UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Revista Científica

http://revistas.udistrital.edu.co/ojs/index.php/revcie/index

CIDC

Artículo de investigación científica y tecnológica

Buenas prácticas para el despliegue seguro del servicio de correo electrónico

Good Practices for the Secure Deployment of the Email Service

Boas práticas para a implantação segura do serviço de e-mail

Dairis Almaguer-Pérez[1]
Adrian Hernández-Yeja[2]

Recibido: octubre de 2020 **Aceptado:** enero de 2021

Para citar este artículo: Almaguer-Pérez, D., y Hernández-Yeja, A. (2021). Buenas prácticas para el despliegue seguro del servicio de correo electrónico. *Revista Científica*, *41*(2), 199-212.
https://doi.org/10.14483/23448350.15838

Resumen

Actualmente el correo electrónico es uno de los servicios más afectados por los problemas de seguridad que proliferan en la Red, tanto en internet como en redes locales o intranet. Los especialistas en servicios telemáticos de las organizaciones tienen el gran reto de proveer un servicio de correo electrónico que garantice su estabilidad, su disponibilidad y que minimice los riesgos de la suplantación de identidad, los correos no deseados y los llamados correos spam. El objetivo de la presente investigación es realizar un análisis de los principales problemas de seguridad que proliferan en este servicio y describir un conjunto de buenas prácticas para una configuración y un despliegue seguros del servicio de correo electrónico. De esta manera se contribuirá a disminuir los problemas de seguridad asociados a este servicio y por consiguiente una mayor satisfacción de los usuarios.

Palabras clave: buenas prácticas; correo electrónico; seguridad; servicio; vulnerabilidades.

Abstract

Email is currently one of the services most affected by the security problems that proliferate on both the Internet and in local networks or intranet. Specialists in telematic services have the great challenge of providing an email service that guarantees its stability and availability, as well as minimizing the risks of identity theft, unwanted emails, and so-called spam emails. The objective of this research is to carry out an analysis of the main security problems that proliferate in this service and to describe a set of good practices for a secure configuration and deployment of the email service, which, in turn, contributes to reducing the security problems associated with this service and consequently achieving greater user satisfaction.

Keywords: context; problem-based learning; scientific competences; science teaching.

1. Esp. Universidad de las Ciencias Informáticas. La Habana, Cuba. dairis@uci.cu.
2. M. Sc. Universidad de las Ciencias Informáticas. La Habana, Cuba. ayeja@uci.cu.

Resumo
E-mail is currently one of the services most affected by the security problems that proliferate on the Internet, both on the Internet and in local networks or intranet. The specialists in telematic services of the organizations have the great challenge of providing an email service that guarantees its stability, availability and that minimizes the risks of identity theft, unwanted emails and so-called spam emails. The objective of this research is to carry out an analysis of the main security problems that proliferate in this service and to describe a set of good practices for a secure configuration and deployment of the email service. In this way, it will contribute to reduce the security problems associated with this service and consequently greater user satisfaction.
Palavras-chaves: boas práticas; email; segurança; serviço; vulnerabilidades.

Introducción

Las tecnologías de la información y la comunicación (TIC) han estado en constante evolución desde su surgimiento. Su uso creciente ha constituido un alto beneficio para las diferentes empresas e instituciones a lo largo del tiempo, pero cabe destacar que con el mismo vienen asociados grandes problemas de confidencialidad, integridad y disponibilidad de la información que se maneja si no se tiene en cuenta la seguridad.

Existen disímiles servicios que ofrecen el uso de las TIC, y el correo electrónico es, sin lugar a dudas, uno de los pilares sobre los que se asienta la Sociedad de la información, tanto por el número de usuarios como por la frecuencia con que se utiliza. En este momento es una aplicación vital para el funcionamiento diario de muchas empresas e instituciones.

En las empresas, el correo electrónico se utiliza constantemente durante el horario laboral y en ocasiones cuando los trabajadores están en su casa, por lo que debe permanecer disponible en todo momento. Un tiempo de inactividad de apenas treinta minutos puede ocasionar consecuencias graves para la productividad de los empleados y los ingresos de las instituciones (Viera y Pérez, 2014).

En las instituciones la mayor parte de la dinámica se sustenta en el uso del correo para la comunicación entre directores y empleados, la distribución de información interna o externa, soporte de ayuda a clientes y ciudadanos, seguimiento de concursos públicos y distribución rápida y efectiva de información a los ciudadanos. Para poder ofrecer servicios como este resulta imprescindible contar con una red que soporte la familia de protocolos TCP/IP y tener programas clientes y servidores instalados y correctamente configurados (Baluja, 2003).

Estos programas, incorrectamente configurados, introducen determinadas vulnerabilidades y fallos en el funcionamiento, como la utilización de puertos que si no se filtran por un cortafuego pueden ser un agujero por el cual accedan intrusos. Otro de los problemas es el uso de protocolos no cifrados que permiten que la información viaje en texto plano, lo que hace que sea visible para personas malintencionadas y estas la utilicen para acceder a los servidores o utilizarlos para realizar ataques a terceros. Por otro lado, las prestaciones o posibilidades de cada uno de ellos son diferentes, no todos poseen las mismas opciones. Asimismo, la configuración para lograr determinadas garantías de seguridad tiende a ser compleja y difícil de comprobar y requiere un alto conocimiento de seguridad del personal encargado.

Existen a nivel mundial vectores de ataques a través del correo electrónico enfocados en las vulnerabilidades como la propagación de programas malignos, la suplantación de identidad y los correos no deseados. Este servicio se compone de múltiples sistemas, cada sistema individual puede ser vulnerable debido a que su configuración en la variante de instalación por defecto está orientada a la facilidad de instalación y funcionamiento, no a la seguridad, incluyendo los protocolos. La integración de múltiples aplicaciones con configuraciones deficientes hace que aumente la aparición de vulnerabilidades e

inseguridad de la red, bajo el principio del eslabón más débil.

Los especialistas en servicios telemáticos de las organizaciones tienen el gran reto de proveer un servicio de correo electrónico que garantice su estabilidad, su disponibilidad y que minimice los riesgos de la suplantación de identidad, los programas malignos que afectan el funcionamiento del servicio, los correos no deseados y los llamados correos spam. Para ello es necesario gestionar adecuadamente las medidas de seguridad durante el despliegue y el uso de este servicio.

Los sistemas que se utilizan para gestionar el servicio de correo electrónico, así como las herramientas que lo integran, están en constante cambio. Diariamente a nivel mundial se descubren nuevas vulnerabilidades, así como nuevas formas y métodos de ataques para las mismas. Es debido a esto que las medidas de seguridad también deben evolucionar y estar en constante cambio.

Metodología

Para la realización de la propuesta de solución los autores tuvieron en cuenta varios métodos científicos que permitieron una mayor organización en el trabajo y obtener un resultado aceptable y acorde a las necesidades de la institución. Estos métodos se dividen en empíricos y teóricos, los cuales se describen a continuación.

Métodos teóricos

- **Histórico-lógico**: se utiliza para determinar los antecedentes relacionados con el servicio de correo electrónico, así como problemas de seguridad que existen desde su surgimiento. Además, permitió conocer muchas de las configuraciones de seguridad necesarias en los mismos.
- **Analítico-sintético**: se utiliza en la investigación de los servicios de correo, así como las herramientas y las tecnologías para la gestión y la configuración segura de los servicios de correo electrónico. Permitió seleccionar programas que gestionan la seguridad del servicio de correo electrónico y escoger las mejores configuraciones de seguridad para ser utilizadas en él mismo.

Métodos empíricos

- **Observación**: se realiza para conocer cómo funciona el servicio de correo electrónico en algunas instituciones cercanas y el nivel de exposición a amenazas y ataques de seguridad. También para para conocer los mecanismos y procedimientos de seguridad que se implementan, así como su organización y su predictibilidad.
- **Entrevista**: se realiza a diferentes especialistas en servicios telemáticos para conocer la manera cómo se configuran las políticas y los procedimientos de seguridad en el servicio de correo electrónico. Además de conocer si las configuraciones de seguridad que aplican están formalmente descritas o automatizadas.
- **Análisis documental**: se utiliza para analizar toda la documentación consultada y dar solución al problema planteado.

Resultados

La seguridad del correo electrónico se convierte en un caso sensible para estudiar en el campo de la seguridad de la información. Uno de los problemas de mayor importancia en la red es cómo minimizar la exposición a incidentes de seguridad de la información que viaja a través de los mensajes de correo electrónico. Son varios los componentes y los protocolos que involucra este servicio y a su vez, incorrectamente configurado, introduce problemas de seguridad, por lo que la configuración adecuada en los mismos es indispensable. Para gestionar la seguridad en un servicio determinado se hace indispensable conocer su funcionamiento, es por ello que a continuación se describen los componentes del servicio de correo electrónico.

Agentes del servicio de correo electrónico

Para el correcto funcionamiento del servicio de correo electrónico influye un conjunto de tecnologías básicas, las cuales están relacionadas entre sí. Cuando un emisor envía un correo electrónico hacia un receptor, lo hace a través del agente de mensaje de usuario (MUA), el cual puede ser un navegador o una aplicación de escritorio. Este, a su vez, le entrega el mensaje al agente de envío de correo (MSA) el cual impone requisitos, como el permiso de acceso y hace que el correo se adhiera a los estándares de internet. El MSA hace entrega del mensaje al agente de transferencia de correo (MTA), el cual enruta y retransmite el correo de host a host. El MTA le envía el correo al agente de entrega de correo (MDA) y este hace llegar el mensaje al buzón del receptor, el cual puede consultado desde su MUA (Figura 1).

Protocolos y estándares que son parte del servicio de correo electrónico

- **SMTP (Protocolo simple de transferencia de correo)**. SMTP es el protocolo estándar para el envío de correos electrónicos a través de internet. Se basa en el modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores (Scott, Simson y Garfinkel 2019; Álvarez, 2008).
- **POP3 (Protocolo de oficina de correos versión 3)**. POP3 es un protocolo de correo estándar utilizado para **recibir mensajes de correo electrónico** desde un servidor remoto a un cliente de correo electrónico local. Permite descargar mensajes de correo electrónico en el ordenador local y los lee, incluso cuando no esté conectado (Scott, Simson y Garfinkel 2019).
- **IMAP (Protocolo de acceso a mensajes de internet)**. IMAP es un protocolo utilizado para administrar y recuperar mensajes de correo electrónico. Incluye funciones de creación, borrado y renombrado de buzones y es compatible con el estándar MIME (Multipurpose Internet Mail Extensions, por su sigla en inglés). Es una alternativa a POP3, pero incluye más funciones integradas que lo hacen más atractivo para el uso empresarial. Los clientes IMAP pueden descargar mensajes de correo electrónico, pero los mensajes permanecen en el servidor; esto permite que varios clientes puedan acceder al mismo buzón simultáneamente, lo cual significa que los usuarios finales pueden mantener su correo electrónico sincronizado en múltiples dispositivos. Este protocolo al igual que POP3 en su configuración por defecto utiliza un puerto por el cual la comunicación viaja sin cifrar (Scott, Simson y Garfinkel 2019; Álvarez, 2008; Dumka, Tomar, Patni y Anand, 2014).

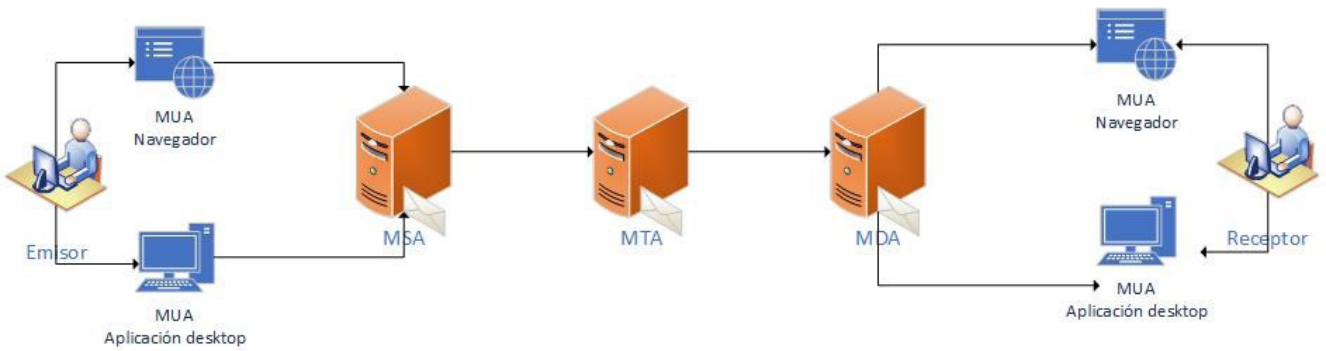

Figura 1: Funcionamiento básico del correo electrónico.
Fuente: elaboración propia.

– **HTTP (Protocolo de transferencia de hipertexto).** HTTP funciona como un protocolo de solicitud-respuesta en el modelo informático cliente-servidor. Un navegador web, por ejemplo, puede ser el cliente, y una aplicación que se ejecuta en una computadora que aloja un sitio web puede ser el servidor. El cliente envía un mensaje de solicitud HTTP al servidor. El servidor, que proporciona recursos como archivos HTML y otro contenido, o realiza otras funciones en nombre del cliente, devuelve un mensaje de respuesta al cliente. La respuesta contiene información sobre el estado de finalización de la solicitud y también puede contener contenido solicitado en el cuerpo del mensaje (Kumar y Vaidya, 2016). En el modelo de referencia OSI , corresponde a un protocolo de capa de aplicación que opera tomando servicio del protocolo TCP en la capa de transporte (Tolosa y Fernández, 2016).

Ataques a través del servicio de correo electrónico

Es imposible tener un servicio de correo electrónico cien por ciento seguro. Los servicios de correo electrónico, como cualquier otro servicio, tanto basado en intranet como en internet, podrían ser atacados por personas malintencionadas, causar daños a los usuarios o la propia institución y atentar contra la privacidad y la integridad de la información enviada a través del mismo. A continuación se describen las principales amenazas de seguridad que pueden afectar a los usuarios o instituciones a través del servicio de correo electrónico.

Malware

Es un programa o archivo malicioso que puede afectar la funcionalidad de su dispositivo o causar daños a sus datos con su permiso. Esto es peligroso para la seguridad del correo electrónico porque el malware puede incluir virus, troyanos, gusanos y spyware. Los programadores de este software dañino generalmente usan el correo electrónico para garantizar su entrega al usuario objetivo. El peligro de dicho software dañino radica en su capacidad, si se explota con éxito, para tomar el control del dispositivo o incluso de toda la red mediante la aplicación de privilegios que se escalan al sistema (Kaspersky, s.f.).

Spam

El spam se puede definir como correo electrónico no solicitado (no deseado, basura) para un destinatario o cualquier correo electrónico que el usuario no desea tener en su bandeja de entrada. También se define como "Internet Spam es uno o más mensajes no solicitados, enviados o publicados como parte de una colección más grande de mensajes, todos con contenido sustancialmente idéntico". Hay problemas graves por los correos no deseados: a saber, desperdicio de recursos de red (ancho de banda), pérdida de tiempo, daños a las PC y computadoras portátiles debido a virus y problemas éticos (Basavaraju y Prabhakar, 2010).

Phishing

El correo electrónico phishing es un tipo especial de mensaje de spam. Dicho correo electrónico es un mecanismo criminal que se basa en reclamaciones falsas de correo electrónico, supuestamente originarias de una compañía o banco legítimo. Posteriormente, a través de un enlace incrustado dentro del correo electrónico, el *phisher* intenta redirigir a los usuarios a sitios web falsos, que están diseñados para obtener de manera fraudulenta datos financieros como nombres de usuario, contraseñas y números de tarjetas de crédito (Almomani, Gupta, Atawneh, Meulenberg y Almomani, 2013; Scott, Simson y Garfinkel 2019; Nightingale, 2017; Pal, 2019).

Modificación de mensajes de hombre en el medio

Como su nombre indica, un ataque de hombre en el medio ocurre cuando alguien entre dos usuarios intercepta la comunicación supervisando, capturando y controlando la comunicación sin el conocimiento de los usuarios. Por ejemplo, un agresor puede negociar claves de cifrado con ambos usuarios y cada usuario envía datos cifrados al atacante, que puede descifrar los datos con las claves públicas y privadas (Cueva y Alvarado, 2017).

Ingeniería social

La ingeniería social se refiere a la manipulación psicológica de las personas para revelar información o realizar una acción (Butavicius, Parsons, Pattinson y McCormac, 2016). Es el arte de manipular a las personas y aprovechar de manera inteligente sus vulnerabilidades. Las estafas de phishing también se pueden considerar como una táctica de ingeniería social. Es más fácil engañar a alguien para obtener su contraseña en lugar de tratar de adivinarla o piratearla técnicamente, a menos que sea realmente muy débil o fácil.

Ransomware

El *ransomware* es un programa malicioso que infecta la computadora objetivo, encripta todo su contenido y luego exige un rescate, que de no ser pagado esta información no sería recuperada o puede ser usada para chantajes u otros fines, incluso lucrativos. Estos programas tienen la habilidad de destruir los datos de esa computadora si así lo determina el atacante. Algunas variantes de *ransomware* pueden bloquear todo intento de acceso a la computadora (Kaspersky, s.f.).

Spoofing

La suplantación de identidad es cuando un mensaje de correo electrónico parece provenir de una fuente legítima, pero de hecho es de un impostor. La suplantación de identidad del correo electrónico se puede utilizar con fines maliciosos, como propagar virus, rastrear datos comerciales confidenciales y otras actividades de espionaje industrial. Los remitentes hacen esto por varias razones, que incluyen (Babu, Bhaskari y Satyanarayana, 2010):

Ataques Open Relay

Un servidor SMTP que funciona como un *open relay*, es un servidor de correo electrónico que no verifica si el usuario está autorizado a enviar correos electrónicos desde la dirección de correo electrónico especificada. Por lo tanto, los usuarios podrán enviar correos electrónicos que provengan de cualquier dirección de correo electrónico de terceros que deseen (Skwarek et al., 2019). Esto es una vulnerabilidad que aprovechan los ciberdelincuentes para utilizar ese servidor como destino de los ataques que provienen realmente desde otro servidor. Lo que provoca esto es que la empresa con el servidor *open relay* sea puesto en listas negras de otras compañías como servidores spam.

- **Denegación de servicio (DOS).** Consiste en enviar un gran número de peticiones a un servidor para saturarlo y dejarlo fuera de servicio, de manera que los usuarios legítimos del servicio no puedan acceder a esos recursos. Este ataque generalmente se realiza mediante *bots*, software automatizado que envían una gran cantidad de solicitudes falsas que excede la capacidad del búfer del servidor (Cueva y Alvarado, 2017; Pal, 2019).
- **Denegación de servicio distribuido (DDos).** Consiste en generar una cantidad relativamente pequeña de tráfico a partir de una gran cantidad de sistemas (conocidos como zombis o *bots*) que están conectados con un controlador de *botnet*. Estos sistemas generan colectivamente un gran volumen de tráfico para reducir

los servicios de cualquier organización (Pal, 2019).

– **Envenenamiento de caché.** Los ataques de envenenamiento de caché funcionan al causar intencionalmente que un servidor DNS guarde en caché información falsa, como la dirección de Protocolo de Internet (IP) incorrecta para un nombre de dominio en particular. Este tiene como objetivo que cuando se emite una consulta para determinar el nombre de dominio de destino, el servidor DNS responda con la dirección incorrecta debido a la caché envenenada en él. Como el servidor de correo no sabe identificar que se le ha dado información errónea, se conecta a la dirección resuelta y entrega los mensajes de correo electrónico. De esta manera, el envenenamiento de caché puede permitir que un atacante redirija los mensajes de correo electrónico a un servidor de mensajería no autorizado (Kumari, Agrawal y Lilhore, 2017).

Hasta el momento se han descrito los agentes y los protocolos que soportan el servicio de correo electrónico y los distintos tipos de amenazas que se realizan tanto a través de él, como hacia la infraestructura del mismo. Gestionar la seguridad en este servicio para garantizar su disponibilidad y la confidencialidad de los datos que se trasmiten a través de él se hace complejo. Es necesario tener un conocimiento adecuado en cuanto a su funcionamiento, las tecnologías y los problemas de seguridad asociados para poder gestionar su seguridad.

Estándares y regulaciones relacionados con la seguridad en el correo electrónico

Es necesario para una adecuada gestión de la seguridad realizar una valoración de los principales modelos, estándares, recomendaciones y regulaciones que, tanto a nivel internacional como nacional, están relacionados con la gestión de la seguridad de la información (Montesino, R, Baluja, W. y Porvén, J., 2013). A continuación se resumen los principales estándares relacionados con el servicio de correo electrónico y su seguridad a nivel internacional y nacional. Además, se describen otros mecanismos de seguridad que no se encuentran recogidos en estas regulaciones o estándares, pero son fundamentales durante la gestión de la seguridad de este servicio.

Estos Registros Federales de Contribuyentes (RFC) definen algunos estándares de seguridad para protocolos y formatos de correo electrónico (RFC, s.f.).

- •RFC 2595 - Uso de TLS con IMAP, POP3 y ACAP. Este es un protocolo utilizado para actualizar una conexión IMAP / POP de texto sin formato a una encriptada SSL / TLS.
- •RFC 3207 - Extensión de servicio SMTP para SMTP seguro sobre la seguridad de la capa de transporte. Este es un protocolo utilizado para actualizar una conexión SMTP de texto sin formato a una encriptada SSL / TLS.
- •RFC 5246 - Protocolo de seguridad de la capa de transporte (TLS) versión 1.2. Este es un protocolo utilizado para cifrar una conexión.
- •RFC 6376 - Firmas de correo identificado de DomainKeys (DKIM). Esto permite que los correos electrónicos sean firmados por un dominio en particular para garantizar que no hayan sido alterados y decir que ese dominio se responsabiliza por el mensaje.
- •RFC 8617 - Cadena recibida autenticada (ARC). Este es un protocolo para proporcionar una cadena de custodia autenticada para mensajes que han pasado a través de servidores de correo intermedios, como el reenvío.
- •RFC 2045 - Extensiones multipropósito de correo de internet (MIME) Primera parte: Formato de los cuerpos de mensajes de internet. Esta es una extensión del formato de mensaje de correo electrónico para admitir archivos adjuntos y datos no ASCII en los correos electrónicos.
- •RFC 2046 - Extensiones multipropósito de correo de internet (MIME) Segunda parte: Tipos de medios.

- •RFC 2047 - Extensiones multipropósito de correo de Internet (MIME) Tercera parte: Extensiones de encabezado de mensaje para texto no ASCII.

Otros mecanismos para gestionar la seguridad en el servicio de correo electrónico

Mecanismos para combatir el spam

Existen varios mecanismos que hoy día se implementan o configuran para combatir el flujo de correos basura o los llamados correos spam. Muchos de estos mecanismos vienen en las herramientas antivirus o son aplicaciones específicas que pueden ser instaladas en el programa de gestión de correo electrónico. En este acápite se describen algunos mecanismos que a nivel mundial son utilizados para combatir estos correos maliciosos.

Mecanismos que se configuran en el programa de gestión de correo o en el antivirus de correo

> **DKIM:** El remitente crea un valor hash MD5 de algunos elementos del correo electrónico (por ejemplo, el encabezado del correo electrónico). El remitente luego usa una clave privada (solo conocida por él) para cifrar ese hash MD5. La cadena encriptada se inserta en el correo, es conocida como la firma DKIM. El remitente almacena una clave pública en un registro DNS (Hu, Peng, y Wang, 2018).

- El receptor encuentra la clave pública del DNS para ese dominio. El receptor luego usa esta clave pública para descifrar la firma DKIM del correo electrónico de vuelta al hash MD5 original. El receptor genera un nuevo hash MD5 a partir de los elementos del correo electrónico firmado por DKIM, y lo compara con el hash MD5 original. Si coinciden el receptor sabe que (Hu, Peng, y Wang, 2018):
- El dominio de correo electrónico de envío es el propietario de ese dominio (es matemáticamente casi imposible falsificar una firma DKIM correcta que descifra el hash MD5 original usando la clave pública).
- Los elementos del correo electrónico firmado por DKIM no se modificaron en tránsito (de lo contrario, el hash MD5 original y el hash MD5 generado por el receptor no coincidirían).
- La desventaja de DKIM es que solo puede proteger el correo que se ha firmado, pero no proporciona un mecanismo para probar que un mensaje sin firmar debería haberse firmado.

SPF - Marco de políticas del remitente

El registro SPF proporciona una confirmación al servidor del destinatario de que el servidor de envío de correo electrónico está autorizado a enviar el correo electrónico en su nombre.

El servidor receptor verifica si existe SPF en el DNS para el dominio en la dirección MAIL FROM (también llamada dirección del remitente del sobre). Si existe SPF, el receptor verifica si la dirección IP del servidor emisor coincide con la lista de IP en el SPF (Tiwari, Ansari y Dubey, 2018).

La desventaja de SPF es que valida el servidor de origen solo mirando el dominio en la dirección MAIL FROM, no el encabezado del correo From address. La dirección MAIL FROM es la dirección de correo electrónico que utilizan los servidores receptores para notificar al servidor remitente y para los problemas de entrega. También se denomina remitente del sobre, sobre desde, dirección de devolución o dirección de ruta de retorno (Tiwari, Ansari y Dubey, 2018).

DMARC: autenticación, informes y conformidad de mensajes basados en el dominio

Todo el análisis de entrega de un mensaje recibido se realiza en el receptor y se escribe en la base de datos. El procesamiento posterior de los registros de la base de datos se deja a un trabajo periódico del reportero DMARC, que se despierta cada dos minutos para procesar todos los registros aún

no reportados en la base de datos (Nightingale, 2017). DMARC está construido sobre SPF y DKIM para abordar las deficiencias de estos dos estándares de autenticación. DMARC permite aplicar la validación DKIM o SPF, y confirmar que la dirección mostrada es auténtica (Dogan, 2017).

Sistemas para la detección y rechazo de mensajería spam

Los sistemas para la detección de correos no deseados o los llamados correos spam contienen filtros que se configuran en laboratorios antispam, que crean y perfeccionan las reglas de filtrado. Los remitentes de spam intentan constantemente superar las protecciones creadas por los filtros. El proceso de modificar y perfeccionar estas reglas de filtrado también es continuo. La efectividad de estos filtros depende de las actualizaciones oportunas de las reglas de filtrado. No todos los programas que existen en la actualidad realizan este filtrado de manera efectiva, en consecuencia, es necesario implementar una solución antispam que no solo utilice actualizaciones automáticas de reglas de filtrado, sino que además actualice el filtro de reglas basadas en estadísticas producidas por un gran número de receptores de spam (Stewart et al., 2016).

> **ClamAV**: es un kit de herramientas antivirus de código abierto, diseñado especialmente para el escaneo de correo electrónico en pasarelas de correo. Proporciona una serie de utilidades que incluyen un demonio multiproceso flexible y escalable, un escáner de línea de comandos y una herramienta avanzada para actualizaciones automáticas de bases de datos. El núcleo del paquete es un motor antivirus disponible en forma de biblioteca compartida. ClamAV permite las siguientes funcionalidades (ClamAV, s.f.):

- Escaneo rápido de archivos.
- Protección en tiempo real (solo Linux). El demonio de escaneo admite escaneo en acceso en versiones modernas de Linux, incluida la capacidad de bloquear el acceso a archivos hasta que se haya escaneado completamente.
- Detecta más de un millón de virus, gusanos y troyanos, incluidos los virus de macro de Microsoft Office, malware móvil y otras amenazas.
- El intérprete de código de bytes incorporado permite a los escritores de firmas ClamAV crear y distribuir rutinas de detección muy complejas y mejorar de forma remota la funcionalidad del escáner.
- Las bases de datos de firmas firmadas aseguran que ClamAV solo ejecutará definiciones de firmas confiables.
- Escanea dentro de archivos y archivos comprimidos, pero también protege contra las bombas de archivo. Las capacidades de extracción de archivo incorporadas incluyen *tar*, *zip*, *gzip*, *rar*, entre otros.

> **SpamAssassin**: es una herramienta que en algunas plataformas de correo viene implícita y en otras permite su integración. Utiliza una variedad de normas para identificar el spam y captura tráfico spam real. Utiliza un sistema de puntos para categorizar los mensajes, por lo que, si un mensaje acumula demasiados puntos, es etiquetado como spam y, si se cuenta con un filtro para su MDA, puede almacenar los mensajes sospechosos en una carpeta específica. Utilizando SpamAssassin, se le pueden enseñar los mensajes deseados y no deseados mediante el uso de su función de filtro bayesiano y de esta forma se realizará un aprendizaje supervisado para que mensajes similares sean categorizados de acuerdo con los mensajes de muestra (Viera y Pérez, 2014).

> **Postscreen**: Zimbra, a partir de su versión colaborativa 8.7 y superior, presenta Postscreen como una estrategia adicional contra el correo no deseado. Esta herramienta proporciona protección adicional contra la sobrecarga del servidor de correo. Un proceso posterior a la pantalla maneja múltiples conexiones SMTP

entrantes y decide qué clientes pueden comunicarse con un proceso del servidor SMTP posterior a la reparación. Al mantener alejados a los robots de spam, la pantalla posterior deja más procesos de servidor SMTP disponibles para clientes legítimos y retrasa el inicio de las condiciones de sobrecarga del servidor (Zimbra, s.f.).

> **Amavis**: Se utiliza de intermediario entre el antivirus y el antispam. Es un filtro de contenido de código abierto para correo electrónico, que además sirve para implementar la transferencia de mensajes de correo y para la decodificación, sin contar con que también interactúa con filtros de contenido externo para dar protección contra virus, otros malware y spam. Es usable, adicionalmente, para detectar contenidos prohibidos o para capturar errores de sintaxis en los mensajes de correo electrónico. Se puede utilizar, además, para poner en cuarentena y luego liberar o archivar mensajes en buzones o en una base de datos SQL (Amavis, s.f.).

Otras recomendaciones de seguridad

> **Sistemas de detección de intrusos de red**: Los sistemas de detección de intrusiones de red (NIDS) son herramientas esenciales para que los administradores de sistemas de red detecten varias infracciones de seguridad dentro de la red de una organización. Un NIDS monitorea y analiza el tráfico de red que ingresa o sale de los dispositivos de red de una organización y genera alarmas si se observa una intrusión. En cuanto a los métodos de detección de intrusos, los NIDS se clasifican en dos clases: basados en firma (SNIDS) y de detección de anomalías (ADNIDS). En SNIDS las firmas de ataque están preinstaladas y se realiza una coincidencia de patrón para el tráfico contra las firmas instaladas para detectar una intrusión en la red. Este es eficaz en la detección de ataques conocidos y muestra una alta precisión de detección con menos tasas de falsa alarma. Un ADNIDS clasifica el tráfico de red como una intrusión cuando observa una desviación del patrón de tráfico normal (Niyaz et al., 2016).

> **NIDS Snort**: es el sistema de prevención de intrusiones (IPS) de código abierto más importante del mundo. Snort IPS usa una serie de reglas que ayudan a definir la actividad de red maliciosa y usa esas reglas para encontrar paquetes que coincidan con ellas y genera alertas para los usuarios. Snort también se puede implementar en línea para detener estos paquetes. Snort tiene tres usos principales: como rastreador de paquetes como tcpdump, como registrador de paquetes, que es útil para la depuración del tráfico de red, o como un sistema de prevención de intrusiones en la red en toda regla. Snort se puede descargar y configurar tanto para uso personal como comercial (Snort, s.f.; Ecured, s.f.).

> **Configurar HIDS OSSEC**: es una plataforma para monitorear y controlar sus sistemas. Combina todos los aspectos de detección de intrusos basada en host, monitoreo de registros y gestión de incidentes de seguridad / gestión de eventos e información de seguridad en una solución simple, potente y de código abierto. OSSEC permite a los administradores gestionar políticas específicas de aplicaciones y servidores en múltiples plataformas. Con él se puede detectar y alertar sobre modificaciones no autorizadas del sistema de archivos y comportamientos maliciosos incrustados en los archivos de registro de productos. Cubre las secciones de monitoreo de integridad de archivos, inspección y monitoreo de registros, así como verificación y aplicación de políticas (OSSEC, s.f.).

> **Cortafuegos**: proporciona una barrera contra varios tipos de amenazas. El cortafuegos instalado en una red privada evita cualquier acceso no autorizado. Se puede implementar tanto en hardware como software, o una combinación

de ambos. En general, los cortafuegos son empleados para restringir a usuarios no autorizados de internet que acceden a las redes privadas. Todas las conexiones entrantes o salientes son examinadas y se bloquean aquellas que no cumplen con los criterios de seguridad especificados en las reglas del mismo (Lopez, Mihelich y Hepburn, 2016).

> **Programas Antivirus**: son programas que contienen métodos de escaneos, los cuales son algoritmos que ordenan acciones sobre el objeto que escanea, con atributos, acciones y datos; durante la ejecución de estas acciones es posible observar o detectar actividad realizada por código malicioso. Los métodos de análisis antivirus incluyen, entre otros, análisis de firmas, análisis heurístico, método de detección de cambios (Levchenko, 2017).

> **Kaspersky Security 8.0 para Linux Mail Server (KLMS)** (Kaspersky support, 2019): protege las entradas y mensajes de correo electrónico salientes contra malware y spam, y proporciona filtrado de contenido. Se ejecuta bajo sistemas operativos Linux y FreeBSD, y se puede usar en servidores de correo de alta carga. La aplicación permite:

- Análisis antispam del correo entrante y saliente.
- Detectar objetos que están infectados, probablemente infectados, protegidos con contraseña o inaccesibles para escanear.
- Neutralizar las amenazas reveladas en archivos y mensajes de correo; desinfectar objetos.
- Copia de seguridad a un archivo en el disco duro y entrega de mensajes de copia de seguridad a los destinatarios.
- Procesamiento de correo de acuerdo con las reglas definidas para grupos existentes de remitentes y destinatarios.
- Realización de filtrado de contenido de mensajes de correo por tamaño, nombre y tipo de archivo adjunto.
- Notificación al remitente, a los destinatarios y al administrador de los mensajes detectados que contienen objetos infectados, probablemente infectados, protegidos con contraseña o inaccesibles para escanear.
- Actualización de las bases de datos antivirus y antispam desde los servidores de actualización de Kaspersky Lab de acuerdo con horario o bajo demanda.
- Generación de estadísticas e informes de tiempo de ejecución de la aplicación.
- Obtención de información y estadísticas de tiempo de ejecución de la aplicación a través de SNMP, así como habilitar / inhabilitar capturas de eventos.
- Análisis de los sistemas de archivos del servidor de correo en busca de amenazas bajo demanda.
- Configuración de los ajustes y administración de la aplicación usando las herramientas estándar del sistema operativo desde línea de comando o usando una interfaz basada en web.

> **MailCleaner**: es una solución completa y gratuita de filtrado de correo electrónico del lado del servidor. Se puede instalar en casi cualquier sistema de virtualización y actúa como una puerta de enlace SMTP. Debe instalarse entre internet y el servidor de correo final, ya sea convirtiéndose en el nuevo registro MX para los dominios o recibiendo correo de sus puertas de enlace. Una vez filtrados, los mensajes se reenviarán al servidor de correo de destino o al próximo Gateway. No es necesario configurar todos los buzones, MailCleaner filtra automáticamente todos los mensajes válidos, una vez que es configurado un dominio (MailCleaner, 2020).

> **Proxmox Mail Gateway**: es una solución que se implementa entre el firewall y el servidor de correo; todo el tráfico de correo electrónico (SMTP) se reenvía primero a Mail Gateway, todos los correos electrónicos no deseados se filtran y eliminan o rechazan (filtrado antes de la cola), y solo entonces se envían al servidor de correo (Proxmox, s.f.).

- **Separación lógica en la zona desmilitarizada**: es bien conocida como capa de seguridad y también como red perimetral que se utiliza para proteger el sistema interno donde todos los puertos están abiertos para que puedan ser vistos por extraños. Por lo tanto, cuando alguien realiza un ataque a un servidor que se encuentra en la DMZ solo puede acceder al host en DMZ, no en la red interna (Iskandar, Virma y Ahmar, 2019). En esta zona se deben instalar los servicios que son accedidos desde internet con el objetivo de proteger la red interna de una institución. Esta zona es la más protegida en una institución ya sea con programas antivirus, cortafuegos o sistemas de detección de intrusos o todos a la vez.
- **Autenticación**: los enfoques basados en la autenticación están diseñados para confirmar si el correo electrónico fue enviado por una ruta válida y el *phisher* no está falsificando el nombre de dominio. La autenticación aumenta la seguridad de la comunicación, tanto a nivel de usuario como de dominio. La autenticación a nivel de usuario es empleada por contraseña como credenciales. Sin embargo, la autenticación de contraseña se puede romper fácilmente mientras que la autenticación a nivel de dominio se implementa en el lado del proveedor (por ejemplo, de un servidor de correo a otro). Además, para que la autenticación a nivel de dominio sea efectiva, los proveedores de ambos, el emisor y el receptor, deben emplear la misma tecnología (Al-Mashhadi, Alabiech, 2017).
- **Monitoreo**: el monitoreo del servicio permite detectar posibles ataques, amenazas, nivel de usabilidad, disponibilidad del servicio para tomar acciones en consecuencia. Para el correcto monitoreo del servicio de correo electrónico se hace necesaria la utilización de algunas herramientas que brindan información con respecto a disponibilidad, integridad y uso de este servicio.
- **Icinga**: es un motor de monitoreo eficiente que, dada su infraestructura, brinda la posibilidad de mirar cualquier host y aplicación. Es capaz de monitorear todo el centro de datos y las nubes. Los resultados recopilados se procesan y almacenan de manera eficiente en el uso de recursos. Posee una interfaz web rápida y bien organizada y brinda acceso a todos los datos relevantes. Las vistas personalizadas se crean agrupando y filtrando elementos individuales y combinándolos en paneles personalizados. La atractiva interfaz web permite actuar con solo un clic, lo que le facilita reaccionar ante cualquier evento (Icinga, s.f.). Es la herramienta que se utiliza para el monitoreo de disponibilidad, generación y envío de alarmas para parámetros definidos como memoria, disco y CPU utilizados.
- **InfluxDB**: es la base de datos de series temporales de código abierto y el corazón de toda la obtención de la métrica, puesto que es donde se almacenan todos los datos; trae consigo un lenguaje semi SQL, por lo que los pedidos de datos son bastantes intuitivos. Tiene la posibilidad de especificar cómo se quiere almacenar los datos en el tiempo, por cuántos días, cuántos datos mantener después de que pase cierto tiempo (Influxdata, s.f.).
- **Telegraf**: es un agente de servidor impulsado por complementos para recopilar e informar métricas. Tiene complementos para obtener una variedad de métricas directamente desde el sistema en el que se está ejecutando, extraer métricas de API de terceros o incluso escuchar métricas a través de un servicio de consumidor de estadísticas. También tiene complementos de salida para enviar métricas a una variedad de otros almacenes de datos, servicios y colas de mensajes, incluidos InfluxDB (Influxdata, s.f.).
- **Grafana**: es un software de visualización y análisis de código abierto que permite consultar, visualizar, alertar y explorar métricas sin importar dónde estén almacenadas. Proporciona

herramientas para convertir los datos de la base de datos de series temporales (TSDB) en gráficos y visualizaciones. La configuración cubre tanto los archivos de configuración como las variables de entorno. Puede configurar puertos predeterminados, niveles de registro, direcciones IP de correo electrónico, seguridad, entre otros. Semanalmente son creados complementos para esta herramienta con nuevas funcionalidades (GrafanaLabs, s.f.).

Conclusiones

La descripción de los elementos teóricos relacionados con el servicio de correo electrónico permitió tener un mayor entendimiento de su funcionamiento.

La identificación y el estudio de los principales problemas de seguridad asociados a este servicio contribuyó en la toma de decisiones en cuanto a las medidas de seguridad a implementar.

El estudio de las regulaciones internacionales y nacionales relacionadas con la seguridad de este servicio, así como de otras recomendaciones de seguridad identificadas, permitió describir las medidas a implementar para gestionar adecuadamente la seguridad en un servicio de correo electrónico.

Referencias

Álvarez, H. A. (2008). *Propuesta de implementación de un servidor de correo sobre linux para sustituir el servidor de correo MDaemon* (Tesis de pregrado). Universidad Central Marta Abreu de las Villas, Cuba.

Al-Mashhadi, H. M. Alabiech, M. H. (2017). A Survey of Email Service; Attacks, Security Methods and Protocols. *International Journal of Computer Applications*, *162*(11), 31-40. https://doi.org/10.5120/ijca2017913417

Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., Almomani, E. (2013). A Survey of Phishing Email Filtering Techniques. *IEEE Communications Surveys & Tutorials*, *15*(4), 2070-2090. https://doi.org/10.1109/surv.2013.030713.00020

Amavis. (s.f.). *Amavis*. https://www.amavis.org/

Babu, P. R., Bhaskari, D. L., Satyanarayana C. (2010). A Comprehensive Analysis of Spoofing. *International Journal of Advanced Computer Science and Applications*, *1*(6). https://doi.org/10.14569/IJACSA.2010.010623

Baluja, W., Fernandez, I. (2003). SAVMailer: filtro de correo para servidores sendmail. *Ingeniería Electrónica, Automática y Comunicaciones, 24*(3), 71-76.

Basavaraju, M., Prabhakar, R. (2010). A Novel Method of Spam Mail Detection Using Text Based Clustering Approach. *International Journal of Computer Applications*, *5*(4), 15-25. https://doi.org/10.5120/906-1283

Butavicius, M., Parsons, K., Pattinson, M., McCormac, A. (2016). Breaching the Human Firewall: Social Engineering in Phishing and Spear-Phishing Emails. *Cornell University*. https://arxiv.org/abs/1606.00887

ClamAV. (s.f.). *Introduction*. https://www.clamav.net/documents/introduction

Cueva, M. E., Alvarado, D. J. (2017). Analysis of free SSL/TLS Certificates and their implementation as Security Mechanism in Application Servers. *Enfoque UTE*, *8*(1), 273-286. https://doi.org/10.29019/enfoqueute.v8n1.128

Dogan, H. (2017). *Email Authentication Best Practices the Optimal Ways to Deploy SPF, DKIM and DMARC*. Cisco.

Dumka, A., Tomar, R. Patni, J. C., Anand, A. (2014). Taxonomy of E-Mail Security Protocol. *International Journal of Innovative Research in Computer and Communication Engineering*, *2*(4), 4104-4108.

Ecured. (s.f.). *Snort*. https://www.ecured.cu/Snort

GrafanaLabs. (s.f.). *What is Grafana?*. https://grafana.com/

Hu, H., Peng, P., Wang, G. (2018). Towards the Adoption of Anti-spoofing Protocols. *Arxiv*. https://arxiv.org/pdf/1711.06654.pdf

Icinga. (s.f.). *Icinga*. https://icinga.com/

Influxdata. (s.f.). *Getting started with InfluxDB OSS*. InfluxDB.

Influxdata. (s.f.). *Telegraf 1.12 documentation*. Telegraf.

Iskandar, A., Virma, E., Ahmar, A. S. (2018). Implementing DMZ in Improving Network Security of Web

Testing in STMIK AKBA. *International Journal of Engineering & Technology*, *7*(2.3), 99-104. https://doi.org/10.14419/ijet.v7i2.3.12627

Kaspersky support. (2019). *Kaspersky Security 8.0 for Linux Mail Server*.

Kaspersky. (s.f.). *Malware & Computer Virus Facts & FAQs*. https://usa.kaspersky.com/resource-center/threats/computer-viruses-and-malware-facts-and-faqs

Kumar, R., Vaidya, V. K. (2016). Computer Network - Application Layer Protocol. *International Journal of Advanced Research*, *4*(6), 51-63.

Kumari, A., Agrawal, N., Lilhore, U. (2017). Attack over Email System: Review. *International Journal of Scientific Research & Engineering Trends*, *3*(5), 200-206.

Levchenko, V. I. (2017). *System and Method for Configuring Antivirus Scans*. Google Patents.

Lopez, E., Mihelich, J., Hepburn, M. F. (2016). *Load Balancing among a Cluster of Firewall Security Devices*. Google Patents.

MailCleaner. (2020). *About*. https://www.mailcleaner.org/about/

Montesino, R, Baluja, W., Porvén, J. (2013). Gestión automatizada e integrada de controles de seguridad informática. *RIELAC, XXXIV*(1), 40-58.

Nightingale, S. (2017). *Email Authentication Mechanisms: DMARC, SPF and DKIM*. Technical Note (NIST TN), National Institute of Standards and Technology. https://doi.org/https://doi.org/10.6028/NIST.TN.1945

Niyaz, Q., Sun, W., Javaid, A., Alam, M. (2016). A Deep Learning Approach for Network Intrusion Detection System. *EAI*, *16*(9), e2. https://doi.org/10.4108/eai.3-12-2015.2262516

OSSEC. (s.f.). *OSSEC*. https://www.ossec.net/

Pal, R. (2019). Cyber Security in Banks. *Staff Paper Series*, *4*(1), 1-31.

Proxmox. (2020). *Proxmox Mail Gateway*. https://www.proxmox.com/en/proxmox-mail-gateway

RFC. (s.f.). *Official Internet Protocol Standards*. https://www.rfc-editor.org/standards

Scott, R., Simson, L., & Garfinkel, R. C. (2019). Trustworthy Email. *NIST Special Publication 800-177 Revision 1*, IV. https://doi.org/10.6028/NIST.SP.800-177r1

Skwarek, M., Korczynski, M., Mazurczyk, W., Duda, A. (2019). Characterizing Vulnerability of DNS AXFR Transfers with Global-Scale Scanning. *IEEE Security and Privacy Workshops (SPW)*, 193-198. https://doi.org/10.1109/spw.2019.00044

Snort. (s.f.). *Snort*. https://www.snort.org/

Stewart, A., Zarakhovsky, E., Palow, C., Gowda, C., Dorman, B. (2016). *Methods and Systems of Classifying Spam URL*. Google Patents.

Tiwari, A., Ansari, A., Dubey, R. (2018). An Effective Email Marketing using Optimized Email Cleaning Process. *International Journal of Computer Sciences and Engineering*, *6*(4), 277-285. https://doi.org/10.26438/ijcse/v6i4.277285

Tolosa, G., Fernández, M. (2016). *HTTP/2. Un nuevo protocolo para la web*. Universidad Nacional de Luján, Argentina.

Viera, A., Pérez, I. (2014). *Estrategia para la migración de servicios de correo electrónico en Cuba*. Tesis de Maestría. Universidad de las Ciencias Informáticas, Cuba.

Zimbra.(2020).*ZimbraCollaborationPostscreen*.https://wiki.zimbra.com/wiki/Zimbra_Collaboration_Postscreen