Ingeniería Social: El Ataque Silencioso

Carlos Edgardo López Grande

Técnico en Ingeniería Eléctrica y Electrónica opción Mantenimiento y Servicio de Computadoras, Docente Escuela de Ingeniería Eléctrica y Electrónica, ITCA-FEPADE Sede Central. Email: carlos.lopez@itca.edu.sv

Ricardo Salvador Guadrón

Ingeniero Electricista y Master en Administración de Empresas, Director de la Escuela de Ingeniería Eléctrica y Electrónica, ITCA-FEPADE Sede Central. Email: rguadron@itca.edu.sv

Resumen

La seguridad informática en una organización depende en gran medida de la adquisición y de una adecuada configuración del hardware diseñado con ese propósito, además se debe tener un equipo de trabajo calificado para realizar las tareas de seguridad correspondientes. Sin embargo, las organizaciones olvidan que el eslabón más débil de su infraestructura informática son los usuarios de los sistemas y servicios de computadoras. Se cree que el servidor más seguro es el que está apagado, pero deja de ser cierto mientras exista un usuario que pueda encenderlo.

Palabras clave

Virus informáticos, seguridad social – informática, ingeniería de sistemas, seguridad informática, delitos informáticos, fraude informático.

Abstract

The IT security in an organization depends in a great range on the acquisition and the proper hardware configuration designed for this purpose. In addition, there must be a highly qualified staff to perform such tasks safely. However, organizations forget that the weakest link in their infrastructure are users of computer systems and services. It is believed that the most secure server is one that is kept turned off, but that's not true if there exists a user who can turn it on.

Keywords

Computer viruses, social security-informatics, systems engineering, computer security, computer crime, computer fraud.

Introducción

Victor Lustig[1], nacido en el año 1890 en la ciudad de Hostinné, Imperio Astrohúngaro (el día de hoy República Checa), fue uno de los mayores estafadores de su tiempo. La habilidad de Lustig para persuadir a las personas, lo llevó a realizar una de las estafas más famosas de todos los tiempos y que, hasta nuestros días, lo mantienen vigente en la historia. Fue capaz de vender la Torre Eiffel, el monumento parisino, dos veces con tan solo 1 mes de diferencia.

En la actualidad, pareciera absurdo que este hecho pudiera repetirse. Sin embargo, la forma en la que Lustig realizó la estafa no deja de tener vigencia. Mientras usted lee este artículo, habrá muchas personas que están siendo estafadas. El alto consumo de las nuevas tecnologías, medios y formas de comunicación, han hecho que este tipo de casos se den a diario en todo el mundo, generando muchas veces, pérdidas económicas millonarias.

Pero ¿Por qué Victor Lustig tuvo la capacidad de llevar a cabo semejante estafa? ¿Cuáles fueron las claves de éxito de ésta estafa y de todas las que él realizó a lo largo de su vida? Según la psicología, la psique humana[2] es el orden mental establecido para el funcionamiento del intelecto, la emoción y la voluntad, los tres elementos de acción del ser humano. A lo largo del tiempo se ha demostrado que, manipulando uno o todos estos elementos, se puede lograr manejar la mente del ser humano para que éste actúe según los deseos del estafador o, al que llamaremos de ahora en adelante, el atacante.

Recepción: 29/01/2016 - Aceptación: 15/06/2016

(1) Victor Lustig (4 de enero de 1890 – 11 de marzo de 1947), https://es.wikipedia.org/wiki/Victor_Lustig (2) Psique humana - http://www.significados.com/psique/ (3) Frank William Abagnale, Jr. (Bronxville, 27 de abril de 1948), https://es.wikipedia.org/wiki/Frank_Abagnale_Jr.

Frank William Abagnale Jr.[3] es un vivo ejemplo de los resultados que se obtienen por la manipulación de la psique humana. A los 19 años de edad, Frank ya había trabajado por dos años como copiloto autorizado de la compañía Pan Am[4], gracias a que, usando engaños, obtuvo un uniforme de la aerolínea y pudo falsificar una identificación de trabajo. Falsificó cheques y antes de cumplir los 20 años, Abagnale había cometido fraudes por un valor de 2.5 millones de dólares. Laboró once meses como pediatra certificado del Hospital de Georgia utilizando documentos falsos; además fingió ser un abogado graduado de Harvard, que le permitió ejercer la abogacía por varios meses. Definitivamente Frank supo aprovechar la manipulación de la psique humana para conseguir lo que se propuso.

La producción cinematográfica "Catch me if you can"[5] del famoso director Steven Spielberg trata de mostrar las técnicas que Frank Abagnale Jr. utilizó para cometer los fraudes que se le imputaron.

En nuestros tiempos, las medidas de seguridad se han incrementado en las organizaciones para que, las formas de engaño que Victor Lustig y Frank Abegnale utilizaron, no tengan un gran impacto. Ahora existen instituciones para averiguar si se puede realizar una transacción sobre un inmueble, cosa que en los tiempos de Lustig y la venta de la Torre Eiffel no existía. Ahora existen mecanismos de seguridad en los cheques, billetes, documentos de identidad, entre otros, que reducen en gran medida las posibilidades de fraude, pero, la manipulación de la psique humana sigue siendo igual de efectiva como en los años en los que estos estafadores se mantuvieron activos.

INGENIERÍA SOCIAL

A) *Origen y Evolución del término*

El empresario y filántropo holandés J. C. van Marken comenzó a impulsar el concepto de la Ingeniería Social orientado al trato emocional que en el año 1894 no era cubierto en las industrias; la concepción de un departamento de Recursos Humanos no existía, por lo tanto, los ingenieros sociales eran los que se encargaban de lidiar con los problemas personales de los empleados de la empresa a las que estaban designados, con el objetivo de mantener el rendimiento laboral. En primera instancia, la Ingeniería Social se definió como un método para ayudar al ser humano, pero con el tiempo, el concepto se fue deformando a tal grado que, Edward L. Bernays, publicista y periodista, la utilizó para poder dominar a las masas, que a su criterio eran indisciplinadas, carentes de principios morales y por lo tanto, debían ser "guiadas". Por tanto comenzó a usar la Ingeniería Social como medio para manipular a las personas a su conveniencia.

B) *Ingeniería Social en Informática*

El primero en usar el término "Ingeniería Social" en el ámbito de la seguridad informática fue el hasta hoy reconocido como el mejor hacker del mundo, Kevin Mitnick[6], quien sostiene que la Ingeniería Social se refiere a la aplicación de técnicas, que los hackers utilizan para engañar a un usuario autorizado de sistemas informáticos de una compañía para que revele información sensitiva, o para lograr que de forma insospechada realice acciones que creen un hueco de seguridad que pueda ser explotado.

El fin del atacante que aplica ingeniería social es el de explotar al eslabón más débil de la organización, el usuario. Dependiendo de su osadía, el atacante puede utilizar herramientas tecnológicas o incluso los encuentros cara a cara para obtener la información que necesita. Es importante reconocer que, no solamente el usuario de los sistemas está expuesto a sufrir un ataque de Ingeniería Social; el mismo personal de seguridad informática está expuesto e igual de vulnerable, situación que pudo ser comprobada por el Experimento Robin Sage[7], Fig. 1.

Fig. 1. Experimento Robin Sage

(4) Pan American World Airways, https://es.wikipedia.org/wiki/Pan_Am (5) Catch Me If You Can (2002), http://www.imdb.com/title/tt0264464/ (6) Kevin Mitnick (6 de Agosto de 1963) https://es.wikipedia.org/wiki/Kevin_Mitnick (7) Resultados del Experimento Robin Sage - http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf

Considerando que los ataques de Ingeniería Social están basados en el estudio del comportamiento humano, entonces la principal premisa es: "¿Por qué crackear una contraseña cuando simplemente se puede preguntar por ella?". Según el Dr. Robert Cialdini, existen motivadores básicos en las personas por medio de los cuales se invita a alguien a actuar[8]:

1. ***Reciprocidad:*** la gente siempre siente que le debe un favor a aquellos que han hecho algo por ellos. Sobre todo cuando lo que se hizo es algo significativo, inesperado y personalizado.
2. ***Orientación Social:*** siempre buscamos un modelo a seguir, a alguien que nos oriente o nos diga lo que tenemos que hacer.
3. ***Consistencia / Compromiso:*** desarrollamos patrones de conducta que se convierten en hábitos y nos comprometemos con ellos como modo de vida
4. ***Aceptación:*** queremos "encajar" en determinado escenario y al buscar la aceptación nos dejamos persuadir por aquellas personas que nos gustan o admiramos.
5. ***Autoridad:*** somos receptivos a las órdenes y peticiones de las personas que representan autoridad jerárquica.
6. ***Tentación:*** tendemos a conseguir aquello que está limitado o prohibido para nosotros, incluso, realizando acciones que en situaciones o escenarios cotidianos no haríamos.

C) *Técnicas de Ingeniería Social en la Seguridad Informática*

Basado en los motivadores del ser humano, propuestos por el Dr. Robert Cialdini, existen diversas técnicas utilizadas para realizar ataques de Ingeniería Social, tales como:

1. ***Baiting:*** esta técnica juega mucho con la psique humana. El atacante puede dejar un dispositivo que contenga un virus o malware, como una memoria USB, en algún área para que cualquier persona de la organización pueda encontrarla. La víctima seguramente la conectará a su computadora para revisar que pueda tener la memoria y en ese momento es cuando el malware puede ser inyectado al sistema.

2. ***Phishing:*** posiblemente una de las técnicas más viejas pero también una de las más efectivas, ya que los atacantes tratan de utilizar diferentes niveles de influencia a través de correos electrónicos que aparentan ser de una compañía legítima, como un banco, una institución de gobierno, entre otras, como vemos en la Fig. 2. Generar miedo a través de un correo electrónico, hace que la persona tome decisiones basadas en sus emociones más que en su sentido común. Otra táctica que se vuelve muy efectiva al atacar usando phishing, es la de hacerse pasar por una figura que represente autoridad dentro de la organización; difícilmente las personas se negarán a realizar algo si la orden de hacerlo viene "directamente" del Gerente General de la compañía en la que trabaja.

Fig. 2. En el año 2014, se propagó un correo electrónico que aparentaba ser del Ministerio de Hacienda de El Salvador, haciendo un llamado al contribuyente a ponerse al día con sus obligaciones. En el correo se colocaba un link para descargar malware

3. ***IVR o Phone Phishing:*** esta técnica utiliza una copia del sistema IVR (Respuesta de Voz Interactiva, por sus siglas en inglés) de un banco o cualquier otra institución. La víctima es manipulada (por lo general, con un ataque de phishing) para que realice una llamada telefónica a un número gratuito para, por ejemplo, hacer una verificación de la información de su cuenta bancaria. Por lo general, estos sistemas rechazarán de forma intencionada el ingreso de las credenciales del usuario, con el objetivo de que éste introduzca su PIN varias veces. Algunos atacantes más avanzados y arriesgados, trasladan las llamadas a "agentes de call center" para cuestionar puntos específicos a los usuarios.

4. ***Quid Pro Quo:*** esta técnica se basa en que el atacante promete algún beneficio a la víctima a cambio de información sensible de la organización o del mismo usuario. Por ejemplo, el atacante podría haber investigado alguna carencia sobre algún sistema de uso diario en la organización y puede llamar a un usuario haciéndose pasar por personal de soporte técnico para "solventar ese problema" pero para hacerlo, le pide a cambio las credenciales de inicio de sesión a dicho sistema.

(8) "Influence: The Psychology of Persuasion", 1984, Dr. Robert Cialdini.

5. ***Pretexting:*** es una de las técnicas más elaboradas, ya que el atacante debe crear un buen pretexto o incluso, un buen escenario para poder robar información importante y sensible a la víctima, al contrario del phishing que lo que busca es generar miedo en la mayoría de los casos, el pretexting busca ganarse la confianza de la víctima.

6. ***Farming:*** con esta técnica, el atacante busca crear una relación personal con la víctima, creando un entorno de confianza basado en la información que el atacante ha investigado de su objetivo, donde las principales fuentes de información son las redes sociales. Este es un ataque un poco más complejo, ya que se pueden utilizar otras técnicas en conjunto para que el ataque sea más efectivo.

D) *Efectos de los ataques de Ingeniería Social*

En la mayoría de los casos, el uso de técnicas de Ingeniería Social solamente representa el principio del ataque en sí. Recordemos que lo que se busca, es vulnerar la seguridad de la infraestructura informática y una vez alcanzado el objetivo, la posibilidad de ataques a realizar puede volverse hasta infinita y con distintas variantes.

No los mencionaremos a todos, porque un solo artículo no alcanzaría para ello, pero algunos virus y malware que los atacantes utilizan una vez cumplido el objetivo de la Ingeniería Social son los siguientes:

1. ***Bombas Lógicas:*** son aplicaciones o parte de una aplicación que espera que se cumplan una o más condiciones pre-programadas para que, en ese momento se ejecute la acción maliciosa. Por ejemplo, si se engañó al usuario para que descargara una aplicación para "eliminar" cualquier spyware de su equipo, la bomba lógica podría estar programada para que se ejecute luego de haber hecho el primer escaneo a la computadora. Entre las acciones maliciosas que una bomba lógica puede realizar están: eliminar información del disco duro, esparcir virus en la pc que se aloja y en las que estén conectadas a la red, dejar puertos abiertos, entre otros.

2. ***Backdoors:*** permiten al atacante tener acceso al sistema evitando los algoritmos de seguridad (autentificación) para poder acceder a él. En la mayoría de los casos, las puertas traseras o backdoors son utilizados con fines maliciosos y generados por el atacante, incluso, existen fabricantes de software que en sus aplicaciones incluyen backdoors secretos para que sean utilizados como medios de conexión al momento de realizar soporte a los sistemas, convirtiéndose en una vulnerabilidad fácil de explotar dentro de la infraestructura de informática.

3. ***Troyanos:*** tomando como referencia la historia del Caballo de Troya, estos virus se caracterizan por aparentar ser aplicaciones buenas pero que internamente pueden contener algún elemento malicioso (por ejemplo, una bomba lógica). Se encuentra comúnmente en aplicaciones de descarga directa, P2P, en generadores de llaves de instalación de productos, juegos descargados ilegalmente, entre otros. Una vez que la aplicación o el archivo residen en la computadora de la víctima, se pueden generar estragos en el sistema sin que el usuario se percate.

4. ***Botnets:*** es el conjunto o red de robots controlados por el atacante. Cuando una computadora es infectada, esta pasa a formar parte de esta red para que el atacante la utilice para los fines que él necesita; por lo general, las botnets son utilizadas para hacer envío de spam, generar ataques de denegación de servicios, instalar keyloggers o cualquier otro malware en la red, o utilizar las características de hardware de los equipos que pertenecen a la botnet para aumentar la capacidad de cálculo. Kevin Mitnick utilizó, lo que en la actualidad sería catalogado como una botnet, para poder descifrar un potente algoritmo de seguridad diseñado por Tsutomu Shimomura[9], que protegía un software para el control de teléfonos móviles y varias herramientas de seguridad en internet.

5. ***Ransomware:*** Es una aplicación que realiza un secuestro de la información en la computadora de la víctima pidiendo un rescate por ella, como podemos ver en la Fig. 3. Una vez que el ransomware está alojado en el equipo, comienza a encriptar los archivos que el usuario comúnmente utiliza para realizar sus actividades diarias: archivos pdf, doc, xls, jpg y similares, generando un cifrado de tipo asíncrono, donde se genera una llave privada y una llave pública. Una de estas llaves tiene la capacidad de encriptar los archivos y la otra de desencriptarlos, por lo que, el atacante, almacena la llave que se utilizará para desencriptar los archivos, en un servidor externo, no accesible para la víctima. Una vez que el pago se haya realizado, según el atacante, se le entregará la

(9) *https://en.wikipedia.org/wiki/Tsutomu_Shimomura*

llave de desencriptación a la víctima para que recupere sus archivos. Existe un plazo de tiempo para realizar el pago del rescate, de excederse el tiempo, el atacante amenaza con eliminar la llave de desencriptación, que, de suceder, será imposible eliminar el algoritmo de cifrado aplicado a los archivos. A finales del 2014 e inicios del 2015, este ataque se hizo común, afectando mayormente a México en el área latinoamericana.

Fig. 3. Pantalla que notifica a la víctima que toda su información ha sido encriptada, que debe pagar el monto establecido en el tiempo determinado por el atacante

ESTADÍSTICAS

Según una investigación realizada por el sitio www.social-engineer.org[10] en Estados Unidos, las 3 principales técnicas de Ingeniería Social utilizadas para cometer fraude, robar información, entre otros fines son las siguientes:

1) ***Phishing:*** recordemos que ésta técnica se refiere al envío de correos electrónicos de parte de instituciones que aparentemente son las reales, con el objetivo de generar confianza al usuario o de robarle su información. A diario se envían 294 billones de correos electrónicos, que representan 107 trillones de envíos al año, de los cuales, el 90% son spam y virus.
   El phishing representa el 77% de los ataques basados en Ingeniería Social; solo el año pasado, 37.3 millones de usuarios reportaron haber sido víctimas de este tipo de ataque, donde el factor común era simular ser instituciones bancarias pidiendo a los usuarios que hicieran clic sobre enlaces que venían embebidos en el mismo correo electrónico.

2) ***Vishing:*** técnica que se utiliza para que a través de una llamada telefónica o mensaje de texto, el atacante pueda obtener información de la víctima o que pueda influenciarlo a realizar acciones convenientes al atacante. Este tipo de ataque puede incluir tecnologías que oculten el número telefónico real del atacante y que lo sustituya por un número cualquiera o por otro que sea de confianza de la víctima. Solo en el año 2012, al menos 2.4 millones de clientes se convirtieron en objetivos de fraude telefónico y en el primer semestre del 2013 se contaban 2.3 millones de víctimas. Se calcula que la pérdida por cada organización o usuario víctimas de este ataque asciende a $42,546. Del 100% de las víctimas encuestadas, se determinó que el 60% dio clic sobre un link que le enviaron a través de un mensaje de texto, 14% respondieron el mensaje y el 26% realizó la llamada al número indicado.

3) ***Impersonation:*** es una técnica basada en el pretexting, en donde el atacante genera un escenario de confianza para la víctima con el objetivo de obtener información sensible, acceso a una organización o a un sistema de información.
   Según esta investigación, en 2013 se reportaron 1.8 millones de víctimas que fueron atacadas con robo de identidad, entre ellas, médicos que participaron en una red de su profesión, donde los ataques demostraron un 80% de suplantación de identidad. Cada una de las víctimas ronda un promedio de 41 años y se estima una pérdida por cada uno de $4,187.00. Del 100% de atacantes, al menos un 80% logró evadir controles de seguridad.

En el caso de Latinoamérica, ESET[11] presentó su Security Report 2015[12], donde destacan que el ataque que más ha crecido a lo largo de los últimos 5 años es el de Accesos Indebidos a la Información, tal como podemos verlo en la Fig. 4. De los 14 países encuestados, en 9 países, más de la mitad de las organizaciones declararon

(10) Social-Engineer - http://www.social-engineer.org/social-engineering/social-engineering-infographic/ (11) ESET Latinoamérica - http://www.eset-la.com/compania (12) ESET Security Report 2015 - http://www.welivesecurity.com/la-es/2015/03/19/eset-security-report-2015-estado-seguridad-corporativa-latinoamerica/

haber tenido problemas con este ataque. La pérdida de información es solamente una de las consecuencias al caer en este tipo de ataque. Las organizaciones que lo sufren tienden a perder reputación, tal como sucedió con Ebay[13] o Target[14], al exponer a sus usuarios al robo de sus credenciales debido a fallas en sus sistemas.

Fig. 4. Crecimiento de los últimos 5 años correspondiente al Acceso Indebido de la Información

Cabe destacar que en la región centroamericana, Panamá, con un 69%, posee el porcentaje más alto de organizaciones que sufrieron este tipo de ataques; seguido de Honduras con un 54%, Nicaragua con 53%, Costa Rica con un 50%, Guatemala con 48% y El Salvador con un 46%.

ESCENARIO

Para este artículo se ha decidido presentar un escenario típico de ataque de Phishing. El atacante generará un correo electrónico para enviarlo a "n" cantidad de víctimas, Fig. 5; dicho correo electrónico será enviado en nombre del equipo de soporte técnico de Gmail, indicándole al usuario que existe una amenaza que puede robar sus credenciales de inicio de sesión de su cuenta de correo, por lo tanto es necesario y de carácter urgente que configure sus opciones de seguridad de forma inmediata. Se agrega un enlace en el cuerpo del correo electrónico para que el usuario de clic en él y haga lo que se le pide. Lo importante acá es que el link lo llevará a un servidor web que tiene una página de inicio de sesión de Gmail clonada, Fig. 6.

Fig. 5. Creación de correo electrónico en equipo del atacante

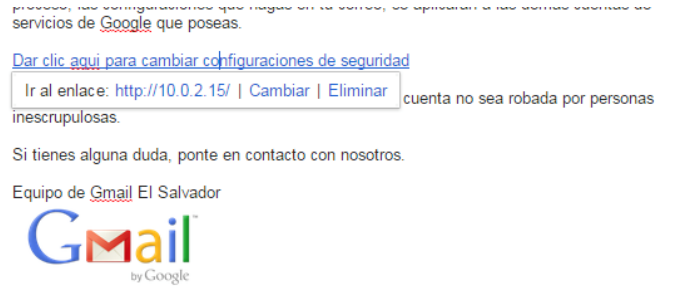

Fig. 6. Dirección real del servidor con la página web clonada a la que apuntará el enlace del correo electrónico

Al dar clic sobre el enlace, el atacante recibirá en su terminal de monitorización la notificación del equipo que se está enlazando con el sitio web clonado,

(13) Caso Ebay - http://www.welivesecurity.com/la-es/2014/05/21/ebay-confirma-brecha-seguridad-recomienda-cambiar-contrasenas/ (14) Caso Targert - http://www.welivesecurity.com/la-es/2014/05/05/renuncia-ceo-target-tras-grave-falla-sistemas/

Fig. 7, y al mismo tiempo, la víctima es redireccionada al servidor con la página web clonada para que ingrese sus credenciales de inicio de sesión, Fig. 8. Una vez que el usuario ingrese los datos de inicio de sesión y de clic sobre el botón "Sign In" enviará de forma inmediata sus credenciales al atacante que lo está monitorizando, Fig. 9.

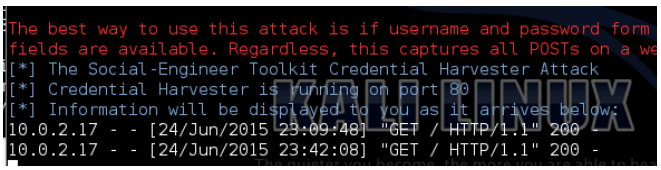

Fig. 7. Notificación en máquina de atacante de conexión de una víctima al sitio web clonado

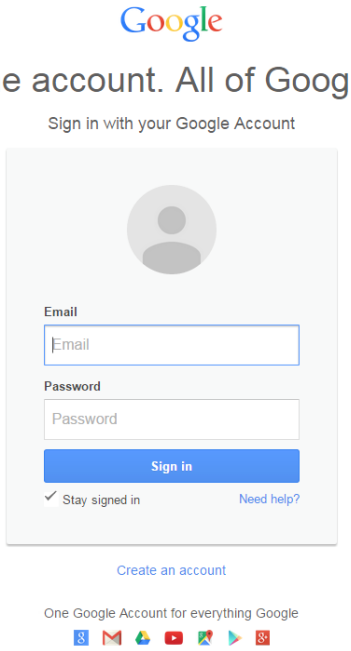

Fig. 8. Sitio web que se le presenta a la víctima con la página de inicio de sesión de Gmail clonada

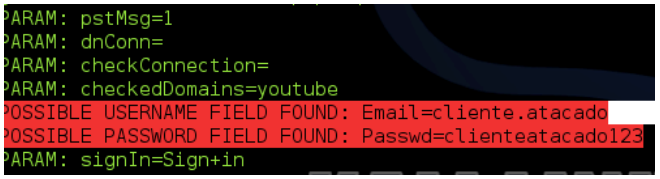

Fig. 9. Credenciales de inicio de sesión de la víctima recuperadas por el atacante

RECOMENDACIONES

En la actualidad, no existe hardware o software con la capacidad de detener los ataques de Ingeniería Social en un 100%. Si bien es cierto que, la mayoría de ataques utilizan algún tipo de tecnología, el sentimiento de miedo, el sentido de urgencia o cualquier otra manipulación de la psique humana que suframos, no será detectado por ellos. Los resultados y las consecuencias estarán definidos por la víctima, que al final es el eslabón más débil en la cadena de seguridad de la infraestructura de una organización.

Pero no todo está perdido, a continuación se harán algunas recomendaciones que deben considerarse para minimizar las vulnerabilidades que se puedan generar en la organización a partir de los ataques de Ingeniería Social, basadas en la educación al usuario de los sistemas de información:

1. ***Realizar acciones defensivas:*** es importante educar al usuario para que sepa cómo prevenir un ataque de Ingeniería Social o qué hacer al momento de encontrarse con un posible ataque. Debe proveérsele de lineamientos y políticas que deben seguir para evitar convertirse en víctimas, como por ejemplo: no descargar ni abrir archivos adjuntos de correos electrónicos de remitentes desconocidos o dudosos; no dar clic sobre enlaces sin antes haber verificado hacia dónde realmente redireccionan los mismos; no ingresar a sitios web de dudosa reputación; no complementar información en formularios que no aparenten ser seguros; no compartir con nadie sus credenciales de inicio de sesión, incluyendo el personal de informática, nadie más que el usuario debe conocerlas; mantener actualizados, tanto el sistema operativo, las aplicaciones así como los software antivirus, entre otras.

2. ***Realizar pruebas de penetración en la infraestructura de seguridad de la organización:*** es importante dimensionar el nivel de seguridad configurado en la infraestructura de la organización, para ello, se deben realizar pruebas de penetración para encontrar las vulnerabilidades que puedan existir con el objetivo de solventarlas o por lo menos reducirlas. El mismo personal de informática puede encargarse de llevar a cabo estas pruebas, pero es recomendable que se contraten agentes

externos para que lo hagan, garantizando que los resultados obtenidos de las pruebas servirán para mejorar las medidas de seguridad adoptadas por la organización. Solamente conociendo las vulnerabilidades que tenemos sabremos como contrarrestar las amenazas.

3. ***Vivir una filosofía de seguridad:*** no se trata de entrar en paranoia sobre la seguridad informática, pero es necesario que la seguridad se convierta en una filosofía de vida en la organización, que tanto los usuarios de los sistemas como el personal de informática permanezca en constante vigilancia sobre los posibles ataques de Ingeniería Social de los que podrían ser víctima; continuamente se deben realizar talleres, charlas, capacitaciones y aplicación de nuevas formas de prevención de ataques según la evolución que estos tengan; hacer sentir a los usuarios que forman parte activa de la organización, los llevará a usar con responsabilidad los sistemas de información.

Conclusiones

Aunque el hardware y software destinado a la administración de seguridad informática es de suma importancia para una organización, no debe olvidarse que, igual de importante es el usuario de los sistemas de información. De nada sirve tener configurado eficientemente nuestro hardware y software, si al final el usuario puede ser manipulado fácilmente para que entregue credenciales de inicio de sesión, información sensible de la empresa o incluso hasta acceso físico a las instalaciones de la organización a un atacante. Es necesario educar a nuestros usuarios para que en lugar de convertirse en el eslabón más débil de nuestra infraestructura de seguridad, nos ayuden y se conviertan en nuestros aliados en contra de los ataques y amenazas que a diario intentan explotar nuestras vulnerabilidades; tenemos que enseñarle al usuario que no todo lo que brilla es oro y por más tentadora que parezca alguna oferta o publicidad en la web que nos lleve a sitios sospechosos, debemos evitar su visita. El usuario tiene que aprender a no dejarse intimidar por las amenazas, hay que enseñarle que lo mejor es ignorar las tácticas que intenten atemorizarlo. Muchas veces, hacer uso del sentido común nos puede ayudar a prevenir las duras consecuencias que pueden generar los ataques de Ingeniería Social.

Referencias

LIBROS

[1] Bio. TheBiography.com.
Disponible en: http://www.biography.com/people/victor-lustig-20657385

[2] Psique.
Disponible en: http://definicion.de/psique/

[3] Kaspersky Lab Daily. Santiago Pontiroli.
Disponible en: https://blog.kaspersky.es/ingenieria-social-hackeando-a-personas/2066/

[4] Trend Micro. José Miguel Rufo.
Disponible en: http://www.trendmicro.es/newsroom/pr/cinco-motivos-por-los-que-las-trampas-de-la-ingeniera-social-funcionan/

[5] C. Tori, (2008). Hacking ético. Rosario, Argentina: el autor. pp. 86-104

[6] Symantec Corporation.
Disponible en: http://www.symantec.com/connect/blogs/what-social-engineering

[7] Social Engineer.
Available: http://www.social-engineer.org/resources/social-engineering-infographic/

[8] ESET. We Live Security.
Available: http://www.welivesecurity.com/la-es/articulos/reportes