Métodos Orientados a Reducir Ataques de Ingeniería Social en Organizaciones

Paola Andrea Ugarte Espada
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
paugarte210@gmail.com

***Resumen*—El presente artículo describe la problemática de la ingeniería social en las organizaciones. Se indica cómo funciona la ingeniería social, la problemática que esta representa para las organizaciones; así como los métodos más utilizados de ingeniería social y que métodos se pueden emplear para reducir los ataques o mitigar el impacto de estos.**

Palabras clave—ingeniería social, seguridad informática, internet, phishing, pretexting, baiting, tailgating, piggybacking.

I. INTRODUCCIÓN

Para tener éxito en este mundo, se debe tener conocimiento: conocimiento para realizar tareas, construir desde lo más pequeño hasta algo inimaginable. En definitiva, el conocimiento es poder. Por otro lado, cualquier empresa, gobierno o individuo puede ser destruido por la falta de conocimiento o porque la información que es la base de su conocimiento ha sido revelada a terceros o en algunos casos a la competencia directa.

La ingeniería social es una de las amenazas más destructivas para cualquier empresa sin embargo muchas de ellas no se encuentran consientes del verdadero impacto ya que la ingeniería social no es algo que se puede ver, tocar o rastrear a través de herramientas de seguridad. Esta amenaza puede dañar de manera muy crítica a las organizaciones debido a que mediante la ingeniería social se pueden obtener hasta los datos más sensibles sin siquiera notarlo. Las personas que realizan la ingeniería social utilizan una personalidad suave, se basan en ganar la confianza de la víctima, esto con el fin de engañar a las personas a través de una conversación inteligente en la cual la víctima no se dé por enterada que le intentan extraer datos. Estas conversaciones tortuosas con frecuencia proporcionan al atacante suficiente información para comprometer la red informática de la empresa que, a diferencia de un ataque técnico común, los ataques de ingeniería social no se pueden prevenir tan fácilmente y pueden pasar desapercibidos sin generar alertas. [1] [2].

El proceso de la ingeniería social puede llegar a ser complejo o bastante rápido, dependiendo de la habilidad del atacante. Primeramente, la persona encargada de realizar el ataque de ingeniería social recolecta información acerca de su víctima. Haciendo uso de esa información el atacante explota la psicología humana y obliga a la víctima a divulgar inadvertidamente la información que necesita el atacante sin que la víctima se dé cuenta de lo suscitado. El aumento de la popularidad de las redes sociales ha aumentado enormemente el arsenal de información disponible para el ingeniero social y con esto los ataques de ingeniería social perpetuados a empresas y personas.

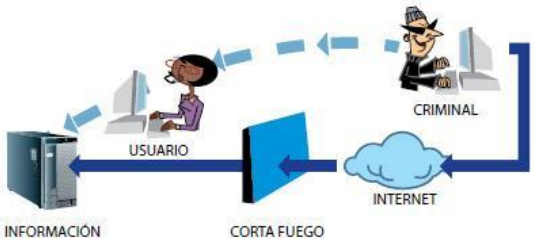

Fig. 1. Proceso de ingeniería social
Fuente: https://www.timetoast.com/

A. *El problema de la ingeniería social*

A pesar de que las empresas hoy en día destinan un porcentaje de su presupuesto en la seguridad de la información haciendo uso de herramientas y software para evitar programas maliciosos o reduciendo los huecos de seguridad, la ingeniería social es un tipo de ataque que puede ser aún más peligroso que un ataque a los ordenadores ya que se podrían perder datos muy sensibles de la organización.

La ingeniería social es sumamente frecuente en la sociedad debido a su simplicidad. No es posible tener un número exacto de cuantos ataques de ingeniería social se han realizado en una organización debido a que afectaría la imagen de la empresa y en casos en que los ataques hayan sido realizados de manera totalmente discreta, las empresas no llegan a enterarse que han sido víctimas de este tipo de ataque.

El problema que los ataques de ingeniería social estén incrementando parte del hecho que el usuario es el eslabón más débil de la cadena de seguridad, la psicología empleada en el usuario al momento de cometer el ataque hace que éste sea aún más exitoso ya que se juega con las emociones de las personas, se apela a aumentar el ego de una persona, se expresa interés en temas en los que el usuario se encuentra apasionado, se hacen comentarios falsos en orden que la víctima corrija y se obtengan datos, los atacantes prácticamente establecen confianza en la victima haciendo uso del carisma y halagando a las personas [1][3].

B. *Ataques más recurrentes de la ingeniería social*

Para poder obtener medidas de control y poder mitigar los ataques de ingeniería social, es necesario primeramente conocer

Para referenciar este artículo (IEEE):
[N] P. Ugarte, «Métodos Orientados a Reducir Ataques de Ingeniería Social en Organizaciones» *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 7, pp. 76-79, 2020.

los ataques más comunes a los cuales se ven expuestos los usuarios en un día a día, acorde a la empresa desarrolladora de soluciones ante amenazas de seguridad y preservación de datos Tripwire, los métodos más utilizados son los siguientes:

1) Phishing: Es el ataque más común de la ingeniería social y acorde a los al hacker Kevin Mitnick y al CEO y fundador e KnowBE4 Stu Sjouwerman 91% de las pérdidas de datos son provenientes de este tipo de ataque en el que generalmente se obtiene información personal haciendo uso de correos electrónicos, links acortados y se hace uso del sentido de urgencia de las personas, así como del miedo [6].

2) Pretexting: Este tipo de ataque se enfoca en la creación de un falso sentido de confianza con la víctima basado en una historia. Este tipo de ataque se utiliza para ganar acceso a las organizaciones, así como para obtener información.

3) Baiting: Es un tipo de ataque similar al phishing, pero la diferencia es que ofrece una recompensa a la víctima. En algunos casos se ofrece la descarga de música o películas a cambio de las credenciales de acceso a un determinado servicio. Se han dado casos en los que los empleados de las organizaciones han encontrado una memoria flash y al insertarla en sus estaciones de trabajo se ha dispersado malware en la organización.

4) Tailgating o "Piggybacking": Este tipo de ataque lo utilizan personas que carecen de la debida autenticación para ingresar a un área restringida, lo que realiza es esperar que el usuario autorizado ingrese y el atacante gana su confianza o muestra un falso sentido de urgencia para ingresar con él [7] [3].

C. Estado del arte

Para adentrarnos más en la relación de la seguridad de la información y la ingeniería social se presentan las siguientes investigaciones y artículos relacionados.

En la tesis de maestría "Clasificación de Phishing utilizando minería de datos adversarial y juegos con información incompleta" se hace referencia a una de las técnicas utilizadas en Inteligencia de Negocios que es la minería de datos. En la tesis se comprende el diseño y desarrollo de una metodología para clasificar mensajes de fraude por correo electrónico considerando la semántica de estos [8].

En el artículo denominado "Hacia la automatización de la ingeniería social haciendo uso de sitios de redes sociales" los autores hacen uso de técnicas de Inteligencia de Negocios para automatizar ataques de ingeniería social en redes sociales. Los autores proponen un dispositivo el cual automatizará la obtención de información de miembros que pertenecen a la red del usuario desde el cual se realiza el ataque posteriormente se hace uso de esa información para contactar a las personas y ejecutar el ataque ya sea solicitando información o enviando archivos los cuales contienen software malicioso [9].

Este proyecto "Ingeniería social: psicología aplicada a la seguridad informática" presentado por Sergio Arcos Sebastián se recogen los fundamentos de los ataques de ingeniería social en los sistemas informáticos, especialmente en las grandes plataformas de Internet. El objetivo principal es lograr comprender su naturaleza y ser capaces de valorarlos como la amenaza que representan. Por tal de conseguir el objetivo se realizan pruebas de concepto para valorar el riesgo, cambiando a menudo la perspectiva a la del atacante [10].

D. Seguridad de la información

La Seguridad de la Información, de acuerdo con la norma ISO 27000:2014, se define como la preservación de la confidencialidad, integridad y disponibilidad de la información [11].

La seguridad de la información apoya a las empresas a asegurar que su información se encuentre protegida frente a usuarios no autorizados (confidencialidad), que la misma no sea modificada de manera indebida (integridad), y apoya a que la información se encuentre disponible cuando la misma sea necesaria (disponibilidad).

La seguridad de la información es una disciplina en constante evolución ya que día a día se presentan nuevas amenazas las cuales pueden llevar a que la organización no cumpla con sus objetivos planteados [12].

E. Ingeniería Social

La ingeniería social es el lado humano de los virus informáticos, la piratería y el robo de información. Se refiere a un tipo de intrusión no técnica que se basa en la interacción social - en efecto, los atacantes engañan a los usuarios para que se les conceda acceso a los recursos de la red, a menudo se aprovechan de la tendencia humana natural para ayuda. Además, los hackers pueden intentar aprovechar la falta de conocimiento de un usuario; gracias a la velocidad de la tecnología, muchos consumidores y empleados no se dan cuenta el valor total de los datos personales y no están seguros de cómo proteger esta información de una manera más adecuada [13][5].

La definición que Kevin Mitnick en el libro el arte de la decepción es la siguiente:

"Ingeniería social es el uso de la influencia y la persuasión para engañar a la gente convenciéndolos de que el atacante es alguien que no es, o a través de la manipulación. Como resultado, el ingeniero social es capaz de aprovecharse de la gente para obtener información, o persuadirlos a realizar una acción, con o sin el uso de tecnología" [6].

La ingeniería social puede llevarse a cabo a través de una serie de medios [14]:

- Por teléfono,
- Por correo electrónico,
- Por correo tradicional,
- Por mensajería instantánea, etc.

F. Uso de la Ingeniería Social

¿Qué motiva a una persona para llevar a cabo un ataque de ingeniería social? Existe una variedad de motivos, que incluyen, pero no están limitados a:

- Resultados financieros: por varias razones, una persona puede quedar paralizado ante ganancias monetarias. Por ejemplo, se puede creer que se merece más dinero del que gana o tal vez hay la necesidad de satisfacer un hábito de juego que se encuentra fuera de control.

- El interés propio: un individuo puede, por ejemplo, que desee acceder y/o modificar la información que se asocia a un familiar, amigo o incluso un vecino.
- Venganza: por razones únicas verdaderamente conocidas por el individuo, que podría ser para difamar a un amigo, colega, organización o incluso un completo desconocido satisfaciendo un deseo emocional de venganza.
- La presión externa: un individuo puede estar recibiendo la presión de los amigos, la familia o los organizados sindicatos del crimen por razones tales como el beneficio económico, el interés personal y / o la venganza [15].

G. Ataques de Ingeniería Social

Acorde a Gartner Research los ataques de ingeniería social constan de las siguientes 4 etapas,

Recolección de información: Para realizar la recolección de información el agresor puede hacer uso de una variedad de técnicas, entre las cuales se puede hacer uso de técnicas haciendo uso de la tecnología o de la proximidad a la víctima. El atacante puede hacer un uso combinado de las técnicas y en base a las piezas obtenidas generar conocimiento acerca del objetivo [16].

- Desarrollo de la relación: El atacante desarrolla un sentido de confianza en la víctima lo cual permite que la víctima pueda revelar información confiable de una manera más fácil. [18][17].
- Explotación de la relación: Obtenida la confianza de la víctima el atacante aprovecha el lazo formado y aprovecha para obtener información sensible o aprovecha la situación para que la víctima realice acciones que beneficien al atacante [16][17].
- Ejecución para logar el objetivo: Esta etapa es la última de ciclo, básicamente es en la cual el atacante cierra o pausa el contacto con la víctima una vez conseguido el objetivo del ataque [16][17].

Estas etapas se encuentran presentes en los ataques de ingeniería social, sin embargo, es importante mencionar que cada ataque es único ya que las etapas pueden ser llevadas a cabo en forma paralela o en base a las 4 etapas se puede considerar incluir otras técnicas.

II. Métodos Utilizados

A. Tipo de la Investigación

El tipo de investigación que se empleará para el desarrollo de la presente investigación es exploratorio y descriptivo ya que se identificó que el tema a ser desarrollado no ha sido investigado de manera exhaustiva y gracias a la investigación descriptiva va a ser posible la descripción de situaciones y eventos que tengan influencia en la metodología creada.

B. Métodos de la Investigación

Para realizar la presente investigación se consideró el empleo de un análisis cualitativo del tema, ya que se consideró necesario el analizar los documentos relacionados, así como la información disponible y algunas de las investigaciones identificadas que se encuentran relacionadas al tema de investigación.

Una vez obtenida la información y después de concentrar la misma en un solo repositorio se prosiguió con la evaluación de la misma, para realizar esta tarea se optó por el método de una revisión sistemática de la literatura mediante la cual se identificó, evaluó y se interpretó todas las fuentes recabadas a fin de que entre las mismas se obtenga los conceptos, los procesos principales que se deben implementar. Para obtener esa información se aplicó el criterio de inclusión de información referente a la etapa desarrollada.

Se tuvo una etapa de inclusión de información, la cual se encontró basada en que se revise las fuentes obtenidas buscando conceptos o procedimientos los cuales se encuentren relacionados a la etapa que se estaba desarrollando el momento de la consulta, esto quiere decir que cuando se estaba haciendo el análisis de las bases para la investigación se necesitaba información como conceptos, indicadores, factores clave para mitigar la amenaza de los ataques de ingeniería social.

La revisión sistemática de la información fue el factor más importante para la investigación realizada, ya que a través de este proceso se pudo obtener los principales conceptos, las amenazas, las consecuencias, las contramedidas que deben ser tomadas, entre otros.

III. Resultados

Habiendo realizado una investigación exhaustiva acerca de la ingeniería social, los métodos de ingeniería social más comúnmente utilizados y las consecuencias de este tipo de ataque se llega a la conclusión que existen diversas capas para defenderse de la ingeniería social.

La primera capa es la prevención en la cual se realizan diversos pasos en los que drásticamente se reduce la probabilidad de ocurrencia de un ataque. En esta etapa lo que se realiza es proporcionar a los usuarios más conocimientos más que fortalecer la tecnología.

El primer paso a tomar es crear consciencia en los empleados de que la ingeniería social existe y que es un ataque que puede tomar por sorpresa a cualquiera, motivo por el cual es importante que los mismos se encuentran preparados y prevenidos ante estos posibles ataques.

El siguiente paso es la capacitación, sólo mediante la capacitación los empleados van a ser capaces de reconocer claros ejemplos de ingeniería social y de esta manera se crea un comportamiento alerta y una mentalidad que se encuentra siempre a la defensiva.

Con la capacitación vienen las políticas de la empresa que deben ser explicadas y difundidas a cada uno de los trabajadores de la empresa en todos los niveles que cuenta la misma, se considera que también es importante que los mismos tengan en cuenta los posibles efectos que tienen sus acciones a fin de que a medida de precautelar su seguridad hagan lo mismo con la seguridad de las organizaciones.

La siguiente capa es la de minimizar el impacto en caso de que el atacante haya logrado su acceso. Se puede hacer uso del cifrado de los archivos. Segmentar la red y los accesos acorde a las necesidades y privilegios de los usuarios, hacer uso de software que previene la filtración de información, así como de sistemas de detección de intrusos.

La última capa llega a ser la de la corrección, en caso que se haya perpetuado un ataque se deben tomar medidas correctivas

para que no vuelva a ocurrir un ataque similar y en caso que la empresa desee mantenerse libre de riesgos se pueden efectuar auditorías a la seguridad de la información y también en aspectos de ingeniería social para medir el nivel de consciencia de los empleados [4][5].

IV. Discusión

La ingeniería social toma diversas formas; desde el ingreso físico a la organización, correos electrónicos con malware hasta llamadas telefónicas que piden con urgencia la solución de un problema a cambio de claves de acceso.

En el artículo "¿Podemos vencer a la ingeniería social?" [4] se toma en cuenta que la ingeniería social tiene siglos de uso, no sólo ha sido empleada en el tema de la informática, sino que ha sido un medio de extracción de información durante cientos de años. La conclusión a cuál se llega en este artículo es que no se puede vencer a la ingeniería social, pero se pueden implementar medidas para que el riesgo al que la empresa se encuentra expuesta se reduzca.

V. Conclusión

La meta de una organización es tener éxito y para lograr esto es necesario tener una buena seguridad de la información tanto física como en las personas que la conforman. La seguridad de la información que se encuentra en manos de los usuarios no puede ser garantizada de encontrarse protegida al 100%, esto quiere decir que es necesario que las entidades establezcan acciones y medidas para atacar los posibles ataques de seguridad de información a los que son propensos.

Con la investigación se identificó que mínimamente para que una empresa cuente con un nivel razonable de seguridad brindada por sus funcionarios es necesario que se realicen capacitaciones de manera frecuente con el fin que se cree una consciencia de seguridad por parte de los funcionarios responsables y que la empresa se encuentre menos propensa a ataques de ingeniería social, ya que los mismos pueden llegar a tener grandes y graves consecuencias en la operativa de una organización.

Pero para minimizar las posibilidades de ataques esto se pueden aplicar capacitaciones acerca de temas de seguridad, auditorías a la seguridad de la información para ver si realmente en la empresa se ha creado una cultura de seguridad ya que ésta se encuentra en manos de todos.

Referencias

[1] David Bisson, "5 Social Engineering Attacks to Watch Out For", 2015

[2] Sergio Arcos Sebastián, "Ingeniería Social: Psicología Aplicada a la Seguridad Informática"

[3] Shaun Kolich, "Fundamentals of Ethical Hacking", 2015

[4] Kaspersky Lab, "Can we beat social engineering?", 2014

[5] Kaspersky Lab, "Ingeniería Social: Hackeando El Sistema Operativo Del Ser Humano", 2013.

[6] Mitnick, K., & Wozniak, S., The art of deception: controlling the human element of security. Indianápolis: John Wiley & Sons, 2002.

[7] Jared Kee, "Social Engineering: Manipulating the Source", 2008

[8] L'Huillier, G. A. (2010). Clasificación de Phishing utilizando minería de datos adversarial y juegos con información incompleta. Santiago.

[9] Huber, M., Kowalski, S., Nohlberg, M., & Tjoa, S. (2009). Towards Automating Social Engineering.

[10] Arcos, S. (2011). Ingeniería social: Psicología aplicada a la seguridad.

[11] ISO/IEC. (2014). ISO/IEC 27000:2014.

[12] Areitio, J. (2008). Seguridad de la Información Redes Informática y Sistemas de Información. Madrid: Paraninfo.

[13] Mann, I. (2008). Hacking the Human. Cornwall: MPG Books Ltd.

[14] Chubb. (2014). Guide to preventing social engineering fraud.

[15] Reichard, A. (2006). Ingeniería Social.

[16] Allen, M. (2006). Social Engineering. SANS Institute.

[17] Heikkinen, S. (2016). Social engineering in the world of emerging. 05: 08.

[18] The Social Engineering Framework. (11 de 10 de 2016). Obtenido de Security through education: http://www.social-engineer.org/framework/information-gathering/

Breve CV de la autora

Paola Andrea Ugarte Espada es Licenciada en Ingeniería de Sistemas por la Universidad Católica Boliviana "San Pablo" de La Paz, 2013. Actualmente realiza la Maestría en Informática Forense, Seguridad de la Información y Auditoría Informática en el Postgrado en Informática de la UMSA. Trabaja en el Banco de Crédito de Bolivia como Auditora Senior TI, previamente como Ingeniera de Proyectos en Feprom Solutions y en Eressea Solutions. Email: paugarte210@gmail.com.