FORTINET
NSE Training Institute

NSE 2 Secure Email Gateway Scripts—Spanish Version

¡Hola! En esta clase, veremos qué es una puerta de enlace de correo electrónico segura y cómo ha evolucionado.

El correo electrónico fue uno de los primeros servicios utilizados cuando el mundo se conectó a la red en la década de los noventa. Ocupaba un ancho de banda muy pequeño porque la tecnología permitía un uso limitado. Además, era rápido y fácil de usar, y ni siquiera había que comprar un sello postal. De hecho, era tan sencillo y económico que se convirtió en un medio para enviar mensajes a muchas personas, con un precio muy bajo o de forma gratuita.

Algunos correos masivos provenían de empresas legítimas y equivalían a folletos publicitarios recibidos por correo postal, pero otros eran enviados por individuos malintencionados. Así comenzó el envío de correo basura o spam, es decir, mensajes irrelevantes o no solicitados a través de internet y a una gran cantidad de destinatarios.

Era posible enviar y recibir mensajes que no estaban debidamente verificados o por los que no se rendían cuentas. Así, se podía permanecer en el anonimato. Al principio, el spam se consideraba una molestia y no tanto una amenaza. Pero, en 1996, la empresa America Online (AOL) acuñó el término *phishing*, en referencia a la práctica fraudulenta de enviar correos electrónicos de una fuente que aparenta ser confiable, pero que tiene el objetivo de que los usuarios revelen información personal.

Por ejemplo, muchos conocerán al príncipe Salomón, de Abadodo, o a algún otro personaje sagaz que quería compartir su riqueza con ustedes. Otros agentes maliciosos registraban dominios con un nombre que era muy parecido al de una empresa u organización legítima. Luego, enviaban un correo electrónico en el que se hacían pasar por ella y persuadían al destinatario de que hiciera clic en un enlace o un adjunto que contenía un *malware*.

El *phishing* o correo de suplantación de identidad funcionaba debido a la ingenuidad, el descuido o la distracción de las personas. Una de las primeras respuestas de las empresas fue capacitar a los empleados acerca de esta técnica. Sin embargo, la capacitación pudo haber reducido este tipo de prácticas, pero no eliminó la amenaza. Había que hacer algo en el

servidor de correo o en el proveedor de servicios de internet (*internet service provider*, ISP). A modo de solución, las empresas instalaron filtros en los servidores de correo para prevenir el spam y el *phishing*.

Los filtros antispam identificaban palabras o patrones específicos en el encabezado o el cuerpo de los mensajes. Para nombrar un ejemplo sencillo, "dinero" es una palabra que suele aparecer en los mensajes de spam. Si un profesional de TI de una empresa agregaba ese término en el filtro antispam del servidor de correo, todo mensaje que contuviera esa palabra se eliminaba.

Los proveedores de servicios de internet también implementaron filtros antispam. Además, adoptaron medidas para fortalecer los métodos de autenticación. Hacia fines de la primera década del siglo XXI, los proveedores de servicios de internet pusieron en marcha el marco de directivas de remitente (*Sender Policy Framework*, SPF), que poco a poco tomó forma en dicho período, aunque recién en 2014 se lo propuso como estándar.

El SPF es un método de autenticación de correo electrónico que detecta remitentes y mensajes falsos.

Sin embargo, cada vez que las empresas, organizaciones y proveedores de servicios de internet adoptaban una medida defensiva, los atacantes respondían con otra que lograba burlarla.

Retomemos el ejemplo anterior: quienes enviaban spam podían usar la palabra "diner0" u otra similar, en lugar de la grafía correcta, y así evadir el filtro. Y si bien los filtros eran cada vez más sofisticados a la hora de detectar patrones de spam, seguían siendo muy estáticos y fáciles de engañar.

El envío de spam y *phishing* es muy lucrativo para que los atacantes se den por vencidos fácilmente. De hecho, la cantidad de ataques de *phishing* ha crecido de manera significativa desde principios de siglo. En 2004, se registraron 176 ataques únicos. En 2012, el número se elevó a 28 000. Esto no fue una sorpresa: era un método lucrativo. Entre daños y pérdidas en dinero, los atacantes ocasionaron perjuicios por 500 millones de dólares a empresas e

individuos. Hace poco, en el primer trimestre de 2020, el consorcio internacional Anti-Phishing Working Group (APWG) detectó 165 772 sitios dedicados al *phishing*.

Por eso, eran necesarias medidas más eficaces. Las puertas de enlace de correo electrónico seguras surgieron para brindar una defensa más rigurosa. Además del filtro antispam, incorporaron escáneres antivirus, la simulación de amenazas o el entorno seguro de *sandbox* para detectar adjuntos y enlaces maliciosos en tiempo real. Incluso si la capacitación del personal y el filtro antispam fallaban, una de estas herramientas podía detectar y neutralizar la amenaza. Sin embargo, la cantidad de falsos positivos y el gran volumen de ataques fueron demasiado para los equipos de seguridad, quienes se encontraron inmersos en tareas de remediación manual.

Las puertas de enlace de correo electrónico seguras continúan evolucionando a la par de las amenazas.

Hoy en día, el aprendizaje automático y una mayor automatización se utilizan para asegurar estas puertas de enlace, lo que simplifica el trabajo en los centros de operaciones de seguridad. Los sistemas de prevención de pérdidas de datos (*data loss prevention*, DLP) también pueden detectar y detener la salida de información confidencial.

En ocasiones, una puerta de enlace de correo electrónico segura se integra con otros dispositivos de seguridad de red, como el firewall perimetral o el de segmentación. En conjunto, estos dispositivos conforman un tejido de seguridad integrado que los profesionales pueden administrar de manera central y desde un único panel. Además, pueden actualizarse continuamente por medio de la información sobre amenazas, a medida que se conocen nuevos métodos y contagios.

Fortinet ofrece una puerta de enlace de correo electrónico segura conocida como FortiMail®. FortiMail® incluye todas las características mencionadas y además se integra con soluciones de firewall y *sandbox*. Administre todos estos dispositivos de manera centralizada con

FortiManager® y actualice la información sobre amenazas mediante FortiGuard® Labs, el centro global de Fortinet para la información e investigación sobre amenazas.

Gracias por su tiempo, y no olvide responder las preguntas a continuación.