Qué es el Email Spoofing y cómo evitarlo con el registro SPF

Las personas que trabajan continuamente con el correo electrónico, puede ser que se hayan encontrado en la situación de haber recibido correos enviados por ellos mismos o bien un gran número de correos devueltos a direcciones que ellos no han enviado. Entonces es cuando entra el pánico y se tiende a pensar que el correo está comprometido, pero en la mayoría de los casos lo más probable es que se esté dando una situación conocida con el nombre de "Spoofing" o "suplantación de identidad".

A lo largo de este White Paper ahondaremos más en este problema y veremos cómo solucionarlo mediante el uso de registros SPF.

¿Qué es el Spoofing?

Lo primero que debemos saber es que se trata de una técnica utilizada por los spammers a la hora de enviar correo basura. El hecho de que los filtros antispam cada vez funcionen mejor ha provocado que los atacantes tengan que utilizar nuevas técnicas a la hora de realizar este tipo de envíos para saltarse los filtros. Una de las más utilizadas es la conocida como "Mail Spoofing", que no es otra cosa que la suplantación de identidad de la persona que realiza el envío del email. Dicho de otra forma más sencilla, el Mail Spoofing es cuando alguien nos envía un correo donde el campo FROM del remitente es falso, de forma que podrían decirte que el correo te lo ha enviado una persona, empresa o entidad bancaria conocida, pero que realmente no son ellos los que realizan este envío. El spoofing también es muy utilizado para llevar a cabo ataques mediante técnicas de Phising.

¿Está mi cuenta de correo electrónico comprometida?

El principal temor que nos puede aparecer cuando recibimos algún correo enviado por nosotros mismos o bien un amplio número de correos devueltos, es pensar si nuestra cuenta está comprometida. Lo primero que debemos tener claro es que el Mail Spoofing es un engaño, alguien que se hace pasar por nosotros, lo que significa que nuestra cuenta no tiene por qué estar comprometida.

Para estar más seguros aún, lo que se puede hacer es revisar las cabeceras de los correos o revisar los emails enviados para comprobar que no han salido de nuestra cuenta de correo. También es bueno contactar con el servicio técnico de vuestra empresa de hosting para que revise que realmente la cuenta no está comprometida.

En caso de que se compruebe que los emails se envían desde nuestra cuenta, deberemos revisar nuestro equipo en busca de algún tipo de virus y también cambiar la contraseña de la cuenta de correo.

¿Por qué es posible el Mail Spoofing?

La suplantación de identidad es posible debido a que el protocolo SMTP (Simple Mail Transfer), el principal protocolo utilizado para el envío de los correos electrónicos, no incluye un mecanismo de autenticación. A decir verdad, sí que existe una extensión del protocolo SMTP (especificada en el IETF RFC 2554) que permite a un cliente SMTP negociar un nivel de seguridad con un servidor de correo, aunque esta funcionalidad no siempre se toma.

Si no se establecen las precauciones adecuadas, cualquiera que tenga ciertos conocimientos de informática puede modificar el envío de los correos para que parezca que han sido enviados por una cuenta cuando realmente no ha sido así. De esta forma cualquiera puede enviar emails falsificados que parecen ser tuyos, con un mensaje que no escribiste desde tu propio dominio.

Utilizar registro SPF para evitar el Mail Spoofing

El método más eficaz y seguro para combatir el problema del Mail Spoofing, es mediante el uso de los registros SPF (Sender Policy Framwork). Gracias al uso de estos registros, conseguiremos que un dominio autorice a un servidor el envío de correo electrónico. De esta forma, si alguien realiza el envío de un correo desde un servidor diferente al que se ha autorizado, el mensaje será considerado directamente SPAM o bien no será entregado.

Haciendo uso del registro SPF el problema del spoofing desaparece, ya que tanto los servidores de salida como los de entrada se encargarán de verificar que se ha enviado desde un servidor autorizado. El problema que nos podemos encontrar con este tipo de verificación es que debe estar activado en ambos servidores, cosa que sí ocurre con la mayoría de proveedores de alojamiento web. A continuación pasaremos a explicar el funcionamiento de la validación mediante SPF:

1. El emisor realiza el envío de un correo electrónico.
2. El mail llega al servidor de correo entrante del destinatario, el cual se encarga de llamar a su Sender ID Framework (SIDF).
3. El SIDF consulta el registro SPF del dominio que realiza el envío y determina si pasa o no pasa.
4. Si el correo ha sido enviado desde un servidor autorizado, el mensaje pasa a ser analizado por los filtros antispam para que sea catalogado como corresponda.
5. Por último, el mensaje es entregado al buzón del destinatario.

Un ejemplo de registro SPF para combatir este tipo de problemas podría ser el siguiente:

v=spf1 a ip4:223.45.60.5 include:_spf.google.com ~all

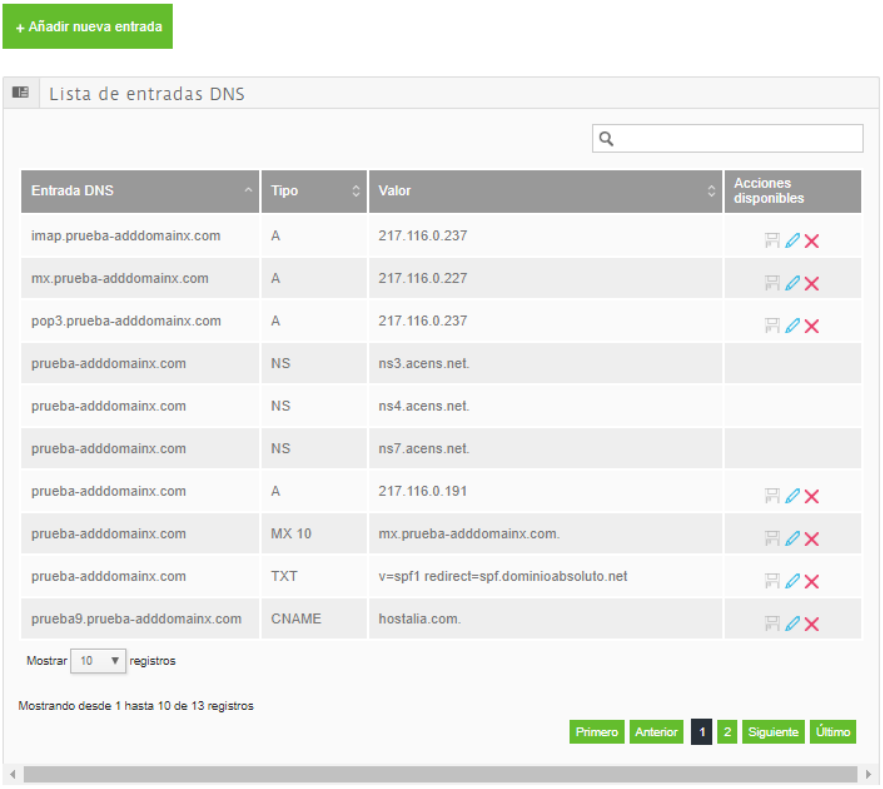
Veamos lo que significa cada una de sus partes:

- **v**: define la versión usada de SPF, en este caso se trataría de la primera versión.
- **a**: autoriza al host identificado en el registro A del dominio a enviar correos electrónicos.
- **ip4**: permite indicar una sola dirección IPv4 o un rango aceptable de direcciones IPv4.
- **include**: autoriza que los correos electrónicos sean enviados de parte del dominio que ahí se indique.
- **~all**: denota que esta lista tiene todas las inclusiones y que a ningún otro servidor se le permite enviar correos electrónicos desde nuestro dominio.

Crear registro SPF en acens

En el caso de los alojamientos web de acens, crear uno de estos registros es muy sencillo. Lo primero de todo será entrar a nuestro panel desde la dirección “panel.acens.net”. Una vez dentro, en el menú de la izquierda seleccionaremos la opción “**Gestión DNS**”.

Nos aparecerá un menú con las diferentes entradas de DNS que tenemos asociadas al dominio. Pulsaremos en el botón añadir nueva entrada.



Nos aparecerá un pequeño formulario con tres campos que deberemos cumplimentar.

- **Entrada**: lo dejaremos vacío.
- **Tipo**: del menú desplegable seleccionaremos el tipo TXT.
- **Valor**: ahí indicaremos el valor que tendrá el registro SPF que vamos a crear. En nuestro caso de ejemplo, indicaríamos "v=spf1 a ip4:223.45.60.5 include:_spf.google.com ~all". Tendríais que sustituir la IP y el nombre del dominio por los que utilice vuestro correo.

Por último, quedaría pulsar sobre el botón "**Agregar Entrada**" para que esta se generase en el sistema.

Como hemos podido ver, el registro SPF es nuestro gran aliado para combatir la suplantación de identidad. Crearlo es muy sencillo, pero en caso de duda, consultar a vuestro proveedor de alojamiento web.