Concientización en Ciberseguridad a través de Ataques de Ingeniería Social

Juan Pablo Conde Mendoza
Posgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
juanpablo.condemendoza76@gmail.com

***Resumen*—En este trabajo, se presenta el contexto del tratamiento de riesgos procedentes de ataques de ingeniería social a través de la exploración de trabajos similares y el estudio de los resultados obtenidos en los mismos, de acuerdo al análisis realizado sobre estas investigaciones, se observó que los criterios de respuesta son limitados en cuanto a la aplicación del tratamiento puesto que se enfocan en grupos específicos, por tanto y en la búsqueda de un medio con enfoque general sobre la optimización de este tipo de riesgos se optó por la elección de la filosofía de concientización de Paulo Freire como medio de tratamiento para los riesgos procedentes de ataques de ingeniería social, por tanto la presente investigación presenta el trabajo de concientización de Paulo Freire en profundidad y su aplicación como modelo de concientización de personas en pro de optimizar el tratamiento de riesgos procedentes de ataques de ingeniería social.**

Palabras clave—ingeniería social, riesgos, concientización ciberseguridad.

I. Introducción

Los principios de seguridad de la información: confidencialidad, integridad y disponibilidad, tienen como principal objetivo proteger la información de la entidad, en la actualidad existen diversos mecanismos de protección a nivel de software y hardware los cuales precautelan la seguridad de la información frente a ciberataques, sin embargo, en la actualidad varios ciberataques tienen como vector principal de ataque a la ingeniería social.

Puesto que no se trata solamente de aplicar controles a los activos tecnológicos sino también precautelar la seguridad del usuario mismo que se encuentra expuesto a riesgos de ciberseguridad procedentes de ataques de ingeniería social.

Como respuesta al riesgo identificado, la presente investigación pretende a través de la propuesta del diseño de un modelo de concientización en ciberseguridad, optimizar el tratamiento de riesgos procedentes de ataques de ingeniería social el cual: Sistematice los fundamentos teóricos referentes a tratamientos de riesgos procedentes de ataques de ingeniería social y caracterice el estado actual de la gestión de riesgos procedentes de ataques de ingeniería social.

II. Ingeniería social

La Ingeniería Social, conocida como la ciencia y arte del engaño a seres humanos, se encuentra en aumento en los últimos años de acuerdo al reporte emitido por Verizon 2018 *Data Breach Investigations Report*, el mismo se debe al crecimiento de las redes sociales, los correos electrónicos y demás formas de comunicación online que posibilitan la utilización de herramientas OSINT (*Open Source Intelligence*), a través de los cuales se perfilan las características de las víctimas.

Referente a los ataques de ingeniería social, se cuentan con diversos tipos trabajos de investigación respecto al análisis de ataques de ingeniería social:

A. Social Engineering Attack Detection Model: SEADMv2

Este trabajo exploró la ingeniería social como dominio y social y caracterizo las técnicas de detección de ataques de ingeniería como proceso dentro de este dominio [1].

B. Towards an ontological model defining the social engineering domain

El Modelo Ontológico de Ataque de Ingeniería Social amplía la clasificación de Ataques de Ingeniería Social al proporcionar seis entidades de un ataque, así como las relaciones entre estas entidades. Este modelo representa actualmente la definición de un ataque de ingeniería social y representa parcialmente la definición de un ingeniero social [2].

C. Generic taxonomy of social engineering attack

En este estudio, los investigadores han revisado y analizado el ataque de la ingeniería social en una vista específica. Además, la discusión sobre el ataque se basa en la perspectiva de la gestión. Este documento ha realizado un análisis preliminar en ambas vistas para generar una taxonomía genérica que agrupa los ataques en las categorías adecuadas. A partir del análisis, se ha propuesto una taxonomía de ataque de ingeniería social que consiste en un ataque de ingeniería social basado en humanos y un ataque de ingeniería social de base técnica. Bajo estas categorías, pocos ataques han sido listados en base a la comparación de ataques. Este artículo es un trabajo preliminar para el mecanismo de defensa de la ingeniería social mediante el uso de un sistema de detección de intrusos [3].

D. A taxonomy for social engineering attacks

En este documento se detallan los diferentes tipos de ataques de ingeniería social a través del enfoque de taxonomía. La cual es útil para que las organizaciones entiendan mejor los vectores de ataque y, en consecuencia, sean útiles para construir contramedidas sólidas y efectivas para las amenazas que imponen. Definitivamente, existe la conciencia del autor de que esta taxonomía puede no estar completa aún en su totalidad. Los

Para referenciar este artículo (IEEE):

[N] J. Conde, «Concientización en Ciberseguridad a través de Ataques de Ingeniería Social,» *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 7, pp. 62-64, 2020.

métodos sociales empleados para sortear las contramedidas tecnológicas son un proceso dinámico en el que el atacante motivado siempre intentará elevar la apuesta inicial contra la víctima.

Los trabajos citados presentan la caracterización de ataques precedentes de ingeniera social y como gestionar los mismos sugiriendo en todos ellos la realización de campañas de concientización [4].

III. Gestión de los riesgos procedentes de ataques de ingeniería social

De acuerdo a todo lo expuesto en los puntos precedentes, es posible sistematizar que los ataques de ingeniería social se encuentran presentes en el día a día y más aún cuando no se cuentan con controles implementados para este tipo de amenazas, por tanto, la gestión de riesgos como proceso inicial de las medidas preventivas es la teoría aplicada para la administración de estos hechos adversos, la cual en su etapa de tratamiento de riesgos debe desarrollar de manera rápida e integra controles efectivos y eficaces ante eventos de posibles ataques de ingeniería social

Dado el nivel de exposición de los usuarios y los posibles impactos como consecuencia de ataques de ingeniería social, lleva al siguiente problema de investigación:

¿Cómo optimizar el tratamiento de riesgos procedentes de ataques de ingeniería social?

Para encarar el presente trabajo investigativo, se realizó una búsqueda referida a trabajos, publicaciones, tesis, artículos, etc. que tomen en cuenta la gestión de gestión de riesgos procedentes de ingeniería social y específicamente la aplicación del modelo de concientización, sobre la misma; se encontró información relacionada de manera directa.

Adicionalmente y respecto del modelo de concientización a elegir para el desarrollo de la investigación, se optó por el método de concientización de Paulo Freire, puesto que, para Freire, la educación es un evento gnoseológico, ejercicio de la libertad, aproximación crítica a la realidad. Esto es así porque su enfoque muestra críticamente la íntima relación y la armonía que deberían existir entre la práctica y la teoría. Freire presenta de manera consistente y explicita las conexiones que existen entre los fundamentos filosóficos y los principios de la práctica educativa.

IV. Trabajos relacionados

Para encarar el presente trabajo investigativo, se realizó una búsqueda referida a trabajos, publicaciones, tesis, artículos, etc. que tomen en cuenta la gestión de gestión de riesgos procedentes de ingeniería social y específicamente la aplicación del modelo de concientización, sobre la misma; se encontró información relacionada de manera directa.

A. Human Exploits in Cybersecurity: A Social Engineering Study

Presenta una idea de investigación, combinada con un diseño único para la ingeniería social, la cual ha dado lugar a una sólida colección de muestras para las cuatro combinaciones de factores que describen la antecedencia de un sujeto a la susceptibilidad de la ingeniería social. Con suficientes puntos de datos, pudieron identificar tendencias y patrones en los datos para determinar estadísticas de resumen dentro y entre las categorías y las preguntas respondidas por los sujetos. Mediante la aplicación de análisis estadísticos, pudieron proporcionar información y resultados significativos. Las implicaciones de los resultados podrán aplicarse a la formación de una mejor capacitación en los sectores corporativo y público, así como tener una aplicación directa en la generación de políticas. Esta investigación también permite la capacidad de continuar la investigación en el campo de la psicología del comportamiento en relación con la seguridad de la información y la ingeniería social [5].

B. Managing Social Engineering Risk

La tesis se divide en investigación teórica y empírica. La investigación teórica se describe de acuerdo con las preguntas de investigación y se verifica durante la investigación empírica.

En el capítulo 6 se analiza la investigación empírica para proporcionar una base sólida para el diseño final de un modelo de gestión de riesgos de ingeniería social. Finalmente, se extraen conclusiones tanto de la investigación teórica como empírica, a partir de la cual se hacen las siguientes recomendaciones. En resumen, las organizaciones aún carecen de una visión general consistente de la ingeniería social. La tesis combina la investigación actual sobre ingeniería social con la investigación en otros campos y la investigación empírica para hacer que la ingeniería social sea transparente para las organizaciones y ayudarles a actuar sobre el riesgo de la ingeniería social [6].

C. Social Engineering and Internal Threats in Organizations

En este documento, se propone un método de dos pasos para reducir la efectividad de los ataques dirigidos a los empleados internos, ya sea mediante el uso de ingeniería social u otras técnicas maliciosas. Este método se basa en el diseño de una política de seguridad correcta y completa que cubra todos los aspectos de la seguridad de la información y el segundo paso consiste en crear un programa de capacitación y concientización sobre la seguridad de los usuarios, en el que los usuarios tomen conciencia del importante papel que desempeñan en el programa de seguridad de la información y la capacitación. Los usuarios son una base regular en vulnerabilidades de seguridad [7].

D. Assessing generational differences in susceptibility to Social Engineering attacks

Los resultados obtenidos permitieron a esta tesis cumplir con su objetivo principal, destacando la importancia de diferenciar a las víctimas de fraudes de ingeniería social en base a la generación en estudios futuros. Mediante un análisis del desempeño de los objetivos en la evaluación de phishing, esta investigación encontró que la generación actual de hoy muestra una mayor probabilidad de ser engañada por los ataques de ingeniería social. Teniendo en cuenta que la fecha de inicio es la misma que la del Sistema de nombres de dominio de Internet, fue sorprendente descubrir que la generación con más conocimientos de Internet es más vulnerable a los ataques de ingeniería social en comparación con la generación de Baby Boomer. Esto implica que solo porque uno tenga conocimiento de las amenazas de ingeniería social, no se vuelva más consciente o menos vulnerable y viceversa [8].

V. La concientización

Para Freire la concientización se define de la siguiente manera:

Proceso de acción cultural a través del cual las mujeres y los hombres despiertan a la realidad de su situación sociocultural,

avanzan más allá de las limitaciones y alienaciones a las que están sometidos, y se afirman a sí mismos como sujetos conscientes y co-creadores de su futuro histórico [9].

En la pedagogía de Freire educar consiste en crear la capacidad de una actitud crítica permanente que permita al hombre captar la situación de opresión a la que se halla sometido y entenderla como limitante y transformable. Una educación liberadora en la que el hombre ha de encontrarse así mismo, aprender a tomar conciencia del mundo que le rodea y a reflexionar sobre él para descubrir las posibilidades de reestructurarlo y modificarlo.

Se optó por el método de concientización de Freire, puesto que, para él la educación es un evento gnoseológico, ejercicio de la libertad, aproximación crítica a la realidad [9]. Esto es así porque su enfoque muestra críticamente la íntima relación y la armonía que deberían existir entre la práctica y la teoría. Freire presenta de manera consistente y explicita las conexiones que existen entre los fundamentos filosóficos y los principios de la práctica educativa.

VI. Modelo de concientización

Freire menciona que tiene que haber relación de la teoría y la práctica; no debe ser únicamente la teoría, sino llevarla a la vida real, a la sociedad en la que el individuo se va a desenvolver y desarrollar, ambos están unidos y no pueden ser separados. Freire a esto le llama en uno de sus principales principios "Práctica-teoría-práctica".

En cada una de ellas, el oprimido define sus problemas, luego reflexiona sobre las causas y, finalmente, actúa; es decir, cumple con las tareas concretas que supone la realización de los objetivos liberadores.

Fase mágica: El oprimido se encuentra en situación de impotencia ante fuerzas abrumadoras que lo agobian y que no conoce ni puede controlar. No hace nada para resolver los problemas. Se resigna a su suerte o a esperar que ésta cambie sola.

Fase ingenua: El oprimido ya puede reconocer los problemas, pero sólo en términos individuales. Al reflexionar sólo logra entender a medias las causas. No entiende las acciones del opresor y del sistema opresivo. En consecuencia, cuando pasa a la acción, adopta el comportamiento del opresor. Dirige su agresión hacia sus iguales (agresión horizontal) o a su familia y, a veces, hacia sí mismo (intrapunición).

Fase crítica: En la fase crítica, se alcanza el entendimiento más completo de toda la estructura opresiva y logra ver con claridad los problemas en función de su comunidad. Entiende cómo se produce la colaboración entre opresor y oprimido para el funcionamiento del sistema opresivo.

VII. Discusión

Con base en todo lo planteado se establece que la concientización es un enfoque educativo que plantea problemas y afronta conflictos, que afirma la iniciativa de los seres humanos en la búsqueda de alternativas humanizadoras, y confronta las condiciones de privación, opresión y marginación características de las situaciones límite.

La cual de acuerdo a los criterios planteados en el presente artículo afirma que la implementación de un modelo de concientización en ciberseguridad optimiza el tratamiento de riesgos procedentes de ataques de ingeniería social.

Referencias

[1] Mouton, Francois & Leenen, Louise & Venter, H.s. (2015). Social engineering attack detection model: SEADMv2. 10.1109/CW.2015.52.

[2] F. Mouton, L. Leenen, M. M. Malan, and H. Venter, "Towards an ontological model defining the social engineering domain," in ICT and Society, ser. IFIP Advances in Information and Communication Technology, K. Kimppa, D. Whitehouse, T. Kuusela, and J. Phahlamohlaka,Eds. Springer Berlin Heidelberg, 2014, vol. 431, pp. 266–279.

[3] F. Mohd Foozy, R. Ahmad, M. Abdollah, R. Yusof, and M. Mas'ud,"Generic taxonomy of social engineering attack," in Malaysian Technical Universities International Conference on Engineering & Technology, Batu Pahat, Johor, November 2011.

[4] K. Ivaturi and L. Janczewski, "A taxonomy for social engineering attacks" in International Conference on Information Resources Management, G. Grant, Ed. Centre for Information Technology, Organizations, and People, June 2011.

[5] Kaufer, Human Exploits in Cybersecurity: A Social Engineering Study. University of. Arizona Master's Report. Long, J., 2011

[6] Bernard Oosterloo, "Managing Social Engineering Risk", Utrecht, October 6th 2008

[7] Miguel Tames Arenas, "Social Engineering and Internal Threats in Organizations", Department of Computer Science School of Engineering Blekinge Institute of Technology, March 2008

[8] Lejla Islami, "Assessing generational differences in susceptibility to Social Engineering attacks", University of Tartu, Institute of Computer Science, June 2018

[9] Freire, P. (1970a) "Conscientization". Cross Currents, 24 (1), 23-28