TLP:CLEAR

ALERTA TÉCNICA

MICITT-DC-CSIRT-AT-1232-2025

Protocolos de autenticación para correo electrónico

Se les comunica a los Directores (as) /jefes (as) de Tecnologías de Información y a los enlaces de ciberseguridad para que tomen las medidas necesarias.

Los protocolos de autenticación de correo electrónico son sistemas que verifican la identidad del remitente y aseguran la integridad del mensaje, previniendo el spam y la suplantación de identidad. Estos protocolos funcionan validando que el correo electrónico proviene de la fuente autorizada y no ha sido alterado durante la transmisión.

Los principales protocolos en uso son DMARC, DKIM y SPF. Los cuales, al utilizarlos de manera conjunto ayudan a evitar que los spammers, phishers y otras partes no autorizadas envíen correos electrónicos en nombre de un dominio que no poseen.

Por tanto, los protocolos de autenticación de correo electrónico son esenciales para garantizar la seguridad y confiabilidad de las comunicaciones por correo electrónico, protegiendo tanto a remitentes como a destinatarios.

Importancia de los protocolos de autenticación

SPF (Sender Policy Framework): Es un protocolo que permite a los propietarios de un dominio especificar qué servidores están autorizados para enviar correos electrónicos en su nombre. Esto ayuda a prevenir el phishing y la suplantación de identidad (spoofing) al verificar que el correo proviene de un servidor autorizado.

DKIM (DomainKeys Identified Mail): Añade una firma criptográfica a los correos electrónicos que permite al servidor receptor verificar que el mensaje no ha sido alterado y que realmente fue enviado por el dominio que dice ser. Esto garantiza la integridad y autenticidad del mensaje.

DMARC (Domain-based Message Authentication, Reporting & Conformance): Es un protocolo que indica a los servidores receptores cómo deben tratar los correos que fallan las verificaciones SPF y DKIM, además de permitir recibir reportes sobre intentos de suplantación o problemas de autenticación. DMARC mejora la protección contra ataques de phishing y spoofing al definir políticas claras y facilitar el monitoreo

Riesgos por mala configuración o ausencia

Los dominios que no hayan configurado correctamente el SPF, el DKIM y el DMARC pueden encontrarse con que sus correos electrónicos son puestos en cuarentena como spam, o no son entregados a sus destinatarios. También corren el peligro de que los spammers se hagan pasar por ellos.

Phishing y Spoofing: Sin una configuración correcta de SPF, DKIM y DMARC, los atacantes pueden enviar correos falsificados haciéndose pasar por tu dominio, lo que puede llevar a robo de información, fraude financiero y daño a la reputación de la empresa.

Rechazo o filtrado de correos legítimos: La falta de estos protocolos puede hacer que tus correos legítimos sean marcados como spam o rechazados por los servidores receptores, afectando la comunicación con clientes y socios.

Pérdida de confianza y reputación: Los usuarios y clientes pueden perder confianza en tu marca si reciben correos fraudulentos que aparentan ser tuyos, lo que impacta negativamente en la imagen corporativa

Beneficios de la autenticación de correo electrónico:

- Mayor seguridad: Protege contra el phishing, el spam y la suplantación de identidad, evitando que mensajes fraudulentos lleguen a los usuarios.
- Mejora la reputación del dominio: Aumenta la confianza de los destinatarios y mejora la tasa de entrega de correos electrónicos legítimos.
- Cumplimiento de regulaciones: Ayuda a cumplir con las políticas de seguridad y privacidad de dato.

Recomendaciones

- **Implementar y publicar registros SPF, DKIM y DMARC en el DNS de tu dominio**, es decir, configura correctamente cada uno de estos protocolos para asegurar la autenticidad y protección de tus correos electrónicos.
- **Monitorear los reportes DMARC**, proceder a realizar la configuración de un buzón para recibir reportes DMARC y analiza los intentos de suplantación para ajustar las políticas y mejorar la seguridad.
- **Mantener actualizados los registros SPF**, revisar que solo los servidores autorizados estén incluidos en el registro SPF para evitar falsificaciones.
- **Firmar todos los correos salientes con DKIM**, ya que esto garantiza la integridad del mensaje y ayuda a los servidores receptores a validar la autenticidad del correo.
- **Configurar políticas DMARC estrictas**, para que los servidores receptores sepan cómo actuar ante correos que no pasen las verificaciones (rechazar o poner en cuarentena).

Referencias

- ¿Qué son DMARC, DKIM y SPF? | Cloudflare. (n.d.). https://www.cloudflare.com/es-es/learning/email-security/dmarc-dkim-spf/
- Práctica recomendada para la autenticación de correo electrónico: formas óptimas de implementar SPF, DKIM y DMARC. (2024, August 8). Cisco. https://www.cisco.com/c/es_mx/support/docs/security/email-security-appliance/215360-best-practice-for-email-authentication.html

En caso de alguna duda o consulta, se pueden comunicar al CSIRT-CR por medio del correo electrónico csirt@micitt.go.cr

GREGORY ALEJANDRO PACHECO CANTILLO (FIRMA)
Firmado digitalmente por GREGORY ALEJANDRO PACHECO CANTILLO (FIRMA)
Fecha: 2025.07.07 17:28:59 -06'00'

Analista de Ciberseguridad

JOSE ALONSO ROCHA VILLALOBOS (FIRMA)
Firmado digitalmente por JOSE ALONSO ROCHA VILLALOBOS (FIRMA)
Fecha: 2025.07.07 17:32:12 -06'00'

Analista de Ciberseguridad