RACEv2: Red Avanzada de Correo Electrónico

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

Criterios de autenticación y cifrado

Comité RACEv2 V2.2

11/03/2008

3.3 Criterios de autenticación y cifrado

Esta sección engloba la valoración de criterios y recomendaciones de uso de autenticación en el contexto de la autenticación (mecanismos, protocolos y arquitecturas) que garanticen la privacidad de las credenciales y la integridad de la información transferida.

3.3.1 Criterio 14: Autenticación centralizada

Valoración - 100 puntos

El proveedor DEBERÍA disponer de un sistema de autenticación centralizada, aplicado a su infraestructura de servicio.

3.3.2 Criterio 15: Acceso externo cifrado

Valoración - 100 puntos

La organización DEBERÍA ofrecer únicamente servicios basados en protocolos de recogida de mensajes con cifrado SSL/TLS (POPs, IMAPs) y un servicio de correo saliente SMTP con TLS, así como acceso al correo por Web vía HTTPs para los usuarios externos.

El RFC 2595 (Newman, C., “Using TLS with IMAP, POP3 and ACAP,” June 1999.) [RFC2595] detalla el uso de TLS en los protocolos más comunes de recogida de mensajes.

3.3.3 Criterio 16: Servicio SUBMISSION

Valoración - 100 puntos

El proveedor DEBERÍA ofrecer acceso autenticado (SASL) y cifrado (TLS) a través del puerto 587 (SUBMISSION) para todos sus usuarios, dejando el puerto 25 (SMTP) para tráfico entre MTAs, tal y como se define en el RFC4409 (Gellens, R. and J. Klensin, “Message Submission for Mail,” April 2006.) [RFC4409].

La separación de ambos tráficos SMTP, desde el punto de vista del administrador aporta la posibilidad de aplicar reglas y controles más específicos en cada caso. Adicionalmente, desde el punto de vista de un usuario desplazado fuera de su organización, no se verá afectado por posibles cortes del puerto 25 en las instalaciones que visita, pudiendo seguir utilizando el servicio, cifrado y autenticado, de correo saliente de su institución origen en el TCP/587.

Se recomienda leer el RFC5068 (BCP 134,RFC5068 on Email Submission Operations: Access and Accountability Requirements) que complementa al RFC4409 y que define unas buenas prácticas para administradores de correo para gestionar el servicio de correo por el puerto 587 tanto para usuarios locales como viajeros (*roaming*).

3.3.4 Criterio 17: Cifrado MTAi-MTAi

Valoración - 60 puntos

El proveedor DEBERÍA configurar sus sistemas para permitir la comunicación cifrada (SMTP con TLS)

entre las distintas MTAs de su organización, tal y como se establece en el RCF 3207 (Hoffman, P., “SMTP Service Extension for Secure SMTP over Transport Layer Security,” February 2002.) [RFC3207], que define la extensión del protocolo SMTP para su cifrado sobre TLS.

El cumplimiento de este criterio aporta privacidad adicional al mensaje, y evita que entornos de la red de la organización expuestos a captura de tráfico sirvan a los fines de usuarios maliciosos.

3.3.5 Criterio 18: Cifrado MTA-MTA

Valoración - 60 puntos

Tal y como se indicó en el criterio anterior, y aplicado al tráfico externo, el proveedor DEBERÍA configurar sus sistemas para permitir la comunicación cifrada (SMTP con TLS) con *relays* externos (RFC 3027 (Hoffman, P., “SMTP Service Extension for Secure SMTP over Transport Layer Security,” February 2002.) [RFC3207]).