Cuaderno Activa
Revista científica de la Facultad de Ingeniería

Modelo de seguridad de información para determinar el perfil de un candidato o empleado de una organización[*]

Information Security Model to Determine a Candidate or Employee's Profile in a Given Company

Mauricio Amariles Camacho[**]

UNIVERSIDAD DE SAN BUENAVENTURA

Tipo de artículo: resultado de investigación

Recibido: 6 de mayo de 2016
Aceptado: 31 de mayo de 2016

Resumen

Los ciberdelincuentes están enfocándose en obtener información confidencial personal o de una organización a través del usuario. Para clasificar el perfil del usuario, se necesita conocer las vulnerabilidades del ser humano, las cuales el atacante explota, usando estrategias, técnicas psicológicas y herramientas tecnológicas. El perfil del ser humano, puede ser definido a través del resultado cuantitativo y cualitativo que genera la prueba psicométrica. La personalidad es un indicador de los patrones comunes del comportamiento en una situación específica y se reflejan en su actuar y puede ser usado para evaluar el comportamiento y el accionar de un individuo, con el fin de diagnosticar si es susceptible a ser víctima de los ciberdelincuentes. La prueba psicométrica puede ser aplicada a un empleado o candidato dentro de una organización, de esta forma determinar si tiene el perfil psicológico de la víctima. Se propone un modelo que permita utilizarse como herramienta para determinar el perfil de un candidato o empleado, que genere al final del proceso, un informe con los resultados de la evaluación y las recomendaciones para analizar por parte del evaluador.

Palabras clave: Hacking humano; seguridad de la información; vulnerabilidades

Abstract

Hackers focus on obtaining confidential personal or organizational information through users. In order to classify user profile, it is necessary to know the human vulnerabilities exploited by the attacker, by using strategies, psychological techniques and technological tools. Psychological profile of human beings can be defined through quantitative and qualitative outputs generated by the psychometric test. Personality is an indicator of common patterns of human behavior in a specific situation, and may be used to assess an individual's behavior and actions, to diagnose whether he could be a victim of hackers. Psychometric testing is applied on companies' employees or candidates, thus determining if they have the victim's psychological profile. A model is proposed which could be used as a tool to determine the profile of a given employee or candidate, and, at the end of the process, generate a report with the assessment results and recommendations for the evaluator to analyze.

Keywords: Human hacking; Information Security; vulnerabilities

[**] Este artículo es resultado del proyecto de Investigación titulado Modelo de seguridad de información para determinar y clasificar perfiles de usuario en organizaciones

[*] M.Sc. Redes y Seguridad de la Información. Docente Investigador. Facultad de Ingenierías. Universidad de San Buenaventura. Correo electrónico: mauricio.amariles@usbmed.edu.co.

Introducción

Un sistema se considera seguro si cumple con los siguientes pilares fundamentales como son; la confidencialidad, la integridad y la disponibilidad de la información. Para proteger dicho activo tan importante como es la información, la mayoría de las compañías invierten grandes esfuerzos enfocándose en asegurar su infraestructura física, y de software, también se implementan políticas, herramientas de software y hardware buscando salvaguardar la información. Sin embargo, como en todos los sistemas de información, siempre en algún punto dependerá su gestión, de la vigilancia y el control de ser humano, lo que conlleva a que exista un agujero en la seguridad (Mitnick, 2011).

A diferencia de los sistemas informáticos, el humano puede ser persuadido o engañado usando técnicas psicológicas e informáticas. Esta consiste en manipular a una persona para que realice una acción que puede ser o no lo más conveniente para cumplir con cierto objetivo. Este puede ser la obtención de información, conseguir algún tipo de acceso o lograr que se realice una determinada acción (Hadnagy, 2010).

Con la manipulación del usuario, en el contexto de la información individual y los sistemas de información, se han producido enormes pérdidas por los ataques perpetrados. Se presenta como una amenaza constante a la seguridad, y por la conciencia de este fenómeno que es actualmente lento; existe la carencia de un modelo conceptual que represente este fenómeno y que afecta a miles de empresas a nivel mundial empresas (Fujikawa, 2011).

La víctima, tiene un comportamiento y patrón que se caracteriza por tener vulnerabilidades psicológicas tales como, exponer fácilmente la información confidencial, y ser persuasibles ante el engaño y la astucia que logra al manipular sus acciones para alcanzar el objetivo. Interpretar este tipo de factores de comportamiento según las teorías de los factores de personalidad, usando de una prueba psicométrica medible, permitiría determinar el perfil de la víctima.

En la primera parte de este artículo se presentan los antecedentes a nivel mundial sobre las víctimas y las técnicas utilizadas por los ciberdelincuentes; seguidamente, se presenta el modelo propuesto con sus componentes, características, y funcionalidad; por último, las conclusiones.

Antecedentes

Para dimensionar la problemática que existe a nivel mundial sobre la seguridad de la información y su incidencia en los altos costos que pierden las organizaciones sobre su activo más importante como es la información, se describe a continuación algunos antecedentes en el mundo sobre los ataques que se enfocan en la manipulación de los usuarios y que son una real amenaza a la seguridad de la información y su confidencialidad.

Los ataques usados por el cibercrimen, pueden ocurrir tanto a nivel físico como psicológico. La configuración física de estos ataques se produce cuando una víctima se siente seguro: a menudo el lugar de trabajo, el teléfono, la basura, e incluso en internet. La psicología se utiliza a menudo para crear un ambiente rígido que ayuda al ciberdelincuente para engatusar al empleado, con el fin de obtener la información sobre cómo acceder al sistema (Maan, 2012).

Como amenaza a la seguridad de la información, la ingeniería social es efectiva, debido a que el ser humano, como ser social, necesita tener una relación con el otro, por ejemplo la comunicación y la forma como nos comunicamos (vía correo electrónico, a través de una llamada, face-to-face, etcétera.) y la confianza que genera nuestro interlocutor, hace que, de alguna manera, empecemos a entregar información confidencial, y como resultado ser víctima (Mouton, 2016).

Redes sociales como Facebook, Linkedin y twitter, tienen un gran crecimiento en número de suscriptores en línea. Una de las características que tienen las redes sociales son de proveer información de amigos y posibles posibilidades de nuevos contactos, según los amigos que se tienen

en común. Claramente las redes sociales son criticadas con respecto a la seguridad y privacidad de los usuarios, mucha información privada es publicada y compartida con otros, lo que hace cada vez más atractivo este medio para sustraer información confidencial (Irani, 2011).

Para enfrentar las posibles amenazas que se enfocan en los usuarios, se han hecho diferentes metodologías de pruebas de penetración dentro de una empresa usando, por ejemplo, herramientas informáticas. Es así como, durante la prueba se evalúa un grupo de empleados de una Compañía. La prueba determina la vulnerabilidad del empleado y lo métodos para obtener la información deseada usando herramientas informáticas y el desconocimiento de los usuarios sobre la seguridad de la información. Esta información se recolecta en el informe final, que describe los intentos fallidos y los exitosamente culminados (Dimkov, 2010).

La anatomía de un ataque usando la ingeniería social, puede realizarse obteniendo información desde varias fuentes, en la Figura 1, se ilustra el paso a paso de un ataque usando esta técnica.

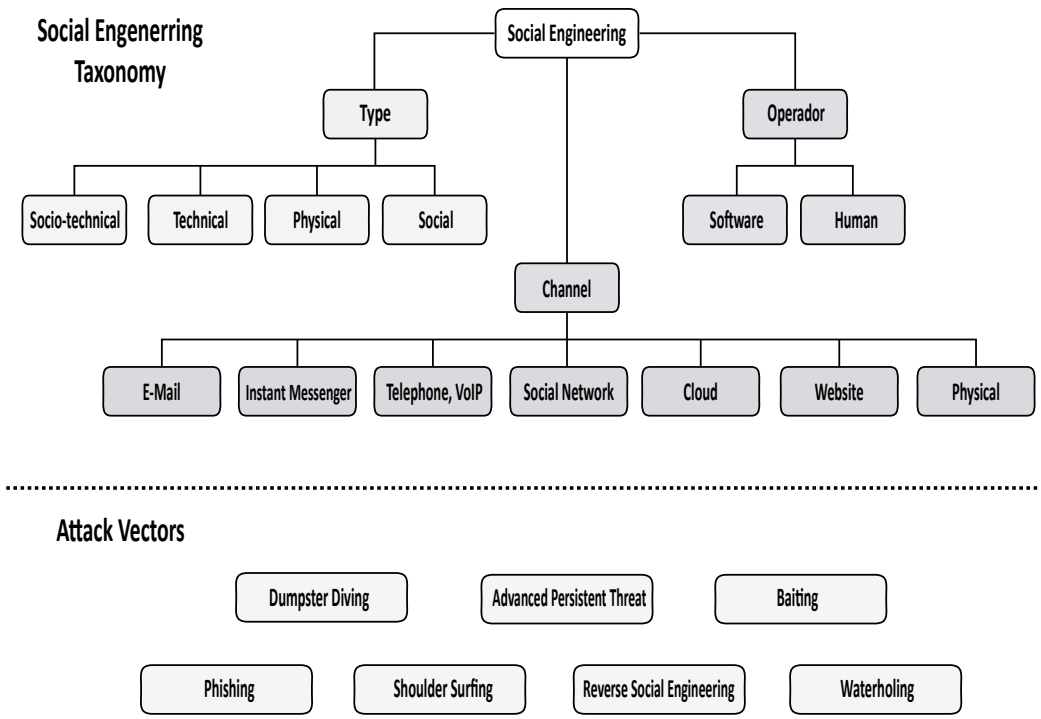

Figura 1. Anatomía de un Ataque enfocado al usuario
Fuente: (Krombholz, 2013)

Las fuentes y los canales donde se obtiene la información pueden variar según sea el caso. Los canales pueden ser vía correo electrónico, redes sociales, sitios web, llamadas telefónicas y las fuentes pueden ser informáticas o humanas. En la mayoría de los casos existe un alto grado de análisis y comprensión de las vulnerabilidades que existen dentro de la organización, con el fin de que el ataque tenga un mayor nivel de éxito (Krombholz, 2013).

Los ciberdelincuentes, atacan en la mayoría de los casos, el punto más débil del sistema, cada vez más personas utilizan e interactúan con un sistema basado en una computadora. Una gran cantidad de investigaciones se ha dedicado a la protección de los activos basados en computadoras, pero mediante la explotación de vulnerabilidades humanas, un atacante puede eludir muchas defensas basadas en herramientas la informática (Bhakta, 2015).

Uno de los aspectos más destacados de la seguridad, que está vinculado a los seres humanos, es la confianza. Se puede asumir que la confianza va a jugar un papel importante en cualquier entorno de seguridad de la información y puede influir en el papel que juega en la seguridad de manera significativa (Kearney, 2014).

Una de las técnicas que se utiliza contra lo usuario es el *phishing*. Un estudio que examina el comportamiento de las víctimas de este delito y por qué caen tan fácilmente en sitios web falsos, el 90% mostró que al recibir un correo electrónico que fue diseñado para parecer sospechoso, abrió el correo electrónico, sino que adicionalmente hizo clic en el enlace proporcionado, juzgando la legitimidad del sitio por la apariencia del contenido y que tan profesional parecía ser. (Hong, 2012).

Modelo propuesto para determinar el perfil

El modelo que se propone está divido en cuatro fases. Cada fase tiene su respectiva función y componente que lo integra dentro del modelo.

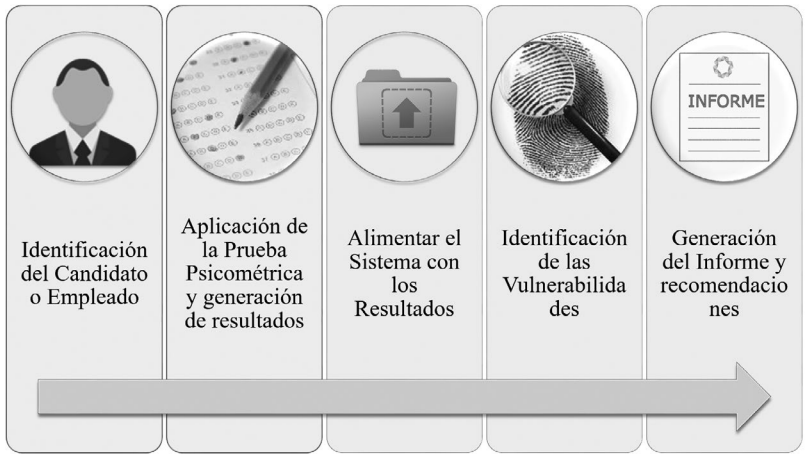

Figura 2. Modelo de clasificación del perfil del candidato o empleado
Fuente: elaboración propia

En la primera fase de la Figura 2, se define cuáles son los actores, y se establece cuál es la población a evaluar (empleado o candidato). Para el primer caso (empleados), se debe evaluar su cargo actual, funciones asignadas, responsabilidades y la relación que existe entre los demás empleados. Los empleados a evaluar pertenecen a diversas jerarquías, desde la recepcionista, oficial de seguridad, hasta los directivos que integran la organización. Para el segundo grupo poblacional (candidato), la organización debe tener en cuenta, el perfil que requiere del futuro empleado a ocupar el cargo y si la información con la cual tendrá acceso, deberá mantener su integridad, disponibilidad y la confidencialidad de la misma.

Una vez aplicada las pruebas psicométricas, en la segunda fase, se generan resultados cuantitativos sobre las variables evaluadas en la prueba psicométrica, los valores y rasgos fundamentales de la personalidad del individuo evaluado (empleado o candidato). La prueba que se aplica desde el modelo propuesto, es de tipo psicotécnico o psicométrico, y se elabora científicamente. Cabe destacar que la prueba tiene mecanismos de control para descubrir el grado de honestidad en la respuesta y de atención suficiente que deriva un resultado válido

Sobre la fase tres del modelo, la identificación de perfiles, características de la personalidad (Omar, 2005), arroja como resultado la identificación de los riesgos o vulnerabilidades que caracterizan la personalidad del individuo evaluado, siendo el caso que se utilizará la manipulación de los usuarios como herramienta para acceder a la información confidencial de la organización. La identificación de las vulnerabilidades del empleado evaluado,

se compara en un banco de hechos, que permite al modelo clasificar el perfil del empleado y las características de personalidad que lo hacen débil ante el engaño o la manipulación.

En la fase cuatro, el seguimiento de la prueba queda consignado en un reporte final, que hace especial énfasis en las debilidades y los mecanismos de seguridad encontrados en el perfil del evaluado. En base al reporte, se toman las medidas correctivas y preventivas, con el fin de salvaguardar la información de la organización y su manipulaciónpor parte de los empleados o futuros candidatos.

El modelo propuesto está compuesto por seis componentes que integran cada fase. En la Tabla 1, se describen las características de cada uno de ellos, además de las funcionalidades con respeto al modelo propuesto.

Tabla 1. Elementos del Modelo

ELEMENTOS		DESCRIPCIÓN
	Identificación del actor	Empleados, o candidato seleccionados para la aplicación de la prueba.
	Aplicación de prueba psicométrica.	Test psicológico que identifica características y rasgos de la personalidad de cada candidato o empleado que se somete a la prueba.
	Resultados de aplicación de la prueba	Datos generados y obtenidos a partir de la aplicación del Test psicológico.
	Alimentar el sistema	Fuente de datos que se le proporciona al sistema.
	Identificación de vulnera-bilidades	Proceso interno del sistema que corresponde a la interacción con parámetros psicométricos previamente establecidos con el fin de encontrar las vulnerabilidades de cada candidato o empleado.
	Generación de informe	Documento con el informe de resultados de la evaluación y las vulnerabilidades que presenta el candidato o empleado. Lista de recomendaciones para la Organización frente a la gestión de la seguridad de la información.

Fuente: elaboración propia (2016).

Conclusiones y trabajo futuro

Un ataque a la seguridad de la información enfocado a los usuarios, puede en general, explotar las vulnerabilidades similares sobre la seguridad de la información en muchas organizaciones. Sin embargo, las fuentes usadas para llevar a cabo un ataque, dependerán del análisis y el objetivo que el atacante desea alcanzar.

Analizar el perfil de los empleados o candidatos a puestos de trabajo que tengan acceso a información confidencial de la Organización, es una manera de minimizar los riesgos que puedan presentarse

sobre la seguridad de la información, ya que no todas las herramientas tecnológicas que se aplican hoy en día, logran detectar este tipo de amenazas.

El modelo propuesto logra caracterizar y determinar las vulnerabilidades del empleado o candidato evaluado, a partir de los rasgos fundamentales de la personalidad, al generar datos cuantitativos que son interpretados por expertos, y determinan su relevancia con respecto al rol que tiene o tendrá dentro de la organización, con respecto al acceso de información confidencial.

Como trabajo futuro, se tiene previsto la aplicación del modelo en cada una de sus fases, sobre un caso de estudio. Se propone que sea un grupo de diez empleados que se encuentren laborando en una Organización y que puedan ser susceptibles a ser víctimas de los ciberdelincuentes.

Referencias

Bhakta, R. &. (2015). Semantic analysis of dialogs to detect social engineering attacks. *In Semantic Computing (ICSC), 2015 IEEE International Conference on*, 424-427.

Dimkov, T. V. (2010). Two methodologies for physical penetration testing using social engineering. *In Proceedings of the 26th annual computer security applications conference*, 399-408.

Fujikawa, M. &. (2011). A Study of Prevention for Social Engineering Attacks using Real/fake Organization's Uniforms Application of radio and Intra-Body Communication technologies. *Sixth international Conference IEEE*, 597-602.

Hadnagy, C. (2010). *Social Engineering: The art of human hacking.* John Wikley & Sons.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, 74-81.

Irani, D. B. (2011). Reverse social engineering attacks in online social networks. *In Detection of intrusions and malware, and vulnerability assessment*, 55-74.

Kearney, W. D. (2014). Considering the influence of human trust in practical social engineering exercises. *In Information Security for South Africa (ISSA)*, 1-6.

Krombholz, K. H. (2013). Social engineering attacks on the knowledge worker. *In Proceedings of the 6th International Conference on Security of Information and Networks*, (pp. 28-35).

Maan, P. &. (2012). Social Engineering: A Partial Technical Attack. *International Journal of Computer Science Issues*, 9-12.

Mitnick, K. D. (2011). *the art of Deception: Controlling the Human Element of Security.* John Wiley & Sons.

Mouton, F. L. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, 186-209.

Omar, A. (2005). Las dimensiones de la Personalidad como predictores de los comportamientos de ciudadanía organiacional. *Estudios de Psicología*, 157-166.

Pipreola riefferii /Autor: Diego Alonso Rivera Vergara