GLOBAL CYBER ALLIANCE

DEFEND & DELIVER

DMARC

Email authentication for better email security

ONLINE BOOTCAMP

Shehzad Mirza

Director de operaciones

smirza@globalcyberalliance.org

gca-dmarc@globalcyberalliance.org

Introducción a SPF y DKIM

SPF
(Sender Policy Framework, convenio de remitentes)

SPF
Convenio de remitentes

- Define qué servidores están autorizados para enviar correo con el dominio de una organización
- Utiliza el valor del sobre remitente (‘envelope from’) para determinar el dominio de procedencia
- En el registro de texto del DNS
  - Solo puede haber un registro de SPF

Registro de texto en el DNS para SPF

- Configuración básica:

  Nombre: <*dominio*> o @ o dejar en blanco

  Valor: "v=spf1 mx -all"

- Configuración compleja:

  Nombre: <*dominio*>

  Valor: "v=spf1 mx a:<*otros servidores de correo*> include:<*dominio externalizado*> ip4:<*dirección IP/rango*> ~all"

Etiquetas SPF (I)

v=spf1	El registro de texto empieza siempre así; define la versión de SPF que se está usando (en estos momentos, la única disponible es la versión 1)
mx	Cuando se incluye, los servidores de correo entrante del dominio (MX) también tendrán autorización para enviar correo con ese dominio
a:<*dominio*>	Solo debe incluirse si, aparte de los servidores de correo, hubiera otros sistemas con autorización para enviar correo con el domino
include: <*dominio externo*>	Todo lo que el dominio externo indicado (de confianza) tome como legítimo será considerado legítimo para el dominio de la organización
ipv4: ipv6:	Solo deben usarse cuando únicamente haya disponibles direcciones IP

Etiquetas SPF (y II)

ptr

- Utiliza el registro PTR (puntero) de la IP de origen y una consulta de mapeo inverso

exists

- Habrá validación SPF siempre y cuando exista el dominio en cuestión (un registro A válido)

redirect

- Redirige el proceso de verificación para que utilice los registros SPF del dominio en cuestión

exp

- Define un nombre de DNS cuyo registro de texto pueda retornarse con los mensajes de error
- Debe ir al final de la configuración

Expresiones macro: complicadas y poco claras

La etiqueta ‘*all*’

- **-all (bloqueo estricto en caso de validación fallida)**
  - Solo podrán enviar correo con el dominio en cuestión los servidores asociados a este (y aquellos incluidos en las secciones ‘a’ e ‘include’). El resto de servidores serán bloqueados.
- **~all (bloqueo parcial en caso de validación fallida)**
  - Se aceptarán mensajes procedentes de servidores no incluidos en la configuración, aunque con una marca de validación fallida.
- **?all**
  - Marca explícita de la ausencia de reacción ante una validación fallida.
- **+all**
  - Cualquier host puede enviar correo con el dominio en cuestión **(no utilizar nunca)**.

Ejemplos de registros SPF

- v=spf1 mx include:_spf.google.com -all
- v=spf1 mx include:spf.protection.outlook.com –all
- v=spf1 include:spf.protection.outlook.com ip4:161.11.10.20 –all

¿Qué se necesita para activar SPF?

- Tener acceso al DNS público de la organización
- Saber si hay registros MX en uso
- Conocer la dirección IP o los dominios de los sistemas que envíen correo en nombre de la organización
- En caso de que los servicios de correo externalizados acepten SPF...
  - averiguar en qué medida se ve afectada nuestra configuración SPF
- Confirmar la alineación SPF (comprobar que se esté utilizando el dominio de la organización para el envío de correo)

Alineación SPF

Correcta:

From: info@globalcyberalliance.org

Return-Path: <info@globalcyberalliance.org>

Received-SPF: pass (google.com: domain of info@globalcyberalliance.org designates 2607:f8b0:4864:20::d34 as permitted sender) client-ip=2607:f8b0:4864:20::d34;

Fallida:

From: info@globalcyberalliance.org

Return-Path: < bounce-mc.us15_71628198.660451-8bd9e9bfe7@mail58.atl11.rsgsv.net >

Received-SPF: pass (google.com: domain of bounce-mc.us15_71628198.660451-8bd9e9bfe7@mail58.atl11.rsgsv.net designates 205.201.133.58 as permitted sender) client-ip=205.201.133.58;

Para que la alineación SPF sea correcta, el dominio del encabezado de remitente (From:) debe ser el mismo utilizado para la validación SPF (dominios de 'From:' y 'Return-Path' en el ejemplo).

Alineación SPF

SPF DMARC	SPF solo	SPF Dominio
no alineado	valida	mail95.suw111.mcdlv.net
no alineado	valida	mail95.suw111.mcdlv.net

SPF DMARC	SPF solo	SPF Dominio
alineado	valida	globalcyberalliance.org
alineado	valida	globalcyberalliance.org
alineado	valida	globalcyberalliance.org
alineado	valida	globalcyberalliance.org
alineado	valida	globalcyberalliance.org
alineado	valida	globalcyberalliance.org
alineado	valida	globalcyberalliance.org
alineado	valida	globalcyberalliance.org
alineado	valida	globalcyberalliance.org
alineado	valida	globalcyberalliance.org

Inconvenientes

- La decisión sobre qué hacer con los mensajes fallidos recae en el servidor de destino
- Una vez en marcha, no hay forma de saber si un mensaje ha sido rechazado o devuelto
- Si se usa de forma aislada, no se puede evitar que los dominios alojados en un mismo servicio de hosting puedan suplantarse entre sí
- Consultas limitadas a un máximo de 10 dominios
- La validación del dominio de envío no se hace en el encabezado (‘header from’) sino en el sobre remitente (‘envelope from’)

Formas de sortear el límite de 10 consultas

- Evitar los nombres de dominio
  - Y usar la dirección IP en su lugar
  - Muchísimo cuidado con esta opción
- Recurrir al SPF dinámico
  - Mecanismo ofrecido por varios proveedores de DMARC
  - Utiliza macros
- Dedicar subdominios exclusivamente a los flujos de correo electrónico
- Eliminar las declaraciones ‘include’ que no sean necesarias

SPF 2.0

- Sin Sender Policy Framework
- **Es Sender ID**
  - es un protocolo obsoleto e independiente
  - diseñado para mejorar el SPF
- Diferencia
  - Que esta siendo validado
    - SPF 2.0 comprueba PRA y / o MFROM
    - SPF comprueba las identidades MAIL FROM y HELO
  - Cada uno trabaja en diferentes "capas" del sistema de mensajería

DKIM
(DomainKeys Identified Mail, correo identificado por DomainKeys)

DKIM

Correo identificado por DomainKeys

Valida la identidad de un dominio asociado a un mensaje de correo electrónico mediante un proceso de autenticación por firma digital

En el registro de texto (TXT) o CNAME del DNS

- Puede haber más de un registro

Generación de claves DKIM

- Dos claves:
  - Privada
  - Pública
- Condicionantes para la generación de claves:
  - Uso de un servicio externo para tanto el correo como el DNS (por ejemplo, G Suite o 0365)
  - Uso de un servidor propio de correo o una pasarela

DKIM con proveedores externos de correo y sistemas de marketing

- El proveedor externo deberá proporcionar la clave pública, que quedará publicada como registro TXT o CNAME en el DNS
  - En algunos casos, el proveedor podría proporcionar el registro TXT completo
- La clave privada queda bajo custodia del proveedor externo, que rara vez la comparte con sus clientes

DKIM en organizaciones con servidor de correo o pasarela

- Algunas pasarelas de correo generan las claves DKIM (por ejemplo, Cisco Ironport y Mimecast)
- En Linux, existe un proyecto de código abierto llamado **opendkim** (http://www.opendkim.org/):
  - Incluye varias herramientas para ayudar en la creación de las claves y en la integración de las firmas DKIM en distintos sistemas de correo electrónico
- MS Exchange: dkim-exchange (GitHub)
- Otra opción es utilizar OpenSSL para generar las claves DKIM:
  - Privada: **openssl genrsa -out dkim-private.pem 1024 -outform PEM**
  - Pública: **openssl rsa -in dkim-private.pem -out dkim-public.pem -pubout -outform PEM**
- Una vez creada, la clave DKIM privada deberá moverse a la ubicación que se especifique en la instalación DKIM:
  - **Comprobar siempre que la ubicación se encuentra en una carpeta con acceso restringido**

Registro de texto en el DNS para DKIM

Nombre: <selector>._domainkey.<*domain*>

Valor: "k=rsa;
p=MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAKJ2lzDLZ8XlVambQfMXn
3LRGKOD5o6l;"

Registro de nombre para DKIM

- **<selector>**
  - Nombre de la clave DKIM en el DNS
  - Antes de “.”, puede usarse cualquier nombre, aunque poniendo siempre “_domainkey” después
- **_domainkey: obligatorio**
- **<*dominio*>:** no siempre hace falta

Etiquetas DKIM

- **k=rsa:** define el algoritmo de generación de claves utilizado
- **p=<*cadena de clave contenida en un archivo de clave pública generado previamente*>:** define la cadena de la clave pública
  - 1024: tamaño más habitual
  - 2048*

¿Qué se necesita para activar DKIM?

- Tener acceso al DNS público de la organización
- Definir el selector
- Tener un generador de claves DKIM y una herramienta de firma digital
  - Incorporados al servidor de correo electrónico o a la pasarela de seguridad
  - Proporcionados por un proveedor externo
- En caso de que los servicios de correo externalizados acepten SPF...
  - averiguar que es necesario añadir al DNS (registro TXT o CNAME)
- Confirmar la alineación DKIM (comprobar que el servidor de la firma digital esté utilizando el dominio de la organización)

Alineación DKIM

Encabezado del mensaje:

De: info@globalcyberalliance.org

Firma DKIM: v=1; a=rsa-sha256; c=relaxed/relaxed; d=globalcyberalliance.org; s=gca; h=mime-version:references:in-reply-to:from:date:message-id:subject:to:cc;

DKIM DMARC	DKIM solo	DKIM d=
alineado	valida	globalcyberalliance.org
no alineado	valida	mail9.mcsignup.com
alineado	valida	globalcyberalliance.org
alineado	valida	globalcyberalliance.org
alineado	valida	globalcyberalliance.org
no alineado	valida	mail13.mcsignup.com
no alineado	valida	mail8.mcsignup.com
no alineado	valida	gmail.mctxapp.net
no alineado	valida	mail10.mcsignup.com
no alineado	valida	gmail.mctxapp.net

Inconvenientes

- No define qué hacer con la firma, ya sea válida o no
- No incorpora ningún mecanismo de generación de informes
- No permite determinar si el servidor de un remitente tiene permiso para enviar correo de un dominio concreto
- Permite que los filtros de los destinatarios puedan determinar la autenticidad de los mensajes enviados
  - El servidor de destino deberá decidir qué hacer con los mensajes fallidos

DMARC

Domain-based **M**essage **A**uthentication, **R**eporting, & **C**onformance*

Política de autenticación de mensajes mediante SPF y DKIM (la **M** y la **A** de DMARC) integrada con la regla de conformidad definida por la organización (la **C**) y con una función de generación de informes o *reportes* (la **R**).

La política queda definida por el nombre de dominio o DNS (la **D**).

*Autenticación de mensajes, informes y conformidad basada en dominios

DMARC respecto a SPF y DKIM

- Resuelve la mayoría de problemas de SPF y DKIM
- SPF y DKIM deberán implementarse tanto en dominios que compartan servicios de hosting como que utilicen servidores de correo propios
  - DMARC se servirá de la validación de SPF y DKIM
- Permite generar informes
- Indica qué hacer con los mensajes que pasen o no pasen la validación

Recursos disponibles

- Foro de la comunidad de la GCA: community.globalcyberalliance.org

- Recursos de DMARC de la GCA: dmarc.globalcyberalliance.org/dmarc-bootcamp/

¿Preguntas?

¡Gracias!

Shehzad Mirza
gca-dmarc@globalcyberalliance.org
smirza@globalcyberalliance.org