Estrategias para evitar ataques de Phishing en Empresas

Lourdes Isabel Chambi Machaca
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
luchambim@gmail.com

***Resumen*—El phishing y las estafas son llevadas a cabo por personas malintencionadas, estos encuentran diferentes medios para acceder a información confidencial, privada o de uso interno de diferentes empresas, como ser el envío de mensajes de correo electrónico, documentos con spyware, aprovechar vulnerabilidades en los sistemas de información y comunicación, mensajes de texto, utilizar la ingeniería social u otros medios pueden utilizarse para distribuir información errónea, obtener ganancias financieras ilícitas y buscar información personal y sensible de una víctima. Los empleados víctimas de los ataques pueden exponer datos críticos de la empresa o personal ubicados no sólo en su propia computadora, sino en toda una red y así robar credenciales de acceso, directorios de correos electrónicos corporativos, números de cuenta, números de Seguro Social, entre otra información, estos métodos se encuentran desde hace mucho tiempo, siendo los más populares y eficaces utilizados por los ciberdelincuentes, Si estos consiguen esa información, podrían acceder a su cuenta de email, banco u otras cuentas y lograrían su objetivo de dañar a una empresa, desde afectar su imagen y generar pérdidas económicas que dependiendo a su impacto, estas pueden concluir en el cierre de la misma.**

Palabras clave—ataque, informática, información, phishing, riesgos, sistemas, tecnología.

I. Introducción

En los últimos años, se presenta un incremento de noticias sobre fraudes, ataques cibernéticos y amenazas en la red, los cuales alcanzan tanto a particulares como a empresas, se ha demostrado la importancia de generar conciencia social sobre la necesidad de proteger la identidad digital de las personas, prevenir los fraudes y mantener la privacidad de la información.

Entre las amenazas que vienen ganando las primeras posiciones en las detecciones de las diferentes soluciones que ofrecen las empresas de seguridad, se ubican las relacionadas con el criptojacking4. El aumento en la cotización de algunas divisas digitales ha generado una especie de "fiebre por las criptomonedas", en la que la minería no solo es llevada a cabo por las personas que intentan ganar dinero de manera legítima. Los cibercriminales aprovechan esta situación desarrollando amenazas y provocando ataques para apropiarse de las monedas digitales, o bien, utilizando los recursos de cómputo de los usuarios de Internet, que de manera involuntaria contribuyen a la minería para beneficios de terceros [1].

A. *Problemática*

Se cuentan con diferentes reportes e informes de seguridad que son realizados por empresas de seguridad informática a nivel región Latinoamérica, permite tener un panorama general para entender qué prácticas se están llevando a cabo, cuáles son sus preocupaciones y cómo trabajan para proteger la infraestructura tecnológica, comunicaciones y activos en seguridad de la información, informática y ciberseguridad.

La empresa Cisco en su reporte anual del año 2018 indica que no importa cuánto cambie el panorama de las amenazas, el correo electrónico malicioso y el correo no deseado siguen siendo herramientas vitales para que los adversarios distribuyen malware porque llevan las amenazas directamente al punto final. Al aplicar la combinación correcta de técnicas de ingeniería social, como phishing y enlaces maliciosos y archivos adjuntos, los adversarios solo tienen que sentarse y esperar a que los usuarios desprevenidos activen sus exploits [2].

El laboratorio de investigación *VU Labs* como resultado del reporte de ciberseguridad anual realizados entre 2018 y 2019 sobre las amenazas online que se perciben con mayor frecuencia, el 88,4% destaca el phishing y el 82,2% menciona al malware, mientras que el 58,2% se refiere al ransomware. La percepción se mantiene constante a través de los diferentes países latinoamericanos encuestados [3].

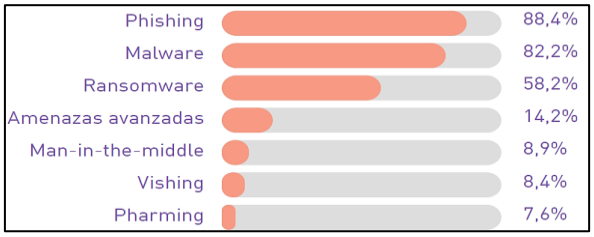

Fig. 1. Ataque cibernético más frecuente. Fuente: VU Labs

Los adversarios están llevando el malware a niveles de sofisticación e impacto sin precedentes. El número y la variedad es cada vez mayor de tipos de malware y familias que perpetúan el caos en el panorama de ataque al socavar los esfuerzos de los defensores para ganar y mantener el terreno ante las amenazas.

B. *Objetivos*

De acuerdo a lo detallado en líneas precedentes y mediante los reportes se pudo evidenciar que el método más utilizado por los ciberdelincuentes para el robo de información, vulneración

Para referenciar este artículo (IEEE):
[N] L. Chambi, «Estrategias para evitar ataques de Phishing en Empresas,» *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 7, pp. 65-68, 2020.

de sistemas de información y comunicación es el Phishing. En ese entendido, es que la investigación científica tiene el siguiente objetivo: "Proponer estrategias para minimizar riesgos de ataques de Phishing a empleados en empresas".

C. Hipótesis

La aplicación de estrategias minimizará los riesgos de ataques de *Phishing* a empleados en empresas.

II. Marco teórico

A. Que es el Phishing

El phishing es un método que los ciberdelincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndose a un sitio web falso [4].

El término Phishing es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndose a un sitio web falso.

El estafador, conocido como phisher, se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico, o algún sistema de mensajería instantánea, redes sociales SMS/MMS, a raíz de un malware o incluso utilizando también llamadas telefónicas.

B. Procedencia del Phishing

Los mensajes de *phishing* parecen provenir de organizaciones legítimas como PayPal, UPS, una agencia gubernamental o su banco. Sin embargo, en realidad se trata de imitaciones. Los correos electrónicos solicitan amablemente que actualice, valide o confirme la información de una cuenta, sugiriendo a menudo que hay un problema. Entonces se le redirige a una página web falsa y se le embauca para que facilite información sobre su cuenta, lo que puede provocar el robo de su identidad [4].

C. ¿Cómo funciona el Phishing?

Los ataques de phishing usan las redes sociales conectadas al correo electrónico como LinkedIn, Facebook y Twitter para recopilar información sobre la persona, su trabajo, sus intereses y sus actividades. Esta información la usan para crear un correo electrónico creíble que contenga un enlace o archivo adjunto malicioso [4].

Aunque muchos correos electrónicos de phishing están mal escritos y son claramente falsos, cada vez se van mejorando. Algunos atacantes ya usan las mismas técnicas que los profesionales del marketing para identificar los tipos de mensajes más efectivos.

Por lo general, la víctima recibe un mensaje que parece haber sido enviado por un contacto u organización conocida. El ataque se lleva a cabo a través de un archivo adjunto malicioso que contiene un software de suplantación de identidad o mediante enlaces que se conectan a sitios web maliciosos.

El objetivo de estos enlaces es instalar un malware en el dispositivo o dirigir a la víctima a un sitio web malicioso configurado para engañarlos y divulgar información personal y financiera, como contraseñas, identificaciones de cuenta o detalles de la tarjeta de crédito [5].

D. ¿Cómo reconocer el Phishing?

Los estafadores suelen actualizar sus tácticas, pero hay algunos indicios que ayudarán a reconocer un email o mensaje de texto de tipo phishing.

Puede que los emails y mensajes de texto phishing parezcan enviados por una compañía conocida o en la cual la empresa confía. Pueden tener el mismo aspecto que los mensajes enviados por un banco, una compañía de tarjeta de crédito, un sitio de redes sociales, un sitio web o aplicación de pagos en línea o una tienda en línea [5].

A menudo, en los emails y mensajes de texto phishing le cuentan una historia para engañarlo y lograr que usted haga clic en un enlace o abra un archivo adjunto. Los mensajes podrían:

- Decir que se ha detectado alguna actividad sospechosa o intentos de inicio de sesión.
- Afirmar que hay un problema con su cuenta o con su información de pago.
- Decir que debe confirmar algunos datos personales.
- Incluir una factura falsa.
- Pedirle que haga clic en un enlace para hacer un pago.
- Decir que usted es elegible para registrarse para recibir un reembolso del gobierno.
- Ofrecerle un cupón para algo gratis.

E. Los usuarios y Phishing

Siendo el phishing el ataque online más frecuente, la prevención de fraude y la protección de la identidad adquieren cada vez mayor importancia. En el último año, los ataques automatizados a corporaciones fueron noticia más de una vez, al causar el robo de datos de miles de millones de usuarios alrededor del mundo [7].

La autenticación de doble factor de autenticación se consolida como una herramienta fundamental para proteger la identidad de los usuarios, seguida de cerca por el análisis de patrones de comportamiento, que facilita la validación de la identidad y la obtención de información adicional para verificar movimientos sospechosos e inusuales.

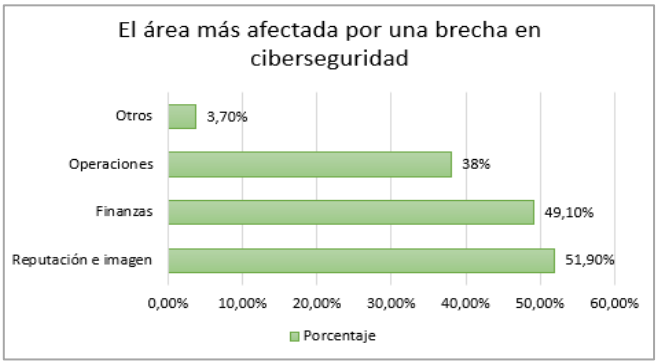

Fig. 2. El área más afectada por una brecha en ciberseguridad.
Fuente: Elaboración propia

F. Ingeniería social

Siendo el phishing el ataque online más frecuente, la prevención de fraude y la protección de la identidad adquieren cada vez mayor, la ingeniería social sigue siendo una plataforma crítica para el lanzamiento de ataques de correo electrónico.

El phishing y el spear phishing son tácticas usadas para robar las credenciales de los usuarios y otra información sensible y eso se debe a que son muy efectivas. De hecho, los correos electrónicos de phishing y spear phishing fueron la raíz de algunas de las brechas más grandes que acaparan los titulares en los últimos años [7].

Para evaluar cuán prevalecientes son las URL y los dominios de phishing en la Internet de hoy, los investigadores de amenazas de Cisco examinaron datos de fuentes que investigan correos electrónicos potencialmente "phishy" enviados por usuarios a través de inteligencia contra amenazas de phishing basada en la comunidad.

La percepción de los ataques más frecuentes descritos anteriormente coincide con los resultados presentados en diferentes reportes dedicados a estudiar los ataques más frecuentes en empresas de América Latina durante 2019 de acuerdo a la información y reportes de diferentes empresas de seguridad, indican los siguientes ataques como frecuentes:

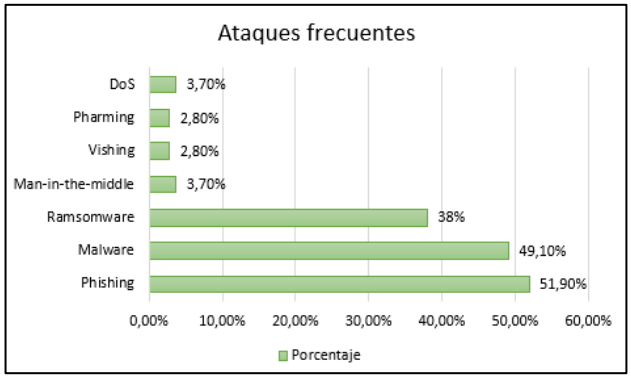

Fig. 3. Ataques frecuentes. Fuente: Elaboración propia

Los ataques de *phishing* siguen siendo tan efectivos en la actualidad. En este sentido, los especialistas identificaron algunos puntos clave para explicar este fenómeno, entre los cuales está: su constante evolución, las técnicas de persuasión que utilizan y el poco conocimiento de los usuarios acerca de qué es el *phishing*.

III. Metodología

La presente investigación es de un enfoque cualitativo. Este es un proceso que recolecta; analiza y vincula datos en un mismo estudio, o una serie de investigaciones para investigar la problemática.

Relevamiento de información: Se utilizaron diferentes reportes e informes de empresas especializadas en seguridad y que cuentan con el reconocimiento, profesionales en el área y laboratorios específicos para realizar las encuestas, entrevistas y estadísticas del resultado de las investigaciones realizadas en diferentes países de la región latinoamericana, como ser Argentina, Bolivia, Chile, Colombia, Costa Rica, Ecuador, España, Guatemala, Italia, México, Panamá, Perú, República Dominicana y Uruguay, entre otros [6].

Adicionalmente, se recolectó y analizó la información del estado actual en cuanto a el conocimiento de los empleados de la empresa que se llevó a cabo entre febrero del 2020 a mayo de 2020:

- Revisión de documentación: Proceder a la revisión de todos los datos recabados en la investigación social, reportes y documentación para obtener resultados que coadyuvará en el avance de la investigación.
- Cuestionarios: Las preguntas de los cuestionarios fueron cerradas y de selección múltiple, dirigido a personal de diferentes áreas, seleccionados aleatoriamente, para obtener el estado actual.
- Entrevistas: Estas fueron dirigidas a personal del área de tecnologías de la información.

La investigación es desarrollada sobre los resultados obtenidos del análisis realizado por las técnicas de investigación y la evaluación de estándares y normas internacionales para la seguridad de la información y así minimizar los ataques de *Phishing* a empleados de empresas. Las estrategias a proponer están sustentadas en los estándares internacionales, buenas prácticas y resultados obtenidos en diferentes reportes publicados por empresas especializadas en seguridad informática. Por otra parte, para definir las estrategias se las realizó en función a los puntos más críticos que fueron detectados en los cuestionarios realizados a diferentes empleados.

IV. Resultados

En las encuestas realizadas a los empleados se obtuvieron los siguientes resultados:

- De acuerdo a los cuestionarios se pudo evidenciar que al menos el 60% de los empleados encuestados no tienen conocimiento del *Phishing*. Cabe indicar que, del 40% que demostró conocer sobre este método, el 30% fue personal del área de tecnologías de la información.
- El resultado de la entrevista a personal del área de Tecnologías de la información demostró que no se cuentan con los equipos en hardware y software suficientes para luchar contra los ataques de *Phishing* como el de la seguridad informática en general.
- Personal del área de tecnologías de la información no tienen reportes y/o informes dedicados a la seguridad informática, por lo cual no se tienen identificadas las vulnerabilidades presentes; asimismo, no se cuenta con personal especializado en seguridad informática.
- La empresa no asigna presupuesto para la seguridad informática que pueda luchar contra los ataques de *Phishing* como también los de *malware, ransomware, man-in-the-middle, DoS, pharming y vishing.*

V. Discusión

Debido al resultado obtenido en los cuestionarios, la educación sigue siendo un factor clave para reducir el número de víctimas de este tipo de ataque. Otro factor clave para reducir el número de víctimas del *phishing* es implementar el uso del doble factor de autenticación en todos los servicios que esté disponible para evitar que terceros puedan acceder a nuestras

cuentas en caso de ser víctimas del robo de credenciales de acceso.

A continuación, se detallan las estrategias propuestas para reducir riesgos de ataques de *Phishing* en función de los resultados obtenidos:

1. Crear un programa de concientización de seguridad que incluya a todos los empleados, en el cual se debe reforzar la concientización en la parte gerencial y empleados que tengan un equipo de computación ubicado en un lugar de acceso por terceros.
2. Realizar un análisis para detectar los altos riesgos y proponer controles para la mitigación de riesgos.
3. Incrementar la inversión en tecnología para la implementación de soluciones tecnológicas de seguridad como defensa.
4. Realizar al menos una vez al año pruebas de pentesting.
5. Incrementar el presupuesto para la capacitación del personal de seguridad informática y/o seguridad de la información.
6. Actualizarse periódicamente sobre la evolución de nuevos métodos de *phishing*.
7. Realizar la división entre el equipo de Tecnologías de información y Seguridad Informática y/o de información.
8. Implementar un servicio de ciberseguridad externo integrado con los servicios core de una empresa.

VI. Conclusiones

Con la ejecución de las estrategias indicadas previamente, se pudo comprobar la hipótesis planteada y minimizar riesgos de ataques de *Phishing* a empleados en la empresa, cumpliendo así con el objetivo propuesto.

Referencias

[1] ESET Security Report 2018. ESET. (18 de junio 2018). Recuperado de https://www.welivesecurity.com/

[2] Cisco Systems (2018). *Cisco 2018 Reporte anual de Ciberseguridad*. Recuperado de https://www.cisco.com

[3] Informe ciberseguridad en entornos digitales. Vu Labs. (2019). Recuperado de https://www.vusecurity.com/

[4] ¿Qué es el Phishing? ESET. (21 de noviembre 2013). Recuperado de https://www.welivesecurity.com/

[5] Phishing. Panda Security. (10 de agosto 2018). Recuperado de https://www.pandasecurity.com/

[6] Latinoamérica registró una media de 9 ciberataques por segundo en doce meses. (15 de agosto de 2018). MercoPress. Recuperado de http://es.mercopress.com

[7] Stephen, F. (25 de abril de 2018). *Lo más destacado del Reporte de Ciberseguridad Cisco 2018*. Blog Cisco Latinoamérica. Recuperado de https://gblogs.cisco.com

Breve CV de la autora

Lourdes Isabel Chambi Machaca es Ingeniera de Sistemas, diplomada en Educación Superior, Auditoría Informática y Seguridad de la Información por el Postgrado en Informática UMSA. Actualmente realiza la Maestría en Informática Forense, Seguridad de la Información y Auditoría Informática en el Postgrado en Informática UMSA. Email: luchambim@gmail.com.