IV Conferencia Científica Internacional
Universidad de las Ciencias Informáticas

Temática: II Taller Internacional de Ciberseguridad

Guía para gestionar la seguridad del servicio de correo electrónico en la plataforma colaborativa Zimbra

Guide to manage the security of the email service on the Zimbra collaborative platform

Dairis Almaguer Pérez [1*], Adrian Hernández Yeja [2], Raydel Montesinos Perurena[3], Joelsy Porvén Rubier[4]

[1]Especialista en Seguridad Informática. Universidad de las Ciencias Informáticas. Carretera a San Antonio de los Baños km 2 ½, reparto Torrens, La lisa, La Habana. dairis@uci.cu.
[2]. Máster en Ciencias. Universidad de las Ciencias Informáticas. Carretera a San Antonio de los Baños km 2 ½, reparto Torrens, La lisa, La Habana. ayeja@uci.cu.
[3]. Doctor en Ciencias. Universidad de las Ciencias Informáticas. Carretera a San Antonio de los Baños km 2 ½, reparto Torrens, La lisa, La Habana. raydelmp@uci.cu.
[4]. Máster en Ciencias. Universidad de las Ciencias Informáticas. Carretera a San Antonio de los Baños km 2 ½, reparto Torrens, La lisa, La Habana. jporven@uci.cu.

[*] Autor para correspondencia: dairis@uci.cu.

Resumen

Actualmente el correo electrónico es uno de los servicios más afectados por los problemas de seguridad que proliferan, 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, disponibilidad y que minimice los riesgos de la suplantación de identidad, los correos no deseados y los llamados correos spam. Entre los servicios telemáticos de mayor impacto a nivel internacional, por su amplia utilidad e importancia, se encuentra el correo electrónico, el cual requiere una amplia gama de configuraciones de seguridad con el objetivo de proteger la información que viaja a través de los mensajes. El objetivo de la presente investigación es describir una guía de configuraciones y buenas prácticas de seguridad para el servicio de correo electrónico utilizando la plataforma colaborativa Zimbra. Para ello se aplican estándares, buenas prácticas y la automatización como proceso clave para el logro del objetivo propuesto. De esta manera se contribuirá a disminuir la exposición a amenazas y ataques de seguridad asociados a este servicio y por consiguiente en una mayor seguridad de la información de los

usuarios que utilizan este servicio. Se consultaron expertos que validaron la guía propuesta y se utilizó el software de automatización Ansible para su aplicación práctica. La guía fue aplicada para el servicio de correo electrónico de la Universidad de las Ciencias Informáticas.

Palabras clave: *automatización, correo electrónico, seguridad, vulnerabilidades, Zimbra.*

Abstract
E-mail is currently one of the services most affected by the proliferating security problems, both on the Internet and in local or intranet networks. The specialists in telematic services of the organizations have the great challenge of providing an email service that guarantees its stability, availability and minimizes the risks of identity theft, unwanted emails and so-called spam emails. Among the telematic services with the greatest international impact, due to its wide utility and importance, is electronic mail, which requires a wide range of security settings in order to protect the information that travels through messages. The objective of this research is to describe a configuration guide and good security practices for the email service using the Zimbra collaborative platform. For this, standards, good practices and automation are applied as a key process to achieve the proposed objective. In this way, it will help to reduce the exposure to threats and security attacks associated with this service and consequently in a greater security of the information of the users who use this service. Experts were consulted who validated the proposed guide and Ansible automation software was used for its practical application. The guide was applied to the e-mail service of the University of Informatics Sciences.

Keywords: *automation, email, security, vulnerabilities, Zimbra.*

Introducción

En la actualidad los 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. Para gestionar este servicio son necesarios varios programas, que 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 para que intrusos accedan a ellos. Otro de los problemas es el uso de protocolos no cifrados que permiten que la información viaje en texto plano, lo que permite que sea visible para personas malintencionadas y estas la utilicen para acceder a los servidores o para utilizarlos para realizar ataques a terceros. Por otro lado, las prestaciones o posibilidades de cada uno de ellos son diferentes, todos no 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 antes mencionadas, 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.

Es por ello que la gestión de la seguridad en este servicio constituye un reto para los especialistas en servicios telemáticos de las organizaciones, que tienen la difícil tarea de proveer un servicio de correo electrónico que garantice su estabilidad, 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.

A nivel internacional hay normas y regulaciones para la gestión de la seguridad del servicio de correo electrónico, enfocadas de forma teórica a qué medidas se deben tener en cuenta, mas no en cómo implementarlas y menos en como automatizarlas para que se realice este proceso con mayor eficacia y en un menor tiempo. Ejemplos de estas normas son los Request for comment (RFC por sus siglas en inglés) (RFC, 2020), la resolución 121/2017 del Ministerio de las comunicaciones (MINCOM), que norma 16 medidas para la seguridad del correo electrónico (Ramos, 2017), entre otras.

A pesar de la utilidad e importancia que tienen estas normas, regulaciones o configuraciones de seguridad conocidas e implementadas en su mayoría por los administradores de este servicio, cabe destacar que diariamente se descubren nuevas vulnerabilidades, aplicaciones que dejan de tener soporte y distintos mecanismos para atacar estos problemas de seguridad. Por ello, las medidas de seguridad y la gestión de las mismas también deben evolucionar en el tiempo. El proceso de gestión en el servicio de correo electrónico nunca se considera suficiente sino mejorable o actualizable.

Por lo antes expuesto, los autores deciden realizar una investigación sobre todas las medidas que puedan ser implementadas para enriquecer el proceso de gestión de la seguridad del servicio de correo electrónico, con enfoque en la plataforma colaborativa Zimbra, la cual tiene flexibilidad en la aplicación de controles de seguridad automatizables, es software de código abierto, soporta una arquitectura multiservidor y tiene la posibilidad de integrarse con sistemas que la complementan en seguridad y usabilidad (Zimbra, 2020).

Materiales y métodos o Metodología computacional

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. Se utilizó el **histórico - lógico** para determinar los antecedentes relacionados con el servicio de correo electrónico, así como problemas de seguridad que existen desde su surgimiento; el **analítico – sintético** para la investigación de los servicios de correo, así como las herramientas y tecnologías para la gestión y configuración segura de los servicios de correo electrónico; el **hipotético - deductivo** para el análisis de la información derivada del uso de otros métodos y de los componentes que conforman el objeto de investigación. También se utilizó el método empírico **criterio de expertos,** con el objetivo de conocer según la experiencia y conocimiento de los expertos seleccionados, si la propuesta de solución cumple con las expectativas y responde al problema planteado.

Se tomaron en cuenta fundamentos necesarios para la seguridad del servicio de correo electrónico en componentes como los agentes que intervienen en el mismo (MUA, MSA, MDA, MTA) (Kumari, Agrawal, and Lilhore, 2017), protocolos y estándares conocidos ((E)SMTP, LMTP, POP3, IMAP, MIME, SSL/TLS, STARTTLS, HTTP) (Rose, Nightingale, Garfinkel, and Chandramouli, 2017) (Shitole and Divekar, 2019) (Dumka, Tomar, Patni and Anand, 2014) (RFC, 2020). De esta forma, se logró un entendimiento de los componentes del correo electrónico que deben protegerse utilizando técnicas y estándares conocidos. También, se estudiaron los ataques a través del servicio de correo electrónico, los cuales pueden 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. Estos se clasifican en malware, spam, phishing, modificación de mensajes, ingeniería social, ransomware, spoofing (Kaspersky 2020) (Basavaraju, 2010) (Butavicius, Parsons, Pattinson and McCormac, 2016) (Babu, 2010). Otros tipos de ataques incluyen a los de infraestructura, como son la denegación de servicio y el envenenamiento de caché de servidores DNS (Pal, 2019) (Hurtado y Sarango 2017).

Se tomaron en cuenta estándares y regulaciones internacionales relacionadas con el correo electrónico. Entre las principales se encuentran:

- Request for comment (RFC por sus siglas en inglés), específicamente las publicaciones 2595, 3207, 5246, 6376, 8617, 2045, 2046 y 2047 (RFC, 2020).
- Resolución 121 del MINCOM enfocada al servicio de correo electrónico (Ramos, 2017).

La solución presentada tiene en cuenta mecanismos necesarios para gestionar la seguridad del correo electrónico de forma automatizada. Estos mecanismos se enfocan en combatir el spam y virus, los intrusos en la red, diseño de la infraestructura de red, monitorización, entre otros. Con la utilización de herramientas de automatización se permite la reducción de los costes de producción, la reducción de los residuos, la mejora de la calidad y la fiabilidad y la reducción drástica de los accidentes laborales. Se utilizó en ese sentido Ansible, la cual es una herramienta simple, flexible y extremadamente poderosa que le brinda la capacidad de automatizar tareas de infraestructuras comunes, ejecutar comandos e implementar aplicaciones de varios niveles que abarcan varias máquinas (Ansible, 2020).

Resultados y discusión

Se obtuvo una guía que se basa en la descripción de los parámetros de seguridad que se definen en una lista de chequeo elaborada por los autores, basado en las publicaciones y estándares estudiados. En esta lista se identifican los parámetros de seguridad con que debe contar la guía. Todos los parámetros serán formalmente escritos en la guía, la cual está dividida en dos etapas, la etapa 1 está enfocada a la preparación de un entorno seguro y gestión de la seguridad durante el despliegue de la infraestructura de correo y la etapa 2 a la gestión de la seguridad durante la ejecución de este servicio. Cada una de las etapas está compuesta por un grupo de actividades y estas a su vez por tareas que definen explícitamente cuáles son las configuraciones a ejecutar para gestionar adecuadamente la seguridad de este servicio. Además, por cada tarea se especifica cuál o cuáles son los roles que intervienen en la ejecución de las mismas, si son o no automatizables, o incluso puede ser que sean automatizadas parcialmente y el nivel de importancia de la tarea dada por (Necesario o Recomendado). Las configuraciones necesarias son aquellas que no pueden faltar en la gestión de la seguridad de correo, las recomendadas son aquellas que constituyen una mayor seguridad del servicio de acuerdo a la criticidad del mismo. En la **Figura 1** se ilustra la estructura general de la guía.

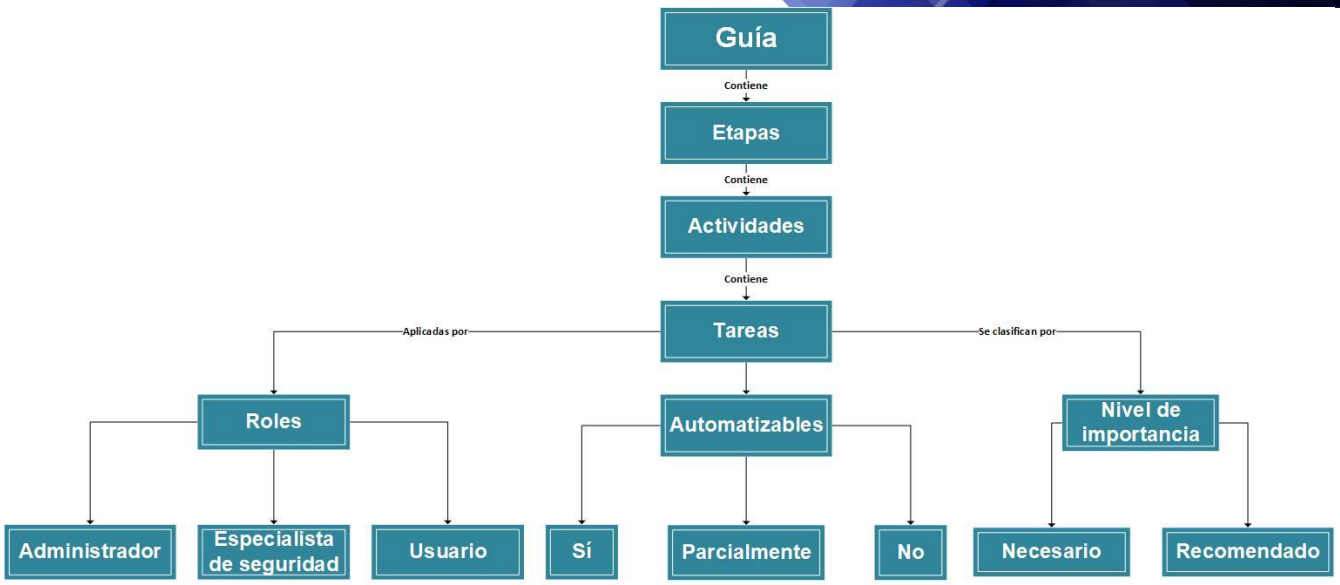

Figura 1: Estructura de la guía propuesta. (Fuente: elaboración propia).

En la Tabla 1 se presenta un resumen de la guía propuesta, teniendo en cuenta todos los elementos que la componen y la relación entre ellos.

Etapas	Actividades	Tareas	Roles	Nivel de importancia	Automatizable
Etapa 1: elementos para gestionar la seguridad durante el despliegue	Diseñar y preparar un entorno seguro para el despliegue del servicio de correo electrónico	Definir la separación lógica de los servidores que componen el correo en la DMZ	Administrador / Especialista de seguridad	Recomendado	No
		Diseñar el despliegue multiservidor	Administrador	Recomendado	No
		Definir configuraciones y parámetros de seguridad requeridos	Administrador / Especialista de seguridad	Necesario	No

		Ajustar configuraciones de seguridad de servidores en el sistema operativo	Administrador	Necesario	Sí
	Instalar y configurar herramientas para la seguridad del servicio de correo electrónico	Configurar cortafuego en los servidores	Administrador	Necesario	Sí
		Instalar actualizaciones del sistema operativo.	Administrador	Necesario	Parcialmente
		Instalar y configurar sistema de detección de intrusos de host	Administrador	Recomendado	Sí
		Configurar herramientas antivirus y antispam	Administrador	Necesario	Sí
		Configurar cortafuego e IDS en el borde de la red	Administrador	Necesario	Parcialmente
		Instalar y ajustar herramientas para el monitoreo	Administrador	Necesario	Sí
		Configurar salvas	Administrador	Necesario	Sí
		Configurar trazas	Administrador	Necesario	Sí
	Gestionar seguridad en la DMZ	Configurar seguridad en el MTA	Administrador	Necesario	Sí

	Ajustar parámetros de seguridad de Zimbra	Realizar configuraciones contra la denegación de servicio para protocolos usados en el correo electrónico	Administrador	Necesario	Sí
		Establecer mecanismos para que la comunicación sea segura	Administrador	Necesario	Sí
		Ajustar parámetros inseguros por defecto de Zimbra	Administrador	Necesario	Sí
Etapa 2: elementos para gestionar la seguridad durante su utilización	Gestionar la seguridad	Realizar análisis de vulnerabilidades	Administrador / Especialista de seguridad	Necesario	Parcialmente
		Realizar monitoreo del servicio	Administrador / Especialista de seguridad	Necesario	No
		Realizar chequeo de trazas	Administrador / Especialista de seguridad	Recomendado	No
		Realizar chequeo de salvas	Administrador / Especialista de seguridad	Recomendado	No
		Describir elementos de seguridad que deben implementar los usuarios	Especialistas de seguridad / Usuarios	Necesario	No

		Resolver incidentes de seguridad	Administrador / Especialista de seguridad	Necesario	No

Tabla 1. Guía para la gestión de la seguridad en el servicio de correo electrónico (Fuente: elaboración propia).

Para la validación de la guía se utilizó el método científico criterio de expertos. Para la implementación del mismo, se seleccionaron 13 expertos que valoraron de **Muy Adecuada** la propuesta, evidenciando de esta manera el nivel de pertinencia de la propuesta de solución.

Para automatizar las configuraciones de seguridad se implementaron *playbooks* utilizando la herramienta de automatización Ansible. En primer lugar, se automatizó la lista de chequeo con el objetivo de comprobar las configuraciones de seguridad que tiene en la variante por defecto la plataforma colaborativa de Zimbra. En segundo lugar, se automatizaron las configuraciones de seguridad seleccionadas por los autores como automatizables por separado: las necesarias, las recomendadas o ambas, permitiendo que el administrador que desee usar ese *playbook* ejecute las configuraciones que desee. Para la comprobación de los mismos se montó un entorno de prueba, donde se realizó un despliegue del servicio de correo utilizando Zimbra en su instalación por defecto. Luego de haber instalado el servicio, se ejecutó el *playbook* de chequeo de las configuraciones de seguridad donde se detectaron configuraciones de seguridad incorrectas. Luego se ejecutó el *playbook* de aplicación de configuraciones y, en tercer lugar, se volvió a ejecutar el *playbook* de chequeo donde se pudo observar que las configuraciones fueron aplicadas correctamente.

Luego de la validación de la guía propuesta, se aplicó la misma en la Universidad de las Ciencias Informáticas, obteniendo resultados satisfactorios.

Conclusiones

En este trabajo se desarrolló una guía para gestionar la seguridad del servicio de correo electrónico para la plataforma colaborativa de Zimbra, basado en configuraciones y buenas prácticas con un enfoque hacia la automatización. Del trabajo realizado se obtuvieron las siguientes conclusiones:

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

- La identificación y estudio de los principales problemas de seguridad asociados a este servicio y las regulaciones internacionales y nacionales relacionadas a la seguridad de este servicio contribuyó, en una mejor visión de cuáles son los elementos a tener en cuenta para la elaboración de la propuesta de solución y gestionar adecuadamente la seguridad de este servicio.

- La aplicación práctica de la guía en el servicio de correo electrónico de la Universidad de las Ciencias Informáticas permitió la automatización de las configuraciones de seguridad que se aplican manualmente y posibilitó minimizar los riesgos asociados a la ocurrencia de errores humanos durante la ejecución de las operaciones de seguridad y en un menor tiempo de ejecución de las mismas.

- Se sugiere extender esta propuesta de solución a otras instituciones del país donde se utilice la plataforma colaborativa de Zimbra, adaptándolo a sus necesidades.

Referencias

Ansible. (2020). Why Ansible? Recuperado de: https://www.ansible.com/overview/it-automation

Babu, P. R., Bhaskari, D. L., & Satyanarayana, C. H. (2010). A comprehensive analysis of spoofing. International Journal of Advanced Computer Science and Applications, 1(6), 157-62.

Basavaraju, M., & Prabhakar, D. R. (2010). A novel method of spam mail detection using text based clustering approach. International Journal of Computer Applications, 5(4), 15-25.

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. arXiv preprint arXiv:1606.00887.

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).

Hurtado, M. E. C., & Sarango, D. J. A. (2017). Análisis de Certificados SSL/TLS gratuitos y su implementación como Mecanismo de seguridad en Servidores de Aplicación. Enfoque UTE, 8, 273-286.

Kaspersky. (2020). Malware & Computer Virus Facts & FAQs. Recuperado de: https://usa.kaspersky.com/resource-center/threats/computer-viruses-and-malware-facts-and-faqs.

Kumari, A., Agrawal, N., & Lilhore, U. (2017). Attack over email system. International Journal of Scientific Research & Engineering Trends, 3(5), 200-206.

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

Ramos, M. M. (2017). Resolución 57 de 2017 de Ministerio de Comunicaciones.

RFC. (2020). Official Internet Protocol Standards. Recuperado de: https://www.rfc-editor.org/standards

Rose, S., Nightingale, S., Garfinkel, S., & Chandramouli, R. (2017). Trustworthy Email (2nd Draft) (No. NIST Special Publication (SP) 800-177 Rev. 1 (Draft)). National Institute of Standards and Technology.

Shitole, H. P., & Divekar, S. Y. (2019). Secure Email Software using e-SMTP.

Zimbra. (2020). Best Practices for personal email security. Recuperado de: https://s3.amazonaws.com/files.zimbra.com/website/docs/Zimbra_Email_Security_Checklist-Whitepaper-2017.pdf