EL ARTE DE LA INGENIERÍA SOCIAL

Romero, Diego
diaromero.86@hotmail.com
Universidad Piloto de Colombia

Resumen *- **Este artículo nos muestra la forma de actuar de la ingeniería social en ambientes personales y laborales dentro del campo de la seguridad de la información, esto con el fin de que el lector pueda llegar a comprender el significado de la ingeniería social, como interviene en la vida de las personas, las diferentes modalidades de ataque, la manera de prevenirla, y la importancia que esta rama tiene en el mundo de la seguridad informática. Partiendo de esta información, se espera que el lector pueda establecer una base sólida de conocimientos que contribuyan a la prevención de este tipo de ataques en los sistemas de su interés, bien sean empresariales o simplemente en la vida cotidiana. También se pretende que en un futuro sea posible incrementar los controles de seguridad a los sistemas de información, mediante múltiples campañas de sensibilización en las empresas, generando cultura en las personas que contribuyan a la prevención de posibles ataques informáticos.***

Abstract *- **This article shows us the way of acting of social engineering in personal and work environments within the field of information security, this so that the reader can come to understand the meaning of social engineering, as it intervenes in the lives of people, the different modes of attack, the way to prevent it, and the importance that this branch has in the world of computer security. Based on this information, it is expected that the reader can establish a solid base of knowledge that contributes to the prevention of such attacks in the systems of interest, whether they are business or simply in everyday life. It is also intended that in the future it will be possible to increase security controls to information systems, through multiple awareness campaigns in companies, generating culture in people who contribute to the prevention of possible computer attacks.***

Índice de términos *- **Defensa contra la ingeniería social, ingeniería social, sistemas de encriptación, técnicas de ataque.***

I. INTRODUCCIÓN

En la actualidad y en el campo de la seguridad informática el término de ingeniería social es muy reconocido, pues sin duda alguna son las compañías las que más resguardan y protegen su información, puesto que es considerada como la columna vertebral de sus negocios y se debe conservar su integridad.

Las empresas siempre buscan tomar medidas de seguridad que ayuden a gestionar su información, para ello se tiene en cuenta tres pilares de suma importancia para la seguridad, tales como: *la* confidencialidad, la integridad, y la disponibilidad. Con el pasar de los días la tecnología va avanzando y con ello se asocian los diferentes riesgos de mantener un sistema de información seguro, herramientas como firewall para aplicaciones (WAF), sistemas de detección de intrusos (IDS), sistemas de protección de intrusos (IPS), entre otras, resultan cada vez más costosas y presentan altos grados de complejidad en su administración, los cuales requieren mano de obra especializada y con experiencia en el manejo de dichas soluciones tecnológicas. Adicional a esto, tenemos que reconocer que también existe en todas las empresas del mundo un recurso inseguro que almacena información sensible, que es “la mente humana,” y a la cual hoy en día todavía no se le ha dado la importancia requerida, por ello muchas compañías no lo consideran importante dentro de sus políticas de seguridad de la información, y a nivel de conceptos dentro de los términos de seguridad informática. De todo ello nace una necesidad en todos los usuarios que operan sistemas tecnológicos que es tomar conciencia de lo importante de mantener controles que fortalezcan sus mecanismos de seguridad, antes de que llegue a suceder siniestros en su información.

De acuerdo con lo anterior, uno de los más importantes activos de información que se deben identificar en las organizaciones son las personas, pues son estos los que albergan gran cantidad de datos, procedimientos, accesos, y controles que pueden actuar como mecanismos de seguridad o de peligro para el acceso a información.

Este documento también pretende enseñar al lector las diferentes modalidades y manipulaciones a las que un ser humano a través de elementos psicológicos puede verse sometido en el momento de operar un equipo tecnológico y ejecutar ciertas actividades inconscientemente. Este tipo de acciones hace referencia a los más conocidos ataques de ingeniería social *abreviado a partir de ahora en este documento como I.S.* Cuando escuchamos el término ingeniería tal vez nos imaginamos personas con cascos, planos, grandes matemáticos, genios de la computación, robótica, astronomía, o ambientales, etc. Sin embargo, existe otra clase de ingeniería, una tan sutil que incluso puede generar grandes cambios y crecer de una manera más rápida y fuerte que las anteriores, *la I.S.* Pero ¿por qué está tan de moda este término?, a ¿qué se debe que sea tan común hoy en día?, todos estos interrogantes se discuten durante el desarrollo de este documento, desde los orígenes de la ingeniería social, su definición, grandes especialistas en el tema, diferentes técnicas de ataque, hasta como defenderse de la I.S.

II. EL AYER Y EL HOY

La I.S no es un término moderno su existencia es de muchos años atrás, desde la creación del ser humano, la edad antigua, y la edad moderna, retrocediendo en el tiempo tenemos un primer ejemplo de ingeniería social que ocurrió en la ciudad de Troya ubicada hoy en día en el país de Turquía cuando fue conquistada alrededor del año 1300 a.C. El plan de los griegos en ese entonces para su conquista incluía un caballo gigante construido en madera el cual denominaron los griegos “Caballo de Troya,” y que guardaba en su interior los soldados que acabarían con la ciudad entera, lo que parecía un obsequio resultó ser la trampa y la perdición para la ciudad de Troya [4].

La Ingeniería social que se manifestó en aquel entonces y comparándola con el presente, hoy en día depende en gran medida de la interacción humana, y para este caso suele implicar “el engaño” a las víctimas para ganar su confianza y que rompan procedimientos normales de seguridad, siendo ellos mismos los que van abriendo las puertas a los atacantes por su propia voluntad.

De lo anterior nace un interrogante, ¿será posible hoy en día presentarse un escenario de caballo de Troya a través de las redes sociales?, la respuesta es sí, ya que las redes sociales se han convertido en parte fundamental, esencial y tal vez irremplazable para las personas, pues se convierte en un espacio donde la mayoría de usuarios muestran y hacen visible información sobre gustos, necesidades y hasta problemáticas de su vida personal, y es ahí cuando los atacantes aprovechan para persuadir y llegar a ellos utilizando publicidades engañosas, tan llamativas a las que los usuarios no se pueden resistir, cayendo así en la trampa como en aquel entonces de la ciudad de Troya.

III. LA INGENIERÍA SOCIAL EN LAS REDES SOCIALES

El aumento de múltiples opciones en internet para tener una red social como Facebook, Instagram, Twitter, entre otras, es directamente proporcional a la necesidad del ser humano de consumir servicios como estos, compartir información personal y hacerla pública es la que aprovechan los ciberdelincuentes para vulnerar las personas y conseguir sus objetivos, que por lo general no son nada buenos [4]. Los ataques de ingeniería social han ido en aumento día tras día y la estrategia que utilizan los ciberdelincuentes supone un gran trabajo de investigación para ellos, lo que los lleva también a ser cada vez más eficientes y obtener mejores resultados, la eficiencia de esta modalidad es por lo siguiente:

1) Primero recolectan toda la información posible extrayéndola de las redes sociales, para ello se registran en las plataformas creando perfiles falsos ya sea en Facebook, Twitter, LinkedIn, etc.

2) Consolidan un plan de ataque para transmitir fiabilidad.

3) Recolectan información particular, entienden su comportamiento (temas de interés, amigos, gustos, etc.), y ganan su confianza.

4) El atacante hace su primer acercamiento (con un falso perfil) teniendo ya definida la táctica de engaño que va a utilizar.

5) Cuando la víctima lo considera “su amigo,” el delincuente se muestra cercano y siempre intentará sonsacarle aún más información a través de mentiras.

6) Una vez siendo “amigos,” el ciberdelincuente pedirá datos más personales (correo electrónico, dirección, número de teléfono, etc.).

7) En este punto, la identidad podría suplantar de una manera más rápida y eficiente, o se le enviaría a través de correo electrónico un enlace llamativo que al abrirlo ejecutase un troyano que infecta el computador y diera acceso a las cuentas bancarias de la víctima.

8) Después de obtener lo que buscaba el atacante borra todo rastro, abandona perfiles y no vuelve a hablar con la víctima. [4].

Se puede observar que hoy en día casi todas las personas poseen una cuenta de correo electrónico registrada en redes sociales, por lo que se convierte en una moda y una necesidad de los seres humanos contar con estos servicios para su vida cotidiana. En estas redes se puede crear grupos, compartir fotos, calendario, eventos, videos, comentarios, información personal con sus allegados o amigos. Si nos centramos a observar detalladamente todo lo que se publica por estas redes sociales nos encontraríamos con información sensible, como fotos con ubicaciones y/o lugares frecuentes, direcciones de vivienda o trabajo, nombre de la empresa donde trabaja, nombres de familiares, gustos, y hasta números de celular, siendo todo esto una gran ayuda para personas malintencionadas que busquen investigar acerca de nosotros, lo cual le facilita la tarea al ciberdelincuente para obtener información valiosa para su propio beneficio o con fines delictivos. Estas personas tendrían la posibilidad de recopilar información y almacenarla en una base de datos de posibles "víctimas" a los cuales poder atacar más adelante, las pretensiones de estas personas podrían ser la investigación o la realización de inteligencia a una o a un grupo de personas, la identificación de familiares y amigos para posibles acciones criminales, la violación a la privacidad de la información y el posterior robo de datos confidenciales como cuentas bancarias o contraseñas.

IV. ENTENDIENDO LA INGENIERÍA SOCIAL

La I.S se puede definir como la práctica de obtener información confidencial, en la mayoría de los casos información de gran valor a través de la manipulación de la mente en las personas, donde los atacantes por medio del engaño intentan obtener información sensible o privilegios en algún sistema, en definitiva se trata de engañar y confundir al usuario de un sistema informático para que acabe haciendo algo que realmente no quiere hacer, cómo ejecutar un software, facilitar sus claves de acceso, o acceder a determinados servicios [8]. Este tipo de ataque es muy simple, pero a la vez bastante efectivo, ya que se puede conseguir información en muy poco tiempo, a comparación de otras técnicas de hackeo sofisticadas, como un programa maligno desarrollado para acceder a sistemas y encriptarlos que lleven a la recolección de datos.

Es importante entonces decir que la ingeniería social podría presentarse de dos maneras: una es interactuando con máquinas y software y la otra basada en el ser humano. En la actualidad los ataques de ingeniería social utilizan las dos maneras para potenciar los resultados, esta combinación es letal para una víctima que por lo general en ocasiones no es consciente de que esta siendo atacado por esta técnica [9].

Mencionaré algunos ejemplos nada lejanos de la realidad, en donde se aplica la ingeniería social en todo su esplendor, invito al lector que coloque mucha atención en estos dos casos muy cercanos a lo que hoy en día se presenta en nuestras vidas profesionales y personales, es a través de ejemplos y enseñanzas que se aprende de las cosas, tal vez en un futuro o porque no en el presente logremos identificar un ataque de esta índole.

A. *Cediendo al engaño*

Imaginemos que usted es un oficial de seguridad de la información de una multinacional y recibe una llamada a su número fijo de la oficina, en donde le ofrecen un sorteo de premios por una compra que usted realizó hace poco en un establecimiento de ropa, los premios incluían entradas para un partido de fútbol de su equipo favorito, así como viajes a destinos turísticos en donde se encuentra su destino favorito, al que siempre ha querido ir y no ha sido posible. Para ello accede a una serie de preguntas realizadas por el ciberdelincuente en donde al final le solicitan su dirección de correo electrónico (allí usted ya cedió), a este correo electrónico le sería enviado un archivo en formato PDF con más información sobre cómo participar en los sorteos, inclusive durante la llamada el ciberdelincuente le indica que ya mismo le envía el correo y que por favor lo abra para confirmar que el documento adjunto es legítimo y está completo con su información legible, asegurando que el archivo PDF que le envío es el correcto, usted accede, pero es allí donde viene el ataque, gracias a que usted abrió ese mensaje y su adjunto allí su equipo se infectó de un malware que permitió accesos no autorizados al sistema.

La reflexión a este primer caso de I.S es que el ataque inicia con una llamada, sin embargo antes de esa llamada muy probablemente el ciberdelincuente ya hubiese tenido información de la víctima, como nombre, gustos, empresa donde labora, cargo en la compañía y todo ello muy posiblemente con una investigación en internet (redes sociales), o con un registro de datos personales durante la compra que realizó en el almacén de ropa días atrás, por lo que es importante controlar el uso de las redes sociales y el tratamiento de datos personales en los diferentes ámbitos. Posterior a ello la víctima cede al abrir el archivo PDF adjunto del correo electrónico, importante no abrir adjuntos de remitentes desconocidos por más presión que ejerzan sobre nosotros, el que nos pidan abrir el correo es lo que más desconfianza nos debe crear, y por último sorteos, viajes, recompensas y demás ofrecimientos tan llamativos no es de confiar mucho, pues son estos el *"anzuelo"* (artimaña que se utiliza para atraer la atención de alguien y conseguir lo que se quiere) que colocan los ciberdelincuentes a sus víctimas para convencerlos.

El ataque informático se ve reflejado en dos maneras una social y la otra técnica, que es a través del programa maligno, el cual se propagó mediante la ejecución del documento PDF, no sin antes abrir las puertas a la misma víctima por medio de la ingeniería social.

B. *Víctima de la ingenuidad*

Ahora imaginemos que nos hacemos pasar por el nuevo supervisor de un supermercado o tienda de cadena, (en muchos casos sin ni siquiera teniendo un carnet de identificación sino únicamente con una vestimenta similar a la de un supervisor del mismo almacén) y llamamos a un empleado (persona que maneja la caja registradora) diciéndole que se va a realizar un cambio en las contraseñas para ingresar a la caja de pagos, ya que estas se están bloqueando con frecuencia, el empleado muy amablemente abre la caja y digita la clave en frente del supervisor (allí ya logramos observar la clave) o simplemente nos da su clave de acceso.

La reflexión de este segundo caso es que el ataque de I.S inicia de manera presencial y es cara a cara, se observa que con una sola frase se logra conseguir información como en este caso la clave de la caja, y a su vez acceso a la misma (dinero, bonos, cheques, etc.) información con gran valor para el supermercado y que en otros escenarios nos hubiera costado muchos días, semanas, o hasta meses conseguirla de otra manera (mediante fuerza bruta, buscando vulnerabilidades en el software, mediante virus sobre el sistema operativo), además todo esto y sin haber dejado rastro alguno físico o lógico (log en el sistema), ya que fueron tan solo unas frases y palabras muy convincentes y eficaces.

C. *Aprovechando las redes sociales*

En el ámbito personal también se presentan muchos casos de fraude y en gran parte con ayuda de las redes sociales, algunas noticias falsas y scams relacionados con muertes de celebridades que causaron polémica y

que buscaban que los usuarios de las redes sociales siguieran enlaces u opinaran sobre el tema dando clic a una de las URL falsas, algunas de ellas:

La falsa muerte del cantante Ricardo Arjona en un accidente aéreo, la noticia generada en el año 2015 se propagó por Facebook y redireccionaba a un enlace que obtuvo en su momento más de 12.000 clics en menos de dos días, el phishing consistió en abrir un supuesto video del accidente del artista que en realidad era una falsa página de Facebook para iniciar nuevamente sesión y robar credenciales de la víctima, después de ver el supuesto video que no era cierto se debía dar clic en compartir lo cual permitirá que el enlace falso se enviará a otra víctima y la propagación del mismo sería más rápida [12].

Fig. 1. Suplantación, imágenes tan llamativas e impactantes de las que debemos desconfiar y analizar su procedencia. [12].

Se logró observar después de la noticia que dos de los cuatro países más afectados en nuestra región fueron Argentina y Colombia con el 35% y 32% de los clics totales respectivamente [12].

Otro de los engaños fue la famosa opción del botón "no me gusta" en Facebook, que terminaba ocasionándole a la víctima un gasto extra al quedar suscrita en servicios de SMS Premium. A fin de cuentas, en ese entonces Facebook nunca había anunciado la implementación de esta controversial característica, y fue un gran engaño para los usuarios de esta red social [12].

Ejemplos y casos de I.S en la vida real existen muchos en el mundo y aquí podría relatar bastantes, lo cual no es el caso ni me quedaré realizando discusión de cada uno de ellos, sin embargo, es muy importante que de cada caso se obtenga una reflexión que nos ayude a reconocer cuándo estamos siendo víctimas de estos ciberdelincuentes y cómo prevenir este tipo de ataque social. Los medios de comunicación en muchos de los casos son el camino para que los ciberdelincuentes muestren todas sus armas y aprovechen esos canales para llegar a muchos de los usuarios, colocando así a prueba a gran multitud y esperando quienes caen en el engaño por si solos.

D. *Reconociendo la ingeniería social a otro nivel*

Después de cada ejemplo visto anteriormente nos preguntamos ¿en qué momento estamos siendo afectados por la I.S?, para ello puedo decir que cualquier ayuda o consejo no solicitado debe tratarse con precaución, especialmente si se trata de hacer clic en un enlace, abrir un adjunto de correo electrónico o brindar información sensible, ya que es probable que se trate de un intento de fraude por ingeniería social. Decir que reconocer un ataque de ingeniera social es fácil no es cierto, ya que en muchas ocasiones no nos damos cuenta de estas amenazas, tal vez sea menos complejo el darnos cuenta de que convivimos con un posible engaño y que en algún momento de nuestras vidas podemos identificarlo y actuar de manera correctiva. Es de resaltar que cualquier petición de su contraseña o información confidencial sin duda es un principio de fraude y posible ataque de ingeniería social del cual podemos estar siendo víctimas, las organizaciones legítimas nunca piden su contraseña, ya que esto es algo confidencial e intransferible, además es importante comprobar la dirección de correo electrónico del remitente y validar que sea legítima, la manera más fácil de hacerlo es a través de su dominio de correo electrónico, y si nos dirigimos a la parte técnica existen herramientas que analizan el mensaje de correo y su cabecera al detalle [1].

Herramientas como messageheader de Google, messageheader analyzer de Microsoft en donde podemos revisar que los dominios de confianza no sean suplantaciones de otros, esto a través de campos como:

From: Aquí se muestra de quien viene el mensaje.

Subject: Esto es lo que el remitente coloca como un tema del contenido del correo electrónico, es decir el asunto.

Return-Path: La cuenta de correo electrónico para devolver el correo.

Received: Esta cabecera es la más importante y normalmente es la de más confianza. Muestra una lista de todos los servidores y ordenadores por las que el correo ha viajado para llegar al destinatario.

X-Spam-Status: Esto muestra la puntuación de Spam generada por tu servicio o cliente de correo, importante a la hora de reconocer un correo malicioso.

X-Spam-Level: Esto muestra la puntuación de Spam normalmente generada por tu servicio o cliente de correo, entre más alta la puntuación mayor riesgo de ser un spam.

Message Body: El contenido del correo electrónico escrito por el remitente.

X-Mailer: En algunos clientes de correo o plataformas se puede visualizar desde que cliente de correo se ha enviado el mail [1].

V. PRÁCTICAS COMUNES Y ESPECIALISTAS EN EL TEMA

Phishing: Consiste en enviar correos electrónicos que parecen confiables con el objetivo de robar información personal y confidencial, se dice que esta modalidad de ataque abarca un 77% de los ataques sociales reportados. La mayoría de estos casos simulan ser entidades financieras que buscan actualizar datos de tarjetas bancarias y/o información de las personas para posteriormente engañar a la víctima [11].

Vishing: Consiste en obtener información o generar acciones a través un teléfono móvil o fijo y suele realizarse en prácticas como suplantar la identidad de otra persona, es una técnica que al ser combinada con otras se convierten letales [11].

Smishing: Son los ciberdelincuentes que realizan phishing a través de mensajes de texto y buscan hacer caer a la víctima bien sea abriendo un enlace falso, que se comuniquen a un número telefónico para sacar información o respondan a un mensaje de texto enviado con anterioridad [11].

Según el famoso informático estadunidense reconocido en el campo de la seguridad informática Kevin Mitnick, los pilares psicológicos y sociales en que se apoyan estas técnicas sociales son cuatro:

1) Las ganas de ayudar, a mi criterio en Colombia tenemos una ventaja de esta primera técnica y es que el ciudadano promedio en nuestro país es muy desconfiado, pensando que siempre tras una ayuda o favor se viene algo a cambio y va el concepto que tenemos como malicia del pueblo.

2) El primer movimiento es de confianza hacia el otro, como todo acercamiento a un ser humano y ganarse la confianza del otro es esencial para extraer información de gran valor que queramos.

3) A todos nos gusta que nos alaben, la admiración hacia otra persona y el ego es gratificante para un ser humano de allí el sentirse importante, es un camino hacia la confianza entre las personas.

4) No nos gusta decir “no,” y esta frase es muy importante debido a que se debe aprender a decir no independientemente de a quien se dirijan, puede ser un superior quien nos este indicando una instrucción que no sea integra o que no este acorde a nuestros valores [4], [6].

Estos pilares nos alertan para reconocer cuando estamos siendo víctimas de la ingeniería social y la manera en que nos está afectando. Este tema de la I.S hace reflexión a varios expertos en la materia como los son Kevin Mitnick, Fran Abagnale, Marcus Nohlberg, Markus Huber, entre otros. Recopilando el estado del arte que ha realizado cada uno de ellos es posible obtener una visión mucho más precisa, dada la rápida evolución tecnológica que ha habido durante los últimos años.

Fran Abagnale por ejemplo fue uno de los hackers más famosos con sus múltiples identidades, falsificaciones de cheques y engañando la mente humana de miles de personas, todo para obtener información que ayudará a sus grandes estafas, hoy en día es el director de Abagnale and Associates, compañía financiera de consultas de fraudes, dentro de sus frases famosas está la siguiente: "Lo que hacía en mi juventud, es mil veces más fácil, hoy en día la tecnología alimenta al crimen" - Frank W. Abagnale [2], [3].

También tenemos el ciclo de I.S diseñado y mencionado por Kevin Mitnick, quien es uno de los hackers, crackers, y phreakers más famosos de la historia y hoy en día se dedica a la consultoría desde la óptica particular de la I.S. en uno de sus famosos libros del arte, que decía lo siguiente "El ciclo es muy simple, pero no por ello poco eficaz. Se puede resumir en buscar información, crear confianza y utilizarla" [2], [3].

Dentro de sus frases famosas y que a mi criterio es muy importante para concientizar a la alta dirección en las compañías en donde piensan que el área de TI es solo gastos e inversiones es: "Una compañía puede gastar cientos de miles de dólares en firewalls, sistemas de encriptación y demás tecnologías de seguridad, pero si un atacante engaña a un empleado, todo ese dinero no habrá servido para nada"- Kevin Mitnick [2].

VI. MÉTODOS DE ATAQUE

La mayoría de los cibercriminales no invierten mucho tiempo en probar tecnologías complejas para sus ataques; saben que es más sencillo y menos costoso utilizar la ingeniería social, incluso existen páginas web con información valiosa donde aprender los métodos para engañar a las víctimas, uno de estos portales es socialengineer.org, plataforma que proporciona datos realmente útiles como los fundamentos teóricos, el funcionamiento de cada ataque y ejemplos que aclaran cada uno de los conceptos de esta rama [7].

¿Tal vez muchos se pregunten cómo podemos eliminar la ingeniería social?, para ello solo puedo decir que *no es posible*, pero lo que sí podemos hacer es mitigarla pues siempre estaremos expuestos a esta técnica de ataque y la mejor forma de evitarla es no dejarse engañar, en toda etapa de nuestras vidas nos encontraremos con gente de toda índole, en donde algunos quieren ayudarnos a salir adelante y otros quieren aprovecharse de nuestra humildad para sacar provecho de cualquier situación. Quiero dejar una frase muy representativa, y tal vez muchos de ustedes la escucharon a especialistas en seguridad de la información o la han visto en diferentes sitios web, imágenes y campañas publicitarias, y es que "nuestra mente es el eslabón más débil de nuestro ser y en algún momento de nuestras vidas fuimos o seremos marionetas" [8].

Las técnicas de ataque de la I.S son muy variadas y existen diferentes modalidades, pero para este artículo tomaré las mencionadas en la referencia [5] de la revista de seguridad de defensa digital, de la universidad nacional autónoma de México, en donde se menciona que en general, los ataques de I.S actúan en dos niveles: el físico y el psicosocial.

El primero describe los recursos y medios a través de los cuales se llevará a cabo el ataque, y el segundo es el método con el que se engañará a la víctima. Para dejar más claro el tema mencionaré unos ejemplos de ellos a continuación:

A. Nivel físico

Ataque por teléfono: Es la forma más persistente de I.S, en esta el atacante realiza una llamada telefónica a la víctima haciéndose pasar por otra persona, es un modo muy efectivo ya que no se requiere una cara a

cara, por lo tanto, la forma de engaño es más difícil de descubrir y más fácil para el delincuente [10].

Shoulder surfing: Esta técnica es una de las más antiguas, y se realiza a través de la observación directa, esto es tratando de ver información confidencial, como las contraseñas. [6].

Ataque vía internet: Es de los más famosos, ya que los servicios ofrecidos allí son bastantes y de diferentes maneras: vía correo, página web, software p2p, mensajería instantánea, hoy en día la mayoría de los ataques provienen del método del correo electrónico.

Dumpster diving o trashing (zambullida en la basura), consiste en buscar información relevante en la basura, como: agendas telefónicas, organigramas, agendas de trabajo, unidades de almacenamiento (CD, USB, etc.), entre muchas otras, para los administradores de TI, en donde por alguna razón escribieron claves de acceso a sistemas de información o bases de datos se recomienda no arrojar estos papeles de apuntes a la papelera de basura. [6], [10].

Ataque vía SMS: Ataque que aprovecha las aplicaciones de los celulares. El intruso envía un mensaje SMS a la víctima haciéndola creer que el mensaje es parte de una promoción o un servicio, luego, si la persona lo responde puede revelar información personal, ser víctima de robo o dar pie a una estafa más elaborada [10].

Office snooping: Esta técnica aprovecha la ausencia de la persona responsable de la oficina para husmear en su PC o documentos. De allí la importancia de generar el bloqueo de la sesión al momento de retirarnos de nuestros PC. Es importante dar este tipo de capacitación al personal de operadores en las centrales de monitoreo [6].

Ataque cara a cara: El método más eficiente, pero a la vez el más difícil de realizar. El atacante requiere tener una gran habilidad social y extensos conocimientos para poder manejar adecuadamente cualquier situación que se le presente, de allí es donde surge la palabra arte de la I.S [10].

Cabe resaltar que también existen ataques psicológicos que pueden ayudar a que un ataque cara a cara o de otra modalidad sea exitoso, los más comunes de acuerdo con la revista de seguridad de la universidad nacional autónoma de México [5], son:

B. Nivel psicosocial

Exploit de familiaridad: Táctica en que el atacante aprovecha la confianza que la gente tiene en sus amigos y familiares, haciéndose pasar por cualquiera de ellos. Un ejemplo claro de esto ocurre cuando un conocido llega a una fiesta con uno de sus amigos. En una situación normal nadie dudaría de que ese individuo pudiera no ser de confianza. Pero ¿de verdad es de fiar alguien a quien jamás hemos tratado? [10].

Crear una situación hostil: El ser humano siempre procura alejarse de aquellos que parecen estar locos o enojados, o en todo caso, salir de su camino lo antes posible. Crear una situación hostil justo antes de un punto de control en el que hay vigilantes, provoca el suficiente estrés para no revisar al intruso o responder sus preguntas [10].

Conseguir empleo en el mismo lugar: Cuando la recompensa lo amerita, estar cerca de la víctima puede ser una buena estrategia para obtener toda la información necesaria. Muchas pequeñas y medianas empresas no realizan una revisión meticulosa de los antecedentes de un nuevo solicitante, por lo que obtener un empleo donde la víctima labora puede resultar fácil [10].

Leer el lenguaje corporal: Un ingeniero social experimentado puede hacer uso y responder al lenguaje corporal. El lenguaje corporal puede generar, con pequeños, detalles una mejor conexión con la otra persona. Respirar al mismo tiempo, corresponder sonrisas, ser amigable, son algunas de las acciones más efectivas. Si la víctima parece nerviosa, es bueno reconfortar. Si está reconfortada, ¡al ataque! [10].

Explotar la sexualidad: Técnica casi infalible. Las mujeres que juegan con los deseos sexuales de los hombres poseen una gran capacidad de manipulación, ya que el hombre baja sus defensas y su percepción.

Probablemente suene asombroso, pero es aprovechar la biología a favor. Esta técnica suele ser utilizada en la mayor parte por las mujeres ya que al vestirse llamativas y ser el centro de atención de un hombre la distracción es mayor y todo juega a favor del atacante para cumplir sus objetivos [10].

VII. DEFENSA CONTRA LA INGENIERÍA SOCIAL

La forma de defenderse contra estos tipos de ataques de I.S es capacitando y formando a las personas en sus casas, universidades, y aquellas que laboran en las diferentes compañías, para prevenir riesgos que se puedan ocasionar sobre los sistemas informáticos, con ello se toman medidas preventivas sobre la información y no se corren riesgos de pérdida parcial o total de la misma. Algunos mecanismos válidos para este tipo de defensa son los mencionados en la revista de seguridad de la universidad nacional autónoma de México [5] así:

1) Nunca divulgar información sensible con desconocidos o en lugares públicos (como redes sociales, anuncios, páginas web, etc.)

2) Si se sospecha que alguien intenta realizar un engaño, hay que exigir se identifique y tratar de revertir la situación intentando obtener la mayor cantidad de información del sospechoso y sin alertarlo.

3) Implementar un conjunto de políticas de seguridad en la organización que minimice las acciones de riesgo, y comunicarlas a todos los funcionarios de la compañía.

4) Efectuar controles de seguridad física para reducir el peligro inherente a las personas.

5) Realizar rutinariamente auditorías y pen test usando I.S para detectar huecos de seguridad de esta naturaleza.

6) Llevar a cabo programas de concientización sobre la seguridad de la información.

VIII. CONCLUSIONES

La seguridad de la información abarca muchos campos y muchas áreas de estudio, por ello no solo es tecnología o herramientas de software lo que ayudan a controlar vulnerabilidades o tipos de malware que intente atacar contra un computador o cualquier hardware de la compañía, lo más vital y que muchas veces no tomamos con la importancia que se merece, es que toda organización debe reforzar a su personal en la concientización de temas en seguridad de la información, esto a través de charlas, capacitaciones, actividades de seguridad, los cuales adopten sólidos conocimientos y esten capacitados para manejar y solucionar posibles situaciones donde se presenten casos de ingeniera social, con esto ayudamos a prevenir y mitigar riesgos sobre los diferentes ataques que puedan presentarse.

Es importante resaltar que la mente humana, así como puede ser la más grande tumba de secretos, también puede ser la mayor ventana abierta de información sensible, importante y relevante para una compañía o para su vida misma, brindando así todo aquello que conlleve a lograr los oscuros objetivos de un atacante, es por ello que debemos de ser cuidadosos a la hora de interactuar con personas desconocidas y de brindar información relevante para los demás.

REFERENCIAS

[1] Base de conocimiento, entender una cabecera de correo. Sitio web. [Online]. Disponible: https://clouding.io/kb/entender-una-cabecera-de-correo/

[2] Ingeniería social, hackeando a personas. Sitio web. [Online]. Disponible: https://csirt.utpl.edu.ec/ingenieria-social-hackeando-personas

[3] Aspectos profesionales: Protección de Datos, Cloud Computing y Sistemas de Gestión. Sitio web. [Online]. Disponible:http://www.aspectosprofesionales.info/2014/01/ingenieria-social-hackeando-personas.html

[4] Cómo funciona la ingeniera social. [Online]. Disponible: https://mrhouston.net/blog/como-funciona-la-ingenieria-social/

[5] Escrito por Edgar Jair Sandoval Castellanos “Ingeniería Social: Corrompiendo la mente humana” revista seguridad, defensa digital | 1 251 478, 1 251 477 | revista bimestral. Volumen 10. 04/05/2011. México.

[6] Ingeniera social, hackear al ser humano. Sitio web. [Online].Disponible: https://www.seguridadenamerica.com.mx/noticias/articulos/18940/ingenierIa-social-hackear-al-ser-humano-

[7] Ingeniera social. Sitio web. [Online]. Disponible: http://www.social-engineer.org/

[8] K-oox seguridad informática. Sitio web. [Online]. Disponible: http://k-oox.blogspot.com/2016/05/ingenieria-social-la-amenaza-invisible.html

[9] Mitnick, K. John Wiley & Sons. El arte de la decepción. México D. F. (2002).

[10] Profa. Gabriela Cruz Montalvo. Sitio web. [Online]. Disponible: https://docentegabrielacruz.wordpress.com/aplicacion-de-la-seguridad-informatica/unidad-1-aplica-estandares-de-proteccion-de-la-informacion/r-a-1-1-determina-riesgos-de-seguridad-informatica-con-base-en-las-caracteristicas-del-equipo-y-las-necesidades-del-usuario/

[11] Welivesecurity eset, ingeniera social: los usuarios como víctimas de la falta de atención. Sitio web. [Online]. Disponible:https://www.welivesecurity.com/la-es/2014/05/01/ingenieria-social-los-usuarios-como-victimas-de-la-falta-de-atencion/

[12] Welivesecurity eset, las 5 historias de ingeniera social más ridículas de los últimos tiempos. Sitio web. [Online]. Disponible: https://www.welivesecurity.com/la-es/2015/12/01/historias-de-ingenieria-social-ridiculas/

Autor

Diego Alexander Romero Rubio, nacido el 17 de septiembre de 1986 en el municipio de Nocaima, Cundinamarca. Egresado de ingeniería de sistemas de la Corporación Unificada Nacional (CUN), certificado en ITIL fundamentos v3, especialista tecnológico en seguridad de redes, cursó y aprobó los módulos I y II de CCNA y en la actualidad está cursando la especialización de seguridad informática en la Universidad Piloto de Colombia.