las normas legales vigentes.

3.1.1 Criterio 1: Reglas anti-relay

Valoración - 100 puntos

El proveedor DEBE configurar adecuadamente el puerto 25 de sus estafetas de primer nivel, disponiendo de reglas *anti-relay* que garanticen un uso legítimo, aceptando mensajes cuyo destino sea la propia organización o bien dominios delegados.

La adopción de medidas *anti-relay* se considera uno de los pasos básicos para la puesta en marcha de una estafeta de correo, y si no se cumple este criterio seremos listados en múltiples repositorios utilizados para bloquear estafetas mal configuradas, utilizadas habitualmente como salto de envío de *spam*. La práctica totalidad de las aplicaciones utilizadas para poner en marcha una MTA incluyen estas medidas, por lo que su uso es simple y sencillo.

Se dispone de variadas recomendaciones generales sobre la lucha contra el *spam*, donde se refleja la importancia para los responsables del Servicio de Correo de no ser considerados*relays* incontrolados: RFC 2505 (Lindberg, G., “Anti-Spam Recommendations for SMTP MTAs,” February 1999.) [RFC2505] y RFC 2635 (Hambridge, S. and A. Lunde, “DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*),” June 1999.) [RFC2635].

3.1.2 Criterio 2: Política de logs (trazas)

Valoración - 100 puntos

El proveedor DEBE almacenar y conservar convenientemente los ficheros de trazas (logs) de acuerdo a la legislación vigente en cada momento.

Las trazas permitirán la identificación de posibles problemas o incidentes, y servirán como fuente de datos para estudios estadísticos. A estos efectos, DEBEN contener los siguientes datos: fecha y hora de la

transacción, nombres de las MTAs que reciben y envían, identificador (ID) del mensaje, dirección de origen y destino, la MTA que actúa de relay, el estado de la transacción y el tamaño del mensaje.

Sería RECOMENDABLE que en dichas trazas además apareciesen datos propios de los filtros de la institución (puntuaciones de spam, virus detectados y tipo de contenido en cada parte de los mensajes multiparte). Con estos datos se facilitaría el estudio de nuevas técnicas usadas por spammers, extensión y peligrosidad de virus, filtros que ya no son efectivos y estadísticas.

En concreto, la legislación española obliga a conservar, por un periodo mínimo de 6 meses, todos los ficheros de traza generados (Boletín Oficial de las Cortes Generales, 121/000128 “Conservación de datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones”)

3.1.3 Criterio 3: Resolución inversa de MTAs

Valoración - 100 puntos

El proveedor DEBE definir la resolución inversa de las direcciones IP asignadas a las estafetas de primer nivel, encargadas del encaminamiento de entrada y salida de la organización.

De hecho, es muy común que las MTAs receptores apliquen como restricción al tráfico SMTP el que la MTA emisora no disponga de resolución inversa, por lo que incumplir este criterio nos situaría en un escenario de posibles rechazos y problemas de entrega de los mensajes emitidos por nuestros usuarios.

El RFC 3172 (Huston, G., “Management Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain ("arpa"),” September 2001.) [RFC3172] detalla éste y otros requisitos asociados al direccionamiento y encaminamiento en la Red.

3.1.4 Criterio 4: Número máximo de destinatarios

Valoración - 100 puntos

El numero máximo de destinatarios de un correo DEBE estar comprendido entre 100 (RFC 2821 Klensin, J., "Simple Mail Transfer Protocol," April 2001) y 150 (recomendación de RedIRIS).

3.1.5 Criterio 5: Control de acceso al puerto 25 en entrada / salida

Valoración - 100 puntos

El proveedor DEBERÍA diseñar y aplicar una topología del Servicio de Correo que concentre en varias estafetas todo el tráfico de entrada y salida de su organización (estafetas de primer nivel), estando éstas bajo su directa administración.

Este criterio pretende enfatizar la necesidad de implantar una topología de encaminamiento del correo con el fin de homogeneizar de una forma centralizada el tratamiento del correo electrónico, de entrada/salida, de cada unidad organizativa del proveedor, facilitando el uso adecuado de las infraestructuras, previniendo posibles ataques y haciendo posible la implantación de los demás criterios de RACEv2

3.1.6 Criterio 6: Tamaño máximo de mensaje

Valoración - 100 puntos

El tamaño máximo de mensaje DEBERÍA ser controlado, formando parte de la configuración de las

estafetas de primer nivel corporativas. El tamaño máximo de mensaje lo definirá cada institución atendiendo a las cuestiones que considere oportunas.

Dado que los sistemas de correo electrónico no están pensados para transferir ficheros de gran tamaño, el proveedor DEBERÍA ofrecer a los usuarios algún sistema de transferencia de ficheros para paliar esta situación. Existen varios desarrollos para ofrecer este servicio a los usuarios.

3.1.7 Criterio 7: Definición de registros SPF (Sender Policy Framework)

Valoración - 100 puntos

El proveedor DEBERÍA definir en su zona DNS los registros SPF (Sender Policy Framework) de todos los dominios de su responsabilidad, asociándolos a los nodos de correo que efectúen el encaminamiento de salida SMTP (estafeta de primer nivel)

Con esta medida el proveedor pone a disposición de toda aquella MTA que implemente chequeos SPF la relación de MTAs que están autorizadas para enviar el correo que se encuentra bajo su responsabilidad, lo que disminuiría la probabilidad ante posibles ataques y/o aumentos de carga en sus estafetas por mensajes devueltos.

La especificación SPF actual está contenida en el RFC 4408 (Wong, M. and W. Schlitt, “Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1,” April 2006.) [RFC4408].

3.1.8 Criterio 8. Uso de Lista Blanca de RedIRIS

Valoración – 100 puntos

El proveedor DEBERÍA declarar y mantener actualizadas en la Lista Blanca de RedIRIS las direcciones IP de sus relays de correo así como incluirlas en los chequeos de conexión SMTP para evitar el bloqueo de tráfico generado en dicha Lista Blanca

La Lista Blanca de RedIRIS incluye direcciones IP de Estafetas de salida de universidades españolas y de operadores españoles de confianza para RedIRIS. El chequeo de dicha lista garantizará que no se bloquee el tráfico procedente de las estafetas incluidas reduciendo la posibilidad de falsos positivos.

La Lista Blanca es un Servicio de RedIRIS cuyas especificaciones pueden ser encontradas en http://www.rediris.es/abuses/

3.1.9 Criterio 9: Chequeo de SPF en correo entrante

Valoración - 55 puntos

El proveedor DEBERÍA configurar sus estafetas de primer nivel para que se lleven a cabo los correspondientes chequeos SPF del correo entrante.

Es posible que nuestra aplicación habitual de MTA ya incorpore esta posibilidad, y por tanto simplifique las tareas de integración de los chequeos de SPF. Este criterio establece en todo caso la posibilidad de analizar los mensajes entrantes a nuestra organización para determinar si cumplen los registros SPF publicados por el dueño del dominio, pero no indica las acciones a realizar con los mensajes que no pasen el test aplicado.

3.1.10 Criterio 10: Control de destinatarios

Valoración - 95 puntos

La organización DEBERÍA disponer de algún tipo de mecanismo que permita rechazar en sus estafetas de primer nivel aquellos mensajes dirigidos a destinatarios no existentes.

3.1.11 Criterio 11: Control de flujo SMTP

Valoración - 80 puntos

Se DEBERÍA disponer de algún tipo de mecanismo de control de flujo en transacciones SMTP internas y externas. Este mecanismo permite controlar el numero de correos enviados por una IP en un intervalo de