Directrices de autenticación del remitente (SPF)

SPF: Sender Policy Framework

INFORME

Resumen

La mayor parte de los problemas del correo electrónico proceden de direcciones falsificadas. El protocolo SMTP no contempla la posibilidad de comprobar si un correo es auténtico o si ha sido enviado desde una dirección de correo falsificada. Esto es lo que hace SPF (Sender Policy Framework), una iniciativa internacional que está ganando terreno. RedIRIS considera necesario apostar y apoyar esta tecnología para intentar frenar los problemas que afectan al correo electrónico.

SPF funciona mediante la declaración de registros SPF en el DNS. Al igual que se publican registros MX para el correo entrante, SPF recomienda también su publicación para el correo saliente. En este informe se describe cómo hacerlo.

Palabras clave: correo electrónico, spf, autenticidad.

Summary

Most of the problems of electronic mail arise from spoof email addresses. The protocol SMTP does not contemplate the possibility of verifying wether a mail is authentic or if it has been sent from a falsified mail address.

This can be done via SPF (Sender Policy Framework), an international iniciative that is advancing quickly. RedIRIS considers necessary to bet and to support this technology to try to stop the problems concerning electronic mail.

SPF works by declaring SPF records in the DNS. In the same way as MX records are published for inbound mail, SPF recommends its publication also for outbound mail. In this inform the way to do it is described.

Keywords: electronic mail, spf authenticity.

1.- Introducción

SPF (http://spf.pobox.com) traducido al castellano podría ser algo parecido a directrices de autenticación del remitente, es decir, un entorno que permite comprobar si el remitente de un correo particular está o no falsificado. SPF necesita que la empresa del remitente tenga publicado un registro SPF en el DNS de su dominio de forma que los servidores de correo destino puedan ser capaces de determinar si el correo fue realmente enviado por el emisor o si fue falsificado. Si una empresa no publica sus registros SPF el resultado del chequeo será *desconocido*. Esta tecnología constituirá una de las mejores herramientas contra la distribución de *phishing* que tanto afecta a las entidades financieras en la actualidad.

SPF es un esfuerzo conjunto de la comunidad internacional que está ganando terreno rápidamente. Aunque a día de hoy SPF no es todavía un estándar en Internet, es la única esperanza consolidada para mitigar muchos de los problemas y fraudes que se producen a través del correo electrónico. Su éxito básicamente es la sencillez de implementación. Consideramos que no se podrá solucionar el problema del spam ni los fraudes si previamente no se definen soluciones para autenticar el dominio emisor, y SPF es la solución más simple, implantada y desarrollada que existe.

La inversión en tiempo necesaria, para desplegar SPF en cualquier institución o empresa es escasa y siempre positiva independientemente de su futura estandarización; ya que su implantación internacional es creciente. Este informe pretende dar a conocer esta iniciativa y que las instituciones y empresas españolas lo adopten en sus estrategias tecnológicas.

Desde el grupo IRIS-MAIL, RedIRIS pretende fomentar el despliegue de SPF en su Comunidad en dos fases diferenciadas:

- Fase pasiva. Declaración de los registros SPF por parte de las instituciones lo que implica una revisión de los propios servicios de correo. Actualmente hay 35 instituciones RedIRIS que han definido estos registros.
- Fase activa. Promover el chequeo SPF del correo entrante.

SPF es un mecanismo que proporciona un método para autenticar el dominio de una dirección de correo. Permite a las estafetas receptoras comprobar que la estafeta emisora que desea entregar un mensaje identificado como procedente de un determinado dominio, está autorizada a hacer dicha entrega.

Supongamos, por ejemplo, que un equipo cualquiera de la Red intenta entregar un mensaje al servidor de la Institución ABC, un mensaje que dice proceder de la dirección `<usuario@centro.es>` que es una dirección existente de un dominio correctamente registrado y configurado. Es muy posible que el servidor de ABC acepte sin muchas más comprobaciones el mensaje. Si otro equipo diferente intenta entregarlo utilizando la misma dirección origen del mensaje seguramente el servidor de ABC también lo acepte. ¿Y desde un nuevo equipo? también lo acepta. ¿Y otro más? idem.

Como vemos los mecanismos actualmente no comprueban el origen del mensaje antes de aceptarlo. Una comprobación que nos confirme que el equipo emisor, es un servidor que los responsables del dominio *centro.es* han designado para la entrega. SPF permite esta comprobación. Mucho software de spam, de inoculación de virus y distribución de phishing aprovecha esta ausencia de comprobaciones en la entrega para usar direcciones falsificadas y entregar correo infectado y no deseado.

SPF permite garantizar en la Red la autoría del correo que lleve nuestro dominio y comprobar el origen de lo que recibimos. SPF no es un sistema para eliminar el spam ni el phishing sino para evitar el uso ilegítimo de direcciones de correo y garantizar la legitimidad, imagen y honor de nuestro dominio que es la marca de nuestra presencia en la Red y por tanto de nuestra institución.

Contra este tipo de intrusiones en el correo electrónico sirve SPF. Pero debemos remarcar que **no es un sistema diseñado para erradicar el spam** sino para solucionar el problema del uso ilegítimo de las direcciones de correo y garantizar la legitimidad de nuestro dominio. SPF no comprueba el contenido del mensaje sino sólo la legitimidad del tráfico de entrada eliminando el falsificado que actualmente es un alto porcentaje.

2.- ¿Cómo funciona, a grandes rasgos, SPF?

La idea de SPF es mimetizar el mecanismo que se utiliza para la entrega de correo y aplicarlo también en la recepción. Es conveniente recordar que: **durante el envío** de mensajes de un dominio a otro, la estafeta emisora comprueba el dominio destino del mensaje y utiliza el sistema de nombres dominios (DNS) para localizar los servidores que están designados para la *recepción* (simplificando: registros MX y registros A). Es lo que se llama enrutamiento de correo.

SPF es una imagen especular del mecanismo anterior: **durante la recepción** de mensajes, la estafeta receptora, comprueba el dominio origen del mensaje y utiliza el sistema de nombres de dominios (DNS) para localizar los servidores que están designados y autorizados para dicho *envío* (en este caso: registros TXT con un formato propio, formato spf).

Llegados a este punto, la estafeta receptora puede decidir rechazar el mensaje si el equipo que ha establecido la conexión no está convenientemente autorizado en los registros spf para la emisión de mensajes con determinado dominio.

3.- Implementación de SPF

Implementar SPF no es necesario para que nuestro servicio de correo funcione. Es una buena práctica, fácil de implantar y que garantizará al exterior la buena imagen de nuestro dominio y del correo que sale de los servidores. Para desplegar SPF debemos actuar en dos frentes aunque ambas acciones son independientes y no importa el orden en el que sean implantadas.

- **Salida correo**: publicación de registros SPF para cada dominio de la institución.
- **Entrada correo**: instalación de mecanismos de gestión basados en SPF en las estafetas receptoras de mensajes (SPF-enabled MTAs).

Aunque independientes, como hemos dicho, ambas operaciones son complementarias y de poco sirve una sin la otra: que todos los dominios publiquen sus registros SPF no es útil si no hay estafetas que utilicen estos registros para la gestión de recepción (y eventualmente el rechazo de mensajes); análogamente, poco eficaces serán aquellas estafetas capaces de interpretar registros SPF, si el número de dominios que publican estos registros no aumenta.

Los pasos recomendados para implementar SPF son:

1º.- Tráfico entrante: Publicar en DNS los registros SPF de los dominios bajo nuestra responsabilidad.
2º.- Divulgarlo entre nuestros usuarios.
3º.- Tráfico entrante. Instalar y configurar los módulos SPF adecuados a su MTA para analizar el correo entrante y tomar las correspondientes acciones.

4.- Publicación de registros SPF

Operativamente es la más sencilla de las dos acciones para avanzar hacia la implantación completa de SPF, pero hay que estar muy seguros de lo que hacemos. Publicar consiste en declarar –para cada uno de los dominios de nuestra institución–, unos registros que indicarán las IPs responsables de enviar correo. Este registro designa los servidores que **están autorizados** para enviar correo desde este dominio. Básicamente al publicar estos registros en DNS estamos definiendo nuestra política de salida del correo, y de alguna forma mejorar la reputación de nuestro dominio de correo en Internet. Se deben definir registros SPF para todos nuestros **dominios** y subdominios de correo, no para nuestros **servidores**.

Es importante destacar que, al publicar estos registros, **la institución accede de forma explícita a que sean rechazados (o tratados de forma diferenciada) todos aquellos mensajes que sean emitidos desde servidores distintos a los descritos por los mismos, aceptando, de alguna forma, la responsabilidad del rechazo, que no recae, como suele ser habitual, en la estafeta rechazante.** En cierta manera, la estafeta receptora rechazará un mensaje por "motivos SPF" porque la institución responsable del dominio así lo solicita en sus registros SPF

Para intentar explicarlo mejor, lo haremos con un ejemplo tipo de registro SPF en un servidor DNS (tipo Bind) tendría el siguiente aspecto:

```
centro.es      IN TXT  "v=spf1 a mx ptr -alll"
```

Donde,

- *centro.es* es el nombre del dominio afectado (por tanto, este registro se aplica a los mensajes con origen (MAIL FROM) del tipo <user@centro.es>. Es importante resaltar que este registro no se aplica a subdominios debajo del dominio afectado, es decir no se aplica a mensajes del tipo <user@subdom.centro.es> que debería tener su propio registro SPF según política institucional.
- *IN TXT*, identifica la categoría de registro en el sistema de nombres de dominio (DNS). Se trata de un registro de tipo "texto" de direcciones Internet.
- "v=spf1 a mx -all" es la parte spf del registro DNS; la más importante. Más concretamente:

  - v=spf1 indica que se trata de un registro spf versión 1 (la única hasta el momento)

  - a y ***mx*** identifican los servidores que podrán enviar mensajes del tipo user@centro.es, en este caso identificados como:

"a" está indicando que podrán hacerlo las IPs asociadas a los registros de tipo A del dominio centro.es.

- "mx" está indicando que podrán hacerlo las IPs asociados a los registros MX del dominio centro.es

"ptr" está indicando que podrán hacerlo las IPs cuya resolución inversa pertenezca al dominio *.centro.es*

-all indica el valor de la información declarada anteriormente con las opciones de este ejemplo: "a", "mx","ptr". En este caso indica que el valor de lo declarado es alto y por tanto cualquier chequeo spf deberá dejarlo pasar. El resultado definido en el protocolo SPF por parte del MTA es "Pass". No es necesario hacer chequeos adicionales al mensaje.

Podríamos poner "**~all**" en el registro spf con lo que estaríamos declarando que las IPs indicadas en los registros "a","mx" o "ptr" las estamos dando un valor menor y que cualquier chequeo spf lo dejará pasar pero avisando que es conveniente hacer otro tipo de chequeos pues no son de confianza. El resultado definido en el protocolo spf por parte del MTA es "softail".

"~all" es considerada una opción transitoria y para eso fue definida dentro del protocolo spf. Es decir cuando queremos declarar nuestros registros SPF pero no estamos seguros que algún usuario no vaya a utilizar nuestras IPs para enviar correo como @centro.es.

Por tanto ¿qué estamos declarando cuando definimos unos registros SPF para el dominio correo.es?

```
centro.es       IN TXT  "v=spf1 a mx ptr -alll"
```

Estamos **garantizando** la reputación de la institución asociada al dominio *centro.es* certificando que exclusivamente (-all) podrán enviar correo como @centro.es las IPs correspondientes a:

- Registro A del dominio *centro.es*.
- Registros MX del dominio *centro.es*
- Cualquier IP cuya resolución inversa tenga el dominio *.centro.es*

En resumen un registro spf tiene dos partes:

1.- Parámetros que nos permiten indicar las IPs que declaramos como emisoras de correo de nuestra institución
2.- Parámetro del valor que damos a lo declarado que está asociado a un resultado en el algoritmo SPF y que por tanto intervendrá en las acciones que tomen los servidores remotos al entrar el correo.

5.- Ejemplos SPF

A continuación damos ejemplos básicos de dos configuraciones típicas en RedIRIS.

- Varias direcciones institucionales (@centro.es, @subd.centro.es)
- Un sólo punto de encaminamiento de entrada/salida (smtp.centro.es)
- Servicio a usuarios móviles institucionalizado

Como se ha comentado previamente es necesario declarar registros SPF para cada una de las direcciones oficiales de la institución con o sin subdominios. Es necesario declarar las máquinas que sacan al exterior el correo. Todos los usuarios de esta institución conocen y disfrutan de los servicios de correo institucionales cuando salen fuera del dominio: en su casa, congreso, etc. Por tanto los registros en este caso serían:

```
centro.es           IN TXT   "v=spf1 mx -all"
subd.centro         IN TXT  "v=spf1 mx -all"
```

Los usuarios no podrán encaminar correo con ninguno de los Sender institucionales a través de servidores diferentes que los declarados como registros MX. Cualquier servidor que reciba correo con estos dominios procedente de las IPs de los registros MX deberá aceptarlos (-all indicado en el registro dice al servidor **PASS**). El procedente de IPs diferentes que las declaradas en los registros MX podrá ser rechazado (**FAIL**), pero recordemos que no lo rechazan los servidores que chequean el correo sino que es rechazado porque lo indica la política declarada por la propia institución a través de los registros spf.

6.- Recomendaciones para la declaración de registros SPF

Un resumen de recomendaciones básicas previas a declarar registros SPF en el DSNS en su institución es el siguiente:

- Estudio de evaluación acerca de...
  - la disponibilidad de dominios y Estafetas salientes
    1.- Relación de dominios de correo electrónico de la Institución
    2.- Relación Estafetas salientes para cada uno de los dominios
  - los servicios externos para enviar correo desde el exterior con direcciones institucionales
  - ¿ofrecemos servicios conocidos por los usuarios? SMTP-AUTH, WebMail, SSH, VPNs...SAUCE
  - ¿Algún usuario utiliza otros proveedores para enviar correo de nuestra institución?
  - los servicios de forwarding
    1.- ¿Son soportados por la política del Servicio?
    2.- Grado de uso en la institución

Después del estudio de evaluación de estos aspectos

- Teniendo claro y seguro...
  - que todos los dominios y Estafetas oficiales de nuestra institución
  - que todos (-all) o algunos (~all) usuarios utilizan los servicios institucionales de correo desde el exterior (casa, viajes etc.)
  - que el uso que se hace del forwarding en la institución
- Informar y avisar a los usuarios acerca de estas novedades
- Proceder a declarar los registros SPF de nuestra institución, teniendo en cuenta algunas recomendaciones como:
  - Dar prioridad a direcciones canónicas (mx, include etc.) frente a las IPs (a, ipv4, etc.) que son más sensibles a posibles cambios
  - Utilizando la opción ~all de forma provisional podrá ir declarando sus registros SPF mientras se solucionan los problemas de acceso al correo desde el exterior
  - Si no dispone de servicios externos de correo y desea declara registros SPF podrá usar los registros SPF de SAUCE

centro.es IN TXT "v=spf1 mx include:sauce.rediris.es -all"

7.- Conclusiones

La ventaja operativa fundamental de SPF es que gracias a que ayuda a autenticar al emisor, nos permitirá:

- Reducir el Spoofing, phishing, fraudes etc.
- Reducir tráfico basura: propagación de virus, "*user unknow*"
- Reducir el Spam falsificado (% alto del spam)
- Denunciar, filtrar al spam sin falsificar
- Asegurar en la Red la presencias de nuestro dominio en el tráfico SMTP

En general recuperar la confianza de los usuarios de correo electrónico y aliviar la carga de las estafetas de correo, mejorando el uso de los recursos (cpu, almacenamiento y red) y en general la calidad del Servicio de correo electrónico.

SPF comienza a modificar el paradigma que hasta ahora impera en el intercambio de correo electrónico: "se asume la inocencia del emisor hasta que no se demuestre su culpabilidad" por otro donde "se asume culpabilidad hasta que no se pruebe la inocencia del emisor".

SPF no es la solución definitiva para eliminar el spam. Es sólo una del abanico de opciones entre las que elegir para mantenerlo bajo un control razonable. Por sí sola, ya sabemos que no es suficiente. La combinación de varias soluciones de este tipo colabora a mantener el volumen de spam en unos márgenes aceptables.

El grado del éxito de SPF dependerá del número de dominios registrados a nivel internacional. Actualmente su crecimiento es exponencial. El conjunto de dominios SPF registrados en Internet puede ser interpretado como una gran lista blanca de dominios en los que podremos confiar. Nada impedirá que un dominio con registro SPF distribuya correo no deseado basura o spam pero dispondremos de más datos para canalizar una denuncia.

Os animo a evaluar e implementar esta tecnología y si tenéis cualquier duda os integréis en el Grupo de Trabajo IRIS-MAIL (http://listserv.rediris.es/iris-mail.html) donde se tratan estos temas y comparten experiencias.

Jesús Sanz de las Heras
(jesus.heras@rediris.es)
Servicio de correo electrónico

Directrices de autenticación del remitente (SPF)