Contrarrestando la Ingeniería Social: El reto de combatir las vulnerabilidades no informáticas de su organización

Palomá Montaña, Carlos Iván
Universidad Piloto de Colombia
Especialización en Seguridad Informática
carlospaloma@ingenieros.com

Resumen - Día a día, cada vez son más las empresas que comienzan a tener una conciencia de los peligros a los que está expuesta la información de sus organizaciones, tanto así que ya muchas compañías comienzan a contar con un área independiente del área de TI, dedicada exclusivamente al aseguramiento de la información y con un personal capacitado que pueda asumir los retos que surgen día a día y cuya misión es hacer todo lo posible por garantizar un nivel de seguridad básico de la información en sus empresas.

El problema crece cuando las vulnerabilidades dejan de ser sobre los equipos físicos o sobre los servidores y se traslada a otro activo de la organización, muchas veces el activo más descuidado: el personal. A menudo ignorado o no tenido en cuenta dentro de las empresas, el personal puede llegar a representar un gran impacto negativo sobre la organización, pudiendo convertirse en el eslabón más débil en la cadena de seguridad y pudiendo ser el objetivo de ataque simple de cientos de hackers que están a la espera de un movimiento no calculado para atacar.

PALABRAS CLAVES: Ingeniería Social, Principios de la ingeniería social, contramedidas para combatir la ingeniería social, Kevin Mitnick.

Abstract - Every day, companies begin to have an awareness of the dangers they are exposed with their information into organization. Many companies are beginning to have an independent area of the IT area dedicated to the information assurance integrated by a trained staff to meet the challenges that arise every day and whose mission is to make every effort to ensure a basic level of information security in their companies.

The problem grows when vulnerabilities are no longer on physical computers or servers, and is present in another asset of the organization, often the most neglected asset: the staff. Generally ignored or disregarded within companies, staff may represent a great negative impact on the organization, may become the weakest link in the security chain and can be target by simple attacks of hundreds of hackers who are waiting for a not calculated move to attack.

I. INTRODUCCIÓN

La ingeniería social cada vez más está siendo considerada como una ciencia, que se ha venido desarrollando y fortaleciendo a lo largo del tiempo, que tiene unos alcances que no han sido contemplados y cuyo desconocimiento nos expone a unos peligros que aún no dimensionamos. La ignorancia en este campo no nos permite ponderar el daño que puede llegar a representar, relacionado con el robo de información, tanto personal como de la empresa.

II. PROBLEMÁTICA

La información es uno de los activos más importantes con los que puede contar una organización. Las ideas y los conceptos, materializados en la forma en la que se desarrollan las diferentes actividades de la operación diaria, es un activo que en la mayoría de los casos es el resultado de años de

experiencia, en los que se ha logrado el punto en que se encuentra hoy día luego de un arduo trabajo, casi siempre a punta de prueba y error, o en muchos casos, es el resultado de la inversión de diferentes recursos de la compañía -recursos económicos, de tiempo, esfuerzo, etc.- y del aporte de los mismos empleados, representado en una investigación oportuna para la mejora y para el logro de la continuidad de los negocios dentro de la organización. Es aquí cuando la información comienza a tener una mayor relevancia y llega a convertirse en un factor diferenciador entre una empresa y otra: un concepto, una idea, un pensamiento, un procedimiento, un instructivo, un manual y cualquier otro conjunto de datos, indiferente del medio, siempre reflejará el quehacer diario que permite dar continuidad a los diferentes procesos y, por ende, al éxito de la organización.

Con el paso de los años y la evolución de los sistemas informáticos, la calidad de la información creció tanto, hasta el punto de volverse muy valiosa, lo que la convirtió en objetivo directo de millones de hackers y piratas informáticos a nivel mundial, que con sus cientos de técnicas y herramientas encontraron la forma de burlar la seguridad de los diferentes equipos y redes, para hacerse con este premio muy apetecido: la información. A medida que este problema seguía avanzando, se hizo necesario buscar la forma de comenzar a mitigar los posibles problemas que se estaban presentando, por medio de diferentes procedimientos, técnicas, antivirus, anti espías y demás. De esta forma, el objetivo de conseguir la información de una empresa o de una persona en particular, se fue volviendo un negocio para algunos y un reto para otros, al proponerse buscar métodos para evadir todas las diferentes barreras que estaban entre el atacante y la información y comprobar ante los demás hasta donde podían llegar sus conocimientos. En medio de esa carrera por demostrar ser el mejor en obtener cierta información, se comenzó a ver que la gran debilidad de las redes informáticas y de la computación, estaba relacionada con el personal que operaba dichos sistemas dentro de la organización. Debilidades tales como el uso de contraseñas por defecto, un empleado no capacitado o muchas veces un empleado inconforme, era la oportunidad perfecta para ingresar a ese mundo paralelo.

Hoy en día, muchos expertos en seguridad informática siguen creyendo y afirmando que "el eslabón más débil en la cadena de seguridad es el ser humano". De nada sirve tener un equipo asegurado con los mejores estándares a nivel mundial, si la contraseña de acceso configurada sigue siendo la clave por defecto o simplemente una demasiado fácil de adivinar por cualquier persona que quiera ingresar. Es aquí donde nace el concepto de ingeniería social, cuyo objetivo es buscar la debilidad a través del personal de una organización, por medio de diferentes técnicas psicológicas y habilidades que buscan relacionar al atacante con la posible víctima y hacerle caer en un juego, donde el atacante ordena y la victima solo cumple.

La ingeniería social ha logrado incursionar mucho con el paso de los tiempos, tanto que las personas ya no tienen la misma mentalidad de antes, es decir, ya son conscientes que la información puede correr peligro y que por esta razón, los controles mínimos de seguridad de la información deben ser aplicados para que ésta no corra ningún tipo de riesgo. No obstante, muchas veces esto no es suficiente. A pesar de que cada día surjan técnicas nuevas que dificulten la obtención de información por parte del delincuente, estos atacantes cuentan con métodos más audaces para poder irrumpir en las empresas y lograr el objetivo deseado, que casi siempre es buscar la fuga de información.

Los ingenieros sociales han descubierto que las personas más vulnerables de las organizaciones, tienden a ser las personas que cuentan con menos conocimientos, no solo en el área informática, sino en formación académica en general. De igual forma, aquellas personas que son descuidadas, distraídas y

aquellas personas que se pueden persuadir fácilmente.

"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

Kevin Mitnick, reconocido hacker a nivel mundial, por ser un experto en el campo de la ingeniería social durante muchos años, plantea siete principios básicos que todo ingeniero social tiende a usar frente a sus víctimas y son las siguientes:

1. **Buscar un rol en particular**: Casi siempre pasar como un alto ejecutivo, con traje formal y corbata, puede dar la impresión de ser una persona importante, a la cual muchas veces no se les puede cuestionar nada. De esta manera, se puede solicitar información sin que las víctimas noten que están cayendo en la trampa de un atacante.

2. **Todos queremos ayudar**: Por naturaleza, los seres humanos tendemos a ser solidarios y siempre que vemos a una persona indefensa o con problemas lo vemos como una oportunidad para brindarle un poco de ayuda. Estudios en los que se evaluó la mente humana, por cientos de psicólogos, ha demostrado que ayudar a los demás nos pueden hacer sentir que tenemos poder y nos puede hacer sentir bien consigo mismos.

3. **El primer movimiento es siempre de confianza hacia el otro:** Si el ingeniero social logra que la víctima sienta confianza hacia él, va a ser más fácil cumplir el objetivo planteado.

4. **Dar credibilidad de la situación que se plantea y ganar simpatía**: Que junto con el anterior principio, básicamente busca que el ingeniero social gane la confianza de la víctima y crea cada una de las historias que se plantean antes de atacar.

5. **No nos gusta decir NO**: Ya sea por demostrar amabilidad o por demostrar cierto poder a lo que se nos pide, los seres humanos tendemos a evitar decir que no, y menos cuando una persona se acerca en un tono amigable y que antes ha ganado la confianza de la víctima.

6. **A todos nos gusta que nos alaben**: Este principio es el más usado, ya que luego de ganar la confianza de la víctima, se busca reconocer características o habilidades de la víctima, lo que la mayoría de las veces facilita la obtención de información.

7. **Inculcar miedo**: Los ingenieros sociales van a buscar que las víctimas sientan que algo malo va a pasar si no se siguen las indicaciones del atacante. De esta forma, el atacante usa el miedo como un arma que la víctima generalmente no nota.

Queda evidenciado entonces que educar y entrenar al personal de las organizaciones es una de las mejores defensas, y en muchas ocasiones la única forma de combatir la ingeniería social, más si esto se vuelve política de las compañías para combatirla. Cuando se habla de educar y entrenar al personal, se busca hacer jornadas de capacitación y concientización en las que se vean involucradas todas las personas de la compañía y no solamente el personal de TI, como suele suceder. Estas jornadas de capacitación deberían ser dinámicas, logrando que el personal se sienta involucrado y no simplemente regañado o juzgado. Usar carteles o afiches ubicados en sitios estratégicos y a la vista de todos, así como usar el fondo de pantalla en los computadores, suelen ser buenas herramientas de difusión y de

concientización de las políticas de seguridad de la empresa.

"Despertar la conciencia de que es prácticamente seguro de que los ingenieros sociales atacarán su compañía en alguna ocasión y, quizás, repetidas veces"
Kevin Mitnick

Aunque muchos empleados lo saben -y desafortunadamente no todos, lo que hace que no pase de moda-, es la existencia de mensajes por correo electrónico, así como mensajes de texto enviados por los celulares, prometiendo dar valiosas cantidades de dinero a cambio de una consignación en una cuenta extraña, las supuestas loterías que van a dar una gran suma de dinero o aquellos mensajes en los que amenazan con bloquear las cuentas bancarias en caso de no ingresar a un portal con el nombre de usuario y contraseña. Estos suelen ser los mensajes más usados en los que se busca crear ilusiones o intimidar a las víctimas para forzarlas a que realicen algo en concreto que quiere el atacante.

III. CONTRAMEDIDAS DENTRO DE UNA ORGANIZACIÓN:

La tarea del área de seguridad de la información en las empresas, apoyados por el área de TI, busca crear contramedidas que eviten los posibles ataques de ingeniería social, para asegurar los principios de Integridad, Disponibilidad y Autenticidad. De esta forma, se puede:

- Crear un Sistema de Gestión, que permita tener controles para mitigar los posibles riesgos a los que está expuesta la seguridad dentro de la empresa. Se busca crear una serie de actividades que estén coordinadas, en las que se identifique la fase de planear las ideas que se quieren desarrollar, la fase de implementación, en donde se pueda ejecutar lo planeado, la fase de verificación, donde se pueda hacer un seguimiento a todo lo implementado y la fase donde se tramiten las correcciones sobre el sistema de gestión. Todo esto, en un ciclo de retroalimentación constante.

- Definir estándares que sirvan como un modelo o una norma, que permitan guiar a los trabajadores en la realización de sus tareas diarias.

- Configuración de los dispositivos de red, para evitar que los usuarios tengan perfiles y contraseñas por defecto. Contar con software antivirus, anti espías y similares, junto con el debido aseguramiento de las plataformas tecnológicas con las que se cuenta en la organización.

- Desarrollar políticas y protocolos de seguridad, que se apliquen a todas las áreas de la organización. Debe incluir a la gerencia técnica, dependencia que muchas veces tiende a ser una de las principales barreras para implementar soluciones de Seguridad y de TI.

- Clasificar la información de acuerdo a las características de privacidad o confidencialidad y, así mismo, otorgar permisos de acceso, de acuerdo a los roles de cada miembro en la compañía. De esta forma se puede controlar la accesibilidad a los sistemas, a las diferentes áreas y a la información en general.

- Crear planes de formación con el fin de generar conciencia en los trabajadores de los peligros a los que puede estar expuesta la información por falta de conocimiento en la ejecución de sus labores.

- Evaluar y poner a prueba la susceptibilidad de cada uno de los trabajadores por medio de ataques de ingeniería social. Estos ataques se pueden realizar en las auditorías internas o en las jornadas de seguridad. De igual forma, se debe buscar que los empleados aprendan a

oponer resistencia a los ataques de la ingeniería social. Así mismo, se debería modificar las normas de la organización, para enseñarles a los trabajadores a decir NO de acuerdo a las circunstancias.

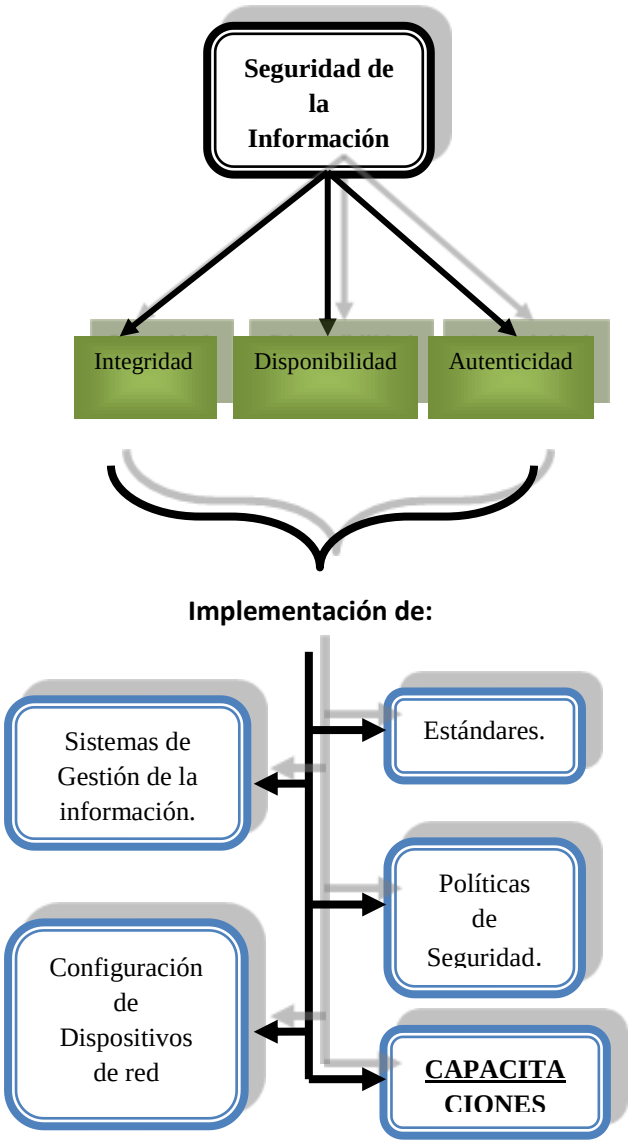

Figura 1 – Implementación de factores para ayudar a garantizar la seguridad en las organizaciones (Palomá, Carlos Iván, 2014)

IV. CONCLUSIONES

1. La ingeniería social es una ciencia que busca la forma de hacer que las personas revelen información por medio de la manipulación de la mente y de las ideas que se plantean de acuerdo a la situación. Es acá, donde los ingenieros de la seguridad de la información, se deben encargar de garantizar que los datos se mantengan seguros y libres de cualquier tipo de intrusión no deseada, garantizando que los servicios y los procesos que se realizan dentro de las organizaciones, sean eficientes y adicionalmente, brindando la disponibilidad, integridad y confidencialidad a la información.

2. Las empresas siempre están buscando mejorar los procesos que tienen, en cuanto a seguridad de la información se refiere, ya sea mediante la implementación de estándares o herramientas especializadas, pero muchas veces dejan de lado el personal, volviéndose el factor más vulnerable y el objetivo principal de diversos atacantes.

3. La principal forma para combatir la ingeniería social dentro de las organizaciones, es brindar capacitaciones en las que se vea involucrado todo el personal de la compañía, desde la alta gerencia, pasando por el personal de TI hasta los trabajadores de limpieza de la empresa.

4. Utilizar el sentido común y hacer preguntas siempre que se reciba un mensaje de correo electrónico o una llamada telefónica sospechosa, puede ser una de las herramientas más valiosas para evaluar un posible ataque de ingeniería social.

REFERENCIAS

- Mitnick, Kevin. El arte de la intrusión. 1° Ed., México D.F., México. Editorial Alfaomega, Abril, 2007. Páginas 380

- "Los 4 principios básicos de la Ingeniería Social", UnPocoDeMucho.com, [en línea]. [Consultado 14 de Marzo de 2014]. Disponible en la Web: http://unpocodemucho.com/los-cuatro-principios-basicos-de-la-ingenieria-social

- "¿Cómo se evita la Ingeniería Social?" Ingeniería Social [en línea]. [Consultado 14 de Marzo de 2014]. Disponible en la Web: http://ingenieriasocialsigloxxi.wordpress.com/category/6-como-evitar-la-ing-social/

- "What is Social Engineering?" SECURITY THROUGH EDUCATION [en línea]. [Consultado 14 de Marzo de 2014]. Disponible en la Web: http://www.social-engineer.org/about/

- "Ingeniería social, hackeando a personas" KASPERSKY lab [en línea]. [Consultado 14 de Marzo de 2014]. Disponible en la Web: http://blog.kaspersky.es/ingenieria-social-hackeando-a-personas/

- "Ingeniería Social: El eslabón más débil en la Cadena de Seguridad de toda organización" Business Transformation [en línea]. [Consultado 14 de Marzo de 2014]. Disponible en la Web: http://web1.gbm.net/bt/bt51/tendencias/ingenieria-social.php