Email Spoofing: un enfoque técnico-jurídico

Margarita Robles Carrillo
Network Engineering and Security Group (NESG)
Universidad de Granada
mrobles@ugr.es

Marc Almeida Ros
Analista técnico/Director
Domain Hunter DMARC Edition
marc@cibernicola.es

***Resumen*—El análisis del email spoofing desde una doble perspectiva técnica y jurídica se realiza exponiendo, en primer lugar, la problemática que plantea esta modalidad de ciberataque sobre la base de la experimentación realizada analizando la aplicación de los protocolos SPF, DKIM y DMARC. En segundo lugar, se aborda el marco teórico de comprensión del email spoofing con el doble objetivo de conocer su naturaleza y caracteres y de explicar las medidas de protección diseñadas frente al mismo y las obligaciones y responsabilidades de los distintos sujetos implicados en su aplicación: diseñadores, proveedores de servicios y usuarios. En tercer lugar, se consideran las soluciones arbitradas frente a esta práctica en el plano doctrinal para, finalmente, formular unas propuestas de solución desde un enfoque técnico y jurídico.**

***Index Terms*—spoofing, dominios, seguridad, tecnología, derecho**

I. Introducción

La suplantación de correo electrónico, conocida como email spoofing, es una práctica maliciosa que, a pesar de las distintas medidas de seguridad articuladas para combatirla, muestra no solo *un crecimiento exponencial* sino, también, una *diversificación funcional y teleológica*, que complica adicionalmente la lucha contra este tipo de ciberataque. La definición de protocolos de seguridad específicos para la configuración segura de las comunicaciones por correo electrónico, en particular SPF, DKIM y DMARC, no ha servido realmente para resolver el problema porque no se ha traducido en una reducción de este tipo de incidentes, como demuestra el estudio realizado sobre la realidad del email spoofing (Sección II).

Para explicar esta situación, se analiza el *marco conceptual y funcional* del spoofing (Sección III) que permite identificar los tres motivos principales que conducen a la misma: 1) La no utilización de los protocolos [1]; 2) La inadecuada implementación de los mismos [2]; y 3) Las propias deficiencias o carencias de esos estándares de seguridad [3]. El *análisis del estado del arte y las soluciones* propuestas para combatir el email spoofing (Sección IV) difieren en cuanto al impacto de cada uno de esos parámetros, pero coinciden en su naturaleza técnica. En la práctica, estas tres variables que se utilizan para explicar la problemática de los protocolos SPF, DKIM y DMARC no necesariamente actúan de modo individual o por separado, sino que interaccionan y se retroalimentan entre ellas. Los aspectos defectuosos de los protocolos justificarían tanto su falta de uso como su incorrecta aplicación. A su vez, los problemas detectados en su implementación podrían estar evidenciando disfunciones en el propio modelo de seguridad diseñado y explicarían su limitado uso. Finalmente, la escasa utilización de los protocolos podría deberse a la constatación de los defectos en su configuración o a los problemas planteados en su aplicación.

Desde un punto de vista metodológico, la posibilidad de dar prioridad a una variable concreta de análisis -la configuración de los dominios y/o la implementación incorrecta o inadecuada de los protocolos de seguridad- se justifica por dos razones principales: por una parte, la pertinencia y el valor de un estudio práctico basado en la experimentación; y, por otra, la exclusión, por su carácter limitado y parcial, de un trabajo de corte fundamentalmente teórico -como el que requeriría la tercera de las variables- o principalmente estadístico -como exigiría la primera de ellas-. Siguiendo la propuesta de métodos de análisis de protocolos de Zhou y Chin, basada en la distinción entre comprobación de teoremas y de modelos, se aplica la segunda opción [4].

La metodología consistente en el análisis de la configuración de los dominios y la implementación de los protocolos de seguridad ofrece datos sobre la segunda de las variables que pueden llevar a resultados independientes de las otras dos porque se trata de valorar el nivel de aplicación de esos estándares y se puede concluir con datos válidos por sí mismos relativos únicamente a ese extremo. Esos datos pueden arrojar, asimismo, algunas conclusiones sobre los dos otros aspectos, pero admiten un análisis independiente desde el punto de vista técnico y jurídico.

El objetivo de este trabajo es analizar la problemática que plantea el email spoofing, mediante un enfoque integral técnico-jurídico, a partir de los datos que ofrece el análisis de la práctica tanto por zonas geográficas como por parte de responsables de la configuración de dominios y de los proveedores de correo (II). Sobre esa base, se estudia el marco conceptual y funcional de comprensión de esta modalidad de ciberataque (III), así como las soluciones doctrinales aportados con propuestas de naturaleza técnica (IV). A lo largo del trabajo y en las conclusiones se argumenta sobre la necesidad de una solución combinada técnico-jurídica.

II. La Realidad del Email Spoofing

Para explicar la realidad del spoofing se ha realizado un estudio basado en un trabajo de campo mediante la recopilación masiva de configuraciones de dominio. Para ello se ha utilizado una herramienta de recopilación, un script de código abierto, que se ha modificado para añadirle la funcionalidad de gestión necesaria para ese amplio volumen de datos. Los resultados se han volcado a Elastic Search mediante la herramienta Logstash y las visualizaciones de trabajo con Kibana (ELK).

El estudio se basa en el análisis de implementación de SPF y DMARC, puesto que DKIM puede alojarse en un campo (DKIM Selectors) con valor variable lo que elevaría la complejidad del análisis de forma drástica. Los parámetros de

validez de los protocolos SPF y DMARC son, básicamente, dos. El primero es que la configuración no contenga ningún error tipográfico (comas dobles, campos inexistentes, campos duplicados, etc.). El segundo es que dichos parámetros se sitúen dentro de los márgenes aconsejados por la IETF.

A 16 de febrero de 2021, el estudio comprende 235 millones de dominios. Los dominios que se excluyen del análisis son aquellos que, por algún motivo, no han dado respuesta en el tiempo estipulado al leer los campos SPF y/o DMARC o, en su defecto, no están disponibles en el momento del escaneo. El total de dominios no accesibles asciende a 12.856.514 en el primer caso y 12.947.859 en el segundo. Es interesante observar una casuística concreta en la que el dominio no presenta registros MX. Puede considerarse que se trata de dominios aparcados, es decir, sin contenido y, en muchas ocasiones, mantenidos para su re-venta, dominios sin servicio de correo electrónico o dominios que envían correo electrónico pero que no pretenden recibirlo, lo que puede dar una falsa sensación de seguridad puesto que el no uso del servicio no impide que se pueda suplantar la identidad del dominio. Es destacable que del total de dominios analizados, 89.063.371 están configurados de esta forma. Entre ellos, solo 7.019.520 tienen el protocolo SPF válido y únicamente 1.219.862 DMARC. Afinando algo más, 1.121.436 cuentan con la política REJECT en DMARC y una configuración SPF estricta (SPF-all).

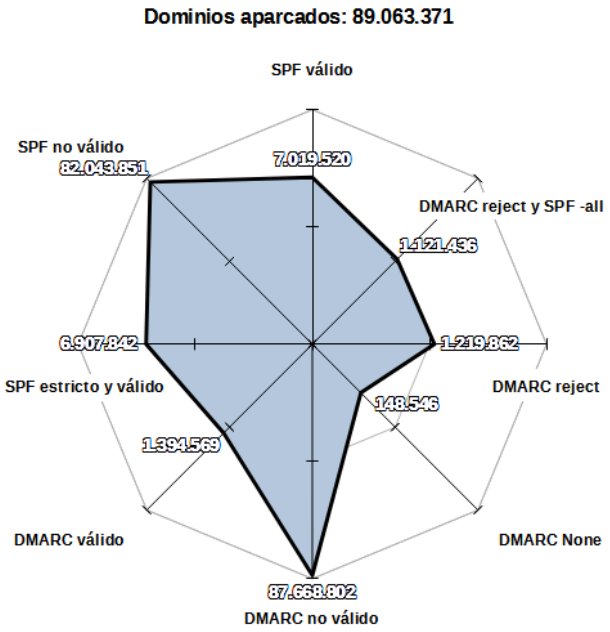

Figura 1. Dominios aparcados

Teniendo en cuenta las características de este tipo de dominios, la configuración óptima es SPF (-all) y DMARC (reject) estrictos. Pero, como se puede observar en la Figura 1, de los 89 millones, 82 tienen mal configurado o carecen de SPF y cerca de 88 carecen de una configuración DMARC adecuada. Estos datos, en su totalidad, indican que el uso de dominios en Internet bajo estas premisas tiende a ser desatendido casi en su totalidad en lo referente a un mínimo de medidas de seguridad.

El análisis global de los dominios, una vez excluidos esos supuestos específicos, se ha desarrollado sobre dos campos de estudio. El primero, de *naturaleza geográfica*, permite observar la cantidad total de dominios, así como su configuración distinguiendo entre diversas categorías de mayor a menor -o ningún- grado de protección, esto es: 1) Dominios con DMARC+SPF; 2) Dominios con DMARC; 3) Dominios con SPF; 4) Dominios sin DMARC válido; y 5) Dominios sin SPF válido.

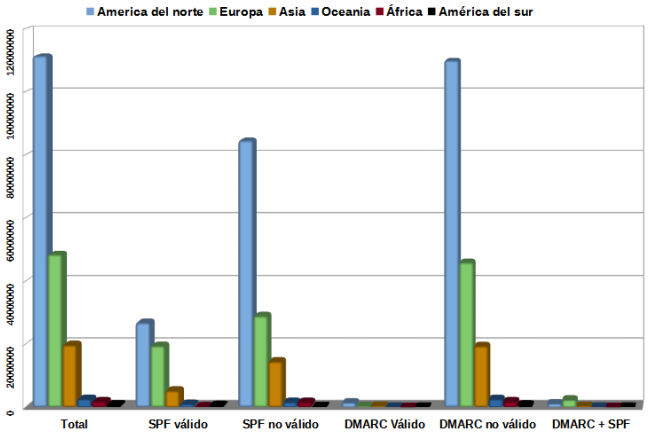

Figura 2. Áreas geográficas

En la figura 2 se puede comprobar el resultado donde cabría destacar los dos parámetros extremos: por una parte, América del Norte combina el mayor número de dominios con el menor grado de implementación de los protocolos; y, por otra parte, en el polo opuesto, América del Sur representa el menor número de dominios con el mayor porcentaje de aplicación de los protocolos.

El segundo de los campos de estudio atiende a los *proveedores de servicios*. Por las limitaciones de espacio, que impiden una panorámica más amplia y exhaustiva, se han seleccionado dos de ellos: de un lado, el que mayor cantidad de dominios aloja (GoDaddy Figura 3); y, por otro, aquel a cuyos usuarios se suele reconocer un mayor grado de conocimiento y de concienciación en materia de seguridad (Cloudflare Figura 4). Ello permite combinar un criterio cuantitativo y otro de orden cualitativo.

Los resultados de ambos análisis permiten observar, con carácter general, una implementación extraordinariamente baja de los protocolos a lo que se suma un porcentaje significativo de configuración errónea de los parámetros establecidos en dichos protocolos. De hecho, hay estudios científicos que demuestran la existencia de una brecha preocupante entre la detección de spoofing de correo electrónico del lado del servidor y la protección real de los usuarios [6]. Para apreciar mejor la situación y abordar las posibles soluciones, hay que explicar el marco conceptual y funcional del email spoofing.

III. Marco Conceptual y Funcional

El estudio del marco conceptual y funcional del email spoofing tiene un triple objetivo: 1) Definir y caracterizar esta actividad; 2) Identificar las medidas de protección diseñadas para combatirla; y 3) Delimitar las funciones y obligaciones

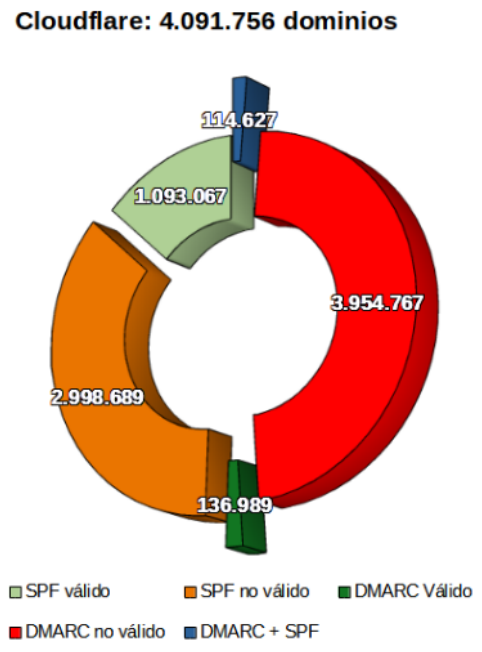

Figura 3. Proveedores de hosting, Cloudflare

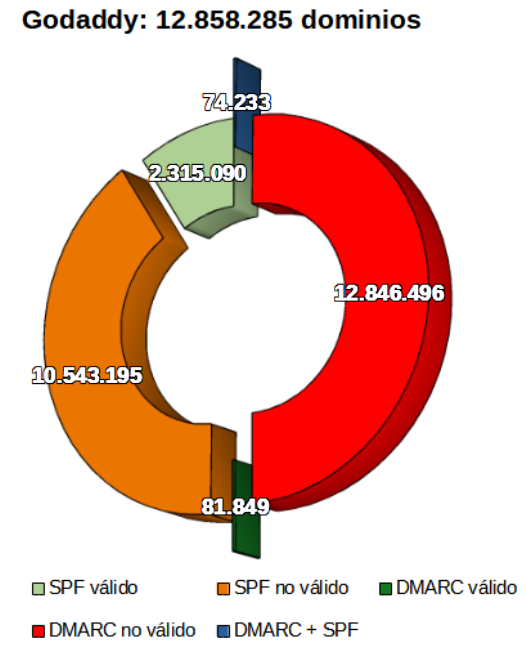

Figura 4. Proveedores de hosting, Godaddy

de los distintos sujetos implicados en ella, en particular, configuradores de dominios y proveedores de servicios.

III-A. Conceptos y categorías

El email spoofing exige una delimitación conceptual desde una doble perspectiva para distinguirlo de otras modalidades de spoofing y para diferenciarlo de otras figuras afines.

El spoofing es un concepto que se identifica genéricamente con una suplantación de identidad. Esta práctica puede tener diversos objetivos: la IP, el DNS, un GPS, una web, la ARP o el correo electrónico, entre otros. El núcleo común es la idea de suplantación, pero los procedimientos, los objetivos y los resultados son diferentes en cada caso [7].

El spoofing debe distinguirse conceptualmente, por otra parte, de otras figuras afines como el *hijacking*, el *spear phishing* o el *Business Email Compromise* (BEC) [8] [9] [5]. El spoofing es una modalidad de ciberataque de naturaleza básicamente instrumental, porque no suele ser un fin por sí mismo sino un medio para conseguir otras finalidades que pueden, a su vez, ser diversas. En los otros casos, el principal elemento definitorio es su finalidad.

Los parámetros de victimización característicos del spoofing difieren asimismo de lo que suele ser habitual porque, en este supuesto, tanto el dominio receptor del correo como el dominio remitente, que ha sido suplantado, son víctimas con la agravante de que resulta más complicado tener conocimiento de la existencia de esa suplantación. En condiciones normales, el titular del dominio suplantado no sabrá que se ha producido la suplantación de su dominio salvo que y hasta que el receptor, sospechando sobre el correo, proceda a comunicarlo al titular del dominio objeto de spoofing. Ello explica la especial importancia de articular medidas de prevención y protección.

III-B. Medidas de Protección frente al Email Spoofing

La necesidad de garantizar la seguridad de las comunicaciones realizadas a través del correo electrónico ha justificado la adopción de distintos protocolos dirigidos a su protección, así como, en general, a la adopción de contramedidas para detectar y rechazar correos no deseados. Entre ellas se incluyen mecanismos de autenticación, listas negras o el filtrado de spam basado en el contenido [10].

El *Simple Mail Transfer Protocol* (SMTP) no contempla originariamente medidas de seguridad frente a la suplantación de identidad [11]. Por ello se proponen protocolos de extensión de SMTP, que han sido publicados y normalizados por el Grupo de Tareas de Ingeniería de Internet (*Internet Engineering Task Force*: IETF) [12]. Los principales son SPF, DKIM y DMARC.

El SPF (*Sender Policy Framework*), propuesto en 2000 y estandarizado en 2014 (RFC 7208), permite al dominio determinar las IP autorizadas a enviar correo en su nombre. Por su parte, DKIM (Domain Keys Identified Mail),propuesto en 2004 y estandarizado en 2011 (RFC 6376), consiste en el uso de claves públicas para autenticar el remitente del correo electrónico y comprobar la integridad del mismo. Finalmente, DMARC (*Domain-based Message Authentication, Reporting and Conformance*), propuesto en 2011 y publicado en 2015 (RF 7489), no es un protocolo autónomo, sino que necesita trabajar con SPF y/o DKIM. DMARC diseña un procedimiento escalable mediante el cual el sujeto de origen de correo puede expresar políticas y preferencias a nivel de dominio para la validación, disposición y notificación de mensajes, que el receptor puede, a su vez, utilizar para mejorar el manejo del mismo. Permite publicar una ”política de fallos”, donde especifica qué acciones debe tomar el receptor cuando el correo electrónico entrante no supera sus comprobaciones [8]. Entre los 10 proyectos de seguridad más importantes de Gartner para 2020-2021 se incluye DMARC que, aunque no resuelve todos los problemas de seguridad del correo electrónico, es una pieza importante dentro de un enfoque de seguridad holístico [13]. Hay también una versión DMARC Box propuesta por la doctrina [14].

Open PGP (*Pretty Good Privacy*) y S/MIME (*Secure Multipurpose Internet Mail Extensions*) son los dos principales estándares para encriptar y firmar digitalmente correos electrónicos proporcionando autenticidad de extremo a extremo de los mensajes mediante firmas digitales [15]. Estos protocolos garantizan la seguridad de la transmisión. Pero no impiden la suplantación de identidad, ni son una garantía frente a los ataques de falsificación [16] [9]. La principal desventaja del despliegue de aplicaciones que utilizan la PKC es la distribución de claves públicas con una vinculación legítima con su propietario [17]. Por su parte, los protocolos BIMI (*Brand Indicators for Message Identification*) y ARC (*Authenticated Received Chain*) son recientes, pero BIMI se construye sobre DMARC y ARC sobre SPF, DKIM y DMARC. Ambos dependen de la verificación de DMARC [18].

En definitiva, en el ámbito del email spoofing, SPF, DKIM y DMARC son los protocolos operativos cuya aplicación, sin embargo, como se ha visto en la sección II, resulta problemática. Gran parte de esta situación se debe a la actuación de los distintos sujetos implicados en la prestación de servicios de correo electrónico.

III-C. Funciones y obligaciones

En la experimentación sobre la configuración de dominios y la aplicación de los protocolos es esencial identificar las atribuciones y responsabilidades de los distintos sujetos que intervienen en el proceso. Ello incluye, de modo principal, a los propios diseñadores de los protocolos, en particular, el IETF, los proveedores de servicios y los usuarios [3].

En relación con los usuarios, hay que distinguir dos posibles situaciones. Si son los propios configuradores de su dominio, en caso de spoofing, podrían tener una responsabilidad derivada de la incorrecta o insegura configuración. Pero, respecto del resto de los usuarios, que no interviene en la configuración de su dominio, normalmente la mayoría, la cuestión se plantea en otros términos. Es cierto que sería deseable una mayor concienciación e implicación [2], porque las protecciones a nivel de usuario pueden ser muy eficaces [6]. Pero hay dos datos que pueden servir para minimizar o excluir la responsabilidad del usuario básico: por una parte, el desconocimiento sobre el funcionamiento de estos servicios, sus requerimientos técnicos y de seguridad, que caracteriza a la gran mayoría de los usuarios; y, por otra parte, el hecho de que, como clientes del servicio, pueden legítimamente aspirar a recibir unas prestaciones seguras de correo [2], sin tener que aportar por sí mismos o asumir deberes específicos en materia de seguridad.

En el caso de los diseñadores, hay evidentemente un alto grado de responsabilidad en sentido genérico, por ser los autores de los protocolos de seguridad, pero ello no implica una responsabilidad en sentido jurídico por dos motivos: por un lado, no son una autoridad pública o una entidad privada con una personalidad jurídica que permita hacerlos jurídicamente responsables de las carencias de los protocolos; y, por otro lado, los protocolos son estándares carentes de obligatoriedad que se aplican de forma voluntaria [6], esto es, mediando un consentimiento, implícito o explícito, del proveedor o del usuario que limita la posibilidad de trasladar la responsabilidad a los creadores del protocolo. A ello se suma el hecho de que, por su posición y sus funciones, tienen menos posibilidades de identificar las cuestiones prácticas que plantea la configuración de un dominio o la aplicación de los protocolos de seguridad.

Por ello, en principio, la mayor responsabilidad recae sobre los configuradores de dominios y los proveedores de servicios de correo como consecuencia de la función que cumplen en el diseño del dominio y en la aplicación de los protocolos y, en particular, porque las distintas modalidades de configuración y de implementación, usadas por cada uno de ellos, tienen consecuencias mayores de las que cabría esperar.

III-D. Responsabilidades de los Proveedores de Servicios

Los estudios realizados han demostrado que, incluso fallando la autenticación, muchos proveedores de correo electrónico optan por entregar un correo electrónico falsificado en la bandeja de entrada sin, ni siquiera, aplicar algún mecanismo de alerta para notificar a los usuarios [6]. Cuando ello ocurre, cabría la opción de habilitar medidas de protección por parte de los usuarios, pero esta garantía adicional no puede sustituir, ni desplazar, la obligación principal de los configuradores de dominio y de los servidores de correo de ofrecer sus servicios cumpliendo los requisitos de seguridad

Los proveedores de servicios de Internet (ISP) han de desarrollar su actividad cumpliendo con la normativa en vigor, en general y respecto de cada ámbito de actuación, en particular, en materia de seguridad de redes y sistemas de información y de comunicaciones. Pero, los Protocolos SPF, DKIM y DMARC están recogidos en *Request for Comment* (RFC) que son una serie de monográficos que utiliza el IETF para publicar sus directrices o recomendaciones de actuación sobre los aspectos técnicos del funcionamiento de Internet. La cuestión estriba en que ni los protocolos contienen reglas obligatorias, ni el IETF es una entidad con autoridad para imponerlas. Ello implica que la aplicación de los protocolos depende de la voluntad de los prestadores de servicios -configuradores de dominios o servidores de correo-, que tienen la capacidad de decidir si los aplican o no y cómo lo hacen. No cabe, en principio, la posibilidad de exigirles jurídicamente el cumplimiento de los protocolos.

El problema de fondo estriba en la combinación de esa doble circunstancia. Por una parte, no es obligatorio *per se* cumplir lo dispuesto en estos protocolos donde se establecen requisitos y procedimientos para garantizar técnicamente la seguridad en la configuración de los dominios y en la prestación de servicios de correo electrónico. Pero, por otra parte, los ISP están *obligados* por la normativa en vigor que establece reglas vinculantes y precisas en materia de seguridad en relación con el desempeño de su actividad y respecto de sus atribuciones, deberes y responsabilidades. La pregunta es: ¿cómo se pueden cumplir esas reglas jurídicas obligatorias en materia de seguridad si no se aplican las medidas técnicas voluntarias dirigidas a garantizar la seguridad?

Hay varias respuestas posibles. Una primera sería mantener el *statu quo* apelando a y confiando en el buen hacer de los ISP y, en su caso, arbitrando mecanismos de protección adicionales por parte de los usuarios. Una segunda opción podría ser convertir los estándares técnicos en obligaciones jurídicas, esto es, transformando los protocolos en normas. Esta alternativa parece poco viable tanto por la dificultad

de trasladar los requisitos técnicos en disposiciones jurídicas como, sobre todo, por la práctica imposibilidad de atribuir al IETF una autoridad -y la necesaria legitimidad- para dictar preceptos obligatorios con carácter general. Una tercera posibilidad sería adoptar una norma jurídica como las que se han adoptado en otras materias, por ejemplo, datos o seguridad de redes y sistemas. Es una opción, pero a medio o largo plazo por los problemas competenciales y técnicos que plantea su regulación y porque, a pesar de la gravedad de la situación, ni siquiera se visibiliza por el momento su necesidad. Una cuarta y posible opción, con carácter inmediato, consistiría en integrar los requerimientos técnicos de seguridad dentro del concepto de seguridad en sentido jurídico. Esta solución tendría la ventaja adicional de la inmediatez y la simplicidad porque, sin cambios en la dinámica de los protocolos, ni en el derecho en vigor, permitiría resolver el problema mediante la fórmula de la interpretación normativa, esto es: interpretar el cumplimiento de los requisitos de seguridad estipulados jurídicamente atendiendo a los requisitos establecidos en los estándares técnicos.

Hay una enorme diferencia entre la ausencia de valor jurídico, la obligatoriedad jurídica y la integración de los estándares técnicos como criterio de interpretación y de validación del cumplimiento de las obligaciones jurídicas en materia de seguridad. Por esta vía se conseguiría, además y en particular, coadyuvar al cumplimiento voluntario de los protocolos por parte de los ISP. En caso de incumplimiento, intervendría la garantía y la sanción jurídica.

Esta solución técnico-jurídica resultaría más efectiva que una respuesta jurídica al margen de los aspectos técnicos o que una respuesta exclusivamente técnica carente de la garantía última que supone el recurso al derecho. Hasta ahora, sin embargo, el derecho ha estado ausente de las propuestas doctrinales para combatir el email spoofing.

IV. Análisis y Soluciones sobre el Spoofing

Los estudios científicos realizados sobre spoofing se centran en aspectos concretos como el análisis de *emails headers* [19] o abordan todos los componentes del email [18]. En algunos casos se realizan desde la perspectiva de la eficacia de las protecciones a nivel de usuario [3], la articulación de técnicas para detectar e informar al usuario remitente cuyo email ha sido objeto de spoofing [11] o el diseño de aplicaciones de correo [17], bien de control activo del spoofing mediante una alerta y un filtro específico [20] o bien con una aplicación anti-spoofing basada en el protocolo SSL (*Secure Socket Layer*) orientada al cliente [21]. Hay también propuestas basadas en el uso de las huellas dactilares para autenticar a los usuarios y proporcionarles un proceso transparente de firma y verificación de los mensajes de correo electrónico [17]. El recurso a técnicas de autenticación biométrica no está, sin embargo, exento de controversia.

La implementación de los protocolos SPF, DKIM [15] y DMARC plantea una serie de problemas que han sido identificados por la doctrina [11] [18]. En el estudio realizado por Chen *et ali*, se analizan los casos de 10 proveedores y 19 usuarios, respecto de tres modalidades de ataque con el resultado de que solo 6 proveedores se han visto afectados por ataques *intra-server*, mientras que todos ellos han sido víctimas de ataques tipo *UI-mismatch* y *ambiguous-replay*. Chen *et ali* concluyen que los ataques de spoofing tienen en común un alto nivel de incoherencia entre los componentes del software que se debe a tres factores principales: 1) los protocolos definen múltiples identidades de remitente, dejando espacio para interpretaciones erróneas en la implementación; 2) los protocolos están basados en textos con sintaxis compleja que pueden dar lugar a una variedad de incoherencias; y 3) el proceso de autenticación del remitente implica una cadena de componentes con una fuerte dependencia en la aplicación [18]. Aunque la respuesta de los proveedores a su estudio es muy variada, solo Microsoft excluye que se trate de una vulnerabilidad -porque atribuye la amenaza a un problema de ingeniería social- y Yahoo.com considera que es un tema de mala configuración del DNS [18]. La dependencia del DNS es para algunos un importante vector de ataque [2].

El estudio realizado por Foster *et ali* se centra en los principales proveedores y servicios como el comercio online o las redes sociales aplicando una metodología con dos instrumentos de medición: los que pueden automatizarse y escalarse fácilmente y los que requieren cierta interacción manual. Para los autores, el uso de TLS con IMAP, POP y SMTP proporciona la confidencialidad de los mensajes incluso en presencia de un adversario activo, mientras que DKIM con DNSSEC garantiza la autenticidad e integridad. Estas garantías exigen confiar en el proveedor de correo electrónico. Los mecanismos de extremo a extremo no requieren esa confianza, pero la adopción por parte del usuario de PGP y S/MIME es deficiente. Por ello, los protocolos SPF y DKIM proporcionan una solución para lograr esos objetivos de seguridad.

Hang Hu *et ali* realizan un análisis cualitativo sobre la escasa implementación de los protocolos que atribuyen, básicamente a sus carencias técnicas de las que son conocedores los proveedores. Esos defectos técnicos son tres: SPF y DKIM comparten el problema del *identifier alignment*; SPF plantea dificultades con el reenvío de correo; y la lista de correo es un asunto complicado tanto para SPF como para DKIM. Para los autores, los protocolos son útiles pero insuficientes para resolver el tema del email spoofing [3].

En su estudio titulado “End-to-End Measurements of Email Spoofing Attacks”, sobre los 35 principales proveedores, Hu y Wang llegan a tres conclusiones: 1) la mayoría de los proveedores tienen los protocolos necesarios para detectar la suplantación de identidad, pero permiten que los correos falsificados lleguen a la bandeja de entrada del usuario (por ejemplo, Yahoo Mail, iCloud, Gmail); 2) Una vez que ese correo llega a la bandeja de entrada, la mayoría de los proveedores no avisa a los usuarios e, incluso, algunos (por ejemplo, la bandeja de entrada de Gmail) tienen una interfaz de usuario engañosa que hace que dicho correo parezca auténtico; 3) Solo unos pocos proveedores (9/35) implementan indicadores visuales de seguridad en los correos electrónicos no verificados [22].

Tras un trabajo publicado en 2020 con los 500 principales dominios de 139 países, Maroofi *et ali* concluyen que gran parte de los dominios no configura correctamente las reglas SPF y DMARC, lo que permite entregar con éxito correos falsos en las bandejas de entrada de los usuarios [23].

V. Conclusiones

Desde las propuestas de solución realizadas por Zhou y Chin en 1999 [4], la doctrina ha planteado diferentes opciones para combatir el email spoofing: el uso de sistemas automáticos de detección [3]; el diseño de aplicaciones de correo de control activo del spoofing mediante un alerta y un filtro específico [20] o de una aplicación anti-spoofing basada en el protocolo SSL [21]; un software de alerta de anomalías en el código fuente [1]; el recurso a tarjetas inteligentes de verificación de remitentes de correo [9]; la opción de seguridad en la nube mediante DMARCBox [14]; o la inscripción de la huella digital del usuario en un registro único para autenticar, firmar y verificar los correos [17]. No son muchos los autores que se centran en la correcta aplicación de los protocolos y en hacer cumplir una política de seguridad que excluya el correo no conforme a sus parámetros [2]. Aunque aquella variedad de propuestas pueda aportar soluciones, como también el componente adicional de seguridad que pueda adicionar el usuario, ello no excluye la necesidad de habilitar procedimientos generales y públicos de garantía de seguridad en la configuración de los dominios y en la prestación de servicios de correo.

Los protocolos de seguridad son estándares técnicos emanados de instituciones y organismos privados de manera que no son parámetros o normas obligatorias ni tampoco cuentan con la legitimidad jurídica que implica que su autoría corresponda a una autoridad pública. La naturaleza técnica y no jurídica de los protocolos constituye el primer obstáculo para su implementación porque es voluntaria. No se puede exigir, ni se puede imponer, ni se puede sancionar a quienes no aplican o incumplen los protocolos de seguridad. El carácter voluntario de estas medidas es el límite primero y principal en términos de efectividad. No obstante, y a pesar de ello, podría ocurrir que, por vía mediata o indirecta, el cumplimiento de esos protocolos adquiriese un cierto valor jurídico o una relativa obligatoriedad.

La normativa sobre seguridad tiene que ser una obligación, razón por la cual ha de estar establecida en normas jurídicas que permitan exigir y garantizar su cumplimiento. Pero, los estándares técnicos de seguridad no resultan fácilmente subsumibles en el concepto de norma jurídica, por su propia naturaleza técnica, por sus propios contenidos y por su carácter marcadamente evolutivo. Por ello, la posibilidad de que el IETF fuese una entidad autorizada para adoptar normas vinculantes y, en consecuencia, los protocolos fuesen obligatorios, no parece una solución viable. No es previsible, tampoco, a medio plazo, un interés normativo sobre la cuestión. A pesar de la gravedad del problema, no se trata de una prioridad en la agenda de los legisladores. Pero, en cualquier caso, el mantenimiento del *statu quo*, atendiendo a los datos existentes, sería una irresponsabilidad.

La posibilidad, en cambio, de que la obligación de cumplir la normativa jurídica sobre seguridad incluya la implementación de los estándares técnicos definidos en los protocolos parece ser la única opción viable por el momento. La solución ideal sería conciliar esas dos dimensiones identificando los aspectos básicos de seguridad de la implementación técnica como requisitos mínimos de seguridad desde una perspectiva jurídica.

Agradecimientos

Este trabajo se ha realizado en el marco del Proyecto Domain Hunter DMARC edition y del Proyecto de Investigación MDSM del Network Engineering and Security Group. El Proyecto MDSM ha sido financiado parcialmente por el Gobierno de España, con fondos FEDER, a través del proyecto TIN2017-83494-R.

Referencias

1 B. Opazo, D. Whitteker y C.-C. Shing. “Email trouble: Secrets of spoofing, the dangers of social engineering, and how we can help”. 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), pp. 2812-2817, 2017.
2 I. Foster, J. Larson, M. Masich, A.C. Snoeren, S. Savage y K. Levchenko. “Security by Any Other Name: On the Effectiveness of Provider Based Email Security”, 2015 (https://cseweb.ucsd.edu/ klevchen/flmssl-ccs15.pdf).
3 H. Hu, P. Peng y G. Wang. “Towards the Adoption of Anti-spoofing Protocols”, 2017 (https://arxiv.org/pdf/1711.06654.pdf).
4 D. Zhou y S.-K. Chin. “Formal Analysis of a Secure Communication Channel: Secure Core-Email Protocol”, Electrical Engineering and Computer Science, n. 138, 1999. https://surface.syr.edu/cgi/viewcontent.cgi?article=1137&context=eec
5 Cyber Insurance Claims Report.
6 H. Hu y Ga. Wang. “Revisiting Email Spoofing Attacks”, 2018 (https://arxiv.org/abs/1801.00853)
7 S.A.C. Schuckers. “Spoofing and Anti-Spoofing Measures”, Information Security Technical Report, vol. 7, n. 4, pp. 56-62, 2002.
8 S. Nightingale. Email Authentication Mechanisms: DMARC, SPF and DKIM, National Institute of Standards and Technology, USA, 2017.
9 K. Pandove, A. Jindal y R. Kumar. “Email Spoofing”, International Journal of Computer Applications, vol. 5, n. 1, pp. 27-30, 2010.
10 H. Siadati, S. (Tahereh) Jafarikhah y M. Jakobsson: ”Traditional Countermeasures to Unwanted Emails”, 2020 (https://www.researchgate.net/publication/309425892_Traditional_Countermeasures_to_Unwanted_Email).
11 M. Kumar, M. Hanumanthappa y S. Kumar. “A Countermeasure Technique for Email Spoofing”, International Journal of Advanced Research in Computer Science, vol. 4, n. 2, pp. 128-133, 2013.
12 S. Rose, S. Nightingale, S. L. Garfinkel y R. Chandramouli: Trustworthy Email, National Institute of Standards and Technology, USA, 2019.
13 https://www.gartner.com/smarterwithgartner/gartner-top-security-projects-for-2020-2021/
14 T. Nanaware, P. Mohite y R. Patil. ”DMARCBox – Corporate Email Security and Analytics using DMARCÏEEE 5th International Conference for Convergence in Technology (I2CT), Bombay, India, pp. 1-5, 2019.
15 P. García Teodoro y G. Maciá Fernández. Seguridad en redes y sistemas de comunicación. Teoría y práctica, Granada, 2020.
16 J. Müller, M. Brinkmann, D. Poddebniak, H. Böck, S. Schinzel, J. Somorovsky y J. Schwenk. “Johnny, you are fired!” – Spoofing OpenPGP and S/MIME Signatures in Emails”, 2019. https://www.usenix.org/system/files/sec19fall_muller_prepub.pdf.
17 A. S. Zadgaonkar, V.Ch. Pandey y P.S. Pradhan. “Developing a Model to Enhance E-Mail Authentication against E-Mail Address Spoofing using Application”, International Journal of Science and Modern Engineering, vol. 1, n. 6, pp. 3-17, 2013.
18 J. Chen, V. Paxson y J. Jiang. “Composition Skills. A Case Study of Email Sender Authentication”, Proc. of USENIX Security, 2020.
19 N. Mistry, R.S. Bhati, H. Jain y M. Parmar. “Email Spoofing Analysis”. Institute of Forensic Science, 2019. https://www.researchgate.net/publication/332877193_Paper_on_Email_Spoofing_Analysis.
20 T. P. Fowdur y L. Veerasoo. .An email application with active spoof monitoring and control”. 2016 International Conference on Computer Communication and Informatics (ICCCI), pp. 1-6, 2016.
21 D. Mooloo y T. P. Fowdur. .An SSL-based client-oriented anti-spoofing email application”. 2013 Africon, pp. 1-5, 2013.
22 H. Hu y G. Wang. “End-to-End Measurements of Email Spoofing Attacks”. Proceedings of the 27th USENIX Security Symposium, Baltimore, USA, 2018.
23 S. Maroofi, M. Korczynski y A. Duda. ”From Defensive Registration to Subdomain Protection: Evaluation of Email Anti-Spoofing Schemes for High-Profile Domains”. Proc. Network Traffic Measurement and Analysis Conference (TMA), 2020.