Ingeniería social

Supongamos que una persona desea introducirse al sistema que usted utiliza o accede a información sensible, ya sea personal o de la organización. Los fines que persigue este individuo pueden ser diversos: robo de información confidencial para cometer fraudes cibernéticos, llevar a cabo algún tipo de acción ilegal y responsabilizar al usuario de lo sucedido, cometer un secuestro o simplemente hacer pasar a la víctima un mal momento. Para lograr lo anterior este individuo primeramente deberá identificar plenamente a su víctima. Para ello será necesario recabar algunos datos básicos, como nombre de la organización, dirección, teléfono, nombres de las personas que laboran ahí, tipo de *software* que emplean, plataforma de cómputo instalada, entre otros; y para tener éxito en esta encomienda, requerirá desarrollar ciertas habilidades y aplicar algunas técnicas que en su conjunto se denominan ingeniería social. Según Mitnick (2002) la ingeniería social es el conjunto de técnicas empleadas para convencer y persuadir a la gente de ser alguien que en realidad no es y cuyo fin será obtener información que permitirá realizar alguna acción normalmente de carácter ilegal. Por su parte, Kissel (2012) señala que la ingeniería social es el intento de engañar a alguien para obtener información que podría ser utilizada posteriormente, a fin de cometer algún ataque a la red o a los sistemas informáticos de la organización.

El objetivo de la ingeniería social es muy claro: obtener información sensible, como contraseñas, datos personales, números de cuenta, directorios telefónicos, información confidencial (proyectos innovadores o de investigación) u obtener acceso a sistemas informáticos críticos. Cuando Kevin Mitnick, uno de los más famosos *hackers* durante la década de los ochenta y noventa, fue entrevistado por la BBC, comentó lo siguiente: "la amenaza real en una organización no es la vulnerabilidad de los sistemas, 'hoyos' en los programas, virus informáticos o problemas con la red; la amenaza real podría estar dentro de la misma organización, es decir, el usuario". Y justamente es ahí donde la ingeniería social hace su trabajo, pues a través del engaño y la confianza es el usuario quien brinda información a personas que tratarán de convencerlo de que son parte de la organización (de algún área en particular), directivos, proveedores importantes o tal vez prestadores de servicio.

De acuerdo con Gulati (2003), existen dos formas de operación de los ingenieros sociales: engaño basado en la tecnología y engaño basado en el individuo. El primero consiste en hacer creer al usuario que está interactuando con un sistema de cómputo "real", para generarle un pseudoconflicto de tal forma que se vea obligado a brindar información confidencial (usuario y contraseña) para "resolver" el problema. El segundo se basa en el desconocimiento, la confianza y el impulso natural de todo ser humano para ayudar al prójimo.

Como se mencionó, los ingenieros sociales primeramente ubican a su víctima (persona u

organización), posteriormente recaban toda la información posible, trabajo sencillo en la actualidad, pues se puede acceder a la página *web* para identificar nombre, misión, visión, números telefónicos, dirección física y hasta proyectos que desarrollan. Una vez realizado lo anterior, intentan conocer parte del lenguaje o términos empleados en la empresa, lo cual les permitirá posicionarse fácilmente en el ambiente donde llevarán a cabo su fechoría.

El siguiente paso es el proceso de convencimiento y el engaño. La gran mayoría de los ingenieros sociales tienen la capacidad de convencer a la gente de que son personas de confianza, y que al solicitar algún tipo de información, lo hacen únicamente porque existe una necesidad imperiosa en puerta, o bien porque pretenden ayudarlos a resolver algún "problema", generalmente de carácter informático, que su víctima no sabía que tenía. Una vez que se ha logrado establecer este vínculo de confianza, será sencillo obtener la información solicitada, pues no existirá impedimento alguno para brindarla. Incluso, algunos ingenieros sociales se comunican en más de una ocasión con la misma víctima para seguir obteniendo datos, pues finalmente, el "robo" de información generalmente no es visto como tal, ya que su propietario la sigue conservando, y no es sino hasta tiempo después que se visualizan las consecuencias de este acto.

Para que el personal pueda identificar con mayor facilidad la presencia de un ingeniero social es fundamental la capacitación, enfocada principalmente en aquellos que representan la primera línea de comunicación: recepcionistas, secretarias o personal de seguridad y operativo. Se ha comprobado que los ingenieros sociales prefieren a este tipo de víctimas porque son más susceptibles a recibir y ejecutar tareas sin hacer cuestionamientos, sobre todo si provienen de personas que se hacen pasar por directivos o gerentes de alguna organización, importantes empresarios o personal altamente especializado en tecnologías de la información.

Finalmente, como regla general e independientemente de la capacitación, siempre es recomendable verificar que aquella persona que dice ser, realmente lo sea, en especial cuando solicita información sospechosamente inusual y más aún, si está relacionada con sistemas de cómputo. Esto puede ser mediante una llamada a la empresa donde trabaja para verificar su identidad, establecer políticas muy claras de qué información se puede brindar o compartir y cuál debe ser proporcionada únicamente por el propietario o responsable de esta. La prevención siempre será el mejor camino para el resguardo de nuestra información.

REFERENCIAS

- Gulati, R. (2003). The threat of social engineering and your defense against it, SANS Institute. Recuperado de http://www.sans.org/reading_room/whitepapers/engineering/threat-social-engineering-defense_1232.
- Kissel, R. (2012). Glossary of key information security terms (draft), USA, National Institute of Standards and Technology, DOI: http://dx.doi.org/10.6028/NIST.IR.7298.
- Mitnick, K. (2002). *The art of deception*, USA, John Wiley & Sons.