Lámpsakos | N°. 10 | pp. 17-19 | julio-diciembre | 2013 | ISSN: 2145-4086 | Medellín - Colombia

SEGURIDAD EN ACTIVOS DE INFORMACIÓN HUMANOS

SECURITY IN HUMAN INFORMATION ASSETS

Jorge Mario Cadavid-Aguirre, Ing.
Fundación Universitaria Luis Amigó
Medellín, Colombia
jmariocadavid@gmail.com

[Recibido el 10-05-2013. Aprobado el 10-06-2013]

A partir del año 2010 América Latina ha sido el nuevo objetivo en la mira para los ciberdelincuentes, ya que el crimen cibernético marcó una subida de hasta un 40% en 2012 [1]. Si se hace un análisis más detallado mes a mes se tiene que en febrero, mediante el uso de novedosas técnicas de Ingeniería Social ─MSIL/Agent.NKY, mejor conocido como Poker Agent y el falso video sobre Justin Bieber con Selena Gómez─, se hicieron significativos estragos en las redes sociales [2]. En marzo, ESET Latinoamérica detectó un correo electrónico que simulaba provenir de Mercado Libre, en donde se informaba que el destinatario "ha sido suspendido para operar"; se trataba pues de un caso de ingeniería social y *phishing* o suplantación de identidad. [3] Finalmente el mes pasado, nuevamente el protagonismo fue para los ataques de ingeniería social y *phishing;* las amenazas más destacadas fueron suplantación a la Banca en Panamá y el famoso ataque a la agencia de prensa The Associated Press (AP) [4], hecho que repercutió incluso en Wall Street.

El éxito de este tipo de técnicas, es la explotación de vulnerabilidades no en la parte técnica ni tecnológica de la organización, sino en el factor humano. Se aprovecha el conocimiento de la parte psicosocial del individuo y de metodologías de manipulación para explotar sentimientos como la confianza, la curiosidad, la inocencia, la desinformación, la atracción física y la sexualidad, la reciprocidad, las ganas de ayudar, la lástima y la aprobación social entre otros muchos.

Teniendo en cuenta el contexto latinoamericano descrito anteriormente, se realizó la ponencia orientada a concientizar al usuario final en materia de seguridad de la información.

INGENIERÍA SOCIAL; EXPLOTANDO A LOS HUMANOS.

"Hecha la ley, hecha la trampa". Conforme avanza la tecnología y se mejoran y reestructuran los sistemas de seguridad, así también, a la par con esta, los atacantes avanzan rápidamente en el desarrollo de estrategias y formas de evadir los perímetros de seguridad de las empresas, apoyados en nuevos vectores de ataque o mejorando los ya existentes; por ejemplo el caso de las APT (*Advanced Persistent Threat*) que son amenazas persistentes como la in-

Citación de artículo, estilo IEEE:
J.M Cadavid-Aguirre, "Seguridad en Activos de Información Humanos", Lámpsakos, N° 10, pp. 17-19, 2013.

geniería social. Esta modalidad de fraude no es algo nuevo, recordemos la famosa estafa nigeriana, timo 419 o timo nigeriano, donde por medio del correo estafaban a las personas inocentes. Las sumas solicitadas son bastante elevadas, pero insignificantes comparadas con la suma de dinero o el gran premio que las víctimas esperan recibir. Pues bien, este tipo de engaños ahora usan las TICS para lograr su cometido.

PERO ENTONCES, ¿QUÉ ES LA INGENIERÍA SOCIAL?

Podría definirse como la explotación de la seguridad de un sistema, orientada al factor humano, no a la parte técnica ni tecnológica de la organización, mediante el uso de técnicas de manipulación y engaños para obtener información sensible. La información sensible no es más que datos "intransferibles" que identifican a una persona en la red o en la vida real. Según laboratorios ESET "La Ingeniería Social puede definirse como una acción o conducta social destinada a conseguir información de las personas cercanas a un sistema. Es el arte de conseguir de un tercero aquellos datos de interés para el atacante, por medio de habilidades sociales. Estas prácticas están relacionadas con la comunicación entre seres humanos". [5].

¿CUÁL ES LA RELACIÓN ENTRE LA INGENIERÍA SOCIAL Y LA SEGURIDAD INFORMÁTICA?

La seguridad de la información busca mantener la integridad, confidencialidad y disponibilidad de la información mediante estrategias y tecnologías que protejan los activos de la misma. Hay que entender que las personas deben ser consideradas como dichos activos, puesto que conocen procesos críticos y almacenan datos e información sensible. Cuando se realiza un ataque dirigido a infraestructura con herramientas y técnicas avanzadas de penetración de sistemas y *hacking*, este demanda mucho tiempo, dinero y esfuerzo.

Mientras que cuando un ataque es dirigido a los activos de información Human O.S. (*Human Operate System*), mediante métodos de ingeniería social, el ciberdelincuente evitará todos los sistemas de control y tecnologías de seguridad haciéndole un *bypass* al sistema de seguridad por completo.

Por lo tanto, las empresas pueden comprar las mejores soluciones, las más costosas del mercado –software o hardware– y tener los mejores controles de seguridad para proteger sus activos, pero no será de gran utilidad si los empleados no son conscientes del valor de la información con la que trabajan. "la seguridad de una compañía es tan fuerte como el eslabón más débil de la cadena". De nada sirve tener el mejor Firewall, IDS, HoneyPOT, Antivirus, HIPS, Endpoint Protection, ni conexiones cifradas, si un usuario inocente da clic a cualquier link e instala software de sitios de dudosa confianza. Esas malas prácticas arrojan por la ventana la seguridad de miles de dólares de la empresa.

CONCLUSIONES

Es muy importante tener en cuenta, dentro de las estrategias de seguridad de la empresa, la concienciación, capacitación y educación del usuario final. Hay que enseñarles a identificar el valor de la información con la que trabajan diariamente, la importancia de sus acciones y hábitos para mantener un nivel adecuado de seguridad.

El éxito de los desarrolladores de malware, virus y spammers depende casi en su totalidad de su capacidad de disfrazar el malware y el spam con ingeniería social. Según Microsoft el 45% del malware necesita interacción con el usuario [5]. La idea es subir un poco el nivel de paranoia, ser muy prudentes, no dar clic a cuanto link aleatorio llega, no dar permisos a cuanto proceso lo solicita, leer muy bien y pensar antes de actuar. La mayoría de usuarios no leen, solo ven colores.

En cuestión de seguridad hay que ser muy proactivos, el subestimar un ataque te hace vulnerable a este, porque no se está preparado. La protección anticipada ahorra tiempo, dinero y esfuerzo al prevenir pérdida de información de manera proactiva, en lugar de los costos generados a partir de las respuestas a un incidente en forma reactiva.

Para asegurar el factor humano contra la ingeniería social es muy necesario fomentar, mediante la educación, comportamientos, conductas y hábitos seguros tanto en el manejo de la información como en el de la navegación a través de Internet. Al final el usuario estará en la capacidad de reconocer y evitar ataques de tipo ingeniería social y *phishing*. En América Latina el 96% de las empresas considera que la importancia de la educación es alta o esencial [6].

REFERENCIAS BIBLIOGRÁFICAS

[1] Trend Micro.(2013). “Latin American and Caribbean Cybersecurity Trends and Government Responses” [Online]. Disponible en: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-tendencias-en-la-seguridad-cibernetica-en-america-latina-y-el-caribe-y-respuestas-de-los-gobiernos.pdf

[2] ESET Latinoamérica.(2013, Feb). Laboratorio “Blog Archive” Resumen de amenazas. Disponible en: http://blogs.eset-la.com/laboratorio/2013/02/28/resumen-amenazas-febrero-2013

[3] ESET Latinoamérica. (2013, Mar). Laboratorio “Blog Archive” Resumen de amenazas. Disponible en: http://blogs.eset-la.com/laboratorio/2013/04/04/resumen-amenazas-marzo-2013

[4] ESET Latinoamérica. (2013, Ab). Laboratorio “Blog Archive” Resumen de amenazas. Disponible en: http://blogs.eset-la.com/laboratorio/2013/05/02/resumen-amenazas-abril-2013/

[5] Microsoft Security. (2011). Intelligence Report volume 11. Disponible en: http://www.microsoft.com/en-us/download/details.aspx?id=27605

[6] ESET. (2012). Prensa – Security Report Latam. Disponible en: http://www.eset-la.com/pdf/prensa/informe/eset-report-security-latinoamerica-2012.pdf